DES-7200

Configuration Guide

Version 10.3(5)

D-Link®

DES-7200 Configuration Guide

Revision No.: Version 10.3(5)
Date: 2009/12/31

Preface

Version Description

This manual matches the firmware version 10.3(5).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

Contents

1 Command Line Interface Configuration

This chapter describes the method to use the command line interface(CLI). You can manage network devices by the command line interface.

This chapter covers the following topics:

- Command Mode
- Getting Help
- Abbreviating Commands
- Using **no** and **default** Options
- Understanding CLI Error Messages
- Using History Commands
- Using Editing Features
- Filtering and Looking Up CLI Output Information
- Using Command Alias
- Accessing CLI

1.1 Command Mode

The management interface of the DES-7200 series switch falls into multiple modes. The command mode you are working with determines the commands you can use.

To list the usable commands in each mode, enter a question mark (?) at the command prompt.

After setting up a session connection to the network device management interface, you enter in the user EXEC mode first. In the user EXEC mode, only a few commands are usable with limited functions, for example, command **show**. The command results are also not saved.

To use all commands, enter the privileged EXEC mode with the privileged password. Then you can use all privileged commands and enter the global configuration mode.

Using commands in a configuration mode (for instance, global configuration or interface configuration) will influence the current configuration. If you have saved the configuration information, these commands will be saved and executed when the system restarts. To enter any of the configuration modes, first enter the global configuration mode.

The following table lists the command modes, access methods, prompts, and exit methods. Suppose the equipment is named "*DES-7210*" by default.

Summary of main command modes:

Command mode	Access method	Prompt	Exit or enter the next mode	Remark

Command mode	Access method	Prompt	Exit or enter the next mode	Remark
User EXEC	Log in.	DES-7210 >	Enter command **exit** to quit this mode. Enter command **enable** to enter the privileged EXEC mode.	Used for basic test and showing system information
Privileged EXEC	In the user EXEC mode, enter command **enable** .	DES-7210 #	To return to the user EXEC mode, enter command **disable**. To enter the global configuration mode, enter command **configure**.	Verify settings. This mode is password-protected.
Global configuration	In the privileged EXEC mode, enter command **configure terminal**.	DES-7210 (config)#	To return to the privileged EXEC mode, enter command **end** or **exit** or press Ctrl+C. To access the interface configuration mode, enter command **interface** with an interface specified. To access the VLAN configuration mode, enter command **vlan** *vlan_id*.	In this mode, you can execute commands to configure global parameters influencing the whole switch.
Interface configuration	In the global configuration mode, enter command **interface**.	DES-7210 (config-if)#	To return to the privileged EXEC mode, enter command **end** or press Ctrl+C. To return to the global configuration mode, enter command **exit**. Moreover, you need specify an interface in the **interface** command.	Configure various interfaces of the equipment in this mode.
Config-vlan (Vlan Mode)	In the global configuration mode, enter command **vlan** vlan-id.	DES-7210 (config-vlan)#	To return to privileged EXEC mode, enter command **end** or press Ctrl+C. To return to the global configuration mode, enter command **exit**.	Configure VLAN parameters in this mode.

1.2 Getting Help

To obtain a list of commands that are available for each command mode, enter a question mark(?) at the command prompt. You can also obtain a list of command keywords beginning with the same character or parameters of each command. See the following table.

Command	Description
Help	Obtain the brief description of the help system under any command mode.
abbreviated-command-entry?	Obtain a list of commands that begin with a particular character string.(Do not leave a space between the keyword and question mark.) For example: DES-7210# **di?** dir disable
abbreviated-command-entry <Tab>	Complete a partial command name. For example: DES-7210# **show conf<Tab>** DES-7210# **show configuration**

Command	Description
Command ?	List a command's associated keywords.(Leave a space between the keyword and question mark.) For example: DES-7210# **show ?**
command keyword ?	List a command's associated arguments.(Leave a space between the keyword and question mark.) For example: DES-7210(config)# **snmp-server community ?** WORD SNMP community string

1.3 Abbreviating Commands

To abbreviate a command, simply enter part of the command that can uniquely identify the command.

For example, **show configuration** can be abbreviated as:

```
DES-7210# show config
```

If the entered command cannot be uniquely identified by the system, the system will prompt "Ambiguous command:".

For example, when you want to view the information about access lists, the following command is not complete.

```
DES-7210# show access
% Ambiguous command: "show access"
```

1.4 Using no and default Options

Almost all commands have the **no** option generally used to disable a feature or function or perform a reversed action of the command. For example, the **no shutdown** command turns on the interface, the opposite operation of the **shutdown** command. You can use the commands without the **no** option to enable the features that have been disabled or are disabled by default.

Most configuration commands have the **default** option that restores the command setting to its default. Most commands are disabled by default. In this case, the **default** and **no** options generally serve the same purpose. However, some commands are enabled by default. In this case, the **default** and **no** options serve different purposes, where the **default** option enables the command and restores the arguments to the default settings.

1.5 Understanding CLI Error Messages

The following table lists the error prompt messages that may occur when you use the CLI to manage equipments.

Common CLI error messages:

Error message	Meaning	How to obtain help
% Ambiguous command: "show c"	The switch cannot identify the unique command for you input insufficient characters.	Re-input the command with a question mark following the ambiguous word. The possible keywords will be listed.
% Incomplete command.	User has not input the required keywords or arguments.	Re-input the command with a space followed by a question mark. The possible keywords or arguments will be displayed.
% Invalid input detected at '^' marker.	The symbol "^" will indicate the position of the wrong words when user inputs a wrong command.	Input a question mark at the command prompt to show the allowed keywords of the command.

1.6 Using Historical Commands

The system records the commands you have input recently, which is very useful when you input a long and complex command again.

To re-execute the commands you have input from the historical records, perform the following operations.

Operation	Result
Ctrl-P or **Up**	Allows you to browse the previous command in the historical command records.
Ctrl-N or **Down**	Allows you to return to a more recent command in the historical command records.

Note

Standards-based terminals like VT100 series support arrow keys.

1.7 Using Editing Features

This section describes the editing functions that may be used for command line edit, including:

- Edit Shortcut Keys
- Sliding Window of Command Line

1.7.1 Editing Shortcut Keys

The following table lists the edit shortcut keys.

Function	Shortcut Key	Description
Move cursor in an editing line	Left direction key or Ctrl+B	Move the cursor to left by one character.
	Right direction key or Ctrl+F	Move the cursor to right by one character.
	Ctrl+A	Move the cursor to the beginning of the command line.
	Ctrl+E	Move the cursor to the end of the command line.
Delete the	Backspace	Delete the character to the left of the cursor.

Function	Shortcut Key	Description
entered characters	Delete	Delete the character where the cursor is located.
Scroll up by one line or one page	Return	Scroll up the displayed contents by one line and make the next line appear. This is used only before the end of the output.
	Space	Scroll up the displayed contents by one page and make the next page appear. This is used only before the end of the output.

1.7.2 Sliding Window of Command Line

You can use the sliding window to edit the commands that exceed the width of one line. When the editing cursor closes to the right border, the whole command line will move to the left by 20 characters. In this case, the cursor can still be moved back to the previous character or the beginning of the command line.

When editing a command line, you can move the cursor using the shortcut keys in the following table:

Function	Shortcut key
Move the cursor to the left by one character	Left direction key or Ctrl+B
Move the cursor to the head of a line	Ctrl+A
Move the cursor to the right by one character	Right direction key or Ctrl+F
Move the cursor to the end of a line	Ctrl+E

For example, the contents of the **mac-address-table static** command may exceed the screen width. When the cursor approaches the line end for the first time, the whole line move left by 20 characters, and the hidden beginning part is replaced by "$" on the screen. The line moves left by 20 characters when the cursor reaches the right border.

```
mac-address-table  static  00d0.f800.0c0c  vlan  1  interface
$tatic  00d0.f800.0c0c  vlan  1  interface  fastEthernet
$tatic  00d0.f800.0c0c  vlan  1  interface  fastEthernet  0/1
```

Now you can press **Ctrl+A** to return to the beginning of the command line. In this case, the hidden ending part is replaced by "$".

```
-address-table  static  00d0.f800.0c0c  vlan  1 interface  $
```

Note

The default line width on the terminal is 80 characters.

Combined with historical commands, the sliding window enables you to invoke complicated commands repeatedly. For details about shortcut keys, see Edit Shortcut Keys.

1.8 Filtering and Looking UP CLI Output Information

1.8.1 Filtering and Looking Up the Information Outputted by the Show Command

To look up the specified message in the information outputted by the **show** command, execute the following command:

Command	Description
DES-7210# **show** *any-command* | **begin** *regular-expression*	Look up the specified content from the information outputted by the **show** command and output all information of the first line that contains this content and subsequent lines.

Caution

1.You can execute **show** command in any mode.

2.The information to be looked up is case sensitive, and the following is the same.

To filter the specified content in the information outputted by the **show** command, execute the following commands:

Command	Description
DES-7210# **show** *any-command* **| exclude** *regular-expression*	Filter the content from the information outputted by the **show** command and output other information excluding the line that includes the specified content.
DES-7210#**show** *any-command* **| include** *regular-expression*	Filter the content from the information outputted by the **show** command and output the line that includes the specified content. Other information will be filtered.

Note

To look up and filter the contents outputted by the **show** command, it is necessary to input the pipeline sign (vertical line, "|") followed by lookup and filtration rules and contents (characters or strings). The contents to be looked up and filtered are case sensitive.

1.9 Using Command Alias

The system provides the command alias function. Any word can be specified as the alias of a command. For example, you can define the word "mygateway" as the alias of "ip route 0.0.0.0 0.0.0.0 192.1.1.1". Inputting this word is equal to inputting the whole string.

You can use one word to replace one command by configuring an alias for the command. For example, you can define an alias to represent the front part of one command, and then continue to enter the following part.

The command that an alias represents must run under the mode you have defined in the current system. In the global configuration mode, you can enter **alias?** to list all command modes that can configure alias.

```
DES-7210(config)#alias ?

  aaa-gs              AAA server group mode
```

```
  acl                  acl configure mode
  bgp                  Configure bgp Protocol
  config               globle configure mode
.....
```

An alias supports help information. An alias appears with an asterisk (*) before it in the following format:

```
*command-alias=original-command
```

For example, in the EXEC mode, the alias “s” indicates the **show** command by default. Enter “s?” to obtain the help information on the command and the aliases beginning with ‘s’.

```
DES-7210#s?
*s=show  show  start-chat  start-terminal-service
```

If the command that an alias represents has more than one word, the command will be included by the quotation marks. As shown in the following example, configure the alias “sv” to replace the **show version** command in the EXEC mode.

```
DES-7210#s?
*s=show  *sv=”show version” show  start-chat
start-terminal-service
```

An alias must begin with the first character of the command line entered without any blank before it. As shown in the above example, the alias is invalid if you have inputted a blank before the command.

```
DES-7210# s?
show  start-chat  start-terminal-service
```

An alias can also be used to get the help information on obtaining command parameters. For example, the alias “ia" represents “ip address” in the interface configuration mode.

```
DES-7210(config-if)#ia ?
  A.B.C.D  IP address
  dhcp     IP Address via DHCP
DES-7210(config-if)#ip address
```

Here lists the parameter information after the command “**ip address**”, and replaces the alias with the actual command.

An alias must be inputted fully for use. Otherwise, it can not be identified.

Use the **show aliases** command to view the setting of aliases in the system.

1.10 Accessing CLI

Before using CLI, you need to use a terminal or PC to connect with the network device. Power on the network device. After the initialization of hardware and software, you can use CLI. If the network device is used for the first time, you can only connect the network device through the serial port (Console), which is referred to as out-band management. In addition, you can connect and manage the network device through Telnet virtual terminal by performing corresponding configuraitons. In either case, you can access the command line interface.

2 Basic Switch Management Configuration

2.1 Overview

This chapter describes how to manage our switches:

Command Authorization-based Access Control

- Logon Authentication Control
- System Time Configuration
- Scheduled Restart
- System Name and Command Prompt Configuration
- Banner Configuration
- System Information Displaying
- Console Rate Configuration
- Telnet Configuration
- Connection Timeout Configuration
- Commands Execution in Batch in the Executable File
- Service Switch Configuration

Note

For more information about the usage and description of the CLI commands mentioned in this chapter, see the *Reference Configuration of Switch Management Command*.

2.2 Command Authorization-based Access Control

2.2.1 Overview

A simple way to manage the terminals' access to a network is to use passwords and assign privileged levels. Password restricts access to a network or network devices. Privileged levels define the commands users can use after they have logged in to a network device.

From the perspective of security, password is stored in the configuration file. Password must be safe when the configuration file is transmitted, for example, over TFTP, across a network. Password is encrypted before being stored into the configuration file, and the clear text password is changed to the cipher text password. The **enable secret** command uses a private encryption algorithm.

2.2.2 Configuring Default Password and Privileged Level

No password at any level is configured by default. The default priviledged level is 15.

2.2.3 Configuring/Changing the Passwords at Different Levels

Our prodects provide the following commands for configuring or changing the passwords at different levels.

Command	Purpose
DES-7210(config)# **enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*}	Set a static password. You can only set a level-15 password only when no level-15 security password is configured. If a non- level -15 password is set, the system will show a prompt and automatically convert it into a security password. If you have set the same level-15 static password as the level 15 security password, the system will show a warning message.
DES-7210(config)# **enable secret** [**level** *level*] {*encryption-type encrypted-password*}	Set the security password, which has the same function but better password encryption algorithm than the static password. For the purpose of security, it is recommended to use the security password.
DES-7210# **enable** [*level*], and DES-7210# **disable** [*level*]	Switch over between user levels. To switch over from a lower level to a higher level, you need to input the password for the higher level.

During the process of setting a password, the keyword "**level**" is used to define the password for a specified privileged level. After setting, it is only applicable for the users who are at that level.

2.2.4 Configuring Multiple Privileged Levels

By default, the system has only two password-protected levels: normal user (level 1) and privileged user (level 15). You can configure up to 16 hierarchical levels of commands for each mode. By configuring different passwords at different levels, you can use different sets of commands by different levels.

When no password is set for the privileged user level, you can enter the privileged mode without password authentication. For security, you are recommended to set the password for the privileged user level.

2.2.4.1 Configuring Command Authorization

To expand the usage range of a command, you can assign it to the users at lower level. On contrary, to narrow the usage range of a command, you can assign it to the users at higher level.

You can use the following commands to authorize users to use a command:

Command	Purpose
DES-7210# **configure terminal**	Enter the global configuration mode.

Command	Purpose
DES-7210(config)# **privilege mode** [**all**] {**level** *level* **| reset**} *command-string*	Set the privileged level for a command. **mode** – The CLI command mode at which you are authorizing the command. For example, **config** indicates the global configuration mode, **exec** indicates the privileged command mode, and **interface** indicates the interface configuration mode. **all** – Change the privileges of all the sub-commands of the specified commands into the same level. **level** *level* – Authorization level in the range from 0 to 15. **Level** 1 is for the normal user level. **Level** 15 is for the privileged user level. You can switch over between various levels by using the **enable/disable** command. *command-string* - The command to be authorized.

To restore the configuration for a specified command, use the **no privilege mode** [**all**] **level** *level command* in the global configuration mode.

2.2.4.2 Example of Command Authorization Configuration

The following is the configuration process that sets the **reload** command and all its sub-commands to be level 1, and brings level 1 into effective (by setting the command as "**test**"):

```
DES-7210# configure terminal
DES-7210(config)# privilege exec all level 1 reload
DES-7210(config)# enable secret level 1 0 test
DES-7210(config)# end
```

Enter the level 1, you can see the command and its subcommands:

```
DES-7210# disable 1
DES-7210> reload ?
  at                  reload at a specific time/date
  cancel               cancel pending reload scheme
  in                  reload after a time interval
  <cr>
```

The following is the configuration process that restores the privilege settings of the **reload** command and all its sub-commands to the default value:

```
DES-7210# configure terminal
DES-7210(config)# privilege exec all reset reload
DES-7210(config)# end
```

Enter the level 1, the privilege setting for the command is removed.

```
DES-7210# disable 1
DES-7210> reload ?
% Unrecognized command.
```

2.2.5 Configuring Line Password Protection

Our products offer password authentication for remote logons (such as Telnet). A password is required for the protection purpose. Execute the following command in the line configuration mode:

Command	Purpose
DES-7210(config-line)# **password** *password*	Specify a line password.
DES-7210(config-line)# **login**	Enable the line password protection.

Note

If no logon authentication is configured, the password authentication on line layer will be ignored even when the line password is configured. The logon authentication will be described in the next section.

2.2.6 Supporting Session Locking

Our products allow you to lock the session terminal temporarily using the **lock** command, so as to prevent access. To this end, enable the terminal locking function in the line configuration mode, and lock the terminal using the **lock** command in the EXEC mode of the terminal:

Command	**Purpose**
DES-7210(config-line)# **lockable**	Enable the function of locking the line terminal
DES-7210# **lock**	Lock the current line terminal

2.3 Logon Authentication Control

2.3.1 Overview

In the previous section, we have described how to control the access to network devices by configuring the locally stored password. In addition to line password protection and local authenticaion, in AAA mode, we can authenticate users' management privilege based on their usernames and passwords on some servers when they log on to the switch, take RADIUS server for example.

With RADIUS server, the network device sends the encrypted user information to the RADIUS server for authentiction rather than autenticates them with the locally stored credentials. The RADIUS server configures user information consistently like user name, password, shared key, and access policy to facilitate the management and control of user access and enhance the security of user informaiton.

2.3.2 Configuring Local Users

Our products support local database-based identify authentication system used for local authentication of the method list in AAA mode and local authentication of line login management in non-AAA mode.

To enable the username identity authentication, run the following specific commands in the global configuration mode:

Command	**Function**
DES-7210(config)# **username** *name* [**password** *password* | **password** *encryption-type encrypted password*]	Enable the username identity authentication with encrypted password.
DES-7210(config)# **username** *name* [**privilege** *level*]	Set the privilege level for the user (optional).

2.3.3 Configuring Line Logon Authentication

To enable the line logon identity authentication, run the following specific commands in the line configuration mode:

Command	Function
DES-7210(config-line)# **login local**	Set local authentication for line logon in non-AAA mode.
DES-7210(config-line)# **login authentication** {**default** | *list-name*}	Set AAA authentication for line logon in AAA mode. The authentication methods in the AAA method list will be used for authentication, including Radius authentication, local authentication and no authentication.

Note

For more information on how to set AAA mode, configure Radius service and configure the method list, see the sections for AAA configuration.

2.4 System Time Configuration

2.4.1 Overview

Every switch has its system clock, which provides date (year, month, day) and time (hour, minute, second) and week. When you use a switch for the first time, you must configure the system clock manually. Of course, you can adjust the system clock when necessary. System clock is used for such functions as system logging that need recording the time when an event occurs.

2.4.2 Setting System Time and Date

You can configure the system time on the network device manually. Once configured, the clock will be running continuously even if the network device is powered off. Therefore, unless you need to modify the time of device, it is not necessary to configure the time again.

However, for the network devices that don't provide the hardware clock, manually setting time actually configures software clock, which only takes effect for this operation. When the network devices are powered off, the manually set time will not be valid.

Command	Function
DES-7210# **clock set** *hh:mm:ss month date day year*	Set system date and time.

For example, change the system time to10:10:12, 2003-6-20:

```
DES-7210# clock set 10:10:12 6 20 2003                //Set system time and date.
DES-7210# show clock              //Confirm the modification takes effect.
clock: 2003-6-20 10:10:54
```

2.4.3 Showing System Time and Date

You can show system time and date by using the **show clock** command in the privileged mode. The following is the format:

```
DES-7210# sh clock                    //Show the current system time and date.
clock: 2003-5-20 11:11:34
```

2.4.4 Updating Hardware Clock

Some platforms use hardware clock (calendar) to implement software clock. Since battery enables hardware clock to run continuously, even though the device is closed or restarts, hardware clock still runs.

If hardware clock and software clock are asynchronous, then software clock is more accurate. Execute **clock update-calendar** command to copy date and time of software clock to hardware clock.

In the privileged mode, execute **clock update-calendar** command to make software clock overwrite the value of hardware clock.

Command	Function
DES-7210# **clock update-calendar**	Update hardware clock via software clock.

Execute the command below to copy current date and time of software clock to hardware clock.

```
DES-7210# clock update-calendar
```

2.5 Scheduled Restart

2.5.1 Overview

This section describes how to use the **reload** [*modifiers*] command to schedule a restart scheme to restart the system at the specified time. This function facilitates user's operation in some circumstance (for the purpose of test, for example). *Modifiers* is a set of options provided by the **reload** command, making the command more flexible. The optional *modifiers* includes **in**, **at** and **cancel**. The following are the details:

1. **reload in** *mmm* | *hhh:mm* [*string*]

This command sets the system restart in fixed intervals in the format of *mmm* or *hhh:mm*. *string* is a help prompt. You can give the scheme a memorable name by the string to indicate its purpose. string is a prompt. For example, to reload the system at the interval of 10 minutes for test, type **reload in *10 test***.

2. **reload at** *hh:mm day month year* [*string*]

This command sets the system restart at the specified time in the future ,which must not be more than 200 days from the curent system time . The usage of *string* is just like above. For example, if the current system time is 14:31 on January 10, 2005, and you want the system to reload tomorrow, you can input **reload at *08:30 11 1 2005 newday***. If the current system time is 14:31 on December 10, 2005, and you want the system to reload at 12:00 a.m. on January 1, 2006, you can input **reload at *12:00 1 1 2006 newyear.***

3. **reload cancel**

This command deletes the restart scheme specified by the user. As mentioned above, you have specified the system to reload at 8:30 a.m. tomorrow, the setting will be removed after you input **reload cancel**.

Note

Only if the system supports clock function can users use option **at**. Before the use, it is recommended to configure the system clock according to your needs. If a restart scheme has been set before, the subsequent settings will overwrite the previous settings. If the user has set a restart scheme and then restarts the system before the scheme takes effect, the scheme will be lost.

The span from the time in the restart scheme to the current time shall be within 200 days and must be greater than the current system time. Besides, after you set reload, you should not set the system clock. Otherwise, your setting may fail to take effect, such as setting system time after reload time.

2.5.2 Specifying the System to Restart at the Specified Time

In the privileged mode, you can configure the system reload at the specified time using the following commands:

Command	Function
DES-7210# **reload at** *hh:mm day month year* [*reload-reason*]	The system will reload at hh:mm,month day,year. *reload-reason* (if any) indicates the reason that the system reloads.

The following is an example specifying the system reload at 12:00 a.m. January 11, 2005 (suppose the current system clock is 8:30 a.m. January 11,2005):

```
DES-7210# reload at 12:00 1 11 2005 midday   //Set the reload time and date.
DES-7210# show reload                        //Confirm the modification takes effect.
Reload scheduled for 2005-01-11 12:00  (in 3 hours 29 minutes)16581 seconds.
At 2005-01-11 12:00
Reload reason: midday
```

2.5.3 Specifying the System to Restart after a Period of Time

In the privileged mode, you can configure the system reload in the specified time with the following commands:

Command	Function
DES-7210# **reload in** *mmm* [*reload-reason*]	Configure the system reload in *mmm* minutes, where the reload reason is described in *reload-reason* (if inputted)
DES-7210# **reload in** *hhh:mm* [*reload-reason*]	Configure the system reload in *hhh* hours and *mm* minutes, where the reload reason is described in *reload-reason* (if inputted)

The following example shows how to reload the system in 125 minutes (assumes that the current system time is 12:00 a.m. January 10, 2005):

```
DES-7210# reload in 125 test    //Set the system reload time
```

Or

```
DES-7210# reload in 2:5 test    //Set the system reload time
DES-7210# show reload           //Confirm whether the restart time change takes effect
Reload scheduled System will reload in 2 hours and 4 minutes7485 seconds.
```

2.5.4 Immediate Restart

The **reload** command without any parameters will restart the device immediately. In the privileged mode, the user can restart the system immediately by typing the **reload** command.

2.5.5 Deleting the Configured Restart Scheme

In the privileged mode, use the following command to delete the configured restart scheme:

Command	Function
DES-7210# **reload cancel**	Delete the configured restart scheme.

If no reload scheme is configured, you will see an error message for the operation.

2.6 Configuring a System Name and Prompt

2.6.1 Overview

For easy management, you can configure a system name for the switch to identify it. If you configure a system name of more than 32 characters, the first 32 characters are used as the system prompt. The prompt varies with the system name. By default, the system name and command prompt are specific device names, for example "DES-7210".

2.6.2 Configuring a System Name

Our products provide the following commands to configure a system name in the global configuration mode:

Command	Function
DES-7210(Config)# **hostname** *name*	Configure a system name with printable characters less than 255 bytes.

To restore the name to the default value, use the **no hostname** command in the global configuration mode. The following example changes the equipment name to D-Link:

```
DES-7210# configure terminal        //Enter the global configuration mode.
DES-7210(config)# hostname D-Link  //Set the equipment name to D-Link
D-Link(config)#                     //The name has been modified successfully.
```

2.6.3 Configuring a Command Prompt

System name will be the default prompt if you have not configured command prompt. (if the system name exceeds 32 characters, intercept the first 32 characters) The prompt varies with the system name.You can use the **prompt** command to configure the command prompt in the global configuration mode, and the command prompt is only valid in the EXEC mode.

Command	Function
DES-7210# **prompt** *string*	Set the command prompt with printable characters. If the name exceeds 32 characters, intercept the first 32 characters.

To restore the prompt to the default value, use the **no prompt** command in the global configuration mode.

2.7 Banner Configuration

2.7.1 Overview

When the user logs in the switch, you may need to tell the user some useful information by configuring a banner. There are two kinds of banners: message-of-the-day (MOTD) and login banner. The MOTD is specific for all users who connect with switches. And when users log in the switch, the notification message will appear on the terminal. MOTD allows you send some urgent messages (for example, the system is to be shut down) to network users. The login banner also appears on all connected terminals. It provides some common login messages. By default, the MOTD and login banner are not configured.

2.7.2 Configuring a Message-of-the-Day

You can create a notification of single or multi-line messages that appears when a user logs in the switch. To configure the message of the day, execute the following commands in the global configuration mode:

Command	Function
DES-7210(Config)# **banner motd** *c message c*	Specify the message of the day, with c being the delimiter, for example, a pound sign (&). After inputting the delimiter, press the **Enter** key. Now, you can start to type text. You need to input the delimiter and then press **Enter** to complete the type. Note that if you type additional characters after the end delimiter, these characters will be discarded by the system. Also note that you cannot use the delimiter in the message and the message length should be no more than 255 bytes.

To delete the MOTD, use the **no banner motd** command in the global configuration mode. The following example describes how to configure a MOTD. The # symbol is used as the delimiter, and the text is “Notice: system will shutdown on July 6th.”

```
DES-7210(config)# banner motd #                          //Start delimiter.
Enter TEXT message.  End with the character '#'.
Notice: system will shutdown on July 6th.#              //End delimiter.
DES-7210(config)#
```

2.7.3 Configuring a Login Banner

To configure a login banner, executing the following commands in the global configuration mode:

Command	Function
DES-7210(Config)# **banner login** *c message c*	Specify the text of the login banner, with c being the delimiter, for example, a pound sign (&). After inputting the delimiter, press the **Enter** key. Now, you can start to type text. You need to input the delimiter and then press **Enter** to complete the type. Note that if you type additional characters after the end delimiter, these characters will be discarded by the system. Also note that you cannot use the delimiter in the text of the login banner and the text length should be no more than 255 bytes.

To delete the login banner, use the **no banner login** command in the global configuration mode.

The following example shows how to configure a login banner. The pound sign (#) is used as the starting and end delimiters and the text of the login banner is "Access for authorized users only. Please enter your password."

```
DES-7210(config)# banner login #      //Start delimiter
Enter TEXT message. End with the character '#'.
Access for authorized users only. Please enter your password.
#                                     //End delimiter
DES-7210(config)#
```

2.7.4 Displaying a Banner

A banner is displayed when you log in the network device. See the following example:

```
C:\>telnet 192.168.65.236
 Notice: system will shutdown on July 6th.
 Access for authorized users only. Please enter your password.
 User Access Verification
Password:
```

As you can see, “Notice: system will shutdown on July 6th." is a MOTD banner and "Access for authorized users only. Please enter your password." is a login banner.

2.8 Viewing System Information

2.8.1 Overview

You can view some system information with the **show** command on the command-line interface, such as version, device information, and so on.

2.8.2 Viewing System Information and Version

System information consists of description, power-on time, hardware version, software version, BOOT-layer software version, CTRL-layer software version, and so on. System information helps you know the system You can show the system information with the following commands in the privileged mode.

Command	Function
DES-7210# **show version**	Show system information.

2.8.3 Viewing Hardware Entity Information

Hardware information refers to the information on physical devices as well as slots and modules assembled in a device. The information on a device itself includes description, number of slots,slot information, slot number, description of the module on the slot (empty description if no module is plugged on the slot), number of physical ports of the module on the slot, and maximum number of ports possibly supported on the slot (number of ports of the module plugged). You may use the following commands to show the information of the device and slots in the privileged mode:

Command	Function
DES-7210# **show version devices**	Show device information.
DES-7210# **show version slots**	Show the information about slots and modules.

2.9 Setting Console Rate

2.9.1 Overview

The switch comes with a console interface for management. When using the switch for the first time, you need to execute configuration through the console interface.You can change the console rate on the equipment if necessary. Note that the rate of the terminal used to managing the switch must be the same as that of the console interface on the switch.

2.9.2 Setting Console Rate

In the line configuration mode, execute the following command to set the console rate:

Command	Function
DES-7210(config-line)# **speed** *speed*	Set transmission rate in bps on the console interface. For a serial interface, you can only set the transmission rate to one of 9600, 19200, 38400, 57600 and 115200 bps, with 9600 bps by default.

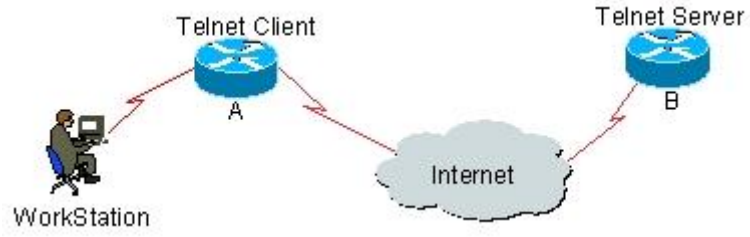
This example shows how to configure the baud rate of the serial interface to 57600 bps:

```
DES-7210# configure terminal              //Enter the global configuration mode.
DES-7210(config)# line console 0          //Enter the console line configuration mode
DES-7210(config-line)# speed 57600        //Set the console rate to 57600bps
DES-7210(config-line)# end                //Return to the privileged mode
DES-7210# show line console 0             //View the console configuration
CON     Type    speed   Overruns
* 0     CON     57600   0
Line 0, Location: "", Type: "vt100"
Length: 25 lines, Width: 80 columns
Special Chars: Escape  Disconnect  Activation
             ^^x     none       ^M
Timeouts:    Idle EXEC    Idle Session
             never         never
History is enabled, history size is 10.
Total input: 22 bytes
Total output: 115 bytes
Data overflow: 0 bytes
stop rx interrupt: 0 times
Modem: READY
```

2.10 Configuring Telnet

2.10.1 Overview

Telnet, an application layer protocol in the TCP/IP protocol suite, provides the specifications of remote logon and virtual terminal communication functions. The **Telnet Client** service is used by the local or remote user who has logged onto the local network device to work with the Telnet Client program to access other remote system resources on the network. As shown below, after setting up a connection with Switch A through the terminal emulation program or Telnet, users can log on the Switch B for management and configuration with the **telnet** command.



2.10.2 Using Telnet Client

You can log in to a remote device by using the **telnet** command on the switch.

Command	Function
DES-7210# **telnet** *host-ip-address*	Log on to a remote device via Telnet. *host-ip-address* may be the host name or IP address.

The following example shows how to establish a Telnet session and manage the remote device with the IP address 192.168.65.119:

```
DES-7210# telnet 192.168.65.119    //Establish the telnet session to the remote device
Trying 192.168.65.119 ... Open
User Access Verification      //Enter into the logon interface of the remote device
Password:
```

2.11 Setting Connection Timeout

2.11.1 Overview

You can control the connections that a device has set up (including the accepted connections and the session between the devece and a remote terminal) by configuring the connection timeout time for the device. When the idle time exceeds the set value and there is no input or output, this connection will be interrupted.

2.11.2 Connection Timeout

When there is no information traveling through an accepted connection within a specified time, the server will interrupt this connection.

Our products provide commands to configure the connection timeout in the line configuration mode.

Command	Function
DES-7210(Config-line)#**exec-timeout** *20*	Configure the timeout for the accepted connection. When the configured time is due and there is no input, this connection will be interrupted.

The connection timeout setting can be removed by using the **no exec-timeout** command in the line configuration mode.

```
DES-7210# configure terminal            //Enter the global configuration mode.
DES-7210# line vty 0                    //Enter the line configuration mode
DES-7210(config-line)#exec-timeout 20   //Set the timeout to 20min
```

2.11.3 Session Timeout

When there is no input for the session established with a remote terminal over the current line within the specified time, the session will be interrupted and the remote terminal becomes idle.

The DES-7200 series provides commands in the line configuration mode to configure the timeout for the session set up with the remote terminal.

Command	Function
DES-7210(Config-line)#**session-time out** *20*	Configure the timeout for the session set up with the remote terminal over the line. If there is no input within the specified time, this session will be interrupted.

The timeout setting for the session set up with the remote terminal over the line can be removed by using the **no exec-timeout** command in the line configuration mode.

```
DES-7210# configure terminal              //Enter the global configuration mode.
DES-7210(config)# line vty 0              //Enter the line configuration mode
DES-7210(config-line)# session-timeout 20   //Set the session timeout to 20min
```

2.12 Executing the Commands in the Executable File in Batch

In system management, sometimes it is necessary to enter multiple configuration commands to manage a function. It takes a long period of time to enter all the commands on CLI, causing error or mission. To resolve this problem, you can encapsulate all the commands in a batch file according to configuration steps. Then, you can execute the batch file for configuration when necessary.

Command	Function
DES-7210# **execute {[flash:]** *filename***}**	Execute a batch file.

For example, the batch file line_rcms_script.text enables the reversed Telnet function on all the asynchronous interfaces as shown below:

```
configure terminal
line tty 1 16
transport input all
no exec
end
```

Result:

```
DES-7210# execute flash:line_rcms_script.text
executing script file line_rcms_script.text ......
executing done
DES-7210# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# line vty 1 16
DES-7210(config-line)# transport input all
DES-7210(config-line)# no exec
DES-7210(config-line)# end
```

Note

The file name and contents of a batch file can be specified. Once edited, users send the batch file to the FLASH of the network device in TFTP. The contents of the batch file will simulate the input completely. Hence, it is necessary to edit the contents of the batch file by the sequence that CIL commands are configured. Furthermore, for some interactive commands, it is necessary to write corresponding response information in the batch file, guaranteeing that the commands can be executed normally.

2.13 Setting Service Switch

During operation, you can adjust services dynamically, enabling or disabling specified services (SSH Server/Telnet Server/Web Server).

Command	Function
DES-7210(Config)# **enable service ssh-sesrver**	Enable SSH Server.
DES-7210(Config)# **enable service telnet-server**	Enable Telnet Server
DES-7210(Config)# **enable service web-server**	Enable Http Server.

In the configuration mode, you can use the **no enable service** command to disable corresponding services.

```
DES-7210# configure terminal                //Enter the global configuration mode.
DES-7210(config)# enable service ssh-server     //Enable SSH Server
```

3 LINE Mode Configuration

3.1 Overview

This chapter describes some operations in LINE mode:

- Enter the LINE mode
- Increase/decrease LINE VTY
- Configure the protocols to communicate on the line
- Configure the ACLs on the line

3.2 Configuring LINE Mode

3.2.1 Entering the LINE mode

After entering the specific LINE mode, you can configure the specified line. Execute the following commands to enter the specified LINE mode:

Command	Function
DES-7210(config)# **line [console | vty]** *first-line* [*last-line*]	Enter the specified LINE mode.

3.2.2 Increasing/Decreasing LINE VTY

By default, the number of line vty is 5. You can execute the following commands to increase or decrease line vty, up to 36 line vty is supported.

Command	Function
DES-7210(config)# **line vty** *line-number*	Increase the number of LINE VTY to the specified value.
DES-7210(config)# **no line vty** *line-number*	Decrease the number of LINE VTY to the specified value.

3.2.3 Configuring the Protocols to Communicate on the Line

To restrain the communication protocol type supported on the line, you can use this command. By default, a VTY supports the communication of all protocols while a TTY do not support the communication of any protocol.

Command	Description
configure terminal	Enter the configuration mode.
line vty *line number*	Enter the line configuration mode.

Command	Description
transport input {**all	ssh	telnet	none**}	Configure the protocol to communicate on the line.
no transport input	Disable the communication of any protocol on the line.
default transport input	Restore the setting to the default value.

3.2.4 Configuring the Access Control List on the Line

To configure the access control list on the line, you can use the command. By default, no access control list is configured on the line.That is, all incoming and outgoing connections are permitted.

Command	Description
configure terminal	Enter the configuration mode.
line vty *line number*	Enter the line configuration mode.
access-class *access-list-number* **{in	out}**	Configure the access control list on the line.
no access-class *access-list-number* **{in	out}**	Remove the configuration.

4 System Upgrade and Maintenance

4.1 Overview

Upgrade and maintenance refers to upgrade the main program or CTRL program or upload and download files on the CLI . There are two ways to upgrade programs: use TFTP through a network interface or use Xmodem protocol through a serial interface.

4.2 Upgrade and Maintenance Method

The following sections describe how to upgrade and maintain the equipment:

- Transfer files by TFTP
- Transfer files by Xmodem

4.2.1 Transferring Files by TFTP

There are two ways to transfer files by TFTP: download files from the host to the equipment, or upload files from the equipment to the host.

In the CLI command mode, download the files by performing the following steps:

Before download, first run the TFTP server software on the local host. Then, select the directory of the file to download. Finally, log in to the equipment. In the privileged mode, download the files by using the following commands. If no location is specified, you need to separately input the IP address of the TFTP server.

Command	Function
DES-7210# **copy tftp:** *//location/ filename* **flash:** *filename* [**vrf** *vrfname*]	Download the specified file from the URL on the host to the equipment.

In the CLI command mode, upload the files by performing the following steps:

Before upload, first run the TFTP server software on the local host. Then, select the destination directory for the file to upload at the host. Finally, upload the files by using the following commands in the privileged mode.

Command	Function
DES-7210# **copy flash:** *filename* **tftp:** *//location/filename* [**vrf** *vrfname*]	Upload the specified file from the equipment to the directory specified by the URL on the host. You can also rename the file.

Caution

It is necessary to put the tftp link in quotes if the filename of the source file has space. For example:

```
copy tftp:"//localtion/filename" flash:filename [vrf vrfname]
```

It is necessary to put the filename in quotes if the filename of the destination file has space. For example:

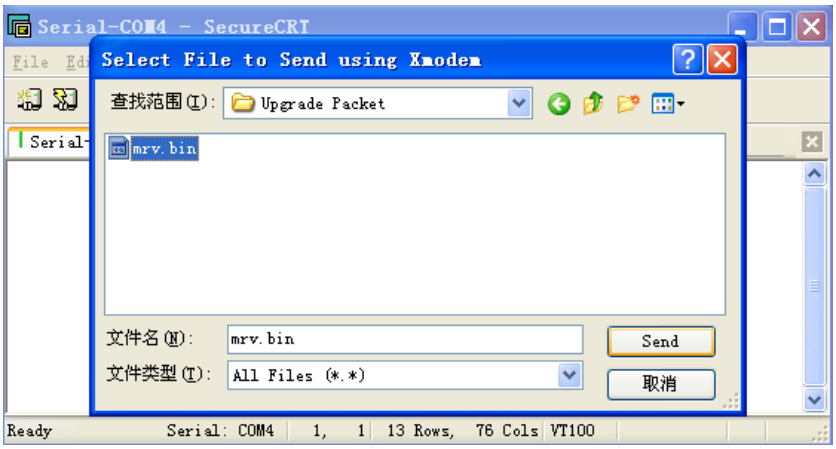
```
copy tftp://localtion/filename flash:"filename" [vrf vrfname]
```

4.2.2 Transferring Files by XMODEM

There are two ways to transfer files by Xmodem: download files from the host to the equipment, or upload files from the equipment to the host.

In the CLI command mode, download the files by performing the following steps:

Prior to download, first log in to the out-band management interface of the device by using the Windows HyperTerminal. Then, download the files by using the following command in the privileged mode. Finally, select the “Send File” from the “Transfer” menu on the Windows HyperTerminal on the local host, as shown in the following figure:

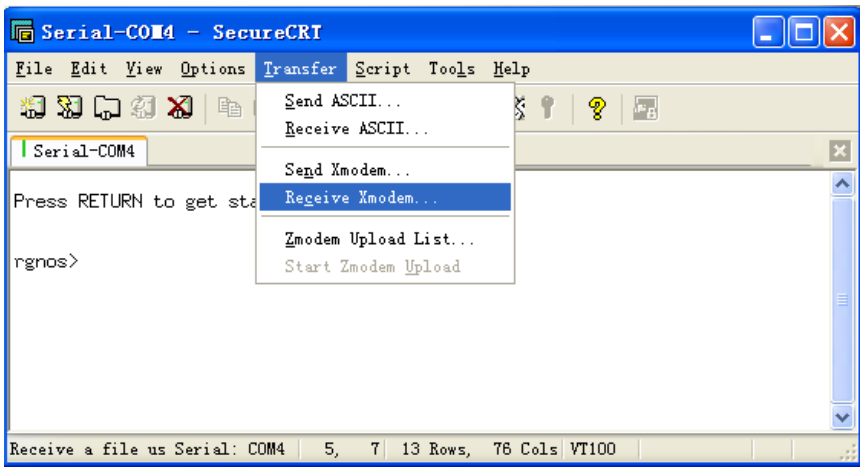


In the pop-up dialog box, select the file to download from the File Name field and Xmodem from the Protocol field. Click “Send”, and the Windows HyperTerminal will show the transmission process and packets.

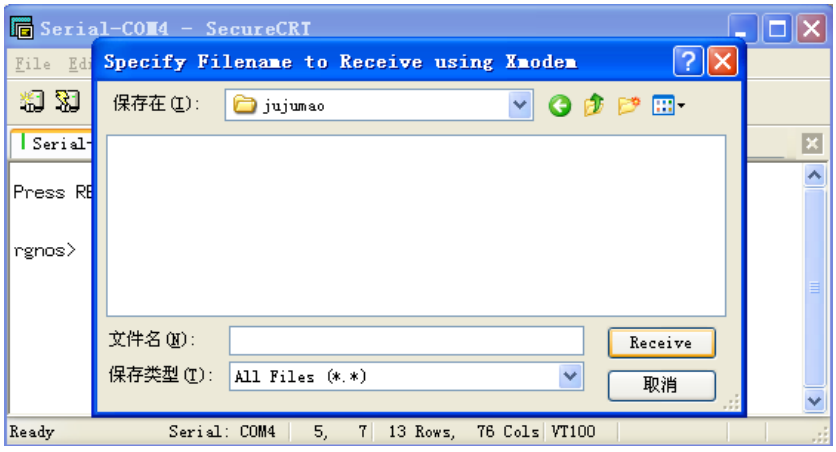
Command	Function
DES-7210# **copy xmodem flash**:*filename*	Download the file from the host to the equipment and name it *filename*.

In the CLI command mode, upload the files by performing the following steps:

Prior to upload, first log in to the out-band management interface of the switch by using the Windows HyperTerminal. Then, upload the files by using the following command in the privileged mode. Finally, select the “Receive File” from the “Transfer” menu on the Windows HyperTerminal on the local host. It’s shown in the following figure:



In the pop-up dialog box, select the storage location for the file to upload and select the "Xmodem" as the reception protocol. Click "Receive", and the Windows HyperTerminal will further prompt the name of the locally stored file. Click "OK" to start reception. The operaton is shown below:



Command	Function
DES-7210# **copy flash**:*filename* **xmodem**	Upload the file from the equipment to the host.

Caution

It is necessary to put the filename with space in quotes. For example:

copy xmodem flash:"filename" OR **copy flash:**"filename" **xmodem**

4.2.3 Upgrading System

You can transfer the upgrading file to a device through TFTP or Xmodem, no matter the device is box-mount or chassis-mount. After transmission, restart the device. The upgrading file will automatically check and upgrade the system without manual interference.

The upgrade procedure on the box-mount equipment is slightly different from that on the chassis-mount equipment:

1. On the box-mount equipment, the upgrading file upgrades only its single supervisor engine. After upgrading, the system automatically resets. The equipment works normally after restart.

2. The chassis-mount equipment includes supervisor engines, line cards and multi-service cards. To upgrade the whole system with a upgrading file, first upgrade the supervisor engine. The system resets. When the equipment restarts, the automatic version synchronization function runs to upgrade line cards and multi-service cards.

Automatic Upgrade: a function running on the supervisor engine that verify the version consistency for the slave supervisor engine, line cards and multi-service cards. When it is found that the version is not consistent with the one in the master supervisor engine, the function sends the upgrading files to those blades for upgrading so as to keep the version consistence in the whole system.

Caution

Whenever you upgrade the master supervisor engine, the slave one (if any) is upgraded at the same time to keep the version consistent. The upgrade of a line card will upgrade all the line cards inserted into the device.Do not power off the device before the upgrade is complete. Otherwise, the upgrade program may be lost.

Before the chassis-mount device is upgraded, you can check whether the software version of all line cards and supervisor engines are consistent with the upgraded object version by the **show version** command. However, you cannot carry out master-slave switch (such as **redundancy force-switchover**). Otherwise, it will cause the upgrade failure and return to the original version.

Note

The upgrade method of the box-mount device is the same as that of the supervisor engine.

4.2.4 Upgrading System by Upgrade Pack

- **What is upgrade pack?**

In essence, upgrade pack is a binary executable file that can be loaded and run as a primary program of a device. The upgrade pack is encapsulated with the BOOT/CTRL/MAIN program of corresponding products. After the upgrade pack runs, it will search for the version information of the BOOT/CTRL/MAIN program of the current system, and compare it with the version of the encapsulated BOOT/CTRL/MAIN program. If the version of some program is not consistent, it will upgrade this program with the encapsulated program. With upgrade packet, you can upgrade the whole system easily.

You can transfer the upgrading file to a device through TFTP or Xmodem, no matter the device is box-mount or chassis-mount. After transport, restart the device. The uprading file will automatically check and upgrade the system without manual interference.

The procedure of upgrade pack on the box-mount equipment is slightly different from that on the chassis-mount equipment:

1. The upgrade pack of the box-mount device upgrades only its board system. Hence, it simply encapsulates its own BOOT/CTRL/MAIN programs. Its upgrade steps are:
   a. Detect and upgrade the BOOT/CTRL in turn.
   b. Decompress the MAIN program and upgrade it as the main program of the device, so as to cover the upgrade pack.
   c. After the upgrade is completed, the system will be reset automatically, and the equipment restarts again and runs normally.
2. The operation of the upgrade pack on the chassis-mount device is more complicated for the chassis-mount device includes the supervisor engine, line card and multi-service card, and needs to carry out the upgrade operation of the whole system by an upgrade

pack. The upgrade pack should encapsulate the BOOT/CTRL/MAIN program of all board cards. In this way, it is necessary to carry out the upgrade and synchronization of the line card individually. The upgrade steps are:

a. Detect and upgrade the BOOT/CTRL of the supervisor engine.

b. Decompress the main program and line card of the supervisor engine to the root directory.

c. After the supervisor engine is upgraded, the system will be reset.

d. When the equipment is rebooted again, the automatic version synchronization function will be enabled to carry out the system upgrade of the line card and the multi-service card.

Automatic Upgrade Function: A function running on the master supervisor engine that verifies the version consistency for the slave supervisor engine, line card and multi-service card. When it found that the version is not consistent with the BOOT/CTRL/MAIN version of the corresponding single board in the master supervisor engine, the function sends the upgrading files to those boards for upgrading so as to keep the version consistence of the whole system.

Caution

The upgrade packs of the supervisor engine, line card and multi-service board decompressed from the upgrade pack on the chassis-mount device (namely the main program of the supervisor engine) cannot be removed or changed at random. Otherwise, the system cannot operate normally.

This upgrade method is applicable for upgrading all versions to 10.1 version.

■ **Upgrade the chassis-mounted device by the upgrade file:**

1. Confirm the filename of the upgrade file to be loaded is **rgos.bin**.
2. Download the file to the device by using the **copy** command.
3. If there is a slave supervisor engine on the device, you need to first upgrade the main programs of the master and slave supervisor engines successfully. After upgrading the main program successfully, the system prompts:

```
Upgrade Slave CM MAIN successful!!
Upgrade CM MAIN successful!!
```

4. Reset the equipment.
5. After reset, the upgrade file will run automatically. The system prompts:

```
Installing is in process ......
Do not restart your machine before finish !!!!!!
......
```

6. After the upgrade operation is completed, the system prompts:

```
Installing process finished ......
Restart machine operation is permited now !!!!!!
```

7. After the operation of the upgrade file is completed, the system resets automatically and prompts:

```
System restarting, for reason 'Upgrade product !'.
```

8. After reset, the upgrading operation of the supervisor engines is completed. The system will load and operate the upgrade pack of boards. Moreover, it prompts informaiton in Steps 5 to 6. Instead of the information in Step 7, it prompts:

```
System load main program from install package ......
```

Load the main program of the supervisor engine to operate from the upgrade file directly.

9. After the main program operates normally, the automatic upgrade function starts. If there is the slave supervisor engine or other modules in the chassis-mount device, the system prompts:

```
A new card is found in slot [1].
System is doing version synchronization checking ......
Current software version in slot [1] is synchronous.
System needn't to do version synchronization for this card ......
```

Or, the system prompts:

```
System is doing version synchronization checking ......
Card in slot [3] need to do version synchronization ......
```

Other Printing Information

```
Version synchronization begain ......
Keep power on, don't draw out the card and don't restart your machine before
finished !!!!!!
```

Other Printing Information

```
Transmission is OK, now, card in slot [3] need restart ...
Software installation of card in slot [3] is in process ......
!!!!!
```

5 Network Communication Detection Tools

5.1 Ping Connectivity Test

To test the connectivity of a network, many network devices support the **Echo** protocol. The protocol sends a special packet to a specified network address and waits for a response. This allows you to evaluate the connectivity, delay and reliability of a network. The ping tool provided by the DES-7200 series can effectively help users diagnose and locate the connectivity problems in a network.

The **Ping** command runs in the user EXEC mode and privileged EXEC mode. In the user EXEC mode, only basic ping functions are available. However, in the privileged EXEC mode, extended ping functions are available.

Command	Function
DES-7210# **ping** [*ip*] [*address* [**length** *length*] [**ntimes** *times*] [**data** *data*][**source** *source*] [**timeout** *seconds*]]	Test the network connectivity.

The basic ping function can be performed in either the user EXEC mode or the privileged EXEC mode. By default, this command sends five 100-byte packets to the specified IP address. If the system receives a response within the specified time (2 seconds by default), it shows "!" . Otherwise, it shows ".". Finally, the system shows statistics. This is a normal ping example:

```
DES-7210# ping 192.168.5.1
Sending 5, 100-byte ICMP Echoes to 192.168.5.1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The extended ping function can be performed in the privileged EXEC mode only. This function allows you specify the number of packets, packet length, and timeout. As with the basic ping function, the extended ping also shows statistics. The following is an example of the extended ping:

```
DES-7210 ping 192.168.5.197 length 1500 ntimes 100 data ffff source 192.168.4.190 timeout
3
Sending 100, 1000-byte ICMP Echoes to 192.168.5.197, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
DES-7210#
```

5.2 Traceroute Connectivity Test

The **Traceroute** command is mainly used to check the network connectivity. It shows all the gateways that a packet passes through from the source to the destination and exactly locates the fault when the network fails.

One of the network transmission rules is that the number in the TTL field in the packet will decrease by 1 every time when a packet passes through a gateway. When the number in the TTL field is 0, the gateway will discard this packet and send an address unreachable error message back to the source. According to this rule, the execution of the traceroute command is as follows: At first, the source sends a packet whose TTL is 1 to the destination address. The first gateway sends an ICMP error message back, indicating that this packet cannot be forwarded for TTL timeout. Then, the first gateway re-sends the packet after the TTL domain adds 1. Likewise, the second gateway returns a TTL timeout error and the process lasts until the packet reaches the destination address. By recording every address returning the ICMP TTL timeout message, you can draw the entire path passed by the IP packet from the source address to the destination address.

The **traceroute** command can run in the user EXEC mode and the privileged EXEC mode. The command format is as follows:

Command	Function
DES-7210# **traceroute** [*protocol*] [*destination*] [**probe** *probe*] [**ttl** *minimum maximum*] [**source** *source*] [**timeout** *seconds*]]	Trace the path that a packet passes through.

The following are two examples that apply **traceroute**. In one example, network connectivity is good. In another example, some gateways in a network are not connected.

- **traceroute** example where network connectivity is good:

```
DES-7210# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36
1     192.168.12.1        0 msec   0 msec   0 msec
2     192.168.9.2         4 msec   4 msec   4 msec
3     192.168.9.1         8 msec   8 msec   4 msec
4     192.168.0.10        4 msec   28 msec  12 msec
5     202.101.143.130     4 msec   16 msec  8 msec
6     202.101.143.154     12 msec  8 msec   24 msec
7     61.154.22.36        12 msec  8 msec   22 msec
```

As you can see, to access the host with an IP address of 61.154.22.36, the network packet passes throuth gateways 1 to 6 from the source address. Meanwhile, you can know the time that the network packet spennds to reach a gateway. This is very useful for network analysis.

- traceroute example where some gateways in a network are not connected:

```
DES-7210# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
1     192.168.12.1        0 msec   0 msec   0 msec
2     192.168.9.2         0 msec   4 msec   4 msec
3     192.168.110.1       16 msec  12 msec  16 msec
4     *  *  *
5     61.154.8.129        12 msec  28 msec  12 msec
6     61.154.8.17         8 msec   12 msec  16 msec
```

```
7     61.154.8.250        12 msec  12 msec  12 msec
8     218.85.157.222      12 msec  12 msec  12 msec
9     218.85.157.130      16 msec  16 msec  16 msec
10    218.85.157.77       16 msec  48 msec  16 msec
11    202.97.40.65        76 msec  24 msec  24 msec
12    202.97.37.65        32 msec  24 msec  24 msec
13    202.97.38.162       52 msec  52 msec  224 msec
14    202.96.12.38        84 msec  52 msec  52 msec
15    202.106.192.226     88 msec  52 msec  52 msec
16    202.106.192.174     52 msec  52 msec  88 msec
17    210.74.176.158      100 msec 52 msec  84 msec
18    202.108.37.42       48 msec  48 msec  52 msec
```

As you can see, to access the host with an IP address of 202.108.37.42, the network packet passes through gateways 1 to 17 from the source address and there is failure in gateway 4.

5.3 Line Detection

The administrator can use command **line-detect** to detect the work status of lines. Line detection can help the administrator judge the work status of lines correctly when the lines are in abnormal status.

In the interface configuration mode, execute command **line-detect**:

Command	Function
DES-7210(config)#**interface** *interface*	Enter the Interface configuration mode.
DES-7210(config-if)# **line-detect**	Detect lines.

Caution

Only L2 exchange ports can support line detection. Optical and AP port can not support line detection.

The following gives an example to execute the command to detect line:

```
DES-7210(config)#inteface gigabitEthernet 3/1
DES-7210(config-if)#line-detect
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state     length(meters)
---- ---------- --------------
A    Ok         2
B    Ok         1
C    Short      1
D    Short      1
```

Command description:

Command	Description

pairs	The number of the line pairs. For example, the twisted pair is composed of four line pairs.
State	1.OK; 2.Short; 3.Open. In normal state, two pairs(A,B) of 100M twisted pair are OK, while other two pairs(C,D) are Short. Four pairs (A,B,C,D) of 1000M twisted pair are OK.
Length	The line length, in meter, takes effect only for the pairs in Ok state. In addition, some inaccuracy is possible because the line length is calculated according to the signal transferring time. The length of lines in Short or Open states refers to the length from the port to the defective line point.

6 Interface Configuration

6.1 Overview of Interface Types

This chapter classifies the interfaces used on DES-7210 devices and defines interface types. Interfaces on DES-7210 devices are divided into two types:

- L2 Interfaces
- L3 Interfaces (supported on layer 3 devices)

6.1.1 L2 Interfaces

This section presents the types of L2 interfaces and their definitions. L2 interfaces fall into the following types

- Switch Port
- L2 Aggregate Ports

6.1.1.1 Switch Port

Switch port refers to a single physical port of only layer 2 switching function on the device. This port can either be an Access Port or a Trunk Port. You can configure a port to be an Access Port or a Trunk Port by using the **Switch Port** command in the interface configuration mode. Switch port is used to manage a physical interface and relevant layer 2 protocols rather than handling routing or bridging.

1.1.1.1.1 Access Port

An access port belongs to only one VLAN that transports only the frames belonging to the same VLAN.Typically, it is used to connect computers.

Default VLAN

An access port belongs to only one VLAN. Therefore, its default VLAN is the VLAN where it locates. You do not need to configure it.

Receiving and sending frames

An access port sends untagged frames and receives frames in the following three formats only:

Untagged frame

- Untagged frames
- Tagged frames whose VID is the VLAN where the access port locates
- Tagged frames whose VID is 0

Untagged frame

An access port receives untagged frames and then adds the tag of the default VLAN to them. The added tag will be removed before the access port sends them out.

Tagged frame

An access port handles tagged frames in the following ways:

- When the VID (VLAN ID) of the tag is the same as the default VLAN ID, the access port receives the frame and removes the tag before sending it out.
- When the VID (VLAN ID) of the tag is 0, the access port receives the frame. In the tag, VID=0 is used to prioritize the frame.
- When the VID (VLAN ID) of the tag is different from the default VLAN ID and is not 0, this frame is discarded.

1.1.1.1.2 Trunk Port

A trunk port can belong to multiple VLANs that receives and sends frames belonging to multiple VLANs. Generally, it is used to connect devices or computers.

Default VLAN

Because a trunk port can belong to multiple VLANs, you need to set a native VLAN as the default VLAN. By default, the trunk port transmits the frames of all VLANs. In order to reduce device load and minimize waste of bandwidth, you can set a VLAN allowance list to specify the frames of which VLANs the trunk port can transmit.

Caution It is recommended to set the native VLAN of the trunk port on the local device to be consistent with that of the trunk port on the remote device. Otherwise, the trunk port cannot forward packets properly.

Receiving and sending frames

The trunk port can receive untagged frames and the tagged frames of the VLANs permitted by the port. All the frames of non-native VLANs sent by the trunk port are tagged, and the frames of native VLAN are untagged.

Untagged frame

If a trunk port receives a frame without IEEE802.1Q TAG, this frame will be transmitted in the native VLAN of the port.

Tagged frame

If a trunk port receives a tagged frame, it handles the frame in the following ways:

- When the trunk port receives a tagged frame whose VID is the same as that of its native VLAN, this frame is accepted. The tag will be removed before it sends the frame.
- When the trunk port receives a tagged frame whose VID is different from that of its native VLAN but is permitted by the port, the frame is accepted. The tag is kept unchanged when it sends the frame.
- When the trunk port receives a tagged frame whose VID is different from that of its native VLAN and is not permitted by the port, the frame is discarded.

Note Untagged packets are ordinary Ethernet packets that can be recognized by the network cards in PCs for communication. Tagging refers to append four bytes of VLAN information, namely the VLAN tag header, at the end of the source MAC address and the destination MAC address.

1.1.1.1.3 Hybrid port

A hybrid port can belong to multiple VLANs that receives and sends packets of multiple VLANs. It can be used to connect devices or computers. The difference between the hybrid port and the trunk port is that the hybrid port sends the untagged frames of multiple VLANs, but the trunk port sends only the untagged frames of the default VLAN. Note that the VLAN that a hybrid port is going to join must already exist.

6.1.1.2 L2 Aggregate Port

An aggregate port consists of several physical ports. Multiple physical connections can be bound into a simple logical connection, which is called an aggregate port (hereinafter referred to as AP).

For layer 2 switching, an AP works like a switch port of high brandwidth. It increases link bandwidth by using the bandwidth of multiple ports together. In addition, the frames that pass through the L2 aggregate port will undergo traffic balancing on the member ports of the L2 aggregate port. If one member link of AP fails, the L2 aggregate port automatically transfers the traffic on this link to other working member links, making the connection more reliable.

Caution

The member port of the L2 aggregate port can be either access port or trunk port. However, the member ports in one AP must be of the same type, namely, all the ports are either access ports or trunk ports.

6.1.2 L3 Interfaces

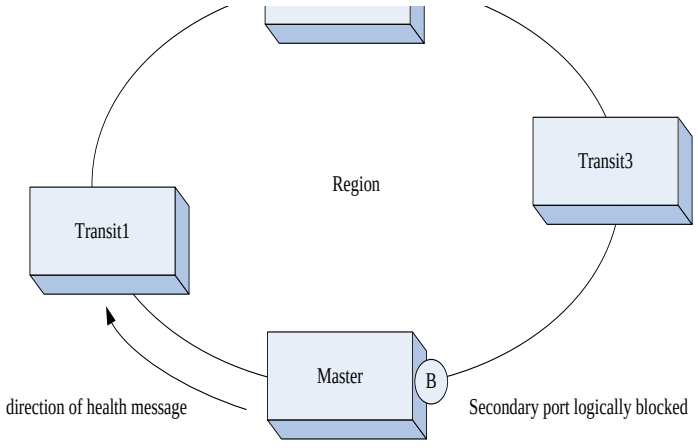
This section discusses the types and definitions of L3 interfaces. L3 interfaces fall into the following categories.

- SVI (Switch virtual interface)
- Routed Port
- L3 Aggregate Ports

6.1.2.1 SVI (Switch virtual interface)

SVI, short for Switch Virtual Interface, is used to implement the logical interface for layer 3 switching. SVI can work as the local management interface through which administrator can manage devices. You can also create SVI as a gateway interface that serves as the virtual sub-interface of each VLAN. It can be used for inter-VLAN routing on layer 3 device. A SVI can be created simply by using the **interface vlan** command in the interface configuration mode. Then an IP address is assigned to the SVI to establish a route between VLANs.

As the following figure depicts, the hosts of VLAN20 can communicate to each other directly without routing through an L3 device. If host A in VLAN20 wants to communicate with host B in VLAN30, it must route through SVI1 corresponding to VLAN20 and SVI2 corresponding to VLAN30.



6.1.2.2 Routed Port

A routed port is a physical port, for example, a port on the layer 3 device. It can be configured by using a layer 3 routing protocol. On the layer 3 device, a single physical port can be set as a routed port that serves as the gateway interface for layer 3 switching. A routed port serves as an access port that is not related to a specific VLAN. A routed port provides no L2 switching function. You may change an L2 switch port into a routed port by using the **no switchport** command and then assign an IP address to it for routing purposes. Note that using the **no switchport** command in the interface configuration mode will close and restart this port and delete all the layer 2 features of this port.

Caution

However, when a port is a member port of an L2 aggregate port or an unauthenticated DOT1x authentication port, the **switchport /no switchport** command will not work.

6.1.2.3 L3 Aggregate Port

Just like a L2 aggregate port, a L3 aggregate port is a logically aggregated port group that consists of multiple physical ports. The aggregated ports must be layer 3 ports of the same type. For layer 3 switching, an AP that serves as the gateway interface for layer 3 switching considers multiple physical links in the same aggregate group as one logical link. This is an important method for expanding link bandwidth. In addition, the frames that pass through the L3 aggregate port will undergo traffic balancing on the member ports of the L3 aggregate port. If one member link of AP fails, the L3 aggregate port automatically assigns the traffic on this link to other working member links, making the connection more reliable.

An L3 aggregate port offers no L2 switching functions. You may establish routes by first changing an L2 aggregate port without members into an L3 aggregate port using the **no switchport** command and then adding multiple routed ports and assigning an IP address to it.

6.2 Configuring Interfaces

This section provides the default setting, guidelines, steps, and examples of configuration.

6.2.1 Interface Numbering Rule

The number of a switch port consists of a slot number and the port number on the slot. For example, the port number is 3 and the slot number is 2, the number of the corresponding interface is 2/3. The slot number ranges from 0 to the total number of slots. The rule of numbering slots is that for panels facing the device, slots are numbered from front to back, from left to right, and from top down starting from 1 and increased in turn. Ports in a slot are numbered from left to right starting from 1 to the number of ports in the slot. For the devices which have a choice of optical or electrical interfaces, in either case, they use the same port number. You can view information on a slot and ports on it by using the **show** command in CLI.

Aggregate ports are numbered from 1 to the number of aggregate ports supported on the device.

A SVI is numbered by the VID of its corresponding VLAN.

Caution

The number of the static slot on a device is always 0. However, dynamic slots (pluggable modules or line cards) are numbered starting from 1.

6.2.2 Using Interface Configuration Commands

Execute the **interface** command to enter interface configuration mode in the global configuration mode.

Command	Function
DES-7210(config)# **interface** *interface ID*	Input **interface** to enter the interface configuration mode in the global configuration mode. You can also configure an interface range by using the **interface range** or **interface range macro** command. However, the interfaces in the same range must be of the same type and features.

This example shows how to access Gigabitethernet2/1:

```
DES-7210(config)# interface gigabitethernet 2/1
DES-7210(config-if)#
```

You can configure the related attributes of the interface in the interface configuration mode.

6.2.3 Using the interface range Command

6.2.3.1 Setting an Interface Range

You can configure multiple interfaces at once by using the **interface range** command in the global configuration mode. As a result, the configured parameters apply to all the interfaces within the range.

Command	Function
DES-7210(config)# **interface range** {*port-range* | **macro** *macro_name*}	Enter an interface range. You can use the **interface range** command to specify multiple ranges separated by a comma. The **macro** parameter can use the macro of a range. See the section of *Configuring and Using Macro Definition for Interface Range*. Be sure that the interfaces of all the ranges specified by a command must be of the same type.

When using the **interface range** command, you should pay attention to the format of **range**.

A valid range format

vlan *vlan-ID - vlan-ID*, with VLAN ID in the range of 1–4094;

Fastethernet *slot*/{*the first port*} - { the last *port*};

Gigabitethernet *slot*/{*the first port*} - { the last *port*};

TenGigabitethernet *slot*/{*the first port*} - { the last *port*};

Aggregate Port Aggregate *port number*, with *Aggregate port number* in the range of 1 to MAX.

The interfaces in an **interface range** must be of the same type, for example fastethernet, gigabitethernet, aggregate port or SVI.

This example shows how to use the **interface range** command in the global configuration mode:

```
DES-7210# configure terminal
```

```
DES-7210(config)# interface range fastethernet 1/1 - 10
DES-7210(config-if-range)# no shutdown
DES-7210(config-if-range)#
```

This example shows how to separate multiple ranges by a comma ",":

```
DES-7210# configure terminal
DES-7210(config)# interface range fastethernet 1/1-5, 1/7-8
DES-7210(config-if-range)# no shutdown
DES-7210(config-if-range)#
```

6.2.3.2 Configuring and Using Macro Definition for Interface Range

You can define a macro instead of inputting port ranges. However, you have to define macros using the **define interface-range** command in the global configuration mode before using the **macro** keyword of the **interface range** command.

Command	Function
DES-7210(config)# **define interface-range** *macro_name interface-range*	Define a macro for interface range. Name of the macro, up to 32 characters. A macro can define multiple interface ranges. The interfaces in all ranges in the same macro must be of the same type.
DES-7210(config)# **interface range macro** *macro_name*	The string defined by the macro will be saved in the memory. When you use the **interface range** command, you can use the macro name to replace the interface-range string.

To delete a macro, use the **no define interface-range macro_name** command in the global configuration mode.

When defining an interface range using the **define interface-range** command, you should pay attention to the range format.

A valid range format is:

– **vlan** *vlan-ID* - *vlan-ID*, with VLAN ID in the range of 1 to 4094;

– **fastethernet** *slot*/{*the first port*} - { the last *port*};

– **gigabitethernet** *slot*/{*the first port*} - { the last *port*};

– **Aggregate Port Aggregate** *port number*, with *Aggregate port number* in the range of 1 to MAX.

Interfaces contained in an i**nterface range** must be of the same type, that is, they should be all switch ports, aggregate ports or SVIs.

This example defines a macro for fastethernet1/1-4 by using the **define interface-range** command:

```
DES-7210# configure terminal
DES-7210(config)# define interface-range resource
fastethernet 1/1-4
DES-7210(config)# end
```

This example defines a macro for multiple ranges:

```
DES-7210# configure terminal
DES-7210(config)# define interface-range ports1to2N5to7
```

```
fastethernet 1/1-2, 1/5-7
DES-7210(config)# end
```

This example uses the macro ports1to2N5to7 to set the specified range of interfaces:

```
DES-7210# configure terminal
DES-7210(config)# interface range macro ports1to2N5to7
DES-7210(config-if-range)#
```

This example deletes the macro ports1to2N5to7:

```
DES-7210# configure terminal
DES-7210(config)# no define interface-range ports1to2N5to7
DES-7210# end
```

6.2.4 Selecting Interface Media Type

Some interfaces come with multiple media types for your choice.Once you have selected a media, interface attributes like connection status, speed, duplex, and flow control will be determined. When you change the media, interface attributes will use their default values. Change the default values when necessary.

This configuration takes effect for only physical ports. Aggregate port and SVI port do not support setting media types.

This configuration command takes effect for only the ports that supports media selection.

The ports configured to be the members of an aggregate port must have the same media type. Otherwise, they cannot be added to the AP. The port type of the members of the aggregate port cannot be changed.

Command	Function
DES-7210(config-if)# **medium-type** { **fiber** | **copper** }	Set the media type of a port.

This example sets the media type of gigabitethernet 1/1:

```
DES-7210# config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# medium-type fiber
DES-7210(config-if)# end
```

6.2.5 Setting Interface Description and Management Status

You may give an interface a particular name (description) to help you remember its functions. You may name the interface what you want to do with it, for example, if you want to reserve Gigabitethernet 1/1 for the exclusive use of user A, you may set its description to “Port for User A”.

Command	Function
DES-7210(config-if)# **description** *string*	Set the interface description in no more than 32 characters.

This example sets the description of Gigabitethernet 1/1:

```
DES-7210# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# description PortForUser A
DES-7210(config-if)# end
```

In some circumstances, you may need to disable some interface. You can do this by setting the management status of the interface. Once disabled, no frames can be received and sent through the interface, and all its functions are disabled. You can also restart an disabled interface by setting its management status. The management status of an interface can be **up** or **down**. When a port is disabled, its management status is **down**; otherwise, it is in the status **up**.

Command	Function
DES-7210(config-if)# **shutdown**	Disable an interface.

The following example illustrates how to disable Gigabitethernet 1/2.

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitethernet 1/2
DES-7210(config-if)# shutdown
DES-7210(config-if)# end
```

Caution

When a port of R2700 switching card(NM2-24ESW/NM2-16ESW) shutdown, the Link lights of the port and the connected peer port are still on. When the port sends packets to the peer port, the Link light flashes, but the port can not forward any packets.

6.2.6 Setting Speed, Duplexing, and Flow Control for an Interface

The section deals with the setting of speed, duplexing, and flow control for interfaces.

The following command takes effect only for switch port and routed port.

Command	Function
DES-7210(config-if)# **speed** {**10** | **100** | **1000** | **auto** }	Select a speed or set it to **auto**. Caution: 1000M applies only to gigabit interfaces. The rate of the 7200-24GE 1000M optical interface can be set as 100M. However, the rate of the optical interface for other devices is forced to be 1000M.
DES-7210(config-if)# **duplex** {**auto** | **full** | **half** }	Set duplex mode. Note that
DES-7210(config-if)# **flowcontrol** {**auto** | **on** | **off** }	Set flow control mode. Note: When **speed**, **duplex**, and **flowcontrol** are all set to non-auto, the system will disable auto-negotiation on the interface.

In the interface configuration mode, you can restore the settings of speed, duplexing, and flow control to the default values (auto-negotiation) by using the **no speed**, **no duplex**, and **no flowcontrol** commands. The following example shows how to set the speed of Gigabitethernet 1/1 to 1000M, its duplex mode to **full**, and its flow control to **off**.

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitethernet 1/1
```

```
DES-7210(config-if)# speed 1000
DES-7210(config-if)# duplex full
DES-7210(config-if)# flowcontrol off
DES-7210(config-if)# end
```

Caution For 7200-24GE, the 1000M and 100M fiber ports can not support the auto-negotiation switchover. You shall manually execute the command to switch.

6.2.7 Configuring Interface MTU

When a heavy throughput of data interchange occurs on a port, there may be a frame beyond the Ethernet standard frame length. This type of frame is called jumbo frame. A user can control the maximum frame length that the port is allowed to receive and send by setting the MTU.

MTU refers to the length of a valid data segment in a frame, excluding the overhead of Ethernet encapsulation.

The MTU of a port is checked during input, not output. If the frame received by the port is longer than the set MTU, it will be discarded.

The MTU is in the range from 64 to 9216 bytes with the granularity of 4 bytes. Its default value is 1500 bytes.

This configuration command takes effect only for physical ports. The SVI interface currently does not support the MTU setting.

Command	Function
DES-7210(config-if)# **Mtu** *num*	Set the MTU for a port. *Num*: <64 to 9216>

This example shows how to set the MTU for Gigabitethernet 1/1:

```
DES-7210# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# mtu 64
DES-7210(config-if)# end
```

6.2.8 Configuring L2 Interfaces

The following table shows the default settings of L2 interfaces. For the configurations of VLAN and ports, please refer to *Configuring VLAN* and *Configuring Port-based Flow Control*.

Attribute	Default Configuration
Working mode	L2 switch mode
Switch port mode	access port
Allowed VLAN range	1 to 4094
Default VLAN (for access port)	VLAN 1
Native VLAN (for trunk port)	VLAN 1
Media Type	copper

Attribute	Default Configuration
Interface management status	Up
Interface Description	Null
Speed	Auto-negotiation
Duplex mode	Auto-negotiation
Flow control	Auto-negotiation
Aggregate port	None
Storm suppression	Off
Port protection	Off
Port Security	Off

6.2.8.1 Configuring Switch Ports

1.2.8.1.1 Configuring Access/Trunk Port

This section is devoted to the setting of working modes (access/trunk port) of switch port and the setting in each mode.

To set the related attributes of a switch port, use the **switchport** command or other commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **switchport mode** {**access** | **trunk** }	Set the operation mode.

The following example shows how to set the operation mode of Gigabitethernet 1/2 to access port.

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitethernet 1/2
DES-7210(config-if)# switchport mode access
DES-7210(config-if)# end
```

Command	Function
DES-7210(config-if)# **switchport access vlan** *vlan-id*	Set the VLAN to which the access port belongs.

The following example shows how to configure the VLAN to which the access port gigabitethernet 2/1 to be 100

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitethernet 2/1
DES-7210(config-if)# switchport access vlan 100
DES-7210(config-if)# end
```

Set the native VLAN of the trunk port.

Command	Function
DES-7210(config-if)# **switchport trunk native vlan** *vlan-id*	Set the Native VLAN of the trunk port.

The following example shows how to set the native VLAN of the trunk port Gigabitethernet 2/1 to be 10.

```
DES-7210# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitethernet 2/1
DES-7210(config-if)# switchport trunk native vlan 10
DES-7210(config-if)# end
```

Set port security. For more information about port security, refer to *Port-based Flow Control*:

Command	Function
DES-7210(config-if)# **switchport port-security**	Set port security.

The following example shows how to enable port security on Gigabitethernet 2/1.

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitethernet 2/1
DES-7210(config-if)# switchport port-security
DES-7210(config-if)# end
```

For more information on configuring the speed, duplexing, and flow control of an interface, see the section of *Setting Speed, Duplexing, and Flow Control foran Interface.*

The following example shows how to set Gigabitethernet 2/1 to access port, its VLAN to 100, its speed, duplexing, and flow control to self-negotiation and enable port security.

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210 (config)# interface gigabitethernet 2/1
DES-7210 (config-if)# switchport access vlan 100
DES-7210 (config-if)# speed auto
DES-7210 (config-if)# duplex auto
DES-7210 (config-if)# flowcontrol auto
DES-7210 (config-if)# switchport port-security
DES-7210 (config-if)# end
```

1.2.8.1.2 Configuring Hybrid Port

You can configure the hybrid port by performing the following steps:

Command	Description
configure terminal	Enter configuration mode
interface <*interface***>**	Enter the interface configuration mode. Megabit, Gigabit, 10 Gigabit
switchport mode hybrid	Configure the port as a hybrid port.
no switchport mode	Delete the port mode.
switchport hybrid native *vlan* **id**	Set the default VLAN for the hybrid port.
switchport hybrid allowed vlan [[**add**] [**tagged	untaged**]] **|remove**] *vlist*	Set the output rule for the port.

```
DES-7210# configure terminal
DES-7210(config)# interface g 0/1
DES-7210(config-if)# switchport mode hybrid
DES-7210(config-if)# switchport hybrid native vlan 3
DES-7210(config-if)# switchport hybrid allowed vlan untagged 20-30
DES-7210(config-if)# end
DES-7210# show running interface g 0/1
```

6.2.8.2 Configuring L2 Aggregate Ports

This section describes how to create an L2 aggregate port and some related settings.

You may create an L2 aggregate port by using the **aggregateport** command in the interface configuration mode. For details, see *Configuring Aggregate Port.*

6.2.8.3 Clearing Statistics and Resetting an Interface

In the privileged EXEC mode, you may clear the statistics of an interface and then reset it by using the **clear** command. This command is only applicable for switch port, port members of an L2 aggregate port, routed port, and port members of an L3 aggregate port. The **clear** command is shown as follows.

Command	Function
DES-7210# **clear counters** [*interface-id*]	Clear interface statistics.
DES-7210# **clear interface** *interface-id*	Reset the interface.

In the privileged EXEC mode, use the **show interfaces** command to display interface statistics, or use the **clear counters** command to clear the counters. If no interface is specified, the counters of all layer 2 interfaces will be cleared.

The following example shows how to clear the counter of gigabitethernet 1/1.

```
DES-7210# clear counters gigabitethernet 1/1
```

6.2.9 Configuring L3 Interfaces

To configure a layer 3 interface, execute the following steps:

Command	Function
DES-7210(config-if)# **no switchport**	Shut down the interface and change it to L3 mode. This command applies to switch port and L2 aggregate port only.
DES-7210(config-if)# **ip address** *ip_address subnet_mask* {[**secondary** | **tertiary** | **quartus**][**broadcast**]}	Configure the IP address and subnet mask of the interface.

To delete the IP address of an L3 interface, use the **no ip address** command in the interface configuration mode.

The **no switchport** operation cannot be performed on one member of an L2 aggregate port.

The following example shows how to set an L2 interface to a routed port and assign an IP address to it.

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitethernet 2/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.20.135.21 255.255.255.0
DES-7210(config-if)# no shutdown
DES-7210(config-if)# end
```

6.2.9.1 Configuring SVI

This section describes how to create a SVI and some related configuration.

You may create a SVI or modify an existing one by using the **interface vlan** *vlan-id* command.

To configure a SVI, execute the following command:

Command	Function
DES-7210(config)# **interface vlan** *vlan-id*	Enter the SVI interface configuration mode.

Then, you can configure the attributes related to the SVI. For detailed information, refer to *Configuring Single IP Address Route*.

The following example shows how to enter the interface configuration mode and assign an IP address to SVI 100.

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface vlan 100
DES-7210(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7210(config-if)# end
```

6.2.9.2 Configuring Routed Ports

This section deals with how to create and configure a routed port.

You may create a routed port by using the **no switchport** command in the interface configuration command.

To create one routed port and assign an IP address to it, execute the following commands:

Command	Function
DES-7210(config-if)# **no switchport**	Shut down the interface and then change it to L3 mode.
DES-7210(config-if)# **ip address** *ip_address subnet_mask*	Configure the IP address and subnet mask.

Caution

No layer switching can be performed by using **switchport/ no switchport** when an interface is a member of an L2 Aggregate Port.

The following example shows how to set an L2 interface to a routed port and then assign an IP address to it.

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface fastethernet 1/6
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7210(config-if)# no shutdown
DES-7210(config-if)# end
```

6.2.9.3 Configuring L3 Aggregate Ports

This section deals with how to create an L3 aggregate port and some related configuration.

In the interface configuratiion mode, you can use the **no switchport** command to convert a L2 aggregate port to a L3 aggregate port:

Command	Function
DES-7210(config-if)# **no switchport**	Shut down the interface and change it to L3 mode.
DES-7210(config-if)# **ip address** *ip_address subnet_mask*	Configure the IP address and subnet mask.

The following example shows how to create an L3 aggregate port and assign an IP address to it.

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface aggregateport 2
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7210(config-if)# no shutdown
DES-7210(config-if)# end
```

6.3 Showing Interface Configuration and Status

This section covers interface status display and gives examples. You may view interface status by using the **show** command in the privileged EXEC mode. To show interface status, use the following commands.

Command	Function
DES-7210# **show interfaces** [*interface-id*]	Show the status and configuration of the specified interface.
DES-7210# **show interfaces** *interface-id* **status**	Show the status of the specified interface.
DES-7210# **show interfaces** [*interface-id*] **switchport**	Show the administrative and operational status of an switch interface (non-routing interface).
DES-7210# **show interfaces** [*interface-id*] **description**	Show the description and status of the specified interface.
DES-7210# **show interfaces** [*interface-id*] **counters**	Show the statistics of the specified port. Where, the rate displayed may have an error of less than 0.5%.

The following example shows how to display the status of Gigabitethernet 1/1.

```
DES-7210# show interfaces gigabitethernet 1/1
GigabitEthernet              : Gi 1/1
Description                  : user A
AdminStatus                  : up
OperStatus                   : down
Hardware                     : 1000BASE-TX
Mtu                          : 1500
PhysAddress                  :
LastChange                   : 0:0h:0m:0s
AdminDuplex                  : Auto
OperDuplex                   : Unknown
AdminSpeed                   : 1000M
OperSpeed                    : Unknown
FlowControlAdminStatus       : Enabled
```

```
FlowControlOperStatus        : Disabled
Priority    : 1
```

The following example shows the status and configuration of SVI 5.

```
DES-7210# show interfaces vlan 5
VLAN   : V5
Description                  : SVI 5
AdminStatus                  : up
OperStatus                   : down
Primary Internet address     : 192.168.65.230/24
Broadcast address            : 192.168.65.255
PhysAddress                  : 00d0.f800.0001
LastChange                   : 0:0h:0m:5s
```

The following example shows the status of aggregate port 3.

```
DES-7210# show interfaces aggregateport 3:

Interface                    : AggreatePort 3
Description                  :
AdminStatus                  : up
OperStatus                   : down
Hardware                     : -
Mtu                          : 1500
LastChange                   : 0d:0h:0m:0s
AdminDuplex                  : Auto
OperDuplex                   : Unknown
AdminSpeed                   : Auto
OperSpeed                    : Unknown
FlowControlAdminStatus       : Autonego
FlowControlOperStatus        : Disabled
Priority                     : 0
```

This example shows the configuration of GigabitEthernet 1/1:

```
DES-7210# show interfaces gigabitEthernet 1/1 switchport
Interface  Switchport Mode     Access    Native    Protected VLAN lists
---------- ---------- --------- --------- --------- --------- ------------
gigabitethernet 1/1     Enabled  Access     1        1        Enabled   All
```

This example shows the description of Gigabitethernet 2/1:

```
DES-7210# show interfaces gigabitethernet 1/2 description
Interface               Status    Administrative    Description
--------------------  ---------   ---------------    ----------------
gigabitethernet 2/1     down        down            Gi 2/1
```

This example shows statistics of the interfaces.

```
DES-7210# show interfaces gigabitethernet 1/2 counters
Interface : gigabitethernet 1/2
5 minute input rate          : 9144 bits/sec, 9 packets/sec
5 minute output rate         : 1280 bits/sec, 1 packets/sec
InOctets                     : 17310045
InUcastPkts                  : 37488
```

```
InMulticastPkts              : 28139
InBroadcastPkts              : 32472
OutOctets                    : 1282535
OutUcastPkts                 : 17284
OutMulticastPkts             : 249
OutBroadcastPkts             : 336
Undersize packets            : 0
Oversize packets             : 0
collisions                   : 0
Fragments                    : 0
Jabbers                      : 0
CRC alignment errors         : 0
AlignmentErrors              : 0
FCSErrors                    : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64:46264, 65-127: 47427, 128-255: 3478,
  256-511: 658, 512-1023: 18016, 1024-1518: 125
```

Caution

For the R2700 switching card(NM2-24ESW/NM2-16ESW), except for the values of two items “5 minute input rate” and “5 minute output rate” are shown normally, the values of other items are always to be 0.

6.4 LinkTrap Policy Configuration

You can determine whether to send the LinkTrap of an interface according to the interface configuration on a device. With this funciton enabled, when the interface’s link status changes, the SNMP protocol will send a LinkTrap message. Otherwise, it will not send a LinkTrap message. By default, this funciton is enabled.

6.4.1 Configuration Command

Command	Function
DES-7210(config-if)# **[no] snmp trap link-status**	Enable or disable the function of sending the LinkTrap function of this interface.

6.4.2 Configuration Example

The following configuration shows how to configure the interface not to send LinkTrap:

```
DES-7210(config)# interface gigabitEthernet 1/1
DES-7210(config-if)# no snmp trap link-status
```

7 Aggregate Port Configuration

This chapter explains how to configure an aggregate port on DES-7210 devices.

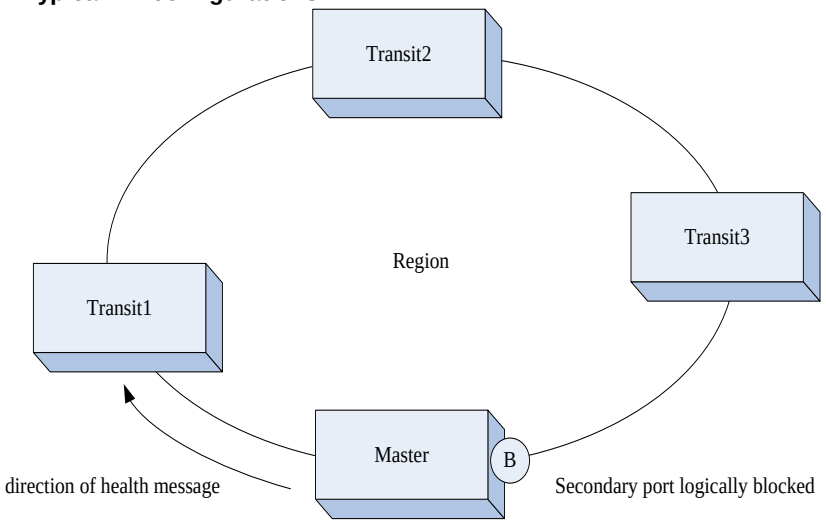
7.1 Overview

7.1.1 Understanding Aggregate Port

Multiple physical links can be bound into a logical link, called an aggregate port (hereinafter referred to as AP). DES-7210 devices provide the AP function that complies with the IEEE802.3ad standard. This function can be used to expand link bandwidth and improve reliability.

AP function supports traffic balancing that evenly allocating the traffic to every member link. AP function also supports link backup. When a link member in an AP is disconnected, the system will automatically allocate the traffic of the member link to other active member links in the AP, except for the broadcast or multicast packets it received.

Typical AP configurations



Each AP includes up to 8 member ports. The following lists the maximum AP numbers supported on different product models.

Caution The DES-7200 series supports up to 128 APs.

7.1.2 Understanding Traffic Balancing

Traffic can be evenly distributed on the member links of an AP according to the features such as source MAC address, destination MAC address, combination of source MAC address and destination MAC address, source IP address, destination IP address, and combination of source IP address and destination IP address. The **aggregateport load-balance** command can be used to set the method to distribute traffic.

Source MAC address-based traffic balancing refers to distribute the traffic on the member links of an AP according to the source MAC addresses of packets. Those packets with different source MAC addresses are evenly distributed on the member links of an AP according to different source MAC addresses. Those packets with the same source MAC address are forwarded through the same member link.

Destination MAC address-based traffic balancing refers to distribute the traffic on the member links of an AP according to the destination MAC addresses of packets. Those packets with different destination MAC addresses are evenly distributed on the member links of an AP according to different destination MAC addresses. Those packets with the same destination MAC address are forwarded through the same member link.

The traffic balancing based on the combination of source MAC address and destination MAC address refers to distribute the traffic on the member links of an AP according to the combination of source MAC address and destiantion MAC address of packets. Those packets with different source and destination MAC addresses are evenly distributed on the member links of an AP according to different source and destination MAC addresses. Those packets with the same source and destination MAC address are distributed on the same member link.

Source IP address- or destination IP address-based traffic balancing refers to distribute the traffic on the member links of an AP according to the source IP addresses or destination IP addresses of packets. Those packets with different source IP addresses or destination IP addresses are evenly distributed on the member links of an AP according to different source or destination IP addresses. Those packets with the same source IP address or destination IP address are forwarded through the same member link. This mode is specific for Layer 3 packets. If layer2 packets are received under this mode, traffic balancing is performed automatically according to the default device setting.

The traffic balancing based on the combination of source IP address and destination IP address refers to distribute the traffic on the member links of an AP according to the combination of source IP address and destiantion IP address of packets. Those packets with different source and destination IP addresses are evenly distributed on the member links of an AP according to different source and destination IP addresses. Those packets with the same source IP address and destination IP address are forwarded through the same member link. This mode is specific for Layer 3 packets. If layer2 packets are received under this mode, traffic balancing is performed automatically according to the default device setting.

All the abovementioned balancing modes are applicable to AP on Layer 2 and Layer 3.

The DES-7200 series supports all the traffic balancing modes, including Source MAC-based, Destination MAC-based, Source+Destination MAC-based, Source IP-based, Destination IP-based, Source+Destination IP-based traffic balancing modes.

An appropriate traffic distribution method should be set according to the actual network environments, so that the traffic can be evenly distributed on the the links for the maximum utilization of network bandwidth.

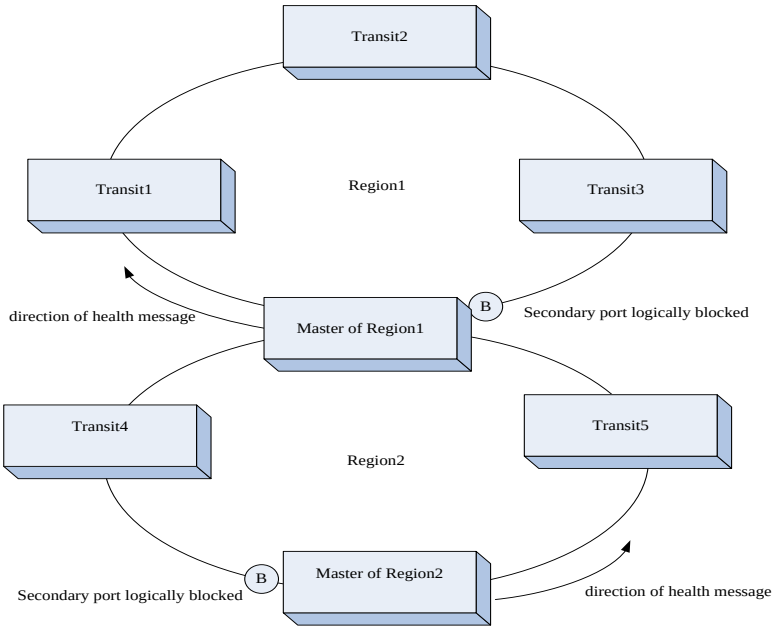
In the following diagram, a switch communicates with a router through an AP, and the router serves as the gateway for all the devices inside the network (such as 4 PCs on the top of the diagram). The source MAC addresses of all the packets that the devices outside the network (such as 2 PCs at the bottom of the diagram) send through the router are the MAC address of the gateway. In order to distribute traffic between the router and other hosts on other links, traffic balancing should

be performed based on the destination MAC address. However, traffic balancing should be performed based on the source MAC address on the switch.

Note

When the traffic balancing mode is source IP address-based, destination IP address-based, or source IP address and destination IP address-based traffic balancing mode, Layer 2 packets are distributed under the default device mode. You can execute **show aggregateport load-balance** command to get the default device mode before setting the parameter *aggregateport load-balance.*

AP traffic balancing



7.2 Configuring Aggregate Port

7.2.1 Default Aggregate Port Configuration

The default AP configuration is shown in the table below.

Attribute	Default value
Layer-2 AP interface	None
Layer-2 AP interface	None
Traffic balancing	Traffic is distributed according to the source MAC addresses of the incoming packets.

Caution

By default, the DES-7200 series performs traffic balancing based on the combination of the source MAC addresses and destination MAC addresses of the incoming packets.

7.2.2 Aggregate Port Configuration Guide

- The rates of the member ports of an AP must be the same.

- L2 ports can only be join a L2 AP, and L3 ports can only join a L3 AP. L2/L3 attributes of AP including member ports must not be modified.
- An AP does not support port security.
- Once a port is added to an AP, its attributes will be replaced by those of the AP.
- Once a port is removed from an AP, its attributes will be restored to original attributes.

Caution

When a port is added to an AP, you cannot perform any configuration on the port before removing the port from the AP.

7.2.3 Configuring a Layer2 Aggregate Port

In the interface configuration mode, add the interface to an AP by performing the following steps.

Command	Function
DES-7210(config-if-range)# **port-group** *port-group-number*	Add the interface to an AP (the system will create the AP if it does not exist).

In the interface configuration mode, use the **no port-group** command to remove a physical port from the AP.

The example below shows how to configure the layer2 Ethernet interface 1/0 to a member of layer2 AP 5.

```
DES-7210# configure terminal
DES-7210(config)# interface range gigabitEthernet 0/1
DES-7210(config-if-range)# port-group 5
DES-7210(config-if-range)# end
```

The command **interface aggregateport** *n* (n is the AP number) in the global configuration mode can be used to directly create an AP (if AP n does not exist).

Caution

- The DES-7200 series supports distributing AP member port to multiple line cards.
- After adding an ordinary port to an AP, when the port exits from the AP again, the previous configuration of the port will be restored to the default one. Different functions deal with the previous configuration of the AP member port differently. Therefore, it is recommended to view and confirm the port configuration after exiting from the AP.

7.2.4 Configuring a Layer3 Aggregate Port

By default, an aggregate port is on layer 2. To configure a layer-3 AP, perform the following operations.

The example below shows how to configure a layer-3 AP (AP 3) and configure its IP address (192.168.1.1):

```
DES-7210# configure terminal
DES-7210(config)# interface aggretegateport 3
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7210(config-if)# end
```

Caution

Only L3 switch support L3 AP.
You shall create a L3 AP before adding the interface to the L3 AP by executing **port-group** command.

The example below shows how to add the interface gigabitEthernet 0/1-3 to L3 AP:

```
DES-7210# configure terminal
DES-7210(config)# interface range gigabitEthernet 0/1-3
DES-7210(config-if)# no switchport
DES-7210(config-if)# port-group 2
```

7.2.5 Configuring Traffic Balancing on an Aggregate Port

In the configuration mode, configure traffic balancing on the AP by performing the following steps:

Command	Function
DES-7210(config)# **aggregateport load-balance** {**dst-mac** | **src-mac | src-dst-mac | dst-ip | src-ip | src-dst-ip** }	Set the AP traffic balancing and select the algorithm: **dst-mac:** Distribute traffic according to the destination MAC addresses of the incoming packets. **src-mac:** Distribute traffic according to the source MAC addresses of the incoming packets. **src-dst-mac:** Distribute traffic according to the combination of the source MAC addresses and destination MAC addresses of the incoming packets. **src-ip**: Distribute traffic according to the source IP addresses of the incoming packets. **dst-ip**: Distribute traffic according to the destination IP addresses of the incoming packets. **src-dst-ip:** Distribute traffic according to the combination of the source IP addresses and destination IP addresses of the incoming packets.

To restore the traffic balancing configuration of an AP to the default value, execute the **no aggregateport loag-balance** command in the global configuration mode:

7.3 Showing an Aggregate Port

In the privileged mode, show the AP configuration by performing the following steps.

Command	Function
DES-7210# **show aggregateport** [*port-number*]{**load-balance | summary**}	Show the AP settings.

```
DES-7210# show aggregateport load-balance
Load-balance : Source MAC address
DES-7210# show aggregateport 1 summary
AggregatePort MaxPorts SwitchPort Mode   Ports
------------- -------- ---------- ------
Ag1             8        Enabled         ACCESS
```

8 LACP Configuration

8.1 Overview

LACP(Link Aggregation Control Protocol) is a protocol based on IEEE802.3ad and aims to implement the dynamic link aggregation and deaggregation. This protocol interacts with its peer by using the LACPDU(Link Aggregation Control Protocol Data Unit).

With LACP enabled on the port, LACP notifies the following information of the port by sending LACPDUs: priority and MAC address of the system, port priority, number and operation key. Upon receiving the information, the peer determines the port that can be aggregated by comparing the reveived information with the information of other ports on the peer device. In this way, the two parties can reach an aggreement in adding/removing the port to/from a dynamic aggregation group.

8.2 Dynamic Link Aggregation Mode

A LACP port can be in one of the two states: Active and Passive.

The port in the active state will transceive the LACP packets and negotiate with the peer end; while the port in the passive state will only respond to the received LACP pacekts.

The port in the active mode can be aggregated with the port in both active or passive mode; while the port in the passive mode can only be aggregated with the port in the active mode.

8.3 LACP Port State

The port member in the aggregation group can be in the following 3 states:

When the link state of the port is Down, no packet is forwarded on the port. The port state is down.

When the link state of the port is Up, after the LACP negotiation, the port joins in the packet forwarding as a port member in the aggregation group. The port state is bndl.

When the link state of the port is Up, the port fails to join in the packet forwarding because the LACP is not enabled on the port, or the attribute of the port and the master port is inconsistent. The port state is sups.

Note

- Only the port with full-duplex attribute can be aggregated.
- The port rate, flow-control, media-type and Layer2&3 port attribute must be consistent.
- After the port aggregation, changing the above port attributes will lead to the aggregation failure of other ports in the same aggregation group.

8.4 Dynamic Link Aggregation Priority Relations

8.4.1 LACP System ID

Only one LACP aggregation system can be configured on each device. Each LACP aggregation system has sole system priority. The system ID consists of LACP system priority and the device MAC address. First compare the two system priorities: the lower the system priority is, the higher the system ID will be. Then compare the two device MAC addresses if the system priorities are equal: the smaller the MAC address is , the higher the system ID will be. The system with the higher system ID determines the port state.

8.4.2 LACP Port ID

Each port owns an independent LACP port priority, which is configurable. The port ID consists of LACP port priority and port number. First compare the two port priorities: the lower the port priority value is, the higher the port ID is. Then compare the two port numbers if the two port priorities are equal: the smaller the port number is, the higher the port ID is.

8.4.3 LACP Master Port

When the dynamic member port is up, LACP selects a port with the highest priority in the aggregation group based on the port rate, duplex rate, ect. Only can the ports with the same attributes with the master port be aggregated and join in the packet forwarding in the aggregation group. When the port attributes change, LACP re-selects the master port without deaggregation. But when the new master port is not aggregated, LACP deaggregates the member ports in the aggregation group and re-aggregates.

8.4.4 LACP Negotiation Procedure

Upon receiving the LACP packets from the peer port, the system ID with higher priority is selected. On the end of higher system ID, set the ports in the aggregation group are to be aggregated in the descending order of port priority(when the number of ports in the aggregation group exceeds the maximum port number, the state of the ports exceeding the aggregation capacity is **sups**.) Upon receiving the updated LACP packets on the peer port, the corresponding port is to be aggregated.

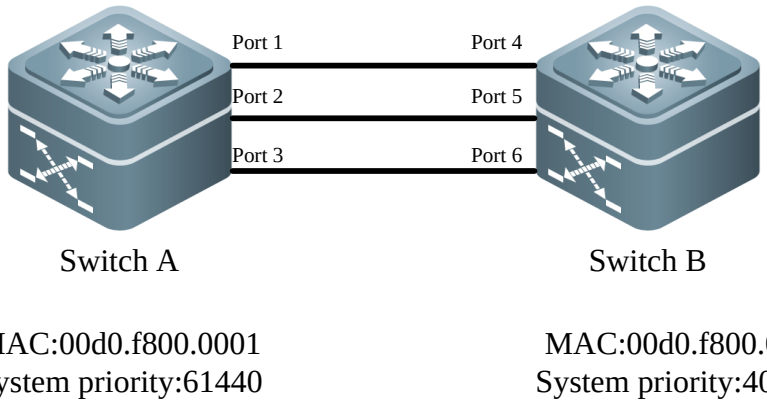


Figure-1 LACP Negotiation

As shown in Figure-1, switch A and switch B are interconnected through the 6 ports. Set the system priority for the switchA and the switchB to be 61440 and 4096 respectively. Enable the LACP function on the 6 ports directly-connected between the switches. Set the aggregation mode for the 3 ports is active, and set the default port priority for the other 3 ports as 32768.

Upon receiving the LACP packets from the switchA, switchB finds its system priority is higher than the switchA, the port4-6 on the switchB are to be aggregated according to the sequence of the port priority. After receiving the updated LACP packets from the switchB, the switchA finds its system priority is lower than the switchB and the port1-3 on the switchA are also aggregated.

8.5 LACP Requirements

LACP is a protocol that automatically add/remove the port to/from the aggregation group. The requirements of the auto-aggreagation of those two ports are:

Only can the ports with the same operation key be aggregated;

Only can the ports that are with the same attributes such as port rate and duplex as the master port be dynamically aggregated.

The port link state is UP, the peer port running LACP and the port or the peer port must be in the Active mode.

8.6 LACP Configuration

8.6.1 Configuring LACP

You can configure the LACP system priority, port priority and administrative key in the aggregation group. All dynamic link groups on one switch share one LACP system priority. Changing the system priority will affect all aggregation groups.

Run the following commands to configure the LACP:

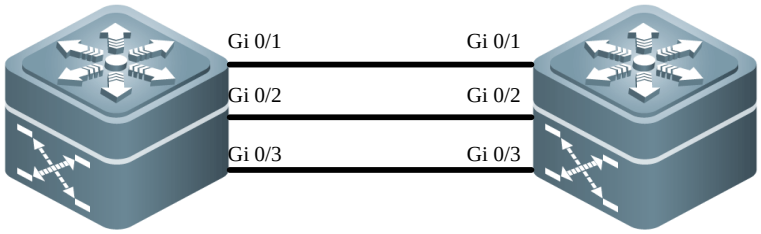
Command	Function
DES-7210# **configure**	Enter the global configuration mode.
DES-7210(config)# **lacp system-priority** *system-priority*	(Optional) Set the LACP system priority, in the range of 0-65535. The default system priority is 32768.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config-if)# **lacp port-priority** *port-priority*	(Optional) Set the LACP port priority, in the range of 0-65535. The default system priority is 32768.
DES-7210(config-if)# **port-group** *key* **mode active | passive**	Add the port to the aggregation group and specify the LACP port mode. If the aggregation group does not exist, an aggregation group will be created. *Key:* the administrative key of the aggregation group. **active | passive:** the port mode in the LACP group.
DES-7210(config-if)# **end**	Return to the privileged mode.

8.6.2 Viewing the LACP Configuration

To view the LACP state, run the following command in the privileged mode:

Command	Function
DES-7210# **show lacp summary**	Show the LACP state information.

8.7 LACP Configuration Example



Switch 1 Switch 2

MAC:00d0.f800.0001 MAC:00d0.f800.02
System priority:4096 System priority:61440

Figure-2 LACP Link Aggregation

As shown in the figure-2, on the switchDES-72101, set the LACP system priority as 4096, enable the LACP on the interface Gi 0/1 Gi 0/2 Gi 0/3, and set the LACP port priority as 4096:

```
DES-72101# configure terminal
DES-72101(config)# lacp system-priority 4096
DES-72101(config)# interface range GigabitEthernet 0/1-3
DES-72101(config-if-range)# lacp port-priority 4096
DES-72101(config-if-range)# port-group 3 mode active
DES-72101(config-if-range)# end
```

On the switchDES-72102, set the LACP system priority as 61440, enable the LACP on the interface Gi 0/1 Gi 0/2 Gi 0/3, and set the LACP port priority as 61440:

```
DES-72101# configure terminal
DES-72101(config)# lacp system-priority 61440
DES-72101(config)# interface range GigabitEthernet 0/1-3
DES-72101(config-if-range)# lacp port-priority 61440
DES-72101(config-if-range)# port-group 3 mode active
DES-72101(config-if-range)# end
```

After the configuration, if the LACP negotiation succeeds, it prompts the following log:

```
*Feb 25 17:11:31: %LACP-5-BUNDLE: Interface Gi0/1 joined AggregatePort 3.
*Feb 25 17:11:32: %LACP-5-BUNDLE: Interface Gi0/2 joined AggregatePort 3.
*Feb 25 17:11:32: %LACP-5-BUNDLE: Interface Gi0/3 joined AggregatePort 3.
*Feb 25 17:11:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface AggregatePort 3, changed
state to up
```

Then show the member port state in the aggregation group on the switchDES-72101:

```
DES-7210(config)#show LACP summary
Flags:  S - Device is sending Slow LACPDUs
        F - Device is sending fast LACPDUs.
A - Device is in active mode.       P - Device is in passive mode.

Aggregate port 3:

Local information:
                          LACP port      Oper    Port     Port
```

```
Port     Flags     State     Priority       Key     Number  State
---------------------------------------------------------------
Gi0/1     SA       bndl       4096          0x3     0x1     0x3d
Gi0/2     SA       bndl       4096          0x3     0x2     0x3d
Gi0/3     SA       bndl       4096          0x3     0x3     0x3d


Partner information:
                  LACP port                Oper    Port    Port
Port     Flags    Priority     Dev ID      Key     Number  State
---------------------------------------------------------------
Gi0/1     SA       61440    00d0.f800.0002  0x3     0x1     0x3d
Gi0/2     SA       61440    00d0.f800.0002  0x3     0x2     0x3d
Gi0/3     SA       61440    00d0.f800.0002  0x3     0x3     0x3d
```

The following table describes the fileds:

Field	Description
Local information	Show the local LACP information.
Port	Show the system port ID.
Flags	Show the port state flag: “S” indicates that the LACP is stable and in the state of periodically sending the LACPPDU; “A” indicates that the port is in the active mode.
State	Show the port aggregation information: “bndl” indicates that the port is aggregated; “Down” represents the disconnection port state; “sups” indicates that the port is not aggregated.
LACP Port Priority	Show the LACP port priority.
Oper Key	Show the port operation key.
Port Number	Show the port number.
Port State	Show the flag bit for the LACP port state.
Partner infomation	Partly show the LACP information of the peer port.
Dev ID	Partly show the system MAC information of the peer device.

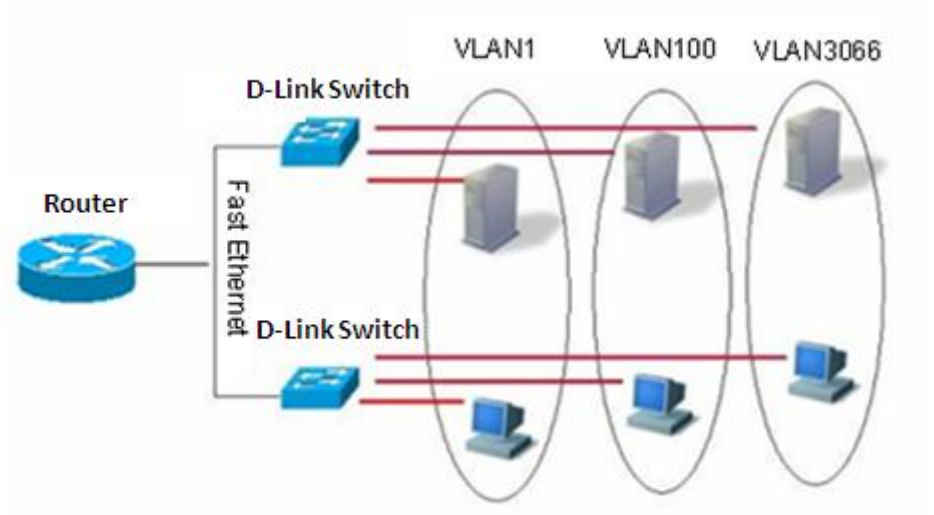
9 VLAN Configuration

This chapter describes how to configure IEEE802.1q VLAN.

9.1 Overview

Virtual Local Area Network (VLAN) is a logical network divided on a physical network. VLAN corresponds to the L2 network in the ISO model. The division of VLAN is not restricted by the physical locations of network ports. A VLAN has the same attributes as a common physical network. Except for no restriction on physical location, unicast, broadcast and multicast frames on layer 2 are forwarded and distributed within a VLAN, not being allowed to directly go to other VLANs.Therefore, when a host in a VLAN wants to communicate with another host in another VLAN, a layer 3 device must be used, as shown in the following diagram.

You can define a port as the member of a VLAN. All the terminals connected to the specified port are part of the VLAN. A network can support multiple VLANs. In this case, when you add, delete, and modify users in the VLANs, you do not need to modify the network configuration physically.



Like a physical network, a VLAN is usually connected to an IP subnet. A typical example is that all the hosts in the same IP subnet belong to the same VLAN. A layer 3 device must be used for communication between VLANs. DES-7210 L3 devices can perform IP routing between VLANs through SVI (Switch Virtual Interfaces). For the configuration about SVI, refer to *Interface Management Configuration* and *IP Unicast Routing Configuration*.

9.1.1 Supported VLAN

Complying with IEEE802.1Q Standard, our products support up to 4094 VLANs(VLAN ID 1-4094), in which VLAN 1 is the default VLAN that cannot be deleted.

Caution

The DES-7200 series supports 4094 VLANs.

9.1.2 VLAN Member Type

You can determine the frames that can pass a port and the number of VLANs that the port can belong to by configuring the VLAN member type of the port. For the detailed description about VLAN member type , see the following table:

Member Type	Port Feature
Access	One access port can belong to only one VLAN, which must be specified manually.
Trunk (802.1Q)	By default, one Trunk port belongs to all the VLANs of the device itself, and it can forward the frames of all the VLANs. However, you can impose restriction by setting a list of allowed VLANs.

9.2 Configuring a VLAN

A VLAN is identified by its VLAN ID. You can add, remove, and modify the VLANs in the range of 2 to 4094 on a device. VLAN 1 is created by a device automatically and cannot be removed.

You can configure the member type of a port in a VLAN, add a port to a VLAN, and remove a port from a VLAN in the interface configuration mode.

9.2.1 Saving the VLAN Configuration

To save the VLAN configuration in the configuration file, execute the **copy running-config startup-config** command in the privileged mode. To view VLAN configuration, execute the **show vlan** command.

9.2.2 Default VLAN Configuration

The following table shows the default configuration of a VLAN.

Parameter	Default value	Range
VLAN ID	1	1 to 4094
VLAN Name	VLAN xxxx, where xxxx is the VLAN ID	None
VLAN State	Active	Two status: active or inactive

9.2.3 Creating/Modifying a VLAN

In the privileged mode, you can create or modify a VLAN by executing the following commands.

Command	Function

Command	Function
DES-7210(config)# **vlan** *vlan-id*	Enter a VLAN ID. If you enter a new VLAN ID, the device will create it. If you enter an existing VLAN ID, the device modifies the corresponding VLAN.
DES-7210(config)# **name** *vlan-name*	(Optional) Name the VLAN. If you skip this step, the device automatically assigns the VLAN a name of VLAN xxxx, where xxxx is a 4-digit VLAN ID starting with 0. For example, VLAN 0004 is the default name of VLAN 4.

To restore the name of a VLAN to its default, simply enter the **no name** command.

The following example creates VLAN 888, names it test888, and saves its configuration into the configuration file:

```
DES-7210# configure terminal
DES-7210(config)# vlan 888
DES-7210(config-vlan)# name test888
DES-7210(config-vlan)# end
```

9.2.4 Deleting a VLAN

You cannot delete the default VLAN (VLAN 1).

In the privileged mode, you can delete a VLAN by executing the following command.

Command	Function
DES-7210(config)# **no vlan** *vlan-id*	Enter the VLAN ID that you want to delete.

9.2.5 Assigning Access Ports to a VLAN

If you assign a port to an inexistent VLAN, the switch will automatically create that VLAN.

In the privileged mode, you can assign a port to a VLAN by executing the following command.

Command	Function
DES-7210(config-if)# **switchport mode access**	Define the member type of the port in a VLAN (L2 ACCESS port).
DES-7210(config-if)# **switchport access vlan** *vlan-id*	Assign the port to the VLAN.

The following example adds Ethernet 1/10 to VLAN20 as an access port:

```
DES-7210# configure terminal
DES-7210(config)# interface fastethernet 1/10
DES-7210(config-if)# switchport mode access
DES-7210(config-if)# switchport access vlan 20
DES-7210(config-if)# end
```

The following example shows how to verify the configuration:

```
DES-7210(config)#show interfaces gigabitEthernet 3/1
 switchport
Switchport is enabled
Mode is access port
Acsess vlan is 1,Native vlan is 1
```

```
Protected is disabled
Vlan lists is ALL
```

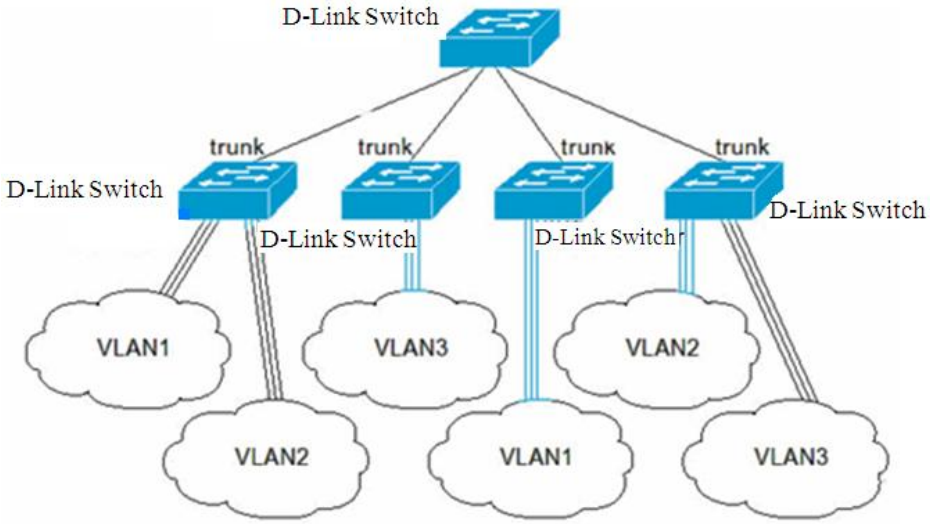
Caution In the R2700 switching card, althought the access vlan can also be configured on the trunk port, the access port configuration does not take effect and the port remains in the trunk port. Only the configuration of native vlan and allowed vlan list takes effect.

9.3 Configuring VLAN Trunks

9.3.1 Overview

A trunk is a point-to-point link that connects one or multiple Ethernet switching interfaces to other network devices (for instance, router or switch). A trunk can transmit the traffics of multiple VLANs.

The Trunk encapsulation of DES-7210 device is 802.1Q-complied. The following diagram shows a network connected with trunks.



You can set a common Ethernet port or aggregate port to be a trunk port. For the details of aggregate port, refer to *Configuring Aggregate Port*.

In order to switch an interface between the access mode and the trunk mode, use the **switchport mode** command:

Command	Function
DES-7210(config-if)# **switchport mode access**	Set an interface to the access mode
DES-7210(config-if)# **switchport mode trunk**	Set an interface to the Trunk mode

A native VLAN must be defined for a trunk port. The untagged packets received and sent through the port are deemed as the packets of the native VLAN. Obviously, the default VLAN ID of the port (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. Moreover, you must untag them before sending the packets of the native VLAN through the trunk port. The default native VLAN of a trunk port is VLAN 1.

When you configure a trunk link, be sure that the ports on both ends of the trunk belong to the same native VLAN.

9.3.2 Configuring a Trunk Port

9.3.2.1 Basic Trunk Port Configuration

In the privileged mode, you can configure a trunk port by executing the following command.

Command	Function
DES-7210(config-if)# **switchport mode trunk**	Configure the port as a L2 trunk port.
DES-7210(config-if)# **switchport trunk native vlan** *vlan-id*	Specify a native VLAN for the port.

To restore all the trunk-related settings of a trunk port to their defaults, use the **no switchport mode** command in the interface configuration mode.

9.3.3 Defining the Allowed VLAN List of a Trunk Port

By default, the traffic of all VLANs in the range of 1 to 4094 can be transmitted over a trunk port. However, you can restrict the traffic of some VLANs from passing the trunk port by setting its allowed VLAN list.

In the priviledged mode, you can modify the allowed VLAN list of a trunk port by executing the following command.

Command	Function
DES-7210(config-if)# **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] } *vlan-list*	(Optional) Configure the allowed VLAN list of the trunk port. The *vlan-list* parameter may be a VLAN or a series of VLANs. It starts with a small VLAN ID and ends with a large VLAN ID. Both IDs are connected with "-", such as 10–20. **All:** Add all the allowed VLANs to the allowed VLAN list; **add**: Add the specified VLAN list to the allowed VLAN list; **remove:** Remove the specified VLAN list from the allowed VLAN list; **except**: Add all the VLANs other than the specified VLAN list to the allowed VLAN list.

To restore the allowed VLAN list of the trunk port to its default, execute the **no switchport trunk allowed vlan** command in the interface configuration mode.

The following example removes VLAN 2 from the allowed VLAN list of port 1/15:

```
DES-7210(config)# interface fastethernet 1/15
DES-7210(config-if)# switchport trunk allowed vlan remove 2
DES-7210(config-if)# end
DES-7210# show interfaces fastethernet 1/15 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
--------- ---------- ----  ------ ------ -------- ----------
Gi0/15    enabled    TRUNK 1      1      Disabled   1,3  4094
```

9.3.4 Configuring a Native VLAN.

Tagged or untagged 802.1Q frames can be received or sent on a trunk port. Untagged frames are used to transmit the traffic of the native VLAN. By default, the native VLAN is VLAN 1.

In the privileged mode, you can configure a native VLAN for a trunk port by executing the following command.

Command	Function
DES-7210(config-if)# **switchport trunk native vlan** *vlan-id*	Configure a native VLAN.

To restore the native VLAN of a trunk port to its default, execute the **no switchport trunk native vlan** command in the interface configuration command.

If a frame carries the VLAN ID of the native VLAN, it will be automatically untagged when being forwarded through the trunk port.

When you set the native VLAN of a trunk port to an inexistent VLAN, the switch will not automatically create the VLAN. In addition, the native VLAN of a trunk port may be out the allowed VLAN list. In this case, the traffic of the native VLAN cannot pass the trunk port.

9.4 Showing VLAN Information

Only in the privileged mode can you view the VLAN information, including VLAN VID, VLAN status, member ports of the VLAN, and VLAN configuration. The related commands are listed as below:

Command	Function
show vlan [**id** *vlan-id*]	Show the information about all or the specified VLAN.

The following example shows the information about a VLAN:

```
DES-7210# show vlan

VLAN  Name      Status             Ports

---- --------  --------   -------------------------------

   1 VLAN0001   STATIC    Gi0/1, Gi0/5, Gi0/6, Gi0/7

                          Gi0/8, Gi0/9, Gi0/10, Gi0/11

                          Gi0/12, Gi0/13, Gi0/14, Gi0/15

                          Gi0/16, Gi0/17, Gi0/18, Gi0/19

                          Gi0/20, Gi0/21, Gi0/22, Gi0/23

                          Gi0/24

  10 VLAN0010  STATIC    Gi0/2, Gi0/3

  20 VLAN0020  STATIC    Gi0/2, Gi0/3, Gi0/4

30 VLAN0030  STATIC    Gi0/3, Gi0/4


DES-7210#show vlan id 20

VLAN  Name              Status    Ports

----  --------          ------    -----------------------
```

```
20  VLAN0020          STATIC    Gi0/2, Gi0/3, Gi0/4
```

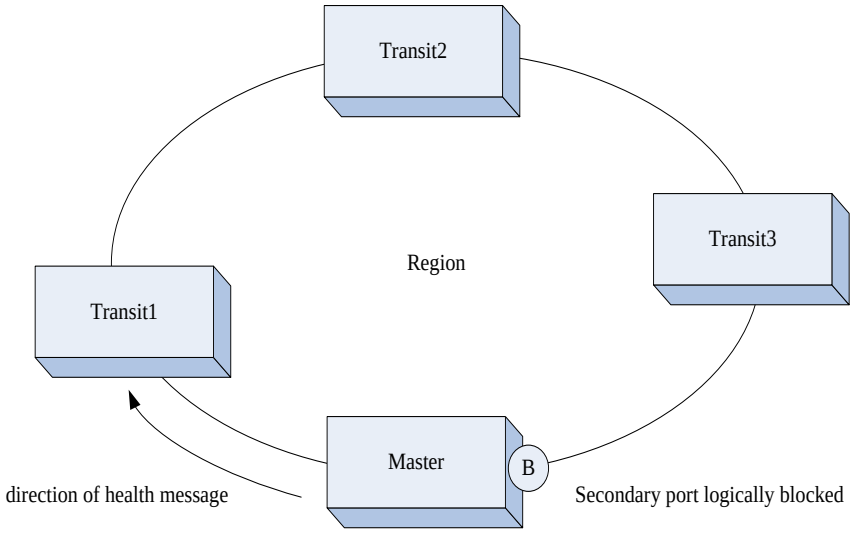
10 Super VLAN Configuration

This chapter describes the Super VLAN configuration of DES-7210 devices.

10.1 Overview

Super VLAN is a method for VLAN division. Super VLAN, also called VLAN aggregation, is a management technology for optimizing IP addresses. Its principle is to assign the IP address of a network segment to different sub VLANs that belong to the same super VLAN. Each sub VLAN is an independent broadcast domain and isolated on the layer 2. Users in a sub VLAN use the IP address of a virtual interface of the super VLAN as the gateway for communication on the layer 3, which allows multiple VLANs to share one IP address and saves IP address resources. At the same time, the ARP proxy function is required to realize layer 3 interoperation between sub VLANs, as well as interoperation between sub VLANs and other networks. The ARP proxy can forward and handle the ARP request and response packets to realize layer 3 interoperation between the isolated layer 2 ports of sub VLANs. By default, the ARP proxy function is enabled for super VLAN and sub VLAN.

Super VLAN not only save lots of IP addresses,but also is convenient for the network management. You only need to assign an IP address to a super VLAN including multiple sub VLANs.



The following presents the communication procedure between two aggregated sub VLANs.

As shown in the above diagram, Sub VLAN2 and Sub VLAN4 are aggregated to form Super VLAN3. An IP address is assigned to Super VLAN3, and both Sub VLAN2 and Sub VLAN4 are located in this subnet. Supposing PC1 in Sub VLAN2 wants to communicate with PC2 in the subnet, after knowing that the peer is located in the same network segment, PC1 directly sends an ARP request packet with a destination IP address. Upon receiving this ARP request packet, the layer 3 device directly broadcasts this packet through layer 2 within Sub

VLAN2, and sends a copy to the ARP module of the device. This module first checks whether the destination IP address in the ARP request packet is in Sub-VLAN2. If so, it will discard this packet because it and PC1 are located in the same broadcast domain, and the destination host will directly respond to PC1. If not, it will respond PC1 with the MAC address of SuperVLAN3, acting as an ARP agent. For example, PC1 and PC2 have to communicate through the ARP agent which forwards packets from PC1 to PC2. However, PC1 and PC3 can communicate directly without a forwarding device.

Restrictions:

- A super VLAN can only contain sub VLANs. The sub VLAN contains actual physical ports.
- A super VLAN cannot serve as a sub VLAN of other Super VLANs.
- A super VLAN cannot be used as the normal 1Q VLAN.
- VLAN 1 cannot be used as a super VLAN.
- A sub VLAN cannot be configured as a network interface, and cannot be assigned with an IP address.
- Super VLAN does not support VRRP, IGMP Snooping and PIM Snooping.
- Super VLAN interface-based ACL and QOS configurations take no effect for sub VLANs.

10.2 Configuring a Super VLAN

To configure a super VLAN, execute the following commands.

Command	Function
DES-7210# **configure**	Enter the global configuration mode.
DES-7210(config)# **vlan** *vlan-id*	Enter the VLAN configuration mode
DES-7210(config-vlan)# **supervlan**	Enable the Super VLAN function
DES-7210(config-vlan)# **end**	Return to the privileged mode.

The super VLAN function is disabled by default. The enabled super VLAN function can be disabled by using the **no supervlan** command.

10.3 Configuring the Sub VLANs of a Super VLAN

A super VLAN is meaningful only when subVLANs are configured.

To configure a VLAN as the sub VLAN of a super VLAN, execute the following command.

Caution

The SubVLAN configuration may fail due to a lack of resources.

Command	Function
DES-7210# **configure**	Enter the global configuration mode
DES-7210(config)# **vlan** *vlan-id*	Enter the VLAN configuration mode
DES-7210(config-vlan)# **supervlan**	Set this VLAN as a super VLAN
DES-7210(config-vlan)# **subvlan** *vlan-id-list*	Specify several sub VLANs and add them to the super VLAN.

Command	Function
DES-7210(config-vlan)# **exit**	Return to the global mode.

To delete a sub VLAN from the super VLAN, execute the **no subvlan** [*vlan-id-list*] command.

Caution

If you want to delete SubVLAN, you must switch it to ordinary VLAN and then use command **no vlan.**

10.4 Setting an Address Range for a Sub VLAN

You can configure an address range for each sub VLAN so that the device can idetnify which sub VLAN that a given IP address belongs to. The address ranges configured for sub VLANs of the super VLAN should not be overlapped or covered each other.

To set an address range for a sub VLAN, execute the following command in the global configuration mode:

Command	Function
DES-7210# **configure**	Enter the global configuration mode
DES-7210(config)# **vlan** *vlan-id*	Enter the VLAN configuration mode
DES-7210(config-vlan)# **subvlan-address-range** *start-ip end-ip*	Set an address range for the sub VLAN. start-ip is the start IP address of this sub VLAN, and end-ip is the end IP address of this sub VLAN.
DES-7210(config-vlan)# **end**	Return to the privileged mode.
DES-7210# **show run**	Verify the configuration.

Note

You can delete previous configurations by using command **no subvlan-address-range**.

10.5 Setting a Virtual Interface for a Super VLAN

When a user in a sub VLAN needs to perform layer 3 communication, a virtual layer 3 interface of the super VLAN should be created first.

The SVI of the super VLAN itself is used as the virtual interface.

To set a virtual interface for a supre VLAN, execute the following commands in the global configuration mode.

Command	Function
DES-7210# **configure**	Enter the global configuration mode.
DES-7210(config)# **interface vlan** *vlan-id*	Enter the SVI mode .

Command	Function
DES-7210(config-vlan)# **ip address** *ip mask*	Set an IP address for the virtual interface.
DES-7210(config-vlan)# **end**	Return to the privileged mode.
DES-7210# **show run**	Verify the configuration.

10.6 Setting ARP Proxy for a VLAN

You can set ARP Proxy for a VLAN so that sub VLANs can communciate with each other.

ARP Proxy is enabled for a VLAN by default.

To set ARP Proxy for a VLAN, execute the following command in the global configuration mode:

Command	Function
DES-7210# **configure**	Enter the global configuration mode.
DES-7210(config)# **vlan** *vlan-id*	Enter the VLAN mode.
DES-7210(config-vlan)# **proxy-arp**	Enable ARP Proxy function for the VLAN.
DES-7210(config-vlan)# **end**	Return to the privileged mode.
DES-7210# **show run**	Verify the configuration.

To disable ARP Proxy for a VLAN, execute the **no proxy-arp** command.

10.7 Showing Super VLAN Setting

To show the super VLAN setting, execute the following command.

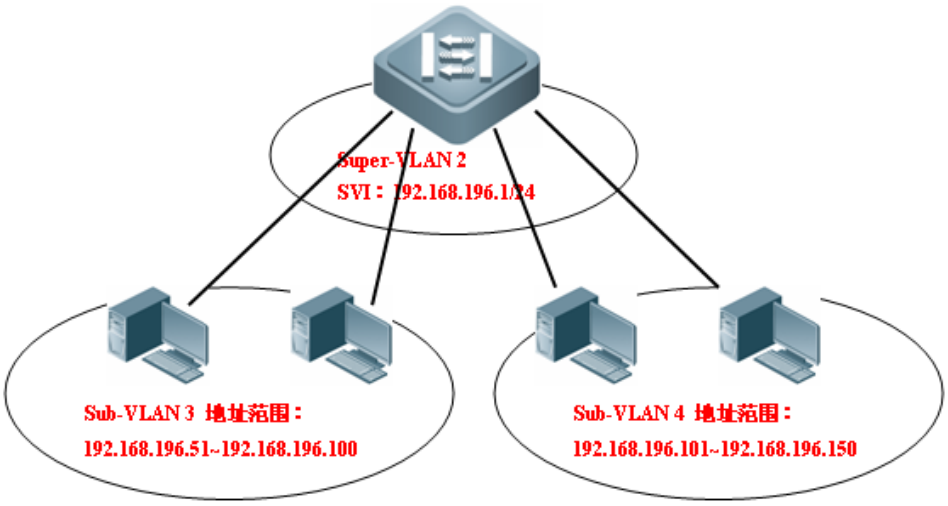
Command	Function
DES-7210# **show supervlan**	Show the super VLAN setting.

10.8 Configuration Example

10.8.1 Configuration Requirements

1. Create Super-VLAN 2 and configure Sub-VLAN 3 and Sub-VLAN 4
2. Set the IP address range for Sub-VLAN 3 and Sub-VLAN 4 as 192.168.196.51~192.168.196.100and 192.168.196.101~192.168.196.150.
3. Set the IP address and subnet mask for the Super-VLAN virtual interface as 192.168.196.1, 255.255.255.0.
4. Enable VLAN ARP Proxy funcrion

10.8.2 Topology



10.8.3 Configuration Steps

Enter the global configuration mode

```
DES-7210# configure terminal
```

Create VLAN 2 and enter VLAN configuration mode

```
DES-7210(config)# vlan 2
```

Set Super-VLAN 2

```
DES-7210(config-vlan)# supervlan
```

Return to the global configuration mode

```
DES-7210(config-vlan)# exit
```

Create VLAN 3

```
DES-7210(config)# vlan 3
```

Return to the global configuration mode

```
DES-7210(config-vlan)# exit
```

Create VLAN 4

```
DES-7210(config)# vlan 4
```

Return to the global configuration mode

```
DES-7210(config-vlan)# exit
```

Enter VLAN 2 configuration mode and set Sub-VLAN 3 and Sub-VLAN 4

```
DES-7210(config)# vlan 2
DES-7210(config-vlan)# subvlan 3,4
```

Return to the global configuration mode, enter VLAN 3 configuration mode and set the IP address range for VLAN 3

```
DES-7210(config-vlan)# exit
DES-7210(config)# vlan 3
```

```
DES-7210(config-vlan)# subvlan-address-range 192.168.196.51 192.168.196.100
```

Return to the global configuration mode, enter VLAN 4 configuration mode and set the IP address range for VLAN 4

```
DES-7210(config-vlan)# exit
DES-7210(config)# vlan 4
DES-7210(config-vlan)# subvlan-address-range  192.168.196.101 192.168.196.150
```

Return to the global configuration mode

```
DES-7210(config-vlan)# exit
```

Enter SVI mode

```
DES-7210(config)# interface vlan 2
```

#Set the IP address and subnet mask for the Super-VLAN virtual interface

```
DES-7210(config-if)# ip address 192.168.196.1 255.255.255.0
```

Return to the global configuration mode, enter VLAN 2 configuration mode and enable ARP Proxy function(enabled by default)

```
DES-7210(config-if)# exit
DES-7210(config)# vlan 2
DES-7210(config-vlan)# proxy-arp
```

View the configurations

```
DES-7210(config-vlan)# end
DES-7210# show supervlan
 supervlan id  supervlan arp-proxy  subvlan id  subvlan arp-proxy  subvlan ip range
 ---------------- ------------- -------------  ------------
 2           ON            3     ON  192.168.196.51 - 192.168.196.100
                           4    ON  192.168.196.101 - 192.168.196.150
```

11 Protocol VLAN Configuration

11.1 Protocol VLAN Technology

Every packet received on a port of the device should be classified and added to an unique VLAN. There are three possibilities:

1. If the packet has no VLAN ID (for instance, UNTAG or Priority packet), and the device only supports port-based VLAN classification, the VLAN ID in the tag added to the packet is the PVID of the inbound port.

2. If the packet has no VLAN ID (for instance, UNTAG or Priority packet), and the device supports protocol type-based VLAN classification, one of the VLAN IDs corresponding to the protocol suite configured on the inboud port will be selected as the VLAN ID in the tag added to the packet. However, if the protocol type of the packet matches none of the protocol suite configured on the inbound port, the VLAN ID will be assigned by port-based VLAN classification.

3. If the packet is tagged, its VLAN is determined by the VLAN ID in the tag.

As a protocol type-based VLAN classification technology, the protocol VLAN classifies the packets that have no VLAN ID and be of the same protocol type to the same VLAN.

The protocol VLAN configuration takes effect for Trunk port and Hybrid port, not for the Access port.

DES-7210 products support both global IP address-based VLAN classification, and packet type and Ethernet type-based VLAN classification on a port.

Because IP address-based VLAN classification is a global configuration, once configured, it will apply to all trunk ports and Hybrid ports.

1. If the incoming packet has no VLAN ID, and its IP address matches the configured IP address, this packet will be classify into the configured VLAN.

2. If the incoming packet has no VLAN ID, and its packet type and Ethernet type match those you configured on the inbound port respectively, this packet will be classified into the configured VLAN.

IP address-based VLAN classification takes precedence over packet type and Ethernet type-based VLAN classification. Hence, if you have configured both IP address-based VLAN classification and packet type and Ethernet type-based VLAN classification, and the incoming packet matches them both, IP address-based VLAN classification takes effect.

You should configure a VLAN, trunk port, hybrid port, access port and AP attributes before configuring the protocol VLAN. If you have configured protocol VLAN on a trunk port or a hybrid port, the allowed VLAN list for the trunk port and hybrid port must include all the VLANs related to the protocol VLAN.

11.2 Configuring a Protocol VLAN

11.2.1 Default Protocol VLAN

No Protocol VLAN is configured by default.

11.2.2 Configuring IP Address-based VLAN Classification

To configure IP address-based VLAN classification, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
protocol-vlan ipv4 *Ip-address* **mask** *mask-address* **vlan** *vid*	Configure IP address, subnet mask and VLAN classification.
no protocol-vlan ipv4 *IP-address* **mask** *mask-address*	Remove the IP address configuration.
no protocol-vlan ipv4	Remove all IP address configuration.
end	Exit the VLAN mode
show protocol-vlan ipv4	Show the configured IP address

Note

Specify the IP address and subnet mask in the x.x.x.x format.

The following command configures the IP address of 192.168.100.3, and the mask of 255.255.255.0 VLAN 100.

```
DES-7210# configure terminal
DES-7210(config)# protocol-vlan ipv4 192.168.100.3 mask 255. 255.255.0 vlan 100
DES-7210(config-vlan)# end
DES-7210# show protocol-vlan ipv4
ip              mask            vlan
--------------  --------------   -----

192.168.100.3   255.255.255.0   100
```

11.2.3 Configuring Packet Type and Ethernet Type Profile

To configure the packet type and Ethernet type profile, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
protocol-vlan profile *id* **frame-type** [*type*] **ether-type** [*type*]	Configure packet type and Ethernet type profile.
no protocol-vlan profile *id*	Delete an profile.
no protocol-vlan profile	Clear all profiles.
End	Exit the VLAN mode

Command	Description
show protocol-vlan profile	Show all profiles.
show protocol-vlan profile *id*	Show a profile.

For example:

```
DES-7210# configure terminal
DES-7210(config)# protocol-vlan  profile 1 frame-type  ETHERII ether-type EHTER_AARP
DES-7210(config)# protocol-vlan  profile 2 frame-type  SNAP ether-type 0x809b
DES-7210(config-vlan)# end
DES-7210# show protocol-vlan profile
profile    frame-type    ether-type      Interfaces|vid
-------     ---------   ----------        -----------
1           ETHERII     EHTER_AARP       NULL|NULL
2           SNAP         ETHER_APPLETALK  NULL|NULL
```

Note

The configuration will not become effective until the profile is applied to a port.

Before updating a profile, you must delete the profile and then reconfigure it.

11.2.4 Applying a Profile

To apply a profile, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
interface *[interface ID]*	Enter the interface configuration mode.
protocol-vlan profile *id* **vlan** *vid*	Apply a profile to this port.
no protocol-vlan profile	Clear all profiles on this port .
no protocol-vlan profile *id*	Clear a profile on this port
end	Exit the interface configuration mode

The following example applies profile 1 and profile 2 to the GE interface 1 of Slot 3. The VLAN categories are VLAN 101 and 102:

```
DES-7210# configure terminal
DES-7210(config)# interface gi 3/1
DES-7210(config-if)# protocol-vlan profile 1 vlan 101
DES-7210(config-if)# protocol-vlan profile 2 vlan 102
DES-7210(config-if)# end
DES-7210# show protocol-vlan profile
profile     frame-type  ether-type      Interfaces|vid
-------     ---------   ----------       --------------
1           ETHERII     EHTER_AARP       gi3/1|101
2           SNAP         ETHER_APPLETALK  gi3/1|102
```

Note

1. All profiles can be applied to each interface.
2. Different VIDs can be specified for the same profile on different interfaces.
3. The number of VIDs vary with different series of products. The DES-7200 series supports 4094 VLANs.

11.3 Showing a Protocol VLAN

To show a protocol VLAN, execute the following command:

Command	Description
show protocol-vlan	Show a protocol VLAN.

```
DES-7210# show protocol-vlan
ip              mask            vlan
--------------   -------------   ----
192.168.100.3   255.255.255.0   100
profile     frame-type   ether-type      Interfaces|vid
-------     ---------    ----------      --------------
1           ETHERII     EHTER_AARP       gi3/1|101
2           SNAP         ETHER_APPLETALK  gi3/1|1
```

12 Private VLAN Configuration

12.1 Private VLAN Technology

If the service provider offers a VLAN to each subscriber, the service provider supports a limited number of subscribers because one device supports 4096 VLANs at most. On the layer 3 device, each VLAN is assigned with a subnet address or a series of addresses, which results in a waste of IP addresses. In this case, private VLAN comes into being.

A private VLAN divides the layer 2 broadcast domain of a VLAN into several sub domains. Each sub domain consists of a private VLAN pair: primary VLAN and secondary VLAN.

A private VLAN domain can have multiple private VLAN pairs, and each VLAN pair represents a sub domain. All the private VLAN pairs in one private VLAN domain share a primary VLAN. Each sub domain has a different secondary VLAN IDs.

There is only one primary VLAN in each private VLAN domain. The secondary VLAN is used for layer 2 separation in the same private VLAN domain. There are two types of secondary VLANs:

- Isolated VLAN: Layer 2 communication is not possible for the ports in the same isolated VLAN. There is only one isolated VLAN in a private VLAN domain.
- Community VLAN: The ports in the same community VLAN can perform layer 2 communication, but not with the ports in other community VLANs. There can be multiple community VLANs in a private VLAN domains.

Promiscuous port, a port in the primary VLAN, can communicate with any port, including the isolated port and community port of the secondary VLAN in the same private VLAN.

Isolated port, a port in the isolated VLAN, can only communicate with the promiscuous port.

Community port, a port in the community VLAN, can communicate with other community ports in the same community VLAN as well as the promiscuous port in the primary VLAN. However, they cannot communicate with the community ports in other community VLANs and isolated ports in the isolated VLANs.

In a private VLAN, an SVI interface can be created for the primary VLAN rather then the secondary VLANs.

A port in the private VLAN can be a SPAN source port instead of a mirrored destination port.

12.2 Configuring a Private VLAN

12.2.1 Default Private VLAN Configuration

No Private VLAN is configured by default.

12.2.2 Configuring a VLAN as a Private VLAN

To configure a VLAN as a private VLAN, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
vlan *vid*	Enter the VLAN configuration mode.
private-vlan{community | isolated| primary}	Configure a private VLAN.
no private-vlan{community | isolated | primary}	Remove the configured private VLAN.
end	Exit the VLAN configuration mode.
show vlan private-vlan [*type*]	Show a private VLAN

Note

The member port in the 802.1Q VLAN cannot be declared as a private VLAN. VLAN 1 cannot be declared as a private VLAN as well. If there is a trunk or uplink port in the 802.1Q VLAN, first delete this VLAN from the allowed VLAN list. The following conditions must be met in order to make a private VLAN become active:

1. The primary VLAN is available.
2. The secondary VLANs are available.
3. The secondary VLANs are associated with the primary VLAN.

The following example configures 802.1Q VLAN as a private VLAN:

```
DES-7210# configure terminal
DES-7210(config)# vlan 303
DES-7210(config-vlan)# private-vlan community
DES-7210(config-vlan)# end
DES-7210# show vlan private-vlan community
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
303 comm   inactive  Disabled             no association
DES-7210#configure terminal
DES-7210(config)#vlan 404
DES-7210(config-vlan)# private-vlan isolated
DES-7210(config-vlan)# end
DES-7210# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
303 comm  inactive  Disabled             no association
404 isol  inactive  Disabled             no association
```

12.2.3 Associating the Secondary VLANs with the Primary VLAN

To associate the secondary VLANs with the primary VLAN, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
vlan *p_vid*	Enter the primary VLAN configuration mode.

Command	Description
private-vlan association {svlist | add *svlist* **| remove** *svlist***}**	Associate with the secondary VLANs.
no private-vlan association	Remove the association with all the secondary VLANs.
end	Exit the VLAN mode.
show vlan private-vlan [*type***]**	Show the private VLAN

For example:

```
DES-7210# configure terminal
DES-7210(config)# vlan 202
DES-7210(config-vlan)# private-vlan association 303-307,309,440
DES-7210(config-vlan)# end
DES-7210# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
202 prim  inactive   Disabled             303-307,309,440
303 comm  inactive   Disabled             202
304 comm  inactive   Disabled             202
305 comm  inactive   Disabled             202
306 comm  inactive   Disabled             202
307 comm  inactive   Disabled             202
309 comm  inactive   Disabled             202
440 comm  inactive   Disabled             202
```

Note

This operation is performed in the configuration mode of the VLAN declared as the primary VLAN.

12.2.4 Mapping Secondary VLANs to the Layer 3 Interface of the Primary VLAN

To map the secondary VLANs to the layer 3 interface of the primary VLAN, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
interface vlan *p_vid*	Enter the interface configuration mode of the primary VLAN.
private-vlan mapping {svlist | add *svlist* **| remove** *svlist***}**	Map the secondary VLANs to the layer 3 SVI of the primary VLAN.
end	Exit the interface configuration mode.

The following example configures Secondary VLAN routing:

```
DES-7210# configure terminal
DES-7210(config)# interface vlan 202
DES-7210(config-if)# private-vlan mapping add 303-307,309,440
```

```
DES-7210(config-if)# end
DES-7210#
```

Note The primary VLAN and the secondary VLANs in this process are associated.

12.2.5 Configuring a Layer 2 Interface as the Host Port of a Private VLAN

To configure a layer 2 interface as the Host Port of a private VLAN, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
interface <*interface***>**	Enter the interface configuration mode. Three kinds of interfaces are available: fastethernet, GE and 10GE.
switchport mode private-vlan host	Configure the interface as the host interface of the private VLAN.
no switchport mode	Remove the configuration.
End	Exit the interface mode.
switchport private-vlan host-association *p_vid s_vid*	Associate the layer 2 interface with the private VLAN.
no switchport private-vlan host-association	Remove the association.

For example:

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitEthernet 0/2
DES-7210(config-if)# switchport mode private-vlan host
DES-7210(config-if)# switchport private-vlan host-association
202 203
DES-7210(config-if)# end
```

Note The primary VLAN and the secondary VLANs in this process are associated.

12.2.6 Configuring a Layer 2 Interface as the Promiscuous Port of a Private VLAN

To configure a layer 2 interface as the promiscuous port of a private VLAN, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.

Command	Description
interface <*interface***>**	Enter the interface configuration mode. Three kinds of interfaces are available: Megabit, Gigabit, 10 Gigabit.
switchport mode private-vlan promiscuous	Configure the interface as the promiscuous port of the private VLAN.
no switchport mode	Remove the configuration.
switchport private-vlan mapping p_vid{svlist | add *svlist* **| remove** *svlist***}**	Map the secondary VLANs to the promiscuous port.
no switchport private-vlan mapping	Remove the mapping.

For example:

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitEthernet 0/2
DES-7210(config-if)# switchport mode private-vlan promiscuous
DES-7210(config-if)# switchport private-vlan mapping 202 add 203
DES-7210(config-if)# end
```

Note The primary VLAN and the secondary VLANs in this process are associated.

12.3 Showing a Private VLAN

12.3.1 Showing a Private VLAN

To show a private VLAN, execute the following command:

Command	Description
show vlan private-vlan [*type*]	Show the private VLAN.

```
DES-7210# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
202 prim   active   Enabled    Gi0/1      303-307,309,440
303 comm   active   Disabled   Gi0/2      202
304 comm   active   Disabled   Gi0/3      202
305 comm   active   Disabled   Gi0/4      202
306 comm   active   Disabled              202
307 comm   active   Disabled              202
309 comm   active   Disabled              202
440 comm   active   Enabled    Gi0/5      202
```

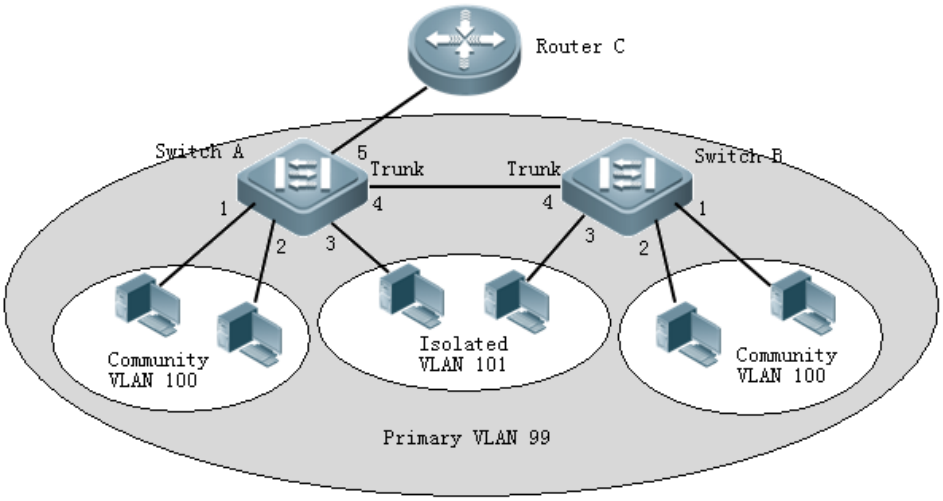
12.4 Configuration Examples

12.4.1 Private VLAN configuration on multiple switches

12.4.1.1 Configuration Purpose

Create a Primary VLAN, a Community VLAN and an Isolated VLAN and realize Private VLAN configuration on two devices. The hosts in the same Community VLAN can communicate in L2 network. The hosts in Isolated VLAN can not communicate with other hosts. But all the hosts in Private VLAN can communicate with routers.

12.4.1.2 Topology



12.4.1.3 Configuration Steps

Create Primary VLAN 99, Community VLAN 100, Isolated VLAN 101 and associate the Primary VLAN and Secondary VLANs.

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#vlan 99
DES-7210(config-vlan)#private-vlan primary
DES-7210(config-vlan)#exit
DES-7210(config)#vlan 100
DES-7210(config-vlan)#private-vlan community
DES-7210(config-vlan)#exit
DES-7210(config)#vlan 101
DES-7210(config-vlan)#private-vlan isolated
DES-7210(config-vlan)#exit
```

```
DES-7210(config)#vlan 99
DES-7210(config-vlan)#private-vlan association 100,101
DES-7210(config-vlan)#exit
```

Set interface gigabitEthernet 0/1, 0/2 in Community VLAN 100, interface gigabitEthernet 0/3 in Isolated VLAN 101, interface gigabitEthernet 0/4 as Promiscuous Port

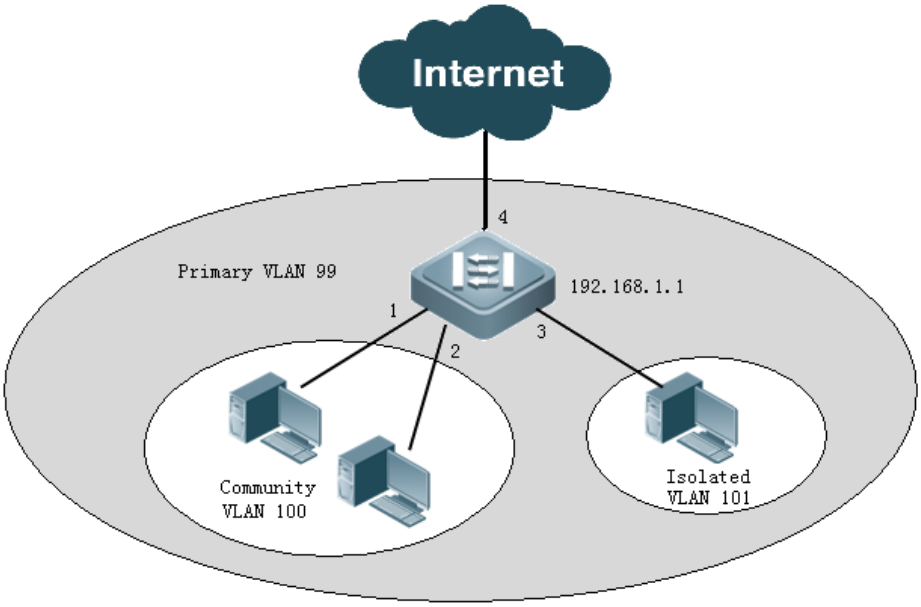
```
DES-7210(config)#interface gigabitEthernet 0/1
DES-7210(config-if)#switchport mode private-vlan host
DES-7210(config-if)#switchport private-vlan host-association 99 100
DES-7210(config-if)#exit
DES-7210(config)#interface gigabitEthernet 0/2
DES-7210(config-if)#switchport mode private-vlan host
DES-7210(config-if)#switchport private-vlan host-association 99 100
DES-7210(config-if)#exit
DES-7210(config)#interface gigabitEthernet 0/3
DES-7210(config-if)#switchport mode private-vlan host
DES-7210(config-if)#switchport private-vlan host-association 99 101
DES-7210(config-if)#exit
DES-7210(config)#interface gigabitEthernet 0/4
DES-7210(config-if)#switchport mode trunk
DES-7210(config-if)#exit
DES-7210(config)#interface gigabitEthernet 0/5
DES-7210(config-if)#switchport mode private-vlan promiscuous
DES-7210(config-if)#switchport private-vlan mapping 99 add 100-101
DES-7210(config-if)#show vlan private-vlan
VLAN  Type      Status   Routed   Ports    Associated   VLANs
----- ---------- -------- -------- --------------------------
99    primary    active    Disabled Gi0/4, Gi0/5      100-101
100   community  active   Disabled Gi0/1, Gi0/2, Gi0/4    99
101   isolated   active   Disabled Gi0/3, Gi0/4            99
```

12.4.2 Private VLAN configuration on single L3 switch

12.4.2.1 Configuration Purpose

On L3 switch supporting Private VLAN, you can set a SVI for Private VLAN. Because all VLANs(including Primary VLAN and Secondary VLANs) in the same Private VLAN can be in the same SVI, you just set an IP address for the Primary VLAN and map the Secondary VLAN to the L3 interface of Primary VLAN on the basis of the previous configuration example.

12.4.2.2 Topology



12.4.2.3 Configuration Steps

Create Primary VLAN 99, Community VLAN 100, Isolated VLAN 101 and associate the Primary VLAN and Secondary VLANs.

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#vlan 100
DES-7210(config-vlan)#private-vlan community
DES-7210(config-vlan)#exit
DES-7210(config)#vlan 101
DES-7210(config-vlan)#private-vlan isolated
DES-7210(config-vlan)#exit
DES-7210(config)#vlan 99
DES-7210(config-vlan)#private-vlan primary
DES-7210(config-vlan)#private-vlan association 100,101
DES-7210(config-vlan)#exit
```

Set interface gigabitEthernet 0/1, 0/2 in Community VLAN 100, interface gigabitEthernet 0/3 in Isolated VLAN 101, interface gigabitEthernet 0/4 as Promiscuous Port

```
DES-7210(config)#interface gigabitEthernet 0/1
DES-7210(config-if)#switchport mode private-vlan host
DES-7210(config-if)#switchport private-vlan host-association 99 100
DES-7210(config-if)#exit
DES-7210(config)#interface gigabitEthernet 0/2
```

```
DES-7210(config-if)#switchport mode private-vlan host
DES-7210(config-if)#switchport private-vlan host-association 99 100
DES-7210(config-if)#exit
DES-7210(config)#interface gigabitEthernet 0/3
DES-7210(config-if)#switchport mode private-vlan host
DES-7210(config-if)#switchport private-vlan host-association 99 101
DES-7210(config-if)#exit
DES-7210(config)#interface gigabitEthernet 0/4
DES-7210(config-if)#switchport mode private-vlan promiscuous
DES-7210(config-if)#switchport private-vlan mapping 99 add 100-101
DES-7210(config-if)#exit
```

Set a SVI(192.168.1.1) for Primary VLAN and map Secondary VLANs to the L3 interface of Primary VLAN.

```
DES-7210(config)#interface vlan 99
DES-7210(config-if)#ip address 192.168.1.1 255.255.255.0
DES-7210(config-if)#private-vlan mapping 100-101
DES-7210(config-if)#show vlan private-vlan
VLAN  Type    Status    Routed    Ports    Associated VLANs
----- ---------- -------- -------- -------------------------
99    primary    active   Enabled  Gi0/4            100-101
100   community  active   Enabled  Gi0/1, Gi0/2     99
101   isolated   active   Enabled  Gi0/3             99
```

13 802.1Q Tunneling Configuration

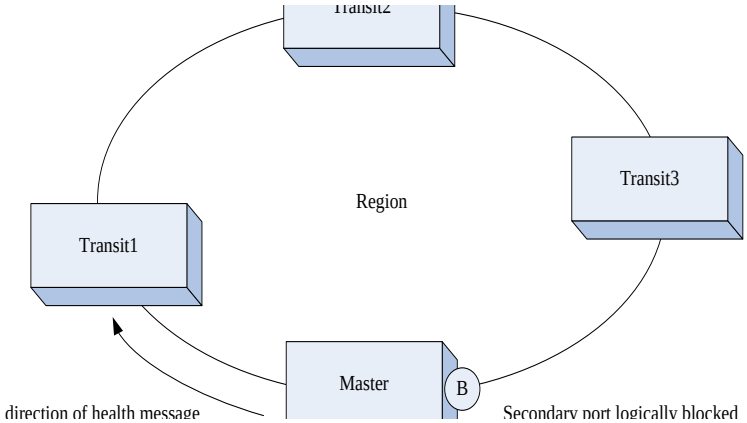
13.1 Understanding 802.1Q Tunneling

Commercial users usually have special requiremetns on the range of supported VLANs and VLAN IDs to network service providers. For users of the same vendor, VLAN ranges may be overlapped. Users may share the switching channels of the core networks. Specifying a range of VLANs for a user will impose limit on configuration and make the VLAN ID exceed 4096 defined by 802.1Q easily.

IEEE 802.1Q tunneling enables vendors to use a VLAN (the vendor VLAN) to support the users with multiple VLANs. A user's own VLAN is reserved. In this way, the traffic from different users to a vendor can be transmitted separately in the vendor's intranet, even if its VLANs are the same. Through dual tags, IEEE 802.1Q tunneling extends the range of a VLAN. A port that supports IEEE 802.1Q tunneling is called a tunnel port. When configuring a tunnel, you can assign a VLAN to the tunnel port as its dedicated VLAN. Thus, every user just needs to use the VLAN of one vendor. The user's traffic is packaged into dual-tagged frames while being transmitted through the VLAN in the vendor's network.

The traffic goes with 802-1Q tag from a trunk port on the user side to a tunnel port on the edge device of the verndor. Such an asymmetrical connection between the user and the vendor is called the asymmetrical link, because one end is a Trunk port while the other end is a tunnel port. The tunnel ports of different users are assigned with different VLANs. See the following application scheme diagram:

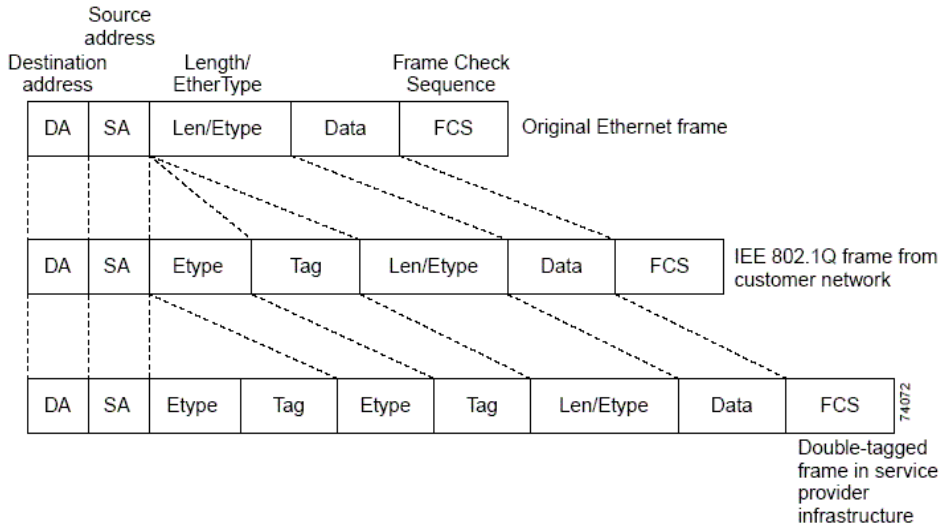
Figure-1



The frames going from a trunk port on the user side to a tunnel port on the edge device of the verndor usually carry an IEEE 802.1Q tag with a VLAN ID. After arriving the tunnel port, it will be added with another 802.1Q tag (called the vendor tag) including another VLAN ID. This VLAN ID varies with users. The user's tag will be reserved inside the frames. In this way, the frames destined to the vendor's network are dual-tagged, in which the vendor tag

contains the user's VID and the internal tag maintains the VID of the incoming frame. The following diagram shows the process of adding dual tags.

Figure-2



When the dual-tagged frames go out of the tunnel port of the edge device, the vendor tag will be removed and the frames resume their original 802.1Q frame format before they enter the edge device, and the user VLAN is restored.

All frames to the edge device are regarded as untagged frames, no matter whether they are untagged or are attached with 802.1Q tag header. When the frames go through the vendor network, they are encapsulated with the vendor tag and VLAN number (that is, the access VLAN of the tunnel port). The priority field of the vendor tag is the priority configured on the tunnel port (0 by default in case of no configuration).

In the application scheme diagram, user A is assigned with VLAN 30, and user B with VLAN 40. When the frames with 802.1Q tag arrive at the edge device, they are encapsulated with a vendor tag and become dual-tagged, the vendor tag contains VLAN 30 or 40 while the internal tag contains the original VLAN information (such as VLAN 40) of the frames. Even if the frames of both users A and B to the vendor network have VID 100, their traffic is transmitted separately in the vendor network because their vendor tags contain different VIDs. Every user can assign its VLAN range independent of other users and vendor networks.

13.2 Configuring 802.1Q tunneling

This chapter includes:

- Default 802.1Q Tunneling Configurations
- 802.1Q Tunneling Configuration Guide
- Restriction of 802.1Q Tunneling Configuration
- Configuring an 802.1Q Tunneling Port
- Configuring an Uplink Port
- Configuring the TPID Value in the Vendor Tag
- Configuring Priority Duplication of User Tag

13.3 Default 802.1Q Tunneling Configurations

By default, the 802.1Q tunneling function is disabled.

13.3.1 802.1Q Tunneling Configuration Guide

To configure 802.1Q, you need to confirm that the connection of a 802.1Q tunnel is an asymmetric link with each tunnel a dedlicated VLAN and a native VLAN and the maximum frame length are correctly configured.

Native VLAN: When you configure 802.1Q tunneling on an edge device, you need to connect a tunnel port through the 802.1Q trunk port. Frames can be switched in the vendor's intranet in many ways, for example, 802.1Q trunk port or non-trunk port. When core devices connect to each other through a trunk port the native VLAN of the trunk port should be different from the access VLAN of the tunnel port, the vendor tag of the frames whose VID is the native VLAN will be removed when they are sent out through the trunk port.

Maximum frame length: Because the frames will be added 4-byte vendor VLAN tag on the tunnel port, the maximum frame length increases from 1518 bytes to 1522 bytes.

Uplink port: The uplink port is used to connect the uplink devices or vendor devices in other networks. For example, the trunk ports of the vendor network in Figure-1. The uplink port is actually a special trunk port. The difference is that the packets that go out of the uplink port are tagged, but the packets that go out of the trunk port are not tagged if they are forwarded from the native VLAN.

TPID value in the vendor Tag: TPID (Tag Protocol Identifier) is a field in the VLAN Tag. The IEEE 802.1Q protocol specifies that the value of this field is 0x8100. Ethernet frame TAG includes 4 fields: TPID User Priority CFI VLAN ID. By default, TPID value is 0x8100. But TPID value for the devices of some manufacturer is 0x9100 or other value. DES-7210 products provide port-based packet TPID configuration function to make the TPID value be compatible with those devices. Users can set TPID value on a port by themselves. When a packet is forwarded through the port, the TPID value for outer Vlan Tag of the packet will be replaced by the TPID value users have set on the port.

Tag priority duplication: It refers to copy the priority value of the inner tag (or user tag) to the priority value of the outer tag (or vendor tag) in case of dual tags.

13.3.2 Restriction of 802.1Q Tunneling Configuration

The following restrictions apply to 802.1Q tunneling configuration:

- The routed ports cannot be configured as tunnel ports.
- The AP ports can be configured as tunnel ports.
- The 802.1x function cannot be enabled on the port configured as a tunnel port.
- Cluster cannot be enabled on the port configured as a tunnel port.
- The STP algorithm cannot be added to the port configured as a tunnel port.
- GVRP cannot be enabled on the port configured as a tunnel port.
- System-guard cannot be enabled on the port configured as a tunnel port.
- For the DES-7200 series, it's recommended to configure the outgoing port of the user's network that connects to the vendor network as an Uplink port. If you have configured the TPID of the vendor tag of 802.1Q tunneling in the user's network, it's required to configure the same TPID of the vendor tag on the uplink port.

13.3.3 Configuring an 802.1Q Tunneling Port

In the global configuration mode, input the **interface** command to enter the interface configuration mode. Follow these steps to configure a tunnel port:

Command	Description
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
switchport mode dot1q-tunnel	Set the port as a dot1q-tunnel port.
switchport dot1q-tunnel allowed vlan [**add**] { **tagged** | **untagged** } *v_list*	Add the allowed VLAN for dot1q-tunnel port and specify that whether the VLAN is tagged or not when outputting the packet in the correspondent allowed VLAN.
switchport dot1q-tunnel allowed vlan remove *v_list*	Delete the allowed VLAN for dot1q-tunnel port.
switchport dot1q-tunnel native vlan *VID*	Set the default VLAN for dot1q-tunnel port.
end	Exit the interface mode.
show running-config	View the global configuration.

Note

It is recommended not to set the native VLAN of trunk port in the vendor network as the default VLAN of tunnel port, because the Tag with native VID will be stripped off on trunk port.

The following example demonstrates how to configure a 802.1q tunneling port:

```
DES-7210(config)# interface fastEthernet 0/1
DES-7210(config-if)# switchport mode access vlan 22
DES-7210(config-if)# switchport dot1q-tunnel
DES-7210(config)# end
```

13.3.4 Configuring an Uplink Port

In the global configuration mode, input the **interface** command to enter the interface configuration mode. Follow these steps to configure an uplink port:

Command	Description
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
switchport mode uplink	Configure the port as an uplink port.
end	Exit the interface mode.

The following example demonstrates how to configure an uplink port:

```
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode up-link
DES-7210(config)# end
```

13.3.5 Configuring the TPID Value of the Vendor Tag

In the global configuration mode, input the **interface** command to enter the interface configuration mode. Follow these steps to configure the TPID value in the vendor tag:

Command	Description
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
frame-tag tpid *tpid*	Set the TPID value of the vendor tag. If you want to set it as 0x9100, directly enter frame-tag tpid 9100. Note that the hexadecimal system is used by default. This function takes effect when configuring the outgoing port.
end	Exit the interface mode.
show frame-tag tpid	View the TPID value list on the port.

The following example demonstrates how to configure TPID:

```
DES-7210(config)# interface gigabitethernet 0/1
DES-7210(config-if)# frame-tag tpid 9100
DES-7210(config)# end
DES-7210# show frame-tag tpid interface gigabitethernet 0/1
Port     tpid
------- -------------
Gi0/1    0x9100
```

13.3.6 Configuring Priority Duplication of the User Tag

In the global configuration mode, input the **interface** command to enter the interface configuration mode. Follow these steps to configure priority duplication:

Command	Description
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
inner-priority-trust enable	Copy the priority value of the inner tag (user tag) to the priority value of the outer tag. (vendor tag).
end	Exit the interface mode.
show inner-priority-trust	View the priority duplication configuration of the user tag.

Note

You can configure priority duplication of the user Tag only on dot1q-tunnel port, whose priority is higher than QOS in the trusted mode but lower than flow-based QOS.

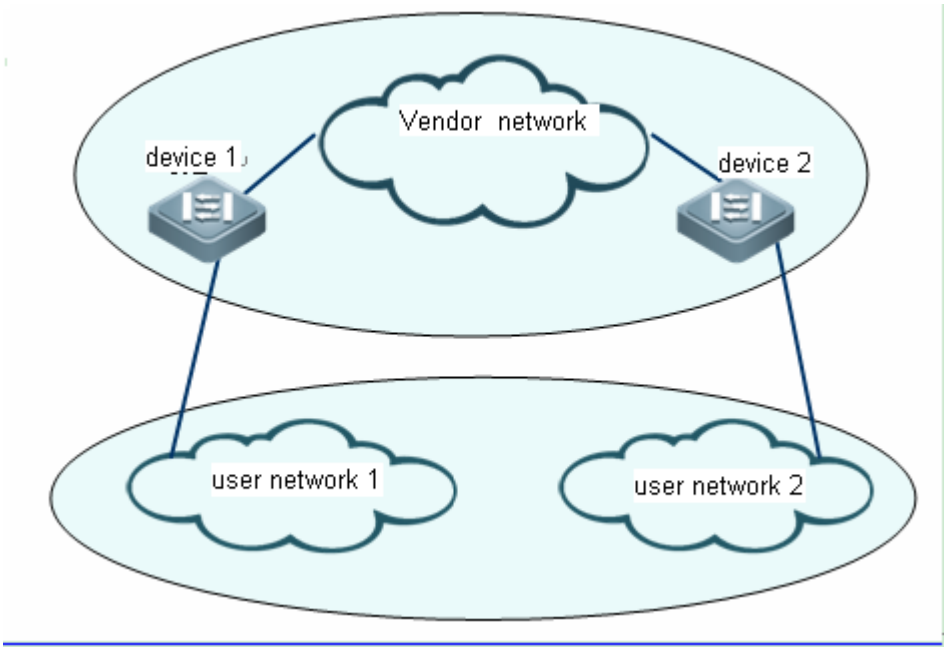
The priority duplication of the untagged packets on the dot1q-tunnel port on the line card 7200-24GE takes no effect. But the dot1q-tunnel port on other line cards duplicate the priority of the untagged packets by setting the inner priority value at 0.

The following example shows how to configure the priority duplication of the user tag:

```
DES-7210(config)# interface gigabitethernet 0/1
DES-7210(config-if)# inner-priority-trust enable
DES-7210(config)# end
DES-7210# show inner-priority-trust interface gigabitethernet 0/1
Port     inner-priority-trust
------   --------------------

Gi0/1    enable
```

13.4 Configuring Transparent Transmission of L2 Protocol Message

In some environment, you need to transparently transmit L2 protocol message in some network. Take the following figure for example, on the inputting port, device1 modifies the destination MAC address of L2 protocol message from user network as particular multicast MAC address. And then in the vendor network, the modified message is forwarded as datagram in the VLAN belongs to the user. On the outputting port, device 2 recognizes the modified message, restores the destination MAC address to be the original source MAC address of L2 protocol message and sends the L2 protocol message to the specified user network. In this environment, you should enable the function of transparent transmission between the interfaces of device 1/2 and user network.



13.4.1 Configuring Transparent Transmission of stp Protocol Message

In the privileged mode, you can configure transparent transmission of STP protocol message as the following steps:

Command	Description
configure terminal	Enter the global configuration mode.
l2protocol-tunnel stp	Configure to enable transparent transmission of STP protocol message globally.
interface *interface-id*	Enter the interface configuration mode.
l2protocol-tunnel stp enable	Enable transparent transmission of STP protocol message on the interface.
show l2protocol-tunnel stp	View the configuration.

An example below shows how to enable transparent transmission of STP protocol message:

```
DES-7210# configure
DES-7210(config)# l2protocol-tunnel stp
DES-7210(config)# interface fa 0/1
DES-7210(config-if)# l2protocol-tunnel stp enable
```

13.4.2 Configuring Transparent Transmission of gvrp Protocol Message

In the privileged mode, you can configure transparent transmission of GRVP protocol message as the following steps:

Command	Description
configure terminal	Enter the global configuration mode.
l2protocol-tunnel gvrp	Configure to enable transparent transmission of GRVP protocol message globally.
interface *interface-id*	Enter the interface configuration mode.
l2protocol-tunnel gvrp enable	Enable transparent transmission of GRVP protocol message on the interface.
show l2protocol-tunnel gvrp	View the configuration.

An example below shows how to enable transparent transmission of G protocol message:

```
DES-7210# configure
DES-7210(config)# l2protocol-tunnel gvrp
DES-7210(config)# interface fa 0/1
DES-7210(config-if)# l2protocol-tunnel gvrp enable
```

Note

After globally enabling transparent transmission of protocols, transparent transmission takes effect on the interfaces which do not join the protocol computation. If the interface receives the packet that the destination MAC address is particular multicast address, it implies that there is something wrong in the multinet and the interface will discard the packet directly.

13.5 Configuring Protocol-based vid Change Policy List

Caution

Protocol-based vid change policy takes effect after creating a destination VLAN of this policy and adding the port to this destination VLAN. Therefore, it is recommended that users shall create a destination VLAN and add the port to the destination VLAN before policy configuration.

13.5.1 Configuring vid Add Policy List

For the input packet on **dot1q-tunnel** port, sometimes you need to add VID of different outer TAG when the packet is forwarded. Execute **dot1q outer-vid** to specify inner-vid list to add outer VID of outer TAG; execute **no dot1q outer-vid** to delete the corresponding configuration. According to this command, to make the output packet as the original inner TAG message, you can specify inner VLAN to add the same outer VID as innner VID and add the exit port to the UNTAG port set in the VLAN. For the detailed information, please refer to command reference.

Configuration steps:

Command	Description
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
switchport mode dot1q-tunnel	Configure port as dot1q-tunnel.
dot1q outer-vid *vid* **register inner-vid** *v_list*	Configure VID policy of adding outer TAG based on protocol.
no dot1q outer-vid *vid* **register inner-vid** *v_list*	Delete VID policy of adding outer TAG based on protocol.
end	Exit the interface mode.
show registration-table	View the configuration.

The example below configures VID in the TAG of input packet as 4-22, adding VID of outer TAG to be 3:

```
DES-7210# configure
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode dot1q-tunnel
DES-7210(config-if)# switchport dot1q-tunnel allowed vlan add tagged 3
DES-7210(config-if)# dot1q outer-vid 3 register inner-vid 4-22
DES-7210(config-if)# end
```

The DES-7200 series only supports the function of mapping 768 consecutive inner VIDs to the same outer VID. It is recommended to set the member ports before setting this function on an AP. You shall make sure that the line cards are online when setting this function, or the configured capacity may be inconsistent with actual capacity.

Note

When learing the MAC address, the incoming packets on tunnel port in the non-E series line card of the DES-7200 series can only learn the VID of inner TAG(the VID in the user network) when adding the outer TAG. Because the VID in user network plays no role in the vendor network, the packets that need adding the outer TAG can not learn the MAC address on tunnel port in the vendor network. The learnt MAC address is the destination MAC address for the incoming packet on uplink port. When the switch searches for the MAC address list by VID of outer TAG, it will fail and the packets will be broadcast in the VLAN of the outer TAG, leading to the bandwidth waste.

13.5.2 Configuring vid Modify Policy List

For the input packet on Access,Trunk,Hybrid port, sometimes you need to modify VID of different outer TAG when the packet is forwarded. Execute **dot1q relay-vid vlan** to modify the specified local vid list as new VID; execute **no dot1q outer-vid vlan** to delete the corresponding configuration. For the detailed information, please refer to command reference.

Configuration steps:

Command	Description
Configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
switchport mode trunk	Configure switchport as Access,Trunk or Hybrid port.
dot1q relay-vid *vid* **translate local-vid** *v_list*	Configure VID policy of modifying outer TAG based-on protocol.
no dot1q relay-vid *vid* **translate local-vid** *v_list*	Delete VID policy of modifying outer TAG based-on protocol.
end	Exit the interface mode.
show translation-table	View the configuration.

Note

The 7200-24GE line card supports the function.

The example below configures VID in the TAG of input packet as 10-20, modifying VID as 100:

```
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode trunk
DES-7210(config-if)# dot1q relay-vid 100 translate local-vid 10-20
```

```
DES-7210(config-if)# end
```

13.6 Configuring Flow-based vid Change Policy List

Caution It is recommended to set the native VLAN of the trunk port on the local device to be consistent with that of the trunk port on the remote device. Otherwise, the trunk port cannot forward packets properly.

13.6.1 Configuring vid Add Policy List

For the input packet on **dot1q-tunnel** port, according to different packet contents, sometimes you can specify different VIDs when the forwarded packet is added outer TAG by executing command **traffic-redirect access-group** acl **nested-vlan** VID **in.** When the input packet on **dot1q-tunnel** port matches acl, you can specify the VID as command-specified value when the forwarded packet is added with outer TAG. Execute **no traffic-redirect access-grou**p acl **nested-vlan** to delete the corresponding configuration. For the detailed information, please refer to command reference.

Configuration steps:

Command	Description
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
switchport mode dot1q-tunnel	Configure interface as dot1q-tunnel port.
traffic-redirect access-group *acl* **nested-vlan** *vid* **in**	Configure VID policy of adding outer TAG based on flow.
no traffic-redirect access-group *acl* **nested-vlan**	Delete VID policy of adding outer TAG based on flow.
end	Exit the interface mode.
show traffic-redirect	View the configuration.

Note
1. When using line cards below to configure this function, the outgoing port and dot1q-tunnel must be in different chips and dot1q-tunnel will be configured with flow isolation. Those line cards are: 7200-24P, 7200-24, 7200-48, 7200-48P, 7200-2XG, 7200-4XG.
2. VID change policy list based on flow is prior to that based on protocol.

The example below configures to add VID of the input packet whose source address of interface is 1.1.1.3 as 9:

```
DES-7210# configure
DES-7210(config)# ip access-list standard 20
DES-7210(config-std-nacl)# permit host 1.1.1.3
```

```
DES-7210(config-std-nacl)# exit
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode dot1q-tunnel
DES-7210(config-if)# traffic-redirect access-group 20 nested-vlan 10 in
DES-7210(config-if)# end
```

13.6.2 Configuring Modify Policy List of Outer vid

For the input packet on Access,Trunk,Hybrid port, according to different packet contents, sometimes you can modify VID of outer TAG by executing command **traffic-redirect access-group** acl **outer-vlan** VID **in.** When the input packet matches acl, you can modify the VID in the outer TAG of packet as command-specified value. Execute **no traffic-redirect access-grou**p acl **outer-vlan** to delete the corresponding configuration. For the detailed information, please refer to command reference.

Configuration step:

Command	Description
configure terminal	Enter the gloabal configuration mode.
interface *interface-id*	Enter the interface configuration mode.
switchport mode trunk	Configure switchport as Access,Trunk or Hybrid port.
traffic-redirect access-group *acl* **outer-vlan** *vid* **in**	Configure VID policy of modifying outer TAG based on flow.
no traffic-redirect access-group *acl* **outer-vlan**	Delete VID policy of modifying outer TAG based on flow.
end	Exit the intereface mode.
show traffic-redirect	View the configuration.

Note

1. The 7200-24GE line card supports this function.
2. Outer VID modify policy list based on flow is prior to that based on protocol.

The example below configures to modify outer VID of the input packet whose source address of interface is 1.1.1.1 as 3:

```
DES-7210# configure
DES-7210(config)# ip access-list standard 2
DES-7210(config-std-nacl)# permit host 1.1.1.1
DES-7210(config-std-nacl)# exit
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode trunk
DES-7210(config-if)# traffic-redirect access-group 2 outer-vlan 3 in
DES-7210(config-if)# end
```

13.6.3 Configuring Modify Policy List of Inner vid

For the input packet on Access,Trunk,Hybrid port, according to different packet contents, sometimes you can modify VID of inner TAG by executing command **traffic-redirect access-group** acl **inner-vlan** VID **out.** When the input packet matches acl, you can modify the VID in the inner TAG of packet as command-specified value. Execute **no traffic-redirect access-grou**p acl **inner-vlan** to delete the corresponding configuration. For the detailed information, please refer to command reference.

Configuration step:

Command	Description
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the intereface configuration mode.
switchport mode trunk	Configure switchport as Access,Trunk or Hybrid port.
traffic-redirect access-group *acl* **inner-vlan** *vid* **out**	Configure VID policy of modifying inner TAG based on flow.
no traffic-redirect access-group *acl* **inner-vlan**	Delete VID policy of modifying inner TAG based on flow.
end	Exit the interface mode.
show traffic-redirect	View the configuration.

Note

1. The 7200-24GE line card supports this function.
2. When adding member port to or deleting member port from AP port, the VID add or modify policy configured on AP port will be deleted. Therefore, it is recommended that you should configure VID policy on AP after configuring AP member port.
3. If the packet outer Tag VID is the same as the native VID, the packet outer Tag will be stripped off in the out direction. No inner tag in this packet at this time will result in the failure of matching inner tag, that is, the policy of inner tag modification will not take effect.
4. The policy of inner VID modification is processed after trusted mode configuration. Therefore, when matching DSCP or outer COS in the associated flow policy, the value to be matched with is the one modified in the trusted mode.

The example below configures to modify outer VID of the input packet whose source address of interface is 1.1.1.2 as 6:

```
DES-7210# configure
DES-7210(config)# ip access-list standard to_6
DES-7210(config-std-nacl)# permit host 1.1.1.2
DES-7210(config-std-nacl)# exit
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode trunk
DES-7210(config-if)# traffic-redirect access-group to_6 inner-vlan 6 out
```

```
DES-7210(config-if)# end
```

14 MAC Address Configuration

Using the information in the MAC address table, the Ethernet switch rapidly searches for the address to which the messages in the data link layer are forwarded. This chapter describes the MAC address configuration, including the following sections:

- Understanding the MAC Address Table
- Default Configuration
- Configuring the Dynamic Address
- Configuring the Dynamic Address Aging Time
- Configuring the Management Learning mode of Dynamic Address
- Configuring the Limit of Dynamic Addresses for a VLAN
- Configuring the Static Address
- Configuring the Filtering Address
- Configuring the MAC Addres Change Notification Function
- Configuring IP address and MAC address binding
- Configuration Examples

14.1 Understanding the MAC Address Table

14.1.1 Overview

Layer-2 forwarding, a major function of the Ethernet Switch, is to forward the messages by identifying the data link layer information. The switch forwards the messages to the corresponding interface through the destination MAC addresses carried by the messages, and stores the information about the relationship between the destination MAC address and the interface in the MAC address table.

All the MAC addresses in the MAC address table are associated with the VLAN. Different MAC addresses are allowed to be in the same VLAN. Each VLAN maintains a MAC address table logically. It is possible that a MAC address learned by a VLAN is unknown to other VLANs and shall be learned again.

The MAC address contains the following information:

State	VLAN	MAC address	Interface

Figure-1 MAC Address Entry

- State: Dynamic,static or filtering address.
- VLAN: VLAN to which the MAC address belongs;
- MAC address: the MAC address information in the entry;
- Interface: the information of the interface with which the MAC address is correspondent.

The MAC address entries are updated and maintained by the following two ways:

- Learning the Dynamic Address
- Configuring the Dynamic Address Manually

The switch searches for the corresponding outgoing forward interface according to the destination MAC address and the VLAN ID for the message in the MAC address table, and then forwards the messages in unicast, multicast and broadcast way.

- Unicast forwarding: if the switch searches for the corresponding entry of the packet destination MAC address and VLAN ID in the MAC address table and the outgoing forward interface is sole, the packets are forwarded through this interface.
- Multicast forwarding: if the switch searches for the corresponding entry of the packet destination MAC address and VLAN ID in the MAC address table and this entry is correspondent with a group of outgoing forward interfaces, the packets are forwarded through the interfaces directly.
- Broadcast forwarding: if the switch receives the packets destined to ffff.ffff.ffff, or it can not search for the corresponding entry in the MAC address table, the packets are sent to the VLAN to which belongs and forwarded through the outgoing interfaces except for the incoming interface.

Note

This chapter describes management of dynamic, static and filtering addresses. For the management of multicast address, please refer to *IGMP Snooping Configurations*.

14.1.2 Learning the Dynamic Address

14.1.2.1 Dynamic Address

A dynamic address is the MAC address learnt automatically from the packets received by the switch. Only the dynamic address be removed by the aging mechanism of the address table.

14.1.2.2 Address Learning Process

In general, it maintains the MAC address table by learning the dynamic address. The operation principle is:

The MAC address table in the switch is null and User A shall communicate with User B. User A sends the packet to interface GigabitEthernet 0/2 and the MAC address for User A is learnt in the MAC address table.

There is no source MAC address for User B in MAC address table. Therefore, the switch sends the packets to all ports except for the ports of User A in broadcast form. User C can receive the packets sent from User A and don’t belong to User A.

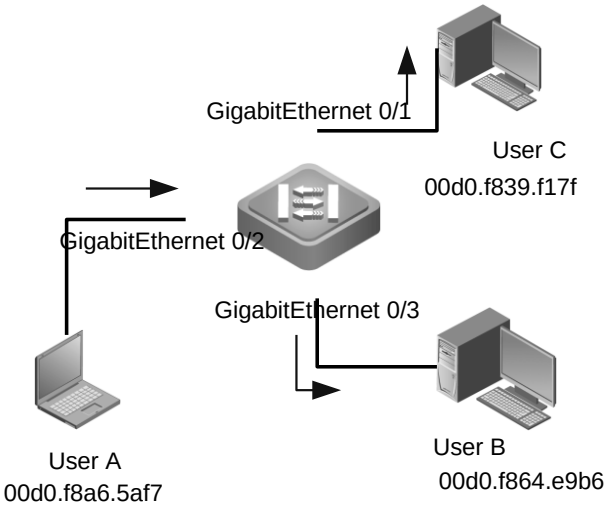


Figure2 Dynamic Address Learn (Step 1)

Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2

Figure3 MAC Address Table1

Upon receiving the packets, UserB will send them to UserA through interface GigabitEthernet 0/3. The MAC address for UserA exits in the MAC address table. Therefore, the packets are forwarded to interface GigabitEthernet 0/2 in the unicast form and the switch learns the MAC address for UserB at the same time. The difference from the step one is that UserC can not receive the packets sent from UserB to UserA.

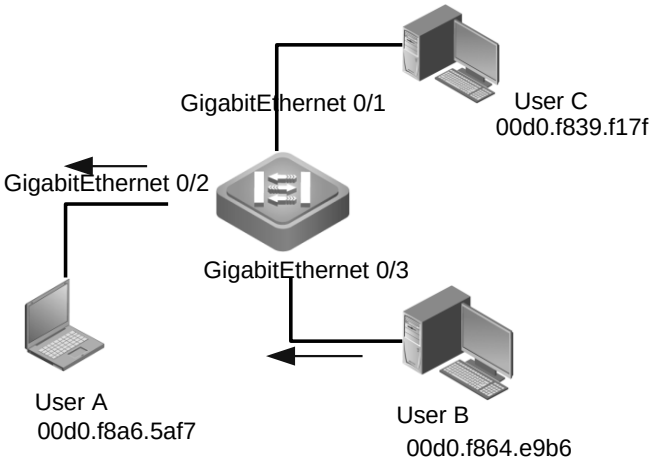


Figure4 Dynamic Address Learn (Step 2)

Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2
Dynamic	1	00d0.f8a4.e9b6	GigabitEthernet 0/3

Figure5 MAC Address Table 2

After the communication between UserA and UserB, the switch learns the source MAC addresses for UserA and UserB. The mutual packets between UserA and UserB are forwarded in the unicast form and UserC can not receive them again.

Caution	In the stack system, the address tables of each member device are asynchronous. For example: Suppose the device A and device B stack and the device A is the host, send the broadcast packets to the device A, the port receiving the frames on the device A will learn the MAC1 address, which will be recorded in the address table. Since the packets are broadcasted to the device B through the stack port, the stack port on the device B will also learn this MAC1 address but not record it in the address table. Removing the MAC address learned from the frame-receiving port on the device A, the MAC1 address in the address table will also be removed. However, the stack port of the device B still learn this MAC address, the inconsistency of the hardware address table of the master and slave devices occurs. Send the packets destined to MAC1 address to other ports of the device A, those packets can not be broadcasted to the device B for the reason that the MAC1 address has already been learned by the stack port of the device B. After this MAC address ages out, the packets are broadcasted to the port of the device B.

14.1.2.3 Address Aging

The capacity of MAC address is restricted. The switch updates the MAC address list by learning new addresses and aging out unused addresses.

For an address in the MAC address table, if the switch has not received any packet from the MAC address for a long time (depending on the aging time), the address will be aged out and removed from the MAC address table.

14.1.3 Management Learning mode of the Dynamic Address

Product Support	Only the DES-7200 series supports the management learning mode configuration of the dynamic address.

The DES-7210 high-density modular Ethernet switches support the management learning mode of the dynamic address, including:

- Uniform MAC address learning mode
- Dispersive MAC address learning mode

14.1.3.1 Uniform MAC address learning mode

A. Operation Mechanism

In this mode, multiple line cards in the switch learn the MAC addresses, with each line card learning the MAC address independently. The MAC address learn process is described as follows:

The UserA under the Line Card1 sends the packets to the UserB. For the MAC address for the UserB does not exist on the switch, the packets will be sent to all line cards on the switch in broadcast form.

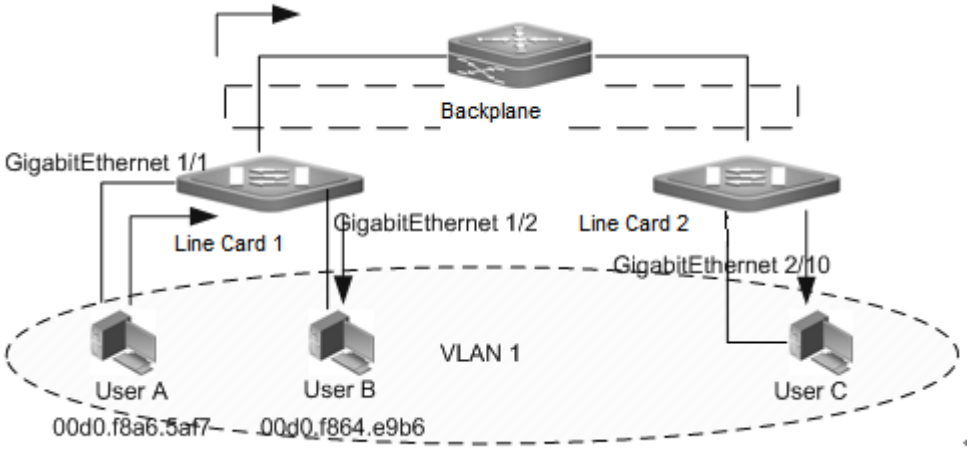


Figure-6 Uniform MAC Address Forward Process 1

The UserA under the Line Card1 sends the packets to the UserB. For the MAC address for the UserB does not exist on the switch, the packets will be sent to all line cards on the switch in broadcast form. The switch learns the address after receiving the packets from the UserA. At this time, Line Card 1 and Line Card 2 both receive the packets from the UserA, so they learn the MAC address for the UserA simultaneously.

MAC address table(Line card 1)			
Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 1/1

MAC address table(Line card 2)			
Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 1/1

Figure-7 Uniform MAC address Learning: MAC address table

After receiving the packets from the UserA, the UserB sends the reply packets to the Line Card1. Since the Line Card 1 has learned the MAC address for the UserA, the packets will be sent to the port of UserA in the unicast form and will not be sent to the Line Card 2.

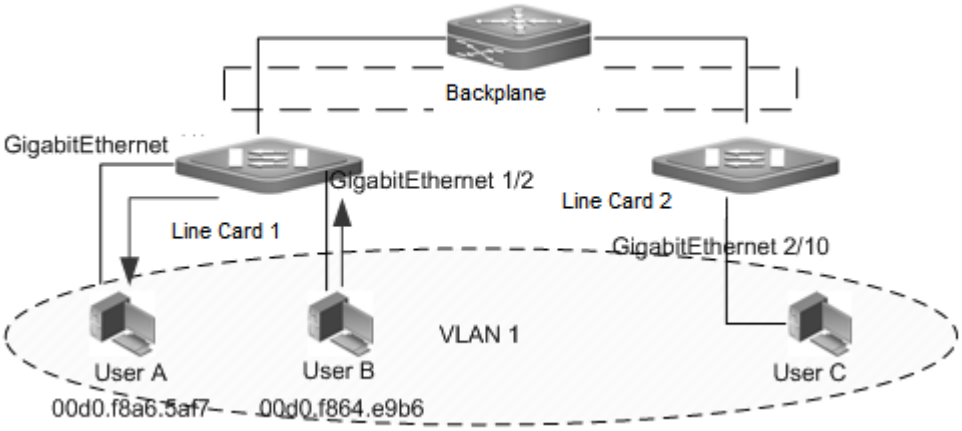


Figure-8 Uniform MAC Address Forward Process 2

For the reply packets sent by the UserB are forwarded to the port of UserA through the Line Card 1, the switch only learn the Mac addresses on the Line Card 1 and the MAC addres for UserB can not be learned on the Line Card 2.

MAC address table(Line card 1)			
Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 1/1
Dynamic	1	00d0.f864.c9b6	GigabitEthernet 1/2

MAC address table(Line card 2)			
Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 1/1

Figure-9 Uniform MAC address Learning: MAC address table 2

The advantages of the uniform MAC address learning:

The capacity of the address table for all linecards in the switch is allocated on demand: If two users exchange the packets on the same line card, only the MAC address space of the line card 1 is occupied.

High System Performance: Small system expenditure since the internal system adopts the dispersive MAC address learning mode.

The disadvantages of the uniform MAC address learning: since the address tables for all line cards in the switch are asynchronous, the packets are sent in the unicast form for Line Card 1 while in the broadcast form for Line Card 2.

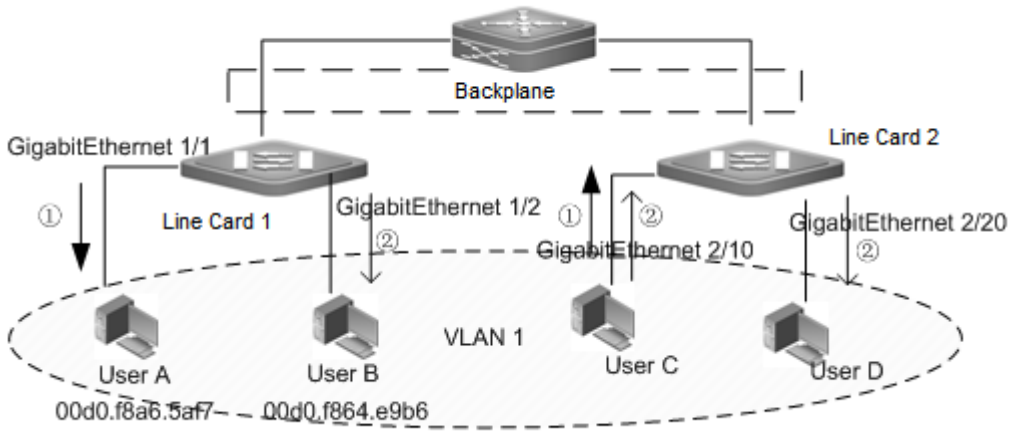


Figure-10 Uniform MAC address Learning: Unicast and Multicast Packets Forward

When the UserC under the Line Card 2 sends a packet to the UserA, since the Line Card 2 has learned the MAC address for the UserA, the packet will be forwarded to the UserA in the unicast form.

When the UserC under the Line Card 2 sends a packet to the UserB, since the Line Card 2 has learned the MAC address for the UserB, the packet will be forwarded in the broadcast form. At this time, the UserD that is in the same VLAN of UserC also receives the packet. The packet will be forwarded in the unicast form to the UserB after being sent to the Line Card 1.

B. MAC Address Synchronization

In the uniform MAC address learning mode, the Ethernet switch supports the MAC address synchronization function. All line cards in the switch no longer learn the MAC address in the dispersive MAC address learning mode and synchronize the new MAC address learned by any line card.

The advantages of the MAC address synchronization: the MAC addresses within the switch are synchronous. It helps prevent the packets in the network from being forwarded in the broadcast form if the number of users connecting to the switch exceeds the MAC address table limit.

The disadvantages of the MAC address synchronization:

- Occupy the large space of the MAC address table: Even though two users exchange the packets on the same line card, the MAC address space of other line cards will also be occupied.
- Decrease the System Performance: The system performance is decreased and it needs the extra synchronous expenditure because the line card adopts the non-dispersive MAC address learning mode.

Caution

With the dynamic MAC address synchronization enabled, every time the address learning or address aging occurs, the corresponding operation is executed by the switch. Frequent address learning or address aging in a short time consumes a lot of CPU resources, which results in the high utilization of CPU. The administrator shall enable this function prudently.

14.1.3.2 Dispersive MAC address learning mode

In the uniform mode, all line cards join the address learning in all VLANs. Even though a port in a specified VLAN is only distributed on one line card, other line cards still learns the address when receiving the packet from this specified VLAN.

In the dispersive mode, the line card is responsible for learning the address only in the VLAN where the port that is on this line card is in, not learning the address in other VLANs.

In the VLAN 1, all ports are on the line card 1. In the VLAN 2, all ports are on the line card 2. In the VLAN 3, all ports are on the line card 3.

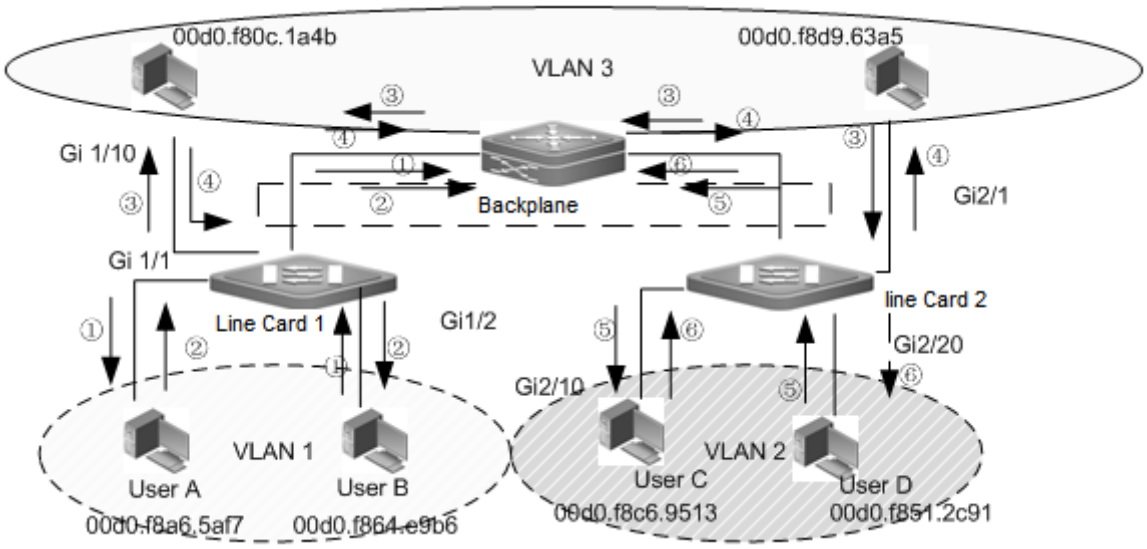


Figure-11 Separated MAC address Learning Forward

If the address tables of the line card 1 and line card 2 are null, the UserA and the UserB exchanges the packets in VLAN1, the UserC and the UserD exchanges the packets in VLAN2, the UserE and the UserF exchanges the packets in VLAN3. The following shows the MAC address table learned by the switch:

MAC address table(Line card 1)			
Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 1/1
Dynamic	1	00d0.f864.c9b6	GigabitEthernet 1/2
Dynamic	3	00d0.f8d9.63a5	GigabitEthernet 2/1
Dynamic	3	00d0.f80c.1a4b	GigabitEthernet 1/10

MAC address table(Line card 2)			
Status	VLAN	MAC address	Interface
Dynamic	2	00d0.f8c6.9513	GigabitEthernet 2/10
Dynamic	2	00d0.f851.2c91	GigabitEthernet 2/20

Dynamic	3	00d0.f8d9.63a5	GigabitEthernet 2/1
Dynamic	3	00d0.f80c.1a4b	GigabitEthernet 1/10

Figure-12 Separated MAC address Learning: MAC address table

In the dispersive mode, the line card learns the neccesary address information only. To this end, it maximizes the resources of the MAC address table in the system.

Caution

1. In the dispersive mode, theoretically, when the line cards in different models are mix-inserted, the total capacity of the address table equals to the sum of the capacity of the address table of all line cards. In the uniform mode, when the line cards in different models are mix-inserted, the minimum capacity of the address table of the line card determines the maximum total capacity of the address table. For example, in the dispersive mode, seven line cards of 7200-48P and one line card of 7200-24 are mix-inserted, the total capacity of the address table equals to 32K*7+16K; while in the uniform mode, the total capacity of the address table is 16K.
2. In the dispersive mode, for 7200-4XG, to reach the limited capacity, the port 1 and 2, 3 and 4 on this line card can not be configured in the same VLAN.

14.1.4 Limit of Dynamic Addresses for a VLAN

The capacity of the MAC address table on the Ethernet switch is limited and shared by all VLANs. To prevent large amout of dynamic addresses in a VLAN from occupying the whole MAC address table and disabling other VLANs to learn the dynamic addresses which leads the packets in other VLANs to be forwarded in the broadcast way, the switch provides the limit of dynamic addresses for a VLAN. The user can specify the number of dynamic addresses learned in each VLAN and configure the upper limit of dynamic addresses for each VLAN.

For the VLAN with the limit of dynamic addresses configured, only the specified MAC addresses can be learned. The MAC addresses that exceeds the upper limit are not learned and the packets destined to those MAC addresses are forwarded in the broadcast form.

Caution

If the upper limit of the dynamic addresses for a VLAN is less than the number of the learned dynamic addresses in the current VLAN, the Ethernet switch no longer learns the address in the VLAN and learns again untill the the number of the addresses is less than the upper limit due to the address aging and deletion.

Product Support

For the DES-7200 series, only 7200-24GE supports this function.

14.1.5 Static Address

A static address is a manually configured MAC address. A static address is the same as a dynamic address in terms of funciton. However, you can only manually add and delete a static address rather than learn and age out a static address. A static address is stored in the configuration file and will not be lost even if the device restarts.

By configuring the static address manually, you can bind the MAC address for the network device with the interface in the MAC address table.

14.1.6 Filtering Address

A filtering address is a manually configured MAC address When the device receives the packets from a filtering address, it will directly discard them. You can only manually add and delete a filtering address rather than age it out. A filtering address is stored in the configuration file and will not be lost even if the device restarts.

If you want the device to filter some invalid users, you can specify their MAC addresses as filtering addresses. Consequently, these invalid users cannot communicate with outside through the device.

Caution A filtering address is invalid for the packets sent to the CPU. For example, the L2 source MAC address for an ARP packet is a filtering address, this ARP packet can still be sent to the CPU, but can not be forwarded.

14.1.7 MAC Address Change Notification

The MAC address notification function is an effective way to let you know user changes for the devices in a network.

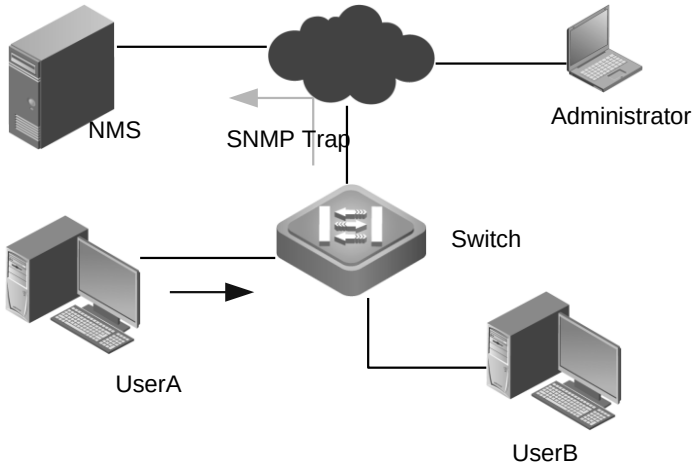


Figure-13 MAC address Change Notification

After the MAC address change notification is enabled, the MAC address change notification infornation is generated and sent in the SNMP Trap message form to the specified NMS when the switch learns a new MAC address or ages out a learned MAC address.

The notification about adding a MAC address lets you know a newcomer (identified by the MAC address) is using the device. The notification about deleting a MAC address (in the case of that the user did not communicate with the device within the aging time) lets you know that a user does not use the device any more.

When many users use the device, lots of MAC address changes may occur in a short period of time (for example, when the device is powered on), incurring additional network traffic. In order to release network burden, you can set the time interval of sending MAC address notifications. All the notification messages within the interval time will be bundled in one SNMP Trap message. So one notification message includes multiple MAC address changes, reducing netowrk traffic significantly.

When a MAC address change notification is generated, it will be recorded in the MAC address notification history list. Then even though the NMS has not been specified to

receive the SNMP Trap message, the administrator can view the information about address change by checking the MAC address notification history list.

Caution

MAC address change notification is effective only for dynamic addresses, not for static addresses and filtering addresses.

14.1.8 IP address and MAC address Binding

14.1.8.1 Overview

IP address and MAC address binding lets you filter pakcets. After you bind an IP address and a MAC address, the switch will only receive the IP packets whose source IP address and MAC address match the binding address ;or it will be discarded.

Taking advantages of IP address and MAC address binding, you can check the legality of the input sources. Note that this funciton takes precedence over 802.1X, port-based security and ACL effectiveness.

14.1.8.2 Address Binding Mode

The address binding mode divides into 3 modes: compatible, loose and strict. By default, the address binding mode is strict. The following table lists the corresponding forwarding rules:

Mode	IPv4 packet forward rule	IPv6 packet forward rule
Strict	Packets with IPV4+MAC are forwarded.	No IPV6 packet is forwarded.
Loose	Packets with IPV4+MAC are forwarded.	All IPV6 packets are forwarded.
Compatible	Packets with IPV4+MAC are forwarded.	The IPV6 packets binded with the source MAC addresses are forwarded.

14.1.8.3 Exceptional Ports for the Address Binding

By default, the IP address and MAC address binding function is effective on all ports. You can configure the exceptional ports to make this address binding function ineffective on some ports.

Note

Because the binding relationship on the uplink port is uncertain, generally the uplink port is configured as the exceptional port. It is not necessary to check the IP address and MAC address binding on the uplink port.

14.1.9 Related Protocols

IEEE Std 802.3™ Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications

IEEE Std 802.1Q™ Virtual Bridged Local Area Networks

14.2 Default MAC Address Table Configuration

Function	Default
Dynamic address aging time	300s
Dynamic address learning mode	dispersive
Dynamic address synchronization	disabled
Limit of VLAN dynamic address	disabled
MAC address change notification	disabled
Address-bind mode	compatible

14.3 Setting Dynamic Addresses

14.3.1 Clearing Dynamic Addresses

Command	Function
DES-7210#**clear mac-address-table dynamic**	Clear all dynamic addresses.
DES-7210#**clear mac-address-table dynamic address** *mac-address* **vlan** *vlan-id*	Clear the specified MAC address. *mac-address* the specified MAC address to be cleared. *vlan-id* the specified VLAN to which the MAC address to be cleared belongs.
DES-7210#**clear mac-address-table dynamic interface** *interface-id* [**vlan** *vlan-id*]	Clear all dynamic addresses on the specified port or Aggregate Port, or clear all dynamic addresses on all interfaces. *Interface-id:* the specified port or Aggregate Port; *vlan-id* the specified VLAN to which the dynamic address to be cleared belongs.
DES-7210#**clear mac-address-table dynamic vlan** *vlan-id*	Clear all dynamic addresses in the specified VLAN. *vlan-id* the specified VLAN to which the dynamic address to be cleared belongs.

The following example shows how to clear all dynamic addresses in VLAN 1 on interface GigabitEthernet 0/1:

```
DES-7210#clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
```

14.3.2 Viewing Configurations

Command	Function
DES-7210#**show mac-address-table dynamic**	Show all dynamic addresses.
DES-7210#**show mac-address-table dynamic address** *mac-address* [**vlan** *vlan-id*]	Show the specified dynamic MAC address. *mac-address* the specified MAC address. *vlan-id* the specified VLAN to which the MAC address belongs.
DES-7210#**show mac-address-table dynamic interface** *interface-id* [**vlan** *vlan-id*]	Show all dynamic addresses on the specified port or Aggregate Port. *Interface-id:* the specified port or Aggregate Port; *vlan-id* the specified VLAN to which the dynamic address belongs.
DES-7210#**show mac-address-table dynamic vlan** *vlan-id*	Show all dynamic addresses in the specified VLAN. *vlan-id* the specified VLAN to which the dynamic address belongs.
DES-7210# **show mac-address-table count**	Show the statistics in the mac address table.

The following example shows all dynamic MAC addresses in VLAN 1 on interface GigabitEthernet 0/1:

```
DES-7210#show mac-address-table dynamic interface gigabitEthernet 0/1
vlan 1
Vlan         MAC Address          Type     Interface
----------  -------------------- -------- ------------------
 1         0000.5e00.010c       DYNAMIC  GigabitEthernet 0/1
 1         00d0.f822.33aa       DYNAMIC  GigabitEthernet 0/1
 1         00d0.f822.a219       DYNAMIC  GigabitEthernet 0/1
 1         00d0.f8a6.5af7       DYNAMIC  GigabitEthernet 0/1
```

The following example shows the statistics in the MAC address table:

```
DES-7210# show mac-address-table count
Dynamic Address Count  : 30
Static  Address Count  : 0
Filtering Address Count: 0
Total Mac Addresses    : 30
Total Mac Address Space Available: 8159
```

14.4 Setting the Address Aging Time

14.4.1 Setting the Aging Time

The following table shows how to set the aging time of address:

Command	Function

Command	Function
DES-7210(config)# **mac-address-table aging-time** [*0 |10-1000000*]	Set the time for an address to be stored in the dynamic MAC address table after it has been learned. It is in the range of 10 to 1000000 seconds, 300 seconds by default. When you set the aging time as 0, the address aging function is disabled and the learned addresses will not be aged.
DES-7210(config)# **no mac-address-table aging-time**	Restore the aging time to the default value.

The following example shows how to set the address aging time to 180s:

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#mac-address-tabsle aging-time 180
```

14.4.2 Viewing Configurations

Command	Function
DES-7210)#**show mac-address-table aging-time**	Show the aging time of all addresses.

The following example shows how to view the address aging time configurations:

```
DES-7210#show mac-address-table aging-time
Aging time    : 180 seconds
```

Caution

The actual aging time may be different from the setting value for the MAC address table. However, it will not be 2 times than the setting value.

14.5 Setting the Management Learning Mode of Dynamic Addresses

14.5.1 Setting the Dynamic Address Learning Mode

Command	Function
DES-7210(config)# **mac-manage-learning dispersive**	Set the management learning mode of the dynamic address as the dispersive mode.
DES-7210(config)# **mac-manage-learning uniform**	Set the management learning mode of the dynamic address as the uniform mode.

The following example shows how to set the dispersive address learning mode:

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#mac-manage-learning dispersive
```

14.5.2 Setting the Uniform Address Learning-Sync

Command	Function

Command	Function
DES-7210(config)# **mac-manage-learning uniform learning-synchronization**	In the uniform address learning mode, enable dynamic address synchronization.
DES-7210(config)# **no mac-manage-learning uniform learning-synchronization**	In the uniform address learning mode, disable dynamic address synchronization.
DES-7210(config)# **mac-manage-learning uniform**	Set the management learning mode of the dynamic address as the uniform mode.

The following example shows how to enable dynamic address synchronization:

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#mac-manage-learning uniform learning-synchronization
```

14.5.3 Viewing Configurations

```
DES-7210 #show mac-address-table mac-manage-learning
MAC manage-learning
running mode: dispersive.
configuration mode: dispersive.
dynamic address learning-synchronization: off.
```

14.6 Setting the Limit of Dynamic Addresses for a VLAN

14.6.1 Setting the Limit of Dynamic Addresses for a VLAN

You can set the limit of dynamic MAC addresses that a VLAN can learn.

The table below sets the limit of the dynamic addresses for a VLAN.

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **vlan** [*1-4094*]	Enter the VLAN configuration mode.
DES-7210(config-vlan)# **max-dynamic-mac-count** [*1-32768*]	Set the maximum number of dynamic MAC addresses that the VLAN can learn.

To disable the limit of the dynamic addresses for a VLAN, use the **no max-dynamic-mac-count** command.

The following example shows how to set the maximum dynamic address number to 160:

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#vlan 1
DES-7210(config-vlan)#max-dynamic-mac-count 160
```

Caution

Above listed commands can only be supported by 7200-24GE.

14.6.2 Viewing Configurations

Show the maximum number of dynamic addresses for a specified VLAN:

```
DES-7210#show mac-address-table max-dynamic-mac-count vlan 1
vlan limit   mac count learning
---- ------- --------- --------
 1   160       6        YES
```

Show the maximum number of dynamic addresses for all VLANs:

```
DES-7210#show mac-address-table max-dynamic-mac-count
vlan limit   mac count learning
---- ------- --------- --------
 1   160     6        YES

 3   500     124      YES
```

Caution Above listed commands can only be supported by 7200-24GE.

14.7 Setting the Static MAC Addresses

14.7.1.1 Adding and Removing the Static MAC Addresses

You can add a static address to the MAC address table by specifying the destination MAC address, the VLAN (the static address will be added to the address table of this VLAN), and the interface (the packets to the destination MAC address are forwarded to this interface).

To add a static address, execute the following commands:

Command	Function
DES-7210(config)# **mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*	*mac-addr*: Specify the destination MAC address to which the entry corresponds. *vlan-id*: Specify the VLAN to which this address belongs. *interface-id:* specify the interface (physical port or aggregate port) to which the packet is forwarded. Upon receiving the packets to the destination MAC address in the VLAN, the switch will forward them to the interface.
DES-7210(config)# **no mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*	Remove the static MAC address entries.

The following example shows how to configure the static address 00d0.f800.073c. When a packet to this address is received in VLAN 4, it is forwarded to Gigabitethernet 0/3.

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# mac-address-table static 00d0.f800.073c vlan 4 interface
gigabitethernet 0/3
```

The following example shows how to remove the static address 00d0.f800.073c.

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#no mac-address-table static 00d0.f800.073c vlan 4 interface
gigabitethernet 0/3
```

14.7.1.2 Viewing Configurations

Command	Function
DES-7210# **show mac-address-table static**	Show the information of all the static MAC addresses.

The following example shows how to view the information of all the static MAC addresses:

```
Vlan        MAC Address         Type      Interface
----------  ------------------- --------- -------------------
          4       00d0.f800.073c       STATIC    GigabitEthernet 0/3
```

14.8 Setting the Filtering MAC Addresses

14.8.1.1 Adding and Removing the Filtering Addresses

To add a filtering address, specify the MAC address to be filtered and the VLAN that the MAC address belongs to. The device will directly discard the packets from the MAC address in the VLAN.

To add a filtering address, execute the following command:

Command	Function
DES-7210(config)# **mac-address-table filtering** *mac-addr* **vlan** *vlan-id*	mac-addr: Specify the MAC address to be filtered by the device. vlan-id: Specify the VLAN to which this address belongs.
DES-7210(config)# **no mac-address-table filtering** *mac-addr* **vlan** *vlan-id*	Remove the filtering MAC address entries.

The following example shows how to configure the filtering address 00d0.f800.073c. When a packet to or from this address is received in VLAN 4, it will be discarded.

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# mac-address-table filtering 00d0.f800.073c vlan 4
```

The following example shows how to remove the filtering address 00d0.f800.073c.

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#no mac-address-table filtering 00d0.f800.073c vlan 4
```

14.8.1.2 Viewing Configurations

Command	Function
DES-7210# **show mac-address-table filtering**	Show the information of all the filtering MAC addresses.

The following example shows how to view the information of all the filtering MAC addresses:

```
Vlan        MAC Address         Type      Interface
----------  ------------------- --------- -------------------
          4       00d0.f800.073c       FILTER    GigabitEthernet 0/3
```

14.9 Setting MAC Address Change Notification

14.9.1 Setting MAC Address Change Notification

By default, the global switch of MAC addresses is turned off, so the MAC address change notification function is disabled on all interfaces.

To configure the MAC address change notification function, execute the following command:

Command	Function
DES-7210(config)# **snmp-server host** *host-addr* **traps** [**version** {**1 | 2c |3 [auth | noauth | priv**]}] *community-string*	Configure the NMS to receive the MAC address change notification. *host-add*: IP address of the receiver. *version:* Specify the version of the SNMP Trap message to be sent. *community-string*: Specify the authentication name carried with the SNMP Trap message.
DES-7210 (config)#**snmp-server enable traps**	Allow the switch to send the SNMP Trap message.
DES-7210(config)# **mac-address-table notification**	Turn on the global switch of the MAC address change notification function.
DES-7210(config)# **mac-address-table notification** {**interval** *value* | **history-size** *value*}	*interval value* :Interval of generating the MAC address change notification (optional), in the range of 1 to 3600 seconds, 1 second by default. *history-size value*: Maximum number of the records in the MAC notification history list, in the range of 1 to 200, 50 by default.
DES-7210(config-if)# **snmp trap mac-notification** {**added | removed**}	Enable the MAC address change notification on the interface. added: Send a MAC address change notification when a MAC address is **added** on this interface. Removed: Send a MAC address change notification when a address is deleted.

To disable the MAC address change notification function, use the **no snmp-server enable traps** command in the global configuration mode. To turn off the global switch of the MAC address change notification function, use the **no mac-address-table notification** command. To disable the MAC address change notification funciton on a specified interface, use the **no snmp trap mac-notification** {**added** | **removed**} command in the interface configuration mode.

This example shows how to enable the MAC address change notification funciton, use public as the authentication name to send a MAC address change notification to the NMS whose IP address is 192.168.12.54 at the interval of 40 seconds, set the size of the MAC address change history list to 100, and enable the MAC address change notification funciton on gigabitethernet 0/1 when a MAC address is added or removed.

```
DES-7210(config)# snmp-server host 192.168.12.54 traps public
DES-7210(config)# snmp-server enable traps
DES-7210(config)# mac-address-table notification
DES-7210(config)# mac-address-table notification interval 40
DES-7210(config)# mac-address-table notification  history-size 100
DES-7210(config)# interface gigabitethernet 0/1
DES-7210(config-if)# snmp trap mac-notification added
```

```
DES-7210(config-if)# snmp trap mac-notification removed
```

14.9.2 Viewing the MAC Address change Notification Information

In the privileged mode, you can view the information on the MAC address table of the device by using the commands listed in the following table:

Command	Function
DES-7210# **show mac-address-table notification**	Show the global configuration of the MAC address change notification function.
DES-7210# **show mac-address-table notification interface**	Show the configuration of the MAC address change notification on the interface.
DES-7210# **show mac-address-table notification history**	Show the history list of the MAC address change notification.

The following examples show how to view the MAC address change notification.

View the global configuration of the MAC address change notification:

```
DES-7210# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 2
Maximum History Size : 154
Current History Size : 2
DES-7210# show mac-address-table notification interface
Interface          MAC Added Trap MAC Removed Trap
---------------- -------------- ----------------
Gi0/1              Disabled      Enabled
Gi0/2              Disabled      Disabled
Gi0/3              Enabled       Enabled
Gi0/4              Disabled      Disabled
Gi0/5              Disabled      Disabled
Gi0/6              Disabled      Disabled
DES-7210# show mac-address-table notification history
History Index:1
Entry Timestamp: 15091
MAC Changed Message :
Operation   VLAN MAC Address    Interface
---------- ---- -------------- --------------------
Added       1    00d0.f808.3cc9 Gi0/1
Removed     1    00d0.f808.0c0c Gi0/1
History Index:2
Entry Timestamp: 21891
MAC Changed Message :
Operation   VLAN  MAC Address    Interface
---------- ---- -------------- --------------------
Added       1    00d0.f80d.1083 Gi0/1
```

14.10 Setting IP Address and MAC Address Binding

14.10.1 Setting IP Address and MAC address Binding

In the global mode, to configure IP address and MAC address binding, execute the following commands.

Command	Function
DES-7210(config)# **address-bind** *ip-address mac-address*	Configure IP address and MAC address binding.
DES-7210(config)# **address-bind install**	Enable the address binding function.

To cancel the IP address and MAC address binding, use the **no address-bind** *ip-address mac-address* command in the global configuration mode.

To disable the address binding function, execute the **no address-bind install** command.

The following example shows how to bind the IP address and MAC address:

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#address-bind 192.168.5.1 00d0.f800.0001
DES-7210(config)#address-bind install
```

Caution

Problem: In the stack environment, if one switch learns the MAC address when receiving the IP packets not correspond to the address binding, this MAC address can only be learned by the chip of that switch and cannot be learned by the chips of other switches in the stack environment.

Phenomenon: In the stack environment, if one switch learns the MAC address when receiving the IP packets not correspond to the address binding, this address entry is displayed using the **show mac** command and the IP packets can still be broadcasted to other stack switches. The MAC address learning is normal when receiving the non-IP packets or the IP packets correspond to the address binding.

14.10.2 Setting the Address Binding Mode

In the global mode, to configure the address binding mode, execute the following commands.

Command	Function
DES-7210(config)# **address-bind ipv6-mode** { **compatible**| **loose** | **strict** }	Configure the address binding mode.
DES-7210(config)# **no adress-bind ipv6-mode**	Restore to the default address binding mode.

The following example shows how to set the address binding mode to strict:

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#address-bind ipv6-mode strict
```

Caution

In the IPV6 mode, DHCP Snooping address binding, port security MAC+IP address binding functions are enabled at the same time.

Mode	IPv4 packet forward rule	IPv6 packet forward rule
Strict	Only packets with IPV4+MAC are forwarded.	Only IPV6 packets with IPv6 security address configured are allowed to be forwarded.
Loose	Only packets with IPV4+MAC are forwarded.	All IPV6 packets are aloowed to be forwarded.
Compatible	Only packets with IPV4+MAC are forwarded.	Only IPV6 packets binded with the source MAC address or the security address configured are allowed to be forwarded.

14.10.3 Setting the Exceptional Ports for the IP Address and MAC Address Binding

To make the IP address and MAC address binding not to take effect on some ports, you can set these ports as exceptional ports. To configure an exceptional port, execute the following command in the global configuration mode.

Command	Function
DES-7210(config)#address-bind uplink *interface-id*	Configure the exceptional port for the IP address and MAC address binding. *Interface-id:* port or Aggregate port

Use the **no address-bind uplink** *interface-id* command to cancel the configuration of the specified exceptional port.

The following example shows how to set the interface GigabitEthenet 0/1 to the exceptional port:

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# address-bind uplink GigabitEthernet 0/1
```

14.10.4 Viewing the IP Address and MAC Address Binding Table

To show the IP address and MAC address binding table, use the **show address-bind** command in the privileged mode:

Command	Function
DES-7210(config)#show address-bind	View the IP address and MAC address binding table.

The following example shows how to view the IP address and MAC address binding table :

```
DES-7210#show address-bind
Total Bind Addresses in System : 1

IP Address        Binding MAC Addr
---------------    ----------------
    192.168.5.1    00d0.f800.0001
```

14.11 Configuration Examples

14.11.1 Network Topology

As Figure-14 shows, the database server connects to the switch through the interface GigabitEthernet 0/1, the web server connects to the switch through the interface GigabitEthernet 0/2, and the server administrator connects to the switch through the interface GigabitEthernet 0/3. Other users access the web server through the interface GigabitEthernet 0/10. All data are forwarded in VLAN 1.

The static MAC address configuration enables the data exchanged between the web server and the database server, the administrator and the server to be forwarded in the unicast form, preventing these data from being forwarded in the broadcast form in the user network and ensuring the security of the information exchanged between the web server and the database server, the administrator and the server .

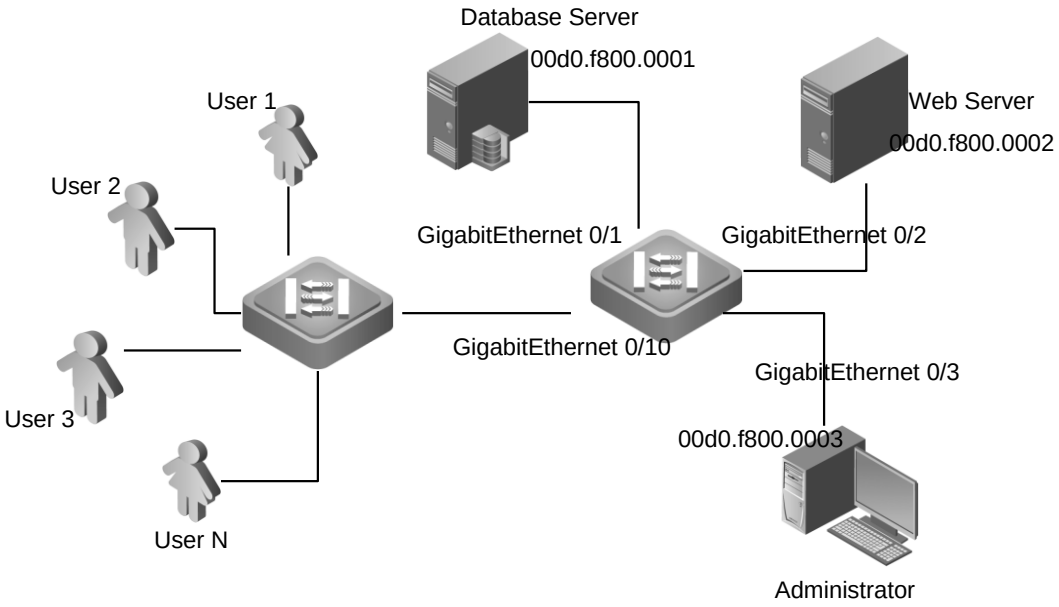


Figure 1 Typical Configuration Topology

14.11.2 Configurations

The following example shows how to configure the switch:

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)#mac-address-table static 00d0.f800.0001 vlan 1 interface GigabitEthernet 0/1
DES-7210(config)#mac-address-table static 00d0.f800.0002 vlan 1 interface GigabitEthernet 0/2
DES-7210(config)#mac-address-table static 00d0.f800.0003 vlan 1 interface GigabitEthernet 0/3
```

The following example shows the switch configurations:

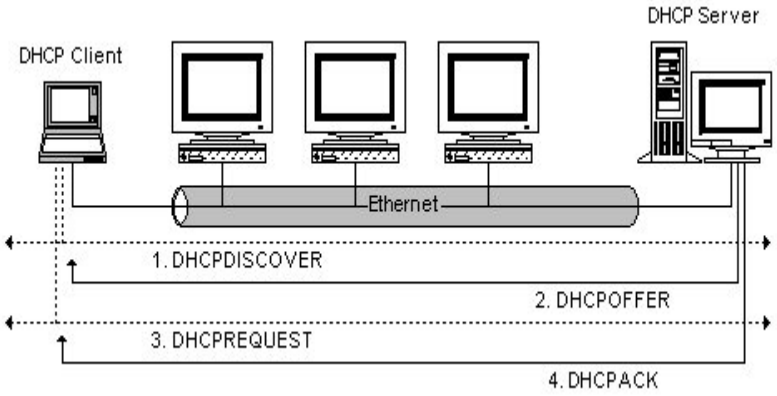
```
DES-7210#show mac-address-table static
Vlan       MAC Address         Type     Interface
---------- -------------------- -------- --------------------
   1       00d0.f800.0001      STATIC   GigabitEthernet 0/1
   1       00d0.f800.0002      STATIC   GigabitEthernet 0/2
   1       00d0.f800.0003      STATIC   GigabitEthernet 0/3
```

15 DHCP Snooping Configuration

15.1 Overview

15.1.1 Understanding DHCP

The DHCP protocol is widely used to dynamically allocate the recycled network resources, for example, IP address. A typical IP acquisition process using DHCP is shown below:



The DHCP Client sends a DHCP DISCOVER broadcast packet to the DHCP Server. The Client will send the DHCP DISCOVER again if it does not receive a response from the server within a specified time.

After the DHCP Server receives the DHCP DISCOVER packet, it allocates resources to the Client, for example, IP address according to the appropriate policy, and sends the DHCP OFFER packet.

After receiving the DHCP OFFER packet, the DHCP Client sends a DHCP REQUEST packet to obtain the server lease.

After receiving the DHCP REQUEST packet, the server verifies whether the resources are available. If so, it sends a DHCP ACK packet. If not, it sends a DHCP NAK packet. Upon receiving the DHCP ACK packet, the DHCP Client starts to use the resources assigned by the server in condition that the ARP verification resources are available. If it receives the DHCP NAK packet, the DHCP Client will send the DHCP DISCOVER packet again.

15.1.2 Understanding DHCP Snooping

DHCP Snooping monitors users by snooping the packets exchanged between the clients and the server. DHCP Snooping can filter DHCP packets and illegal servers by proper configuration. Some terms and functions used in DHCP Snooping are explained below:

DHCP Snooping TRUST port: Because the packets for obtaining IP addresses through DHCP are in the form of broadcast, some illegal servers may prevent users from obtaining IP addresses, or even cheat and steal user information. To solve this problem, DHCP Snooping classifies the ports into two types: TRUST port and UNTRUST port. The device forwards only the DHCP reply packets received through the TRUST port while discarding all the DHCP reply packets from the UNTRUST port. In this way, the illegal DHCP Server can be shielded by setting the port connected to the legal DHCP Server as a TRUST port and other ports as UNTRUST ports.

DHCP Snooping binding database: By snooping the packets between the DHCP Clients and the DHCP Server, DHCP Snooping combines the IP address, MAC address, VID, port and lease time into a entry to form a DHCP Snooping user database.

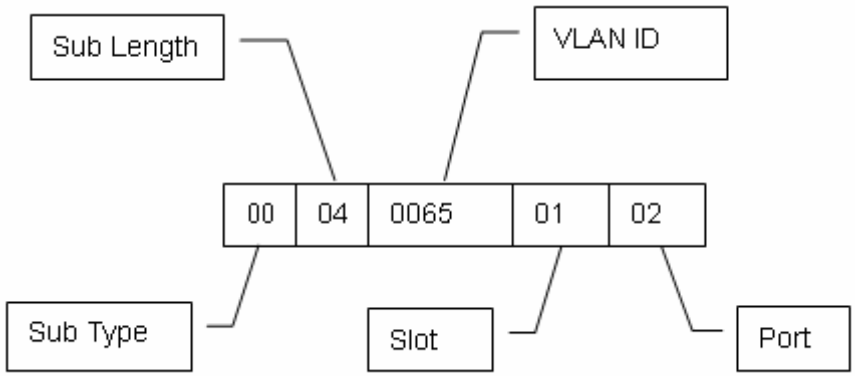
DHCP Snooping checks the validity of DHCP packets that pass through the device, discards illegal DHCP packets, and records user information to create a DHCP Snooping binding database for ARP inspection and query. The following DHCP packets are considered illegal:

- The DHCP reply packets received on the UNTRUST ports, including DHCPACK, DHCPNACK, DHCPOFFER, etc.
- DHCP Client values in the source MAC and DHCP packets are in different packets when MAC check is enabled.
- DHCPRELEASE packets whose port information is inconsistent with that in the the DHCP Snooping binding database.

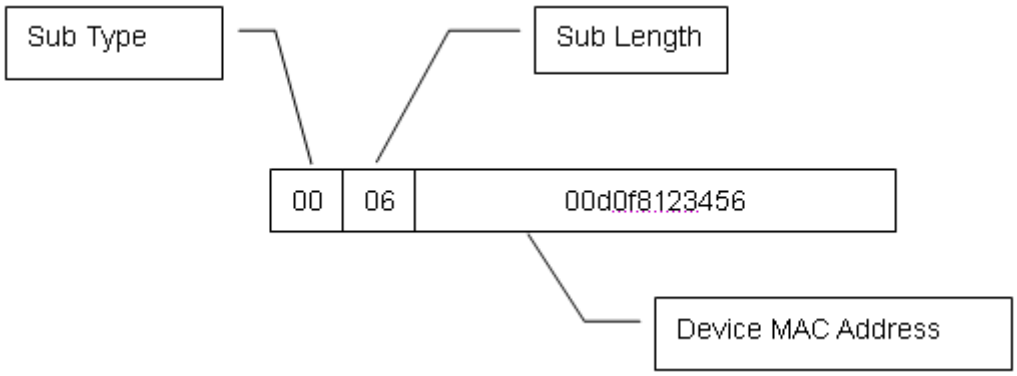
15.1.3 Understanding DHCP Snooping Information Option

Some network administrators want to assign IP address to current users upon their positions. That is, they want to assign IP addresses to users according to the information on the network equipments that users connect so that the switch can add the user-related device information to the DHCP request packet in DHCP option way while performing DHCP Snooping. According to RFC3046, the option number used is 82. You can obtain more user information by uploading option82 to the content server. As a result, you can assign IP addresses accurately. The format of option82 uploaded by DHCP Snooping is shown as follows:

Agent Circuit ID



Agent Remote ID



15.1.4 Understanding DHCP Snooping Address Binding

By snooping the packets between the DHCP Clients and the DHCP Server, DHCP Snooping combines the legal user information, including IP address, MAC address, VID, port and lease time, into a entry to form a DHCP Snooping user database. By adding the user information in the DHCP Snooping database to the IP packet hardware filtering entry, DHCP Snooping only allows those legal users to send the IP packets, preventing the illegal users from setting the private IP addresses.

15.1.5 Understanding DHCP Snooping Bootp Binding

DHCP Snooping function is designed based on the DHCP protocol and is not fully compatible with Bootp because no related options exist in the Bootp packets, such as packet type, lease time, ect. Therefore, it is diffilcult for DHCP Snooping to control the users in the Bootp application environment effectively.

As more and more diskless working station applications arise in the market, DES-7210 products extend the DHCP Snooping function and add the Bootp support. DHCP Snooping not only snoops the exchaged packets between DHCP Clients and DHCP server, but also is able to deal with the Bootp packets by combining IP address, MAC address, port and VID into a static binding entry to form a DHCP Snooping user database.

In the DHCP Snooping user database, a Bootp user is a static binding user. The same is true with the manually-bind user. The Bootp user dynamically forms in the process of Bootp exchange. However, it wants the administrator to execute commands manually to remove the Bootp user.

15.1.6 DHCP Snooping Related Security Functions

DHCP Snooping address binding only filters the IP packets, rather than the ARP packets. To enhance the security and prevent ARP spoof, it is necessary to filter the illegal ARP packtes. DHCP Snooping database can provide the information on filtering the ARP packets. (For the detailed information about the ARP packet filtering, please refer to the related chapters of ARP-CHECK and DAI.)

15.1.7 Other Precautions on DHCP Snooping Configuration

1. The DHCP Snooping function and the DHCP Relay Option82 function are mutually exclusive. That is, you can not enable the DHCP Snooping function and the DHCP Relay Option82 function at the same time.
2. Security control is disabled for the users on the TRUST port.

15.2 DHCP Snooping Configuration

15.2.1 Enabling and Disabling DHCP Snooping

The DHCP Snooping function of the device is disabled by default. To enable DHCP Snooping and then monitor DHCP packets, execute the following command.

Command	Description
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# [**no**] **ip dhcp snooping**	Enable or disable DHCP snooping.

The following example demonstrates how to enable the DHCP snooping function of the device:

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping
DES-7210(config)# end
```

Caution DHCP Snooping and Private VLAN function can not be co-used.

15.2.2 Configuring Enabled DHCP Snooping VLAN

This command enables DHCP Snooping in corresponding VLAN, adding this VLAN to enabled DHCP Snooping VLAN range.

Command	Description
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# [**no**] **ip dhcp snooping vlan** {*vlan-rng* | {*vlan-min* [*vlan-max*]}}	Configures enabled Snooping VLAN.

Here is an example of configuring DHCP snooping enabled in VLAN1000:

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping vlan 1000
DES-7210(config)# end
```

15.2.3 Configuring DHCP Snooping Bootp Binding

By default, DHCP Snooping does not support Bootp binding. After configuring this command, DHCP Snooping snoops all Bootp packets through the device and add the legal Bootp user to DHCP Snooping user database.

To configure the DHCP Snooping Bootp-bind function, execute the following command:

Command	Description
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# [**no**]**ip dhcp snooping bootp-bind**	Enable or disable the DHCP Snooping Bootp binding function.

The following example shows how to enable the DHCP Snooping Bootp binding function:

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping bootp-bind
DES-7210(config)# end
```

15.2.4 Configuring DHCP Source MAC Address Check Function

After configuring this command, the device will match the MAC address of the DHCP Request packet from the UNTRUST port against the one in the client field and discard unmatched packet. By default, this funciton is not enabled.

To configure the source MAC address check function, execute the following command:

Command	Description
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# [**no**]**ip dhcp snooping verify mac-address**	Enable or disable the source MAC address check function.

The following example shows how to enable the DHCP source MAC address check function:

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping verify mac-address
DES-7210(config)# end
```

15.2.5 Configuring DHCP Snooping Information Option

By default, this function is disabled. After configuring this command, when DHCP Snooping forwards the packets, option82 will be added to all DHCP request packets and removed from all reply packets.

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# [**no**] **ip dhcp snooping Information option**	Enable or disable the DHCP snooping information option.

The following configuration enables DHCP snooping information option:

```
DES-7210# configure terminal
```

```
DES-7210(config)# ip dhcp snooping information option
DES-7210(config)# end
```

Caution

After this function is configured, DHCP relay option82 function configured in the same device will be ineffective.

15.2.6 Writing the DHCP Snooping Database to Flash Periodically

By default, this function is disabled. DHCP Snooping provides a command to write the DHCP Snooping database to the flash periodically in order to prevent loss of DHCP user information when the device restarts due to an electricity failure.

Command	Description
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# [**no**] **ip dhcp snooping database write-delay** [*time*]	Specify the interval at which the switch writes the DHCP database to the flash. *time*: 600s to 86400s. The default value is 0.

The following example sets the interval at which the switch writes the DHCP databse to the flash to 3600s:

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping database write-delay 3600
DES-7210(config)# end
```

Caution

You need to set a proper time for writing to the flash since erasing and writing to the flash frequently shortens its life. A shorter time helps to save the device information more effectively. A longer time reduces the times of writing to the flash and increases service life of flash.

15.2.7 Writing DHCP Snooping Database to Flash Manually

To prevent loss of DHCP user information when the device restarts due to an electricity failure, the administrator can write the DHCP Snooping binding database to the flash manually.

Command	Description
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **ip dhcp snooping database write-to-flash**	Write the DHCP Snooping binding database to the flash manually.

The following example demonstrates how to write the DHCP Snooping binding database to the flash:

```
DES-7210# configure terminal
DES-7210(config)# ip dhcp snooping database write-to-flash
DES-7210(config)# end
```

15.2.8 Configuring a Port in Suppression State

By default, this function is disabled. After configuring this command, a port can be set in the suppression state and refuse all DGCP request packets:

Command	Description
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config-if)# [**no**] **ip dhcp snooping trust**	Set the port in the suppression state.

The following example shows how to set GigabitEthernet 4/2 in the suppression state:

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitEthernet 4/2
DES-7210(config-if)# ip dhcp snooping suppression
DES-7210(config-if)# end
```

15.2.9 Configuring a Port as a TRUST Port

By default, all the ports are UNTRUST ports. After configuring this command, a port is set as the TRUST port and connected to the legal DHCP server.

Command	Description
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config-if)# [**no**] **ip dhcp snooping trust**	Set the port as a trust port.

The following example shows how to set GigabitEthernet 4/1 as a TRUST port:

```
DES-7210# configure terminal
DES-7210(config)# interface GigabitEthernet 4/1
DES-7210(config-if)# ip dhcp snooping trust
DES-7210(config-if)# end
```

15.2.10 Configuring Rate of Receiving DHCP Packet

This command configures rate of receiving DHCP in the corresponding interface:

Command	Description
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config-if)# [**no**] **ip dhcp snooping limit rate** *rate-value*	Configures rate of receiving DHCP packet on the port.

The following example shows how to set the rate of receiving DHCP packet on GigabitEthernet 4/1 as 100pps:

```
DES-7210# configure terminal
DES-7210(config)# interface GigabitEthernet 4/1
DES-7210(config-if)# ip dhcp snooping limit rate 100
DES-7210(config-if)# end
DES-7210# show ip dhcp snooping
```

```
Switch DHCP snooping  status                  :   ENABLE
DHCP snooping  Verification of hwaddr field status    :   DISABLE
DHCP snooping database write-delay time        :   0 seconds
DHCP snooping option 82 status                :   ENABLE
DHCP snooping Support Bootp bind status       :   ENABLE

Interface                   Trusted      Rate limit (pps)
------------------------      -------      ----------------
GigabitEthernet 4/1          NO                     100
```

15.2.11 Clearing Dynamic User Information from the DHCP Snooping Binding Database

To clear dynamic user information from the DHCP Snooping binding database, execute the following command.

Command	Description
DES-7210# **clear ip dhcp snooping binding**	Clear information from the current database.

The following example shows how to clear information from the current database manually:

```
DES-7210# clear ip dhcp snooping binding
```

15.3 Showing DHCP Snooping Configuration

15.3.1 Showing DHCP Snooping

To show DHCP Snooping, execute the following command:

Command	Description
DES-7210# **show ip dhcp snooping**	Show the configuration of DHCP snooping.

For example:

```
DES-7210# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr fieled status      :   DISABLE
DHCP snooping database wirte-delay time         :   0 seconds
DHCP snooping option 82 status             :   ENABLE
DHCP snooping Support Bootp bind status    :   ENABLE
Interface                   Trusted      Rate limit (pps)
------------------------      -------      ----------------
GigabitEthernet 4/1          NO                     100
```

15.3.2 Showing the DHCP Snooping Binding Database

To show the DHCP Snooping binding database, execute the following command:

Command	Description
DES-7210# **show ip dhcp snooping binding**	View the static user information in the DHCP Snooping binding database.

For example:

```
DES-7210# show ip dhcp snooping binding
Total number of bindings: 1
MacAddress        IpAddress      Lease(sec)   Type         VLAN  Interface
------------------ --------------- ------------ ------------- -----
--------------------

  00d0.f801.0101   192.168.1.1   -     static       1      fastethernet 0/1
```

15.3.3 Showing the DHCP Snooping Debugging Switch

To enable the DHCP Snooping debugging switch, execute the following command:

Command	Description
DES-7210# **debug ip dhcp snooping {event | packet}**	Enable the DHCP Snooping debugging switch.

For example:

```
DES-7210# debug ip dhcp snooping event
DES-7210# debug ip dhcp snooping packet
```

16 IGMP Snooping Configuration

16.1 Overview

16.1.1 Understanding IGMP Snooping

Internet Group Management Protocol, abbreviated as IGMP Snooping, is an IP multicast flow mechanism running in the VLAN, and used to manage and control the IP multicast flow forwarding in the VLAN and belongs to the Layer2 multicast funtion. The IGMP Snooping function described below is in the VLAN, and the related ports are the member ports in the VLAN.

The device running IGMP Snooping sets up the mapping for the port and the multicast address by analyzing the received IGMP packets, and forwards the IP multicast packets based on the mapping. As shown in the Figure-1, with IGMP Snooping enabled, the IP multicast packets are broadcasted in the VLAN; while without IGMP Snooping enabled, the known IP multicast packets are not broadcasted in the VLAN but sent to the specified recipient.

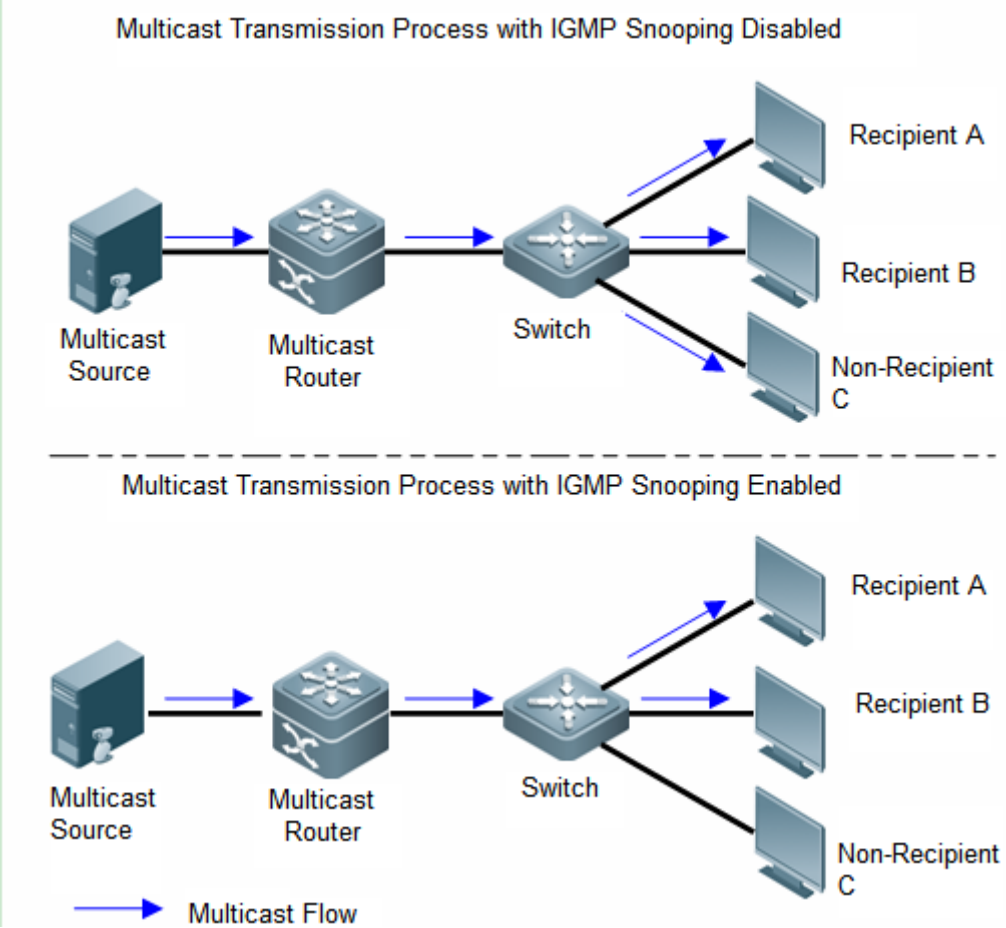


Figure-1

DES-7210 multicast products support both the layer 2 multicast(IGMP Snooping) function and the layer 3 multicast(Multicast-routing) function. That is to say, to realize better packet forwarding function, DES-7210 device supports not only the layer 3 multicast route forwarding, but also the snooping in the VLAN.

Caution The DES-7200 series supports the co-use of Layer2 multicast(IGMP Snooping) and Layer3 multicast(Multicast-routing)..

16.1.2 Understanding IGMP Snooping Port Type

As shown in the Figure-2, the Router is connected with the multicast source, enable the IGMP Snooping on the SwitchA, HostA and HostC are the receive host(that is, the IP multicast group member)

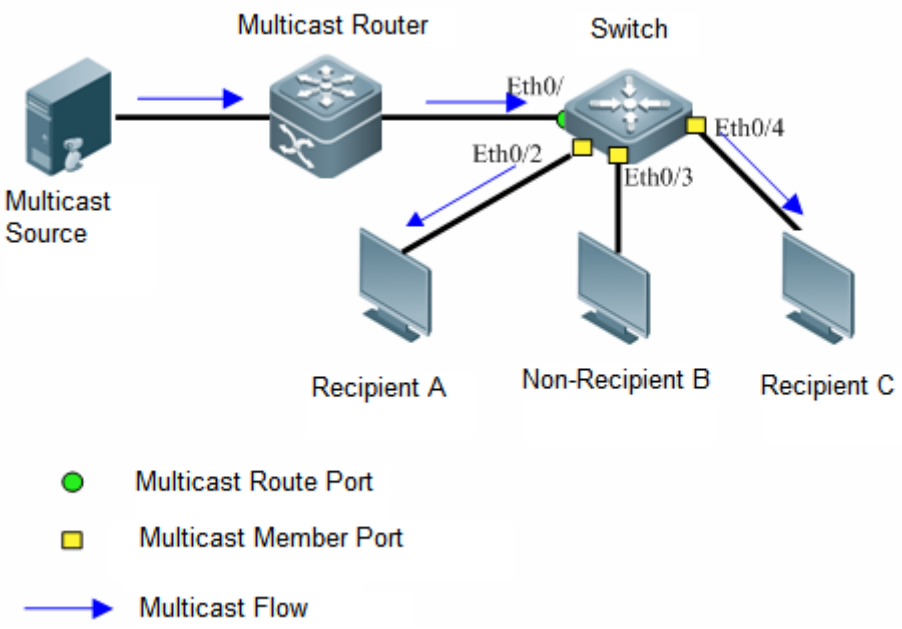


Figure-2 IGMP Snooping Port Type

Multicast Router Port: the switch is connected with the multicast router(the Layer3 multicast device), take the SwitchA interface Eth0/1 for example. All router ports on the switch(including the dynamic and static ports) are recorded in the router port list. By default, the router port corresponds to the recipient of the multicast data in the VLAN, and can also be added to the IGMP Snooping forwarding list.

Member Port: the abbreviation of the IP multicast group member port, also named Listener Port, representing the port connected with the IP multicast group member on the switch, take the SwitchA interface Eth0/2, Eth0/3 and Eth0/4 for example. All member ports on the switch(including the dynamic and static ports) are recorded in the IGMP Snooping forwarding list.

16.1.3 Understanding the Aging Timer for the Dynamic Port

Table-1 Aging timer on the IGMP Snooping on the Dynamic Port

Type	Description	Timer Trigger Event	Timeout Action
Aging timer for the dynamic router port	Enable a timer for each dynamic router port. The timeout time is the aging time of the dynamic router port.	Receive the IGMP general query packet or the IP PIM Hello packet.	Remove the port from the router port list.
Aging timer for the dynamic member port	Enable a timer for each dynamic member port. The timeout time is the aging time of the dynamic member	Receive the IGMP query packet.	Remove the port from the IGMP Snooping multicast group forwarding list.

	port.		

16.1.4 Understanding IGMP Snooping Operation Mechanism

1.1.1.1.1 1.1.4.1 General Query and Specific-Group Query

IGMP querier sends the general query packets to all hosts and routers(with the address: 224.0.0.1) in the local network segment periodically to query for the IP multicast group member in the network segment. Upon receiving the IGMP general query packets, the switch forwards those query packets to all ports in this VLAN, and processes the packet-receiving port as follows:

- If this port has already been in the router port list, reset the aging timer.
- If this port has not been in the router port list, add the port to the list and enable the aging timer.
- After receiving the IGMP general query packets, the multicast device enable the aging timer for all member ports. Set the aging time as the maximum respond time of the IGMP query packets. When the aging time is 0, no member port receives the multicast flow and the port will be removed from the IGMP Snooping forwarding list.

After receiving the IGMP specific-group query packets, the multicast device enable the aging timer for all member ports in the specific group. Set the aging time as the maximum respond time of the IGMP query packets. When the aging time is 0, no member port receives the multicast flow and the port will be removed from the IGMP Snooping forwardin.

For the IGMP specific-group source query packets, it is no need to update the aging timer.

1.1.1.1.2 1.1.4.2 Membership Report

In the following circumstances, the host sends the IGMP membership report to the IGMP querier:

- After receiving the IGMP query(general or specific-group query) packets, the IP multicast group member host responds to the received packets.
- If the host wants to join in an IP multicast group, it will take the initiative to send the IGMP membership report to the IGMP querier and claim to join in the IP multicast group.

Upon receiving the IGMP membership report message, the switch forwards the message through all router ports in the VLAN, analyzes the IP multicast group address from the message to add to the host, and deals with the packet-receiving port as follows:

If the corresponding forwarding entry of IP multicast group is inexistent, create a forwarding entry, add the dynamic member port to the outgoing port list, and enable the aging timer.

If the corresponding forwarding entry of IP multicast group exists but the outgoing port list excludes the port, add the dynamic member port to the outgoing port list, and enable the aging timer.

If the corresponding forwarding entry of IP multicast group exists and the outgoing port list includes the port, reset the aging timer.

1.1.1.1.3 1.1.4.3 Leaving the Multicast Group

When leaving the IP multicast group, the host notifies the multicast router of the leave event by sending the IGMP leave group packets. Upon receiving the IGMP leave group packets on a dynamic member port, the switch forwards those packets to the router ports.

16.1.5 Understanding IGMP Profiles

IGMP Profiles is the group filterings actually, defines a series of multicast address range and the access to those multicast addresses(permit/deny), including “Multicast address range in the SVGL mode”, “Filtering multicast data range of router port”, “IGMP Filtering range”.

16.1.6 Understanding IGMP Snooping Working Mode

DISABLE: The IGMP Snooping does not work in this mode. That is, the switch does not snoop the IGMP messages between the host and the router. Multicast frames are forwarded in the VLAN in the broadcast form.

IVGL(Independent VLAN Group Learning): In this mode, the multicast flows in different VLANs are independent. A host can only request multicast flows to the router interface in the same VLAN. Upon receiving the multicast flow in any VLAN, the switch forwards the flow to the member port in the same VLAN.

SVGL(Shared VLAN Group Learning): In this mode, the hosts in different VLANs share the same multicast flow. A host can request multicst flows across VLANs. By designating a Shared VLAN, you can only forward the multicast flows received in this Shared VLAN to other member ports in different VLANs. In the SVGL mode, IGMP Profile must be used to divide the multicast address range, within which the multicast flow can be forwarded across VLANs. By default, all group range is not within the SVGL range and all multicast flows are dropped. As shown in Figure-3:

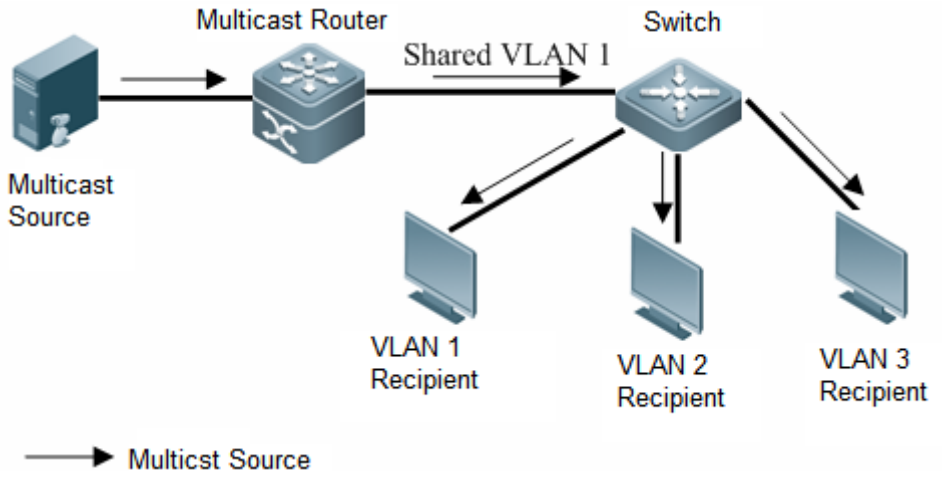


Figure-3 Multicast Flow in the Shared VLAN forwarding across VLANs

Promiscuous mode: also known as IVGL-SVGL mode. In this mode, the IVGL mode and the SVGL mode can co-exist. Use IGMP Profile to divide a set of multicast address range to the SVGL, within which the member port of the multicast forwarding entry can be forwarded across VLANs and without which the member ports are forwarded in the same VLAN.

16.1.7 Understanding Source Port Check

Some DES-7210 multicast switches support the source port check function of IGMP Snooping for higher network security.

The source port check function refers to strictly managing the inbounding port of IGMP multicast flows. When the function is disabled, the video flows from any port are considered legal and the switch will forward them to the registered ports based on the IGMP Snooping forwarding list. When the source port check function is enabled, only the multicast flows from the router port are considered legal. The multicast flows through the non-router port are illegal and will be dropped.

Note

The DES-7200 series supports IGMP SNOOPING Source Port Check.

16.1.8 Understanding Source IP Check

The DES-7200 series supports the source IP check function of IGMP Snooping for higher network security.

IGMP SNOOPING source IP checking refers to strictly limit the IGMP multicast IP address. When the function is disabled, the video flows from any port are considered legal and the switch will forward them to the registered ports based on the IGMP Snooping forwarding list. When the source port check function is enabled, only the video flows from the router interface are considered legal and the switch forwards them to the registered ports while discarding the video flows from other ports.

16.2 Configuring IGMP Snooping

We will describe how to configure IGMP snooping in the following sections

Function Configuration		Description
Configure Basic IGMP Snooping Function	Enable IGMP Snooping	Required
	Set the aging timer for the dynamic port	Optional
	Set the maximum respond time of the IGMP Query Packet	Optional
Configure IGMP Snooping Port Funtion	Set the router port.	Optional
	Set the member port.	Optional
	Set the port fast-leave	Optional
	Set the IGMP membership report packet suppression.	Optional

Configure the IP Multicast Group Policy on the Port	Set the IP multicst group filtering	Optional
	Set the source port check.	Optional
	Set the source IP check.	Optional

16.2.1 Enabling IGMP Snooping

By default, when enabling IGMP Snooping, the IGMP Snooping working mode(IVGL SVGL and IVGL-SVGL) must be specified.

Caution

The Layer2 multicast device does not support IGMP Snooping if the device works in the private VLAN mode.

16.2.2 Configuring IVGL Mode

In the global configuration mode, run the following commands to configure the IGMP Snooping IVGL mode:

Command	Function
DES-7210(config)# **ip igmp snooping ivgl**	Enable the IGMP Snooping IVGL mode. By default, the IGMP Snooping is disabled.
DES-7210 (config)#**show ip igmp snooping**	Verify the configuration.
DES-7210(config)# **no ip igmp snooping**	Disable the IGMP Snooping function.

This example sets the IGMP Snooping IVGL mode:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping ivgl
DES-7210(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL
SVGL vlan: 1
SVGL profile number: 0
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

16.2.3 Configuring SVGL Mode

In the global configuration mode, run the following commands to configure the IGMP Snooping SVGL mode:

Command	Function
DES-7210(config)# **ip igmp snooping svgl**	Enable the IGMP Snooping SVGL mode. By default, the IGMP Snooping is disabled.

Command	Function
DES-7210 (config)#**show ip igmp snooping**	Verify the configuration.
DES-7210(config)# **no ip igmp snooping**	Disable the IGMP Snooping function.

This example sets the IGMP Snooping SVGL mode:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping svgl
DES-7210(config)# show ip igmp snooping
IGMP Snooping running mode: SVGL
SVGL vlan: 1
SVGL profile number: 11
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

Note

In the SVGL mode, an IGMP Profile must be associated to specify the multicast address range in the SVGL mode, or the configuration related to the SVGL mode will not take effect. For the details, see the chapter of "Configuring the Multicast Address Range in the SVGL mode".

The layer 3 multicast-routing function can not be enabled, or the command **ip multicast-routing** can not be executed when the running mode is SVGL. Similarly, you can not enter the SVGL mode when the layer 3 multicast-routing function has been enabled.

16.2.4 Configuring IVGL-SVGL Mode

In the global configuration mode, run the following commands to configure the IGMP Snooping IVGL-SVGL mode:

Command	Function
DES-7210(config)# **ip igmp snooping ivgl-svgl**	Enable the IGMP Snooping IVGL-SVGL mode. By default, the IGMP Snooping is disabled.
DES-7210 (config)#**show ip igmp snooping**	Verify the configuration.
DES-7210(config)# **no ip igmp snooping**	Disable the IGMP Snooping function.

This example sets the IGMP Snooping IVGL-SVGL mode:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping ivgl-svgl
DES-7210(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL SVGL
SVGL vlan: 1
SVGL profile number: 11
```

```
Source port check: Disable

Source ip check: Disable

IGMP Fast-Leave: Disable

IGMP Report suppress: Disable
```

Note

In the SVGL mode, an IGMP Profile must be associated to specify the multicast address range in the SVGL mode, or the configuration related to the SVGL mode will not take effect. For the details, see the chapter of "Configuring the Multicast Address Range in the SVGL mode".

The layer 3 multicast-routing function can not be enabled, or the command **ip multicast-routing** can not be executed when the running mode is SVGL. Similarly, you can not enter the SVGL mode when the layer 3 multicast-routing function has been enabled.

16.2.5 Disabling IGMP Snooping

In the global configuration mode, run the following command to disable IGMP Snooping:

Command	Function
DES-7210(config)# **no ip igmp snooping**	Disable the IGMP Snooping function.
DES-7210 (config)#**show ip igmp snooping**	Verify the configuration.

This example disables the IGMP Snooping:

```
DES-7210# configure terminal

DES-7210(config)# no ip igmp snooping svgl

DES-7210(config)# show ip igmp snooping

IGMP Snooping running mode: DISABLE

SVGL vlan: 1

SVGL profile number: 11

Source port check: Disable

Source ip check: Disable

IGMP Fast-Leave: Disable

IGMP Report suppress: Disable
```

16.2.6 Enabling IGMP Snooping in the VLAN

By default, with IGMP Snooping globally enabled, the IGMP Snooping function is auto-enabled in all VLANs. To disable the IGMP Snooping in the specified VLAN, run the following command.

In the global configuration mode, run the following command to disable IGMP Snooping:

Command	Function
DES-7210(config)# **no ip igmp snooping vlan** *num*	Disable the IGMP Snooping in the specified VLAN. By default, the IGMP Snooping in the VLAN is enabled.

Command	Function
DES-7210 (config)# **ip igmp snooping vlan** *num*	Enable the IGMP Snooping in the specified VLAN.

This example disables the IGMP Snooping in the VLAN3:

```
DES-7210# configure terminal
DES-7210(config)# no ip igmp snooping vlan 3
DES-7210(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL
SVGL vlan: 1
SVGL profile number: 11
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable

vlan 1
-------------
IGMP Snooping                :Enabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave        :Disabled

vlan 2
-------------
IGMP Snooping                :Enabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave        :Disabled

vlan 3
-------------
IGMP Snooping                :Disabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave        :Disabled

vlan 4
-------------
IGMP Snooping                :Enabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave        :Disabled
```

16.2.7 Configuring the Aging Time for the Dynamic Router Port

If no IGMP general query packets or PIM Hello packets are received on the dynamic router port within the aging time, the router port will be deleted.

To configure the aging time for the dynamic router port, execute the following commands in the global configuration mode.

Command	Function
DES-7210(config)# **ip igmp snooping dyn-mr-aging-time** *time*	Configure the aging time for the dynamic router port. *Time:* aging time in the range of 1 to 3600s. Default value: 300s.
DES-7210(config)# **no ip igmp snooping dyn-mr-aging-time**	Return the aging time to the default value.

The following example configures the aging time of the dynamically learned router interface to 100s:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping dyn-mr-aging-time 100
```

16.2.8 Configuring the Maximum Response Time of the IGMP Query Message

The multicast router periodically sends an IGMP Query message to query whether a multicast member exists or not. If the multicast router has not received the IGMP Report message from a host within a period of time, the switch will think this port no longer receives multicast frames, and delete this port from the multicast forwarding table. The default time is 10 seconds.

To configure the maximum response time of the IGMP Query message, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip igmp Snooping query-max-respone-time** *seconds*	Set the maximum response time of the IGMP Query message in the range of 1 to 65535 seconds. The default time is 10 seconds.
DES-7210(config)# **no ip igmp Snooping query-max-respone-time**	Restore the maximum response time to the default value.

The following example configures the maximum response time of the IGMP Query message to 15s:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping query-max-respone-time 15
```

16.2.9 Configuring the Router Port

By default, the router port is dynamically learned in the VLAN. Use the **no** option of the command to disable the dynamic learning function for the router interface in the VLAN and clear all router ports learned dynamically.

Use the command to set the switch port as the static router port.

To configure a router port, execute the following command:

Command	Function
DES-7210(config)# **ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	Set the interface as the static router interface.
DES-7210(config)# **no ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	Cancel the static router interface setting.
DES-7210(config)# **ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp**	Enable the dynamic learning function for the router interface in the VLAN. By default, the dynamic learning function is enabled.
DES-7210(config)# **no ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp**	Disable the dynamic learning function for the router interface in the VLAN and clear all router ports learned dynamically.

This example sets GigabitEthernet 1/1 as the router port and enables dynamic learning function in the VLAN1:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping vlan 1 mrouter interface gigabitEthernet 0/7
DES-7210(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
DES-7210(config)# end
DES-7210# show ip igmp snooping mrouter
Vlan    Interface         State        IGMP profile
----    ---------         ------       -------------
1   GigabitEthernet 0/7    static           0
1   GigabitEthernet 0/12   dynamic          0
DES-7210# show ip igmp snooping mrouter learn
Vlan    learn method
----    ------------------
1       pim-dvmrp
```

16.2.10 Configuring Static Member Port

When IGMP Snooping is enabled, you can statically configure a port to receive a specific multicast flow in disregard of various IGMP packets.

To configure a static member port of IGMP Snooping, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip igmp Snooping ivgl**	Enable IGMP Snooping and set it as the IVGL mode.

Command	Function
DES-7210(config)# **ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *[interface-id]*	Statically configure a port to receive a certain multicast flow. • *vlan-id*: vid of multicast flow • *ip-addr* : multicast group address • *interface-id:* Interface ID
DES-7210(config)# **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *[interface-id]*	Remove a static member port. • *vlan-id*: vid of multicast flow • *ip-addr* : multicast group address • *interface-id:* Interface ID

Use **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id* to delete the static member of IGMP Snooping.

This example configures a static member port of IGMP snooping:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping vlan 1 static 233.3.3.4 interface GigabitEthernet 0/7
DES-7210(config)# end
DES-7210(config)# show ip igmp snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address              Member ports
---- --------------   ----------------------------
1    233.3.3.4            GigabitEthernet 0/7(S)
```

16.2.11 Configuring Fast-Leave

According to the IGMP protocol, a port cannot leave a multicat group immediately after the host sends the IGMP Leave message. Instead, the multicast router should first send an IGMP Query packet and lets a port leave the group only when the host does not respond. However, in specific environments (for example, one port is connected to only one multicast user), the port can immediately leave the multicast group after the multicast router receives the IGMP Leave message, a mechanism known as Fast Leave.

To enable fast-leave, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip igmp snooping fast-leave enable**	Enable the fast-leave function.
DES-7210(config)# **no ip igmp snooping fast-leave enable**	Disable the fast-leave function.

The following example enables the fast–leave function:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping fast-leave enalbe
DES-7210(config)# end
```

16.2.12 Configuring IGMP Snooping Suppression

For IGMP Snooping-enabled devices, a multicast group address may have multiple IGMP users. When a user joins the multicast group and receives the IGMP Query message, he or

she will send an IGMP Report message. DES-7210 switches will forward every IGMP Query message to the multicast router. In this way, the multicast router will receive multiple IGMP Report messages when it sends an IGMP Query message to the ports on the IGMP Snooping-enabled devices.

To reduce the pressure of the server on processing the IGMP Report messages, the switch only forwards the first received IGMP Report message to the router port while suppressing other IGMP Report messages. This is called IGMP Snooping Suppression.

To enable IGMP Snooping suppression, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip igmp snooping suppression enable**	Enable IGMP Snooping suppression. By default, this function is enabled.
DES-7210(config)# **no ip igmp snooping suppression enable**	Disable IGMP Snooping suppression.

The following example enables the IGMP Snooping suppression function:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping suppression enalbe
DES-7210(config)# end
```

16.2.13 Configuring Source Port Check

To enable source port check, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip igmp snooping source-check port**	Enable source port check.
DES-7210(config)# **no ip igmp snooping source-check port**	Disable source port check.

The following example enables the IGMP Snooping source port check function:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping source-check port
DES-7210(config)# end
```

16.2.14 Configuring Source IP Check

There are two configuration commands for the source IP check: one command is for the configuration of default source IP addresses of the legal multicast flows in all multicast groups; and the other command is for the configuration of the default source IP address for the legal multicast flows in the specified VLAN group. Only with the default source IP check enabled in all groups, the source IP address of the legal multicast server in a specific group can be set.

To enable source IP check, execute the following commands in the global configuration mode:

Command	Function

Command	Function
DES-7210(config)# **ip igmp snooping source-check default-server** *address*	Enable source IP check and configure the default source IP address of the legal multicast flows in all multicast groups. By default, this function is disabled.
DES-7210(config)# **no ip igmp snooping source-check default-server**	Disable source IP check.
DES-7210(config)# **ip igmp snooping limit-ipmc vlan** *vid* **address** *address* **server** *address*	Add the source IP address of the legal multicast flow to a specified multicast group addresses. By default, the source IP address of the legal multicast flow is the IP address of the default-server.
DES-7210(config)# **no ip igmp snooping limit-ipmc vlan** *vid* **address** *address*	Cancel a limit-ipmc configuration.

The following example enables source IP check and set the default source IP address to 1.1.1.1. In the example, a multicast group address-source IP address entry is added, where vid is 1, group IP address is 233.3.3.3 and source ip address is 1.1.1.2.

```
DES-7210# configure Terminal
DES-7210(config)# ip igmp snooping source-check default-server 1.1.1.1
DES-7210(config)# ip igmp snooping limit-ipmc vlan 1 address 223.3.3.3 server 1.1.1.2
DES-7210(config)# end
```

16.2.15 Configuring IGMP Profiles

An IGMP Profile entry defines a set of multicast address range and permit/deny activity for the funcitons like multicast address range for SVGL mode, multicast data range filtered on the router interface, and IGMP Filtering range. Note that modifying an IGMP Profile after associating it with a function will influence the multicast forwarding table generated by the function.

To configure an IGMP profile, execute the following commands:

Command	Function
DES-7210(config)# **ip igmp profile** *profile-number*	Enter the IGMP Profile mode. Assign a number in the range of 1 to 1024 to identify. By default, no profile is configured.
DES-7210 (config-profile)# **permit** | **deny**	(Optional) Permit or deny this range of multicast addresses while deny or permit other multicast addresses. The default value is deny.
DES-7210(config-profile)# **range** *ip multicast-address*	Add one or more multicast address ranges.
DES-7210# **end**	Return to the privileged mode.

To delete an IGMP Profile, use **no ip igmp profile** *profile-number*.

To delete a range of the IGMP Profile, use **no range** *ip multicast address*.

This example shows the IGMP Profile configuration process:

```
DES-7210(config)# ip igmp profile 1
DES-7210(config-profile)# permit
```

```
DES-7210(config-profile)# range 224.0.1.0 239.255.255.255
DES-7210(config-profile)# end
DES-7210# show ip igmp profile 1
IGMP Profile 1
permit
range 224.0.1.0 239.255.255.255
```

As you can see, the rule of the IGMP Profile is to permit the multicast addresses from 224.0.1.0 to 239.255.255.255, while all other multicast addresses are denied.

16.2.16 Configuring the Multicast Address Range in the SVGL /IVGL-SVGL Mode

When the IGMP Snooping works in the SVGL or IVGL-SVGL mode, a profile shall be associated to specify the multicast group address range applied in the SVGL or IVGL-SVGL mode. That is to say, the member ports of the multicast forwarding entry can be forwarded across the VLANs while the member ports of the multicast forwarding entry in the other multicast address range must belong to the same VLAN. By default, no profile is associated.

Command	Function
DES-7210(config)# **ip igmp snooping svgl profile** *profile name*	Set a profile associated with the SVGL.
DES-7210(config)# **no ip igmp snooping svgl profile**	Remove a profile associated with the SVGL. The default value is 0.

This example configures the multicast address range in the SVGL or IVGL-SVGL mode:

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping ivgl-svgl
DES-7210(config)# ip igmp snooping svgl profile 1
DES-7210(config)# end
DES-7210# show ip igmp snooping
IGMP-snooping mode        :IVGL
SVGL vlan-id             : 1
SVGL profile number      : 1
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

16.2.17 Configuring IGMP Filtering

In some cases, you may need to limit a port to receive a specified set of multicast data flows, and control the maximum number of multicast groups that the port is allowed to join dynamically IGMP Filtering can address this requirement.

You can apply one IGMP Profile to a port. If the port receives the IGMP Report message, the switch will check if the IP address of the multicast group that the port wants to join is permitted by the IGMP Profile. If so, the switch allows it to join the multicast group.

You can also configure the maximum number of multicast groups that the port is allowed to join. If the number of the multicast groups that the port joins exceeds the threshold, the switch will no longer receive or handle the IGMP Report message.

To enable IGMP Filtering, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration interface.
DES-7210(config-if)# **ip igmp snooping filter** *profile-number*	(Optional) Apply a profile to the interface. The profile number ranges from 1 to 1024.
DES-7210(config-if)# **ip igmp snooping max-groups** *number*	(Optional) Specify the maximum number of multicast groups that the interface can join, in the range of 0 to 1024.
DES-7210(config-if)# **no ip igmp snooping max-groups**	(Optional) Restore the max-groups to the default value.

The example below shows how to configure IGMP Flitering:

```
DES-7210# configure terminal
DES-7210(config)# interface fastEthernet 0/1
DES-7210(config-if)# ip igmp snooping filter 1
DES-7210(config-if)# ip igmp snooping max-groups 1000
DES-7210 (config-if)#end
DES-7210 #show ip igmp snooping interface fastEthernet 0/1
Interface            Filter profile number      max-group
---------------      ---------------------      ---------
FastEthernet 0/1            1                       1000
```

16.3 Viewing IGMP Snooping Information

You can view the following IGMP Snooping information:

- Current operation mode
- Router interface
- Dynamic forwarding table
- Source port check
- IGMP Profile
- IGMP Filtering

16.3.1 Viewing Current Mode

To view the current operation mode and global configuration of IGMP Snooping, execute the following command in the privileged mode:

Command	Function
DES-7210# **show ip igmp snooping**	View the current operation mode and global configuration of IGMP Snooping.

The following example uses the **show ip igmp snooping** command to view the IGMP Snooping configuration information:

```
DES-7210# show ip igmp snooping
IGMP-snooping mode      : IVGL
SVGL vlan-id            : 1
SVGL profile number     : 0
```

```
Source port check       : Disabled
Source ip check         : Disabled
IGMP Fast-Leave         : Disabled
IGMP Report suppress    : Disable
```

16.3.2 Viewing and Clearing IGMP Snooping Statistics

To view and clear the IGMP Snooping statistics, execute the following commands in the privileged mode:

Command	Function
DES-7210# **show ip igmp snooping statistics** [**vlan** *vlan-id*]	View the IGMP Snooping statistics
DES-7210# **clear ip igmp snooping statistics**	Clear the IGMP Snooping statistics

The following example uses the **show ip igmp snooping statistics** command to view the IGMP Snooping statistics:

```
DES-7210# show ip igmp snooping statistics
Current number of Gda-table entries: 1
Configured Statistics database limit: 1024
Current number of IGMP Query packet received : 1957
Current number of IGMPv1/v2 Report packet received: 5
Current number of IGMPv3 Report packet received: 4
Current number of IGMP Leave packet received: 1

GROUP  Interface  Last Last  Report  Leave report time reporter  pkts   pkts
------   -------- ---------- ----------- ---- -- -------- ----
233.3.3.3 gi1/1   00:02:40   1.1.1.1     3       1
```

16.3.3 Viewing the Router Interface

To view the router interface information of IGMP Snooping, execute the following commands in the privileged mode:

Command	Function
DES-7210# **show ip igmp snooping mrouter**	Show the router interface information of IGMP Snooping

The following example uses the **show ip igmp snooping** command to view the router interface information of IGMP Snooping:

```
DES-7210# show ip igmp snooping mrouter
Vlan    Interface          State       IGMP profile number
----    --------            -------     -------------------
1   GigabitEthernet 0/7    static       1
1   GigabitEthernet 0/12   dynamic      0
```

16.3.4 Viewing Dynamic Forwarding Table

To view the forwarding rule of each port in the multicast group, that is, the GDA(Group Destination Address) table, execute the following commands in the privileged mode:

Command	Function
DES-7210# **show ip igmp snooping gda-table**	Show the forwarding rule of each port in the multicast group.

This example shows the information on various multicast groups of the GDA table and the information on all the member ports of one multicast group:

```
DES-7210# show ip igmp snooping gda-table
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address              Member ports
--------------------    ----------------------------------
1      233.3.3.3          GigabitEthernet 0/7(S)
```

16.3.5 Clearing Dynamic Forwarding Table

To clear the forwarding rule of each port in the multicast group, that is, the GDA(Group Destination Address) table, execute the following commands in the privileged mode:

Command	Function
DES-7210#**clear ip igmp snooping gda-table**	Clear the forwarding rule of each port in the multicast group.

This example clears the information on various multicast groups of the GDA table:

```
DES-7210# clear ip igmp snooping gda-table
```

16.3.6 Clearing IGMP Snooping Statistics

To clear the forwarding rule of each port in the multicast group, that is, the GDA(Group Destination Address) table, execute the following commands in the privileged mode:

Command	Function
DES-7210#**clear ip igmp snooping statistics**	Clear the dynamic statistics of the entry node in the forwarding table.

This example clears the multicast group statistics in the GDA table:

```
DES-7210# clear ip igmp snooping statistics
```

16.3.7 Viewing Source Port Check Status

To view the current source port check status of IGMP Snooping, execute the following command in the privileged mode:

Command	Function
DES-7210# **show ip igmp snooping**	View the current operation mode and global configuration of IGMP Snooping.

This example shows the source port check status of IGMP Snooping:

```
DES-7210(config)# show ip igmp snooping
IGMP-snooping mode        :IVGL
SVGL vlan-id             :1
SVGL profile number      :0
Source check port        :Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

16.3.8 Viewing IGMP Profile

To view the IGMP Profile information, execute the following command in the privileged mode:

Command	Function
DES-7210# **show ip igmp profile** *profile-number*	View the IGMP Profile information.

This example shows the IGMP Profile information:

```
DES-7210# show ip igmp profile 1
Profile    1
       Permit
       range 224.0.1.0,   239.255.255.255
```

16.3.9 Viewing IGMP Filtering

To view the IGMP Filtering information, execute the following command in the privileged mode:

Command	Function
DES-7210# **show ip igmp snooping interface** *interface-id*	View IGMP Filtering information.

The following example views the IGMP Filtering information.

```
DES-7210# show ip igmp snooping interface GigabitEthernet 0/7
Interface         Filter Profile number     max-groups
----------       ----------------------    -----------
GigabitEthernet 0/7          1              4294967294
```

16.4 Configuring Other Restrictions of IGMP Snooping

16.4.1 Mutual Exclusion of SVGL, IVGL-SVGL Mode and Layer 3 Multicast

The SVGL mode and IVGL-SVGL mode of IGMP Snooping and layer 3 multicast-routing are mutually exclusive.

The layer 3 multicast-routing function can not be enabled when the SVGL mode or the IVGL-SVGL mode of IGMP Snooping has been enabled. Similarly, you can not enter the SVGL mode or the IVGL-SVGL mode of IGMP Snooping when the layer 3 multicast-routing function has been enabled.

16.4.2 Mutual Exclusion of SVGL, IVGL-SVGL Mode and PIM Snooping

The SVGL mode and IVGL-SVGL mode of IGMP Snooping and PIM Snooping are mutually exclusive.

PIM Snooping can not be enabled when the SVGL mode or the IVGL-SVGL mode of IGMP Snooping has been enabled.

16.4.3 Mutual Exclusion of Source IP Check and Layer 3 Multicast

The source IP check function of IGMP Snooping and layer 3 multicast-routing are mutually exclusive.

It influences the layer 3 multicast-routing forward when the source IP check function of IGMP Snooping has been enabled.

17 PIM-Snooping Configuration

17.1 PIM Snooping Overview

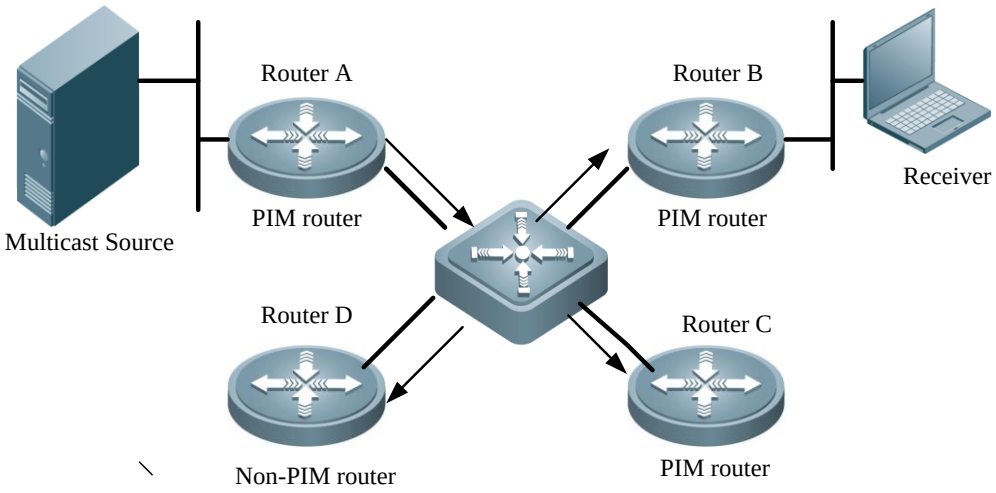
Within the network that the L2 switches connect with several routers, the multicast frames are forwarded in the broadcast form, which easily leads to the multicast flow storm and a waste of network bandwidth.

IGMP Snooping deals with the problem occurs when the connected receiving devices in the VLAN are all hosts and enables the multicast flow to be forwarded only to the port where the registered users are, not influencing other users. However, when the receiving devices in the VLAN in the downstream direction are the routers with PIM protocol enabled, IGMP Snooping fails to regulate the Layer 2 forwarding of the multicast flow. And PIM Snooping deals with the problem of Layer 2 forwarding of the multicast flow for the connected routers in the VLAN with PIM protocol enabled. PIM Snooping must be combined with IGMP Snooping to manage the Layer 2 forwarding of the multicast flow in the VLAN.

The figure below shows the flooding of multicast frames before the PIM snooping is enabled and the restriciton of multicast frames after the PIM snooping is enabled.

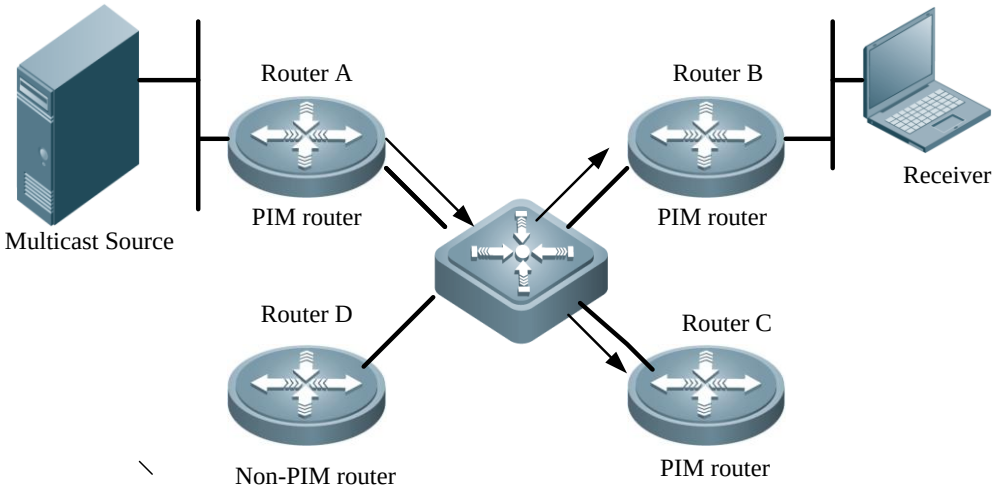
As shown in Figure-1, multicast frames is flooded to all the ports of the switch when the PIM snooping is not enabled.

Figure-1 Multicast flow When the PIM Snooping is not enabled



As shown in the Figure-2, multicst frames flow only to the ports that connect with the multicast routers B and C, but not to the router D.

Figure-2 Multicast flow after the PIM Snooping is enabled



Snooping means “eavesdrop”, from which we can understand the working process easily. When the L2 multicast device “eavesdrops” Hello message from router, it will add the interface to the multicast forwarding table. In a certain time, if the L2 multicast device does not receive Hello message, the interface will be removed from the forwarding table.

17.2 PIM Snooping Cofiguration Task Lists

The PIM snooping configuration task lists contain:

- Enable the IGMP Snooping globally (Mandatory)
- Enable the PIM Snooping globally (Mandatory)
- Enable the PIM Snooping on the interface (Mandatory)
- Disable the DR Flood (Optional)

17.2.1 Enabling the IGMP Snooping Globally

The IGMP Snooping IVGL mode must be enabled globally to ensure the normal running of PIM Snooping.

To enable the IGMP snooping globally, execute the following commands:

Command	Function
DES-7210(config)# **ip igmp snooping ivgl**	Enable the IGMP Snooping IVGL mode.

The following example will show how to enable the IGMP Snooping globally.

```
DES-7210(config)# ip igmp snooping ivgl
DES-7210(config)# end
```

17.2.2 Enabling the PIM Snooping globally

The PIM Snooping can be enabled in the VLAN after the it is enabled globally.

To enable the PIM snooping globally, execute the following commands:

Command	Function
DES-7210(config)# **ip pim snooping**	Enable the IGMP Snooping IVGL mode.

The following example will show how to enable the PIM Snooping globally and verify the configurations.

```
DES-7210(config)# ip pim snooping
DES-7210(config)# end
DES-7210# show ip pim snooping
Global runtime mode       : Enabled
Global admin mode     : Enabled
DR Flooding status        : Enabled
Number of user enabled VLANs: 0
User enabled VLANs:
```

Caution

The IGMP Snooping must be enabled before enabling PIM Snooping.

The PIM Snooping only deals with the Layer 2 multicast flow management for PIM-SM. If the Layer 3 multicast is enabled with PIM-DM protocol, it is possible that the multicast flow cannot be forwarded normally.

17.2.3 Enabling the PIM Snooping on the interface

The PIM Snooping must be enabled on the SVI interfaces respectively. With the PIM Snooping enabled on the interface, you can snoop the PIM messages, maintain and update the Layer 2 multicast forwarding table on the interface.

To enable the PIM snooping on the interface, execute the following commands:

Command	Function
DES-7210(config)# **interface vlan** *vlan_ID*	Enter the SVI interface configuration mode.
DES-7210(config-if)# **ip pim snooping**	Enable the PIM Snooping on the interface.

The following example will show how to enable the PIM Snooping on the interface and verify the configurations.

```
DES-7210(config)# interface vlan 199
DES-7210(config-if)# ip pim snooping
DES-7210(config-if)# end
DES-7210# show ip pim snooping
Global runtime mode: Enabled
Global admin mode: Enabled
DR Flooding status: Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 199
```


Caution

When the VLAN and the multicast source are connected, PIM Snooping floods the multicast flow to the interface connected to DR only. If another device in this VLAN becomes the forwarder for the STP creation, PIM Snooping fails to forward the multicast flow. It is not recommended to enable the PIM Snooping in the VLAN with multicast source.

17.2.4 Disabling the DR-flood

With PIM Snooping enabled in a VLAN, by default, the multicast flow will be flooded to the Layer port connected to the DR neighbor

To disable the DR-flood, execute the following commands:

Command	Function
DES-7210(config-if)# **no ip pim snooping dr-flood**	Disable the DR-flood..

The following example will show how to disable the DR-flood.

```
DES-7210(config)# no ip pim snooping dr-flood
DES-7210(config)# end
DES-7210# show ip pim snooping
Global runtime mode: Enabled
Global admin mode: Enabled
DR Flooding status: Disabled
Number of user enabled VLANs: 1
User enabled VLANs: 199
```


Caution

With the VLAN and the multicast source connected, the multicast flow must be flooded to the DR. Therefore, to disable the DR-flood function, you shall ensure that the VLAN and the multicast source are disconnected.

17.3 Monitoring and Maintaining PIM-Snooping

PIM Snooping offers command **show** to monitor and maintain PIM Snooping. You can view PIM Snooping information such as global configuration, neighboring list and Layer 2 forwarding table by executing command **show.**

17.3.1 Viewing PIM-Snooping

Use the following command to view PIM Snooping running status information:

Command	Function
show ip pim snooping	Show global configuration information of PIM Snooping.
show ip pim snooping neighbor	Show PIM Snooping neighbor information.

show ip pim snooping mroute [*A.B.C.C A.B.C.C*]	Show PIM Snooping forwarding table information.
show ip pim snooping statistics	Show global PIM Snooping statistics.
show ip pim snooping vlan *vlan-id*	Show PIM Snooping in a VLAN.

For the detailed usage of the above command, please refer to *PIM-Snooping Command Reference.*

Here are the examples:

The show ip pim snooping command :

```
DES-7210# show ip pim snooping
Global runtime mode: Enabled
Global admin mode : Enabled
DR Flooding status : Enabled
Number of user enabled VLANs: 2
User enabled VLANs: 199 198
```

The example above explains how to configure PIM Snooping globally and enable the DR-flood function. The PIM Snooping has been enabled on 2 VLANs: 199 and 198 respectively.

The show ip pim snooping neighbor command :

```
DES-7210# show ip pim snooping neighbor
IP Address          Port    Uptime/Expires    Flags
VLAN 199: 2 neighbors
214.199.199.2       Gi2/32  00:18:25/00:01:04
214.199.199.10   Gi2/20  00:18:09/00:01:03  DR
```

The example above shows 2 neighbors in the VLAN199. The neighbor 214.199.199.2 is connected to the interface Gi2/32 . The neighbor’s living time is 18’25” and expires in 1’ 4”.

The show ip pim snooping mroute command :

```
DES-7210# show ip pim snooping mroute
Flags:   JOIN/PRUNE - (*,G), (S,G) Join/Prune
     SGR-PP - (S,G,R) PrunePending, SGR-P - (S,G,R) Prune

VLAN 199: 1 mroutes
(*, 229.1.1.1), 00:06:12/00:03:06
  214.199.199.10->214.199.199.2, 00:06:12/00:03:06, JOIN
  Downstream ports: 2/36
  Upstream  ports: 2/32
  Outgoing  ports: 2/32 2/36
```

The example above lists the (*,229.1.1.1) entry. The entry aging time is 3’6”. The keepalive time for sending the Join message from the downstream neighbor 214.199.199.10 to the

upstream neighbor 214.199.199.2. The downstream Layer 2 port is 2/36, the upstream Layer 2 port is 2/32 and the outgoing Layer 2 port is 2/32, 2/36.

17.4 Examples of PIM-Snooping Configuration

17.4.1 Configuration requirement

As the following figure shows, multicast flow arrives on the interface of L3 switch in VLAN 2. In VLAN 3, being the routers in the downward direction, only router B configures PIM protocol while router A does not.

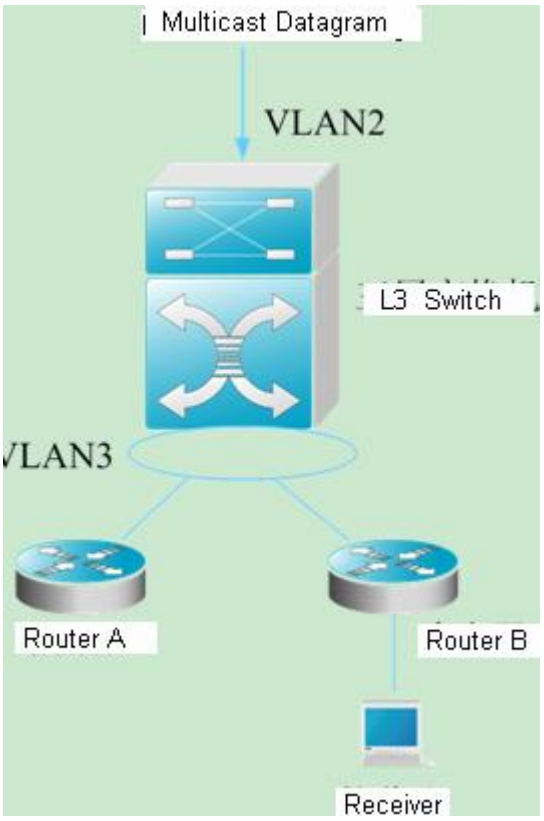


Figure-3 Topology Structure of PIM-Snooping Configuration Example

17.4.2 Device configuration

The following example explains how to configure PIM Snooping on the switch:

Step 1: Enable the IGMP Snooping

```
DES-7210# configure terminal
DES-7210(config)# ip igmp snooping ivgl
```

Step 2: Enable the PIMP Snooping

```
DES-7210(config)# ip pim snooping
DES-7210(config)# interface vlan 3
DES-7210(config-if)# ip pim snooping
DES-7210(config-if)# end
```

You can configure PIM Snooping for L2 multicast device in VLAN 3 according to above steps and view the running status of PIM Snooping by command **show.**

18 MSTP Configuration

18.1 MSTP Overview

18.1.1 STP and RSTP

18.1.1.1 STP and RSTP Overview

DES-7210 series supports both the STP protocol and the RSTP protocol, as well as complying with the IEEE 802.1D and IEEE 802.1w standards.

The STP protocol can prevent broadcast storm caused by link loops and provide link redundancy and backup.

For the layer 2 Ethernet, there is only one active channel between two LANs to avoid broadcast storm. However, it is necessary to set up redundant links to improve the reliability of a LAN. Furthermore, some channels should be in the backup status in order to take up its work when a link fails. It is obviously hard to control this process by manual. The STP protocol can complete this work automatically. It enables a device in a LAN to:

- Discover and activate an optimal tree-type topology of the LAN.
- Detect and fix failures and automatically update the network topology to offer the possible optimal tree-type structure at any time.

The LAN topology is automatically calculated by a set of bridge parameters set by the administrator. The proper configuration of these parameters is helpful to offer an optimal solution.

The RSTP protocol is completely compatible with the 802.1D STP protocol downward. As with traditional protocol, the RSTP protocol can prevent loop and offer link redundency. The most critical feature of the RSTP protocol is quickness. If the bridges in a LAN support the RSTP protocol and are configured appropriately by administrators, it will take no more than 1 second to re-span the topology tree once the network topology changes (it takes about 50 seconds for traditional STP protocol to re-span the topology tree).

Caution

For the switch buffer control, see the chapter *Buffer Control* in *Configuring QOS*.

18.1.1.2 Bridge Protocol Data Units (BPDU):

A stable tree-type topology depends on the following elements :

- The unique bridge ID of each bridge consists of the bridge priority and the MAC address.
- The root path cost refers to the cost from a bridge to the root bridge.
- Each port ID consists of the port priority and port number.

By exchanging the Bridge Protocol Data Units (BPDU) frame destined to the multicast address 01-80-C2-00-00-00 (in hex), bridges gets the information necessary for building the optimal tree-type topology.

A BPDU is comprised of the following elements:

- Root Bridge ID (root bridge ID that a bridge considers)
- Root Path cost (Root Path cost of a bridge).
- Bridge ID (ID of a bridge).
- Message age (the live time of the message)
- Port ID (port ID sending the message).
- Forward-Delay Time, Hello Time and Max-Age: time parameters.
- Other flag bits, such as network topology change and port status.

Once a port of a bridge receives a BPDU message whose priority is higher than its priority (or smaller bridge ID and smaller root path cost), the bridge will store this message on the port while updating and propagating them to all other ports. If the BPDU with lower priority is received, the bridge will discard this message.

This mechanism propagates a BPDU message of higher priority in the whole network. As a result:

- A bridge is elected to be the root bridge in the network.
- Each bridge other than the root bridge has a root port that offers a shortest path to the root bridge.
- Each bridge will calculate the shortest path to the root bridge.
- Each LAN has a designated bridge that lies in the shortest path between this LAN and the root bridge. The port for connecting the designated bridge and the LAN is referred to as the designated port.
- The root port and the designated port are in the forwarding status.
- Other ports beyond the spanning tree are in the discarding status.

18.1.1.3 Bridge ID

As specified in IEEE 802.1W standard, each bridge has an unique bridge ID based on which the root bridge is elected in spanning tree algorithm. The bridge ID consists of eight bytes, in which the last six bytes are the MAC address of the bridge, and the first two bytes are shown in the table below. Of which, the first four bits denote the priority, while the last twelve bits denote the system ID for extending the protocol in the future. This value is 0 in the RSTP, so the priority of the bridge should be configured as the multiple of 4096.

	Priority value				System ID											
Bit	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Value	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

18.1.1.4 Spanning-Tree Timers

The following describes three timers impacting the performance of spanning tree.

- Hello timer: Interval to send the BUDU message.
- Forward-Delay timer: Interval to change the port status, that is, the time interval at which the port switches from the listening status to the learning status and vice versa when the RSTP protocol runs in the compatible STP protocol mode.
- Max-Age timer: The longest time for the BPDU message. The system will discard the message when the timer times out.

18.1.1.5 Port Roles and Status

A port plays a role to present its function in the network topology.

- Root port: The port that provides the shortest path to the root bridge.
- Designated port: The port through which each LAN is connected to the root bridge.
- Alternate port: The alternate port of the root port that will take up its work when the root port fails.
- Backup port: The backup port of the designated port. If two ports of a bridge are connected to a LAN, the port with higher priority is the designated port and the other one is the backup port.
- Disable port: The port that is not in the active status, namely, the ports whose operation status is down.

Figure 1, Figure 2 and Figure 3 below show the roles of various ports:

R = Root port D = Designated port A = Alternate port B = Backup port

Unless otherwise stated, the priorities of these ports are in the descending order from left to right.

Figure-1

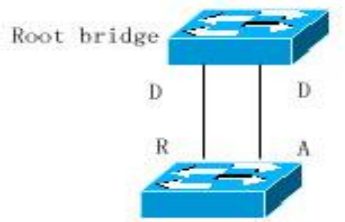


Figure-2

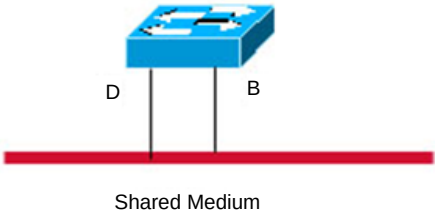
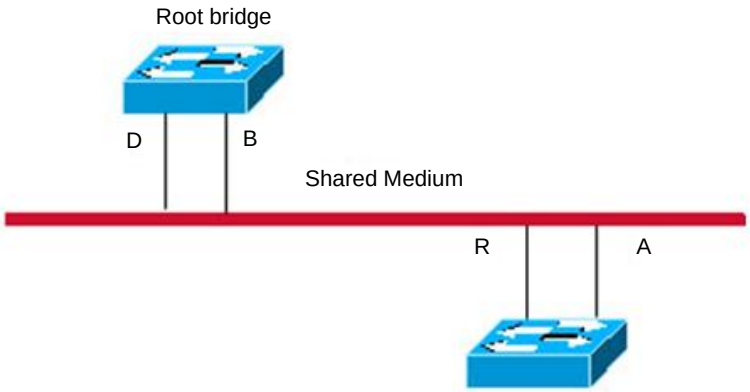


Figure-3



There are three port states for every port to indicate whether the data packet is forwarded and control the topology of the whole spanning tree.

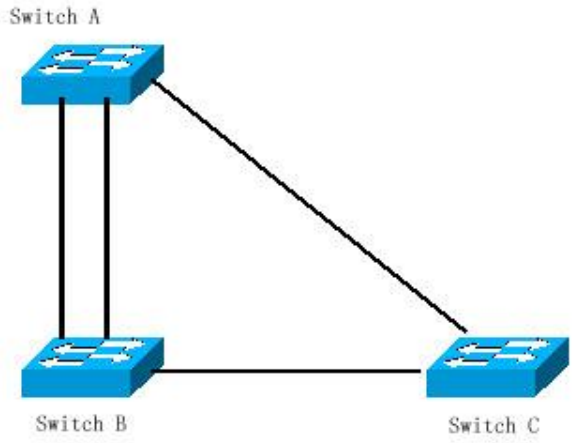
- Discarding: Neither forward the received frame nor learn about the source Mac address.
- Learning: Do not forward the received frame, but learn about the source Mac address, so it is a transitional status.
- Forwarding: Both forward the received frame and learn about the source Mac address.

For the stable network topology, only the root port and designated port can be the forwarding status, while other ports are only in the discarding status.

18.1.1.6 Generating a Network Topology Tree (Typical Application Solution)

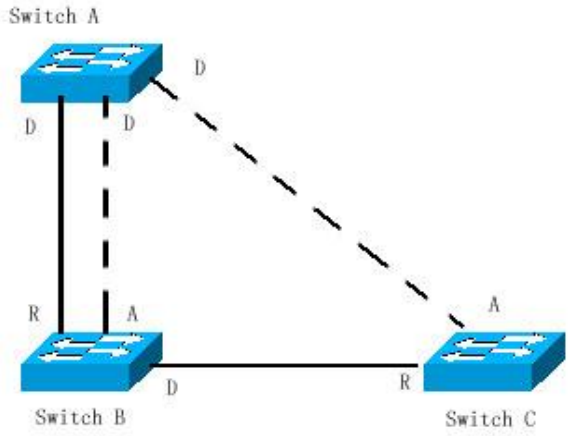
We now describe how the STP and RSTP protocols span a tree-type structure by the mixed network topology. As shown in Figure 4, the bridge IDs of Switches A, B and C are assumed in the ascending order. Namely, Switch A presents the highest priority. There is the 1000M link between switch A and switch B, and the 100M link between switch A and switch C, while it is the 10M link between switch B and switch C. Switch A acts as the backbone switch of this network and implements the link redundancy for both Switch B and Switch C. Obviously, broadcast storm would occur if all these links are active.

Figure-4



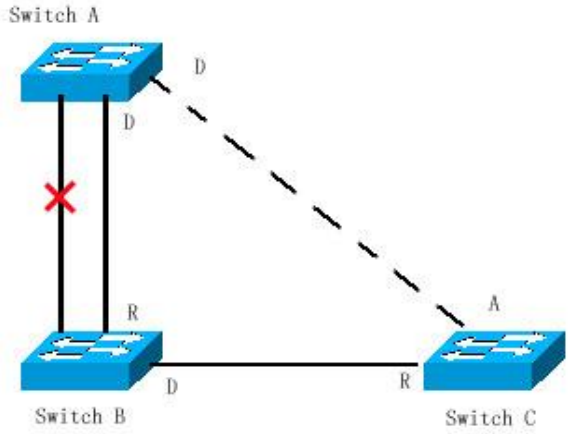
If all of these three switches enable the Spanning Tree protocol, they will select switch A as the root bridge by exchanging BPDU message. Once Switch B detects that two ports are connected to Switch A, it will select the port with the highest priority as the root port, while another one is selected as the alternate port. Meanwhile, Switch C detects that it can reach Switch A through Switch B or directly. However, Switch C discovers that the cost of the path from Switch B to Switch A is lower than that directly (For the costs corresponding to various paths, refer to table ***), so Switch C selects the port connected with Switch B as the root port, while the one that connected with Switch A as the alternate port. Various ports enter the corresponding status after their roles are determined. As a result, the network topology is generated as shown in Figure 5.

Figure-5



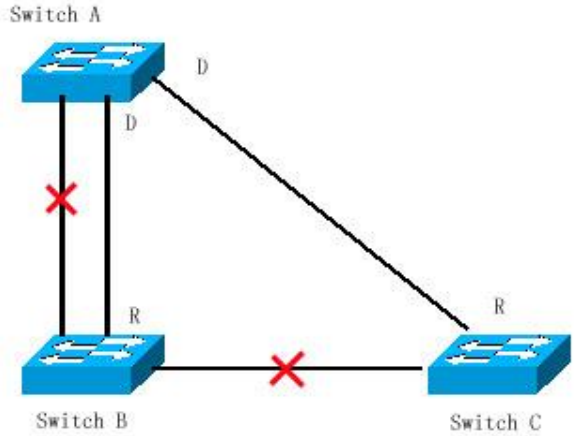
If the active path between Switch A and Switch B fails, the backup path will work. Consequently, the network topology is generated as shown in Figure 6.

Figure-6



If the path between Switch B and Switch C fails, Switch C will automatically switch the alternate port to the root port. Consequently, the network topology is generated as shown in Figure 7.

Figure-7



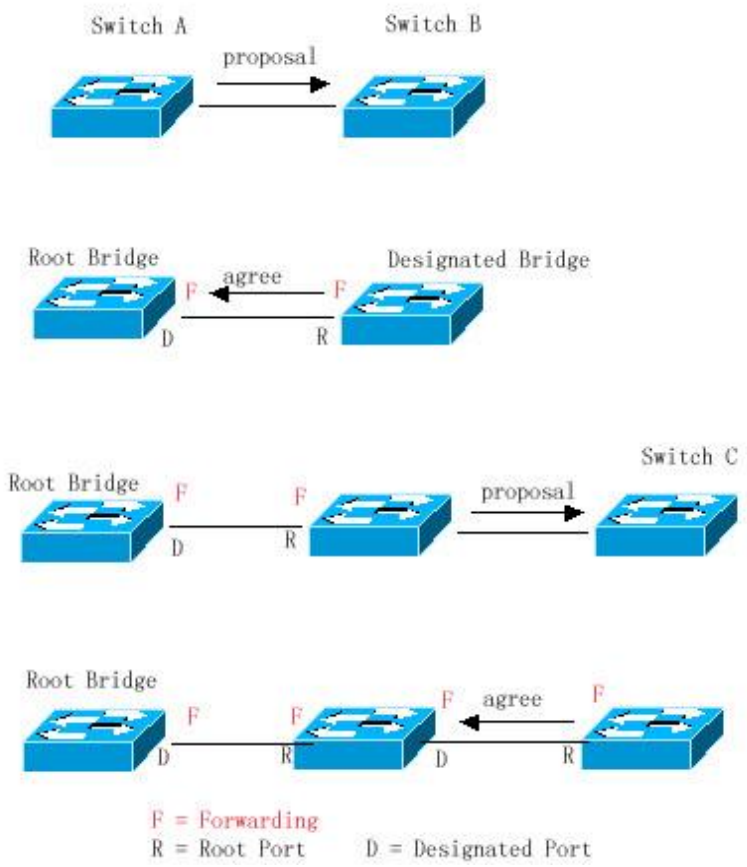
18.1.1.7 Rapid Convergence of RSTP

The following introduces the special function of RSTP: enabling rapid forwarding on a port.

The STP protocol will forward packets after 30s since the port roles are selected, which is twice as the Forward-Delay Time (you can set the Forward-Delay Time, which is 15s by default). Furthermore, the root port and designated port of each bridge will carry out the forwarding again after 30s, so it will take about 50s to stabilize the tree-type structure of the whole network topology.

The forwarding procedure of the RSTP protocol is different from that of the STP protocol. As shown in Figure 8, Switch A sends the specific proposal message of the RSTP protocol. Switch B detects that the priority of Switch A is higher than itself, takes the Switch A as the root bridge and the port that receives the message as the root port and forwards the proposal message. Then it sends the Agree message to Switch A through the root port. Upon the receipt of the proposal message, Switch A will forward the message through its designated port. After that, Switch sends the proposal message through the designated port to extend the spanning tree in turn. In theory, the RSTP protocol can immediately restore the tree-type network structure to implement rapid convergence when the network topology changes.

Figure-8



Caution

"Point-to-point Connection" between ports is required for the above "handshaking" process. In order to make full use of you device, do not use non-point-to-point connection between devices.

Other than Figure 9, other schematics in this chapter are the point-to-point connection. The following lists the example figure of the non point-to-point connection.

Example of Non Point-to-point Connection:

Figure-9

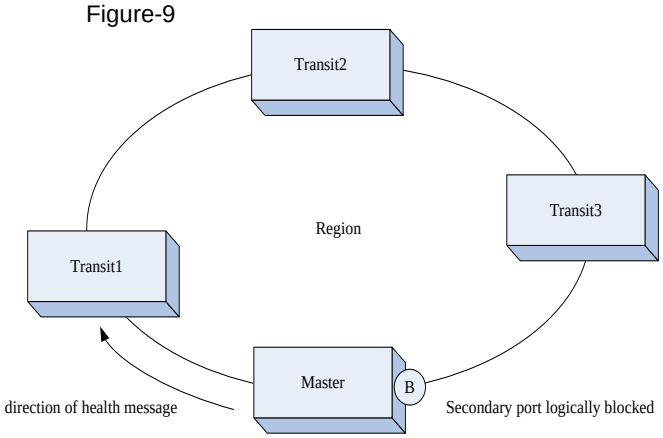
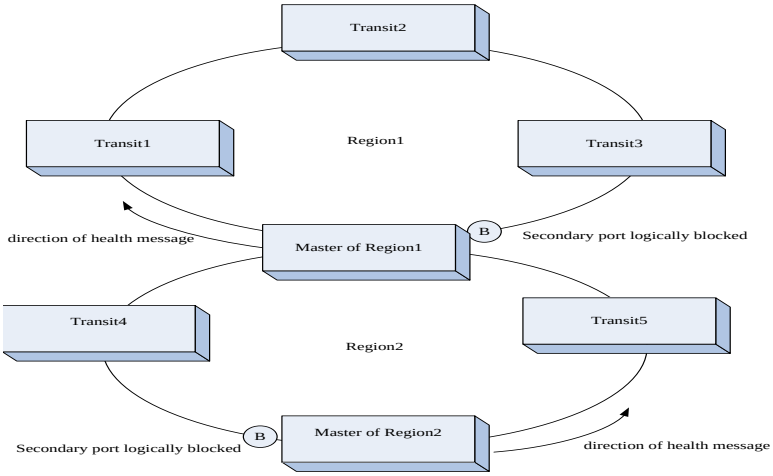
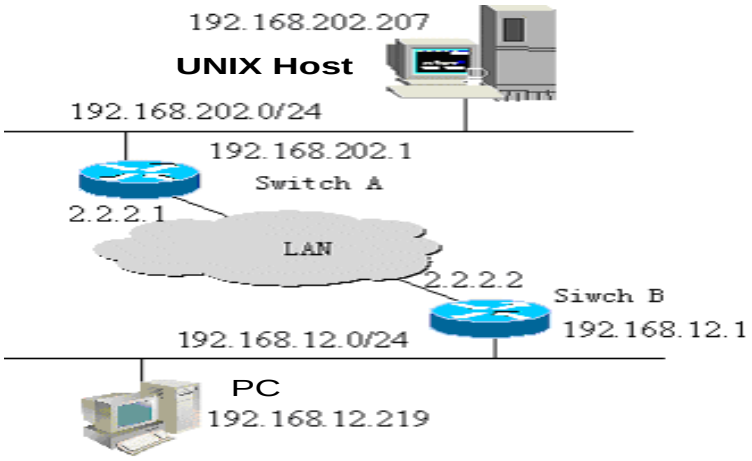


Figure-10



In addition, the following figure is a point-to-point connection and should be differentiated by users carefully.

Figure-11



18.1.1.8 Compatibility of RSTP and STP

The RSTP protocol is completely compatible with the STP protocol. It will judge whether the connected bridge supports the STP protocol or the RSTP protocol by the version number of the received BPDU message automatically. Only the forwarding process of the STP protocol is executed in the case of that the bridge supports the STP protocol. This cannot maximize the performance of the RSTP protocol.

Furthermore, using the RSTP protocol and the STP protocol will cause a problem. As shown in Figure 17-12, Switch A supports the RSTP protocol, while Switch B supports the STP protocol. Both switches are connected with each other. Switch A will send the STP BPDU message to Switch B for compatibility. However, if Switch A is connected with the RSTP-enabled Switch C, Switch A still sends the STP BPDU message, and thus causing that Switch C considers Switch A a STP-enabled bridge. As a result, two RSTP-supported switches run the STP protocol, reducing their efficiency greatly.

For this reason, the RSTP protocol provides the protocol-migration function to send the RSTP BPDU message forcibly in case that the peer bridge must support RSTP. In this way, Switch C will detect the bridge connected with it supports the RSTP protocol, so both two devices can run the RSTP protocol as shown in Figure 13.

Figure-12 Protocol Migration

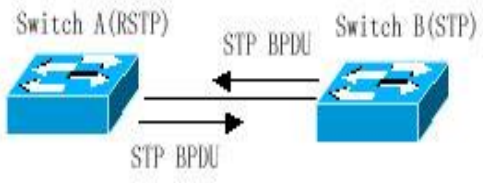
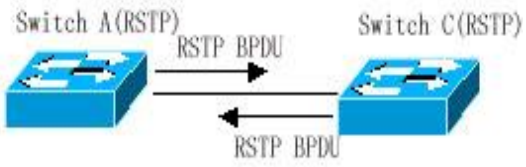


Figure-13



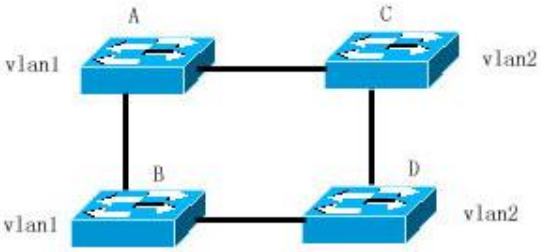
18.1.2 MSTP Overview

DES-7210 series supports the MSTP protocol, a new spanning-tree protocol derived from the traditional STP and RSTP protocols that includes the rapid forwarding mechanism of the RSTP protocol itself.

Since traditional spanning tree protocols are not related to a VLAN, the following problems may occur in a specific network topology.

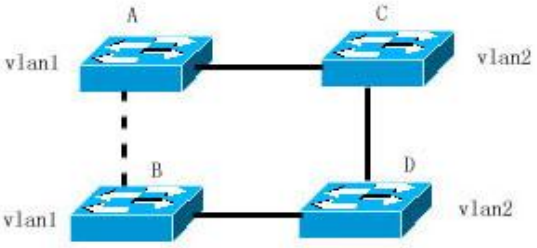
As shown in Figure 14, Switches A and B are located in Vlan1, and switches C and D in Vlan2. They form a loop.

Figure-14



If the cost of the path from Switch A through Switch C, Switch D to Switch B is smaller than that of the direct path from Switch A to Switch B, the latter path will be torn down, as shown in Figure 15. Packets in Vlan1 can not be forwarded because Switches C and D do not contain Vlan1. In this way, Vlan1 of Switch A cannot communicate with Vlan1 of Switch B.

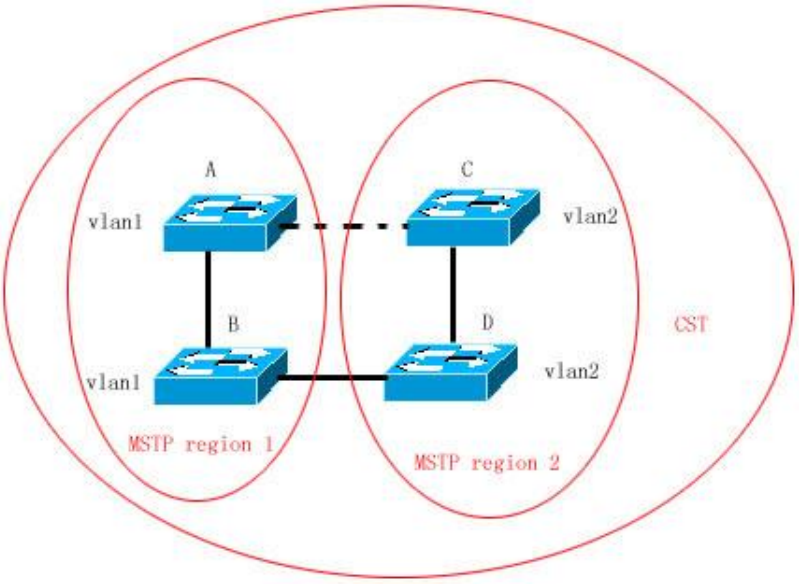
Figure-15



The MSTP protocol is developed to address this problem. It partitions one or more vlans of the switch into an instance, so the switches with the same instance configuration form a region (MST region) to run a separated spanning tree (this internal spanning-tree is referred to as the IST). The MST region is equivalent to a large device, which executes the spanning tree algorithm with other MST regions to obtain a whole spanning tree, referred to as the common spanning tree (CST).

With this algorithm, the above mentioned network can form the topology shown in Figure 16. Switches A and B are within the MSTP region 1 without a loop, so no path is discarded. This is also the case in the MSTP region 2. Region 1 and region 2 serve as two large devices respectively. There is a loop between them, so one path is discarded according to related configuration.

Figure-16



In this way, no loop occurs and the communication between the devices in a VLAN works as well.

18.1.2.1 How to Partition MSTP regions

According to above description, MSTP regions should be partitioned rationally and the switches in a MSTP region should be configured similarly for the MSTP protocol to work properly.

The MST configuration information contains:

- MST region name (name): A string of up to 32 bytes identifying the MSTP region.
- MST revision number: A revision number of 16 bits identifying the MSTP region.
- MST instance-vlan table: Each device can create up to 64 instances with IDs ranging from 1 to 64). Instance 0 always exists, so the system totally supports 65 instances. You can allocate 1 to 4094 VLANs for different instances (0 to 64) as needed, and the unallocated VLANs belong to instance 0 by default. In this way, each MSTI (MST instance) is a VLAN group and executes the spanning tree algorithm within the MSTI according to the MSTI information of the BPDU without the effect of the CIST and other MSTIs.

You can use the **spanning-tree mst configuration** command in the global configuration mode to enter the MST configuration mode and configure above information.

The MSTP BPDU carries above information. If a device has received the same MST configuration information of the BPDU as that of itself, it considers that the device connecting to this port belong to the same MST region as itself.

You are recommended to configure the instance-vlan table while the STP protocol is disable, and then enable the MSTP protocol to ensure the stability and convergence of the network topology.

18.1.2.2 Spanning Tree within a MSTP region (IST)

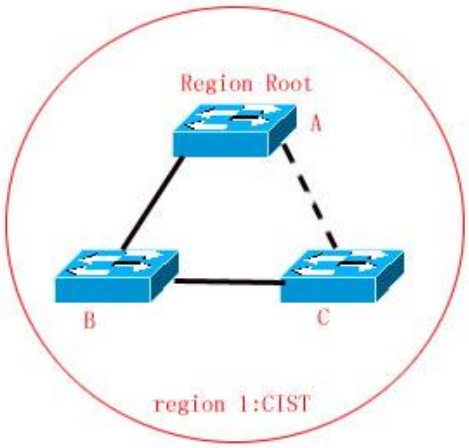
After MSTP regions are partitioned, a root bridge is elected for every instance within a region and the port role is determined for every port on a switch. A port is forwarded or discarded within an instance depneds on its role.

In this way, the IST (Internal Spanning Tree) is formed by exchanging the MSTP BPDU message, and various instances have their own spanning trees (MSTI). The spanning tree corresponding to the instance 0 is referred to as the CIST (Common Instance Spanning Tree) in conjunection with CST. That is to say, each instance provides each VLAN group with a single network topology without loop.

As shown in the following figure, Switches A, B and C form a loop within the region 1.

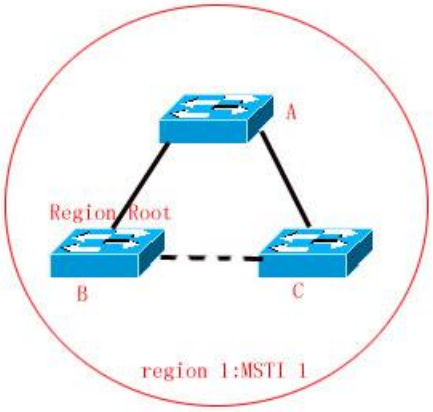
Switch A with the highest priority is selected as the region root in the CIST (instance 0). Then, the path between Switches A and C is discarded according to other parameters. Hence, for the VLAN group of instance 0, only the path from switch A to B and switch B to switch C are available, which break the loop of the VLAN group.

Figure-17



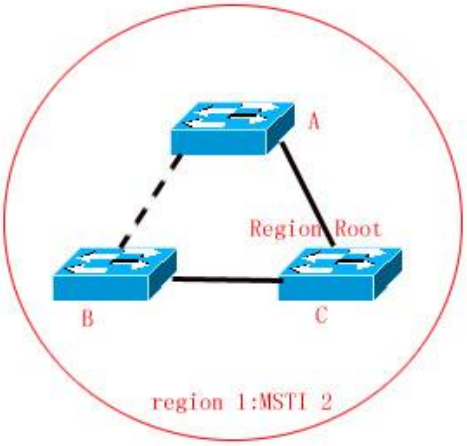
As shown in Figure 18, switch C with the highest priority is selected as the region root in the MSTI 1 (instance 1). Then, the path between switch A and B is discarded according to other parameters. Hence, for the VLAN group of instance 1, only the path from switch A to switch B and switch A to switch C are available, which break the loop of the VLAN group.

Figure-18



As shown in Figure 19, switch B with the highest priority is selected as the region root in the MSTI 2 (instance 2). Then, the path between switch B and switch C is discarded according to other parameters. Hence, for the VLAN group of instance 2, only the path from switch A to switch B and switch B to switch C are available, which break the loop of the VLAN group.

Figure-19

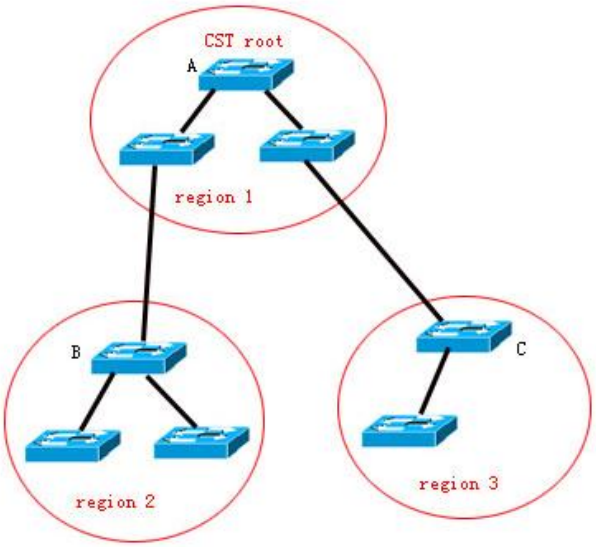


It should note that the MSTP protocol is not concerned on which VLAN a port belongs to, so users should configure corresponding path costs and priorities for ports according to actual VLAN configuration to prevent the MSTP protocol from breaking the loop unnecessarily.

18.1.2.3 Spanning Tree between MSTP regions (CST)

For CST, each MSTP region is equivalent to a large-sized device, and different MSTP regions also form a large-sized network topology tree, referred to as CST (common spanning tree). As shown in Figure 20, for CST, switch A with the smallest bridge ID is selected as the root of the entire CST (CST Root) and the CIST Regional Root in this region. In Region 2, since the root path cost from switch B to the CST root is the lowest one, switch B is selected as the CIST Regional Root in this region. Similarly, switch C is selected as the CIST Regional Root in Region 3.

Figure-20



The CIST Regional Root is not necessarily the device with the smallest bridge ID in that region. It is the device in the region that has the lowest root path cost to the CST root.

At the same time, the root port of the CIST regional root takes a new port role for the MSTI, namely the **Master port,** as the outlet of all instances, which is forwarded to all instances. In order to make the topology more stable, it is recommended to configure the outlet of the regions to the CST root on one device of this region as much as possible!

18.1.2.4 Hop Count

The IST and MSTI will not take the message age and Max age to calculate whether the BPDU message is timeout. Instead, they use the mechanism similar to the TTL of IP packets, namely hop count.

You can set it by using the **spanning-tree max-hops** command in the global configuration mode. The hop count is reduced by 1 when the BPDU message psses through a device in a region starting from the region root bridge until it is 0, which means the BPDU message is timeout. A device will discard the BPDU message whose hop count is 0.

In order to be compatible with the STP protocol and the RSTP protocol out a region, the MSTP protocol still remains the Message age and Max age mechanisms.

18.1.2.5 Compatibility of MSTP with RSTP and STP

For the STP protocol, the MSTP protocol will send the STP BPDU to be compatible with it like the RSTP protocol. For detailed information, refer to the Compatibility of RSTP and STP section.

For the RSTP protocol, it will process the CIST part of the MSTP BPDU, so it is not necessary for the MSTP to send the RSTP BPDU to be compatible with it.

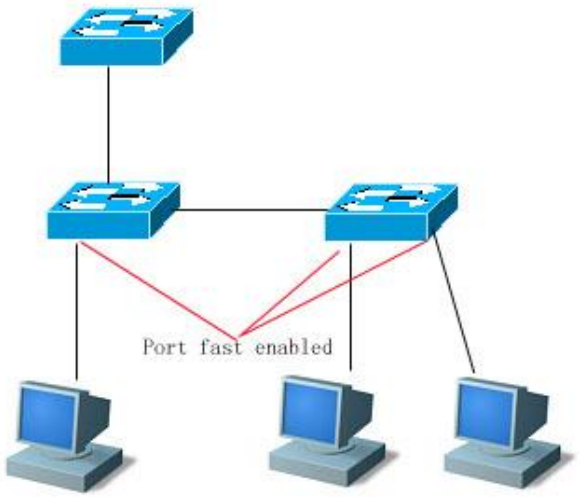
Each device that runs the STP or RSTP protocol is an independent region, and does not form the same region with any other device.

18.2 Overview of Optional Features of MSTP

18.2.1 Understanding Port Fast

If a port of a device is connected with the network terminal directly, this port can be set as the Port Fast to forward packets directly. The port does not need to wait 30 seconds before forwarding packets, which is the case when the port is not set to Port Fast. The following figure indicates which ports of a device can be set to Port Fast.

Figure-21



If the BPDU message is received from the Port Fast enabled port, its Port Fast operational state is disabled. At this time, this port will execute the forwarding by normal STP algorithm.

18.2.2 Understanding AutoEdge

If the specified port doesn't receive the BPDU message sent by the downstream port within a certain period of time (3 seconds), the port will be considered that it connects a network device and set as an edge port to enter the Forwarding status directly. An edge port will be automatically identified as a non-edge port after receiving the BPDU message.

You can disable the automatic identification function of the edge port by the **spanning-tree autoedge disabled** command.

This function is enabled by default.

Caution

1)When the AutoEdge function conflicts with the manually-configured Port Fast function, the latter shall prevail.

2) AutoEdge function can be used for rapid negotiation forwarding between the designated port and the downstream port, so the STP protocol doesn't support AutoEdge. If the designated port is in the forwarding status, Autoedge does not take effect on the port. It will take effect during repaid renegotiation such as pluging/unpluging network cables.

3) If a port enables the BPUD Filter, it forwards the BPDU message directly, but not be identified as the edge port automatically.

4) AutoEdge function is only applicable for the designated port.

5) AutoEdge complies with the standard definition of IEEE 802.1D (version 2004), in which the parameter range of Bridge Hello Time has been modified as 1.0-2.0. Therefore, you shall confirm that the Hello Time value is within the range when using AutoEdge function, or the risk of temporary loop will occur. It is recommended to disable AutoEdge function if it is neccesary to exceed the range of Hello Time.

18.2.3 Understanding BPDU Guard

The BPDU guard can be enabled globally or on individual interface. There are some slightly difference between these two ways.

You can use the **spanning-tree portfast bpduguard default** command to open the global BPDU guard enabled status in the privileged mode. In this status, if the BPDU message is received through a Port Fast-enabled port or a AutoEdge port, this port will enter the error-disabled status, indicating the configuration error. At the same time, the port will be closed to show that some illegal users may add a network device to the network, which change the network topology.

You can also use the **spanning-tree bpduguard enable** command to enable BPDU guard on individual interface in the interface configuration mode (it is not related to whether it is AutoEdge port or not). Under this situation, it will enter the error-disabled status if this interface receives the BPDU message.

18.2.4 Understanding BPDU Filter

The BPDU filter can be enabled globally or on individual interface. There are some slightly difference between these two ways.

You can use the **spanning-tree portfast bpdufilter default** command to enable the BPDU filter globally in the privileged mode. In this status, the BPDU messages can not be received or sent through a Port Fast-enabled port or a AutoEdge port, leading to no BPDU messages received by the host directly connecting the port. The BPDU filter will be disabled when the Port Fast is disabled for the AutoEdge port receives the BPDU message.

You can also use the **spanning-tree bpdufilter enable** command to enable the BPDU filter on individual interface in the interface configuration mode (it is not related to whether it is AutoEdge port or not). In this situation, this interface will not receive or transmit the BPDU message, but execute the forwarding directly.

18.2.5 Understanding Tc-protection

TC-BPDU messages are BPDU messages carrying with TC flag. When the L2 switch receives these messages, the network topology will change and the MAC address table will be deleted. And for L3 switch, the route table will be deleted and the port state in the ARP entry will change. To prevent the switch from processing abovementioned operations when pseudo TC-BPDU messages attack maliciously, too-heavy burden and network turbulance, the TC-protection function comes into being.

Tc-protection can only be enabled or disabled globally. It is enabled by default.

Once Tc-protection is enabled, the switch will delete the message within a certain period of time (usually 4 seconds) after receiving the TC-BPDU message while monitoring the TC-BPDU message. If it receives the TC-BPDU message during this period, it will perform the delete operation again after this period expires. This eliminates the need of frequently deleting MAC address entries and ARP entries.

18.2.6 Understanding TC Guard

The Tc-Protection function can reduce the removal of MAC address entries and ARP entries when a lot number of TC messages are generated in a network. However, you need to do

more delete oeprations in case of TC message attack. Furthermore, the TC message is propagated and will have an effect on the whole network. The TC Guard function allows you to disable the propagation of the TC message globally or on ports. When TC Guard function is configured globally or on a port, the port will shield the TC messages received or produced to prevent from propagating them to other ports. In this way, this funciton can manage TC message attack in the network and maintain the network stability. Moreover, this function can prevent from interrupting core routes due to the oscillation of the devices on the access layer.

Caution

Network communication will be broken off if you use tc-guard function incorrectly.

You are recommended to enable this function when you ensure that there is illegal tc message attack in the network.

If you enable global tc-guard, then all the ports will not spread tc message. It is applicable for those devices that are accessed on the desk to enable this function.

If you enable interface tc-guard, then the topology change and tc message received on this port will not be spreaded to other ports. It is applicable for up-link ports especially aggregated ports to enable this function.

18.2.7 Understanding BPDU Source MAC Check

The gobal of the BPDU source MAC check funciton is to prevent malicious attack on the switch by sending the BPDU message manually and thus cause the MSTP protocol work abnormally. When the peer switch connected to a port in the point-to-point mode is determined, enabling the BPDU source MAC check function can receive only the BPDU message from the remote switch and discard all other BPDU messages to protect against malicious attacks. You can configure the corresponding MAC addresses for the BPDU source MAC check fucntion on a specific port in the interface mode. Only one MAC address is configured for one port. BPDU source MAC check can be disabled by using the **no bpdu src-mac-check** command. In this case, any BPDU message is received on the port.

18.2.8 Understanding Invalid Length Filtering for BPDU

When the Ethernet length field of the BPDU message exceeds 1500 bits, this BPDU message is discarded in order to avoid receiving invalid BPDU messages.

18.2.9 Understanding ROOT Guard

In network design, root bridge and backup root bridge are always divided in the same region. Due to error configuration of accendant and malicious attack in the network, it is possible that root bridge receives configuration message of higher priority and loses the current root bridge position, leading to error turbulance of network topology, which Root Guard function can prevent from occuring.

When enabling Root Guard, it enforces the port role of all the instances as specified port. Once the port receives configuration message of higher priority, Root Guard will set the interface as root-inconsistent (blocked). If there is no configuration message of higher priority during the time long enough, the port will be restored to be the original normal status.

You shall disable ROOT Guard function if this function results in the blocked status for interfaces and it needs manual configuration to restore to the normal status. You can use the command **spanning-tree guard none** in the interface configuration mode to disable Root Guard function.


Caution

1. Incorrectly using ROOT Guard leads to network link breakdown.
2. If you enable ROOT Guard on non-designated port, the non-designated port will be enforced as designated port and show BKN status(blocking status).
3. If MST0 enters BKN status because it receives configuration message of higher priority on a port, ROOT Guard will enforce the port in all the other instances to enter BKN status.
4. ROOT Guard or LOOP Guard takes effect at the same time. That is , they can not both take effect at the same time .
5. The AutoEdge function is disabled when enabling the ROOT Guard-enabled port.

18.2.10 Understanding LOOP Guard

Due to breakdown of one-way link, root port or backup port becomes designated port, being ready to forward because they can not receive BPDU, causing the loop in the network, which Loop Guard function can prevent.

For the ports configured loop guard, if they can not receive BPDU, the port roles will be migrated. However, the port state is always set as discarding till the port receive BPDU again and recalculate spanning tree.


Caution

You can enable LOOP Guard based on global or interface.

ROOT Guard or LOOP Guard takes effect at the same time. That is , they can not both take effect at the same time .

The AutoEdge function on all interfaces is ineffective when enabling LOOP Guard function globally.

The AutoEdge function on the interface is ineffective when enabling LOOP Guard function in the interface configuration mode.

18.3 Configuring MSTP

18.3.1 Default Spanning Tree Configuration

The following table lists the default configuration of the Spanning Tree protocol.

Item	Default value
Enable State	Disable
STP MODE	MSTP
STP Priority	32768
STP port Priority	128
STP port cost	Automatically determine according to port rate.
Hello Time	2 seconds

Item	Default value
Forward-delay Time	15 seconds
Max-age Time	20 seconds
Default calculation method of the Path Cost	Long
Tx-Hold-Count	3
Link-type	Automatically determine by the duplex status of the port.
Maximum hop count	20
Corresponding relationship between vlan and instance	All VLANs belong to instance 0 Only instance 0 exists

You can restore the STP parameters to its default configuration (except for disabling STP) by using the **spanning-tree reset** command.

18.3.2 Enabling and Disabling the Spanning Tree Protocol

By default, the DES-7200 series runs the MSTP protocol.

The spanning tree protocol is disabled on the device by default.

To enable the spanning tree protocol, execute the following command in the privileged mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree**	Enable the spanning tree protocol.
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show spanning-tree**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To disable the spanning tree protocol, use the **no spanning-tree** command in the global configuration mode.

18.3.3 Configuring the Spanning Tree Mode

According to the 802.1-related protocols, it is not necessary for administrators to set much for three versions of the spanning tree protocols such as the STP, RSTP and MSTP. These versions are compatible with one another naturally. However, given that some manufacturers will not develop the spanning tree protocol by standards, it may cause some compatibility problem. Hence, we provide a command to facilitate administrators to switch to the lower version of the spanning tree protocol for compatibility when they detect that this device is not compatible with that of other manufacturers.

Note: When you switch to the RSTP or STP version from the MSTP version, all information about MSTP Region will be cleared.

The default mode of the device is MSTP.

To enable the spanning tree protocol, execute the following command in the privileged mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree mode mstp/rstp/stp**	Switch the spanning tree version.
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show spanning-tree**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the spanning tree mode to the default value, use the **no spanning-tree mode** command in the global configuration mode.

18.3.4 Configuring Switch Priority

Switch priority allows you to select the root and draw the topology of a network. It is recommended that administrators set the core device with higher priority (or smaller value) to facilitate the stablization of the whole network. You can assign different switch priorities for various instances so that various instances can run separate spanning tree protocol.Only the priority of CIST (Instance 0) is related to the devices between different regions.

As mentioned in Bridge ID, there are 16 values for the priority, and all of them are multiples of 4096, which are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. The default value is 32768.

To configure switch priority, execute the following command in the global configuration mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree** [**mst** *instance-id*] **priority** *priority*	Configure different switch priorities for different instances. This command configures the switch priority for instance 0 without the instance-id parameter. *instance-id*: ID of the instance in the range from 0 to 64. *priority*: switch priority in the range from 0 to 61440 and is increased by the integral multiple of 4096, 32768 by default.
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the switch priority to the default value, use the **no spanning-tree mst** *instance-id* **priority** command in the global configuration mode.

18.3.5 Configuring Port Priority

When two ports are connected to the shared media, the device will set the one of the higher priority (or smaller value) to be the forwarding status and the one of the lower priority (or larger value) to be the discarding status.If the two ports are of the same priority, the device will set the one with the smaller port number to the forwarding status. You can assign different port priorities to various instances on one port, by which various instances can run the separated spanning tree protocols.

Same as device priority, it has 16 values, all a multiple of 16. They are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240 respectively. The default value is 128.

To configure a port priority, execute the following commands in the privileged mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate Link.
DES-7210(config-if)# **spanning-tree** [**mst** *instance-id*] **port-priority** *priority*	Configure different priorities for different instances. The command without the *instance-id* parameter will configure a port priority for instance 0. *instance-id*: Interface ID in the range of 0 to 64. *priority*: Port priority of an instance in the range 0 to 240. Furthermore, it is increased by the integral multiple of 16, 128 by default.
DES-7210(config-if)# **end**	Return to the privileged EXEC mode.
DES-7210# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the port priority to the default value, execute the **no spanning-tree mst** *instance-id* **port-priority** command in the interface configuration mode.

18.3.6 Configuring Path Cost of a Port

The switch determines a root port upon the total of the path costs along the path from a port to the boot bridge. The port the total of paths costs from the port to the root brdige is the smallest is elected the root port. Its default value is calculated by the media speed of the port automatically. The higher the media speed, the smaller the cost is. It is not necessary for administrators to change it for the path cost calculated in this way is most scientific. You can assign different cost paths for various instances on one port, by which various instances can run the separated spanning tree protocols.

To configure the path cost of a port, execute the following commands in the privileged mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate Link.
DES-7210(config-if)# **spanning-tree** [**mst** *instance-id*] **cost** *cost*	Configure different priorities for different instances. The command without the *instance-id* parameter will configure a port priority for instance 0. *instance-id*: Interface ID in the range of 0 to 64. *cost*: Path cost of the port in the range of 1 to 200,000,000. The default value is calculated by the media rate of the port automatically.
DES-7210(config-if)# **end**	Return to the privileged EXEC mode.
DES-7210# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the path cost of a port to the default value, execute the **no spanning-tree mst** *cost* command in the interface configuration mode.

18.3.7 Configuring the Default Calculation Method of Path Cost (path cost method)

If the path cost of a port is the default value, the device will calculate the path cost of this port by port rate. However, IEEE 802.1d and IEEE 802.1t specify different path cost values for a port rate respectively. The value range of the 802.1d is short (1 to 65535), while the value range of the 802.1t is long (1 to 200,000,000). Administrators should unify the path cost standard of the whole network. The default mode is long (IEEE 802.1t Mode).

The following table lists the path costs set for different port rates in two standards.

Port Rate	Interface	IEEE 802.1d (short)	IEEE 802.1t (long)
10M	Common Port	100	2000000
	Aggregate Link	95	1900000
100M	Common Port	19	200000
	Aggregate Link	18	190000
1000M	Common Port	4	20000
	Aggregate Link	3	19000

To configure the default calculation method of path cost, execute the following commands in the privileged mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree pathcost method long/short**	Configure the default calculation method of the port path cost as long or short, with long by default.
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the setting to the default value, execute the **no spanning-tree pathcost** method command in the global configuration mode.

18.3.8 Configuring Hello Time

Configure the interval of sending the BPDU message. The default value is 2s.

To configure the Hello Time, execute the following commands in the privileged mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree hello-time** *seconds*	Configure the hello time ranging from 1 to 10s, 2s by default.
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the hello time to the default value, execute the **no spanning-tree hello-time** command in the global configuration mode.

18.3.9 Configuring Forward-Delay Time

Configure the interval for changing port status. The default value is 15s.

To configure the forward-delay time, execute the following commands in the global configuration mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree forward-time** *seconds*	Configure the forward delay time ranging from 4 to 30s, 15s by default.
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the forward-delay time to the default value, execute the **no spanning-tree forward-time** command in the global configuration mode.

18.3.10 Configuring Max-Age Time

Configure the maximum period of time before the BPDU message is aged out. The default value is 20s.

In the privilege mode, perform these steps to configure the Max-Age Time:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree max-age** *seconds*	Configure the max age time ranging from 6 to 40s, 20s by default.
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the max age time to the default value, execute the **no spanning-tree max-age** command in the global configuration mode.

Caution

Hello Time, Forward-Delay Time and Max-Age Time have their own value ranges. Meanwhile, the following condition must be addressed: 2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0 second). Otherwise, it may cause the topology instability

18.3.11 Configuring Tx-Hold-Count

Configure the maximum number of the BPDU message sent per second, 3 by default.

To configure the Tx-Hold-Count, execute the following commands in the global configuration mode:

Command	Function

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree tx-hold-count** *numbers*	Configure the maximum number of the BPDU message sent per second in the range of 1 to10, 3 by default.
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the Tx-Hold-Count to the default value, execute the **no spanning-tree tx-hold-count** command in the global configuration mode.

18.3.12 Configuring Link-type

Configure the link-type of a port. This is crucial for rapid RSTP convergence. For details, refer to Rapid RSTP Convergence. Without configuration, the device will set the link type of a port according to its duplex status automatically, with point-to-point for the full duplex port and shared for the half duplex port.

To configure the link type of a port, execute the following commands in the interface configuration mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config-if)# **spanning-tree link-type point-to-point/shared**	Configure the link type of the interface, with point-to-point for the full duplex port and shared for the half duplex port. Point-to-point indicates the rapid forwarding is enabled on the port.
DES-7210(config-if)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the link type of a port to the default value, execute the **no spanning-tree link-type** command in the interface configuration mode.

18.3.13 Configuring Protocol Migration Processing

This command is to check the version globally or on individual port. For related information, refer to Compatibility of RSTP and STP.

Command	Function
DES-7210# **clear spanning-tree detected-protocols**	Forcibly check the version on all ports.
DES-7210# **clear spanning-tree detected-protocols interface** *interface-id*	Check the version forcibly on the port.

18.3.14 Configuring a MSTP Region

To deploy several devices in the same MSTP Region, you have to configure these devices with the same name, the same revision number, and the same Instance-VLAN table.

You can assign a VLAN to instances 0 to 64 respectively as required. The remaining VLANs will be automatically assigned to instance 0. One vlan can only be of an instance.

It is recommended to configure the Instance-VLAN table when the MSTP protocol is disabled. After configuration, you should enable the MSTP protocol again to ensure the stability and convergence of the network topology.

To configure a MSTP region, execute the following commands in the global configuration mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree mst configuration**	Enter the MST configuration mode.
DES-7210(config-mst)# **instance** *instance-id* **vlan** *vlan-range*	Add a VLAN group to a MST instance. *instance-id*: Instance ID ranging from 0 to 64. *vlan-range:* VLAN range in the range 1 to 4094. For instance: The **instance 1 vlan 2-200** command is to add VLAN 2-200 to instance 1. The **instance 1 vlan 2,20,200** command is to add VLAN 2, VLAN 20 and VLAN 200 to instance 1. You can use the **no** option of this command to delete a VLAN from an instance, and the deleted VLAN will be added to instance 0 automatically.
DES-7210(config-mst)# **name** *name*	Specify the MST configuration name, a string of up to 32 bytes.
DES-7210(config-mst)# **revision** *version*	Specify the MST revision number in the range 0 to 65535. The default value is 0.
DES-7210(config-mst)# **show**	Verify the configuration.
DES-7210(config-mst)# **end**	Return to the privileged EXEC mode.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the MST region configuration to the default value, execute the **no spanning-tree mst configuration** command in the global configuration mode. You can use the **no instance** *instance-id* command to delete an instance. Similarly, the **no name** and **no revision** commands can be used to restore the MST name and MST revision number settings to the default value, respectively.

The following is the example of configuration:

```
DES-7210(config)# spanning-tree mst configuration
DES-7210(config-mst)# instance 1 vlan 10-20
DES-7210(config-mst)# name region1
DES-7210(config-mst)# revision 1
DES-7210(config-mst)# show
Multi spanning tree protocol : Enable Name [region1]
Revision 1
Instance Vlans Mapped
-------- --------------------
```

```
0 1-9,21-4094
1 10-20
------------------------------
DES-7210(config-mst)# exit
DES-7210(config)#
```

Caution Before configuring vlan and instance mapping relationship, please ensure that all configured VLANs have been created. Otherwise, the association of vlan and instance on part of the products may be failed.

18.3.15 Configuring Maximum-Hop Count

Maximum-Hop Count means how many devices the BPDU message will pass through in a MSTP region before being discarded. This parameter takes effect for all instances.

To configure the Maximum-Hop Count, execute the following commands in the global configuraiton mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree max-hops** *hop-count*	Configure the Maximum-Hop Count ranging from 1 to 40, 20 by default.
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To restore the Maxium-Hop Count to the default value, execute the **no spanning-tree max-hops** command in the global configuration mode.

18.3.16 Configuring Intereface Compatibility Mode

In interface compatibility mode, when a port sends BPDU, it will carry different MSTI information according to the current port attribute to realize interconnection with other vendors.

To configure the interface compatibility mode, execute the following commands in the privileged mode:

Command	**Function**
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)#**interface** *interface-id*	Enter the Interface configuration mode.
DES-7210(config-if)# **spanning-tree compatible enable**	Enable interface compatibility mode.

DES-7210(config-if)# **end**	Return to the privileged mode.
DES-7210# **show running-config**	Check configuration items.
DES-7210# **copy running-config startup-config**	Save the configuration.

To remove the settings, you can execute command **no spanning-tree compatible enable.**

18.4 Configuring Optional MSTP Features

18.4.1 Default Setting of Optional Spanning Tree Features

All the optional features are disabled by default, except for AutoEdge function.

18.4.2 Enabling Port Fast

Enabling Port Fast lets a port directly forward the BPDU message. When Port Fast is disabled due to the receipt of the BPDU message, the port will participate in the STP algorithm and forward the BPDU message normally.

To enable Port Fast, execute the following commands in the global configuraiton mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an Aggregate Link.
DES-7210(config-if)# **spanning-tree Portfast**	Enable Port Fast on the interface.
DES-7210(config-if)# **end**	Return to the privileged EXEC mode.
DES-7210# **show spanning-tree interface** *interface-id* **portfast**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To disable Port Fast, execute the **spanning-tree portfast disable** command in the interface configuration mode.

You can use the **spanning-tree portfast default** command in the global configuration mode to enable Port Fast on all ports.

18.4.3 Disabling AutoEdge

If the designated port does not receive any BPDU messages within 3 seconds, it is identified as the edge port automatically. However, Port Fast Operational State is disabled if the AutoEdge port receives BPDU messages. AutoEdge is enabled by default.

To disable AutoEdge, execute the following commands in the global configuraiton mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an Aggregate Link.
DES-7210(config-if)# **spanning-tree autoedge**	Enable AutoEdge on the interface.
DES-7210(config-if)# **end**	Return to the privileged EXEC mode.
DES-7210# **show spanning-tree interface** *interface-id* **portfast**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To disable AutoEdge, execute the **spanning-tree autoedge disable** command in the interface configuration mode.

18.4.4 Enabling BPDU Guard

After BPDU Guard is enabled, a port will in the error-disabled status after receiving the BPDU packet.

To configure the BPDU guard, execute the following commands in the global configuration mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree portfast Bpduguard default**	Enable the BPDU Guard globally.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate link.
DES-7210(config-if)# **spanning-tree portfast**	Enable Port Fast on the interface before the bpduguard configuration takes effect globally.
DES-7210(config-if)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To disable BPDU Guard, execute the **no spanning-tree portfast bpduguard default** command in the global configuration command.

To enable or disable BPDU Guard on an interface, execute the **spanning-tree bpduguard enable** command or the **spanning-tree bpduguard disable** command on the interface respectively.

18.4.5 Enabling BPDU Filter

A port neither transmit nor receive the BPDU message after the BPDU filter is enabled.

To configure the BPDU Filter, execute the following commands in the global configuration mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree portfast bpdufilter default**	Enable BPDU filter globally.
DES-7210(config)# **interface** *Interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate link.
DES-7210(config-if)# **spanning-tree Portfast**	Enable portfast on this interface before the bpduguard configuration takes effect globally.
DES-7210(config-if)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To disable BPDU Filter, execute the **no spanning-tree portfast bpdufilter default** command in the global configuration mode.

To enable or disable BPDU Filter on an interface, execute the **spanning-tree bpdufilter enable** command or the **spanning-tree bpdufilter disable** command in the interface configuration mode.

18.4.6 Enabling Tc_Protection

To configure Tc_Protection, execute the following commands in the global configuration mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree tc-protection**	Enable Tc-Protection
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To disable Tc_Protection, execute the **no spanning-tree tc-protection** command in the global configuration mode.

18.4.7 Enabling TC Guard

To enable TC Guard globally, execute the following commands in the global configuration mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **spanning-tree tc-protection tc-guard**	Enable TC Guard globally.
DES-7210(config)# **end**	Return to the privileged EXEC mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To configure TC Guard on an interface, execute the following commands in the interface configuration mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *Interface-id*	Enter the interface configuration mode. A legal interface includes a physical port and an aggregate link.
DES-7210(config-if)# **spanning-tree tc-guard**	Enable TC Guard on this interface.
DES-7210(config-if)# **end**	Return to the privileged mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

18.4.8 Enable BPDU Source MAC check

After the BPDU source MAC check is enabled, the switch accepts only the BPDU message from the specified MAC address.

To configure the BPDU source MAC check, execute the following commands in the interface configuration mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface includes a physical port and an aggregate link.
DES-7210(config-if)#**bpdu src-mac-check** H.H.H	Enable BPDU source MAC check.
DES-7210(config-if)# **end**	Return to the privileged mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To disable BPDU source MAC check, execute the **no bpdu src-mac-check** command in the interface mode.

18.4.9 Enabing Root Guard

To configure interface ROOT Guard, execute the following commands in the privileged mode:

Command	**Function**
DES-7210# **configure terminal**	Enter the global configuration mode,
DES-7210(config)#**interface** *Interface-id*	Enter the interface configuration mode.Valid interface includes physical port and Aggregate Link.
DES-7210(config-if)#**spanning-tree guard root**	Enable interface ROOT Guard.

DES-7210(config-if)# **end**	Return to the privileged mode.
DES-7210#**show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

18.4.10 Enabling Loop Guard

To configure global LOOP Guard, execute the following commands in the privileged mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode,
DES-7210(config)#**spanning-tree loopguard default**	Enable global LOOP Guard.
DES-7210(config)# **end**	Return to the privileged mode.
DES-7210#**show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

To configure interface LOOP Guard, execute the following commands in the privileged mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **interface** *Interface-id*	Enter the interface configuration mode. Valid interface includes physical port and Aggregate Link.
DES-7210(config-if)#**spanning-tree guard loop**	Enable interface Loop Guard.
DES-7210(config-if)# **end**	Return to the privileged mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

18.4.11 Disabling Interface Guard

To disable interface ROOT or LOOP Guard, execute the following commands in the privileged mode:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode,
DES-7210(config)# **interface** *Interface-id*	Enter the interface configuration mode.Valid interface includes physical port and Aggregate Link.
DES-7210(config-if)#**spanning-tree guard none**	Disable interface Loop Guard.
DES-7210(config-if)# **end**	Return to the privileged mode.
DES-7210# **show running-config**	Verify the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

18.5 Showing MSTP Configuration and Status

You can use the following show commands to view the configuration of MSTP:

Command	Meaning
DES-7210# **show spanning-tree**	Show the information on the parameters and topology of MSTP.
DES-7210# **show spanning-tree summary**	Show the information on various instances and port forwarding status of MSTP.
DES-7210# **show spanning-tree inconsistentports**	Show the block port due to root guard or loop guard.
DES-7210# **show spanning-tree mst Configuration**	Show the configuration information of the MST region.
DES-7210# **show spanning-tree mst** *instance-id*	Show the MSTP information of an instance.
DES-7210# **show spanning-tree mst** *instance-id* **interface** *interface-id*	Show the MSTP information of the specified instance of the interface.
DES-7210# **show spanning-tree interface** *interface-id*	Show the MSTP information of all the instances of the interface.
DES-7210# **show spanning-tree forward-time**	Show forward-time.
DES-7210# **show spanning-tree Hello Time**	Show Hello time.
DES-7210# **show spanning-tree max-hops**	Show max-hops.

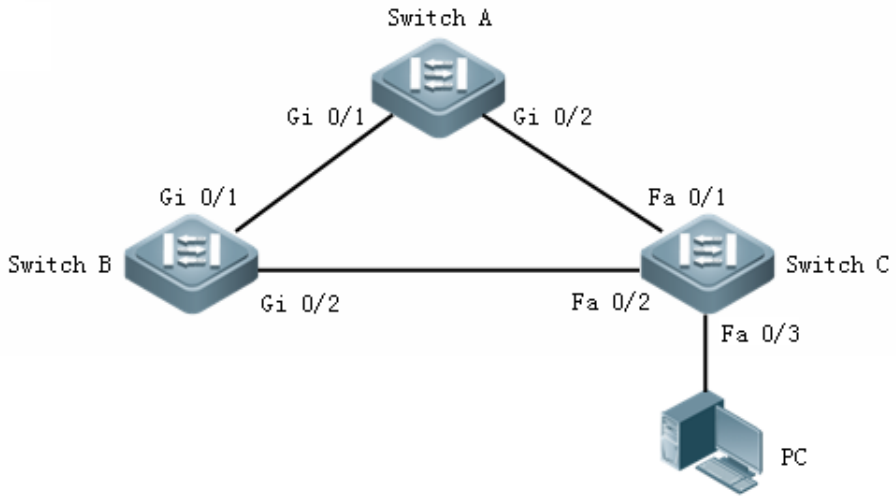
Command	Meaning
DES-7210# **show spanning-tree tx-hold-count**	Show tx-hold-count.
DES-7210# **show spanning-tree pathcost Method**	Show pathcost method.

18.6 MSTP Configuration Example

18.6.1 Configuration Purpose

1. Interconnect three switches to construct a triangle ring network and MSTP configuration mode.
2. Set the corresponding VLAN-INSTANCE mapping, MST configuration name, MST Revision Number and the instance priority on the switches.
3. View the MSTP configurations.
4. Enable BPDU Guard function globally and set PortFast function on the port connecting to the PC directly.

18.6.2 Topology



18.6.3 Configuration Steps

1) **Configuring Switch A**

Set interface Gi0/1 and Gi 0/2 as Trunk port and create VLAN 2 and VLAN 3

```
DES-7210# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode trunk
DES-7210(config-if)# exit
DES-7210(config)# interface gigabitEthernet 0/2
DES-7210(config-if)# switchport mode trunk
DES-7210(config-if)# exit
DES-7210(config)# vlan 2
DES-7210(config-vlan)# exit
DES-7210(config)# vlan 3
```

```
DES-7210(config-vlan)# exit
```

Set the spanning tree to MSTP mode, VLAN 2-Instance 1 and VLAN 3-Instance 2 mapping, and set the MST configuration name to DES-7210, MST Revision Number to 1. View the MST configurations and enable the spanning tree protocol.

```
DES-7210(config)# spanning-tree mode mstp
DES-7210(config)# spanning-tree mst configuration
DES-7210(config-mst)# instance 1 vlan 2
%Warning:you must create vlans before configuring instance-vlan relationship
DES-7210(config-mst)# instance 2 vlan 3
%Warning:you must create vlans before configuring instance-vlan relationship
DES-7210(config-mst)# name DES-7210
DES-7210(config-mst)# revision 1
DES-7210(config-mst)# show
Multi spanning tree protocol : Enable
Name    : DES-7210
Revision : 1
Instance  Vlans Mapped
-------- ---------------------------------------------
0       : 1, 4-4094
1       : 2
2       : 3
-------------------------------------------------------
DES-7210(config-mst)# exit
DES-7210(config)# spanning-tree
Enable spanning-tree.
```

Set the priority for Instance 0 to 4096

```
DES-7210(config)# spanning-tree mst 0 priority 4096
```

2) Configuring Switch B

Set interface Gi0/1 and Gi 0/2 as Trunk port and create VLAN 2 and VLAN 3

```
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport mode trunk
DES-7210(config-if)# exit
DES-7210(config)# interface gigabitEthernet 0/2
DES-7210(config-if)# switchport mode trunk
DES-7210(config-if)# exit
DES-7210(config)# vlan 2
DES-7210(config-vlan)# exit
DES-7210(config)# vlan 3
DES-7210(config-vlan)# exit
```

Set the spanning tree to MSTP mode, VLAN 2-Instance 1 and VLAN 3-Instance 2 mapping, and set the MST configuration name to DES-7210, MST Revision Number to 1. View the MST configurations and enable the spanning tree protocol.

```
DES-7210(config)# spanning-tree mode mstp
DES-7210(config)# spanning-tree mst configuration
DES-7210(config-mst)# instance 1 vlan 2
%Warning:you must create vlans before configuring instance-vlan relationship
DES-7210(config-mst)# instance 2 vlan 3
%Warning:you must create vlans before configuring instance-vlan relationship
DES-7210(config-mst)# name DES-7210
DES-7210(config-mst)# revision 1
DES-7210(config-mst)# exit
DES-7210(config)# spanning-tree
Enable spanning-tree.
```

Set the priority for Instance 0 to 4096

```
DES-7210(config)# spanning-tree mst 1 priority 4096
```

3) **Configuring Switch C**

Set interface Gi0/1 and Gi 0/2 as Trunk port and create VLAN 2 and VLAN 3

```
DES-7210(config)# interface fastEthernet 0/1
DES-7210(config-if)# switchport mode trunk
DES-7210(config-if)# exit
DES-7210(config)# interface fastEthernet 0/2
DES-7210(config-if)# switchport mode trunk
DES-7210(config-if)# exit
DES-7210(config)# vlan 2
DES-7210(config-vlan)# exit
DES-7210(config)# vlan 3
DES-7210(config-vlan)# exit
```

Set the spanning tree to MSTP mode, VLAN 2-Instance 1 and VLAN 3-Instance 2 mapping, and set the MST configuration name to DES-7210, MST Revision Number to 1. View the MST configurations and enable the spanning tree protocol.

```
DES-7210(config)# spanning-tree mode mstp
DES-7210(config)# spanning-tree mst configuration
DES-7210(config-mst)# instance 1 vlan 2
%Warning:you must create vlans before configuring instance-vlan relationship
DES-7210(config-mst)# instance 2 vlan 3
%Warning:you must create vlans before configuring instance-vlan relationship
DES-7210(config-mst)# name DES-7210
DES-7210(config-mst)# revision 1
DES-7210(config-mst)# exit
DES-7210(config)# spanning-tree
```

```
Enable spanning-tree.
```

Set the highest priority for Instance 2

```
DES-7210(config)# spanning-tree mst 2 priority 4096
```

Enable BPDU Guard function globally and set the interface Fa 0/3 to Port Fast-enabled port.

```
DES-7210(config)# spanning-tree portfast bpduguard default

DES-7210(config)# interface fastEthernet 0/3

DES-7210(config-if)#spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs,
DES-7210es, bridges to this interface when portfast is enabled,can cause temporary loops.

DES-7210(config-if)# end
```

View the spanning tree configurations

```
DES-7210# show spanning-tree

StpVersion : MSTP

SysStpStatus : ENABLED

MaxAge : 20

HelloTime : 2

ForwardDelay : 15

BridgeMaxAge : 20

BridgeHelloTime : 2

BridgeForwardDelay : 15

MaxHops: 20

TxHoldCount : 3

PathCostMethod : Long

BPDUGuard : enabled

BPDUFilter : Disabled

LoopGuardDef  : Disabled

###### mst 0 vlans map : 1, 4-4094

BridgeAddr : 00d0.f82a.aa8e

Priority: 32768

TimeSinceTopologyChange : 0d:0h:19m:44s

TopologyChanges : 1

DesignatedRoot : 1000.00d0.f822.33aa

RootCost : 0

RootPort : 1

CistRegionRoot : 1000.00d0.f822.33aa

CistPathCost : 200000

###### mst 1 vlans map : 2

BridgeAddr : 00d0.f82a.aa8e

Priority: 32768

TimeSinceTopologyChange : 0d:0h:1m:46s
```

```
TopologyChanges : 7
DesignatedRoot : 1001.00d0.f834.56f0
RootCost : 200000
RootPort : 2
###### mst 2 vlans map : 3
BridgeAddr : 00d0.f82a.aa8e
Priority: 4096
TimeSinceTopologyChange : 0d:0h:1m:44s
TopologyChanges : 5
DesignatedRoot : 1002.00d0.f82a.aa8e
RootCost : 0
RootPort : 0
```

View the spanning tree configurations on the interface Fa 0/1

```
DES-7210# show spanning-tree interface fastEthernet 0/1
PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode  : None
###### MST 0 vlans mapped :1, 4-4094
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 1000.00d0.f822.33aa
PortDesignatedCost : 0
PortDesignatedBridge :1000.00d0.f822.33aa
PortDesignatedPort : 8002
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort
###### MST 1 vlans mapped :2
PortState : discarding
PortPriority : 128
PortDesignatedRoot : 1001.00d0.f834.56f0
PortDesignatedCost : 0
```

```
PortDesignatedBridge :8001.00d0.f822.33aa
PortDesignatedPort : 8002
PortForwardTransitions : 5
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : alternatePort
###### MST 2 vlans mapped :3
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 1002.00d0.f82a.aa8e
PortDesignatedCost : 0
PortDesignatedBridge :1002.00d0.f82a.aa8e
PortDesignatedPort : 8001
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : designatedPort
```

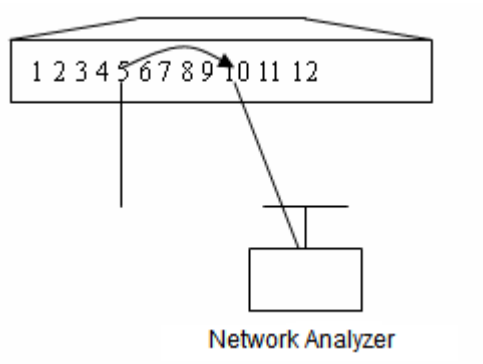
19 SPAN Configuration

19.1 Overview

With SPAN, you can analyze the communications between ports by copying a frame from one port to another port connected with a network analysis device or RMON analyzer. The SPAN mirrors all the packets sent/received at a port to a physical port for analysis.

For example, all the frames on the GigabitEhternet port 5 are mirrored to the GigabitEhternet port 10, as shown in Figure 18-1. Although the network analyzer connected to port 10 is not directly connected to port 5, it can receive all the frames from port 5.

Figure 1-1 SPAN Configuration Example



The SPAN allows you to monitor all the frames incoming/outgoing the source port, including the route input frames.

The SPAN does not affect the normal packet switching of the switch. Instead, it copies the frames incoming/outgoing the source port to the destination port. However, the frames may be discarded on an overflowed destination port, for example, when an 100Mbps port monitors an 1000Mbps port.

Caution

For the DES-7200 series, if IGMP Snooping function is enabled, the IGMP protocol messages cannot be mirrored to the designated port and the unknown multicast packets can not be mirrored neither.

For the DES-7200 series, if the mirrored destination port is congested(for example, a 100Mbps destination port monitors a 1000Mbps source port), the Pause frames are sent from the source port.

For the DES-7200 series, if the STP has not been enabled, the BPDU packets sent from the CPU can not be mirrored to the destination port.

By default, other ports on the DES-7200 series can not send the packets to the mirrored destination port. The mirrored destination port can not learn the address but it sends the packets to other ports. To allow the other ports to send the packets to the mirrored destination port and make the mirrored destination port to learn the address, you can configure the

mirrored destination port switching.

For the DES-7200 series, if the mirrored source port is the route port, the packets on the mirrored destination port are tag packets.

19.2 SPAN Concepts and Terms

This section describes the concepts and terms related to SPAN configuration.

19.2.1 SPAN Session

One SPAN session is the combination of one destination port and source port. You can monitor the inbounding, outbounding, and bi-directional frames of one or multiple interfaces.

You can set up one or multiple SPAN sessions. Switched port and routed port can be configured with only one SPAN session. However, switched port, routed port, and AP can be configured as source port and destination port. The SPAN session does not affect the normal operation of the switch.

You can configure the SPAN session on one disabled port, but the SPAN does not take effect until you enable the destination and source ports. The **Show monitor session** *session number* command allows you to show the operation status of the SPAN session. One SPAN session does not take effect immediately after the swtich is powered on until the destination port is active.

19.2.2 Frame Type

The SPAN session includes the following frame types:

- **Received frames**

Received frames include all known unicast frames and routing frames, and each received frame is copied to the destination port. In one SPAN session, you can monitor the the frames inputted from one or multiple source ports. Although a frame inputted from the source port is dropped due to some reasons, for example, port security, it is still sent to the destination port. This does not affect the function of the SPAN.

- **Transmitted frames**

All the frames sent from the source port are copied to the destination port. In one SPAN session, you can monitor the frames input from one or multiple source ports. If a frame from a port to the source port is dropped due to some reasons, the frame will not be sent to the destination port as well. Moreover, the format of the frames destined to the source port may change, for example, routed frames, source MAC address, destination MAC address, VLAN ID and TTL. Similarly, the format of the frames copied to the destination port will change.

- **Bi-directional frames**

Bi-directional frames include the above mentioned two frames. In one SPAN session, you can monitor the frames received and transmitted from/to one or multiple source ports.

19.2.3 Source Port

A source port (also known as monitored interface) is a switched port or routed port monitored for network analysis. In one SPAN session, you can monitor received, transmitted and bi-directional frames. There is no limit on the maximum number of the source ports.

A source port has the following features:

- It can be a switched port, routed port or AP.
- It cannot be a destination port at the same time.
- It can specify the inbounding or outbounding direction of the monitored frames.
- The source port and the destination port can reside in the same VLAN or different VLANs.

19.2.4 Destination Port

The SPAN session has a destination port (also known as the monitoring port) used to receive the frames copied from the source port.

The destination port has the following features:

- It can be a Switched Port , Routed Port or AP.

19.2.5 SPAN Traffic

You can use the SPAN to monitor all network communications, including multicast frames and BPDU frames.

19.2.6 Interaction between the SPAN and Other Functions

The SPAN interacts with the following functions.

- Spanning Tree Protocol (STP) — the destination port of SPAN participates in the STP.

19.3 Configuring SPAN

This section describes how to configure the SPAN on your switch.

19.3.1 Configuring SPAN

19.3.1.1 Default SPAN Configuration

Function	Default Configuration
SPAN status	Disabled

19.3.2 SPAN Configuration Guide

To configure the SPAN, do the following steps:

Connect the network analyzer to the monitoring port.

Caution

For the DES-7200 series, it costs the mirrored resources by SPAN function. A lack of the mirrored resources leads to the SPAN function failure.

The destination port cannot be the source port, and the source port cannot be the destination port.

You can configure one disabled port as a destination port or source port, but the SPAN does not take effect until the destination port or the source port is enabled again.

The **no monitor session** *session_number* command allows you to delete the source or destination port from the SPAN session in the global configuration mode.

The destination port of SPAN participates in the STP.

When the SPAN is enabled, the configuration change has the following result.

- If you change the VLAN configuration of the source port, the configuration takes effect immediately.
- If you change the VLAN configuration of the destination port, the configuration takes effect immediately.
- If you have disabled the source port or destination port, the SPAN does not take effect.
- If you add the source or destination port to an AP, this will remove the source port or destination port from the SPAN.

19.3.3 Creating a SPAN Session and Specifying the Monitoring Port and Monitored Port

To set up a SPAN session and sepcify the destination port and the source port, execute the following commands.

Command	Function
DES-7210(config)# **monitor session** *session_number* **source interface** *interface-id* [,| -] {**both**	**rx**	**tx**}	Specify the source port. *interface-id*: Specify corresponding interface id.
DES-7210(config)# **monitor session** *session_number* **destination interface** *interface-id* [**switch**]	Specify the destination port. *interface-id*: Specify corresponding interface id. The **switch** parameter supports exchange on the mirrored destination port.

To delete a SPAN session, use the **no monitor session** *session_number* command in the global configuration mode. To delete all the SPAN sessions, use the **no monitor session all** command in the global configuration mode. You can use the **no monitor session** *session_number* **source interface** *interface-id* command or the **no monitor session** *session_number* **destination interface** *interface-id* command to delete the source port or destination port in the global configuration mode.

The following example shows how to create session 1. First, clear the configuration of session 1, and then mirror the frames from port 1 to port 8. The **Show monitor session** command allows you to verify your configuration.

```
DES-7210(config)# no monitor session 1
DES-7210(config)# monitor session 1 source interface gigabitEthernet 3/1 both
DES-7210(config)# monitor session 1 destination interface gigabitEthernet 3/8
DES-7210(config)# end
DES-7210# show monitor session 1
```

```
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

Caution Session 1 is used to support ther global cross-linecard port mirror.

19.3.4 Deleting a Port from the SPAN Session

To delete a port from a SPAN session, execute the following commands:

Command	Function
DES-7210(config)# **no monitor session** *session_number* **source interface** *interface-id* [,| -] [**both**	**rx**	**tx**]	Specify the source port to delete. For *interface-id*: Specify corresponding interface id.

You can use the **no monitor session** *session_number* **source interface** *interface-id* command to delete the source port from a SPAN session in the global configuration mode. The following example shows how to delete port 1 from session 1 and verify your configuration.

```
DES-7210(config)# no monitor session 1 source interface gigabitethernet 1/1 both
DES-7210(config)# end
DES-7210# show monitor session 1
sess-num: 1
dest-intf:
GigabitEthernet 3/8
```

19.3.5 Configuring the Flow-based Mirror

To configure the flow-based mirror, execute the following commands:

Command	Function
DES-7210(config)# [**no**] **monitor session** *session_number* **source interface** *interface-id* **rx acl** *name*	Specify the matched acl name for the mirrored flow and the mirrored source and destination ports.

Only the incoming port mirror is supported.

For the ACL configuration commands, see the related configuration guide.

19.3.6 Configuring one-to –many Mirror

The one-to-many mirror is the mirror with one mirrored source port and multiple mirrored destination ports. An one-to-many mirror includes three types of ports: the source port, the

forwarding port and the destination port. To mirror the same source port to multiple destination ports, you can follow the steps below to:

- Set a RSPAN session(see the RSPAN configuration guide) with the one-to-many mirrored source port and mirrored forwarding port configured.
- Set the MAC loopback of the RSPAN forwarding port in the interface configuration mode.
- Add the forwarding port and the one-to-many mirrored destination port to the RSPAN VLAN in the Aceess mode.

Command	Function
DES-7210(config-if)# **mac-loopback**	Set the MAC loopback in the interface configuration mode.

- Only The DES-7200 series supports this function.
- For the RSPAN forwarding port, no other settings are configured or no network cable is connected.
- You may not configure the switching on the RSPAN forwarding port.
- The following are the warnings for the MAC loopback configuration:

Caution

For the port with MAC loopback configured, if other protocols are enabled on this port, it is possible that the loopback packets lead to the running error of other protocols. For example, when enabling the Spanning Tree Protocol on the port with MAC loopback configured, and enabling the Loop Guard function(See STP configuration guide) at the same time, the BPDU messages from the STP will be sent back to the STP. To this end, for the STP, the loop occurs in the current network. To prevent the loops, you can set the port role as Backup Port and the port state as Block by the STP algorithm. However, it results in the abnormal forwarding of the data packets on this port. It is necessary to disable the MAC loopback function and the Loop Guard function to restore the port forwarding.

19.4 Showing the SPAN Status

The **show monitor** command shows the current SPAN status. The following example illustrates how to show the current status of SPAN session 1.

```
DES-7210# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

20 RSPAN Configuration

RSPAN is the expansion of SPAN, which is able to remote monitor multiple devices. Each RSPAN Session is set up in specific RSPAN Vlan. Remote mirroring breaks the restriction that mirrored port and mirroring port must be on the same device, thus making them across multiple network devices and enabling accendant to observe the data package remote nirrored by analyzer in the center machine room.

All the mirrored packages are transmitted to the remote mirroring port via a special RSPAN Vlan. The following is the group network figure of device.

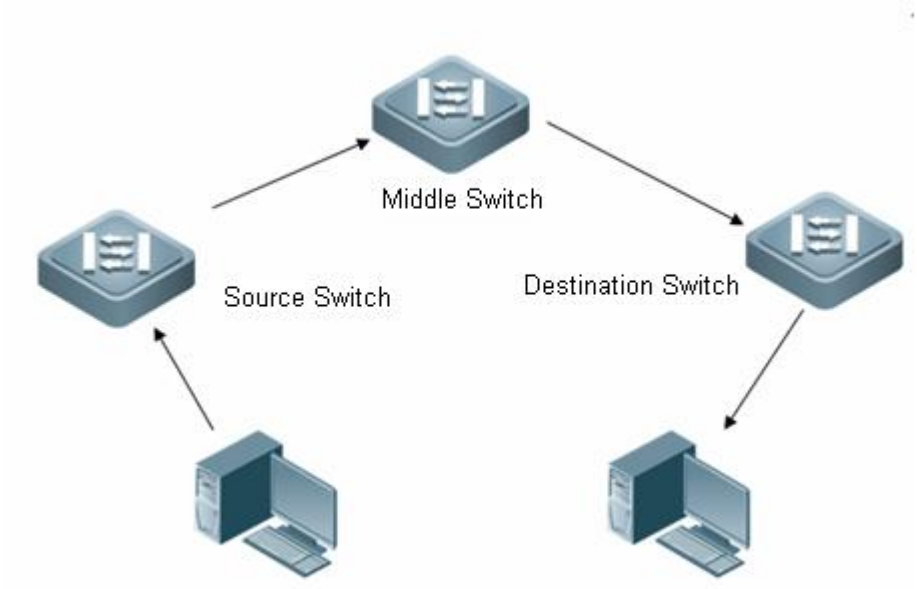


Figure 1

There are three types of the switch with remote mirroring funtion:

- Source switch: where the nirrored port is. It is responsible for copying mirroring flows to Remote VLAN and forwarding them to middle switch or destination switch.
- Middle switch: it is between source switch and destination switch. It transmmits the mirroring flows to next middle switch or destination switch via Remote VLAN. If the source switch is directly connected with destination switch, then there is no middle swith.
- Destination switch: where the mirroring destination port is. It forwards the mirroring flows received from Remote VLAN to the monitoring device via mirroring destination port.

The table below presents ports that participate mirroring on the switch:

Switch	Mirrored Port	Function

Source switch	Source Port	Monitored user port copies UDP to designated output port or reflector port via local port mirror. There are several source ports.
	Output port	Send mirrored packets to middle switch or destination switch.
Middle switch	Ordinary port	Send mirrored packets to destination switch. You are recommended to configure two Trunk ports to connect with two neighbouring devices in middle switch.
Destination switch	Source port	Receive remote mirrored packets.
	Destination port	Monitoring port of remote mirrored packets.

A special VLAN, Remote VLAN is defined to realize the function of remote port mirror, which is only used to transmit mirror packet and not used to bear the normal service data. Remote VLAN transmits all the mirrored packets from source switch to the designated port of the destination switch, realizing the function of monitoring the package on the remote port of the source switch from destination switch.

Caution

1. It is recommended to set the mirrored source port and reflector port in different VLANs.
2. AP can not be set as the Reflector Port.
3. Remote-span Vlan can neither be Vlan 1 nor Private Vlan
4. Remote-span Vlan does not join GVRP.
5. With STP enabled on the switch, it is recommended to configure BPDU Filter on the port which belongs to remote VLAN to prevent the port from being blocked and prevent the mirror packets from being forwarded. It is worth mentioning that you shall prevent the loops occurring in Remote VLAN because the BPDU packets can not go through the ports after cofiguring BPDU Filter.

20.1 Configuring RSPAN Session

20.1.1 Configuration Preparation

- Determine source switch, middle switch and destination switch.
- Determine mirrored source port, mirrored destination port and Remote VLAN.
- Guarentee L2 interconnectivity from source switch to destination switch in Remote VLAN via configuration.
- Determine the direction of monitored packets.
- Enable Remote VLAN

20.1.2 Configuration Process on Source Switch

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **vlan** *vlan-id*	Enter Vlan configuration mode.
DES-7210(config-Vlan)# **remote-span**	Set Vlan as remote-span Vlan.
DES-7210(config-Vlan)# **exit**	Return to the global configuration mode.
DES-7210(config)# **monitor session** *session_num* **remote-source**	Configure remote source mirror.
DES-7210(config)# **monitor session** *session-num* **source interface** *interface-name* [**rx** | **tx** | **both**]	Configure remote mirrored source port(rx,tx of the source port can be set to the same or different destination port; but each of them is set to one destination port only.)
DES-7210(config)#**monitor session** *session_num* **destination remote vlan** *remote_vlan-id* **interface** *interface-name* **[switch]**	Configure Remote VLAN of remote source mirror group. It is unnecessary for the DES-7200 series to configure the Reflector port. It is only necessary to configure the output destination port, but to key in the keyword reflector-port. **Switch** refers to the destination port joins switching.
DES-7210(config)# **monitor session** *session_number* **source interface** *interface-id rx* **acl** *name*	Set the matching acl name of the flow required for mirror.

Caution

- It is not recommended to set the DOWN port as the reflector port and do any other configurations on this DOWN port, for the reflector port can not forward the traffic normally.
- It is not recommended that you add the ordinary port to Remote VLAN.
- Do not set mirror source port on the port that is connected to the middle switch or the destination switch, or it will possibly cause the flow confusion in the network.
- In a RSPAN session, source switch only can set RX or TX mirror at a same time if the middle switch uses the port of 7200-24G, 7200-24, 7200-24P, 7200-48, 7200-2XG, 7200-48P and 7200-4XG line cards as the forwarding port. And if the source switch alternatively set RX and TX mirror, it is required for the middle switch to clear the mac address in remote-span vlan.
- It is not recommended to remove RSPAN in batch in VLAN RANGE 100 –1500 mode if you need to remove many consecutive RSPANs(200, for example) , which influences the system process efficiency badly.

20.1.3 Configuration Process on Middle Switch

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **vlan** *vlan-id*	Enter Vlan configuration mode.
DES-7210(config-Vlan)# **remote-span**	Set Vlan as remote-span Vlan.
DES-7210(config-Vlan)# **exit**	Return to the global configuration mode.

Caution

For the DES-7200 series, only the ports on the v2.x line cards and some v1.x line cards(7200-24GE) can take part in RSPAN as the ports of middle switch.

20.1.4 Configuration process on destination switch

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **vlan** *vlan-id*	Enter Vlan configuration mode.
DES-7210(config-Vlan)# **remote-span**	Set Vlan as remote-span Vlan.
DES-7210(config-Vlan)# **exit**	Return to the global configuration mode.
DES-7210(config)# **monitor session** *session_num* **remote-destination**	Configure remote destination mirror.
DES-7210(config)# **monitor session** *session-num* **destination remote vlan** *vlan-id* **interface** *interface-name* **[switch]**	Configure Remote VLAN and remote mirrored destination port.
DES-7210(config)# **interface** *interface-name*	Enter the remote mirrorred destination port.
DES-7210(config-if)# { **switchport access vlan** *vid* | **switchport trunk native vlan** *vid* }	*Vid:* VID for remote-span vlan. If the destination port is acess port, join the destination port to remote-span vlan; If the destination port is trunk port, join the destination port to remote-span vlan and set the remote-span vlan as the native vlan for the destination port.

20.2 Showing RSPAN Session

Command	Function
DES-7210# **show monitor**	Show the mirror.

For example:

```
DES-7210# show monitor
sess-num: 1
src-intf:
GigabitEthernet 0/4 frame-type Both
dest-intf:
GigabitEthernet 0/6
remote vlan 3
```

20.3 Examples

Device topology is shown as the following figure:

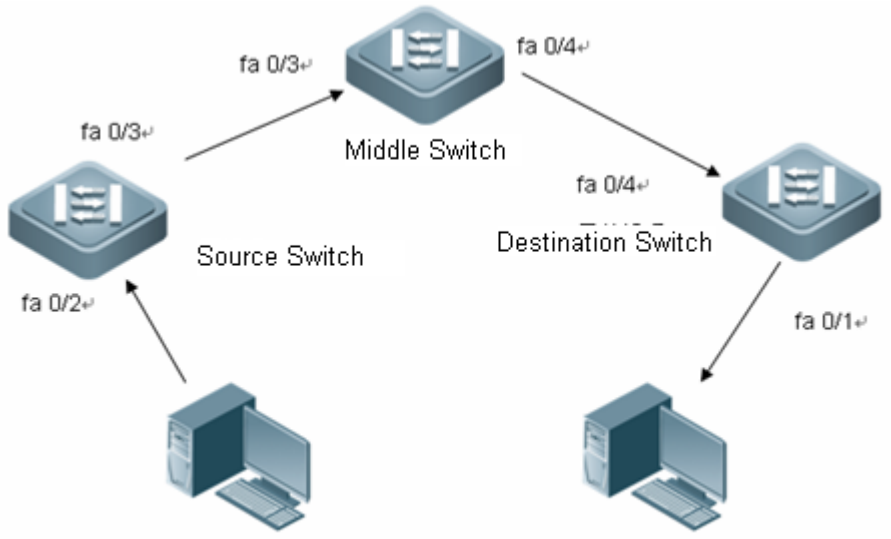


Figure 2

Source switch configuration:

```
DES-7210# configure
DES-7210(config)# Vlan 7
DES-7210(config-Vlan)# remote-span
DES-7210(config-Vlan)# exit
DES-7210(config)#Interface fastEthernet 0/3
DES-7210(config-if)#switchport mode trunk
DES-7210(config-if)#switchport trunk allowed vlan add 7
DES-7210(config-if)# exit
DES-7210(config)# monitor session 2 remote-source
```

```
DES-7210(config)# monitor session 2 source interface fastEthernet 0/2
```

(For the switches do not support the reflector port)

```
DES-7210(config)#monitor session 2 destination remote vlan 7 interface fastEthernet 0/3
switch
```

(For the switches support the reflector port)

```
DES-7210(config)#Interface fastEthernet 0/1

DES-7210(config-if)#switchport access vlan 7

DES-7210(config)#monitor session 2 destination remote vlan 7 reflector-port interface
fastEthernet 0/1 switch
```

Middle switch configuration:

```
DES-7210# configure
DES-7210(config)# Vlan 7
DES-7210(config-Vlan)# remote-span
DES-7210(config-Vlan)# exit
DES-7210(config)#Interface fastEthernet 0/3
DES-7210(config-if)#switchport mode trunk
DES-7210(config-if)#switchport trunk allowed vlan add 7
DES-7210(config-if)#exit
DES-7210(config)#Interface  fastEthernet 0/4
DES-7210(config-if)#switchport mode trunk
DES-7210(config-if)#switchport trunk allowed vlan add 7
```

Destination switch configuration:

```
DES-7210# configure
DES-7210(config)# Vlan 7
DES-7210(config-Vlan)# remote-span
DES-7210(config-Vlan)# exit
DES-7210(config)#Interface fastEthernet 0/4
DES-7210(config-if)#switchport mode trunk
DES-7210(config-if)#switchport trunk allowed vlan add 7
DES-7210(config-if)# exit
DES-7210(config)# monitor session 2 remote- destination
DES-7210(config)#monitor session 2 destination remote vlan 7 interface fastEthernet 0/1
switch
```

21 IP Address and Service Configuration

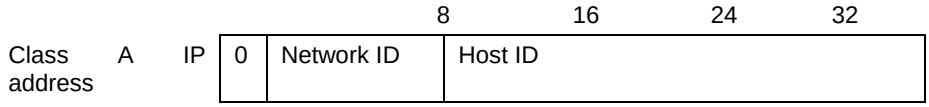
21.1 IP Address Configuration

21.1.1 IP Address Overview

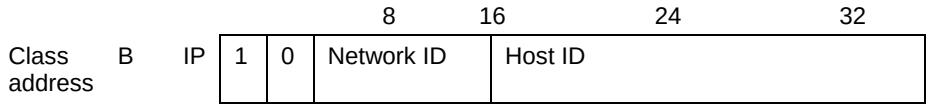
IP address is made up of 32 binary bits and expressed in the dotted decimal format for the convenience of writing and description. In the dotted decimal format, the 32 binary bits are broken into four octets (1 octet equals to 8 bits). Each octet is separated by a period (dot) in the range from 0 to 255. For example, 192.168.1.1 is an IP address in the dotted decimal format.

An IP address is an address that IP protocols use to connect one another. A 32-bit IP address consists of two parts: network address and local address. According to the first several bits of the network address of an IP address, an IP address is divided into four categories.

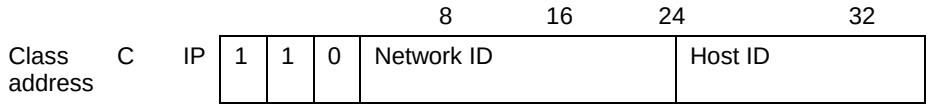
Class A: Total of 128 class-A IP addresses. The highest bit is 0 followed by seven bits identifying Network ID, and the remaining 24 bits identify Host ID.



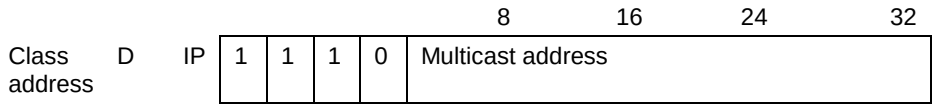
Class B: Total of 16,384 class B IP addresses. The highest two bits are 10 followed by 14 bits identifying Network ID, and the remaining 16 bits identify Host ID.



Class C: Totaol of 2,097,152 class C IP addresses. The highest three bits are 110 followed by 21 bits identifying Network ID, and the remaining eight addresses identify Host ID.



Class D: The highest four bits are 1110 and other bits are multicast IP address..



Note

An IP address whose highest four bits are 1111 is prohibited. This type of IP address, also called Class E IP address, is reserved.

When you build up a network, you should execute IP addressing according to the real network environment. To make the network connect to the Internet, you need apply for IP addresses from a central authority, for example, the China Internet Network Information Center (CNNIC) in China. It is the Internet Corporation for Assigned Names and Numbers (ICANN) that is responsible for IP address allocation. However, a private network does not require the application of IP addresses. It is recommended to assign private IP addresses for them.

The following table lists those reserved and available addresses by class.

Class	Address Range	Status
Class A	0.0.0.0	Reserved
	1.0.0.0 to 126.0.0.0	Available
	127.0.0.0	Reserved
Class B	128.0.0.0 to191.254.0.0	Available
	191.255.0.0	Reserved
Class C	192.0.0.0	Reserved
	192.0.1.0 to 223.255.254.0	Available
	223.255.255.0	Reserved
Class D	224.0.0.0 to 239.255.255.255	Available
Class E	240.0.0.0 to 255.255.255.254	Reserved
	255.255.255.255	Multicast

There are three blocks of IP addresses reserved for private networks that are not used in the Internet. Address translation is required for a private network using one of these IP addresses to access the Internet. The following table details these addresses, which are defined in RFC 1918.

Class	IP Address Range	Network Numbers
Class A	10.0.0.0 to 10.255.255.255	1
Class B	172.16.0.0 to 172.31.255.255	16
Class C	192.168.0.0 to 192.168.255.255	256

For the information on the assignment of IP address, TCP/UDP port and other codes, please refer to RFC 1166.

21.1.2 IP Address Configuration Task List

The IP address configuration task list includes the following tasks, only the first one is required, others are optional depending on your network requirements.

- Assigning IP Addresses to Network Interfaces (Required)
- Configuring Address Resolution Protocol (ARP) (Optional)
- Configuring IP address to WAN Address Translation (Optional)
- Disabling IP Routing (Optional)
- Handling Broadcast Packets (Optional)

21.1.2.1 Assigning IP Addresses to Network Interfaces

Only a host has an IP address configured can it receive and send IP packets. If an interface is configured with an IP address, this means that the interface supports running the IP protocol.

To assign an IP address to an interface, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip address** *ip-address mask*	Assign an IP address for the interface.
DES-7210(config-if)# **no ip address**	Remove the IP address configuration for the interface.

A 32-bit mask identifies the network part of an IP address. In a mask, the IP address bit corresponding to 1 represetns network ID and the IP address bit corresponding to 0 represents host ID. For example, the mask corresponding a Class A IP address is 255.0.0.0. You can partition a network into multiple segments with a mask. The goal of network partition is to use some bits of the host address of an IP address as the network address to reduce hosts and increase networks. At this point, the mask is called subnet mask.

Note Theoretically, any bit of the host address of an IP address can be used as the subnet mask. The DES-7200 series only supports continuous subnet masks from left to right starting from the network ID.

The interface-related IP address configuration task list includes the following tasks, only the first one is required, others are optional depending on your network requirements.

- Assigning multiple IP addresses to an interface

1.1.2.1.1 Assigning multiple IP addresses to an interface

The DES-7200 series supports assigning multiple IP addresses for an interface with one being the primary IP address and others being the secondary addresses. Theoretically, you can configure secondary addresses up your mind. A secondary IP address can reside in the same or different network with the primary IP address. The secondary IP address will be used frequently during the building of a network, for example, in the following cases:

- There may not enough host addresses for a network. For example, a LAN requires a Class C IP address to support up to 254 hosts. However, when there are more than 254 hosts in the LAN, another Class C IP address is necessary. Therefore, a host needs to connect two networks and thus needs configuring multiple IP addresses.
- Many older networks were built based on layer 2 bridges without partition. The use of secondary IP addresses makes them easy to upgrade to IP-based routing networks. An IP address is assigned for every device in a subnet.
- Two subnets of a network might otherwise be separated by another network. By creating a subnet in each separated subnets, you can connect the two separated subnets together by assigning secondary IP addresses. One subnet cannot appear on two or more interfaces in a device.

Note Before configuring secondary IP addresses, you need to confirm that the primary IP address has been configured. All the devices in a network should have the same secondary IP address. If you assign a secondary IP address to a device but do not assign IP addresses for other devices, you can set it to the primary IP address for them.

To assign a secondary IP address to an interface, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip address** *ip-address mask* **secondary**	Assign a secondary IP address to the interface.
DES-7210(config-if)# **no ip address** *ip-address mask* **secondary**	Remove the secondary IP address configuration for the interface.

21.1.2.2 Configuring Address Resolution Protocol (ARP)

Every device in a LAN has two addresses: local address and network address. Local address is contained in the header of the frames on the data link layer. Disputably, the correct term is data link layer address. Since this local address is handled in the MAC sub-layer of the data link layer, it is normally called MAC address representing an IP network device in a network. Network address represents a device in the Internet and indicates the network to which the device belongs.

For inter-communication, a device in a LAN must know the 48-bit MAC address of another device. The ARP can resolve the MAC address upon an IP address and the reversed ARP (RARP) can resolve the IP address upon a MAC address. You can resolve the MAC address in two ways: ARP and Proxy ARP. For the information on ARP, Proxy ARP and RARP, refer to RFC 826, RFC 1027, and RFC 903.

ARP binds the IP and MAC Address. It can resolve the MAC address upon an IP address. Then, the relationship between the IP address and the MAC address is stored in the ARP cache. With the MAC address, a device can encapsulate the frames of the data link layer and send them to the LAN in the Ethernet II-type by default. However the frames can also be encapsulated into other types of Ethernet frame (for example, SNAP).

The principle of RARP is similar to ARP. RARP resolves the IPaddress upon a MAC address. RARP is configured on non-disk workstation in general.

Normally, a device can work without any special address resolution configuration. DES-7210 product can manage address resolution by.

- Configuring ARP Statically
- Setting ARP Encapsulations
- Setting ARP Timeout

1.1.2.2.1 Configuring ARP Statically

The ARP offers dynamic IP address to MAC address mapping. It is not necessary to configure ARP statically in most cases. By configuring ARP Sstatically, DES-7210 product can respond to the ARP request from other IP addresses.

To configure static ARP, execute the following command in the global configuration mode:

Command	Function
DES-7210(config)# **arp** *ip-address mac-address arp-type*	Define static ARP. Only arpa type is supported for arp-type.
DES-7210(config)# **no arp** *ip-address*	Remove static ARP

1.1.2.2.2 Setting ARP Encapsulations

So far the DES-7200 series only supports Ethernet II type ARP encapsulations, also known as ARPA keyword.

1.1.2.2.3 ARP Timeout Setting

ARP timeout takes effect for only the dynamically learned IP address to MAC address mapping. The shorter the timeout, the truer the mapping table saved in the ARP cache is , but the more network bandwidth the ARP occupies. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout time unless there is a special requirement.

To configure ARP timeout time, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **arp timeout** *seconds*	Configure the ARP timeout time in the range from 0 to 2147483, with 0 not being aged.
DES-7210(config-if)# **no arp timeout**	Remove the configuration.

By default, timeout time is 3600 seconds, that is, 1 hour.

21.1.2.3 Disabling IP Routing

IP routing feature is enabled by default. Do not execute this command unless you sure that IP routing is not needed. Disabling IP routing will make the equipment lose all the routes and the route forwarding function.

To disable IP routing, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **no ip routing**	Disable IP routing.
DES-7210(config)# **ip routing**	Enable IP routing

Note

The switch performs the checking of ip checksum towards the routing packets. If the ip checksum error occurs, the routing halts. To this end, the unicast packets will be discarded directly and the multicast packets will only be forwarded on Layer 2.

21.1.2.4 Handling Broadcast Packets

A broadcast packet is destined for all hosts in a physical network. DES-7210 product supports two kinds of broadcast packets: directed broadcast and flooding. A directed broadcast packet is sent to all the hosts in a specific network that the host IDs of their IP addresses are all set to 1. While a flooding broadcast packet is sent to all the hosts whose IP addresses are all set to 1. Broadcast packets are heavily used by some protocols, including the Internet protocol. Therefore, it is the basic responsibility for a network administrator to manage and control broadcast packets.

Forwarding flooding broadcast packets may make the network overburden and thus influencing network operation. This is known as broadcast storm. There are some ways to supress and restrict broadcast storm in the local network. However, layer 2 network devices like bridges and switches will forward and propagate broadcast storm.

The best solution to solve the broadcast storm problem is to specify a broadcast address for each network, that is, directed broadcast. This requires the IP protocol to use directed broadcast instead of flooding broadcast if possible.

For detailed description about broadcast, refer to RFC 919 and RFC 922.

To handle broadcast packets, perform the following tasks according to the network requirement.

- Enabling Directed Broadcast-to-Physical Broadcast Translation
- Establishing an IP Broadcast Address

20.1.2.4.1 Enabling Directed Broadcast-to-Physical Broadcast Translation

A directed broadcast IP packet is the one destined to the broadcast address of an IP subnet. For instance, the packet destined to 172.16.16.255 is a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

Upon the receipt of directed broadcast IP packets, the device indirectly connecting the destination subnet will forward the packets in the same way as forwarding unicast packets. After the directed broadcast IP packets arrive the device directly connecting the subnet, the device transforms them into flooding broadcast IP packets (whose destination address is all 1s in general), and then send them to all the hosts within the subnet by means of broadcast on the link layer.

Enabling directed broadcast to physical broadcast translation on an interface allows the itnerface to forward the directed broadcast IP packets to the directly connected network. This command will only affect the transmission of the directed broadcast IP packets to the final destination subnet, not other directed broadcasts.

You can forward directed broadcast IP packets as required an interface by defining ACLs. Only those IP packets matching the ACLs are translated from directed broadcasts to physical broadcasts.

To configure the directed broadcast-to-physical broadcast translation, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip directed-broadcast** [*access-list-number*]	Enable directed broadcast to physical broadcast translation on the interface.
DES-7210(config-if)# **no ip directed-broadcast**	Disable the translation.

20.1.2.4.2 Establishing an IP Broadcast Address

Currently, the most popular way is the destination address consisting of all 1s (255.255.255.255). DES-7210 product can be configured to generate any form of IP broadcast address and receive any form of IP broadcast packets.

To set a broadcast IP address other than 255.255.255.255, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip broadcast-address** *ip-address*	Create a broadcast address.
DES-7210(config-if)# **no ip broadcast-address**	Remove the configuration.

21.1.3 Monitoring and Maintaining IP Address

To monitor and maintain your network, perform the tasks described in the following sections.

- Clearing Caches and Tables
- Displaying System and Network Status

21.1.3.1 Clearing Caches and Tables

You can remove all contents of a particular cache, table, or database, including: 1) Clearing ARP cache;

2) Clearing the hostname to IP address mapping table;

3) Clearing the routing tables.

Command	Function
DES-7210# **clear arp-cache**	Clear the ARP cache.
DES-7210# **clear ip route** {*network* [*mask*] | *}	Clear the routing table.

21.1.3.2 Displaying System and Network Status

You can show the contents of the IP routing table, cache, and database. Such information is very helpful in troubleshooting the network. You also can display information about reachability of local network and discover the routing path that the packets of your device are taking through the network.

To display system and network status, execute the following commands in the privileged mode :

Command	Function
DES-7210# **show arp**	Show the ARP table.
DES-7210# **show ip arp**	Show the IP ARP table.
DES-7210# **show ip interface** [*interface-type interface-number*]	Show the interface information.
DES-7210# **show ip route** [*network* [*mask*]]	Show the routing table.
DES-7210#**show ip route**	Show the brief information of the routing table.
DES-7210# **ping** *ip-address* [**length** *bytes*] [**ntimes** *times*] [**timeout** *seconds*]	Test network reachability.

21.1.4 IP Address Configuration Examples

This chapter provides some IP address configuration examples as follows:

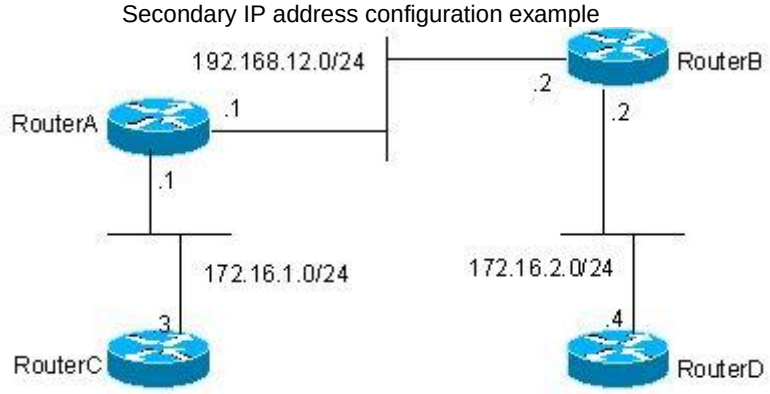
- Secondary IP Address Configuration Example

21.1.4.1 Secondary IP Address Configuration Example

Configuration requirements:

The following figure shows IP address assignment and network device connection.

Secondary IP address configuration example



Configure RIPv1. You can see the routes of 172.16.2.0/24 on router C and the routes of 172.16.1.0/24 on router D.

Configuration of the Routers:

RIPv1 does not support classless-based routes. This means masks are not carried with routing advertisement. 172.16.1.0/24 and 172.16.2.0/24 that belong to the same netowrk are separated by the Class C network 192.168.12.0/2. Generally, router C and router D cannot routes from each other. According to one feature of RIP, the mask of the route to be received should be set to the same value as that of the interface network if the route and the interface network belong to the same network. By configuring routers A and B, you can build a secondary netowrk 172.16.3.0/24 on the network 192.168.12.0/24 to link the two separated subnets. The following presents a configuraiton description of routers A and B.

Router A:

```
interface FastEthernet 0/0
ip address 172.16.3.1 255.255.255.0 secondary
ip address 192.168.12.1 255.255.255.0
!
interface FastEthernet 0/1
ip address 172.16.1.1 255.255.255.0
!
router rip
network 172.16.0.0
network 192.168.12.0
```

Router B:

```
interface FastEthernet 0/0
ip address 172.16.3.2 255.255.255.0 secondary
ip address 192.168.12.2 255.255.255.0
!
interface FastEthernet 0/1
ip address 172.16.2.1 255.255.255.0
!
router rip
network 172.16.0.0
network 192.168.12.0
```

21.2 IP Service Configuration

21.2.1 IP Service Configuration Task List

The IP service configuration includes the following optional configuration tasks. You can perform the task according to the requirements:

- Configuring the default gateway
- Managing IP connections

21.2.2 Configuring the Default Gateway

If no destination IP address to which the packets will be sent is specified, those packets will be sent to the default gateway by default. Use the **show ip redirects** command to view the settings.

To set the default gateway, execute the following command in the global configuration mode. Use the **no** form of this command to remove the default gateway:

Command	Function
ip default-gateway *ip-address*	Disable the ICMP protocol unreachable and host unreachable messages.

To view the configured default gateway, execute the following command:

Command	Function
show ip redirects	Display the default gateway.

This command is supported only for the L2 switches.

21.2.3 Managing IP Connections

The IP protocol stack offers a number of services to control and manage IP connections. Internet Control Message Protocol (ICMP) provides many of these services. Once a network problem occurs, a router or access server will send an ICMP message to the host or other rotuers. For detailed information on ICMP, see RFC 792.

To manage various aspects of IP connections, perform the optional tasks described in the following sections:

- Enabling ICMP Protocol Unreachable Messages
- Enabling ICMP Redirect Messages
- Enabling ICMP Mask Reply Messages
- Setting the IP MTU
- Configuring IP Source Routing

21.2.3.1 Enabling the ICMP Protocol Unreachable Message

When a router receives a non-broadcast packet destined to it, and this packet uses an IP protocol that it cannot handle, it will return an ICMP protocol unreachable message to the source address. Similarly, if the router is unable to forward the packet because it knows of no route to the destination address, it sends an ICMP host unreachable message. This feature is enabled by default.

To enable this service, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip unreachables**	Enable the ICMP protocol unreachable and host unreachable messages.
DES-7210(config-if)# **no ip unreachables**	Disable the ICMP protocol unreachable and host unreachable messages.

21.2.3.2 Enabling the ICMP Redirect Message

Routes are sometimes less than optimal. For example, it is possible for the device to be forced to resend a packet through the same interface on which it was received. If the device resends a packet through the same interface on which it was received, it sends an ICMP redirect message to the originator of the packet telling the originator that the gateway to this destination address is another device in the same subnet. Therefore the originator will transmit the packets based on the optimized path afterwards. This feature is enabled by default.

To enable the ICMP redirect message, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip redirects**	Enable the ICMP redirect message. It is enabled by default.
DES-7210(config-if)# **no ip redirects**	Disable the ICMP redirect message.

21.2.3.3 Enabling the ICMP Mask Reply Message

Occasionally, a network device needs to know the mask of a subnetwork in the Internet. To obtain this information, the device can send the ICMP mask request message. The receiving device will send the ICMP mask reply message. The DES-7200 series can respond the ICMP mask request message. This function is enabled by default.

To enable the ICMP mask reply message, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip mask-reply**	Enable the ICMP mask reply message.
DES-7210(config-if)# **no ip mask-reply**	Disable the ICMP mask reply message.

21.2.3.4 Setting the IP MTU

All interfaces have a default MTU (Maximum Transmission Unit) value. All the packets which are larger than the MTU have to be fragmented before sending. Otherwise it is unable to be forwarded on the interface.

The DES-7200 series allows you to adjust the MTU on an interface. Changing the MTU value can affect the IP MTU value, and the IP MTU value will be modified automatically to match the new MTU. However, changing the IP MTU value has no effect on the value of MTU.

The interfaces of a device in a physical network should have the same MTU for a protocol.

To set the IP MTU, execute the following command in the interface configuration mode:

Command	Function

Command	Function
DES-7210(config-if)# **ip mtu** *bytes*	Set the MTU in the range 68 to 1500 bytes.
DES-7210(config-if)# **no ip mtu**	Restore the setting to the default.

21.2.3.5 Configuring IP Source Routing

The DES-7200 series supports IP source routing. Upon receiving an IP packet, the device will check its IP header like strict source route, loose source route and recorded route, which are defined in RFC 791. If one of these options is enabled, the device performs appropriate action. Otherwise, it sends an ICMP error message to the source and then discards the packet. Our product supports IP source routing by default.

To enable IP source routing, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config)# **ip source-route**	Enable IP source routing.
DES-7210(config)# **no ip source-route**	Disable IP source routing.

Note

For the DES-7200 series, due to the limitation of the hardware chip, the command **trap ip option packet** shall be used to notify the hardware of sending the packets with optional items to the software for handling.

22 DHCP Configuration

22.1 Introduction to DHCP

The DHCP (Dynamic Host Configuration Protocol), specified in RFC 2131, provides configuration parameters for hosts over the Internet. The DHCP works in the client/server mode. The DHCP server assigns IP addresses for the hosts dynamically and provides configuration parameters.

The DHCP assigns IP address in three ways:

1. Assign IP addresses automatically. The DHCP server assigns permanent IP addresses to the clients;

2. Assign IP addresses dynamically. The DHCP server assigns IP addresses that will expire after a period of time to the clients (or the clients can release the addresses by themselves);

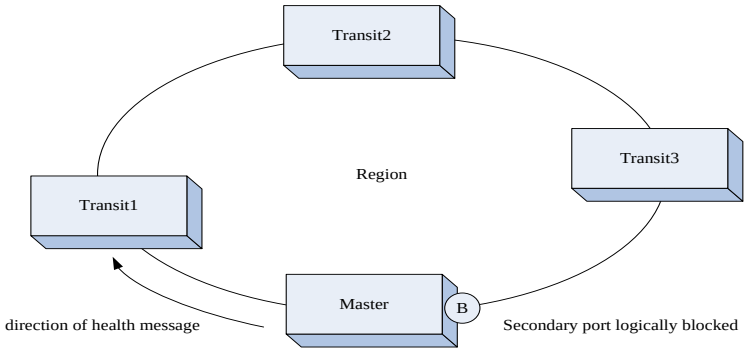
3. Configure IP addresses manually. Network administrators specify IP addresses and send the specified IP addresses to the clients through the DHCP.

Among the above mentioned three methods, only dynamic assignment allows reuse of the IP address that the client does not need any more.

The format of DHCP message is based on that of BOOTP (Bootstrap Protocol) message. Hence, it is necessary for the device to be able to act as the BOOTP relay agent and interact with the BOOTP client and the DHCP server. The function of BOOTP relay agent eliminates the need of deploying a DHCP server in every physical network. The DHCP is detailed in RFC 951 and RFC 1542.

22.2 Introduction to the DHCP Server

As specified in RFC2131, the DHCP server of DES-7210 is implemented to assign and manage IP addresses for the DHCP clients. The DHCP operation process is shown in the following figure.



Process of requesting an IP address:

1. The host broadcasts a DHCPDISCOVER packet in the network to locate the DHCP server;

2. The DHCP server sends a DHCPOFFER packet in unicast form to the host, including IP address, MAC address, domain name and address lease period;

3. The host sends a DHCPREQUEST packet in broadcast form to formally request the server to assign the provided IP address;

4. The DHCP server sends a DHCPACK packet in unicast form to the host to confirm the request.

Note

The DHCP client may receive the DHCPOFFER packets from multiple DHCP servers, and accept any DHCPOFFER packet. However, the DHCP client usually accepts the first received DHCPOFFER packet only. The address specified in the DHCPOFFER packet from the DHCP server is not necessarily the finally assigned address. Generally, the DHCP server reserves this address until the client sends a formal request.

The goal of broadcasting the DHCPREQUEST packet is to let all the DHCP servers that send the DHCPOFFER packet receive this packet and then release the IP address specified in the DHCPOFFER packet.

If the DHCPOFFER packet sent to the DHCP client contains invalid parameters, the DHCP client sends the DHCPDECLINE packet to refuse the assigned configuration.

During negotiation, if the DHCP client does not respond to the DHCPOFFER packet in time, the DHCP server will send the DHCPNAK packet to the DHCP client, initiating the address request process again.

The advantages of using the DHCP server of DES-7210 for network construction are:

- Decrease network access cost. Generally, dynamic address assignment costs less than static address assignment.
- Simplify configuration tasks and reduce network construction cost. Dynamic address assignment significantly simplifies equipment configuration, and even reduces deployment cost if devices are deployed in the places where there are no professionals.
- Centralized management. During configuration management on several subnets, any configuration parameter can be changed simply by modifying and updating configurations in the DHCP server.

22.3 Introduction to the DHCP Client

The DHCP client can obtain IP addresses and other configuration parameters from the DHCP server automatically. The DHCP client brings the following advantages:

- Save device configuration and deployment time.
- Reduce the possibility of configuration errors.
- Centrally manage IP address assignment.

Caution

The DHCP Client are supported on the Ethernet interface, FR, PPP, HDLC interfaces.

22.4 Introduction to the DHCP Relay Agent

The DHCP relay agent forwards DHCP packets between the DHCP server and the DHCP clients. When the DHCP clients and the server are not located in the same subnet, a DHCP

relay agent must be available for forwarding the DHCP request and response messages. Data forwarding by the DHCP relay agent is different from general forwarding. In general forwarding, IP packets are unaltered and the transmission is transparent. However, upon receiving a DHCP message, the DHCP relay agent regenerates and forwards a DHCP message.

From the perspective of the DHCP client, the DHCP relay agent works like a DHCP server. From the perspective of the DHCP server, the DHCP relay agent works like a DHCP client.

22.5 Configuring DHCP

To configure DHCP, perform the following tasks, of which the first three tasks are mandatory.

- Enabling the DHCP Server and the DHCP Relay Agent (required)
- Configuring DHCP Excluded Addresses (required)
- Configuring DHCP Address Pool (required)
- Binding Address Manually (optional)
- Configuring the Ping Times (optional)
- Configuring Ping Packet Timeout (optional)
- Ethernet interface DHCP client configuration (optional)
- DHCP Client Configuration in PPP Encapsulation link (optional)
- DHCP Client Configuration in FR Encapsulation link (optional)
- DHCP Client Configuration in HDLC Encapsulation link (optional)

22.5.1 Enabling the DHCP Server and the DHCP Relay Agent

To enable the DHCP server and the DHCP relay agent, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **service dhcp**	Enable the DHCP server and the DHCP relay agent.
DES-7210(config)# **no service dhcp**	Disable the DHCP server and the DHCP relay agent.

Note

By default, in v10.1 and later, the command **service dhcp** can be used for both DHCP server and DHCP relay, which are two mutually-exclusive functions. The switchover of those two functions depends on whether the DHCP address pool is configured or not.

However, for the product in the version prior to v10.1(excluding v10.1), the command **service dhcp** is not supported by both DHCP server and DHCP relay. You can use the command **service dhcp** to enable the DHCP service or the DHCP server.

For some product in v10.1 and later, DHCP may conflict with some functions. For the details, see the prompting message of specific product.

22.5.2 Configuring DHCP Excluded Addresses

Unless configured particularly, the DHCP server tries to assign all the subnet addresses defined in the address pool to the DHCP clients. If you want to reserve some addresses,

such as those that have been assigned to servers or devices, you must define clearly that these addresses cannot be assigned to the DHCP clients.

To configure the addresses that cannot be assigned to the DHCP clients, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip dhcp excluded-address low-ip-address** [**high-ip-address**]	Define a range of IP addresses that the DHCP server will not assign to the DHCP clients.
DES-7210(config)# **no ip dhcp excluded-address low-ip-address** [**high-ip-address**]	Remove the configuration.

A good practice in configuring the DHCP server is to prohibit the DHCP server from assigning any address that has been assigned specifically. This provides two advantages: 1) No address conflict will occur; 2) When DHCP assigns addresses, the time for detection is shortened and thus DHCP will perform assignment more efficiently.

22.5.3 Configuring DHCP Address Pool

Both DHCP Address assignment and DHCP parameters sent to the client should be defined in the DHCP address pool. If no DHCP address pool is configured, addresses cannot be assigned to the DHCP clients even though the DHCP server has been enabled. However, if the DHCP server has been enabled, the DHCP relay agent is always working regardless of the DHCP address pool.

You can give a meaningful name that can be memorized easily to the DHCP address pool. The name of address pool contains characters and digits. DES-7210 product allows you to define multiple address pools. The IP address of the DHCP relay agent in the DHCP request packet is used to determine which address pool is used for address assignment.

- If the DHCP request packet does not contain the IP address of the DHCP relay agent, the address that is in the same subnet or network as the IP address of the interface that receives the DHCP request packet is assigned to the DHCP client. If no address pool is defined for this network segment, address assignment fails.
- If the DHCP request packet contains the IP address of the DHCP relay agent, the address that is in the same subnet or network as this address is assigned to the DHCP client. If no address pool is defined for this network segment, address assignment fails.

To configure a DHCP address pool, perform the following tasks as appropriate, of which the first three tasks are mandatory:

- Configure an address pool name and enter its configuration mode (required)
- Configure a subnet and its mask for the address pool (required)
- Configure the default gateway for the DHCP client (required)
- Configure the address lease period (optional)
- Configure the domain name of the DHCP client (optional)
- Configuring the domain name server (optional)
- Configure the NetBIOS WINS server (optional)
- Configure the NetBIOS node type for the DHCP client (optional)

22.5.3.1 Configuring an Address Pool Name and Enter Its Configuration Mode

To configure an address pool name and enter the address pool configuration mode, execute the following command in the global configuration mode:

Command	Function
DES-7210(config)# **ip dhcp pool** *dhcp-pool*	Configuring an address pool name and enter the address pool configuration mode

The address pool configuration mode is shown as “DES-7210(dhcp-config)#”.

22.5.3.2 Configuring the Boot File for the DHCP Client

The boot image file is the one used when the client starts. The boot image file is often the operation system to be downloaded by the DHCP client.

To configure the boot file for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7210 (dhcp-config)# **bootfile** *filename*	Configure the name of the boot file for the DHCP client.

22.5.3.3 Configuring the Default Gateway for the DHCP Client

The IP address of the default gateway must be in the same network as the IP address of the DHCP client.

To configure the default gateway for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7210(dhcp-config)# **default-router** *address* [*address2…address8*]	Configure the default gateway.

22.5.3.4 Configuring the Address Lease Period

The lease for the address that the DHCP server assigns to the client is one day by default. The client should request to renew when the lease period is going to expire. Otherwise, it cannot use this address when the lease period expires.

To configure the address lease period, execute the following command in the address pool configuration mode:

Command	Function
DES-7210(dhcp-config)# **lease** {*days* [*hours*] [*minutes*] | **infinite**}	Configure the address lease period.

22.5.3.5 Configuring the Domain Name of the DHCP Client

The domain name of the DHCP client can be specified. In this way, the domain name suffix will be automatically added to the incomplete host name to form a complete host name when the DHCP client accesses the network resources using the host name.

To configure the domain name of the DHCP client, execute the following command in the address pool configuration mode:

Command	Function

Command	Function
DES-7210(dhcp-config)# **domain-name** *domain*	Configure the domain name.

22.5.3.6 Configuring the Domain Name Server

A DNS server should be specified for domain name resolution when the DHCP client accesses the network resources using a host name.

To configure a domain name server for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7210(dhcp-config)# **dns-server** *address* [*address2…address8*]	Configure a DNS server.

22.5.3.7 Configuring the NetBIOS WINS Server

WINS is a domain name resolution service from Microsoft that the TCP/IP network uses to resolve a NetNBIOS name to an IP addresses. The WINS server runs in Windows NT. After started, the WINS server will receive a registration request from the WINS client. When the WINS client is being shut down, it will send a name release message to the WINS server to guarantee the consistency of available computers between the WINS database and the network.

To configure a NetBIOS WINS server for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7210(dhcp-config)# **netbios-name-server** *address* [*address2…address8*]	Configure a DNS server.

22.5.3.8 Configuring the NetBIOS Node Type for the DHCP Client

There are four types of NetBIOS nodes for Microsoft DHCP client:

1. Broadcast. The NetBIOS name is resolved in the broadcast mode;
2. Peer-to-peer. The WINS server is asked directly to resolve the NetBIOS name;
3. Mixed. First, the name is resolved in the broadcast mode, and then the WINS server is connected to resolve the name;
4. Hybrid. First the WINS server is asked directly to resolve the NetBIOS name. If there is no response, the NetBIOS name is resolved in the broadcast mode.

By default, the Windows operation systems support broadcast or hybrid type NetBIOS nodes. If no WINS server is configured, the node is of broadcast type. If a WINS server is configured, the node is of hybrid type.

To configure the NetBIOS node type for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7210(dhcp-config)# **netbios-node-type** *type*	Configure the NetBIOS node type.

22.5.3.9 Configuring the Network Number and Mask of the DHCP Address Pool

To configure dynamic address binding, you must configure the subnet and its mask for the new address pool. A DHCP address pool provides the DHCP server with an address space that can be assigned to clients. All the addresses in the address pool are available for the DHCP clients unless address exclusion is configured. The DHCP server assigns the addresses in the address pool in sequence. If an address already exists in the binding table or this address is detected to be already present in this network segment, the DHCP server will check the next address until it assigns a valid address.

To configure the subnet and its mask of the DHCP address pool, execute the following commands in the address pool configuration mode:

Command	Function
DES-7210(dhcp-config)# **network** *network-number mask*	Configure the network number and mask of the DHCP address pool.

Caution

For the DHCP dynamic address pool of DES-7210 products, addresses are assigned based on the physical address and ID of a DHCP client. This means there should not be two leases for the same DHCP client in the DHCP dynamic address pool. If path redundancy occurs between the DHCP client and the DHCP server (the DHCP client can reach the DHCP server by the direct path or relay path), the DHCP server may fail to assign addresses.

To solve this problem, administrators should avoid path redundancy between the DHCP clients and the DHCP sever in other ways like adjusting physical links or network paths.

22.5.4 Manual Address Binding

Address binding refers to the IP address to MAC address mapping for the DHCP clients. You can bind addresses in two ways.

- Manual binding: Configure the static IP address to MAC address mapping for the DHCP client on the DHCP server manually. Manual binding actually offers a special address pool;
- Dynamic binding: Upon receiving a DHCP request from the DHCP client, the DHCP server dynamically assigns an IP address from the DHCP address pool to the DHCP client, and thus mapping the IP address to the MAC address for the DHCP client.

To define manual address binding, you first need to define a host address pool for each manual binding, and then define the IP address and hardware address (MAC address) or ID for the DHCP client. Generally, a client ID instead of a MAC address, is defined for the Microsoft clients. The client ID contains media type and MAC address. For the codes of media types, refer to Address Resolution Protocol Parameters in RFC 1700. The code of Ethernet type is “01”.

To configure the manual address binding, execute the following commands in the address pool configuration mode:

Command	Function
DES-7210(config)# **ip dhcp pool** *name*	Define the name of the DHCP address pool and enter the DHCP configuration mode.
DES-7210(dhcp-config)# **host** *address*	Define an IP address for the DHCP client.

Command	Function
DES-7210(dhcp-config)# **hardware-address** *hardware-address type* DES-7210(dhcp-config)# **client-identifier** unique-identifier	Define a hardware address for the DHCP client, such as aabb.bbbb.bb88 Define an ID for the DHCP client, such as 01aa.bbbb.bbbb.88
DES-7210(dhcp-config)# **client-name** *name*	(Optional) Define the client name using standard ASCII characters. Don't include domain name in the client name. For example, if you define the mary host name, do not define as mary.rg.com

22.5.5 Configuring Ping Times

By default, when trying to assign an IP address from the DHCP address pool to a DHCP client , the DHCP server will ping the IP address twice (one packet for each time). If there is no response, the DHCP server considers this address an idle address and assigns it to the DHCP client. If there is a response, the DHCP server considers that this address is in use and tries to assign another address to the DHCP client until an address is assigned successfully.

To configure the number of Ping packets, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip dhcp ping** *packets number*	Configure the number of Ping packets before the DHCP server assigns an address. If it is set to 0, the Ping operation is not performed. The default value is 2.

22.5.6 Configuring Ping Packet Timeout

By default, the DHCP server considers the IP address inexistent if it has not received a response within 500 milliseconds after pinging an IP address. You can adjust the Ping packet timeout.

To configure the Ping packet timeout, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip dhcp ping timeout** *milliseconds*	Configure the Ping packet timeout for the DHCP server. The default value is 500ms.

22.5.7 Configuring the DHCP Client on the Ethernet Interface

DES-7210 products support obtaining the IP address dynamicaly assigned by the DHCP server on an Ethernet interface.

To configure the DHCP client on the Ethernet port, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip address dhcp**	Obtain an IP address through DHCP.

22.5.8 Configuring the DHCP Client in the PPP Encapsulation Link

DES-7210 products support obtaining the IP address dynamicaly assigned by the DHCP server on a PPP encapsulation interface.

To configure the DHCP client, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip address dhcp**	Obtain an IP address through DHCP.

22.5.9 Configuring the DHCP Client in the FR Encapsulation Link

DES-7210 products support obtaining the IP address dynamicaly assigned by the DHCP server on an FR encapsulation interface.

To configure the DHCP client, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip address dhcp**	Obtain an IP address through DHCP.

22.5.10 Configuring the DHCP Client in the HDLCEncapsulation Link

DES-7210 products support obtaining the IP address dynamicaly assigned by the DHCP server on an HDLC encapsulation interface.

To configure the DHCP client, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip address dhcp**	Obtain an IP address through DHCP.

Note

For some product in v10.1, DHCP client supports obtaining the IP address assigned by the DHCP server in the point-to-point link of PPP, HDLC, FR encapsulation.

22.6 Monitoring and Maintaining Information

22.6.1 Monitoring and Maintaining the DHCP Server

Three types of commands are available for monitoring and maintaining the DHCP server:

1. Clear commands, used to clear such information as DHCP address binding, address conflict and server statistics;
2. Debug commands, used to output necessary debugging information. Such commands are mainly used to diagnose and fix faults;
3. Show commands, used to show information about DHCP.

DES-7210 products provide three clear commands. To clear information, execute the following commands in the command execution mode:

Command	Function
DES-7210# **clear ip dhcp binding** { *address* | ***** }	Clear the DHCP address binding information.
DES-7210# **clear ip dhcp conflict** { *address* | *}	Clear the DHCP address conflict information.
DES-7210# **clear ip dhcp server statistics**	Clear the DHCP server statistics.

To debug the DHCP server, execute the following command in the command execution mode:

Command	Function
DES-7210# **debug ip dhcp server** [events | packet]	Debug the DHCP server.

To show the working status of the DHCP server, execute the following commands in the command execution mode:

Command	Function
DES-7210# **show ip dhcp binding** [*address*]	Show the DHCP address binding information.
DES-7210# **show ip dhcp conflict**	Show the DHCP address conflict information.
DES-7210# **show ip dhcp server statistics**	Show the DHCP server statistics.

22.6.2 Monitoring and Maintaining the DHCP Client

There are two types of commands for monitoring and maintaining the DHCP client. The following operations can be performed on the DHCP client:

Debug commands, used to output necessary debugging information. Such commands are mainly used to diagnose and clear faults.

Show commands, used to show information about DHCP.

To debug the DHCP client, execute the following command in the command execution mode:

Command	Function
DES-7210# **debug ip dhcp client**	Debug the DHCP client.

To show information about the lease that the DHCP client obtains, execute the following command in the command execution mode:

Command	Function
DES-7210# **show dhcp lease**	Show the information about DHCP lease.

22.7 Configuration Examples

This section provides three configuration examples:

- Address Pool Configuration
- Manual Binding Configuration
- DHCP Client Configuration

22.7.1 Address Pool Configuration Example

In the following configuration, the address pool net172 is defined, the network segment of the address pool is 172.16.1.0/24, the default gateway is 172.16.16.254, the domain name is rg.com, the domain name server is 172.16.1.253, the WINS server is 172.16.1.252, the NetBIOS node is of hybrid type, and the address lease period is 30 days. In this address pool, all the addresses other than 172.16.1.2 to 172.16.1.100 are available for assignment.

```
ip dhcp excluded-address 172.16.1.2 172.16.1.100
!
ip dhcp pool net172
network 172.16.1.0 255.255.255.0
default-router 172.16.1.254
domain-name rg.com
dns-server 172.16.1.253
netbios-name-server 172.16.1.252
netbios-node-type h-node
lease 30
```

22.7.2 Manual Binding Configuration

In the following configuration, the IP address assigned to the DHCP client with the MAC address 00d0.df34.32a3 is 172.16.1.101, the mask is 255.255.255.0, the host name is Billy.rg.com, the default gateway is 172.16.1.254, the WINS server is 172.16.1.252, and the NetBIOS node is of the hybrid type.

```
ip dhcp pool Billy
host 172.16.1.101 255.255.255.0
hardware-address 00d0.df34.32a3 ethernet
client-name Billy
default-router 172.16.1.254
domain-name rg.com
dns-server 172.16.1.253
netbios-name-server 172.16.1.252
netbios-node-type h-node
```

22.7.3 DHCP Client Configuration

In the following configuration, FastEthernet 0/0 is automatically assigned an address by DHCP.

```
interface FastEthernet0/0
ip address dhcp
```

23 DHCP Relay Configuration

23.1 Overview

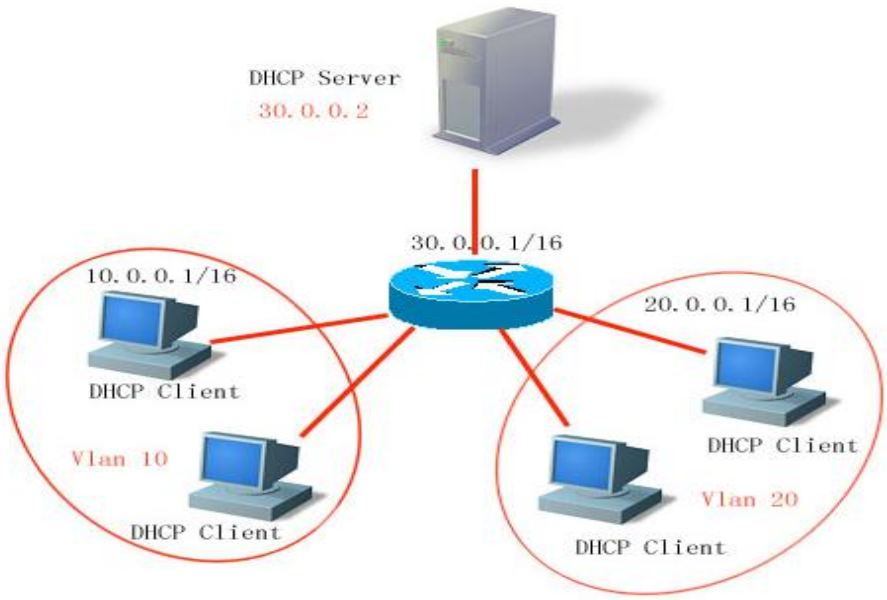
23.1.1 Understanding DHCP

The DHCP protocol is widely used to dynamically allocate the reusable network resources, for example, IP address.

The DHCP Client sends the DHCP DISCOVER packet in broadcast form to the DHCP Server. After the DHCP Server receives the DHCP DISCOVER packet, it allocates resources such as IP address to the the DHCP Client according to the appropriate policy, and sends the DHCP OFFER packet. After the DHCP Client receives the DHCP OFFER packet, it checks if the resources are available. If resources are available, it sends the DHCP REQUEST packet. If not, it sends the DHCP DISCOVER packet. When the DHCP server receives the DHCP REQUEST packet, it checks if the IP addresses (or other limited resources) can be allocated. If yes, it sends the DHCP ACK packet. If not, it sends the DHCP NAK packet. When the DHCP Client receives the DHCP ACK packet, it starts to use the resources allocated by the DHCP server. If it receives the DHCP NAK packet, it may re-send the DHCP DISCOVER packet to request another IP address.

23.1.2 Understanding the DHCP Relay Agent

The destination IP address of DHCP REQUEST packet is 255.255.255.255. This type of packets is only forwarded inside the subnet and is not to be forwarded by the devices. For dynamic IP address allocation across network segments, the DHCP Relay Agent is created. It encapsulates the received DHCP REQUEST packet into unicast IP packets and forwards it to the DHCP server. At the same time, it forwards the received DHCP response pacekt to the DHCP Client. In this way, the DHCP Relay Agent works as a transit station responsible for communicating with the DHCP Clients and the DHCP Server on different network segments. Therefore, one DHCP Server in a LAN can implement the dynamic IP management for all network segments, that is, a dynamic DHCP IP management in the Client - Relay Agent - Server mode.

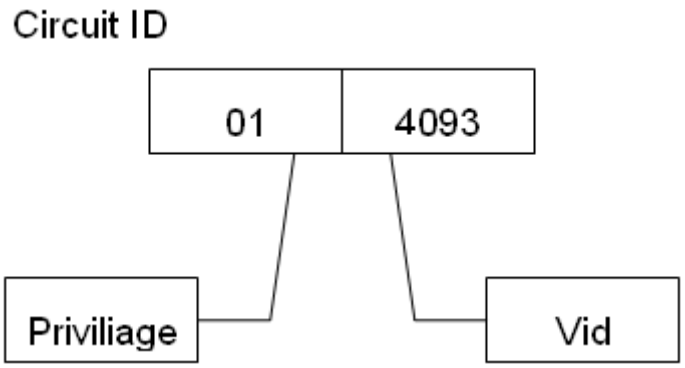


VLAN 10 and VLAN 20 correspond with the 10.0.0.1/16 and 20.0.0.1/16 networks respectively, while the DHCP Server is located on the 30.0.0.1/16 network. To have a dynamic IP management on the 10.0.0.1/16 and 20.0.0.1/16 networks through the DHCP Server at 30.0.0.2, just enable the DHCP Relay Agent on the device that functions as the gateway, and specify the IP address of the DHCP Server to 30.0.0.2.

23.1.3 Understanding DHCP Relay Agent Information(option 82)

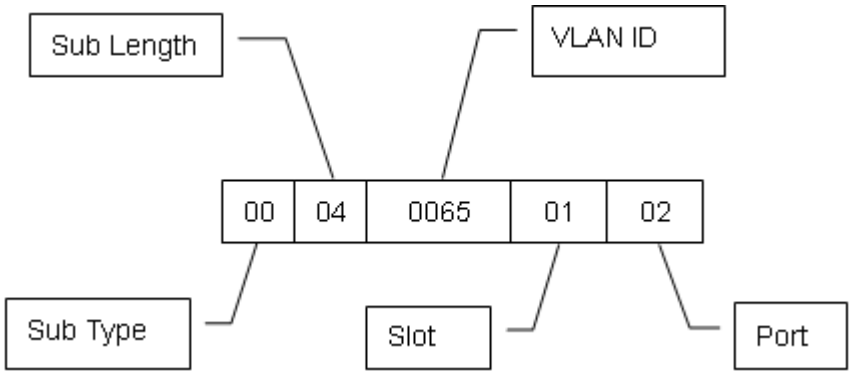
As specified in RFC3046, when a relay device performs DHCP relay, the network information of the DHCP client can be indicated in detail by adding an option, so that the DHCP server can assign users with IP addresses for different privileges. RFC3046 specifies that the option is numbered 82, so it is also called option82. This option can be divided into several sub-options. Currently, the sub-options in frequent use are Circuit ID and Remote ID. DES-7210 provides two types of relay agent information. One is the relay agent information option dot1x that is combined with the 802.1x/SAM application scheme, the other is relay agent information option82 that is combined with the port VID, slot, port and MAC address. Depicted below are the contents in the option, format, and typical application schemes when the two schemes are used:

1. relay agent information option dot1x: This application scheme requires combination of 802.1x authentication and DES-7210 RG-SAM. RG-SAM assigns different IP privileges to devices during 802.1x authentication. The device ‘s IP privilege combiens with the ID of VLAN to which the DHCP client belongs to form the Circuit ID sub-option. When DHCP relay is uploaded to the DHCP server, combined with the configuration of the DHCP server, the DHCP relay agent can assign IP addresses with different privileges to the users with different privileges. The Circuit ID is in the following format, where the **privilege** and **vid** fields respectively have two bytes:

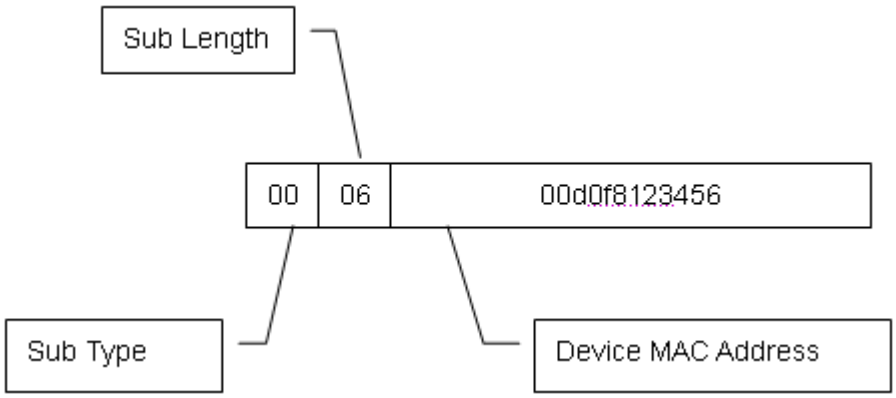


2. relay agent information option82: This option can be used without running other protocol modules. During DHCP relay, the device forms option82 information according to the port that receives the DHCP request message and the physical IP address of the device itself, and uploads the option82 information to the DHCP server. The option is in the following format:

Agent Circuit ID



Agent Remote ID



23.1.4 Understanding DHCP relay Check Server-id Function

When the DHCP is used, generally multiple DHCP servers are configured for a network for the purpose of backup, so that the network will continue to work even if a server fails. During the four interaction processes of DHCP acquisition, a DHCP server has been selected when the DHCP client sends the DHCP request message. Here, the DHCP request message includes the optional server-id. In some particular application circumstances, we need to enable this option for relay in order to reduce loads on the network server. In this way, the

DHCP request message is only sent to the specified DHCP server, instead of to every configured DHCP server. This is the DHCP check server-id function.

23.2 Configuring DHCP

23.2.1 Configuring the DHCP Relay Agent

To configure the DHCP relay agent, execute the following commands in the global configurtion mode:

Command	Function
DES-7210 (config)# **service dhcp**	Enable the DHCP agent.
DES-7210(config)# **no service dhcp**	Disable the DHCP agent.

23.2.2 Configuring the IP Address of the DHCP Server

After you have configured the IP address of the DHCP Server, the DHCP request message received by the device will be forwarded to it. At the same time, the DHCP response message received from the DHCP server will also be forwarded to the DHCP Client.

The IP address of the DHCP server can either be configured globally or on the layer 3 interface. Up to 20 IP addresses can be configured for the DHCP server in every mode. When the DHCP request message is received from an interface, the DHCP server of the interface is first used. If no DHCP server is configured on the interface, the DHCP server globally configured will be used.

The DHCP supports vrf-based relay function by adding the vtf parameter to the IP address of the DHCP server.

To configure the IP address of the DHCP server, exeute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **IP helper-address** [**vrf** *word*] *A.B.C.D*	Configure the IP address of the DHCP server globally.
DES-7210(config-if)# **IP helper-address** [**vrf** *word*] *A.B.C.D*	Configure the IP address of the DHCP server on the interface. This command must be set on the layer 3 interface.
DES-7210(config)# **no IP helper-address** [**vrf** *word*] *A.B.C.D*	Delete the globally configured IP address of the DHCP server.
DES-7210(config-if)# **no IP helper-address** [**vrf** *word*] *A.B.C.D*	Delete the IP address of the DHCP server configured on the interface.

23.2.3 Configuring DHCP option dot1x

Description in Understanding the DHCP Relay Agent Information shows that we can configure **ip dhcp relay information option dot1x** to enable the **option dot1x** function of the DHCP relay when you need to assign the IP addresses with different privileges to the

users of different privileges. When this function is enabled, the device will work with 802.1x to add corresponding option information to the DHCP server when it relays. This function should be used with the dot1x function.

To configure DHCP option dot1x, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip dhcp relay information option dot1x**	Enable the DHCP option dot1x function.
DES-7210(config)# **no ip dhcp relay information option dot1x**	Disable the DHCP option dot1x function.

23.2.4 Configuring DHCP option dot1x access-group

In the option dot1x application scheme, the device needs to restrict the unauthorized IP address or the IP address with low privilege to access certain IP addresses, and restrict the access between users with low privileges. To do so, configure the command **ip dhcp relay information option dot1x access-group** *acl-name*. Here the ACL defined by *acl-name* must be configured in advance. It is used to filter some contents and prohibit unauthorized users from accessing each other. In addition, ACL associated here is applied to all the ports on the device. This ACL has not default ACE and is not conflicted with ACLs associated with other interfaces. For example:

Assign a type of IP addresses for all the unauthorized users, namely 192.168.3.2-192.168.3.254, 192.168.4.2-192.168.4.254, and 192.168.5.2-192.168.5.254. 192.168.3.1, 192.168.4.1, and 192.168.5.1 are gateway addresses that are not assigned to users. In this way, an unauthorized user uses one of the 192.168.3.x-5.x addresses to access the Web portal for downloading client software. Therefore, the device should be configured as follows:

```
DES-7210# config
DES-7210(config)# ip access-list extended DenyAccessEachOtherOfUnauthrize
DES-7210(config-ext-nacl)# permit ip any host 192.168.3.1    //Packet that can be sent
to the gateway
DES-7210(config-ext-nacl)# permit ip any host 192.168.4.1
DES-7210(config-ext-nacl)# permit ip any host 192.168.5.1
DES-7210(config-ext-nacl)# permit ip host 192.168.3.1 any
```

//Permit the packets whose source IP address is the gateway.

```
DES-7210(config-ext-nacl)# permit ip host 192.168.4.1 any
DES-7210(config-ext-nacl)# permit ip host 192.168.5.1 any
DES-7210(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255
```

//Prohibit unauthorized users from accessing each other

```
DES-7210(config-ext-nacl)# deny ip 192.168.3.0  0.0.0.255  192.168.4.0  0.0.0.255
DES-7210(config-ext-nacl)# deny ip 192.168.3.0  0.0.0.255  192.168.5.0  0.0.0.255
DES-7210(config-ext-nacl)# deny ip 192.168.4.0  0.0.0.255  192.168.4.0  0.0.0.255
DES-7210(config-ext-nacl)# deny ip 192.168.4.0  0.0.0.255  192.168.5.0  0.0.0.255
DES-7210(config-ext-nacl)# deny ip 192.168.5.0  0.0.0.255  192.168.5.0  0.0.0.255
DES-7210(config-ext-nacl)# deny ip 192.168.5.0  0.0.0.255  192.168.3.0  0.0.0.255
DES-7210(config-ext-nacl)# deny ip 192.168.5.0  0.0.0.255  192.168.4.0  0.0.0.255
DES-7210(config-ext-nacl)# exit
```

Then, apply the command to the global interfaces using the **ip dhcp relay information option dot1x access-group** *DenyAccessEachOtherOfUnauthrize* command.

To configure **DHCP option dot1x access-group**, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip dhcp relay information option dot1x access-group** *acl-name*	Enable DHCP option dot1x acl.
DES-7210(config)# **no ip dhcp relay information option dot1x access-group** *acl-name*	Disable DHCP option dot1x acl.

23.2.5 Configuring DHCP option 82

When the **ip dhcp relay information option82** command is configured, the device adds **option** in the format as described in Understanding **DHCP Relay Agent Information** to the DHCP server during DHCP relay.

To configure DHCP option82, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip dhcp relay information option82**	Enable the DHCP option82 function.
DES-7210(config)# **no ip dhcp relay information option82**	Disable the DHCP option82 function.

23.2.6 Configuring DHCP relay check server-id

After the **ip dhcp relay check** *server-id* command is configured, the device resolves DHCP SERVER-ID option upon receiving DHCP relay. If this option is set, the DHCP request message is sent to this server only, instead of other configured servers.

To configure **DHCP relay check** *server-id* function, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip dhcp relay check** *server-id*	Enable the DHCP relay check server-di function.
DES-7210(config)# **no ip dhcp relay check** *server-id*	Disable the DHCP relay check server-id function.

23.2.7 Configuring DHCP Relay Suppression

After the **ip dhcp relay suppression** command is configured, the port will not relay the DHCP request broadcast packet by transforming it into the unicast form. However, it will not suppress the normal forwarding of broadcast packets received.

To configure DHCP relay suppression, execute the following commands in the interface configuration mode:

Command	Function

Command	Function
DES-7210(config-if)# **ip dhcp relay Suppression**	Enable the DHCP relay suppression function.
DES-7210(config-if)# **no ip dhcp relay Suppression**	Disable the DHCP relay suppression function.

23.2.8 DHCP Configuration Example

The following commands enable the DHCP relay function and add two groups of IP addresses of the DHCP server:

```
DES-7210# configure terminal
DES-7210(config)# service dhcp                    //Enable the dhcp relay function
DES-7210(config)# ip helper-address 192.18.100.1    //Add an IP address globally
DES-7210(config)# ip helper-address192.18.100.2     //Add an IP address globally
DES-7210(config)# interface GigabitEthernet 0/3
DES-7210(config-if)# ip helper-address 192.18.200.1 //Add an IP address on the
interface
DES-7210(config-if)# ip helper-address 192.18.200.2 // Add an IP address on the
interface
DES-7210(config-if)# end
```

23.3 Other Precausions on DHCP Relay Configuration

For layer 2 network devices, you must enable at least one of the option dot1x, dynamic address binding and option82 functions when the cross-management vlan relay function is required. Otherwise, only the relay function of management VLAN can be enabled for the layer 2 device.

23.3.1 Precautions on DHCP option dot1x Configuration

1. This command works only when the configuration related to AAA/802.1x is correct.
2. When this scheme is adopted, the IP authorization of the DHCP mode of 802.1x should be enabled.
3. This command cannot be used together with command **dhcp option82** because they are conflicted.
4. When the IP authorization of the DHCP mode of 802.1x is enabled, the MAC address and the IP address will also be bound. Therefore, IP authorization and DHCP dynamic binding function cannot be enabled at the same time.

23.3.2 Precautions on DHCP option82 Configuration

The DHCP option82 function and the **dhcp option dot1x** function cannot be used at the same time because they are conflicted.

23.4 Showing DHCP Configuration

Show the DHCP configuration using the **show running-config** command in the privileged mode.

```
DES-7210# show running-config
Building configuration...
Current configuration : 1464 bytes
version DES-7200 10.1.00(1), Release(11758)(Fri Mar 30 12:53:11 CST 2007 -nprd
hostname DES-7210
vlan 1
ip helper-address 192.18.100.1
ip helper-address 192.18.100.2
ip dhcp relay information option dot1x
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
no switchport
ip helper-address 192.168.200.1
ip helper-address 192.168.200.2
interface VLAN 1
ip address 192.168.193.91 255.255.255.0
line con 0
exec-timeout 0 0
line vty 0
exec-timeout 0 0
login
password 7 0137
line vty 1 2
login
password 7 0137
line vty 3 4
login
end
```

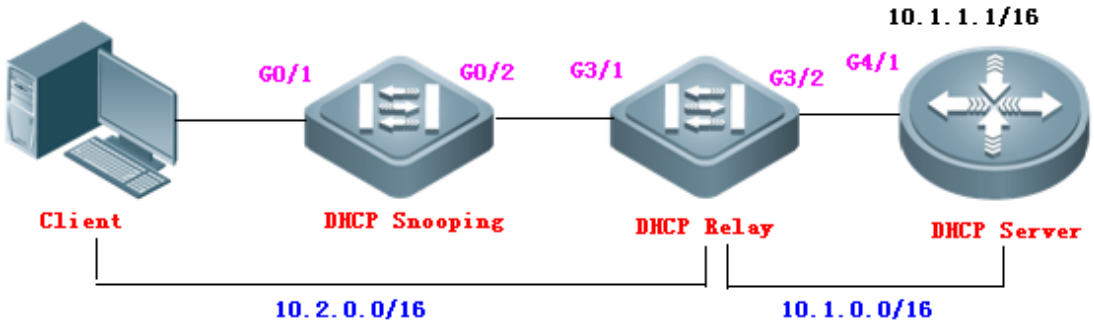
23.5 Typical Configuration Example

23.5.1 Applying for IP address to surf the Internet by the user in different network segments

23.5.1.1 Configuration Requirement

1. Obtaning the IP address and surfing the Internet by the user in different network segment.
2. Preventing illegal user from setting the IP address to surf the Internet.

23.5.1.2 Topology



23.5.1.3 Analysis

The port connecting the DHCP Snooping switch and the DHCP Relay switch is the access port. DHCP Relay is required to enable the DHCP Client to auto-obtain the IP address to surf the Internet across the network segment.

To prevent the illegal users from setting the IP address to surf the Internet, you can: 1) Enable DAI (Dynamic ARP Inspection) function in the global configuration mode; 2) Configure the address-bind in the interface configuration mode, and configuret the arp-check function to prevent the illegal users from surfing the Internet. For this configuration example, you may use the first method.

23.5.1.4 Configuration Steps

Set up the configuration environment based on the above topology figure, and configurate according to the following steps:

- DHCP Snooping Configuration:

Enable DHCP Snooping

```
DES-7210(config)# ip dhcp snooping
```

Set Gi0/2 connecting the server as the Trust Port

```
DES-7210(config)# interface gigabitEthernet 0/2
DES-7210(config-if)# ip dhcp snooping trust
```

Set Gi0/2 as the Trust Port of ARP detection

```
DES-7210(config-if)# ip arp inspection trust
DES-7210(config-if)# exit
```

Enable the DAI function in the specified VLAN

```
DES-7210(config)# ip arp inspection vlan 1
```

Set the IP address(SVI1) for the device

```
DES-7210(config)# interface vlan 1
DES-7210(config-if)# ip address 10.2.0.1 255.255.0.0
```

Set the static route to another network segment(10.1.0.0/16)

```
DES-7210(config)# ip route 10.1.0.0 255.255.0.0 10.2.1.1
```

- DHCP Relay Configuration:

Enable the DHCP relay agent

```
DES-7210(config)# server dhcp
```

Add an IP address for DHCP server in the global configuration mode

```
DES-7210(config)# ip helper-address 10.1.1.1
```

Set the IP address for the port connecting the DHCP Snooping switch

```
DES-7210(config)# interface gigabitEthernet 3/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 10.2.1.1 255.255.0.0
```

Set the IP address for the port connectin the DHCP Server

```
DES-7210(config)# interface gigabitEthernet 3/2
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 10.1.0.1 255.255.0.0
```

- DHCP Server Configuration:

Set the IP address for the port connecting the DHCP Relay device

```
DES-7210(config)# interface gigabitEthernet 4/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 10.1.1.1 255.255.0.0
```

Enable the DHCP Server

```
DES-7210(config)# service dhcp
```

Configure the DHCP excluded address, which will not be assigned to the DHCP Cllient

```
DES-7210(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.10
```

Configure the addresss pool name and enter the address pool configuration mode

```
DES-7210(config)# ip dhcp pool linwei
```

Configure the default gateway for the DHCP Client

```
DES-7210(dhcp-config)# default-router 10.2.1.1
```

Configure the network number and mask for the DHCP address pool

```
DES-7210(dhcp-config)# network 10.2.0.0  255.255.0.0
```

Configure the static route to another network segment (10.2.0.0/16)

```
DES-7210(config)# ip route 10.2.0.0  255.255.0.0  10.1.0.1
```

24 DNS Configuration

24.1 DNS Overview

Each IP address may present a host name consisting of one or more strings separated by the decimal. Then, all you need to do is to remember the host name rather than IP address. This is the function of the DNS protocol.

There are two methods to map from the host name to the IP address: 1) Static Mapping: A device maintains its host name to IP address mapping table and uses it only by itself. 2) Dynamic Mapping: The host name to IP address mapping table is maintained on the DNS server. In order for a device to communicate with others by its host name, it needs to search its corresponding IP address on the DNS server.

The domain name resolution (or host name resolution) is the process that the device obtains IP address which corresponds to the host name by the host name. The DES-7210 switches support the host name resolution locally or by the DNS. During the resolution of domain name, you can firstly adopt the static method. If it fails, use the dynamic method instead. Some frequently used domain names can be put into the resolution list of static domain names. In this way, the efficiency of domain name resolution can be increased considerably.

24.2 Configuring Domain Name Resolution

24.2.1 Default DNS Configuration

The default configurations of DNS are as follows:

Attribute	Default value
Enable/disable the DNS resolution service	Enable
IP address of DNS server	None
Status Host List	None
Maximum number of DNS servers	6

24.2.2 Enabling DNS Resolution Service

This section describes how to enable the DNS resolution service.

Command	Function
DES-7210(config)# **ip domain-lookup**	Enable DNS.

The command **no ip domain-lookup** is used to disable DNS.

```
DES-7210(config)# ip domain-lookup
```

24.2.3 Configuring the DNS Server

This section describes how to configure the DNS server. The dynamic domain name resolution can be carried out only when the DNS Server is configured.

The **no ip name-server** [*ip-address*] command can be used to remove the DNS server. Where, the **ip-address** parameter indicates the specified DNS server to be removed. If this parameter is omitted, all the DNS servers will be removed.

Command	Function
DES-7210(config)# **ip name-server** *ip-address*	Add the IP address of the DNS Server. The switch will add a DNS Server when this command is executed every time. If the domain name can't be obtained from the first DNS Server, the switch will send the DNS request to the subsequent several servers until the correct response is received. The system can support six DNS servers at most.

24.2.4 Configuring the Host Name to IP Address Mapping Statically

This section describes how to configure the host name to IP address mapping. The switch maintains a host name to IP address corresponding table, which is also referred to as the host name to IP address mapping table. You can obtain the mapping table in two ways: manual configuration and dynamic learning.

Command	Function
DES-7210(config)# **ip host** *host-name ip-address*	Configure the host name to IP address mapping manually.

This command with the parameter **no** can be used to remove the mapping between the host name and IP address.

24.2.5 Clearing the Dynamic Buffer Table of Host Names

This section describes how to clear the dynamic buffer table of host names. If the command **clear host** or **clear host** * is entered, the dynamic buffer table will be cleared. Otherwise, only the entries of specified domain names will be cleared.

Command	Function
DES-7210# **clear host** [*word*]	Clear the dynamic buffer table of host names. The host names configured statically will not be removed.

24.2.6 Showing Domain Name Resolution Information

This section describes how to display the DNS configuration.

Command	Function
DES-7210# **show hosts**	Show the DNS configuration.

```
DES-7210# show hosts
DNS name server   :
192.168.5.134   static
    host              type        address
www.163.com           static      192.168.5.243
www.DES-7210.com        dynamic     192.168.5.123
```

24.2.7 Application examples

Ping the host with specified domain name:

```
DES-7210# ping www.ietf.org
Resolving host[www.ietf.org]……
Sending 5,100-byte ICMP Echos to 192.168.5.123,
timeout is 2000 milliseconds.
!!!!!
Success rate is 100 percent(5/5)
Minimum = 1ms Maximum = 1ms, Average = 1ms
```

25 SNTP Configuration

25.1 Overview

Network Time Protocol (NTP) is designed for time synchronization on network devices. Another protocol, Simple Network Time Protocol(SNMP) can be used to synchronize the network time, too.

NTP protocol can be used across various platforms and operating systems, and provide precise time calculation (1-50ms precision) and prevent from latency and jitter in the network. NTP also provides the authentication mechanism with high security level. However, NTP algorithm is complicated and demands better system.

As a simplified version of NTP, SNTP simplifies the algorithm of time calculation but also has great performance, with precision of about 1s.

SNTP Client is totally compatible with the NTP Server due to the consistency of the SNTP and NTP messages.

25.1.1 Understanding SNTP

SNTP works in the way of Client/Server. The standard Server system time is set by receiving the GPS signal or the atomic clock. The Client obtains its accurate time from the service time accessing the server regularly, and adjusts its system clock to synchronize the time.

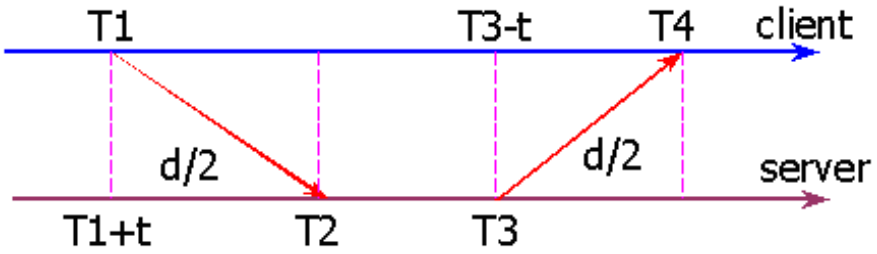


Figure-1

Originate Timestamp	T1	time request sent by client
Receive Timestamp	T2	time request received at server
Transmit Timestamp	T3	time reply sent by server
Destination Timestamp	T4	time reply received at client

T1: time request sent by client(refer to the client time) with the mark “Originate Timestamp”;

T2: time request received at server(refer to the server time) with the mark “Receive Timestamp”;

T3: time reply by server(refer to the server time) with the mark “Transmit Timestamp ”;

T4: time reply received at client(refer to the client time) with the mark “Destination Timestamp”.

T: time deviation between the Server and the Client

d: time between the Server and the Client

The following formula calculates the time:

∵ T2 = T1 + t + d / 2;

∴ T2 - T1 = t + d / 2;

∵ T4 = T3 – t + d / 2;

∴ T3 - T4 = t – d / 2;

∴ d = (T4 - T1) - (T3 - T2);

t = ((T2 - T1) + (T3 - T4)) / 2;

Then, according to the value of t and d, SNTP Client gets the current time: T4+t.

25.2 Configuring SNTP

This chapter describes how to configure the SNTP.

- Default configuration.
- Enabling SNTP.
- Configuring the IP address for the NTP server.
- Configuring the SNTP sync interval.
- Configuring the local time-zone.

25.2.1 Default Configuration

By default, the SNTP configurations are as follows:

Function	Default
SNTP state	Disabled.
IP address for the NTP server	0.
SNTP Sync Interval	1800s
Local Time-zone	GMT+8

25.2.2 Enabling SNTP

To enable the SNTP, run the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **sntp enable**	Enable the SNTP and synchronize the time once immediately. (in order to prevent frequent time synchronization, the sync-interval must not be less than 5s.)

To disable the SNTP, use the **no sntp enable** command.

25.2.3 Configuring the IP address for the NTP server

The SNTP Client is totally compatible with the NTP Server due to the inconsistency of SNTP and NTP messages. There are many NTP servers in the network, you can choose one switch with less latency as the NTP server.

For the detailed NTP server ip addresses, please logon to http://www.time.edu.cn/ or http://www.ntp.org/. For example, 192.43.244.18(time.nist.gov).

To set the IP address for the SNTP server, run the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **sntp server** *ip-address*	Specify the IP address for the SNTP server.

25.2.4 Configuring the SNTP Sync Interval

To adjust the time regularly, you need to set the sync interval for SNTP Client to access the NTP server SNTP Client regularly.

To configure the SNTP sync interval, run the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **sntp interval** *seconds*	Configure the SNTP sync interval, in second. Interval range: 60-65535s; Default value: 1800s.

Caution

The sync interval configuration can not take effect immediately. You shall execute the **sntp enable** command immediately after configuring the SNTP sync interval.

25.2.5 Configuring the Local Time-zone

The time obtained through the SNTP communication is Greenwich Mean Time(GMT). In order to obtain the exact local time, you need to set the local time to adjust the mean time.

To configure the local time-zone, run the following commands in the interface configuration model:

Command	Function
DES-7210(config)#**clock time-zone** *time-zone*	Configure the time-zone, ranging from GMT-23 to GMT+23, wherein “-” indicates western area, “+” indicates eastern area and “0” indicates Greenwich mean time. The default time-zone is GMT+8, Beijing time.

To restore the local time-zone to the default, use the command **no clock time-zone**.

25.3 Showing SNTP Information

Execute the **show sntp** command in the privileged mode to show the current SNTP information.

```
DES-7210# show sntp
SNTP state              : ENABLE          //to view whether SNTP is enabled or not
SNTP server             : 192.168.4.12   //NTP Server
SNTP sync interval       : 60            //SNTP sync interval
Time zone             : +8               //Local Time-zone
```

26 NTP Configuration

26.1 Understanding NTP

Network Time Protocol (NTP) is designed for time synchronization on network devices. A device can synchronize its clock source and the server. Moreover, the NTP protocol can provide precise time correction (less than one millisecond on the LAN and dozens of milliseconds on the WAN, compared with the standard time) and prevent from attacks by means of encryption and confirmation.

To provide precise time, NTP needs precise time source, the Coordinated Universal Time (UTC). The NTP may obtain UTC from the atom clock, observatory, satellite or Internet. Thus, accurate and reliable time source is available.

To prevent the time server from malicious destroying, an authentication mechanism is used by the NTP to check whether the request of time correction really comes from the declared server, and check the path of returning data. This mechanism provides protection of anti-interference.

DES-7210 switches support the NTP client and server. That is, the switch can not only synchronize the time of server, but also be the time server to synchronize the time of other switches. But when the switch works as the time server, it only support the unicast server mode.

26.2 Configuring NTP

This chapter describes how to configure the NTP client and server.

- Configuring the global NTP authentication mechanism.
- Configuring the global NTP authentication key.
- Configuring the global NTP trusted key ID.
- Configuring the NTP server.
- Disabling the interface to receive the NTP message.
- Enabling or disabling NTP.
- Configuring the NTP real-time synchronization
- Configuring the NTP update-calendar
- Configuring the NTP master
- Configuring the access control privilege of the NTP service

26.2.1 Configuring the Global NTP Authentication Mechanism

The NTP client of DES-7210 supports encrypted communication with the NTP server by means of key encryption.

There are two steps to configure the NTP client to communicate with the NTP server by means of encryption:

Step 1, Authenticate the NTP client and configure the key globally;

Step 2, Configure the trusted key for the NTP server.

To initiate the encrypted communication with the NTP server, you need to set authentication key for the NTP server in addition to perfomring Step 1.

By default, the NTP client does not use the global security authentication mechanism. Without this mechanism, the communication will not be encrypted. However, enabling the global security authentication does not mean that the encryption is used to implement the communication between the NTP server and the NTP client. You need to configure other keys globally and an encryption key for the NTP server.

To configure the global security authentication mechanism, run the following commands in the global configuration mode:

Command	Function
ntp authenticate	Configure the global NTP security authentication mechanism.
no ntp authenticate	Disable the global NTP security authentication mechanism.

The message is verified by the trusted key specified by the **ntp authentication-key** or **ntp trusted-key** command.

26.2.2 Configuring the Global NTP Authentication Key

The next step to configure the global security authentication for the NTP is to set the global authentication key.

Each key is identified by a unique key-id globally. The customer can use the command **ntp trusted-key** to set the key corresponding to the key-id as a global trusted key.

To specify a global authentication key, run the following commands in the global configuration mode:

Command	Function
ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]	Specify a global authentication key. *key-id*: in the range of 1 to 4294967295 *key-string*: Any *enc-type*: Two types: 0 and 7
no ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]	Remove a global authentication key.

The configuration of global authentication key does not mean the key is effective; therefore, the key must be configured as a global trusted key before using it.

Caution

The current NTP version can support up to 1024 authentication keys and only one key can be set for each server for secure communication.

26.2.3 Configure the Global NTP Trusted key ID

The last step is to set a global authentication key as a global trusted key. Only by this trusted key the user can send encrypted data and check the validity of the message.

To specify a global trusted key, run the following commands in the global configuration mode:

Command	Function
ntp trusted-key *key-id*	Specify a global trusted key ID.
no ntp trusted-key *key-id*	Remove a global trusted key ID.

The above-mentioned three steps of settings are the first procedure to implement security authentication mechanism. To initiate real encrypted communication between the NTP client and the NTP server, a trusted key must be set for the corresponding server.

Caution

When a global authentication key is removed, its all trusted information are removed.

26.2.4 Configuring the NTP Server

No NTP server is configured by default. DES-7210's client system supports simultaneous interaction with up to 20 NTP servers, and one authentication key can be set for each server to initiate encrypted communication with the NTP server after relevant settings of global authentication and key are completed.

NTP version 3 is the default version of communication with the NTP server. Meanwhile, the source interface can be configured to send the NTP message, and the NTP message from the relevant server can only be received on the sending interface.

To configure the NTP server, run the following commands in the global configuration mode:

Command	Function
ntp server *ip-addr* [**version** *version*][**source** *if-name number*][***key*** *keyid*][**prefer**]	Configure the NTP server. *version* (NTP version number): 1 to 3 *if-name* (interface type): Aggregateport, Dialer GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template and VLAN *keyid*: 1 to 4294967295
no ntp server *ip-addr*	Remove the NTP server.

Only when the global security authentication and key setting mechanisms are completed, and the trusted key for communicating with server is set, can the NTP client initiate the encrypted communication with the NTP server. To this end, the NTP server should have the same trusted key configured.

26.2.5 Disabling the Interface to Receiving the NTP Message

The function of this command is to disable the interface to receive the NTP message.

By default, the NTP messages received on any interface are available to the NTP client for clock synchronization. This function can shield the NTP messages received on the relevant interface.

Caution

This command takes effect only for the interface whose IP address can be configured to receive and send packets.

To disable the interface to receive the NTP message, run the following commands in the interface configuration model:

Command	Function
interface *interface-type number*	Enter the interface configuration mode.
ntp disable	Disable the function of receiving NTP messages on the interface.

To enable the function of receiving NTP messages on the interface, use the command **no ntp disable** in the interface configuration mode.

26.2.6 Enabling or Disabling NTP

The **no ntp** command is to disable the NTP synchronization service, stop the time synchronization, and clear relevant information of NTP configuration.

The NTP function is disabled by default, but may be enabled as long as the NTP server is configured.

To disable the NTP, run the following commands in the global configuration mode:

Command	Function
no ntp	Disable the NTP function.
ntp authenticate or **ntp server** *ip-addr* [**version** *version*][**source** *if-name number*][***key*** *keyid*][***prefer***]	Enable the NTP function.

26.2.7 Configuring the NTP Real-time Synchronization

To configure the NTP real-time synchronization, run the following commands in the global configuration mode:

Command	Function
ntp synchronization	Enable the NTP real-time synchronization.
no ntp synchronization	Disable the NTP real-time synchronization.

During the synchronization, the **no ntp** command and the **no ntp synchronization** command both can stop or disable the time synchronization. The difference of those two commands is that the **no ntp** command not only disables the NTP function, but also clears the related NTP settings.

26.2.8 Configuring the NTP Update-Calendar

The function of this command is to disable the interface to receive the NTP message.

To configure the NTP update-calendar, run the following commands in the global configuration model:

Command	Function
ntp update-calendar	Configure the update calendar.
no ntp update-calendar	Disable the function of NTP update calendar.

By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.

26.2.9 Configuring the NTP Master

The function of this command is to set the local time as the NTP master(the reference source of the local time is reliable), providing the synchronized time for other devices.

In general, the local system synchronizes the time from the external time source directly or indirectly. However, if the time synchronization of local system fails for the network connection trouble, ect, use the command to set the reliable reference source of the local time, providing the synchronized time for other devices.

Once set, the system time can not be synchronized to the time source with higher starum.

Note

The starum indicates the level of current clock, reference indicates the address of the server used for synchronization, freq indicates the clock frequency of current system, precision indicates the precision of current system clock, reference time indicates the UTC time of reference clock on the synchronization server, clock offset indicates the offset of current clock, root delay indicates the delay of current clock, root dispersion indicates the precision of top server, peer dispersion indicates the precision of synchronization server.

To configure the NTP master, run the following commands in the global configuration mode:

Command	Function
ntp master	Set the local time as the NTP master and specify the corresponding starum. The time starum ranges from 1-15, 8 by default.
no ntp master	Cancel the NTP master settings.

The following example shows how to set the reliable reference source of the local time and set the time starum as 12:

```
DES-7210(config)# ntp master 12
```

Caution

Using this command to set the local time as the master (in particular, specify a lower starum value), is likely to be covered by the effective clock source. If multiple devices in the same network use this command, the time synchronization instability may occur due to the time difference between the devices.

In addition, before using this command, if the system has never been synchronized with an external clock source, it is necessary to manually calibrate the system clock to prevent too much bias. (For how to how to manually calibrate the system clock, please refer to the section of system time configuration of "Basic switch management Configuration Guide")

This command is not restricted by ntp access control (even if the NTP access control function has corresponding matching limit, this command is still in force).

26.2.10 Configuring the Access Control Privilege of NTP Service

NTP services access control function provides a minimal security measures (more secure way is to use the NTP authentication mechanism). By default, no NTP access control rules are configured in the system.

To set the NTP services access control privilege, run the following command in the global configuration mode.

Command	Function
ntp access-group { peer | serve | serve-only | query-only } *access-list-number|access-list-name*	**Set the access control privilege of the local service.**
no ntp access-group { peer | serve | serve-only | query-only } *access-list-number|access-list-name*	**Cancel the settings of access control privilege of the local service.**

peer: not only allow the time requests and control queries for the local NTP service, but also allow the time synchronization between the local device and the remote system (full access privilege).

serve: only allow the time requests and control queries for the local NTP service, not allow the time synchronization between the local device and the remote system.

serve-only: only allow the time requests for the local NTP service.

query-only: only allow the control queries for the local NTP service.

access-list-number: IP access control list label; the range of 1 ~ 99 and 1300 ~ 1999. On how to create IP access control list, refer to the relevant description in "Access Control List Configuration Guide".

access-list-name: IP access control list name. On how to create IP access control list , refer to the the relevant description in "Access Control List Configuration Guide" .

When an access request arrives, NTP service matches the rules in accordance with the sequence from the smallest to the largest to access restriction, and the first matched rule shall prevail. The matching order is peer, serve, serve-only, query-only.

Caution

Control query function (the network management device controls the NTP server, such as setting the leap second mark or monitor the working state,ect) is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

If you do not configure any access control rules, then all accesses are allowed. However, once the access control rules are configured, only the rule that allows access can be carried out.

The following example shows how to allow the peer device in acl1 to control the query, request for and synchronize the time with the local device; and limit the peer device in acl2 to request the time for the local device:

```
DES-7210(config)# ntp access-group peer 1
DES-7210(config)# ntp access-group serve-only 2
```

26.3 Showing NTP Information

26.3.1 NTP Debugging

If you want to debug the NTP function, this command may be used to output necessary debugging information for troubleshooting.

To debug the NTP function, run the following commands in the privilege mode:

Command	Function
debug ntp	Enable the debugging function.
no debug ntp	Disable the debugging function.

26.3.2 Showing NTP Information

Execute the **show ntp status** command in the privileged mode to show the current NTP information.

To display the NTP function, run the following command in the privileged mode:

Command	Function
show ntp status	Show the current NTP information.

Only when the relevant communication server is configured can this command be used to print the display information.

```
DES-7210# show ntp status
Clock is synchronized, stratum 9, reference is 192.168.217.100
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is AF3CF6AE.3BF8CB56 (20:55:10.000 UTC Mon Mar 1 1993)
clock offset is 32.97540 sec, root delay is 0.00000 sec
root dispersion is 0.00003 msec, peer dispersion is 0.00003 msec
```

Note

The starum indicates the level of current clock, reference indicates the address of the server used for synchronization, freq indicates the clock frequency of current system, precision indicates the precision of current system clock, reference time indicates the UTC time of reference clock on the synchronization server, clock offset indicates the offset of current clock, root delay indicates the delay of current clock, root dispersion indicates the precision of top server, peer dispersion indicates the precision of synchronization server.

26.4 Configuration Examples

In the following configuration, there is an NTP server specified as the master in the network, relevant authentication mechanism is enabled, a key with the key-id of 6 and the key-string of wooooop is configured as the trusted key for the server. To configure the DES-7210 client to synchronize the time with the NTP server on the network, configure the NTP client as follows: enable security authentication, configure the same key as that for the NTP server, set this NTP server to synchronize the time, and begin to synchronize the time.

The IPv4 configuration example:

```
DES-7210(config)# no ntp
DES-7210(config)# ntp authentication-key 6 md5 wooooop
DES-7210(config)# ntp authenticate
DES-7210(config)# ntp trusted-key 6
DES-7210(config)# ntp server 192.168.210.222 key 6
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# ntp disable
DES-7210(config-if)# no ntp disable
```

The IPv6 configuration example:

```
DES-7210(config)# no ntp
DES-7210(config)# ntp authentication-key 6 md5 wooooop
DES-7210(config)# ntp authenticate
DES-7210(config)# ntp trusted-key 6
DES-7210(config)# ntp server 10::4 key 6
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# ntp disable
DES-7210(config-if)# no ntp disable
```

27 UDP-Helper Configuration

27.1 UDP-Helper Configuration

27.1.1 UDP-Helper Overview

The main function of UDP-Helper is to implement the relay and forward of UDP broadcast packets. By configuring the destination server for the UDP broadcast packets to be forwarded, the UDP-Helper can convert the UDP broadcast packets into the unicast packets and then send them to the specified destination server. The UDP-Helper acts like a relay.

Once enabled, the UDP-Helper will check to see whether the destination UDP port number of the received broadcast packets matches the port number to be forwarded. If so, it modifies the destination IP address of packets as the IP address of the specified destination server, and send the packets to the destination server in unicast form.

When the UDP-Helper is enabled, the broadcast messages from Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.

Note

The relay of BOOTP/DHCP broadcast packet is implemented through the UDP Port 67 and 68 by the DHCP Relay module; therefore, the two ports can not be configured as the relay port of UDP-Helper.

27.2 Configuring UDP-Helper

27.2.1 Default UDP-Helper Configuration

Default UDP-Helper configuration

Attribute	Default value
Relay and forwarding	Disabled
UDP port for relay and forwarding	When the UDP-Helper is enabled, the UDP broadcast packets from Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.
Destination server for delay and forward	None

27.2.2 Enable the Relay and Forward Function of the UDP-Helper

Command	Function

Command	Function
DES-7210(config)# **udp-helper Enable**	Enable the relay and forward function of UDP broadcast packets. This function is disabled by default.

The **no udp-helper enable** command is used to disable the relay and forward funciton of the UDP-Helper.

Note

1. The relay and forwarding function is disabled by default.
2. When the UDP-Helper is enabled, the broadcast packets from UDP Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.
3. When the UDP-Helper is disabled, all of the configured UDP ports including the default ports are cancelled.

27.2.3 Configuring the Destination Server for Relay and Forwarding

Command	Function
DES-7210(config-if)# **ip helper-address** *IP-address*	Configure the destination server to which the UDP broadcast packets are relayed and forwarded. By default, it is not configured.

The **no ip helper-address** command can be used to remove the destination server for relay and forwarding.

Note

1. At most 20 destination servers can be configured for an interface.
2. If the destination server for relay and forwarding is configured on a specified interface, when the UDP-Helper is enabled, the broadcast packets of the specified UDP port received from this interface will be sent to the destination server configured for this interface in unicast form.

27.2.4 Configuring the UDP Port for Relay and Forwarding

Command	Function
DES-7210(config)# **ip forward-protocol udp** *ID*	Configure the UDP port for relay and forwarding. If only the UDP parameter is specified, the default port will be used for relay and forwarding; otherwise, the port can be configured upon necessary. When the UDP-Helper is enabled, the broadcast packets from Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.

The **no ip forward-protocol udp port** command can be used to disable the UDP port for relay and forwarding.

Note

- Only when the function of delay and forwarding is enabled for the UDP-Helper and the destination server is configured for the relay and forwarding, can the UDP port be configured for relay and forwarding. Otherwise, the error prompts will appear.
- When the relay and forwarding function of the UDP-Helper is enabled, the function of forwarding the broadcast UDP packets from the default ports 69, 53, 37, 137, 138 and 49 will be enabled right now without any configuration.
- At most 256 UDP ports are supported for relay and forwading by the switch.
- Two ways can be used to configure the default ports, for example, the **ip forward-protocol udp domain** and **ip forward-protocol udp** *53* commands do the same thing.

28 SNMP Configuration

28.1 SNMP Related Information

28.1.1 Overview

As the abbreviation of Simple Network Management Protocol, SNMP has been a network management standard (RFC1157) since the August, 1988. So far, the SNMP becomes the actual network management standard for the support from many manufacturers. It is applicable to the situation of interconnecting multiple systems from different manufacturers. Administrators can use the SNMP protocol to query information, configure network, locate failure and plan capacity for the nodes on the network. Network supervision and administration are the basic function of the SNMP protocol.

As a protocol in the application layer, the SNMP protocol works in the client/server mode, including three parts as follows:

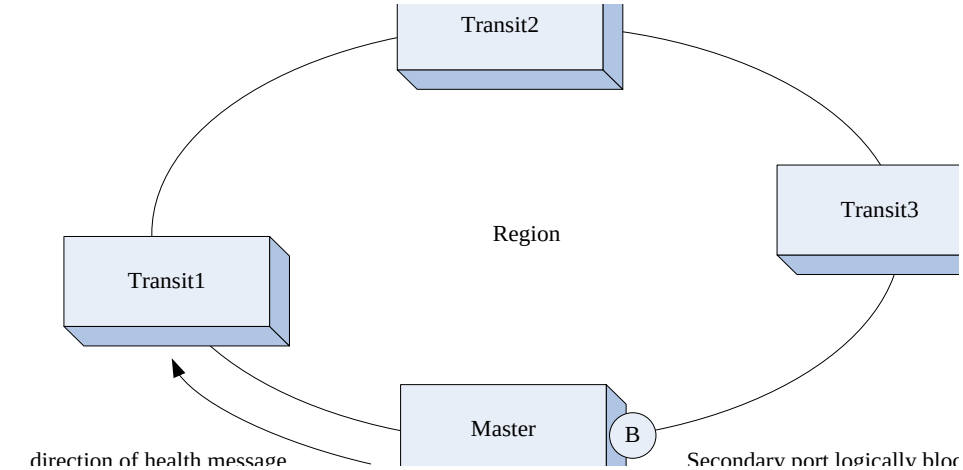
- SNMP network manager
- SNMP agent
- MIB (management information base)

The SNMP network manager, also referred to as NMS (Network Management System), is a system to control and monitor the network using the SNMP protocol. HP OpenView, CiscoView and CiscoWorks 2000 are the typical network management platforms running on the NMS. DES-7210 has developed a suit of software (Star View) for network management against its own network devices. These typical network management software are convenient to monitor and manage network devices.

The SNMP Agent is the software running on the managed devices. It receives, processes and responds the monitoring and controlling messages from the NMS, and also sends some messages to the NMS.

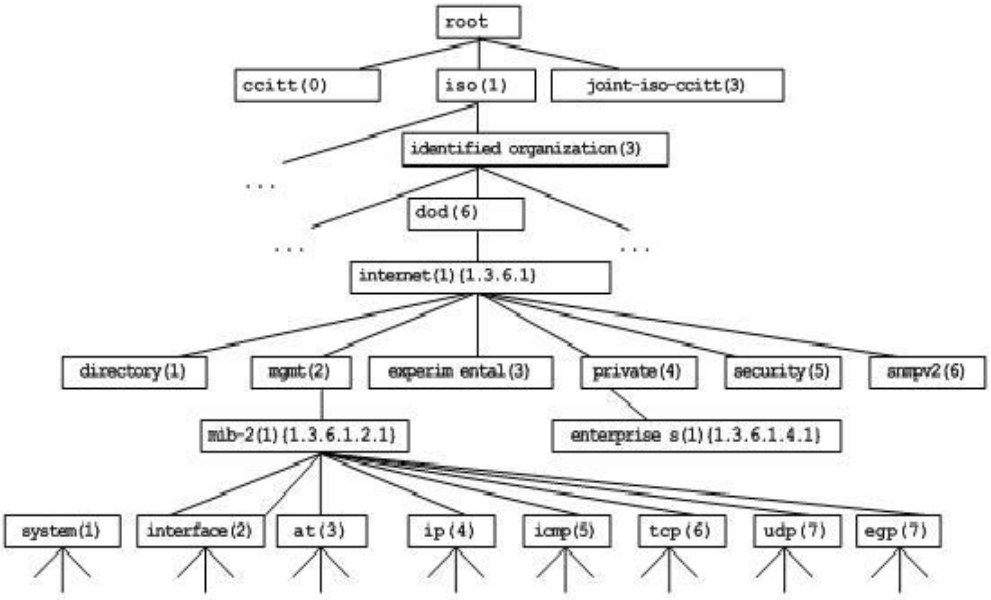
The relationship between the NMS and the SNMP Agent can be indicated as follows:

Relationship between the NMS and the SNMP Agent



The MIB (Management Information Base) is a virtual information base for network management. There are large volumes of information for the managed network equipment. In order to uniquely identify a specific management unit in the SNMP message, the tree-type hierarchy is used to by the MIB to describe the management units in the network management equipment. The node in the tree indicates a specific management unit. Take the following figure of MIB as an example to name the objectives in the tree. To identify a specific management unit system in the network equipment uniquely, a series of numbers can be used. For instance, the number string {1.3.6.1.2.1.1} is the object identifier of management unit, so the MIB is the set of object identifiers in the network equipment.

Tree-type MIB hierarchy



28.1.2 SNMP Versions

This software supports these SNMP versions:

- SNMPv1: The first formal version of the Simple Network Management Protocol, which is defined in RFC1157.
- SNMPv2C: Community-based Administrative Framework for SNMPv2, an experimental Internet protocol defined in RFC1901.

- SNMPv3: Offers the following security features by authenticating and encrypting packets:
  1. Ensure that the data are not tampered during transmission.
  2. Ensure that the data come from a valid data source.
  3. Encrypt packets to ensure the data confidentiality.

Both the SNMPv1 and SNMPv2C use a community-based security framework. They restrict administrator's operations on the MIB by defining the host IP addresses and community string.

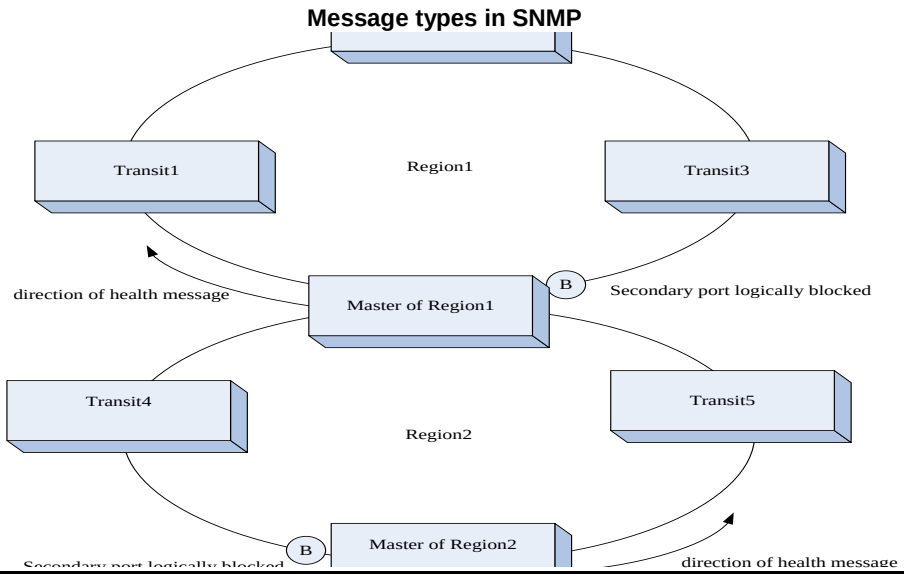
With the GetBulk retrieval mechanism, SNMPv2C sends more detailed error information type to the management station. GetBulk allows you to obtain all the information or a great volume of data from the table at a time, and thus reducing the times of request and response. Moverover, SNMPv2C improves the capability of handing errors, including expanding error codes to distinguish different kinds of errors, which are represented by one error code in SNMPv1. Now, error types can be distinguished by error codes. Since there may be the management workstations supporting SNMPv1 and SNMPv2C in a network, the SNMP agent must be able to recognize both SNMPv1 and SNMPv2C messages, and return the corresponding version of messages.

28.1.3 SNMP Management Operations

For the information exchange between the NMS and the SNMP Agent, six types of operations are defined:

1. Get-request: The NMS gets one or more parameter values from the SNMP Agent.
2. Get-next-request: The NMS gets the next parameter value of one or more parameters from the SNMP Agent.
3. Get-bulk: The NMS gets a bulk of parameter values from the SNMP Agent.
4. Set-request: The NMS sets one or more parameter values for the SNMP Agent.
5. Get-response: The SNMP Agent returns one or more parameter values, the response of the SNMP Agent to any of the above 3 operations of the NMS.
6. Trap: The SNMP Agent proactively sends messages to notify the NMS that some event will occur.

The first four messages are sent from the NMS to the SNMP Agent, and the last two messages are sent from the SNMP Agent to the NMS (Note: SNMPv1 does not support the Get-bulk operation). These operations are described in the following figure:



NMS sends messages to the SNMP Agent in the first three operations and the SNMP Agent responds a message through the UDP port 161. However, the SNMP Agent sends a message in the Trap operation through the UDP port 162.

Caution

When managing the R2700 switching card(NM2-24ESW/NM2-16ESW) via SNMP, NM2-24ESW obtains the inexistent error message of port 17-26, while NM2-16ESW obtains the inexistent error message of port 25-26.

28.1.4 SNMP Security

Both SNMPv1 and SNMPv2 use the community string to check whether the management workstation is entitled to use MIB objects. In order to manage devices, the community string of NMS must be identical to a community string defined in the devices.

A community string Features:

- Read-only: Authorized management workstations are entitled to read all the variables in the MIB.
- Read-write: Authorized management workstations are entitled to read and write all the variables in the MIB.

Based on SNMPv2, SNMPv3 can determine a security mechanism for processing data by security model and security level. There are three types of security models: SNMPv1, SNMPv2C and SNMPv3.

The table below describes the supported security models and security levels.

Model	Level	Authentication	Encryption	Description
SNMPv1	noAuthNoPriv	Community string	None	Ensures the data validity through community string.
SNMPv2c	noAuthNoPriv	Community string	None	Ensures the data validity through community string.
SNMPv3	noAuthNoPriv	User name	None	Ensures the data validity through user name.
SNMPv3	authNoPriv	MD5 or SHA	None	Provides HMAC-MD5 or HMAC-SHA-based authentication mechanism.
SNMPv3	authPriv	MD5 or SHA	DES	Provides HMAC-MD5 or HMAC-SHA-based authentication mechanism and CBC-DES-based encryption mechanism.

28.1.5 SNMP Engine ID

The engine ID is designed to identify an SNMP engine uniquely. Every SNMP entity contains a SNMP engine, a SNMP engine ID identifies a SNMP entity in a management domain. So every SNMPV3 entity has a unique identifier named SNMP Engine ID.

The SNMP Engine ID is an octet string of 5 to 32 bytes, which is defined in RFC3411:

- The first four bytes indicate the private enterprise number of an enterprise (assigned by IANA) in hex system.
- The fifth byte indicates how to identify the rest bytes.

  0: Reserved

  1: The following 4 bytes indicate an IPv4 address.

  2: The following 16 bytes indicate an IPv6 address.

3: The following 6 bytes indicate an MAC address

4: Texts of up to 27 bytes defined by manufacturers

5: A hexadecimal value of up to 27 bytes defined by manufacturers

6-127: Reserved

128-255: In the format specified by manufacturers.

28.2 SNMP Configuration

To configure SNMP, enter the global configuration mode.

28.2.1 Setting the Community String and Access Authority

SNMPv1 and SNMPv2C adopt community string-based security scheme. The SNMP Agent supports only the management operations from the management workstations of the same community string. The SNMP messages without matching the community string will be discarded. The community string serves as the password between the NMS and the SNMP Agent.

- Configure an ACL rule to allow the NMS of the specified IP address to manage devices.
- Set the community's operation right: ReadOnly or ReadWrite.
- Specify a view for view-based management. By default, no view is configured. That is, the management workstation is allowed to access to all MIB objects
- Indicate the IP address of the NMS who can use this community string. If it is not indicated, any NMS can use this community string. By default, any NMS can use this community string.

To configure the SNMP community string, run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **snmp-server community** *string* **[view** *view-name***] [ro** | **rw] [host** *host-ip***] [***num***]**	Set the community string and its right.

One or more coummnity strings can be specified for the NMS of different rights. To remove the community name and its right, run the **no snmp-server community** command in the global configuration mode.

28.2.2 Configuring MIB Views and Groups

With view-based access control model, you can determine whether the object of a management operation is in a view or not. For access control, generally some users are associated with a group and then the group is associated with a view. The users in a group have the same access right.

- Set an inclusion view and an exclusion view.
- Set a Read-only view and a Read-write view for a group.
- Set security levels, whether to authenticate, and whether to encrypt for SNMPv3 users.

To configure the MIB views and groups, run the following commands in the global configuration mode:

Command	Function

Command	Function
DES-7210(config)# **snmp-server view** *view-name oid-tree* {**include	exclude**}	Create a MIB view to include or exclude associated MIB objects.
DES-7210(config)# **snmp-server group** *groupname* {**v1**	**v2c** |**v3** {**auth**	**noauth**	**priv**}} [**read** *readview*] [**write** *writeview*]	Create a group and associate it with the view.

You can delete a view by using the **no snmp-server view** *view-name* command, or delete a tree from the view by using the **no snmp-server view** *view-name oid-tree* command. You can also delete a group by using the **no snmp-server group** *groupname* command.

28.2.3 Configuring SNMP Users

User-based security model can be used for security management. In this mode, you should configure user information first. The NMS can communicate with the SMP Agent by using a valid user account.

For SNMPv3 users, you can specify security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (only DES now) and encryption password.

To configure a SNMP user, run the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **snmp-server user** username groupname {**v1	v2	v3 [encrypted] [auth { md5|sha** } auth-password] [priv des56 priv-password] } [access {num	name}]	Configure the user information.

To remove the specified user, execute the **no snmp-server user** *username groupname* command in the global configuration mode.

28.2.4 Configuring SNMP Host Address

In special cases, the SNMP Agent may also proactively send messages to the NMS.

To configure the NMS host address that the SNMP Agent proactively sends messages to, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **snmp-server host** {*host-addr*	**ipv6** *ipv6-addr* } [**vrf** *vrfname*] [**traps**] [**version** {**1|2c |3 [auth	noauth	priv**]}] *community-string* [udp-port *port-num*] [***type***]	Set the SNMP host address, vtf, community string, message type (or security level in SNMPv3).

28.2.5 Configuring SNMP Agent Parameters

You can configure the basic parameters of the SNMP Agent, including contact, device location and sequence number. With these parameters, the NMS knows the contact, location and other information of the device.

To configure the SNMP agent parameters, run the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **snmp-server contact** *text*	Configure the contact.
DES-7210(config)# **snmp-server location** *text*	Configure the location.
DES-7210(config)# **snmp-server chassis-id** *number*	Configure the sequence number.

28.2.6 Defining the Maximum Message Size of the SNMP Agent

In order to enhance network performance, you can configure the maximum packet size of the SNMP Agent. To configure the maximum packet size of the SNMP Agent, run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **snmp-server packetsize** *byte-count*	Set the maximum packet size of the SNMP Agent.

28.2.7 Shielding the SNMP Agent

The SNMP Agent service is a service provided by DES-7210product and enabled by default. When you do not need it, you can shield the SNMP agent service and related configuration by executing the following command in the global configuration mode:

Command	Function
DES-7210(config)# **no snmp-server**	Shield the SNMP agent service.

28.2.8 Disabling the SNMP Agent

DES-7210 products provide a different command from the shield command to disable the SNMP Agent. This command will act on all of the SNMP services instead of shielding the configuration information of the SNMP Agent. To disable the SNMP agent service, run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **no enable service snmp-agent**	Disable the SNMP agent service.

28.2.9 Configuring the SNMP Agent to Send the Trap Message to the NMS Initiatively

The TRAP message is a message automatically sent by the SNMP Agent to the NMS unsolicitedly, and is used to report some critical and important events. By default the SNMP Agent is not allowed to send the TRAP message. To enable it, run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **snmp-server enable traps** [*type*] [*option*]	Allow the SNMP Agent to send the TRAP message proactively.
DES-7210(config)# **no snmp-server enable traps** [*type*] [*option*]	Forbid the SNMP Agent to send the TRAP message proactively.

28.2.10 Configuring LinkTrap Policy

You can configure whether to send the LinkTrap message of an interface. When this function is enabled and the link status of the interface changes, the SNMP will send the LinkTrap message. Otherwise, it will not. By default, this function is enabled.

Command	Function
DES-7210(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config-if)# **[no] snmp trap** link-status	Enable or disable sending the LinkTrap message of the interface.

The following configures the intereface not to send LinkTrap Message:

```
DES-7210(config)# interface gigabitEthernet 1/1
DES-7210(config-if)#no snmp trap link-status
```

28.2.11 Configuring the Parameters for Sending the Trap Message

To set the parameters for the SNMP Agent to send the Trap message, execute the following commands:

Command	Function
DES-7210(config)# **snmp-server trap-source** *interface*	Specify the source port sending the Trap message.
DES-7210(config)# **snmp-server** queue-length *length*	Specify the queue length of each Trap message.
DES-7210(config)# **snmp-server** trap-timeout *seconds*	Specify the interval of sending Trap message.

28.2.12 Configuring Interface Index Persist

It helps manage the network if the interface index persists after initialization. You can execute this command to persist the interface index after restartin the switch:

Command	Function
DES-7210(config)# **snmp-server if-index persist**	Enable the interface index persist function.

To disable this function, use the **no snmp-server if-index persist** command. By default, this function is disabled.

```
DES-7210(config)# snmp-server if-index persist
```

28.3 SNMP Monitoring and Maintenance

28.3.1 Checking the Current SNMP Status

To monitor the SNMP status and troubleshoot SNMP configurations, DES-7210 product provides monitoring commands for SNMP, with which it is possible to easily check the

SNMP status of the current network device. In the privileged mode, execute **show snmp** to check the current SNMP status.

```
DES-7210# show snmp
Chassis: 1234567890 0987654321
Contact: wugb@i-net.com.cn
Location: fuzhou
2381 SNMP packets input
   5 Bad SNMP version errors
   6 Unknown community name
   0 Illegal operation for community name supplied
   0 Encoding errors
   9325 Number of requested variables
   0 Number of altered variables
   31 Get-request PDUs
   2339 Get-next PDUs
   0 Set-request PDUs
2406 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   4 No such name errors
   0 Bad values errors
   0 General errors
   2370 Get-response PDUs
   36 SNMP trap PDUs
SNMP global trap: disabled
SNMP logging: enabled
SNMP agent: enabled
```

The above statistics is explained as follows:

Showing Information	Description
Bad SNMP version errors	SNMP version is incorrect.
Unknown community name	The community name is not known.
Illegal operation for community name supplied	Illegal operation
Encoding errors	Code error
Get-request PDUs	Get-request message
Get-next PDUs	Get-next message
Set-request PDUs	Set-request message
Too big errors (Maximum packet size 1500)	Too large response message
No such name errors	Not in the specified management unit
Bad values errors	Specified value type error
General errors	General error
Get-response PDUs	Get-response message
SNMP trap PDUs	SNMP trap message

28.3.2 Checking the MIB Objects Supported by the Current SNMP Agent

To check the MIB objects supported by the current SNMP Agent, run the **show snmp mib** command in the privileged mode:

```
DES-7210# show snmp mib
```

```
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices
sysORLastChange
snmpInPkts
snmpOutPkts
snmpInBadVersions
snmpInBadCommunityNames
snmpInBadCommunityUses
snmpInASNParseErrs
snmpInTooBigs
snmpInNoSuchNames
snmpInBadValues
snmpInReadOnlys
snmpInGenErrs
snmpInTotalReqVars
snmpInTotalSetVars
snmpInGetRequests
snmpInGetNexts
snmpInSetRequests
snmpInGetResponses
snmpInTraps
snmpOutTooBigs
snmpOutNoSuchNames
snmpOutBadValues
snmpOutGenErrs
snmpOutGetRequests
snmpOutGetNexts
snmpOutSetRequests
snmpOutGetResponses
snmpOutTraps
snmpEnableAuthenTraps
snmpSilentDrops
snmpProxyDrops
entPhysicalEntry
entPhysicalEntry.entPhysicalIndex
entPhysicalEntry.entPhysicalDescr
entPhysicalEntry.entPhysicalVendorType
entPhysicalEntry.entPhysicalContainedIn
entPhysicalEntry.entPhysicalClass
entPhysicalEntry.entPhysicalParentRelPos
entPhysicalEntry.entPhysicalName
entPhysicalEntry.entPhysicalHardwareRev
entPhysicalEntry.entPhysicalFirmwareRev
entPhysicalEntry.entPhysicalSoftwareRev
entPhysicalEntry.entPhysicalSerialNum
entPhysicalEntry.entPhysicalMfgName
entPhysicalEntry.entPhysicalModelName
```

```
entPhysicalEntry.entPhysicalAlias
entPhysicalEntry.entPhysicalAssetID
entPhysicalEntry.entPhysicalIsFRU
entPhysicalContainsEntry
entPhysicalContainsEntry.entPhysicalChildIndex
entLastChangeTime
```

28.3.3 Viewing SNMP Users

To view the SNMP users configured on the current SNMP agent, run the **show snmp user** command in the privileged mode:

```
DES-7210# show snmp user
User name: test
Engine ID: 800013110300000000000
storage-type: permanent    active
Security level: auth priv
Auth protocol: SHA
Priv protocol: DES
Group-name: g1
```

28.3.4 Viewing SNMP Views and Groups

To view the group configured on the current SNMP agent, run the **show snmp group** command in the privileged mode:

```
DES-7210# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: default
writeview: default
notifyview:

groupname: public
securityModel: v1
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:

groupname: public
securityModel: v2c
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:
```

To view the view configured on the current SNMP agent, run the **show snmp view** command in the privileged mode:

```
DES-7210# show snmp view
```

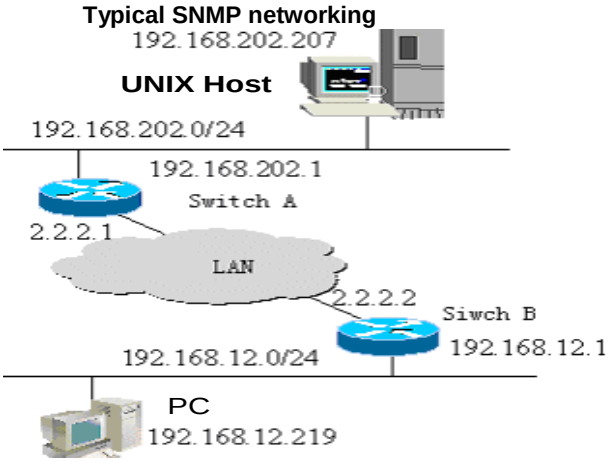
```
default(include) 1.3.6.1
test-view(include) 1.3.6.1.2.1
```

28.4 SNMP Configuration Example

28.4.1 Typical Configuration Example

- **Configuration requirement**

As shown in the following figure, the router is connected with the network management station (NMS) via the Ethernet. The IP addresses of the NMS and the router are 192.168.12.181 and 192.168.12.1 respectively. A network management software (taking HP OpenView as an example) is running on the NMS.



- **Detailed router configuration**

Enable the SNMP agent service:

```
DES-7210(config)# snmp-server community public RO
```

As long as the above command is configured in the global configuration mode, the SNMP agent service is enabled on the router, and then the NMS can monitor the router. However, just read-only right is configured; the NMS can not modify the router's configuration but monitor its running. Other configurations are optional.

If the read-write access right is required, execute the following command:

```
DES-7210(config)# snmp-server community private RW
```

Followings are basic parameters of the SNMP Agent on the router. The NMS can get basic system information of the router via these parameters. This configuration is optional:

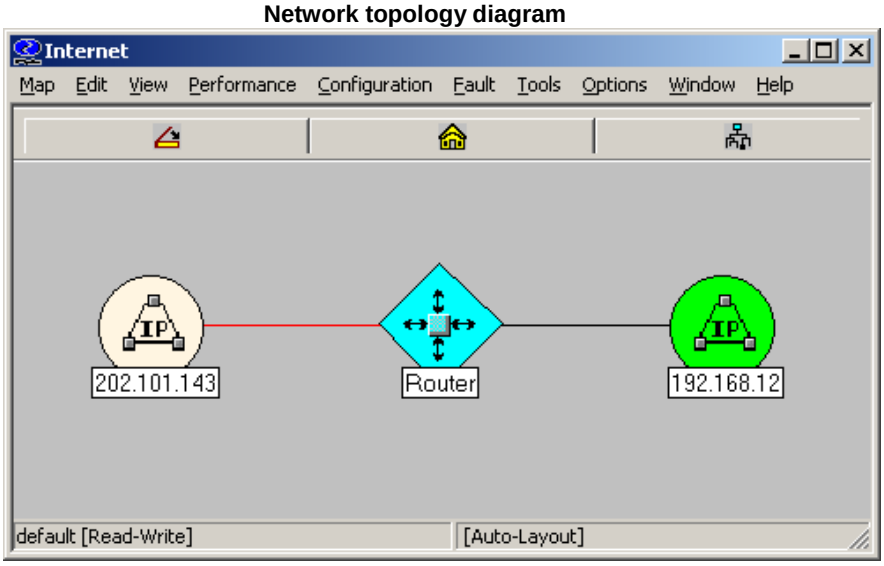
```
DES-7210(config)# snmp-server location fuzhou
DES-7210(config)# snmp-server contact wugb@i-net.com.cn
DES-7210(config)# snmp-server chassis-id 1234567890
0987654321
```

The following configuration is optional; the router is allowed to send some Trap messages to the NMS proactively.

```
DES-7210(config)# snmp-server enable traps
DES-7210(config)# snmp-server host 192.168.12.181 public
```

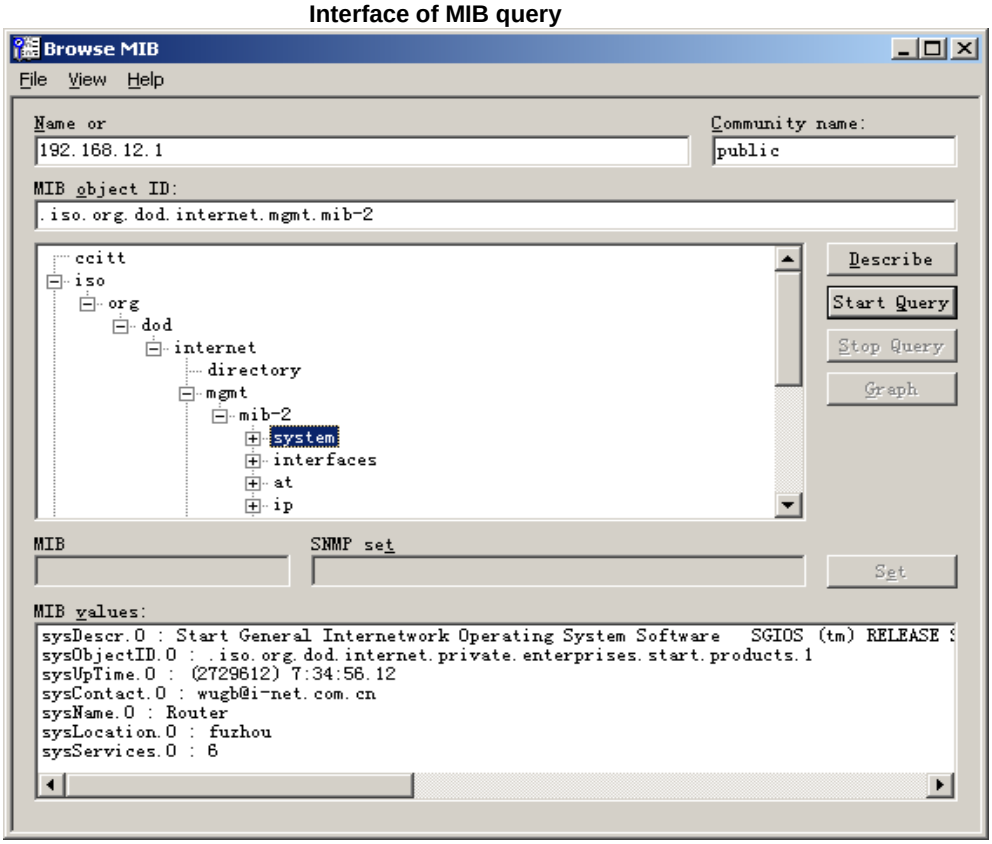
The SNMP agent is configured for the router by the above configuration. Then, the NMS can monitor and manage the router. Take HP OpenView as an example and a network topology is coming into being as follows:

Network topology diagram



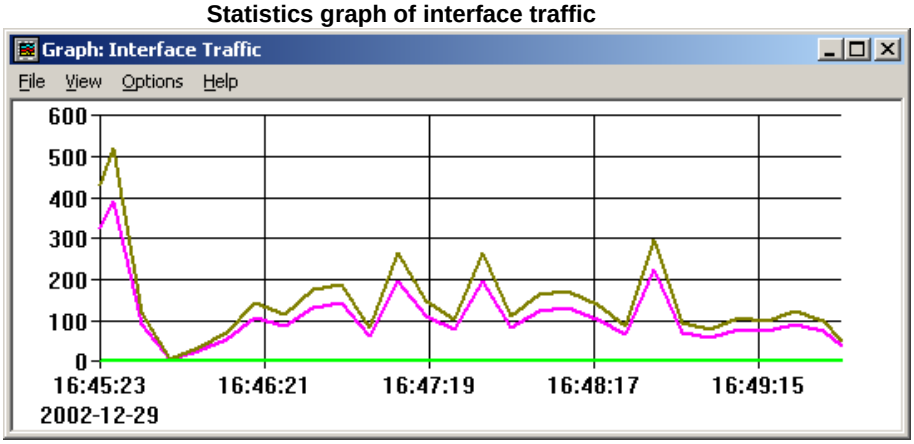
Now it is possible to query or set the management units in the network device. Click the TOOL->SNMP MIB Brower menu on the HP OpenView to display the following dialog box. Enter the IP address 192.168.12.1 in the Name field and "public" in the Community Name field. Select the specific management unit of the MIB, such as the "system" in the diagram below. Click Start Query to initiate MIB query for the network device. The results are displayed in the MIB Values pane of the dialog box.

Interface of MIB query



HP OpenView has powerful function for the network management. For example, the traffic statistics of network interface can be expressed in the form of graph. For the other functions of SNMP, see the document of network management software.

Statistics graph of interface traffic



28.4.2 Example of SNMP Access Control List Association

DES-7210 product allows the setting of access list association mode. Only the NMS allowed in the access list can monitor and manage the SNMP Agent through SNMP. This may limit NMS's accesses to the network devices and improve the SNMP security.

In the global configuration mode:

```
DES-7210(config)# access-list 1 permit 192.168.12.181
DES-7210(config)# snmp-server community public RO 1
```

Now, only the host with IP address 192.168.12.181 can monitor and manage network devices through SNMP.

28.4.3 SNMPv3 Related Configuration Examples

The following configuration allows the SNMPv3 administrator to set and view the management variables under the MIB-2 (1.3.6.1.2.1) by using the v3user as the user name through the authentication and encryption mode. The MD5 is used as the encryption method and the MD5-Auth is used as the authentication password. The DES is used for encryption and the encryption key is Des-Priv. Meanwhile, it is allowed to send the Trap message to 192.168.65.199 in the format of SNMPv3. Use v3user as the user name to send the Trap message in the authentication and encryption mode. The authentication method is MD5 and the authentication password is MD5-Auth. The DES is used for encryption and the encryption key is Des-Priv.

```
DES-7210(config)# snmp-server view v3userview 1.3.6.1.2.1 include
DES-7210 (config)# snmp-server group v3usergroup v3 priv read v3userview write v3userview
DES-7210 (config)# snmp-server user v3user v3usergroup v3 auth md5 md5-auth priv des56
des-priv
DES-7210 (config)# snmp-server host 192.168.65.199 traps version 3 priv v3user
```

29 RMON Configuration

29.1 Overview

RMON (Remote Monitoring) is a standard monitoring specification of IETF (Internet Engineering Task Force). It can be used to exchange the network monitoring data among various network monitors and console systems. In the RMON, detectors can be placed on the network nodes, and the NMS determines which information is reported by these detectors, for example, the monitored statistics and the time buckets for collecting history. The network device such as the switch or router acts as a node on the network. The information of current node can be monitored by means of the RMON.

There are three stages in the development of RMON. The first stage is the remote monitoring of Ethernet. The second stage introduces the token ring which is referred to as the token ring remote monitoring module. The third stage is known as RMON2, which develops the RMON to a high level of protocol monitor.

The first stage of RMON (known as RMON1) contains nine groups. All of them are optional (not mandatory), but some groups should be supported by the other groups.

The switch implements the contents of Group 1, 2 , 3 and 9: the statistics, history, alarm and event.

29.1.1 Statistics

Statistics is the first group in RMON. It measures the basic statistics information of each monitored subnet. At present, only the Ethernet interfaces of network devices can be monitored and measured. This group contains a statistics of Ethernet, including the discarded packets, broadcast packets, CRC errors, size block, conflicts and etc.

29.1.2 History

History is the second group in RMON. It collects the network statistics information regularly and keeps them for processing later. This group contains two subgroups:

1. The subgroup History Control is used to set such control information as sampling interval and sampling data source.
2. The subgroup Ethernet History provides history data about the network section traffic, error messages, broadcast packets, utilization, number of collision and other statistics for the administrator.

29.1.3 Alarm

Alarm is the third group in RMON. It monitors a specific management information base (MIB) object at the specified interval. When the value of this MIB object is higher than the predefined upper limit or lower than the predefined lower limit, an alarm will be triggered. The alarm is handled as an event by means of recording the log or sending the SNMP Trap message.

29.1.4 Event

Event is the ninth group in RMON. It determines to generate a log entry or a SNMP Trap message when an event is generated due to alarms.

29.2 RMON Configuration Task List

29.2.1 Configuring Statistics

One of these commands can be used to add a statistic entry.

Command	Function
DES-7210(config-if)# **rmon collection stats** *index* [**owner** *ownername*]	Add a statistic entry.
DES-7210(config-if)# **no rmon collection stats** *index*	Remove a statistic entry.

Caution

The current version of DES-7210 product supports only the statistics of Ethernet interface. The index value should be an integer between 1 to 65535. At present, at most 100 statistic entries can be configured at the same time.

29.2.2 Configuring History

One of these commands can be used to add a history entry.

Command	Function
DES-7210(config-if)# **rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	Add a history entry.
DES-7210(config-if)# **no rmon collection history** ***i****ndex*	Remove a history entry.

Caution

The current version of DES-7210 product supports only the records of Ethernet. The index value should be within 1 to 65535. At most 10 history entries can be configured.

Bucket-number: Specifies the used data source and time interval. Each sampling interval should be sampled once. The sampling results are saved. The Bucket-number specifies the maximum number of sampling. When the maximum is reached for the sampling records, the new one will overwrite the earliest one. The value range of Bucket-number is 1 to 65535. Its default value is 10.

Interval: Sampling interva in the range of 1 to 3600 seconds, 1800 seconds by default.

29.2.3 Configuring Alarm and Event

One of these command can be used to configure the alarm:

Command	Function
DES-7210(config)# **rmon alarm** *number variable interval* {**absolute | delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Add an alarm entry.
DES-7210(config)# **rmon event** *number* **[log] [trap** *community*] [**description** description-string]	Add an event entry.
DES-7210(config)# **no rmon alarm** *number*	Remove an alarm.
DES-7210(config)# **no rmon event** *number*	Remove an event.

number: Alarm index in the range of 1 to 65535.

variable: Variable to be monitored by the alarm(in integer).

interval: Sampling interval in the range of 1 to 4294967295.

Absolute: each sampling value compared with the upper and lower limits.

Delta: the difference with previous sampling value compared with the upper and lower limits.

value: Upper and lower limits.

Event-number: when the value exceeds the upper or lower limit, the event with the index of Event-number will be triggered.

Log: Record the event.

Trap: Send the Trap message to the NMS when the event is triggered.

Community: Community string used for sending the SNMP Trap message.

Description-string: Description of the event.

29.2.4 Showing RMON status

Command	Function
DES-7210(config)# **show rmon alarms**	Show alarms.
DES-7210(config)# **show rmon events**	Show events.
DES-7210(config)# **show rmon history**	Show history.
DES-7210(config)# **show rmon statistics**	Show statistics.

29.3 RMON Configuration Examples

29.3.1 Example of Configuring Statistics

If you want to get the statistics of Ethernet Port 3 , use the following commands:

```
DES-7210(config)# interface gigabitEthernet 0/3
DES-7210(config-if)# rmon collection stats 1 owner aaa1
```

29.3.2 Example of Configuring History

Use the following commands if you want to get the statistics of Ethernet Port 3 every 10 minutes:

```
DES-7210(config)# interface gigabitEthernet 0/3
DES-7210(config-if)# rmon collection history 1 owner aaa1 interval 600
```

29.3.3 Example of Configuring Alarm and Event

If you want to configure the alarm function for a statistical MIB variable, the following example shows you how to set the alarm function to the instance ifInNUcastPkts.6 (number of non-unicast frames received on port 6; the ID of the instance is 1.3.6.1.2.1.2.2.1.12.6) in ***IfEntry*** table of MIB-II. The specific function is as follows: the switch checks the changes to the number of non-unicast frames received on port 6 every 30 seconds. If 20 or more than 20 non-unicast frames are added after last check (30 seconds earlier), or only 10 or less than 10 are added, the alarm will be triggered, and event 1 is triggered to do corresponding operations (record it into the log and send the Trap with “community” name as “rmon”). The “description” of the event is “ifInNUcastPkts is too much”). The “owner” of the alarm and the event entry is “aaa1”.

```
DES-7210(config)#rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1
falling-threshold 10 1 owner aaa1
DES-7210(config)#rmon event 1 log trap rmon description "ifInNUcastPkts is too much "
owner aaa1
```

29.3.4 Example of Showing RMON Status

29.3.4.1 show rmon alarm

```
DES-7210# show rmon alarms
Alarm : 1
Interval : 1
Variable : 1.3.6.1.2.1.4.2.0
Sample type : absolute
Last value : 64
Startup alarm : 3
Rising threshold : 10
Falling threshold : 22
Rising event : 0
Falling event : 0
Owner : aaa1
```

29.3.4.2 show rmon event

```
DES-7210# show rmon events
Event : 1
Description : firstevent
Event type : log-and-trap
Community : public
```

```
Last time sent : 0d:0h:0m:0s
Owner : aaa1
Log : 1
Log time : 0d:0h:37m:47s
Log description : ipttl
Log : 2
Log time : 0d:0h:38m:56s
Log description : ipttl
```

29.3.4.3 show rmon history

```
DES-7210# show rmon history
Entry : 1
Data source : Gi1/1
Buckets requested : 65535
Buckets granted : 10
Interval : 1
Owner : aaa1
Sample : 198
Interval start : 0d:0h:15m:0s
DropEvents : 0
Octets : 67988
Pkts : 726
BroadcastPkts : 502
MulticastPkts : 189
CRCAlignErrors : 0
UndersizePkts : 0
OversizePkts : 0
Fragments : 0
Jabbers : 0
Collisions : 0
Utilization : 0
```

29.3.4.4 show rmon statistics

```
DES-7210#  show rmon statistics
Statistics : 1
Data source : Gi1/1
DropEvents : 0
Octets : 1884085
Pkts : 3096
BroadcastPkts : 161
MulticastPkts : 97
CRCAlignErrors : 0
UndersizePkts : 0
OversizePkts : 1200
Fragments : 0
Jabbers : 0
Collisions : 0
Pkts64Octets : 128
Pkts65to127Octets : 336
```

```
Pkts128to255Octets : 229
Pkts256to511Octets : 3
Pkts512to1023Octets : 0
Pkts1024to1518Octets : 1200
Owner : Zhangsan
```

30 RIP Configuration

30.1 RIP Overview

The RIP (Routing Information Protocol) is a relatively old routing protocol, which is widely used in small or homogeneous networks. The RIP uses the distance-vector algorithm, and so is a distance-vector protocol. The RIPv1 is defined in RFC 1058 and the RIPv2 is defined in RFC 2453. DES-7210 supports both two versions.

The RIP exchanges the routing information by using the UDP packets, with the UDP port number to be 520. Usually, RIPv1 packets are broadcast packets, while RIPv2 packets are multicast packets with the multicast address of 224.0.0.9. The RIP sends the update packet at the interval of 30 seconds. If the device has not received the route update packets from the peer within 180 seconds, it will mark all the routes from that device unreachable. After that, the device will delete these routes from its routing table if it still has not received any update packets from the peer within 120s.

The RIP measures the distance to the destination in hop, known as route metric. As specified in the RIP, Zero hop exists when the router directly connects to the network. One hop exists when the router connects to the network through one device and so on. Up to 16 hops are supported in a network.

The RIP-enabled device can learn the default routes from the neighbors or generate its own default route. When any of the following condition is met, DES-7210 product will generate the default route and advertise it to its neighbors by using the **default-information originate** command:

- IP Default-network is configured.
- The default routes or static default routes learnt by the routing protocol are imported into the RIP protocol.

The RIP-enabled device will send the update packets to the interface of the network it connects. If the network is not associated with the RIP routing process, the interface will not advertise any update packets. The RIP is available in two versions: RIPv1 and RIPv2. The RIPv2 supports plain-text authentication, MD5 cryptographic text and variable length subnet mask.

DES-7210 RIP offers Split Horizon to avoid a loop.

30.2 RIP Configuration Task List

The RIP configuration task list contains:

- Create the RIP routing process (required)
- Configure the RIP Update Packets in Unicast Form (optional)
- Configure Split Horizon (optional)
- Define the RIP Version (optional)
- Configure the Route Aggregation (optional)
- Configure RIP Authentication (optional)
- Adjust the RIP Timer (optional)

- Configure the RIP Route Source Address Validation (optional)
- Control RIP interface status (optional)
- Configure RIP default route notification on the interface (optional)
- Configure RIP VRF (optional)

For the following topics, refer to the chapter *IP Routing Protocol Independent Feature Configuration*.

- Filter RIP route information
- Route redistribution
- Default route distribution configuration

30.2.1 Creating the RIP Routing Process

For the router to run the RIP, you must first create the RIP routing process and define the network associated with the RIP routing process.

To create the RIP routing process, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **router rip**	Create the RIP routing process.
DES-7210(config-router)# **network** *network-number wildcard*	Define the associated network.

You can configure the *network-number* and *wildcard* parameter at the same time to enable the network segment within the configured address range to run RIP.

If the parameter *wildcard* is not configured, by default, the DES-7200 series will enable the network segment within the class address range to run RIP.

Note

There are two meanings for the associated network defined by the **network** command:

1. The RIP only notifies the route information of the associated network to the outside.
2. The RIP only notifies the route information to the interfaces belonging to the associated network.

30.2.2 Configuring the RIP Update Packet in Unicast Form

The RIP is usually a broadcast protocol. If the RIP route information needs to be transmitted across the non-broadcast networks, you need to configure the router so that it supports the RIP to advertise the route update packets in unicast form.

To configure advertising the update packet in unicast form, execute the following commands in the RIP routing process configuration mode:

Command	Function
DES-7210(conf-router)# **neighbor** *ip-address*	Advertise the RIP update packet in unicast form.

By using this command, you can also control which port is allowed to advertise the RIP route update packets, restrict a port from advertising the broadcast route update packets. You need to configure the **passive-interface** command in the routing process configuration mode. For the related description about the route information advertisement restriction, see

the “Route Filtering Configuration” section in the *IP Routing Protocol Independent Feature Configuration* chapter.

Note

When you configure the FR and X.25, if the **Broadcast** keyword is specified during address mapping, you do not need to configure the **neighbor** command. The **neighbor** command is largely reflected in reducing broadcast packets and filtering routes.

30.2.3 Configuring Split Horizon

Split horizon can be used to avoid loop in the environment where multiple devices running distance-vectortype routing protocols connect to a network in which IP packets are broadcasted. Split horizon can prevent the router from advertising some route information through the port from which it learns such information. This optimizes the route information exchange among multiple routers.

However, split horizon may cause the failure of some routers to learn all the routes in a non-broadcast multi-access network (for example, frame relay, X.25). In this case, you may need to disable split horizon. If a port is configured with the secondary IP address, you also need to pay attention to the split horizon problem.

To enable or disable split horizon, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **no ip split-horizon**	Disable split horizon.
DES-7210(config-if)# **ip split-horizon**	Enable split horizon.

By default, split horizon is enabled on all interfaces.

30.2.4 Defining the RIP Version

DES-7210 product supports RIP version 1 and version 2, where RIPv2 supports authentication, key management, route convergence, CIDR and VLSMs. For the information about the key management and VLSMs, see the *IP Routing Protocol Independent Feature Configuration* chapter.

By default, DES-7210 product can receive RIPv1 and RIPv2 packets, but it can only send RIPv1 packets. You can configure it to receive and send only RIPv1 packets or RIPv2 packets.

To receive and send the packets of a specific version, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210(config-router)# **version** {**1** | **2**}	Defining the RIP Version.

The above command allows the software to receive or send only the packets of the specified version. If needed, you can modify the default setting of every port.

To configure a port to send only the packets of a specific version, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip rip send version 1**	Specify to send the packets of only RIPv1
DES-7210(config-if)# **ip rip send version 2**	Send the packets of only RIPv2.

Command	Function
DES-7210(config-if)# **ip rip send version 1 2**	Send the packets of RIPv1 and RIPv2.

To configure a port to receive only the packets of a specific version, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip rip receive version 1**	Receive the packets of only RIPv1.
DES-7210(config-if)# **ip rip receive version 2**	Receive the packets of only RIPv2.
DES-7210(config-if)# **ip rip receive version 1 2**	Receive the packets of RIPv1 and RIPv2.

30.2.5 Configuring the Route Aggregation

The automatic route aggregation of the RIP means that the routes of subnets are automatically aggregated into the routes of a classful network when they pass through the border of the classful network. By default, the RIPv2 will automatically perform route aggregation, while the RIPv1 does not support this feature.

The automatic route aggregation function of the RIPv2 enhances the scalability and effectiveness of the network. If there are any aggregated routes, the sub-routes contained in them cannot be seen in the routing table. This greatly reduces the size of the routing table.

It is more efficient to advertise the aggregated routes than the separated routes. There are the following factors:

- Aggregated routes will be handled first when you search the RIP database.
- Any sub-routes will be ignored will you search the RIP database, and thus reducing the processing time.

Sometimes, you want to learn the specific sub-net routes rather than only viewing the aggregated routes. In this case,you should disable the automatic route aggregation function.

To configure automatic route aggregation, execute the following commands in the RIP routing process mode:

Command	Function
DES-7210(config-router)# **no auto-summary**	Disable automatic route aggregation.
DES-7210(config-router)# **auto-summary**	Enable automatic route aggregation.

After the automatic route aggregation is disabled, you can configure the route aggregation of IP addresses or subnets on an interface by executing the following command in the interface mode:

Command	Function
DES-7210(config-if)# **ip summary-address rip** *ip-address ip-network-mask*	Enable route aggregation on the interface.
DES-7210(config-if)# **no ip summary-address rip** *ip-address ip-network-mask*	Disable route aggregation on the interface.

30.2.6 Configuring RIP Authentication

The RIPv1 does not support authentication. If the router is configured with the RIPv2, you can configure authentication on the appropriate interface.

DES-7210 product supports two RIP authentication modes: plain-text authentication and MD5 authentication. The default is plain-text authentication.

Use the **ip rip authentication text-password** command to configure the plain-text authentication password string, or associate the key chain to obtain the plain-text authentication password string. The latter takes precedence over the former.

The key chain must be associated for the MD5 authentication.

For the plain-text authentication, no authentication action occurs if the plain-text authentication password string or key chain association is not configured, or the key chain is not configured although it has been associated. Similarly, for the MD5 authentication, no authentication action occurs if the key chain association is not configured, or the key chain is not configured although it has been associated.

To configure RIP authentication, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip rip authentication mode** {**text** | **md5**}	1.1.1.1.4 Configure the RIP authentication on the interface. 1.1.1.1.5 Text : plain-text authentication 1.1.1.1.6 Md5 : MS5 authentication .

Command	Function
DES-7210(config-if)# **ip rip authentication text-password** *password-string*	1.1.1.1.7 Configure the plain-text authentication password string, in the length of 1-16 bytes.
DES-7210(config-if)# **ip rip authentication key-chain** *key-chain-name*	1.1.1.1.8 Configure the authentication using key chain.

30.2.7 Adjusting the RIP Timer

The RIP provides the timer adjustment function, which allows you to adjust the timer so that the RIP routing protocol can run in a better way. You can adjust the following timers:

Route update timer: It defines the interval in seconds for the router to send the RIP update packets;

Route invalid timer: It defines the time in seconds after which the routes in the routing table will become invalid if not updated;

Route clearing timer: It defines the time in seconds after which the routes in the routing table will be cleared;

By adjusting the above timers, you can accelerate the aggregation and fault recovery of the routing protocol. To adjust the RIP timers, execute the following commands in the RIP routing process configuration mode:

Command	Function
DES-7210(config-router)# **timers basci** *update invalid flush*	Adjust the RIP timers.

By default, the update interval is 30 seconds, the invalid period is 180 seconds, and the clearing (flush) period is 120 seconds.

Note

The routers connected in the same network must have the same RIP timers.

30.2.8 Configuring the RIP Route Source IP Address Validation

By default, the RIP will validate the source addresses of the incoming route update packets. The RIP will discard the packets from invalid source IP address. Whether a source IP address is valid or not depends on if the source IP address is in the same network as the IP address of the interface. No validation will be performed on the interface of no IP address.

To configure route source IP address validation, execute the following commands in the RIP routing process configuration mode:

Command	Function
DES-7210(config-router)# **no validate-update-source**	Disable the source IP address validation.
DES-7210(config-router)# **validate-update-source**	Enable the source IP address validation.

30.2.9 RIP Interface Status Control

In some condition, it is necessary to configure the RIP operation flexibly. If you only hope the device to learn the RIP routes, but not carry out the RIP route notification, you can configure the passive interface. Or, if you hope to configure the status of some interface individually, you can use a command to control the sending or receiving of the RIP packets on an interface.

To configure some interface as the passive mode, execute the following command in the RIP route processing configuration mode:

Command	Function
DES-7210(config-router)# **passive-interface {default** | *interface-type interface-num*}	Set the interface to passive.
DES-7210(config-router)#**no passive-interface {default** | interface-type interface-num}	Remove the configuration.

Note

The passive interface responds the non-RIP requests (such as the route diagnosis program) rather than the RIP requests, because these request programs hope to understand the routes of all devices.

To disable or allow some interface to receive the RIP message, execute the following command in the interface configuration mode:

Command	Function
DES-7210(config-if)# no ip rip receive enable	Disable the interface to receive the RIP message.
DES-7210(config-if)# **ip rip receive enable**	Allow the interface to receive the RIP message.

To disable or allow some interface to send the RIP message, execute the following command in the interface configuration mode:

Command	Function

Command	Function
DES-7210(config-if)# **no ip rip send enable**	Disable the interface to send the RIP message.
DES-7210(config-if)# **ip rip send enable**	Allow the interface to send the RIP message.

30.2.10 Configuring RIP Default Route Notification on the Interface

Use the following command to generate a default route (0.0.0.0/0) in the update message on a specified interface in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip rip default-information originate** [**metric** *metric-value*]	1.1.1.1.9 Notify the default route and other routes.
DES-7210(config-if)# **no ip rip default-information**	1.1.1.1.10 Cancel the default route notification on the interface.

In the interface configuration mode, use the following command to generate a default route (0.0.0.0/0) in the update message on a specified interface, and enable this interface only to notify this default route.

Command	Function
DES-7210(config-if)# **ip rip default-information only** [**metric** *metric-value*]	1.1.1.1.11 Notify the default route only.
DES-7210(config-if)# **no ip rip default-information**	1.1.1.1.12 Cancel the default route notification on the interface.

Note

With both the **ip rip default-information** command on the interface and the **default-information originate** command in the RIP process configured, only notify the default route configured on the interface.

30.2.11 Configuring RIP VRF

The RIP supports VRFs. Multiple RIP instances can be created to manage the corresponding VRFs in the RIP process. By default, there is only one RIP instance in the RIP process, which is used to manage the global routing table. After a VRF is created, you can manage the routing table of the VRF by creating a new RIP instance.

Execute the **address-family** command to enter the address family configuration mode (with the prompt (config-router-af)#). When you specify the VRF associated with the sub mode at the first time, the RIP will create the a RIP instance corresponding to the VRF. Under this mode, you can configure the RIP route information of the VRF in the same way as that in global route configuration mode.

To exit the address family configuration sub mode and return to the route configuration mode, execute the **exit-address-family** command or the **exit** command.

To configure the RIP instance managng the VRF, execute the following command in the RIP route processing configuration mode:

Command	Function
DES-7210(config-router)# **address-family ipv4 vrf** *vrf-name*	Create the RIP instance managing the VRF.
DES-7210(config-router)#**no address-family ipv4 vrf** *vrf-name*	Remove the RIP instance managing the VRF.

30.3 RIP Configuration Examples

This section provides four RIP configuration examples:

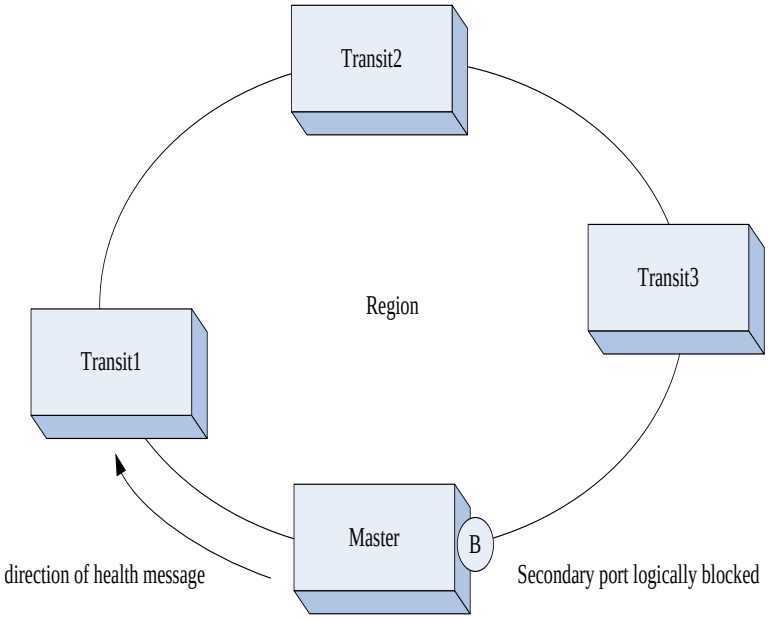
- Example of Configuring Split Horizon
- Example of Configuring RIP Authentication
- Example of configuring the RIP packet in unicast form
- Example of configuring RIP VRF

30.3.1 Example of Configuring Split Horizon

- **Configuration requirements:**

There are five devices. Where, Router A, Router D and Router E are connected via the Ethernet; Router A, Router B and Router C are connected via the frame relay. 0shows IP address distribution and equipment connection, where RouterD is configured with a sub-address.

Figure-1 Example of Configuring RIP Split Horizon



The route should be configured to achieve the following purposes:

1) All routers run the RIP protocol;

2) Router B and Router C can learn the network segment routes advertised to each other;

3) Router E can learn the routes of 192.168.12.0/24.

- **Detailed configuration**

In this example, to achieve the above purposes, Router A and Router D must have split horizon disabled. Otherwise, Router A will not notify the routes advertised by Router B to Router C. Neither will Router D advertise the rotues of 192.168.12.0 to Router E. Detailed configurations of each device are listed as follows.

Router A Configuration:

Configure the Ethernet interface.

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

Configure the WAN port.

```
interface Serial1/0
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
no ip split-horizon
```

Configure the RIP route.

```
router rip
version 2
network 192.168.12.0
network 192.168.123.0
```

Router B Configuration:

#Configure the Ethernet interface.

```
interface FastEthernet0/0
ip address 172.16.20.1 255.255.255.0
```

#Configure the WAN port.

```
interface Serial1/0
ip address 192.168.123.2 255.255.255.0
encapsulation frame-relay
```

#Configure the RIP protocol.

```
router rip
version 2
network 172.16.0.0
network 192.168.123.0
no auto-summary
```

Router C configuration:

Configure the Ethernet interface.

```
interface FastEthernet0/0
ip address 172.16.30.1 255.255.255.0
```

Configure the WAN port.

```
interface Serial1/0
ip address 192.168.123.3 255.255.255.0
encapsulation frame-relay
```

Configure the RIP protocol.

```
router rip
version 2
network 172.16.0.0
network 192.168.123.0
no auto-summary
```

Router D configuration:

Configure the Ethernet interface.

```
interface FastEthernet0/0
ip address 192.168.12.4 255.255.255.0
ip address 192.168.13.4 255.255.255.0 secondary
no ip split-horizon
```

Configure the RIP protocol.

```
router rip
version 2
network 192.168.12.0
network 192.168.13.0
```

Router E configuration:

Configure the Ethernet interface.

```
interface FastEthernet0/0
ip address 192.168.13.5 255.255.255.0
```

Configure the RIP protocol.

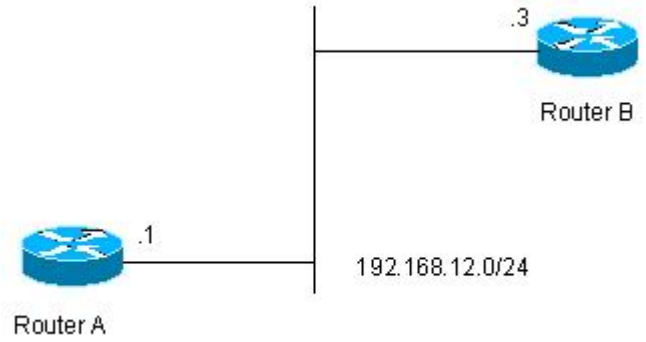
```
router rip
version 2
network 192.168.13.0
```

30.3.2 Example of Configuring RIP Authentication

- **Configuration requirements:**

Two routers are connected via the Ethernet and run the RIP protocol and MD5 for authentication. The connection diagram of the devices and the assignment of IP addresses are shown in Figure-2.

Figure-2 Example of Configuring RIP Authentication



Router A must send RIP packets with the authentication key of keya and can receive the RIP packets whose authentication keys are keya and keyb. Router B sends the RIP packets with the authentication key of keyb and can receive the RIP packets of the authentication keys of keya and keyb.

- **Detailed configuration of devices**

Router A configuration:

#Configure the key chain.

```
key chain ripkey
key 1
key-string keya
accept-lifetime infinite
send-lifetime 00:00:00 Dec 3 2000 infinite
key 2
key-string keyb
accept-lifetime infinite
send-lifetime 00:00:00 Dec 3 2000 infinite
```

Configur the Ethernet interface.

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
ip rip authentication mode md5
ip rip authentication key-chain ripkey
```

Configur the RIP protocol.

```
router rip
version 2
```

```
network 192.168.12.0
```

Router B Configuration:

#Configure the key chain.

```
key chain ripkey
key 1
key-string keyb
accept-lifetime 00:00:00 Dec 3 2000 infinite
send-lifetime 00:00:00 Dec 4 2000 00:00:00 Dec 5 2000
key 2
key-string keya
accept-lifetime 00:00:00 Dec 3 2000 infinite
send-lifetime 00:00:00 Dec 4 2000 infinite
```

Configure the Ethernet interface.

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
ip rip authentication mode md5
ip rip authentication key-chain ripkey
```

Configure the RIP protocol.

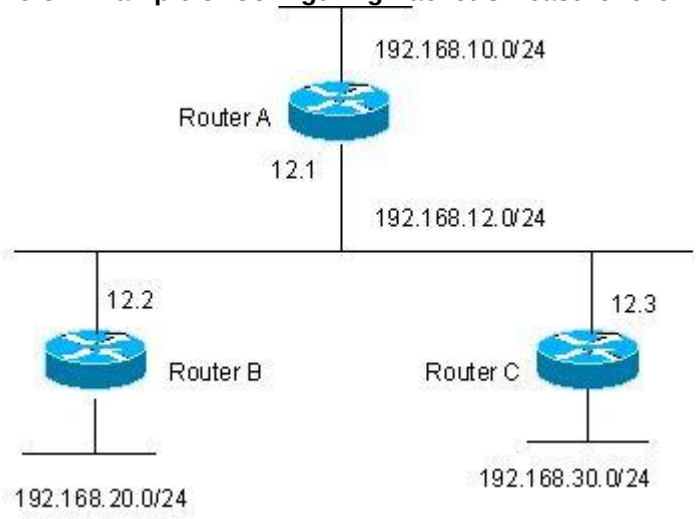
```
router rip
version 2
network 192.168.12.0
```

30.3.3 Example of Configuring the RIP Packets in Unicast Form

- **Configuration requirements:**

All the three routers are connected on the LAN, and all run the RIP protocol. Figure-3 shows the IP address allocation and connection of the equipment.

Figure-3 Example of Configuring Packet Unicast for the RIP



Following are to be implemented via the configuration of RIP message in unicast form:

1. Router A can learn the routes advertised by Router C.

Router C cannot learn the routes advertised by Router A.

- **Detailed configuration of devices**

To achieve the above purposes, RIP packet unicast must be configured at router A.

Router A configuration

Configure the Ethernet interface.

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#Configure the loopback port.

```
interface Loopback0
ip address 192.168.10.1 255.255.255.0
```

Configure the RIP protocol.

```
router rip
version 2
network 192.168.12.0
network 192.168.10.0
passive-interface FastEthernet0/0
neighbor 192.168.12.2
```

Router B configuration:

Configure the Ethernet interface.

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configure the loopback port.

```
interface Loopback0
ip address 192.168.20.1 255.255.255.0
```

Configure the RIP protocol.

```
router rip
version 2
network 192.168.12.0
network 192.168.20.0
```

Router C Configuration:

Configur the Ethernet interface.

```
interface FastEthernet0/0
ip address 192.168.12.3 255.255.255.0
```

#Configure the loopback port.

```
interface Loopback0
ip address 192.168.30.1 255.255.255.0
```

Configure the RIP protocol.

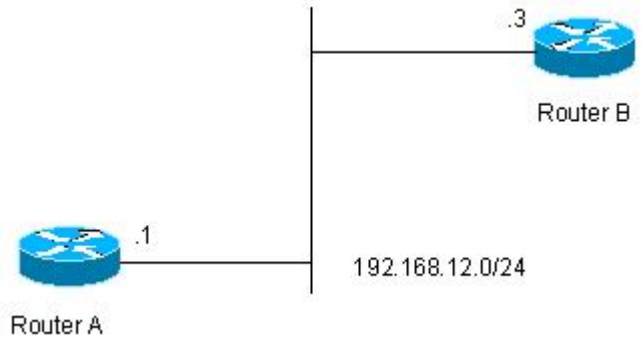
```
router rip
version 2
network 192.168.12.0
network 192.168.30.0
```

30.3.4 Example of Configuring RIP VRF

- **Configuration requirements:**

Two devices running RIP are connected to each other. Figure-4 shows IP address distribution and equipment connection.

Figure-4 Example of Configuring RIP VRF



With RIP, routing information is exchanged between the redvpn VRF of Router A and the bluevpn VRF of Router B.

- **Detailed configuration**

Router A Configuration:

create a VRF.

```
ip vrf redvpn
```

Bind the VRF to the interface and configure an IP address for the interface.

```
interface FastEthernet 1/0
```

```
ip vrf forwarding redvpn
ip address 192.168.12.1 255.255.255.0
```

Configure the RIP and create an RIP instance.

```
router rip
address-family ipv4 vrf redvpn
network 192.168.12.0
exit-address-family
```

Router B Configuration:

create a VRF.

```
ip vrf bluevpn
```

Bind the VRF to the interface and configure an IP address for the interface.

```
interface FastEthernet 1/0
ip vrf forwarding bluevpn
ip address 192.168.12.3 255.255.255.0
```

Configure the RIP and create an RIP instance.

```
router rip
address-family ipv4 vrf bluevpn
network 192.168.12.0
exit-address-family
```

31 OSPF Configuration

31.1 OSPF Overview

OSPF (Open Shortest Path First) is an internal gateway routing protocol based on link status developed by the IETF OSPF work group. OSPF, a routing protocol specific for IP, directly runs on the IP layer. Its protocol number is 89. OSPF packets are exchagned in multicast form using the multicast address 224.0.0.5 (for all OSPF routers) and 224.0.0.6 (for specified routers).

The link status algorithm is an algorithm totally different from the Huffman vector algorithm (distance vector algorithm). The RIP is a traditional routing protocol that uses the Huffman vector algorithm, while the OSPF protocol is the typical implementation of the link status algorithm. Compared with the RIP routing protocol, the OSPF uses a different algorithm, and also introduces the new concepts such as route update authentication, VLSMs, and route aggregation. Even if the RIPv2 has made great improvements, and can support the features such as route update authentication and VLSM, the RIP protocol still has two fatal weaknesses: 1) slow convergence; 2) limited network size, with the maximum hot count of no more than 16. The OSPF is developed to overcome these weaknesses of the RIP, making the IGP protocol applicable for large and complicated network environments.

The OSPF protocol establishes and calculates the shortest path to every destination network by using the link status algorithm. This algorithm is complicated. The following briefly describes how the link status algorithm works:

- In the initialization stage, a router will generate a link status notification including the status of all its links.
- All routers exchange the link status message in the multicast way. Upon receiving the link status update message, each router will copy it to its local database and then transmit it to other routers.
- When every router has a complete link status database, the router uses the Dijkstra algorithm to calculate the shortest path trees to all the target networks. The results include destination network, next-hop address, and cost, which are the key parts of the IP routing table.

If there is no link cost or network change, the OSPF will become silent. If any changes occur on the network, the OSPF advertises the changes via the link status message of only the changed links. The routers involved in the changes will have the Dijkstra algorithm run again, with a new shortest path tree created.

A group of routers running the OSPF protocol form the autonomous domain system of the OSPF routing domain. An autonomous domain system consists of all the routers that are controlled and managed by one organization. Within the autonomous domain system, only one IGP routing protocol is run. However, between multiple such systems, the BGP routing protocol is used for route information exchange. Different autonomous domain systems can use the same IGP routing protocol. To access the Internet, every autonomous system needs to request the related organization for the autonomous system number.

When the OSPF routing domain is large, the hierarchical structure is usually used. In other words, the OSPF routing domain is divided into several areas, which are connected via a

backbone area. Every non-backbone area must be directly connected with this backbone area.

There are three roles for the routers in the OSPF routing domain according to their deployment position:

1) Area Internal Routers, all interface networks of this router are of this area;
2) ABR (Area Border Router): The interfaced networks of this router belong at least to two areas, one of which must be the backbone area;
3) ASBR (Autonomous System Boundary Routers): It is the router between which the OSPF route domain exchanges the external route domain.

DES-7210 product implements the OSPF by fully complying with the OSPFv2 defined in RFC 2328. The main features of the OSPF are described as below:

1) Support multiple OSPF processes, up to 64 OSPF processes running at the same time.
2) Support VRF. You can run OSPF based on different VRFs.
3) Support the definition of stubby area.
4) Support route redistribution with the static route, directly-connected route and the dynamic route protocol such as RIP, BGP, ect.
5) Support plain-text or MD5 authentication between neighbors.
6) Support virtual links.
7) Support VLSMs.
8) Support area division
9) Support NSSA (Not So Stubby Area), as defined in RFC 3101.
10) Support Graceful Restart, as defined in RFC 3623.

Caution

DES-7210 switches do not support the following functions now:

OSPF requied line support ,as defined in RFC 1793;

OSPF rapid convergence.

31.2 OSPF Configuration Task List

The configuration of OSPF should be cooperated with various routers (including internal routers, area boundary routers and autonomous system boundary routers). When no configuration is performed, the defaults are used for various parameters of the routers. In this case, packets are sent and received without authentication, and an interface does not belong to any area of an autonomous system. When you change the default parameters, you must ensure that the routers have the same configuration settings.

To configure the OSPF, you must perform the following tasks. Among them, activating the OSPF is required, while others are optional, but may be required for particular applications. The steps to configure the OSPF protocols are described as below:

- Creating the OSPF Routing Process (required)
- Configuring the OSPF Interface Parameters (optional)
- Configuring the OSPF to Accommodate Different Physical Networks (optional)
- Configuring the OSPF Area Parameters (optional)
- Configuring the OSPF NSSA (optional)
- Configuring the Route Aggregation between OSPF Areas (optional)
- Creating the Virtual Links (optional)

- Creating the Default Routes (optional)
- Using the Loopback Address as the Route ID (optional)
- Changing the OSPF Default Management Distance (optional)
- Configuring the Route Calculation Timer (optional)
- Configuring the LSA Group Pacing Timer (optional)
- Configuring the OSPF Interface Cost Value (optional)
- Configuring whether to Check the MTU Value When the Interface Receives the Database Description Packets (optional)
- Disabling an Interface to Send the OSPF Packets (optional)
- Configuring the OSPF Load Protection (optional)
- Configuring the OSPF Network Management (optional)

For the detailed configuration about the following topics, see the chapter in *Protocol-Independent Configuration*.

- Filter the route information
- Route redistribution

The default OSPF configuration is shown as below:

Interface parameters	Interface cost: none is preset LSA retransmit interval: 5 seconds. LSA transmit delay: 1 second. Hello message transmit interval : 10 seconds (30 seconds for non-broadcast networks) Failure time of adjacent routers: 4 times the hello interval. Priority: 1 Authentication type: 0 (No authentication). Authentication password: None.
Area	Authentication type :0 (No authentication). Default metric of aggregated routes to Stub or NSSA area: 1 Inter-area aggregation scope: Undefined Stub area: Undefined NSSA: Undefined
Virtual Link	No virtual link is defined. The default parameters of the virtual link are as below: LSA retransmit interval: 5 seconds. LSA transmit delay: 1 second. Hello message interval: 10 seconds. Failure time of adjacent routers: 4 times the hello interval. Authentication type: No authentication. Authentication password: No password specified.
Automatic cost calculation	Enabled automatically; Default automatic cost is 100Mbps
Default route generation	Disabled The default metric will be 1 and the type is type-2.
Default metric (Default metric)	The default metric is used to redistribute the other routing protocols;
Management Distance	Intra-area route information:110 Inter-area route information:110 External route information:110
Database filter	Disabled. All interfaces can receive the status update message (LSA).

Neighbor change log	Enabled
Neighbor	N/A
Neighbor database filter Disabled.	All outgoing LSAs are sent to the neighbor.
network area (network area)	N/A
Device ID	Undefined; the OSPF protocol does not run by default
Route summarization (summary-address)	Undefined
Changing LSAs Group Pacing	240 seconds
Shortest path first (SPF) timer	The time between the receipt of the topology changes and SPF-holdtime: 5 seconds The least interval between two calculating operations: 10 seconds
Optimal path rule used to calculate the external routes	Using the rules defined in RFC1583
OSPF overflow memory-lack	Enter the overflow state when the memory lacks. GR restarter: disabled. GR helper:enabled.
OSPFv2 MIB binding	In the OSPFv2 process in the smallest process number.
OSPFv2 TRAP sending	Disabled

31.2.1 Creating the OSPF Routing Process

This is to create the OSPF routing process and define the range of the IP addresses associated with the OSPF routing process and the OSPF area to which these IP addresses belong. The OSPF routing process only sends and receives the OSPF packets at the interface within the IP address range and advertises the link status of the interface to the outside. Currently, 64 OSPF routing process are supported.

To create the OSPF routing process, you can perform the following steps:

Command	Meaning
DES-7210 # **configure terminal**	Enter the global configuration mode.
DES-7210 (config)**# ip routing**	Enable the IP routing (if disabled).
DES-7210(config)# **router ospf** *process-id* [**vrf** *vrf-name*]	Enable OSPF and enter OSPF route configuration mode.
DES-7210 (config-router)**# network** *address wildcard-mask* **area** *area-id*	Define an IP address range for an area.
DES-7210 (config-router)**# End**	Return to the privileged EXEC mode.
DES-7210 # **show ip protocol**	Display the routing protocol that is running currently.
DES-7210 # **write**	Save the configuration.

Note

The parameter vrf *vrf-name* is used to specify the VRF which the OSPF belongs to. If you do not specify the parameter in the OSPF process, it belongs to the default VRF. For the **network** command, 32 bit wildcards are opposed to the mask, where 1 means not to compare the bit and 1 means to compare the bit. However, if you configure the command with mask, DES-7210 products will automatically translate it into a bit wildcard. An interface belongs to the specific area as long as it matches the IP address range defined by the **network** command. When an interface matches more than one IP address range defined by the **network** command in multiple OSPF processes, the OSPF process that the interface takes part in is determined in the way of optimal match.

To disable the OSPF protocol, use the **no router ospf** [*process-id*]command. The example shows how to enable the OSPF protocol:

```
DES-7210(config)# router ospf 1
DES-7210 (config-router)# network 192.168.0.0 255.255.255.0 area 0
DES-7210 (config-router)# end
```

31.2.2 Configuring the OSPF Interface Parameters

The OSPF allows you to change some particular interface parameters. You can set such parameters as needed. It should be noted that some parameters must be set to match those of the adjacent router of the interface. These parameters are set via the **ip ospf hello-interval**, **ip ospf dead-interval**, **ip ospf authentication**, **ip ospf authentication-key** and **ip ospf message-digest-key**. When you use these commands, you should make sure that the adjacent routers have the same configuration.

To configure the OSPF interface parameters, execute the following commands in the interface configuration mode:

Command	Meaning
DES-7210 # **configure terminal**	Enter the global configuration mode.
DES-7210 (config)**# ip routing**	Enable the IP routing (if disabled).
DES-7210 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210 (config-if)# **ip ospf cost** *cost-value*	(Optional) Define the interface cost.
DES-7210(config-if)# **ip ospf retransmit-interval** *seconds*	(Optional) Set the link status retransmission interval.
DES-7210 (config-if)**# ip ospf transmit-delay** *seconds*	(Optional) Set the transmit delay for the link status update packets.
DES-7210 (config-if)**# ip ospf hello-interval** *seconds*	(Optional) Set the hello message send interval, which must be the same for all the nodes of the entire network.
DES-7210 (config-if)**# ip ospf dead-interval** *seconds*	(Optional) Set the dead interval for the adjacent router, which must be the same for all the nodes of the entire network.
DES-7210 (config-if)# **ip ospf priority** number	(Optional) The priority is used to select the dispatched routers (DR) and backup dispatched routers (BDR).
DES-7210 (config-if)# **ip ospf authentication** [**message-digest | null**]	(Optional) Set the authentication type on the network interface.
DES-7210 (config-if)# **ip ospf authentication-key** *key*	(Optional) Configure the key for text authentication of the interface.

Command	Meaning
DES-7210 (config-if)#**ip ospf message-digest-key** *keyid* **md5** *key*	(Optional) Configure the key for MD5 authentication of the interface.
DES-7210 (config-if)#**ip ospf database-filter all out**	(Optional) Prevent the interfaces from flooding the LSAs packets. By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives.
DES-7210 (config-if)#**end**	Return to the privileged EXEC mode.
DES-7210 #**show ip ospf** [*process-id*] **interface** [*interface-id*]	Display the routing protocol that is running currently.
DES-7210 # **write**	(Optional) Save the configuration.

You can use the **no** form of the above commands to cancel or restore the configuration to the default.

31.2.3 Configuring the OSPF to Accommodate Different Physical Networks

According to the transmission nature of different media, the OSPF divides the networks into three types:

- Broadcast network (Ethernet, token network, and FDDI)
- Non-broadcast network (frame relay, X.25)
- Point-to-point network (HDLC, PPP, and SLIP)

The non-broadcast networks include two sub-types according to the operation modes of the OSPF:

1) One is the Non-broadcast Multi-access (NBMA) network. The NBMA requires direct communication for all routers interconnected. Only fully meshed networks can meet this requirement. If the SVC (for example, X.25) connection is used, this requirement can be met. However, if the PVC (for example, frame relay) networking is used, there will be some difficulty in meeting this requirement. The operation of the OSPF on the NBMA network is similar to that on the broadcast network: One Designated Router must be elected to advertise the link status of the NBMA network.
2) The second is the point-to-multipoint network type. If the network topology is not a fully meshed non-broadcast network, you need to set the network type of the interface to the point-to-multipoint network type for the OSPF. In a point-to-multipoint network type, the OSPF takes the connections between all routers as point-to-point links, so it does not involve the election of the designated router.

Whatever the default network type of the interface, you must set it to the broadcast network type. For example, you can set the non-broadcast multi-access network (frame relay, X.25) to a broadcast network. This spares the step to configure the neighbor when you configure the OSPF routing process. By using the **X.25 map** and **Frame-relay map** commands, you can allow X.25 and frame relay to have the broadcast capability, so that the OSPF can see the networks like X.25 and frame relay as the broadcast networks.

The point-to-multipoint network interface can be seen as the marked point-to-point interface of one or multiple neighbors. When the OSPF is configured as the point-to-multipoint network type, multiple host routes will be created. The point-to-multipoint network has the following advantages over the NBMA network:

- Easy configuration without the configuration of neighbors or the election of the designated router.
- Small cost without the need of fully meshed topology

To configure the network type, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip ospf network {broadcast | non-broadcast | point-to-point | {point-to-multipoint [non-broadcast]} }**	Configure the OSPF network type.

For different link encapsulation types, the default network type is shown as below:

- Point-to-point network type
  PPP, SLIP, frame relay point-to-point sub-interface, X.25 point-to-point sub-interface encapsulation
- NBMA (non-broadcast) network type
  Frame relay, X.25 encapsulation (except point-to-point sub-interface)
- Broadcast network type
  Ethernet encapsulation

The default type is not the point-to-multipoint network type

It should be noted that the network type should be consistent at both sides. Otherwise, the abnormality will occur, for instance, the neighbor is Full and the calculation of the routing is incorrect.

31.2.3.1 Configuring Point-to-Multipoint Broadcast Network

When routers are connected via X.25 and frame relay networks, if the network is not a fully meshed network or you do not want the election of the designated router, you can set the network type of the OSPF interface as the point-to-multipoint type. Since the point-to-multipoint network sees the link as a point-to-point link, multiple host routes will be created. In addition, all the neighbors have the same cost in the point-to-multiple networks. If you want to make different neighbors have different costs, you can set them by using the **neighbor** command.

To configure the point-to-multipoint network type, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip ospf network point-to-multipoint**	Configure the point-to-multipoint network type for an interface.
DES-7210(config-if)# **exit**	Exit to the global configuration mode.
DES-7210(config)# **router ospf 1**	Enter the routing process configuration mode.
DES-7210(config-router)# **neighbor** *ip-address* **cost** *cost*	Specify the cost of the neighbor (optional).

Note

Although the OSPF point-to-point network is a non-broadcast network, it can allow non-broadcast networks to have broadcast capability by using the frame relay, X.25 mapping manual configuration or self-learning. Therefore, you do not need to specify neighbors when you configure the point-to-multipoint network type.

31.2.3.2 Configuring Non-broadcast Network

When the OSPF interface works in the non-broadcast network, you can configure it to the NBMA or the point-to-multipoint non-broadcast type. Since it cannot dynamically discover

neighbors without the broadcast capability, you must manually configure neighbors for the OSPF interface working in the non-broadcast network.

You can configure the NBMA network type in the following conditions:

1. When a non-broadcast network has the fully meshed topology;
2. You can set a broadcast network as the NBMA network type to reduce the generation of the broadcast packets and save the network bandwidth, and also avoid arbitrary reception and transmission of routers by some degree. The configuration of the NBMA network should specify the neighbor. For there is the choice to specify the routers, you should determine which router is the designated router. For this reason, it is necessary for you to prioritize rotuers. The higher the router's pirority is, the higher possibility of being the designated router is.

To configure the NBMA network type, execute the following commands in the interface configuration mode:

Command	Function
DES-7210 (config-if)# **ip ospf network non-broadcast**	Specify the network type of the interface to be the NBMA type.
DES-7210 (config-if)# **exit**	Exit to the global configuration mode.
DES-7210 (config)# **router ospf 1**	Enter the routing process configuration mode.
DES-7210(config-router)# **neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*]	Specify the neighbor, its priority and polling interval of Hello messages.

In a non-broadcast network, if it cannot ensure that any two routers are in direct connection, the better solution is to set the network type of the OSPF to the point-to-multipoint non-broadcast network type.

Whether in a point-to-multipoint broadcast or non-broadcast network, all the neighbors have the same cost, which is the value set by using the **ip ospf cost** command. However, the bandwidths of the neighbors may be actually different, so the costs should be different. Therefore, you can specify the necessary cost for each neighbor by using the **neighbor** command. This only applies to the interfaces of the point-to-multipoint type (broadcast or non-broadcast).

To configure the point-to-multipoint type for the interfaces in a non-broadcast network, execute the following commands in the interface configuration mode:

Command	Function
DES-7210 (config-if)# **ip ospf point-to-multipoint non-broadcast**	Specify the network type of the interface to be the point-to-multipoint non-broadcast type.
DES-7210 (config-if)# **exit**	Exit to the global configuration mode.
DES-7210 (config)# **router ospf 1**	Enter the routing process configuration mode.
DES-7210(config-router)# **neighbor** *ip-address* [**cost** number]	Specify the neighbor and the cost to the neighbor.

Pay attention to step 4. If you have not specified the cost for the neighbor, the cost referenced by the **ip ospf cost** command in the interface configuration mode will be used.

31.2.3.3 Configuring Broadcast Network Type

It is necessary to select the designated router (DR) and backup designated router (BDR) for the broadcast type network of OSPF. The DR will notify the link status of this network to outside. All routers keep the neighbor relationship one another and only the adjacent relationship with the designated routers and backup designated routers. That is to say, each router only switches the link status packets with the designated router and backup designated routers, and then the designated router notifies all routers. As a result, each router can keep a consistent link status database.

You can control the election of the designated router by setting the OSPF priority. The parameter does not take effect immediately until in the new round of election. The new election of the designated router occurs only when the OSPF neighbor doesn't receive the Hello message from the designated router within the specified time and consider the DR is down.

To configure the broadcast network type, execute the following commands in the interface configuration mode:

Command	Function
DES-7210 (config-if)# **ip ospf network broadcast**	Specify the type of the interface to be the broadcast network type.
DES-7210 (config-if)# **ip ospf priority** *priority*	(Optional) Specify the priority of the interface.

31.2.4 Configuring the OSPF Area Parameters

To configure area authentication, stub area, and default route summary cost, you need to use the command for configuring the areas.

Area authentication is configured to avoid the learning of non-authenticated and invalid routes and the advertisement of invalid routes to the non-authentication routers. In the broadcast-type network, area authentication can also prevent non-authentication routers from becoming the designated routers for the stability and intrusion prevention of the routing system.

When an area is the leaf area of the OSPF area, orthe area neither acts as the transit area nor injects external routes to the OSPF area, you can configure the area as a stub area. The routers in a stub area can only learn about three routes, namely, 1) Routes in the stub area, 2) Routers in other areas, and 3) Default routes advertised by the border router in the stub area. For there is few external routes, the route tables of the rotuers in the stub area are small, saving resources. So the rotuers in the stub area may be low- or middle-level of routers. To reduce the number of the Link Status Advertisements (LSA) messages sent to the stub areas, you can configure the area as the full stub area (configured with the **no-summary** option). The routers in a full stub area can learn two types of routes: 1) routes in the stub area; 2) default routes advertised by the border router in the stub area. The configuration of the full stub area allows the OSPF to occupy the minimized router resources, increasing the network transmission efficiency.

If the routers in a stub area can learn multiple default routes, you need to set the costs of the default routes (by using the **area default-cost** command), so that they first use the specified default route.

You should pay attention to the following aspects when you configure a stub area:

- The backbone area cannot be configured as a stub area, and the stub area cannot be used as the transmission area of virtual links.
- To set an area as the STUB area, all the routers in the area must be configured with this feature.
- There is no ASBR in stub areas. In other words, the routes outside an autonomous system cannot be propagated in the area.

To configure the OSPF area parameters, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210 (config-router)#**area** *area-id* **authentication**	Set plain-text authentication for the area.

Command	Function
DES-7210 (config-router)#**area** *area-id* **authentication message-digest**	Set MD5 authentication for the area.
DES-7210 (config-router)#**area** *area-id* **stub** [**no-summary**]	Set the area as a stub area. **no-summary:** Set the area as a stub area to prevent the ABR between areas from sending summary-LSAs to the stub area.
DES-7210 (config-router)#**area** *area-id* **default-cost** *cost*	Configure the cost of the default route sent to the stub area.

Note

For authentication configuration, you need to configure the authentication parameters on an interface. See "Configuring the OSPF Interface Parameters" section in this chapter. You must configure the stub area on all the routers in the area. To configure a full stub area, you also have to configure the full stub area parameters on the border router of the stub area in addition to the basic configuration of stub area. You do not need to change the configuration of other routers.

31.2.5 Configuring the OSPF NSSA

The NSSA (Not-So-Stubby Area) is an expansion of the OSPF stub area. The NSSA also reduces the consumption of the resources of the routers by preventing from flooding the type-5 LSA (AS-external-LSA) to the NSSA. However, unlike the stub area, the NSSA can inject some routes outside the autonomous system to the routing area of the OSPF.

Through redistribution, the external type-7 routes of the autonomous system are allowed to import to the NSSA. These external type-7 LSAs will be converted into the type-5 LSAs at the border router of the NSSA and flooded to the entire autonomous system. During this process, the external routes can be summarized and filtered.

You should pay attention to the following aspects when you configure the NSSA:

- The backbone area cannot be configured as a NSSA, and the NSSA cannot be used as the transmission area of the virtual links.
- To set an area as the NSSA, all the routers connected to the NSSA must be configured with the NSSA features by using the **area nssa** command.

To configure an area as the NSSA, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210 (config-router)# **area** *area-id* **nssa** [**no-redistribution**] [**no-summary**] [**default-information-originate**[**metric** *metric*][**metric-type** [**1** | **2**]]]	(Optional) Define a NSSA.
DES-7210 (config-router)#**area** *area-id* **default-cost** *cost*	Configure the cost of the default route sent to the NSSA.

The *default-information-originate* parameter is used to generate the default Type-7 LSA. This option varies slightly between the ARR and ASBR of the NSSA. On the ABR, whether there is a default route or not in the routing table, the Type-7 LSA default route will be created. On the other hand, this is only created when there is a default route in the routing table on ASBR.

The **no-redistribution** parameter allows other external routes introduced by using the **redistribute** commands via the OSPF on the ASBR not to be distributed to the NSSA. This

option is usually used when the router in the NSSA is both an ASBR and an ABR to prevent external routes from entering the NSSA.

To further reduce the LSAs sent to the NSSA, you can configure the **no-summary** attribute on the ABR to prevent the ABR from sending the **summary LSAs (Type-3 LSA)** to the NSSA.

In addition, the area default-cost is used on the ABR connected to the NSSA. This command configures the cost of the default route sent by the border router to the NSSA. By default, the cost of the default route sent to the NSSA is 1.

31.2.6 Configuring the Route Aggregation

31.2.6.1 Configuring the Route Aggregation between OSPF Areas

The ABR (Area Border Router) has at least two interfaces that belong to different areas, one of which must be the backbone area. The ABR acts as the pivot in the OSPF routing area, and it can advertise the routes of one area to another. If the network addresses of the routes are continual in the area, the border router can advertise only one aggregated route to other areas. The route aggregation between areas greatly reduces the size of the routing table and improves the efficiency of the network.

To configure the route aggregation between areas, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210 (config-router)# **area** *area-id* **range** *ip-address mask* [**advertise** | **not-advertise**] [**cost** *cost*]	Configure route aggregation for the area.

Note If route aggregation is configured, the detailed routes in this area will not be advertised by the ABR to other areas.

31.2.6.2 Configuring the External Route Aggregation

When the routes are redistributed from other routing process to the OSPF routing process, every route is advertised to the OSPF-enabled router as a separate link status. If the injected route is in the range of continuous IP addresses, the autonomous area border router can advertise only one aggregated route, and thus reducing the size of the routing table.

To configure the external route aggregation, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210 (config-router)# **summary-address** *ip-address mask*[**not-advertise | tag** *tag-id*]	Configure the external route aggregation.

31.2.6.3 Configuring the Control of Adding the Route Aggregation Entry to RIB

The network range after the route aggregation may exceed the actual range in the RIB(Routing Information Base). If the data are sent to the network beyond the aggregation range, it may result in a loop or the greater burden to the router. It needs to add a discard route to the RIB in ABR or ASBR to prevent that problem.

To allow or disalllow to add the discard route to the RIB, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210 (config-router)# **discard-route** {**internal**|**external**}	Allow to add the discard route to the RIB.
DES-7210 (config-router)# **no discard-route** {**internal**|**external**}	Disallow to add the discard route to the RIB.

By default, it allows to add the discard route to the RIB.

31.2.7 Creating the Virtual Links

In the OSPF routing area, the OSPF route updating between non-backbone areas are exchanged via the backbone area to which all the areas are connected. If the backbone area is disconnected, you need to configure the virtual link to connect the backbone area. Otherwise, the network communication will fail. If physical connection cannot be ensured due to the restriction of the network topology, you can also meet this requirement by creating the virtual links.

Virtual links should be created between two ABRs. The common area of the ABRs become the transmit areas. The stub areas and NSSA areas cannot be used as the transit area. The virtual links can be seen as a logical connection channel established between two ABRs via the transit area. On both its ends must be ABRs and configuration must be performed on both ends. The virtual link is identified by the router-id number of the peer router. The area that provides the two ends of a virtual link with an internal non-backbone area route is referred to as the transit area, whose number must be specified at configuration.

The virtual links will be activated after the route in the transit area has been calculated (that is, the route to the other router). You can see it as a point-to-point connection, on which most parameters of the interface can be configured, like a physical interface, for example, **hello-interval** and **dead-interval**.

The “logical channel” means that the multiple routers running the OSPF between the two ABRs only forward packets (If the destination addresses of the protocol packets are not these routers, the packets are transparent to them and are simply forwarded as common IP packets), and the ABRs exchange route information directly. The route information means the Type-3 LSAs generated by the ABR, and the synchronization mode in the area is not changed as a result.

To create the virtual link, execute the following commands in the routing process configuration mode:

Command	Function

Command	Function
DES-7210 (config-router)# **area** *area-id* **virtual-link** *router-id* [[**hello-interval** *seconds*]| [**retransmit-interval** *seconds*] |[**transmit-delay** *seconds*]|[**dead-interval** *seconds*]| [**authentication** [**message-digest | null**] |[[**authentication-key** *key* | **message-digest-key** *keyid* **md5** *key*]]]	Create a virtual link.

Caution

If the autonomous system is divided into more than one area, one of the areas must be the backbone area to which the other areas must be connected directly or logically. Also, the backbone area must be in good connection.

Note

The *router-id* is the ID of the OSPF neighbor router. If you are not sure of the value of the router-id, you can use the **show ip ospf or show ip ospf neighbor** command to verify it. How to manually configure the router-id, refer to the chapter of *Using the Loopback Address as the Route ID*.

31.2.8 Creating the Default Route

An ASBR can be forced to generate a default route, which is injected to the OSPF routing area. If one router is forced to generate the default route, it will become the ASBR automatically. However, the ASBR will not automatically generate the default route.

To force the ASBR to generate the default route, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210 (config-router)#**default-information originate [always] [metric** *metric-value***] [metric-type** *type-value***] [route-map** *map-name***]**	Generate the default route.

Note

When the stub area is configured, the ABR will generate the default route automatically, and advertise it to all routers within the stub area.

31.2.9 Using the Loopback Address as the Router ID

The OSPF routing process always uses the largest interface IP address as the router ID. If the interface is disabled or the IP address does not exist, the OSPF routing process must calculate the router ID again and send all the route information to the neighbor.

If the loopback (local loop address) is configured, the routing process will select the IP address of the loopback interface as the router ID. If there are multiple loopback interfaces, the largest IP address is selected as the router ID. Since the loopback address always exists, this enhances the stability of the routing table.

To configure the loopback address, execute the following commands in the global configuration mode:

Command	Function
DES-7210 (config)#**interface loopback 1**	Create the loopback interface.
DES-7210 (config-if)#**ip address** *ip-address mask*	Configure the Loopback IP address.

Note

If the OSPF routing process selects the IP address of the common interface as the route identifier, the configuration of the loopback interface will not cause the OSPF process to reselect the identifier.

31.2.10 Changing the OSPF Default Management Distance

The management distance of a route represents the credibility of the source of the route. The management distance ranges from 0 to 255. The greater this value, the smaller the credibility of the source of the route.

The OSPF of DES-7210 product has three types of routes, whose management distances are all 110 by default: intra-area, inter-area, and external. A route belongs to an area is referred to as the intra-area route, and a route to another area is referred to as the inter-area route. A route to another area (learnt through redistribution) is known as the external route.

To change the OSPF management distance, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210(config-router)# **distance ospf {[inter-area** dist1] [**inner-area** dist2] [**external** dist3]}	Change the OSPF management distance.

31.2.11 Configuring the Route Calculation Timer

When the OSPF routing process receives the route topology change notification, it runs the SPF for route calculation after some time of delay. This delay can be configured, and you can also configure the minimum intervals between two SPF calculations.

To configure the OSPF route calculation timer, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210 (config-router)#**timers spf** *spf-delay spf-holdtime*	Configure the route calculation timer.

31.2.12 Changing the LSA Group Pacing Timer

The OSPF LSA group pacing feature allows the switch to group OSPF LSAs and pace the refreshing, verification and calculation, and aging for more efficient use of the device. The default is 4 minutes. This parameter needs not to be adjusted often. The optimum group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10,000 LSAs in the database, decreasing the pacing

interval would be better. If the switch has a small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better. To configure OSPF LSA pacing, follow these steps in the privileged mode:

Execute the following commands in the routing process configuration mode:

Command	Meaning
DES-7210 # **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **router ospf** *1*	Enter the routing protocol configuration mode.
DES-7210 (config-router)# **timers lsa-group-pacing** *seconds*	(Optional) Change the LSAs group pacing.
DES-7210 (config-router)**# end**	Return to the privileged EXEC mode.
DES-7210 # **show running-config**	Verify the configuration.
DES-7210 # **write**	(Optional) Save the configuration.

To restore the settings to the default value, use the **no timers lsa-group-pacing** in the global configuration mode.

31.2.13 Configuring OSPF Interface Cost Value

OSPF calculates the destination route based on the cost, where the route with the least cost is the shortest route. The default route cost is based on network bandwidth. When you configure the OSPF-enabled router, you can set the link cost according to the factors such as link bandwidth, delay or economic cost. The lower its cost, the higher the possibility of that link to be selected as the route. If route aggregation takes place, the maximum cost of all the links are used as the cost of the aggregated route.

Routing configuration includes two parts. In the first place, you set the reference value for the bandwidth generated cost. This value and the interface bandwidth value are used to create the default cost. In the second place, you can set the respective metric of each interface by using the **ip ospf cost** command, so that the default metric is not effective for the interface. For example, the default reference value is 100 Mbps, and an Ethernet interface has the bandwidth of 10Mbps. Other example, the bandwidth is 100Mbps, the bandwidth of an Ethernet interface is 10Mbps, this interface will have the default metric of 100/10 + 0.5 ≈ 10.

The interface cost is selected in the following way in the OSPF protocol. The set interface has the highest priority. If you have set an interface cost, the set value is taken as the interface cost. If you do not set one while the automatic cost generation function is enabled, the interface cost is calculated automatically. If the function is disabled, the default of 10 is taken as the interface cost.

The configuration process is shown as below:

Command	Meaning
DES-7210 # **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **router ospf 1**	Enter the routing protocol configuration mode.
DES-7210(config-router)#**auto-cost [reference-bandwidth** *ref-bw***]**	(Optional) Set the default cost based on the bandwidth on an interface.
DES-7210 (config-router)**# end**	Return to the privileged EXEC mode.
DES-7210 # **show ip protocol**	Display the routing protocol that is running currently.
DES-7210 # **write**	(Optional) Save the configuration.

To remove the setting, use the **no ip ospf cost** or **auto-cost** command.

31.2.14 Configuring OSPF MTU-Ignore

When the OSPF receives the database description packet, it will check the MTU of the neighbor against its own. If the interface indicated in the received database description packet has a MTU greater than that of the receiving interface, the neighborhood relationship cannot be established. In this case, you can disable MTU check as a solution.

To disable the MTU check on an interface, you can execute the following command in the interface configuration mode;

Command	Meaning
DES-7210 (config-if)# **ip ospf mtu-ignore**	Configure not to check the MTU value when the interface receives the database description packets.

By default, the MTU check is enabled on an interface.

31.2.15 Disabling an Interface to Send the OSPF Packets

To prevent other routers in the network from dynamically learning the route information of the router, you can set the specified network interface of the router as a passive interface by using the **passive-interface** command to prevent from sending OSPF packets on the interface.

In the privileged mode, you can configure an interface as a passive interface by performing the following steps:

Command	Meaning
DES-7210 **# configure terminal**	Enter the global configuration mode.
DES-7210(config)# **router ospf 1**	Enter the routing protocol configuration mode (currently RIP and OSPF are supported)
DES-7210 (config-router)# **passive-interface** *interface-name*	(Optional) Set the specified interface as a passive interface.
DES-7210 (config-router)# **passive-interface default**	(Optional) Set all the network interfaces as the passive interfaces
DES-7210 (config-router)# **end**	Return to the privileged EXEC mode.
DES-7210 (config-router)# **write**	Save the configuration.

By default, all interfaces are allowed to receive/send the OSPF packets. To re-enable the network interface to send the route information, you can use the **no passive-interface** *interface-id* command. To re-enable all network interfaces, use the keyword **default.**

31.2.16 Configuring OSPF Load Protection

When the memory lacks, OSPF enters the overflow state. In the overflow state, OSPF protocol will:

- For the learned LSA: receive the Inter-Area/Intra-Area LSA; receive the external LSA if the destination route address represented by LSA is for the non-default learned route; not receive other LSAs.
- For the external LSA generated by itself: clear the external LSAs except for the default route.
- The incompletemess of route learning and advertisement may lead to the route loop in the network. OSPF will generate a default route that is destined to the NULL port to prevent

the route loop. The generated default route exists in the overflow state all the time.

You can configure the overflow memory-lack in the OSPF configuration mode:

Command	Function
DES-7210(config)#**router ospf** *process-id*	Enter the OSPF configuration mode.
DES-7210(config-router)#**overflow memory-lack**	When the memory lacks, OSPF enters the overflow state.

Note

By default, OSPF enters the overflow state automatically when the memory lacks. Use the **no overflow memory-lack** command to disable OSPF to enter the overflow state.

Caution

To exit from the overflow state, you must use the **clear ip ospf process** command, or restart the OSPF protocol.

31.2.17 Configuring the OSPF Network Management

31.2.17.1 Configuring the OSPFv2 MIB Binding

The user can only operate a sole OSPFv2 process by SNMP since the OSPFv2 MIB itself does not have the OSPFv2 process information. By default, OSPFv2 MIB is binded with the OSPFv2 process in the smallest number, and all user operations take effect for this process.

The user can bind OSPFv2 MIB to the process manually if he/she wants to operate the specified OSPFv2 process by SNMP.

In the routing process configuration mode, execute the following command:

Command	Function
DES-7210 (config-router)#**enable mib-binding**	Bind the OSPFv2 MIB to the specified OSPFv2 process.

31.2.17.2 Configuring the OSPFv2 TRAP

The OSPFv2 protocol defines several types of the OSPF TRAP messages, which are used to send the TRAP message to the SNMP server when part of the network configuration changes and some OPSF event occurs for the network management. Sending OSPFv2 TRAP messages is not limited by binding the OSPFv2 process and OSPFv2 MIB. The TRAP switch can be enabled by different processes at the same time.

In the global configuration mode, execute the following command:

Command	Function
DES-7210 # configure terminal	Enter the global configuration mode.

Command	Function
DES-7210 (config)# **snmp-server host** *host-ip* **version** *version-no string* **[ospf**]	Configure the SNMP server to receive the TRAP. *host-ip:* the address corresponding to the SNMP server. *version-no*: the SNMP version corresponding to the SNMP server. *string*: the communication authentication code of SNMP, which is generally public. The optional parameter ospf means that the SNMP server receives the OSPF TRAP message (by default, the SNMP server receives all types of TRAP messages).
DES-7210 (config)# **snmp-server enable traps ospf**	Enable the OSPF TRAP sending switch.
DES-7210 (config)#**router ospf** *process_id* [**vrf** *vrf-name*]	Enable OSPF, enter the OSPF configuration mode.
DES-7210 (config-router)# **enable traps** [**error** [**ifauthfailure | ifconfigerror | ifrxbadpacket | virtifauthfailure | virtifconfigerror | virtifrxbadpacket**] | **lsa** [**lsdbapproachoverflow | lsdboverflow | maxagelsa | originatelsa**] | **retransmit** [**iftxretransmit | virtiftxretransmit**] | **state-change** [**ifstatechange | nbrstatechange | virtifstatechange | virtnbrstatechange**]]	Enable the specified OSPF TRAP switch.
DES-7210 (config)# **end**	Return to the privileged mode.
DES-7210# **write**	Save the configuration.

31.3 Monitoring and Maintaining OSPF

You can show the data such as the routing table, cache, and database of the OSPF. The following table lists some of that data that can be shown for your reference.

Command	Meaning
DES-7210# **show ip ospf** [*process-id*]	Show the general information of the OSPF protocol for corresponding processes. It will display all processes if the process number is not specified.
DES-7210# **show ip ospf** [*process-id area-id*] **database** [**adv-router** *ip-address* | {**asbr-summary** | **external** | **network** | **nssa-external | opaque-area | opaque-as | opaque-link | router** | **summary**} [*link-state-id*] [{**adv-router** *ip-address* | **self-originate}**] | **database-summary** | **max-age** | **self-originate**]	Show OSPF database information. Show the information of each type of LSAs of the specified process.
DES-7210# **show ip ospf** [*process-id*] **border-routers**	Show the route information when the specified process reaches the ABR and ASBR.
DES-7210# **show ip ospf interface** [*interface-name*]	Show the information on the interface participating in the OSPF routing.

Command	Meaning
DES-7210# **show ip ospf** [*process-id*] **neighbor**[*interface-name*] [*neighbor-id*] **[detail]**	Show the information of the adjacent routers of the interface. *interface-name*: The local interface connected to the neighbor *neighbor-id*: The router ID of the neighbor.
DES-7210# **show ip ospf** [*process-id*] **virtual-links**	View the virtual link information of the specified process.
DES-7210# **show ip ospf** [*process-id*] **route [count]**	Show the routes of the OSPF routing table.

For the explanations of the commands, see *IP Routing Protocol Configuration Command Reference*. There are the following common monitoring and maintenance commands:

1. Show the status of the OSPF neighbor

Use the **show ip ospf** [*process-id*] **neighbor** to show all neighbor information of the OSPF process, including the status of neighbor, role, router ID and IP address.

```
DES-7210# show ip ospf neighbor

OSPF process 1:
Neighbor ID      Pri State    Dead Time    Address:     Interface
10.10.10.50 1    Full/DR      00:00:38     10.10.10.50  eth0/0
OSPF process 100:
Neighbor ID      Pri State    Dead Time    Address I    interface
10.10.11.50 1    Full/Backup  00:00:31     10.10.11.50  eth0/1

DES-7210# show ip ospf 1 neighbor

OSPF process 1:
Neighbor ID      Pri State    Dead Time    Address:     Interface
10.10.10.50 1    Full/DR      00:00:38     10.10.10.50  eth0

DES-7210# show ip ospf 100 neighbor

OSPF process 100:
Neighbor ID      Pri State    Dead Time    Address:     Interface
10.10.11.50 1    Full/Backup  00:00:31     10.10.11.50  eth1
```

2. Show the OSPF interface status

The following message shows that the F0/1 port belongs to area 0 of the OSPF, and the router ID is 172.16.120.1. The network type is “BROADCAST”-broadcast type. You must pay special attention to the parameters such as Area, Network Type, Hello and Dead. If these parameters are different from the neighbor, no neighborhood relationship will be established.

```
DES-7210# sh ip ospf interface fastEthernet 1/0
FastEthernet 1/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Ifindex: 2 Area 0.0.0.0, MTU 1500
Matching network config: 192.168.1.0/24,
Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.1.1, Interface Address 192.168.1.1
Backup Designated Router (ID) 192.168.1.2, Interface Address 192.168.1.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 30
Hello received 972 sent 990, DD received 3 sent 4
```

```
LS-Req received 1 sent 1, LS-Upd received 10 sent 26
LS-Ack received 25 sent 7, Discarded 0
```

3. Show the information of the OSPF routing process

The following command shows the route ID, router type, area information, area summary, and other related information.

```
DES-7210 # show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Process uptime is 4 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is enabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
This router is an ASBR (injecting external route information)
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
LsaGroupPacing: 240 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjency Changes : Enabled
Number of areas attached to this router: 1
rea 0 (BACKBONE)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 00:01:26.640 ago
SPF algorithm executed 4 times
Number of LSA 3. Checksum 0x0204bf
Routing Process "ospf 20" with ID 2.2.2.2
Process uptime is 4 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is enabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
LsaGroupPacing: 240 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
umber of non-default external LSA 0
External LSA database is unlimited.
umber of LSA originated 0
Number of LSA received 0
Log Neighbor Adjency Changes : Enabled
Number of areas attached to this router: 0
```

31.4 OSPF Configuration Examples

Seven OSPF configuration examples are provided in this chapter:

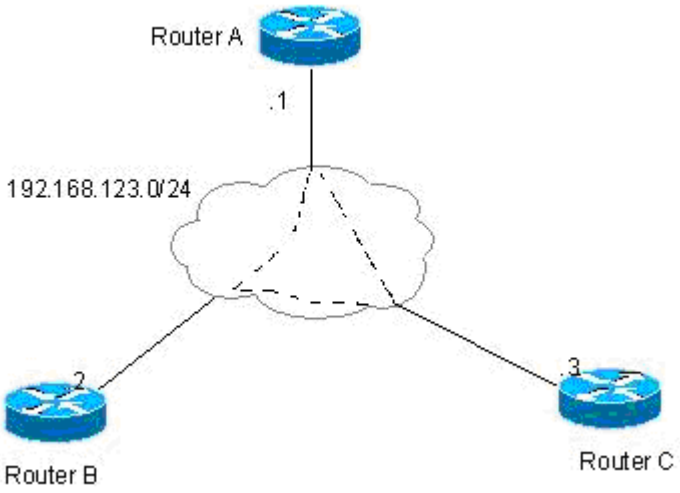
- Example of configuring the OSPF NBMA network type
- Example of configuring the OSPF point-to-multipoint network type
- Example of configuring OSPF authentication
- Example of configuring route aggregation
- Example of configuring OSPF ABR and ASBR
- Example of configuring OSPF stub area
- Example of configuring OSPF virtual link

31.4.1 Example of Configuring the OSPF NBMA Network Type

Configuration requirements:

The three routers must be fully connected in a meshed network via frame relay. Each router has only one frame relay line, which has the same bandwidth and PVC rate. 0 shows the IP address allocation and connection of the equipment.

Figure-1 Example of configuring the OSPF NBMA network type



Requirement:

1) The NBMA network type is configured among router A, B and C;

2) The router A is the designated router, and the router B is the backup designated router;

3) All networks are of one area.

Concrete Configuration of Routers

Since the OSPF has no special configuration, it will automatically discover the neighbors via multicast. If the interface is configured with the NBMA network type, the interface will not send the OSPF multicast packets, so you need to specify the IP address of the neighbor.

Configuration of Router A:

#Configure the WAN port

```
interface Serial 1/0
```

```
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
ip ospf priority 10
```

Configure the OSPF routing protocol to minimize the cost to the router B.

```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.2     priority 5
neighbor 192.168.123.3
```

Configuration of Router B:

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.123.2 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
ip ospf priority 5
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.1 priority 10
neighbor 192.168.123.3
```

Configuration of Router C:

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.123.3 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
```

#Configuring OSPF routing protocol

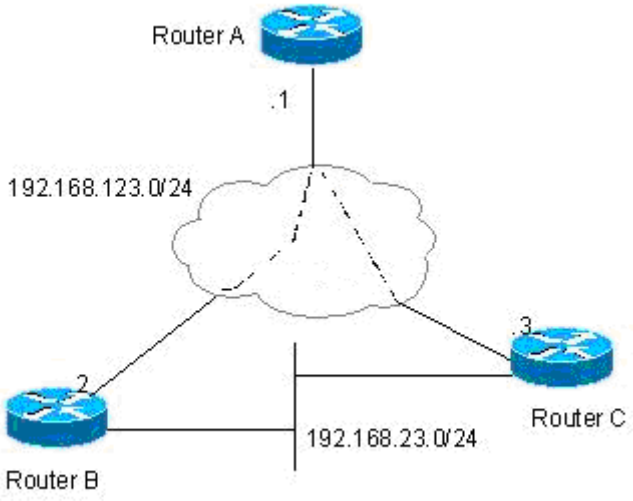
```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.1 10
neighbor 192.168.123.2 5
```

31.4.2 Example of Configuring the OSPF Point-to-multipoint Boardcast Network Type

Configuration requirements:

The three routers must be fully interconnected via frame relay. Each router has only one frame relay line, which has the same bandwidth and PVC rate. 0shows the IP address allocation and connection of the equipment.

Figure-2 Example of Configuring the OSPF Point-to-Multipoint Network Type



Requirements: The point-to-multipoint network should be configured among routers A, B, and C.

Concrete Configuration of Routers

If the interface is configured with the point-to-multipoint network type, the point-to-multipoint network type does not have the process to elect the specified router. The OSPF operation has similar action as the point-to-multipoint network type.

Configuration of Router A:

#Configuring Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.12.1 255.255.255.0
```

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.123.0 0.0.0.255 area 0
```

Configuration of Router B:

#Configuring Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.23.2 255.255.255.0
```

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.123.2 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.123.0 0.0.0.255 area 0
```

Configuration of Router C:

#Configuring Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.23.3 255.255.255.0
```

#Configure the WAN port

```
interface Serial 1/0
ip address 192.168.123.3 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.123.0 0.0.0.255 area 0
```

The above configuration has another assumption:

From router A to the 192.168.23.0/24 target network, router B is the first choice. To achieve preferred routing, you must set the cost of the neighbor when you configure the neighbor.

The following commands can be configured in the router A:

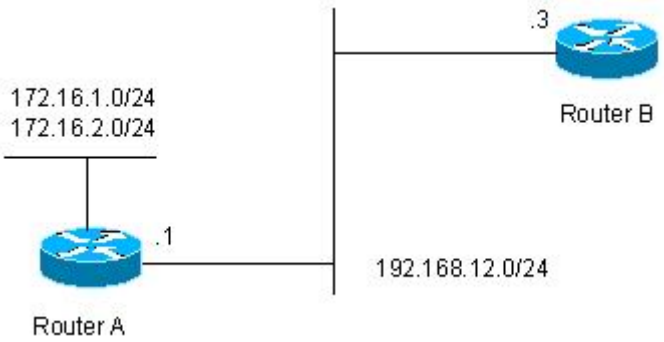
```
router ospf 1
neighbor 192.168.123.2 cost 100
neighbor 192.168.123.3 cost 200
```

31.4.3 Example of configuring OSPF authentication

Configuration requirements:

Two routers are connected via the Ethernet and run the OSPF routing protocol, with the MD5 authentication used. The connection diagram among routers and the assignment of IP addresses are shown as in 0.

Figure-3 Example of configuring OSPF authentication



Concrete Configuration of Routers

The authentication configuration of the OSPF involves two parts:

- Specifying the authentication mode of the area in the routing configuration mode;
- Configuring the authentication method and key in the interface.

If both the area authentication and interface authentication are configured, the interface authentication shall be applied.

Configuration of Router A:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
ip ospf message-digest-key 1 md5 hello
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
area 0 authentication message-digest
```

Configuration of Router B:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
ip ospf message-digest-key 1 md5 hello
```

#Configuring OSPF routing protocol

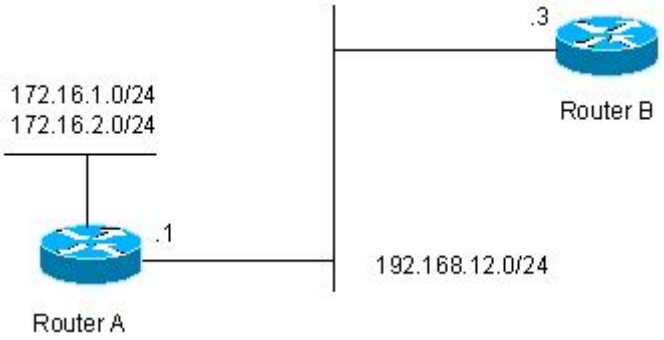
```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
area 0 authentication message-digest
```

31.4.4 Example of Configuring Route Aggregation

Configuration requirements:

The two routers are connected via Ethernet. 0shows the IP address allocation and connection of the equipment.

Figure-4 Example of configuring OSPF route aggregation



Requirements: 1) Both devices run the OSPF routing protocol. The 192.168.12.0/24 network belongs to area 0, while the 172.16.1.0/24 and 172.16.2.0/24 networks belong to area 10; 2) Router A is configured so that route A only advertises the 172.16.0.0/22 route, but not the 172.16.1.0/24 and 172.16.2.0/24.

Concrete Configuration of Routers

You need to configure the OSPF area route aggregation on Router A. Note that the area route aggregation can be configured only on the area border router.

Configuration of Router A:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#Configure the two ports on the Ethernet card

```
interface FastEthernet1/0
ip address 172.16.1.1 255.255.255.0
interface FastEthernet1/1
ip address 172.16.2.1 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 172.16.1.0 0.0.0.255 area 10
network 172.16.2.0 0.0.0.255 area 10
area 10 range 172.16.0.0 255.255.252.0
```

Configuration of Router B:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configuring OSPF routing protocol

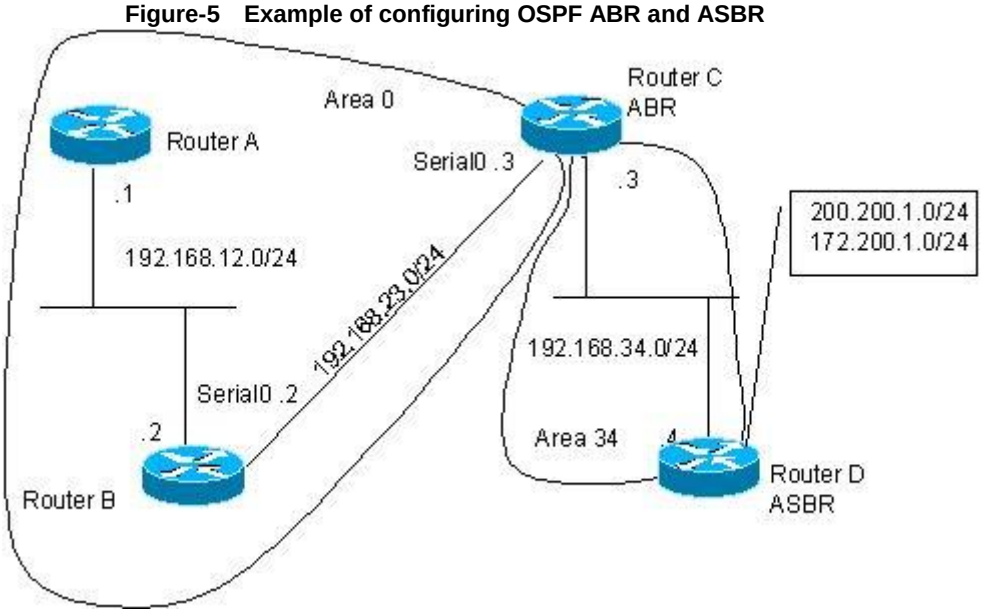
```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

31.4.5 OSPF ABR, ASBR Configuration Examples

Configuration requirements:

Four routers form an OSPF routing area. Networks 192.168.12.0/24 and 192.168.23.0/24 belong to area 0, while network 192.168.34.0/24 belongs to area 34. 0shows the IP address allocation and connection of the equipment.

Figure-5 Example of configuring OSPF ABR and ASBR



As shown in above figure, the router A and router B are of the area internal routers, the router C is of the ABRs, and the router D is of the ASBRs. 200.200.1.0/24 and 172.200.1.0/24 are the networks outside the OSPF routing area. Configure various routers so that all OSPF routers can learn the external routes, which must carry the “34” tag and be Type-I.

Concrete Configuration of Routers

When the OSPF redistributes the routes of other sources, the default type is type II and it does not carry any tag.

Configuration of Router A:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

Configuration of Router B:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configuring the WAN port

```
interface Serial 1/0
ip address 192.168.23.2 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
```

Configuration of Router C:

#Configuring Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.34.3 255.255.255.0
```

#Configuring the WAN port

```
interface Serial 1/0
ip address 192.168.23.3 255.255.255.0
Configuring OSPF routing protocol
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 34
```

Configuration of Router D:

#Configuring Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.34.4 255.255.255.0
```

#Configuring the ports on the Ethernet card

```
interface FastEthernet 1/0
ip address 200.200.1.1 255.255.255.0
interface FastEthernet 1/1
ip address 172.200.1.1 255.255.255.0
```

#Configuring the OSPF routing protocol to redistribute the RIP route

```
router ospf 1
network 192.168.34.0 0.0.0.255 area 34
redistribute rip metric-type 1 subnets tag 34
```

#Configuring RIP routing protocol

```
router rip
network 200.200.1.0
network 172.200.1.0
```

On Router B, you can see the OSPF generates the following routes. Note that the external route type becomes “E1”.

```
O E1 200.200.1.0/24 [110/85] via 192.168.23.3, 00:00:33, Serial1/0
O IA 192.168.34.0/24 [110/65] via 192.168.23.3, 00:00:33, Serial1/0
O E1     172.200.1.0 [110/85] via 192.168.23.3, 00:00:33, Serial1/0
```

On Router B, you can see the link status database as shown below. Note that the tag of the external link has become “34”.

```
RouterB#show ip ospf 1 database
OSPF Router process 1 with ID (192.168.23.2) (Process ID 100)
             Router Link States (Area 0)

Link ID         ADV Router     Age    Seq#      Checksum Link count
SPF Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0.0.0.0)
Link ID        ADV Router     Age  Seq#      CkSum  Link count
1.1.1.1        1.1.1.1        2    0x80000011 0x6f39 2
```

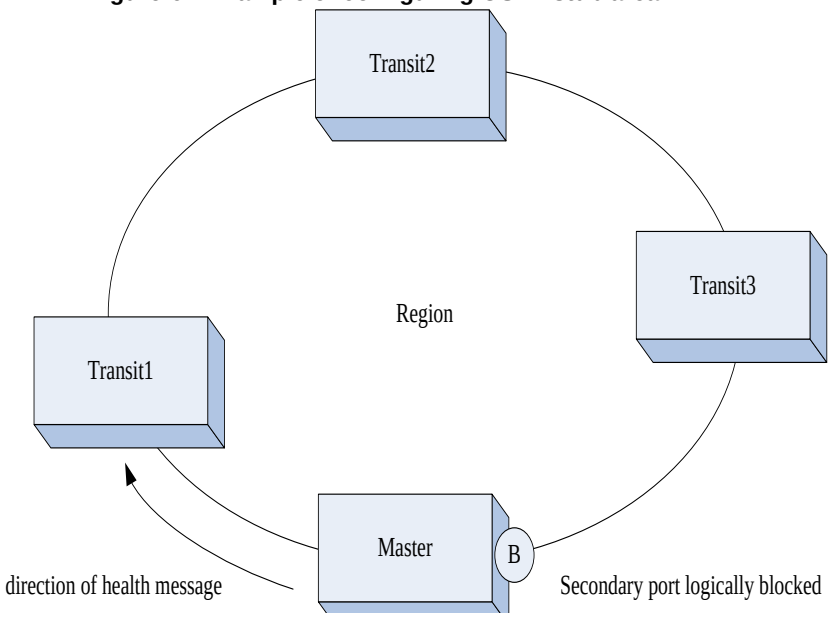
```
3.3.3.3        3.3.3.3        120  0x80000002 0x26ac 1
Network Link States (Area 0.0.0.0)
Link ID        ADV Router     Age  Seq#       CkSum
192.88.88.27    1.1.1.1        120  0x80000001 0x5366
Summary Link States (Area 0.0.0.0)
Link ID        ADV Router     Age  Seq#       CkSum  Route
10.0.0.0       1.1.1.1        2    0x80000003 0x350d 10.0.0.0/24
100.0.0.0      1.1.1.1        2    0x8000000c 0x1ecb 100.0.0.0/16
Router Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Router     Age  Seq#       CkSum  Link count
1.1.1.1        1.1.1.1        2    0x80000001 0x91a2 1
Summary Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Router     Age  Seq#       CkSum  Route
100.0.0.0      1.1.1.1        2    0x80000001 0x52a4 100.0.0.0/16
192.88.88.0     1.1.1.1        2    0x80000001 0xbb2d 192.88.88.0/24
NSSA-external Link States (Area 0.0.0.1 [NSSA])
Link ID        ADV Router     Age  Seq#       CkSum  Route            Tag
20.0.0.0       1.1.1.1        1    0x80000001 0x033c E2 20.0.0.0/24    0
100.0.0.0      1.1.1.1        1    0x80000001 0x9469 E2 100.0.0.0/28   0
AS External Link States
Link ID        ADV Router     Age  Seq#       CkSum  Route            Tag
20.0.0.0       1.1.1.1        380  0x8000000a 0x7627 E2 20.0.0.0/24    0
100.0.0.0      1.1.1.1        620  0x8000000a 0x0854 E2 100.0.0.0/28   0
```

31.4.6 Example of Configuring OSPF Stub Area

Configuration requirements:

Four routers form an OSPF routing area. Networks 192.168.12.0/24 and 192.168.23.0/24 belong to area 0, while network 192.168.34.0/24 belongs to area 34. 0shows the IP address allocation and connection of the equipment.

Figure-6 Example of configuring OSPF stub area



The requirement is that only the OSPF default route and the network routes of the local area can be seen in the routing table of RouterD.

Concrete Configuration of Routers

Only the routers in the full stub area can have their routing tables simplified to eliminate the external and inter-area routes. The stub area must be configured on all the routers in the area. In order to show the inter-area routes of the router D, the router C advertises a 192.168.30.0/24 network.

The configuration of Router A:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

Configuration of Router B:

Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configuring the WAN port

```
interface Serial1/0
ip address 192.168.23.2 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
```

Configuration of Router C:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.34.3 255.255.255.0
```

#Configuring the WAN port

```
interface Serial1/0
ip address 192.168.23.3 255.255.255.0
```

#Adding a network

```
interface Dialer10
ip address 192.168.30.1 255.255.255.0
Configuring OSPF routing protocol
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 34
network 192.168.30.0 0.0.0.255 area 34
area 34 stub no-summary
```

Configuration of Router D:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.34.4 255.255.255.0
```

#Configuring OSPF routing protocol

```
router ospf 1
network 192.168.34.0 0.0.0.255 area 34
area 34 stub
```

The routes generated in the router D by the OSPF are shown as follows:

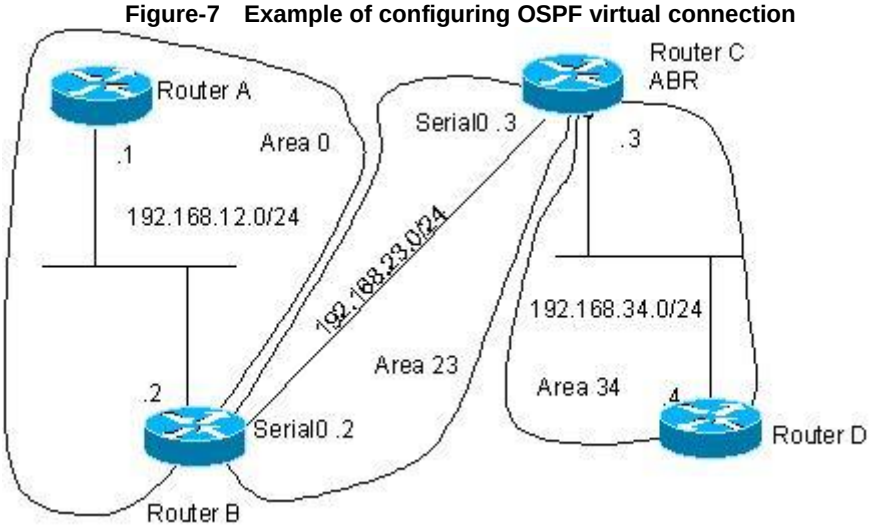
```
O 192.168.30.0/24 [110/1786] via 192.168.34.3, 00:00:03, FastEthernet0/0
O*IA 0.0.0.0/0 [110/2] via 192.168.34.3, 00:00:03, FastEthernet0/0
```

31.4.7 Example of Configuring OSPF Virtual Links

Configuration requirements:

Four routers form an OSPF routing area. Networks 192.168.12.0/24 belongs to area 0, network 192.168.23.0/24 to area 23, while network 192.168.34.0/24 belongs to area 34. 0shows the IP address allocation and connection of the equipment.

Figure-7 Example of configuring OSPF virtual connection



The purpose is to allow router D to learn the routes of 192.168.12.0/24 and 192.168.23.0/24.

Concrete Configuration of Routers

The OSPF routing area consists of multiple sub-areas, each of which must be connected to the backbone area (area 0) directly. If there is no direct connection, a virtual link must be created to ensure logical connection to the backbone area. Otherwise, the sub-areas are not in connection. The virtual connection must be configured on the ABR.

The configuration of Router A:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

#Configure the OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

The configuration of Router B:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

#Configuring the WAN port

```
interface Serial1/0
ip address 192.168.23.2 255.255.255.0
```

#Adding the loopback IP address and taking it as the ID of the OSPF router.

```
interface Loopback2
ip address 2.2.2.2 255.255.255.0
```

#Configuring OSPF route protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 23
area 23 virtual-link 3.3.3.3
```

Configuration of Router C:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.34.3 255.255.255.0
```

#Configuring the WAN port

```
interface Serial1/0
ip address 192.168.23.3 255.255.255.0
```

#Adding the loopback IP address and taking it as the ID of the OSPF router.

```
interface Loopback2
ip address 3.3.3.3 255.255.255.0
```

#Configuring OSPF route protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 23
network 192.168.34.0 0.0.0.255 area 34
area 23 virtual-link 2.2.2.2
```

Configuration of Router D:

#Configuring Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.34.4 255.255.255.0
```

#Configuring OSPF route protocol

```
router ospf 1
network 192.168.34.0 0.0.0.255 area 34
```

The routes generated in the router D by the OSPF are shown as follows:

```
O IA 192.168.12.0/24 [110/66] via 192.168.34.3, 00:00:10, FastEthernet0/0
O IA 192.168.23.0/24 [110/65] via 192.168.34.3, 00:00:25, FastEthernet0/0
```

32 BGP Configuration

32.1 BGP Overview

The Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) designed for routers in different autonomous systems to communicate one another. The goal is to exchange network reachability among different autonomous systems (AS) and eliminate loops by the natural features of the BGP protocol.

The BGP protocol uses the TCP protocol to transmit packets for its reliability, guaranteeing the reliable transmission of packets.

The router which operates the BGP protocol is referred to as the BGP Speaker, and the BGP Speakers which set up a BGP session are referred to as the BGP Peers.

There are two modes of BGP session : IBGP (Internal BGP) and EBGP (External BGP). The IBGP refers to the BGP session set up in an AS, while the EBGP refers to the BGP session set up between different ASs. In a word, the EBGP exchanges the route information among different ASs; the IBGP transits the route information in an AS.

The BGP protocol features:

- Support BGP-4
- Support path attributes
  - ✓ ORIGN Attribute
  - ✓ AS_PATH Attribute
  - ✓ NEXT_HOP Attribute
  - ✓ MULTI_EXIT_DISC Attribute
  - ✓ LOCAL-PREFERENCE Attribute
  - ✓ ATOMIC_AGGREGATE Attribute
  - ✓ AGGREGATOR Attribute
  - ✓ COMMUNITY Attribute
  - ✓ ORIGINATOR_ID Attribute
  - ✓ CLUSTER_LIST Attribute
- Support BGP peer groups
- Support loopback interface
- Support MD5 authentication of TCP
- Support the synchronization of BGP and IGP
- Support the aggregation of BGP routes
- Support BGP route flap dampening
- Support BGP routing reflector
- Support AS confederation
- Support BGP soft reset

32.2 Enabling the BGP Protocol

To enable the BGP protocol, execute the following operations in the privileged mode:

Command	Meaning
DES-7210# **configure terminal**	Enter into the global configuration mode.
DES-7210(config)# **ip routing**	Enable the routing function (if the switch is disabled).
DES-7210(config)# **router bgp** *as-number*	Enable the BGP and configure the AS number. The range of *AS-number* is 1 to 65535.
DES-7210(config-router)# **bgp router-id** *router-id*	(Optional) Configure the ID used when this switch runs the BGP protocol.
DES-7210(config-router)# **end**	Return to the privileged EXEC mode.
DES-7210# **show run**	Show current configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

Use the **no router bgp** command to disable the BGP protocol**.**

32.3 Default BGP Configuration

The BGP protocol is not enabled on the DES-7200 series by default.

After the BGP protocol is enabled, the default configuration of the BGP is shown as follows:

Router ID		To configure the loopback interface, select the maximum one from the loopback interface addresses. Otherwise, select the maximum interface address from the direct-connected interface.
Synchronization of BGP and IGP		Enabled
Generation of Default Route		Disabled
Multi-hop EBGP	Status	Off
	Number of hops	255
TCP MD5 Authentication		Off
Timer	Keepalive Time	60 seconds
	Holdtime	180 seconds
	ConnectRetry Time	120 seconds
	AdvInterval(IBGP)	15 seconds
	AdvInterval(EBGP)	30 seconds
Path Attribute	MED	0
	LOCAL_PREF	100
Route Aggregate		Off
Route Flap Dampening	Status	Off
	Suppress Limit	2000
	Half-life-time	15 minutes
	Reuse Limit	750
	Max-suppress-time	4*half-life-time
Route Reflector	Status	Off
	Cluster ID	Undefined
	Route among reflection clients	Enabled
AS Confederation		Off
Soft Reset		Off

Management Distance	External-distance	20
	Internal-distance	200
	Local-distance	200
Memory lack		OVERFLOW

32.4 Injecting Route information into the BGP Protocol

The route information of the GBP is empty when it operates at just. There are two ways to inject the route information to the BGP:

Manually inject the route information to the BGP by the **Network** commands.

Inject the route information to the BGP from the IGP protocol by the interaction with the IGP protocol.

The BGP will issue the injected route information to its neighbors. This section will describe the manual injection of the route information. For the injection of the route information from the IGP protocol, refer to the *Configuration of BGP and IGP Interaction* in related section.

To inject the network information advertised by the BGP Speaker to other BGP Speaker by means of the Network commands by manual, execute the following operations in the BGP configuration mode:

Command	Meaning
Router(config-router)# **network** *network-number* **mask** *network-mask* [**route-map** ***map-tag***]	(Optional) Configure the network to inject into the BGP routing table within this AS.

Use the **no network** *network-number* **mask** *network-mask* command to remove the configuration. If it is necessary to cancel the used route-map, configure it again by using the *Route-map Not Added* option. If the configured network information is of standard class A, class B or class C network address, the mask option of this command may not be used.

Caution

1. The **network** command is used to inject the route of IGP into the routing table of BGP, and the advertised Networks may be direct-connected route, static route and dynamic route.
2. For the external gateway protocol (EGP), the **network** command indicates the network to be advertised. This is different from the internal gateway protocol (IGP, such as OSPF and RIP). The latter uses the **network** commands to determine where the routing update will be sent to.

Sometimes, we want to use an IGP route rather than an EBGP route. This can be done through the **network backdoor** command. Execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **network** *network-number* **mask** *network-mask* **backdoor**	(Optional) Transmit the reachable network information through the backdoor route.

Use the **no network** *network-number* **mask** *network-mask* **backdoor** command to remove the configuration.


Caution

By default, the management distance of the network information learned about from the BGP Speakers which establishes the EBGP connection is 20. Set the management distance of such network information by the **network backdoor** command as 200. Hence, the identical network information learned from the IGP presents higher priority. These networks learned from the IGP are considered as the backdoor network, and will not be advertised.

32.5 Configuring BGP Peer (Group) and Its Parameters

Since the BGP is an external gateway protocol (EGP), it is necessary for the BGP Speakers to know who is their peer (BGP Peer).

It is mentioned in the overview of the BGP protocol that two modes can be used to set up the connection relationship among BGP Speakers: IBGP (Internal BGP) and EBGP (External BGP). It will judge which connection mode will be established among BGP Speakers by the AS of BGP Peer and that of the BGP Speakers.

Under normal condition, it is required to establish direct connection among BGP Speakers in a physical way for the EBGP connection. However, the BGP Speakers which establishes the IBGP connection may be in any place within the AS.

To configure the BGP peer, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **neighbor** {*address*|*peer-group-name*} **remote-as** *as-number*	Configure the BGP peer. *Address* indicates the IP addresses of the BGP peer. *Peer-group-name* indicates the name of the BGP peer group. The range of *as-number* is 1 to 65535.

Use the **no neighbor** {*address*|*peer-group-name*} to delete one peer or the peer group.

For the BGP Speakers, the configuration information of several peers (including the executed routing policy) is identical. To simplify the configuration and improve the efficiency, it is recommended to use the BGP peer group.

To configure the BGP peer group, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **neighbor** *peer-group-name* **peer-group**	(Optional) Create a BGP peer group.
DES-7210(config-router)# **neighbor** *address* **peer-group***peer-group-name*	(Optional) Set the BGP peer as the member of the BGP peer group.
DES-7210(config-router)# **neighbor** *peer-group-name* **remote-as** *as-number*	(Optional) Configure the BGP peer group. The range of *as-number* is 1 to 65535.

Use the **no neighbor** *address* **peer-group** to delete some member of the BGP peer group.

Use the **no neighbor** *peer-group-name* **peer-group** to delete the whole peer group.

Use the **no neighbor** *peer-group-name* **remote-as** to delete all members of the BGP peer group and the AS number of the peer group.

To configure the peer of the BGP Speakers or the optional parameter of the BGP peer group, execute the following operations in the BGP configuration mode:

Command	Meaning

Command	Meaning
DES-7210(config-router-af)# **neighbor** {*address*|*peer-group-name*} **activate**	(Optional) Activate the address family of the neighbor so that the router can exchange routing information with the address family.
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*}**update-source** *interface*	(Optional) Configure the network interfaces to establish the BGP session with specified BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **ebgp-multihop** [*ttl*]	(Optional) Allow to establish the BGP session among non-direct-connected EBGP peer (group). The range of TTL is 1 to 255, the EBGP is 1 hop by default, and the IBGP is 255 hops by default.
DES-7210(config-router)# **neighbor**{*address* | *peer-group-name*} **password** *string*	(Optional) Enable the TCP MD5 authentication when the connection is established among specified BGP peer (group), and configure the password.
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **times** *keepalive holdtime*	(Optional) Configure the Keepalive and Holdtime value to establish the connection with the specified BGP peer (group). The range of the *keepalive* is 0 to 65535 seconds, 60 seconds by default. The range of the *holdtime* is 0 to 65535 seconds, 180 seconds by default.
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **advertisemet-interval** *seconds*	(Optional) Configure the minimal time interval to send the routing update message to the specified BGP peer (group). The range of advertisement-interval is 1 to 600 seconds, the IBGP peer is 15 seconds by default, and the EBGP peer is 30 seconds by default.
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **default-originate** [**route-map** *map-tag*]	(Optional) Configure to send the default route to the specified BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **next-hop-self**	(Optional) Configure to set the next route information as this BGP speaker when the route is distributed to the specified BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **remove-private-as**	(Optional) Configure to delete the private AS number in the AS path attribute when distributing the route information to the EBGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*}**send-community**	(Optional) Configure to send the community attribute to the specified BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **maximum-prefix** *maximum* [**warning-only**]	(Optional) Limit the number of the route information received from the specified BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **distribute-list** *access-list-name* {**in** | **out**}	(Optional) Configure to implement the routing police according to the access control list when the route information is received from and sent to the specified BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** | **out**}	(Optional) Configure to implement the routing policy according to the prefix list when the route information is received from and sent to specified BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **route-map** *map-tag* {**in** | **out**}	(Optional) Configure to implement the routing policy according to the route-map when the route information is received from and sent to the specified BGP peer (group).

Command	Meaning
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **filter-list** *path-list-name* {**in** | **out**}	(Optional) Configure to implement the routing policy according to the AS path list when the route information is received from and sent to the specified BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **unsuppress-map** *map-tag*	(Optional) Configure to selectively advertise the route information suppressed by the **aggregate-address** command previously when it is distributed to the specified BGP peer.
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **soft-reconfiguration inbound**	(Optional) Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **route-reflector-client**	(Optional) Configure this switch as the route reflector and specify its client.
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **shutdown**	(Optional) Disable the BGP peer (group).

Use the **no** mode of above commands to disable the configurations.

If one peer is not configured with the **remote-as**, each of its members can use the **neighbor remote-as** command to configure it independently.

By default, each member of the BGP peer group will inherit all its configurations. However, each member is allowed to configure the optional configurations which have no effect on the output update independently to replace the unified configuration of the BGP peer group.

Caution

Each member of the BGP peer group is allowed to configure the optional configurations which have no effect on the output update independently to replace the unified configuration of the BGP peer group. That is to say, each member of the BGP peer group will inherit the following configurations: **remote-as update-source local-as reconnect-interval times advertisemet-interval default-originate next-hop-self password remove-private-as send-community distribute-list out filter-list out prefix-list out route-map out unspress-map route-reflector-client.**

The **neighbor update-source** command can be used to select any valid interface to establish the TCP connection. The key function of this command is to provide available Loopback interface, which makes the connection to the IBGP Speaker more stable.

By default, it is required to directly connect with BGP peers physically to establish the EBGP connection. To establish the EBGP peers among non-direct-connected external BGP Speakers, the **neighbor ebgp-multihop** command can be used.

Caution

To avoid route loop and oscillation, the EBGP peers who need multiple hops to establish BGP connection must have non-default routes to each other.

For the sake of the security, you can set the authentication for the BGP peers (group) which will establish the connection, the authentication uses the MD5 algorithm. The authentication password set for the BGP peer should be identical. The process to enable the MD5 authentication on the BGP peer is shown as follows:

Command	Meaning
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **password** *string*	When the BGP connection with the BGP peer is established, use this command to enable the TCP MD5 authentication and set the password.

Use the **no neighbor** {*ip-address* | *peer-group-name*} **password** command to disable the MD5 authentication set for the BGP peer (group).

Use the **neighbor shutdown** command to disable the valid connection established with the BGP peer (group), and delete all route information related to the BGP peer (group).

Caution

To tear down the connection established with the specified BGP peer (group) and reserve the configuration information set for this specified BGP peer (group), use the **neighbor shutdown** command. If such configuration information is not required again, use the **no neighbor** [**peer-group**] command.

32.6 Configuring the Management Strategy for BGP

Whenever the routing policy (including the **distribute-list**, **neighbor route-map**, **neighbor prefix-list and neighbor filter-list)** changes, you need to take effective measure to implement new routing policy. The traditional way is to tear down and then reestablish the BGP session.

This product supports implementing new routing policy without the close of the BGP session connection by the configuration of the soft reset for BGP effectively.

To facilitate the description of the BGP soft reset, the following will refer to the routing policy which has an effect on the input route information as the input routing policy (such as the **In-route-map** and **In-dist-list**), and that has an effect on the output route information as the output routing policy (such as the **Out-route-map** and **Out-dist-list**).

If the output routing policy changes, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **clear ip bgp** {***** | **neighbor** *address* | **peer-group** *peer-group-name* | **external**} **soft out**	Do soft reset of the BGP session and execute the routing policy without resetting up the BGP session.

If the input routing policy changes, its operation will be more complicated than that of the output routing policy, because the implementation of the output routing policy is based on the routing table of this BGP Speaker. The implement of the input routing policy is based on the route information received from the BGP peer. To reduce the memory consumption, the local BGP Speaker will not remain the original route information received from BGP peers.

If it is necessary to modify the input routing policy, the common method is to save the original route information for each specified BGP peer in this BGP Speaker by the **neighbor soft-reconfiguration inbound** command, so as to provide the original foundation of the route information to modify the input routing policy in future.

At present, there is a standard implementation method referred to as the Route Refresh Performance, which can support modifying the routing policy without the storage of the original route information. This product supports the route refreshing performance.

If the input routing policy changes, execute the following operations in the BGP configuration mode:

Command	Meaning

Command	Meaning
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **soft-reconfiguration inbound**	(Optional) Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group). Execution of this command will consume more memory. If both parties support the route refreshing performance, it is not necessary to execute this command.
DES-7210(config-router)# **clear ip bgp** {***** | *neighbor-address* | **peer-group** *peer-group-name* | **external**} **soft in**	Do soft reset of the BGP session and execute the routing policy without resetting up the BGP session.

You can judge whether the BGP peer supports the route refreshing performance by the **show ip bgp neighbors** command. If so, you need to execute the **neighbor soft-reconfiguration inbound** command when the input routing policy changes.

32.7 Configuring Synchronization between BGP and IGP

The routing information can be transmitted to another AS through the local AS only when ,it will pass through this AS and reach anther AS, the route information will be advertised to ll the routers in the local AS have learned the routing information. Otherwise, if some routers running the IGP protocol within this AS have not learn about this route information, the data packets may be discarded for these routers don't know this route when these packets traverses through this AS, namely, it will cause the route black hole.

The BGP-IGP synchronization is designed to ensure all routers within this AS can learn the outbounding route information. A simple way is that the BGP Speakers redistribute all of the routes learned by the BGP protocol to the IGP protocol, guaranteeing that the routers within the AS learn such route information.

The BGP-IGP synchronization mechanism can be cancelled under two conditions:

1. There is no the route information which pass through the local AS (In general, this AS is an end AS).
2. All routers within this AS operate the BGP protocol and the full connection relationship is established among all BGP Speakers (The adjacent relationship is established between any two BGP Speakers).

Caution

By default, the synchronization is disabled. Enable synchronization when not all the routers are running BGP when traversing an AS.

To enable synchronization of BGP speakers, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **synchronization**	(Optional) Enable synchronization of BGP and IGP.

Execute the **no synchronization** command to disable the synchronization mechanism.

32.8 Configuring Interaction between BGP and IGP

To inject the route information generated by the IGP protocol into the BGP protocol, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **redistribute** [**connected** | **rip** | **static**] [**route-map** *map-tag*] [**metric** *metric-value*]	(Optional) Redistribute static route, direct route and the route information generated by RIP.
DES-7210(config-router)# **redistribute ospf** *process-id* [**route-map** *map-tag*] [**metric** *metric-value*] [**match internal external [1 | 2] nssa-external [1 |2**]]	(Optional) Redistribute the route information generated by OSPF.
DES-7210(config-router)# **redistribute isis** [*isis-tag*] [**route-map** *map-tag*] [**metric** *metric-value*] [**level-1| level-1-2| level-2**]	(Optional) Redistribute the route information generated by ISIS.

By default, distribution of default route is disabled. To enable this function, execute the following commands:

Command	Meaning
DES-7210(config-router)# **default-information originate**	(Optional) Redistribute default route.

32.9 Configuring BGP Timer

The BGP uses the Kepalive timer to maintain the effective connection with the peers, and takes the Hldtime timer to judge whether the peers are effective. By default, the value of the Kepalive timer is 60s, and the value of the Holdtime timer is 180s. When the BGP session is established between BGP Speakers, both parties will negotiate with the Holdtime timer and that with smaller value will be selected. While, the selection of the Keepalive timer is based on the smaller one between 1/3 of the negotiated Holdtime timer and the configured Keepalive timer.

To adjust the value of the BGP timer based on all peers, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **timers bgp** *keepalive holdtime*	(Optional) Adjust the keepalive and holdtime value of BGP based on all peers. The range of the *keepalive* is 0 to 65535 seconds, and 60 seconds by default. The range of the *holdtime* is 0 to 65535 seconds, 180 seconds by default.

Certainly, you can adjust the value of the BGP timer based on the specified peers, and execute the following operations in the BGP configuration mode:

Command	Meaning

Command	Meaning
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **times** *keepalive holdtime*	(Optional) Configure the Keepalive and Holdtime value to establish a session with the specified BGP peer (group). The range of the keepalive is 0 to 65535 seconds, 60 seconds by default. The range of the holdtime is 0 to 65535 seconds, 180 seconds by default.

Use the **no** option of corresponding commands to clear the value of configured timer.

32.10 Configuring BGP Path Attributes

32.10.1 AS_PATH Attribute

The BGP protocol controls the distribution of the route information in three ways:

- IP address by using the **neighbor distribute-list** and **neighbor prefix-list** commands
- AS_PATH Attribute(refer to the description in this section)
- COMMUNITY Attribute(refer to the COMMUNITY Attribute configuration)

You can use the AS path-based access control list to control the distribution of the route information, where the AS path-based ACL will use Regular Expression to resolute the AS path.

To configure the AS path-based distribution of the route information, execute the following operations in the privileged mode:

Command	Meaning
DES-7210# **configure terminal**	Enter into the global configuration mode.
DES-7210(config)# **ip as-path access-list** *path-list-name* {**permit** | **deny**} *as-regular-expression*	(Optional) Define an AS path list.
DES-7210(config)# **ip routing**	Enable the routing function (if disabled)
DES-7210(config)# **router bgp** *as-number*	Enable the BGP and configure this AS number to enter into the BGP configuration mode.
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **filter-list** *path-list-name* {**in** | **out**}	(Optional) Implement the routing policy according to the AS path list when the route information is received from and sent to the specified BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **route-map** *map-tag* {**in** | **out**}	(Optional) Implement the routing policy according to the route-map when the route information is received from and sent to the specified BGP peer (group). In the route-map configuration mode, you can use the **match as-path** to operate the AS path attribute by the AS path list, or take the **set as-path** to operate the AS attribute value directly.

The BGP protocol will not take the length of the AS path into account when it selects the optimal path as specified in RFC1771. In general, the shorter the length of the AS path, the higher the path priority is. Hence, we take the length of the AS path when we select the optimal path. You can determine whether it is necessary to take the length of the AS path into account when you select the optimal path according to the actual condition.

If you don't want take the length of the AS path into account when you select the optimal path, execute the following operations in the BGP configuration mode:

Command	Meaning

Command	Meaning
DES-7210(config-router)# **bgp bestpath as-path ignore**	(Optional) Compare with the length of the AS path when selecting the optimal path.

Caution

Within the AS, whether all BGP Speakers take the length of the AS path into account will be consistent when selecting the optimal path. Otherwise, the optimal path information selected by various BGP Speakers will be different.

32.10.2 NEXT_HOP Attribute

To set the next hop as the local BGP Speaker for sending the route information to the specified BGP peer, you can use the **neighbor next-hop-self** command, which is mainly used in the non-mesh networks (such as frame relay and X.25). Execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **next-hop-self**	(Optional) Set the next hop as the local BGP speaker for distributing the route information to the specified BGP peer (group).

You can also modify the next hop of the specified path by the **set next-hop** command of Route-map.

Caution

This command is not recommended to use under the full mesh network environment (such as Ethernet) for it will cause additional hops and incur unnecessary overhead.

32.10.3 MULTI_EXIT_DISC Attribute Configuration

The BGP takes the MED value as the foundation of priority comparision of the paths learned from the EBGP Peers. The smaller the MED value, the higher the priority of the path is.

By default, it will only compare with the MED value for the path of the peers from the same AS when the optimal path is selected. If you hope to compare with the MED value for the path of the peers from different ASs, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **bgp always-compare-med**	(Optional) Compare with the MED value for the path of different ASs.

By default, it will not compare with the MED value for the path of the peers for other ASs within the AS association when the optimal path is selected. If you hope to compare with the MED value for the path of the peers from different AS confederations, execute the following operations in the BGP :configuration mode

Command	Meaning
DES-7210(config-router)# **bgp bestpath med confed**	(Optional) Compare with the MED value for the path of the peers from other ASs within the confederation.

By default, if the path whose MED attribute is not set is received, the MED value of this path will be taken as 0. For the smaller the MED value, the higher the priority of the path is, the MED value of this path reaches the highest priority. If you hope the MED attribute for the

path whose MED attribute is not set presents the lowest priority, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **bgp bestpath med missing-as-worst**	(Optional) Set the priority of the path whose MED attribute is not set as the lowest.

By default, they will be compared with each other according to the sequence the paths are received when the optimal path is selected. If you hope to compare with the path of the peers from the same AS firstly, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **bgp deterministic-med**	(Optional) Compare with the path of the peers from the same AS firstly. By default, they will be compared with by the received sequence, the later received path will be compared with firstly.

32.10.4 LOCAL_PREF Attribute Configuration

The BGP takes the LOCAL_PREF as the foundation of priority comparision of the path learned from the IBGP peers. The larger the LOCAL_PREF value, the higher the priority of the path is.

The BGP Speakers will add the local preference when they send the received external routes to the IBGP peers. To modify the local preference, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **bgp default local-preference** *value*	(Optional) Change the default local preference. The range of the value is 0 to 4294967295, 100 by default.

You can also modify the local preference of the specified path by the **set local-preference** command of Route-map.

32.10.5 COMMUNITY Attribute Configuration

COMMUNITY Attribute is another method to control the distribution of the route information.

The community is a set of destinations. The purpose is to implement the community-based routing policy so as to simplify the configuration to control the distribution of the route information in the BGP Speakers.

Each destination may be of more than one community, and the manager of the AS can define which community the destination is of.

By default, all destinations are of the Internet community carried in the community attribute of the path.

At present, total for four common community attribute values are predefined:

- **Internet**: Indicate the Internet community, and all paths are of this community.
- **no-export**: Indicate this path will not be exported to the BGP peers.
- **no-export**: Indicate this path will not be advertised to the BGP peers.
- **local-as**: Indicate this path will be advertised only in the local AS or the AS confederation if it is configured.

You can control the receiving, priority and distribution of the route information by the community attribute.

The BGP supports up to 32 COMMUNITY attributes for every route. When configuring the **route-map** command, you can set up to 32 COMMUNITY attributes for the parameters **match** and **set COMMUNITY.**

The BGP Speakers can set, add or modify the community attribute value when they learn about, issue or redistribute the route. The aggregated path includes the community attribute of all aggregated paths when the route aggregate is carried out.

To configure the community attribute-based distribution of the route information, execute the following operations in the privileged mode:

Command	Meaning
DES-7210# **configure terminal**	Enter into the global configuration mode.
DES-7210(config)# **ip community-list standard** *community-list-name* {**permit** | **deny**} *community-number*	(Optional) Create the community list. The *community-list-name* is the name of the community list. The community-number is the concrete value of the community list in the range 1 to 4,294,967,200, or the well-known community attribute such as **Internet**, **local-AS**, **no-advertise** and **no-export**.
DES-7210(config)# **ip routing**	Enable the routing function (if disabled).
DES-7210(config)# **router bgp** *as-number*	Enable the BGP and configure this AS number to enter into the BGP configuration mode.
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **send-community**	(Optional) Configure to send the community attribute to the specified BGP peer (group).
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **route-map** *map-tag* {**in** | **out**}	(Optional) Configure to implement the routing policy according to the route-map when the route information is received from and sent to the specified BGP peer (group). In the route-map configuration mode, you can use the **match community-list [exact]** and **set community-list delete** to operate the community attribute by the community list, or take the **set community** command to operate the community attribute value directly.

32.10.6 Other Related Configuration

By default, if two paths with full identical path attributes are received from different EBGP peers during the selection of the optimal path, we will select the optimal path according to the path received sequence. You can select the path with smaller router ID as the optimal path by configuring the following commands.

Command	Meaning
DES-7210(config-router)# **bgp bestpath compare-routerid**	(Optional) Allow the BGP to compare with the router ID when the optimal path is selected.

32.11 Selecting the Optimal Path for BGP

The selection of the optimal route is an important part of the BGP protocol. The following will describe the selection process of the BGP route protocol in details:

1. Discard the unreachable Next-hop route.
2. Select the route with the maximal weight.
3. Select the route with the high LOCAL_PREF attribute value.
4. Select the route generated by the local BGP speaker.
5. The route generated by the local BGP speaker includes the one generated by the **neighbor default-originate, network, redistribute, aggregate** command.
6. Select the route with the shortest AS length.
7. Select the route with the lowest ORIGIN attribute value.
8. Select the route with the smallest MED value.
9. The priority of the EBGP path is higher than that of the route of the IBGP path and the AS
10. confederation, and the priority of the IBGP path and the AS confederation is identical.
11. Select the route with the smallest IGP metric to reach the next hop.
12. Select the route received comparativelly earlier from the EBGP routes.
13. Select the route which advertises that the router ID of the BGP speaker is small.
14. Select the route with the great cluster length.
15. Select the route: the value of neighbor address for which is high.

Caution

Above is the process of select the optimum route under the default configuration. You can change the selection process of the route by the CLI command. For instance, you can use the **bgp bestpath as-path ignore** command to make the step 5 in the process of selecting the optimum route invalid.

32.12 Configuring BGP Route Aggregation

Since the BGP-4 supports CIDR, aggregated entries are allowed to create to reduce the size of the BGP routing table. Certainly, only when there is valid path within the aggregation scope can the BGP aggregated entries be added to the BGP routing table.

To configure the BGP route aggregation, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **aggregate-address** *address mask*	(Optional) Configure the aggregated address.
DES-7210(config-router)# **aggregate-address** *address mask* **as-set**	(Optional) Configure the aggregated address, and remain the AS path information of the path within the scope of the aggregated address.
DES-7210(config-router)# **aggregate-address** *address mask* **summary-only**	(Optional) Configure the aggregated address and only advertise the aggregated path.

Command	Meaning
DES-7210(config-router)# **aggregate-address** *address mask* **as-set summary-only**	(Optional) Configure the aggregated address, and remain the AS path information of the path within the scope of the aggregated address. At the same time, only the aggregated path is advertised.

Use the **no** mode of above commands to disable the configured content.

Caution

By default, the BGP will advertise all route information both before and after aggregation. If you want to advertise only the aggregated path information, use the **aggregate-address summary-only** command.

32.13 Configuring Route Reflector for BGP

To speed up the convergence of the route information, all BGP Speakers within one AS will usually establish the full connection relationship (The adjacent relationship is established between any two BGP Speakers). Too many BGP Speakers within the AS will increase the resource overhead of the BGP Speakers, raise the configuration workload and complexity of network administrators and reduce the network scalability.

For this reason, two measures such as the route reflector and AS confederation are proposed to reduce the connections of the IBGP peers within an AS.

The route reflector is a measure to reduce the connections of the IBGP peer within the AS. One BGP Speaker is set as the route reflector, which divides the IBGP peer within this AS into two types, such as client and non-client.

The rule to implement the route reflector within the AS is shown as follows:

- Configure the route reflector and specify its client, so the route reflector and other clients form a cluster. The route reflector establishes the connection relationship with clients.
- The clients of the route reflector within one cluster should not establish the connection relationship with other BGP Speakers of other clusters.
- Within an AS, the full connection relationship is established among the IBGP peer of non-clients. Where, the IBGP peer of non-clients includes the following conditions: among several route reflectors within one cluster, among the route reflector within the cluster and the BGP Speakers which don't participate in the route reflector function out of the cluster (In general, the BGP Speakers don't support the route reflector function), among the route reflector within the cluster and the route reflector of other cluster.

The processing rule when the route reflector receives one route is shown as follows:

- The route update received from the EBGP Speaker will be sent to all clients and non-clients.
- The route update received from the clients will be sent to other clients and all non-clients.
- The route update received from the IBGP non-clients will be sent to all its clients.

To configure the BGP route reflector, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **neighbor** {*address* | *peer-group-name*} **route-reflector-client**	(Optional) Configure this product as the route reflector and specify its clients.

In general, one group is only configured with one route reflector. In this case, the Router ID of the route reflector can be used to identify this cluster. To increase the redundancy, you can set more than one route reflector within this cluster. In this case, you must configure the cluster ID, so that one route reflector can identify the route update from other route reflectors of this cluster.

Caution

To set several route reflectors for one cluster, it is necessary for you to configure a cluster ID for this cluster.

To configure the cluster ID of the BGP, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **bgp cluster-id** *cluster-id*	(Optional) Configure the cluster ID of the route reflector.

In general, it is not necessary to establish the connection relationship between the clients of the route reflector within the cluster, and the route reflector will reflect the routes among clients. However, if the full connection relationship is established among all clients, this function can be disabled.

To disable the function of reflecting the routes of the client, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **no bgp client-to-client reflection**	(Optional) Disable route reflection on clients.

32.14 Configuring Route Flap Dampening for BGP

Route flap means a route changes between the valid status and the invalid status. The route flap usually causes instable routes to be transmitted on the Internet, and thus a instable network. The BGP route flap dampening is a measure to reduce route flap by monitoring the route information of EBGP peers.

The route flap dampening of BGP uses the following glossaries:

- Route Flap: A route changes between the valid status and the invalid status.
- Penalty: The route flap dampening-enabled BGP Speakers will add a penalty for the route every time when a route flaps. The penalty will be accumulated to exceed the suppress limit.
- Suppress Limit: When the penalty of a route exceeds this value, the route will be suppressed.
- Half-life-time: The time elapsed when the penalty is reduced to half of its value.
- Reuse Limit: When the penalty of the route is lower than this value, the route suppression is released.
- Max-suppress-time: The maximal time the route can be suppressed.

Brief description of route flap dampening: The BGP Speakers will add a penalty for the route every time when a route flaps. The penalty is accumulated. Once the penalty value reaches the suppress limit, the route will be suppressed. When the half-life-time reaches, the penalty value is reduced to half of its value. Once the penalty value is reduced to the reuse limit, the route will be activated again. A route can be suppressed for the maximal suppress time.

To configure the route flap dampening of the BGP, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **bgp dampening**	Enable the route flap dampening of the BGP protocol.
DES-7210(config-router)# **bgp dampening** *half-life-time reuse suppress max-suppress-time*	(Optional) Configure the parameters of the route flap dampening. half-life-time: in the range 1 to 45minutes, 15minutes by default. reuse: in the range 1 to 20000, 750 by default. suppress: in the range 1 to 20000, 2000 by default. max-suppress-time: in the range 1 to 255 minutes, 4*half-life-time by default.

If it is necessary to monitor the route flap dampening information, execute the following operations in the privileged mode:

Command	Meaning
DES-7210# **show ip bgp dampening flap-statistics**	Show the flap statistics information of all router.
DES-7210# **show ip bgp dampening dampened-paths**	Show the dampened statistics information.

To clear the route flap dampening information or clear the dampened routes, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210# **clear ip bgp flap-statistics**	Clear the flap statistics information of all un-dampened route.
DES-7210# **clear ip bgp flap-statistics** *address mask*	Clear the flap statistics information of the specified route (excluding the dampened routes).
DES-7210# **clear ip bgp dampening** [*address mask*]	Clear the flap statistics information of all routes, and release the suppressed routes.

32.15 Configuring AS Confederation for BGP

The confederation is a measure to reduce the connections of the IBGP peer within the AS.

One AS is divided into multiple sub ASs that can form a confederation by setting a unified confederation ID (namely, confederation AS number). An external confederation is still considered to be an AS and only the AS number of the confederation is visible. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers and the EBGP connection is established among the BGP Speakers within the sub AS. Although the EBGP connection is established among BGP Speakers within the sub ASs, the path attribute information of NEXT_HOP, MED and LOCAL_PREF retains intact when the information is exchanged.

To implement the AS confederation, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **bgp confederation identifier** *as-number*	Configure the AS confederation number. The range of *as-number* is 1 to 65535.
DES-7210(config-router)# **bgp confederation peers** *as-numbe* [*as-number*..]	Configure other sub AS numbers within the AS confederation. The range of *as-number* is 1 to 65535.

Use the **no** mode of above commands to disable the configured content.

32.16 Configuring BGP Management Distance

The management distance indicates the reliability of the route information resource, whose range is 1 to 255. The larger the value of the management distance, the lower the reliability is.

The BGP sets different management distances for various information sources learned, such as External-distance, Internal-distance and Local-distance.

- **External-distance:** The management distance of the route learned from the EBGP peers.
- **Internal-distance:** The management distance of the route learned from the IBGP peers.
- **Local-distance:** The management distance of the route learned from the peers. However, it is considered that the optimal one can be learned from the IGP. In general, these routes are indicated by the **Network Backdoor** command.

To modify the management distance of the BGP protocol, execute the following operations in the BGP configuration mode:

Command	Meaning
DES-7210(config-router)# **distance bgp** *external-distance internal-distance local-distance*	(Optional) Configure the management distance. The range of the distance is 1 to 255. For the default configuration: *external-distance 20* *internal-distance 200* *local-distance 200*

Use the **no** command to restore the default management distance of the BGP protocol.

Caution

It is not recommended to change the management distance of the BGP route. If it is necessary to change, please keep it in mind that:

1. The External-distance should be lower than the management distance of other IGP route protocol (OSPF and RIP).
2. The Internal-distance and Local-distance should be higher than the management distance of other IGP route protocol.

32.17 Monitoring BGP

You can use the **Show** commands to view the route table, buffer and database of the BGP. Execute the following operations in the privileged mode:

Command	Meaning
DES-7210# **show ip bgp**	Show the information on all BGP routes.
DES-7210# **show ip bgp** {*network* | *network-mask* } [**longer-prefixes**]	Show the BGP route information of the specified destination.
DES-7210# **show ip bgp prefix-list** *prefix-list-name*	Show the BGP route information of the specified matching against the prefix list.
DES-7210# **show ip bgp community** [**exact**] *community-number*	Show the BGP route information including the specified community.

Command	Meaning
DES-7210# **show ip bgp community-list** *community-lister-number* [**exact**]	Show the BGP route information which matches against the specified community list.
DES-7210# **show ip bgp filter-list** *path-list-number*	Show the BGP route information which matches against the specified AS path list.
DES-7210# **show ip bgp regexp** *as-regular-expression*	Show the BGP route information of the specified regular expression which matches against the AS path attribute.
DES-7210# **show ip bgp dampening dampened-paths**	Show the suppressed flap statistics information.
DES-7210# **show ip bgp dampening flap-statistics**	Show the flap statistics information of all routes with the flap record.
DES-7210# **show ip bgp neighbors** [*address*] [**received-routes** | **routes** | **advertised-routes** | **flap-statistics** | **dampened-routes**]	Show the information of the BGP peer.
DES-7210# **show ip bgp summary**	Briefly show the configuration of the BGP router itself and the information of the peer.
DES-7210# **show ip bgp peer-group** [*peer-group-name*]	Show the configuration information of the BGP peer group.

32.18 Protocol Independent Configuration

32.18.1 route-map Configuration

The BGP protocol applies the Route-map policy on a large scale. For the configuration of the Route-map policy, refer to the Protocol Independent Configuration Part in this manual.

32.18.2 Regular Expression Configuration

The regular expression is the formula to match the string according to a certain template. The regular expression is used to evaluate the text data and return a true or false value. That is to say, whether the expression can describe this data correctly.

32.18.2.1 Description of Control Characters for Regular Expression

The BGP path attribute uses the regular expression. Here will briefly describe the use of the special characters for the regular expression:

Characters	Signs	Special Meanings
Period	**.**	Match with any single character.
Asterisk	*****	Match with none or any sequence of the string.
Plus	**+**	Match with one or any sequence of the string.
Interrogation Mark	**?**	Match with none or one sign of the string.
Plus Sign	**^**	Match with the starting of the string.
Dollar	**$**	Match with the end of the string.

Characters	Signs	Special Meanings
Underlining	_	Match with the comma, bracket, the starting and end of the string and blank.
Square Brackets	[ ]	Match with the single character within the specified scope.

32.18.2.2 Application Example of Regular Expression

Run the **show ip bgp** command on the device:

```
DES-7210# show ip bgp
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status Network           Next Hop     Metric  LocPrf  Path
------ ----------------- ---------------  -------- -------- -------------------
*>  211.21.21.0/24    110.110.110.10  0     1000   200 300
*>  211.21.23.0/24    110.110.110.10  0     1000   200 300
*>  211.21.25.0/24    110.110.110.10  0     1000   300
*>  211.21.26.0/24    110.110.110.10  0     1000   300
*> 1.1.1.0/24      192.168.88.250  444         0   606
*> 179.98.0.0      192.168.88.250  444         0   606
*> 192.92.86.0     192.168.88.250  8883        0   606
*> 192.168.88.0    192.168.88.250  444         0   606
*> 200.200.200.0   192.168.88.250  777         0   606
```

Use the regular expression in the **show** command:

```
DES-7210# show ip bgp regexp _300_
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status Network        Next Hop          Metric  LocPrf  Path
------ ----------------- ---------------  -------- -------- -------------------
*>  211.21.21.0/24  110.110.110.10  0     1000   200 300
*>  211.21.23.0/24  110.110.110.10  0     1000   200 300
*>  211.21.25.0/24  110.110.110.10  0     1000   300
*>  211.21.26.0/24  110.110.110.10  0     1000   300
```

32.19 BGP Load Protection Configuration

Too many BGP routes will always lead to the switch overload, especially for the switch with low memory size. Configuring the BGP load protection can prevent the occurance of the unforeseen switch operation problem due to the overall switch resource usage.

This section includes:

- Limiting the BGP route number
- Configuring Overflow Memory-lack

32.19.1 Limiting BGP Route Number

To limit the route number, you can configure the maximum route number in the BGP address-family mode.

Use the following commands to configure the maximum route number learned from the BGP neighbor:

Command	Meaning
DES-7210(config)# r**outer bgp** *as-num*	Enter the BGP configuration mode.
DES-7210(config-router)#**neighbor** {*peer-address* | *peer-group-name*} **remote-as** *as-num*	Configure the BGP neighbor.
DES-7210(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **maximum-prefix** *maximum* [**threshold**] [**warning-only**]	Configure the maximum route number learned from the BGP neighbor.

Use the following commands to configure the maximum route number in the specified BGP address-family mode:

Command	Meaning
DES-7210(config)# **router bgp** *as-num*	Enter the BGP configuration mode.
DES-7210(config-router)#**address-family ipv4 unicast**	Enter the BGP ipv4 unicast address-family mode.
Or DES-7210(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the BGP ipv4 VRF address-family mode.
Or DES-7210(config-router)#**address-family vpnv4 unicast**	Enter the BGP VPNV4 address-family mode.
DES-7210(config-router)# **maximum-prefix** *maximum*	Configure the maximum route number in the specified BGP address-family mode.

Platform description

The maximum route number limit of the address-family has been supported since version 10.3 (4b3).

32.19.2 Configuring Overflow Memory-lack

BGP is allowed to be in the overflow state when the memory lacks. In general, the routes BGP learned in the overflow state are dropped, and the system memory maintains in a steady state.

Use the following commands to enable BGP to be in the overflow state:

Command	Meaning
DES-7210(config)# **router bgp** *as-num*	Enter the BGP configuration mode.
DES-7210(config-router)# **overflow memory-lack**	Enable BGP to be in the overflow state.

Note

By default, when the memory lacks, BGP is in OVERFLOW state automatically. Use the no overflow memory-lack command to disable the BGP to be in OVERFLOW state.

Caution	In OVERFLOW state, BGP supports the **clear bgp** { *addressfamily* | **all** } * command, or you can disable and reenable BGP to exit the OVERFLOS state. When the memory restores to be enough, BGP exits the OVERFLOW state automatically.

Platform description	The maximum route number limit of the address-family has been supported since version 10.3 (4b3).

32.20 BGP Configuration Examples

The following lists the BGP configuration.

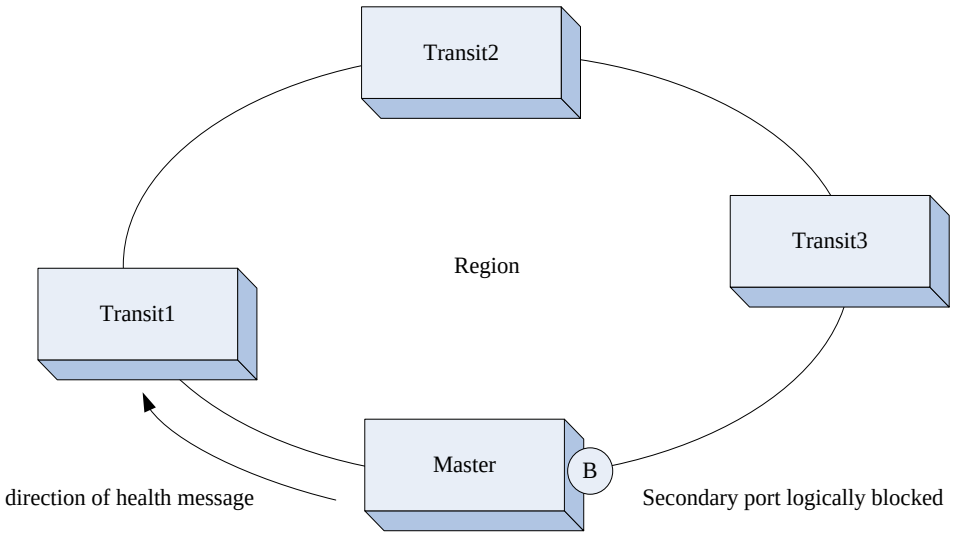
32.20.1 Configuring BGP Neighbor

The following will show how to configure the BGP neighbor. Use the **neighbor remote-as** command to configure the BGP neighbor. The concrete configuration is shown as follows:

```
router bgp 109

neighbor 131.108.200.1 remote-as 167

neighbor 131.108.234.2 remote-as 109

neighbor 150.136.64.19 remote-as 99
```

Configure one IBGP peer 131.108.234.2 and two EBGP peers 131.108.200.1 and 150.136.64.19.

The following is an example to configure the BGP neighbor. For the relationship among routers and the assignment of the IP addresses, refer to the schematics.



In this example, the BGP configuration of various routers is shown as follows:

Router A Configuration:

```
!
router bgp 100
 neighbor 192.168.4.2 remote-as 100
```

Router B Configuration:

```
!
router bgp 100
 neighbor 192.168.4.3 remote-as 100
 neighbor 192.168.5.3 remote-as 200
```

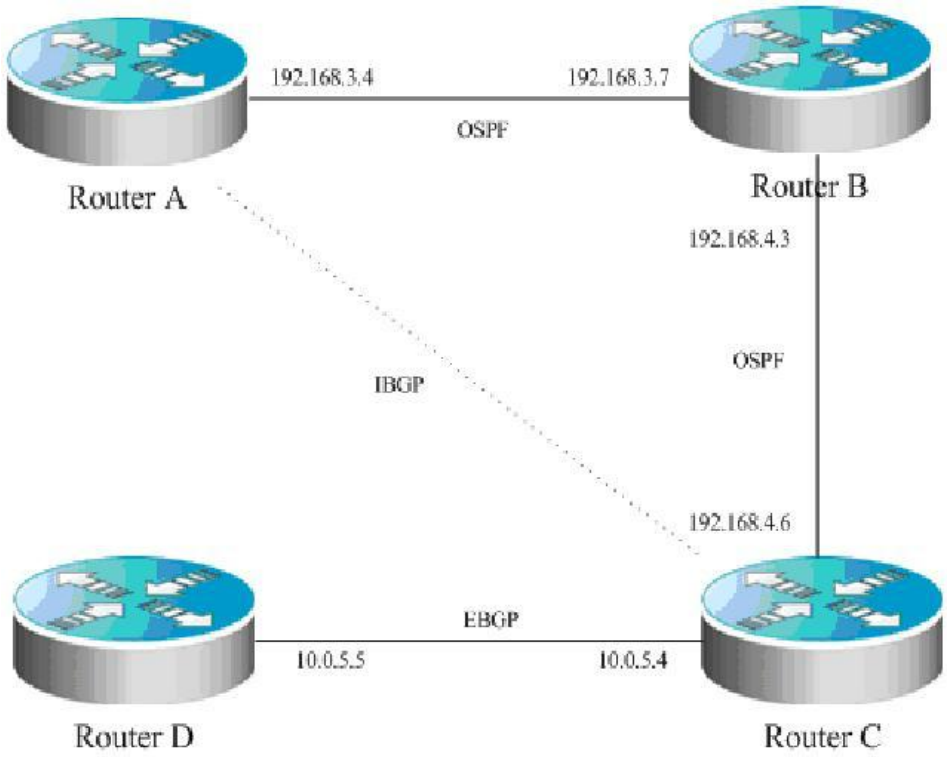
Router C Configuration:

```
!
router bgp 200
 neighbor 192.168.5.2 remote-as 100
```

32.20.2 Configuring BGP Synchronization

Use the **synchronization** command to configure synchronization in the BGP routing configuration mode, and use the **no synchronization** command to cancel the configured synchronization.

The following example shows the function of synchronization. The relationship among equipments and the assignment of the IP addresses are shown as the schematics:



In the schematics, there is a route p in the router A, which is sent to router C by the IBGP neighbor relationship. If the router C is configured with the BGP synchronization, it is necessary for the router C to wait for the IGP (this example uses the OSPF protocol) to receive the same route information p, so as to send the route p to the EBGP neighbor router

D. If the router C is configured asynchronously, it is not necessary for the BGP to wait for the IGP to receive the route p, so as to send the route p to the EBGP neighbor router D.

32.20.3 Configuring Neighbors to Use aspath Filter

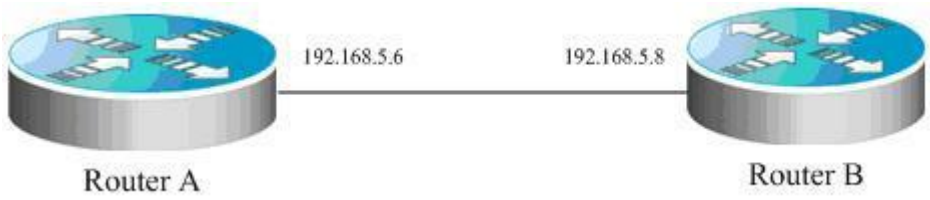
Configure the **as-path access-list** command for filtering in the configuration mode firstly. Enter into the route configuration mode of the BGP after configuration, and use the **neighbor filter-list** command to apply the configured as-path access list among the BGP neighbors to filter AS paths.

The detailed configurations are as below:

```
router bgp 200
neighbor 193.1.12.10 remote-as 100
neighbor 193.1.12.10 filter-list 2 out
neighbor 193.1.12.10 filter-list 3 in
ip as-path access-list 2 permit _200$
ip as-path access-list 2 permit ^100$
ip as-path access-list 3 deny _690$
ip as-path access-list 3 permit .*
```

This configuration indicates that only the routes permitted by the **as-path access-list** *2* can be advertised to the neighbor 193.1.12.10, and the advertised routes from the neighbor 193.1.12.10 can be received only they are permitted by the **as-path access-list** *3.*

The following diagram is a configuration eaxmple showing the relationship and IP addresses of devices:



Do AS path-based filter on Router A.

The following presents the configuraiton of various devices:

Router A configuration:

```
!
ip as-path access-list 4 deny ^300_
ip as-path access-list 4 permit .*
ip as-path access-list 5 deny ^450_65_
ip as-path access-list 5 permit .*
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 192.168.5.8 remote-as 200
 neighbor 192.168.5.8 filter-list 5 in
 neighbor 192.168.5.8 filter-list 4 out
```

Router B configuration:

```
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 192.168.5.6 remote-as 100
```

32.20.4 Configuring Route Aggregation

Use the **aggregate-address** command to configure an aggregated route in the route configuration mode. Once any route is within the configured range, this aggregated route will take into effect.

The concrete configuration is shown as follows:

```
router bgp 100
aggregate-address 193.0.0.0 255.0.0.0
```

Configure one aggregate route:

```
router bgp 100
aggregate-address 193.0.0.0 255.0.0.0 as-set
```

The **as-path** segment of the aggregated route is an collection of **ASs**:

```
router bgp 100
aggregate-address 193.0.0.0 255.0.0.0 summary-only
```

The aggregated route will not be advertised

32.20.5 Configuring Confederation

When configuring a confederatin, you need to use the **bgp confederation identifier** command to configure the AS number for external connection, and use the **bgp confederation peers** command to configure confederation members.

The concrete configuration is shown as follows:

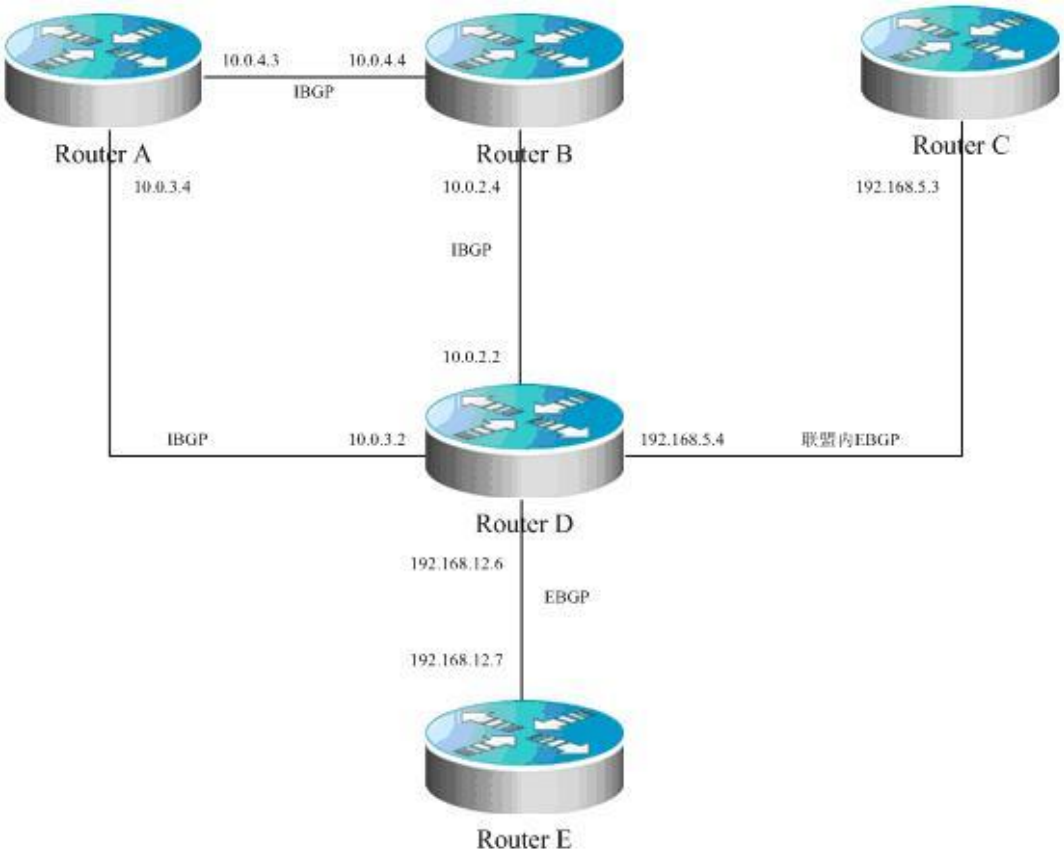
```
router bgp 6003
bgp confederation identifier 666
bgp confederation peers 6001 6002
neighbor 171.69.232.57 remote-as 6001
neighbor 171.69.232.55 remote-as 6002
neighbor 200.200.200.200 remote-as 701
```

The configuration of peer 200.200.200.200 out of the confederation is shown as follows:

```
router bgp 701
neighbor 171.69.232.56 remote-as 666
neighbor 200,200,200,205 remote-as 701
```

For the configuration, the first device is of the confederation, while the second device is not of the confederation, so they are of the EBGP neighbor relationship.

The following is an example showing the relastionship and IP addresses of devices:



The following presents the configuration of various devices:

Router A configuration:

```
!
router bgp 65530
 bgp confederation identifier 100
 bgp confederation peers 65531
 bgp log-neighbor-changes
 neighbor 10.0.3.2 remote-as 65530
 neighbor 10.0.4.4 remote-as 65530
```

Router B configuration:

```
!
router bgp 65530
 bgp confederation identifier 100
 bgp log-neighbor-changes
 neighbor 192.168.5.4 remote-as 65530
```

Router C configuration

```
!
router bgp 65531
 bgp confederation identifier 100
 bgp confederation peers 65530
 bgp log-neighbor-changes
 neighbor 10.0.3.2 remote-as 65530
```

```
 neighbor 10.0.4.4 remote-as 65530
```

Router D configuration:

```
!
router bgp 65530
 bgp confederation identifier 100
 bgp confederation peers 65531
 bgp log-neighbor-changes
 neighbor 10.0.2.4 remote-as 65530
 neighbor 10.0.3.4 remote-as 65530
 neighbor 192.168.5.3 remote-as 65531
 neighbor 192.168.12.7 remote-as 200
```

Router E configuration:

```
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 192.168.12.6 remote-as 100
```

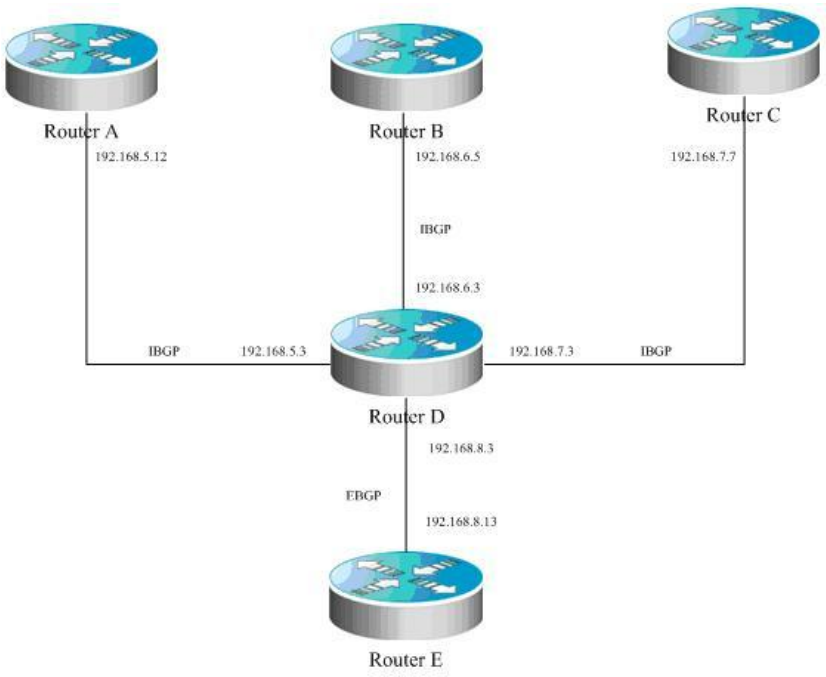
32.20.6 Configuring Route Reflector

When the route reflector is configured, it is necessary to use the **bgp client-to-client reflection** command to enable the route reflection function on the device. If there are more than one route reflector within one cluster, use the **bgp** *cluster-id* command to configure the cluster ID of the reflector, and use the **neighbor** *A.B.C.D* **route-reflector-client** command to add the peer to the client of the route reflection.

The concrete configuration is shown as follows:

```
router bgp 601
bgp cluster-id 200.200.200.200
neighbor 171.69.232.56 remote-as 601
neighbor 200,200,200,205 remote-as 701
neighbor 171.69.232.56 route-reflector-client
```

The following is an example showing the relastionship and IP addresses of devices:



In this configuration example, Router D is a route reflector. The following presents the configuration of various devices:

Router A configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 192.168.5.3 remote-as 100
 neighbor 192.168.5.3 description route-reflector server
```

Router B configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 192.168.6.3 remote-as 100
 neighbor 192.168.6.3 description route-reflector server
```

Router C configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 192.168.7.3 remote-as 100
 neighbor 192.168.7.3 description not the route-reflector server
```

Router D Configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 192.168.5.12 remote-as 100
 neighbor 192.168.5.12 description route-reflector client
```

```
 neighbor 192.168.5.12 route-reflector-client
 neighbor 192.168.6.5 remote-as 100
 neighbor 192.168.6.5 description route-reflector client
 neighbor 192.168.6.5 route-reflector-client
 neighbor 192.168.7.7 remote-as 100
 neighbor 192.168.7.7 description not the route-reflector client
 neighbor 192.168.8.13 remote-as 200
```

Router E configuration:

```
!
router bgp 500
 bgp log-neighbor-changes
 neighbor 192.168.8.3 remote-as 100
```

32.20.7 Configuring peergroup

Here will take the configuration of **peergroup** for IBGP and EBGP as an example.

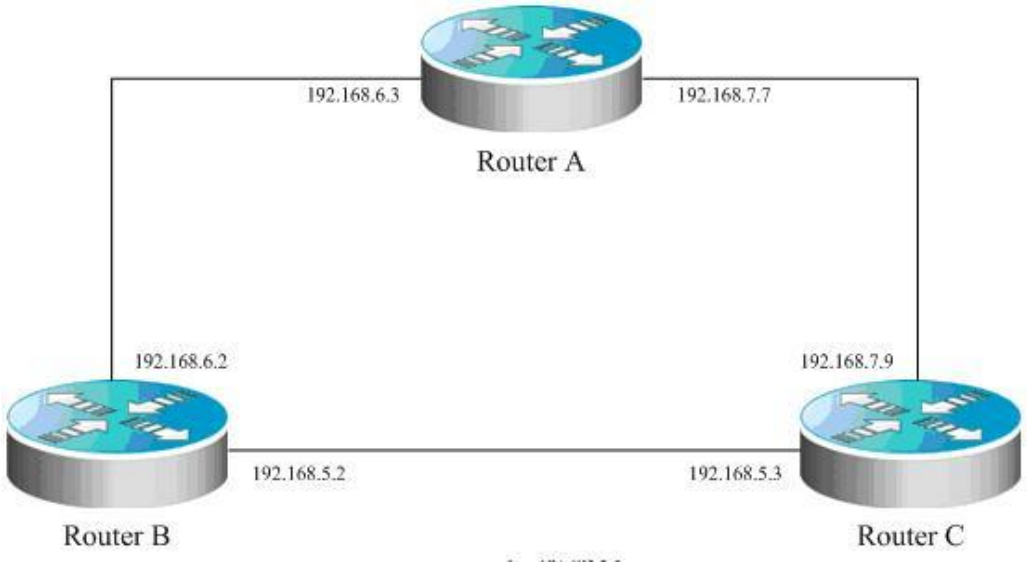
32.20.7.1 Configuring IBGP peergroup

Use the **neighbor** *internal* **peer-group** command to create a peer group named *internal* firstly, and then configure a remote AS and other options for the peer group. Use the **neighbor** *A.B.C.D* **peer-group internal** command to add the peers A.B.C.D into the peer group.

The configuration commands are as below:

```
router bgp 100
neighbor internal peer-group
neighbor internal remote-as 100
neighbor internal update-source loopback 0
neighbor internal route-map set-med out
neighbor internal filter-list 1 out
neighbor internal filter-list 2 in
neighbor 171.69.232.53 peer-group internal
neighbor 171.69.232.54 peer-group internal
neighbor 171.69.232.55 peer-group internal
neighbor 171.69.232.55 filter-list 3 in
```

The following is an example showing the relastionship and IP addresses of devices:



Router A configuration

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor ibgp-group peer-group
 neighbor ibgp-group description peer in the same as
 neighbor 192.168.6.2 remote-as 100
 neighbor 192.168.6.2 peer-group ibgp-group
 neighbor 192.168.6.2 description one peer in the ibgp-group
 neighbor 192.168.7.9 remote-as 100
 neighbor 192.168.7.9 peer-group ibgp-group
```

Router B configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor ibgp-peer peer-group
 neighbor ibgp-peer remote-as 100
 neighbor ibgp-peer route-map ibgp-rmap out
 neighbor 192.168.5.3 peer-group ibgp-peer
 neighbor 192.168.5.3 route-map set-localpref in
 neighbor 192.168.6.3 peer-group ibgp-peer
```

Router C configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor ibgp-group peer-group
 neighbor 192.168.5.2 remote-as 100
 neighbor 192.168.5.2 peer-group ibgp-group
 neighbor 192.168.7.7 remote-as 100
 neighbor 192.168.7.7 peer-group ibgp-group
```

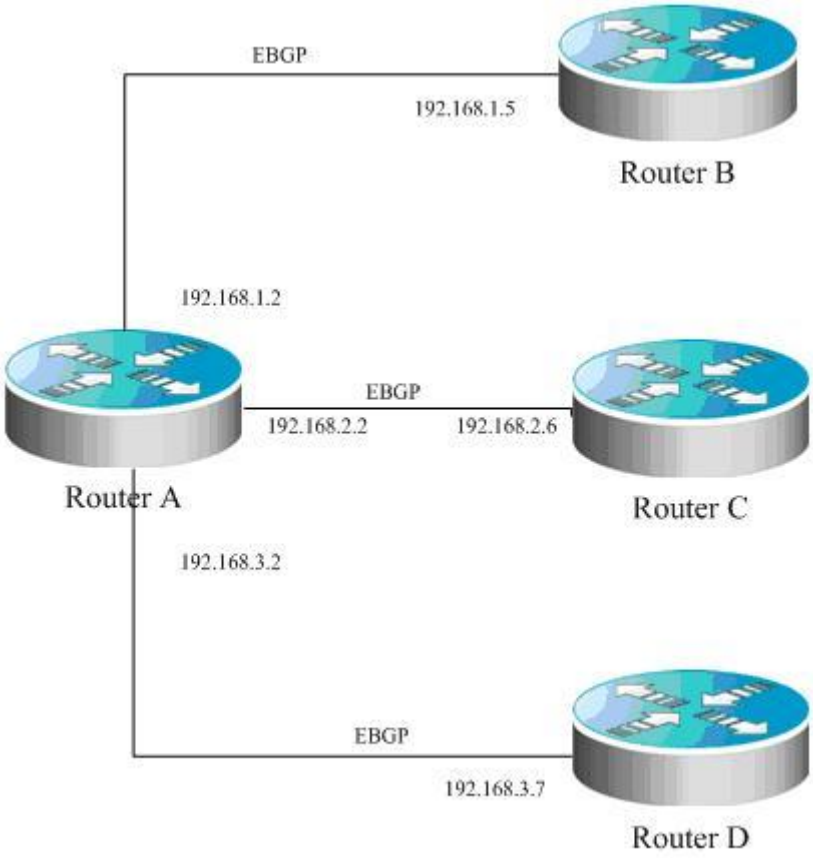
32.20.7.2 Configuring EBGP peergroup

Use the **neighbor** *A.B.C.D* **remote-as** *num* command to configure an EBGP peer . Use the **neighbor external peer-group** command to create a peer group named **external**, and then apply the **neighbor** *A.B.C.D* **peer-group** *external* command to add the peers A.B.C.D into the peer group *external*.

Following is an example of the specific configuration:

```
router bgp 100
neighbor external-peers peer-group
neighbor external-peers route-map set-metric out
neighbor external-peers filter-list 99 out
neighbor external-peers filter-list 101 in
neighbor 171.69.232.90 remote-as 200
neighbor 171.69.232.90 peer-group external-peers
neighbor 171.69.232.100 remote-as 300
neighbor 171.69.232.100 peer-group external-peers
neighbor 171.69.232.110 remote-as 400
neighbor 171.69.232.110 peer-group external-peers
neighbor 171.69.232.110 filter-list 400 in
```

Following is a diagram to show the configuration of peer-group:



The relationship between devices and the assigning of IP address are shown in the figure.
Router A configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor ebgp-group peer-group
 neighbor ebgp-group distribute-list 2 in
 neighbor ebgp-group route-map set-med out
 neighbor 192.168.1.5 remote-as 200
 neighbor 192.168.1.5 peer-group ebgp-group
 neighbor 192.168.2.6 remote-as 300
 neighbor 192.168.2.6 peer-group ebgp-group
 neighbor 192.168.2.6 distribute-list 3 in
 neighbor 192.168.3.7 remote-as 400
 neighbor 192.168.3.7 peer-group ebgp-group
!
```

Router B configuration:

```
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 100
!
```

Router C configuration:

```
!
router bgp 300
 bgp log-neighbor-changes
 neighbor 192.168.2.2 remote-as 100
!
```

Router D configuration:

```
!
router bgp 400
 bgp log-neighbor-changes
 neighbor 192.168.3.2 remote-as 100
!
```

32.20.8 Configuring TCP MD5

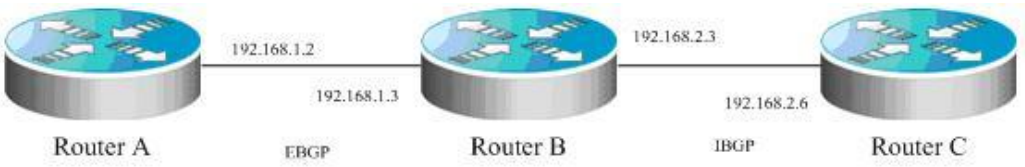
Use the CLI command **neighbor password** to configure the TCP MD5 for the BGP connection in the BGP configuration mode.

The configuration format is shown as follows:

```
router bgp 100
neighbor 171.69.232.54 remote-as 110
neighbor 171.69.232.54 password peerpassword
```

Here configures the *password* of peer 171.69.232.54 as *peerpassword.*

The following diagram shows the configuration of MD5 and IP address on various devices:



The AS of router A is 100, and the AS of router B and router C is 200. Router A establishes EBGP neighbor relationship with router B and uses EBGP as the MD5 password. Router B establishes IBGP neighbor relationship with router C and uses IBGP as the MD5 password.

router A configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 192.168.1.3 remote-as 200
 eighbor 192.168.1.3 password ebgp
!
```

Router B configuration:

```
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 100
 neighbor 192.168.1.2 password ebgp
 neighbor 192.168.2.6 remote-as 200
 neighbor 192.168.2.6 password ibgp
!
```

Router C configuration:

```
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 192.168.2.3 remote-as 200
 neighbor 192.168.2.3 password ibgp
!
```

33 Protocol-Independent Configuration

33.1 IP Routing Configuration

33.1.1 Configuring Static Routes

Static routes are manually configured so that the packets can be sent to the specified destination network go through the specified route. When it fails to learn the routes of some destination networks, it becomes critical to configure static routes. It is a common practice to configure a default route for the packets that do not have a definite route.

To configure static routes, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip route** [**vrf** *vrf_name*] *network mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent**] [**weight** *weight*] [**track** *object-number*]	Configure static routes.
DES-7210(config)# **no ip route** *network mask*	Delete Static Route
DES-7210(config)# **ip static route-limit** *number*	Specify the maximum number of static routes.
DES-7210(config)# **no ip static route-limit**	Restore the default maximum number of static routes.

For the example of configuring static routes, see “Example of Dynamic Routes Overriding Static Routes” in this chapter.

If they are not deleted, DES-7210 product will always retain the static routes. However, you can replace the static routes with the better routes learned by the dynamic routing protocols. Better routes mean that they have smaller distances. All routes including the static ones carry the parameters of the management distance. The following table shows the management distances of various sources of DES-7210 product:

Route source	Default management distance
Directly connected networks	0
Static route	1
OSPF route	110
ISIS route	115
RIP route	120
Unreachable route	255

Note

The static route redistribution shall be configured if the static routes are advertised by the dynamic routing protocols such as RIP and OSPF.

When a port is “down”, all routes to that port will disappear from the routing table. In addition, when DES-7210 product fails to find the forwarding route to the next-hop address, the static route will also disappear from the routing table.

When the specified VRF static routes are added to the corresponding VRF, if the egress is specified at the same time, but the VRF of the egress does not match the specified VRF, the addition will fail. If no VRF is specified, it is added to the global routing table by default.

By default, the weight of static route is 1. To view the static routes of non-default weight, execute the **show ip route weight** command. When there are load balanced routes to an IP address, the switch will assign traffic by their weights. The higher the weight of a route is, the more the route forwards. Router WCMP limit is 32, while the switch WCMP limit is related to product model because the weights supported by various chips are different. For the detailed information about the route weight value of specific model, please refer to the product specification paper.

When the sum of load-balancing route weights exceeds WCMP limit, the exceeded routes will not take effect. For example, if the WCMP limit on a device is 8, only one static route configuration is effective :

```
DES-7210(config)#ip route 10.0.0.0 255.0.0.0 172.0.1.2 weight 6

DES-7210(config)#ip route 10.0.0.0 255.0.0.0 172.0.1.4 weight 6

DES-7210(config)#show ip route 10.0.0.0

Routing entry for 10.0.0.0/8

  Distance 1, metric 0

  Routing Descriptor Blocks:

  *172.0.1.2, generated by "static"

DES-7210(config)#show ip route weight

------------[distance/metric/weight]-----------

S    10.0.0.0/8 [1/0/6] via 172.0.1.2
```

The maximum number of static routes is 1000 by default. If the number of static routes configured exceeds the specified upper limit, they will not be automatically deleted, but the addition will fail.

To view the configuration of IP route, execute the **show ip route** command to view the IP routing table. For details, refer to *Protocol-independent Command Configuration.*

33.1.2 Configuring Default Route

Not all devices have a complete network-wide routing table. To allow every device to route all packets, it is a common practice that the powerful core network is provided with a complete routing table, while the other devices have a default route set to this core router. Default routes can be transmitted by the dynamic routing protocols, and can also be manually configured on every router.

Default routes can be generated in two ways: 1) manual configuration. For details, see *Configuring Static Routes* in the last section; 2) manually configuring the default network.

Most internal gateway routing protocols have a mechanism that transmits the default route to the entire routing domain. The device that needs to transmit the default route must have a

default route. The transmission of the default route in this section applies only to the RIP routing protocol. The RIP always notifies the “0.0.0.0” network as the default route to the routing domain. For more information on how OSPF generates and transmits the default routes, see *OSPF Routing Protocol Configuration Guide*.

To general static routes, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip default-network** network	Configure the default network.
DES-7210(config)# **no ip default-network** network	Delete the default network.

Note

To generate the default routes by using the **default-network** command, the following condition must be met: The default network is not a directly-connected port network, but is reachable in the routing table.

Under the same condition, the RIP can also transmit the default route. Alternatively, there is another way to do so, that is, by configuring the default static route or learning the 0.0.0.0/0 router via other routing protocols.

If the router has a default route, whether learned by the dynamic routing protocol or manually configured, when you use the **show ip route** command, the “gateway of last resort” in the routing table will show the information of the last gateway. A routing table may have multiple routes as alterative default routes, but only the best default route becomes the “gateway of last resort”.

33.1.3 Configuring the Number of Equivalent Routes

If the load balancing function is needed, you can set the number of equivalent routes for control. An equivalent route is an alternative path to the same destination address. When there is only one equivalent route, one destination address can be configured with only one route, and the load balancing function is cancelled.

To configure the number of equivalent routes, execute the following commands in the global configuration mode. The **no** form of this command restores the default number of equivalent routes.

This command is valid for both ipv4 and ipv6. That is to say, after configuring this command, the maximum numbers of the equivalent route path to IPv4 and IPv6 destination are the same value configured.

Command	Function
maximum-paths [*number*]	Configure the number of equivalent routes (in the range 1 to 32).

33.2 Route-Map Configuration

Route-map is a collection of filter policy for the routing protocol and policy route, independent from the detailed routing protocol. Route-map is used to filter and modify the routing information for the routing protocol, and control the packet forwarding for the policy route.

To define the route map, use the following command in the global configuration mode:

Command	Function
DES-7210(config)# **route-map** *route-map-name* [**permit** | **deny**] *sequence*	Define the route map. *Sequence*: 0-65535
DES-7210(config)# **no route-map** *route-map-name* {[**permit** | **deny**] *sequence*}	Remove the route map.

When you configure the rules for a route map, you can execute one or multiple **match** or **set** commands. If there is no match command, all will be matched. If there is no set command, not any action will be taken.

To define the matching conditions for the rules, execute the following commands in the route map configuration mode:

Command	Function
DES-7210(config-route-map)# **match community** {*standard-list-number* | *expanded-list-number* | *community-list-name*}	Match the community attribute of BGP route.
DES-7210(config-route-map)# **match interface** *interface-type interface-number*	Match the next-hop interface for the route.
DES-7210(config-route-map)# **match ip address** *access-list-number* […*access-list-number*]	Match the ACL IP address.
DES-7210(config-route-map)# **match ip next-hop** *access-list-number* […*access-list-number*]	Match the next-hop IP address in the ACL.
DES-7210(config-route-map)# **match ip route-source** *access-list-number* […*access-list-number*]	Match the route source IP address in the ACL.
DES-7210(config-route-map)# **match ipv6 address** { *access-list-name* | **prefix-list** *prefix-list-name* }	Match the IPv6 ACL or prefix list.
DES-7210(config-route-map)# **match ipv6 next-hop** { *access-list-name* | **prefix-list** *prefix-list-name* }	Match the next-hop IP address in the ACL or the prefix list.
DES-7210(config-route-map)# **match ipv6 route-source** { *access-list-name* | **prefix-list** *prefix-list-name* }	Match the route source IP addres in the ACL or the prefix list.
DES-7210(config-route-map)# **match metric** *metric*	Match the route metric value. *metric* 0-4294967295
DES-7210(config-route-map)# **match origin** {**egp** | **igp** | **incomplete**}	Match the route origin type.

Command	Function
DES-7210(config-route-map)# **match route-type** {**local** | **internal** | **external** [**level-1** | **level-2**]}	Match the route type.
DES-7210(config-route-map)# **match tag** *tag*	Match the route tag value. *tag* 0-4294967295

To define the oeration after matching, use the following command in the route map configuration mode:

Command	Function
DES-7210(config-route-map)# **set aggregator as** *as-num ip_addr*	Set the AS attribute value for the route aggregator.
DES-7210(config-route-map)# **set as-path prepend** *as-number*	Set the AS_PATH attribute value.
DES-7210(config-route-map)# **set comm-list** *community-list-number* | *community-list-name* **delete**	Cancel all community attribute value in the COMMUNITY_LIST.
DES-7210(config-route-map)# **set community** {*community-number*[*community-numbe…*] **additive** | **none**}	Set the COMMUNITY attribute value.
DES-7210(config-route-map)# **set dampening** *half-life reuse suppress max-suppress-time*	Set the route dampening parameter.
DES-7210(config-route-map)#**set extcommunity** {**rt** *extend-community-value* | **soo** *extend-community-value*}	Set the extended community attribute value.
DES-7210(config-route-map)# **set interface** *interface-type interface-number*	Set the interface for the packet forwarding.
DES-7210(config-route-map)# **set ip default next-hop** *ip-address*	Set the default next-hop IP address.
DES-7210(config-route-map)# **set ip next-hop** *ip-address*	Set the next-hop IP address.
DES-7210(config-route-map)# **set ip next-hop verify-availability** *ip-address* **track** *track-object-num*	Set the reachability of the next-hop IP address.
DES-7210(config-route-map)# **set level** {**stub-area** | **backbone** | **level-1** | **level-1-2** | **level-2**}	Set the route area.
DES-7210(config-route-map)# **set local-preference** *number*	Set the LOCAL_PREFERENCE value.

Command	Function
DES-7210(config-route-map)# **set metric** *metric*	Set the metric value of the route redistribution.
DES-7210(config-route-map)# **set metric** [+ *metric-value* |- *metric-value* | *metric-value*]	Set the metric type of route redistribution.
DES-7210(config-route-map)# **set metric-type** {**type-1** | **type-2 | external** | **internal**}	Set the metric type of route redistribution.
DES-7210(config-route-map)# **set next-hop** *next-hop*	Set the next-hop IP address for the route redistribution. *next-hop* next-hop IP address.
DES-7210(config-route-map)# **set origin** {**egp** | **igp** | **incomplete**}	Set the route origin attribute.
DES-7210(config-route-map)#**set originator-id** *ip-addr*	Set the route originator id.
DES-7210(config-route-map)# **set tag** *tag*	Set the tag value for the route redistribution.

For different route-map applications, the results of the match and set command are different. To make the user know whether the match and set command is appropriate for the current application or not, DES-7210 provides the user the message in the following circumstances:

When associating the route-map command, check the appropriateness of the match and set command configuration in the route-map and the current associated application. If it is not appropriate, the message prompts.

When configuring the route-map, match or set command, check the appropriateness of all applications associated with the route-map and the match and set command configuration in the route-map. If it is not appropriate, the message prompts.

Caution

The above message promption is not supported by the application of PBR and route-map association.

33.3 Route Redistribution

33.3.1 Configuring Route Redistribution

To support the routers to run multiple routing protocol processes, DES-7210 product provides the function for redistributing the route information from one routing process to another routing process. For example, you can redistribute the routes in the OSPF routing area to the RIP routing area , or those in the RIP routing area to the OSPF routing area. Routes can be redistributed among all the IP routing protocols.

In route redistribution, the route maps are often used to enforce conditional control over the mutual route redistribution between two routers.

To redistribute routes from one routing area to another and control route redistribution, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210(config-router)# **redistribute** *protocol* [*process-id*] [**metric** *metric*] [**metric-type** *metric-type*] [**match internal** | **external** *type*| **nssa-external** *type*] [[**tag** *tag*] [**route-map** *route-map-name*] [**subnets**]	Set route redistribution. *Protocol* (protocol type): bgp, connected, isis, rip, static
DES-7210(config-router)# **default-metric** *metric*	Set the default metric for all redistributed routes.

Route redistribution may easily cause loops, so you must be very careful in using them.

Note

When the route redistribution is configured in the OSPF routing process, the metric of 20 is allocated to the redistributed routes with the type of Type-2 by default. This type belongs to the least credible route of the OSPF.

33.3.2 Configuring Default Route Distribution

To advertise the default route, it is necessary for routing protocol to introduce the default route to the process, or enforce generating a default route.

To distribute the default route, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210(config-router)# **default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]	Introduce the default route to the routing protocol process and advertise the route default. **always(optional):** a default route is always introduced to the process no matter whether the default route exists in the local routing table or not. **metric(optional):** set the metric value for the introduced default route. **metric-type(optional):** set the default route type. **route-map(optional):** filter and set the default route.
DES-7210(config-router)# **no default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]	Cancel the introduction of the default route to the routing protocol process and the route default advertisement.

33.3.3 Route Filtering Configuration

Route filtering is the process to control the incoming/outgoing routes so that the router only learns the necessary and predictable routes, and only advertise the necessary and predictable routes to external trusted devices. The divulgence and chaos of the routes may affect the running of the network. Particularly for telecom operators and financial service networks, it is essential to configure route filtering.

33.3.3.1 Controlling Route Updating Advertising

To prevent other routers or routing protocols from dynamically learning one or more route message, you can configure the control over route updating advertising to prevent the specified route update.

To prevent route updating advertising, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210(config-router)# **distribute-list** {[*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name* **out** [*interface-type interface-number*]	According to ACL rules, permit or deny some routes. **Prefix:** This keyword specifies the prefix list for filtering routes. The prefix list should be separately configured by using the **ip prefix-list** command.
DES-7210(config-router)# **no distribute-list** {[*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name}* **out** [*interface-type interface-number* | *protocol*]	Remove the configuration.

Note When you configure the OSPF, you cannot specify the interface and the features are only applicable to the external routes of the OSPF routing area.

33.3.3.2 Controlling Route Updating processing

To avoid processing some specified routes of the incoming route update packets, you can configure this feature. This feature does not apply to the OSPF routing protocol.

To control route updating processing, execute the following commands in the routing process configuration mode:

Command	Function
DES-7210(config-router)# **distribute-list** {[*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name*} **in** [*interface-type interface-number*]	According to ACL rules, permit or deny receiving distributed routes. **Prefix:** This keyword specifies the prefix list for filtering routes. The prefix list should be separately configured by using the ip prefix-list command. **Gateway:** Use the prefix list to filter the routes distributed according to the source of the routes.

Command	Function
DES-7210(config-router)# **no distribute-list** {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* } **in** [*interface-type interface-number*]	Remove the configuration.

33.4 Configuration Examples

33.4.1 Example of Route-map Configuration

The route map can be configured very flexibly to be used on the route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

In the following example, the OSPF routing protocol redistributes only the RIP routes whose hops are 4. In the OSPF routing area, the type of the routes is external route type-1, the initial metric is 40, and the route tag is 40.

Configure OSPF

```
DES-7210(config)# router ospf 1
DES-7210(config-router)# redistribute rip subnets route-map redrip
DES-7210(config-router)# network 192.168.12.0 0.0.0.255 area 0
```

Configure the access control list

```
DES-7210(config)# access-list 20 permit 200.168.23.0
```

Configure the route map

```
DES-7210(config)# route-map redrip permit 10
DES-7210(config-route-map)# match metric 4
DES-7210(config-route-map)# set metric 40
DES-7210(config-route-map)# set metric-type type-1
DES-7210(config-route-map)# set tag 40
```

In the following configuration example, the RIP routing protocol redistributes only the OSPF routes whose tag is and initial metric is 10.

Configure RIP

```
DES-7210(config)# router rip
DES-7210(config-router)# version 2
DES-7210(config-router)# redistribute ospf 1 route-map redospf
DES-7210(config-router)# network 200.168.23.0
```

Configure route map

```
DES-7210(config)# route-map redospf permit 10
DES-7210(config-route-map)# match tag 10
DES-7210(config-route-map)# set metric 10
```

In the following configuration example, the OSPF routing protocol redistributes the RIP routes. Since the unsupported rule for the route-map application has been configured, after redistributing the route-map, the printed message prompts that the application not support the corresponding rule.

Configure route-map

```
DES-7210(config)# route-map redrip permit 10
DES-7210(config-route-map)# match length 1 3
DES-7210(config-route-map)# match route-type external DES-7210(config-route-map)# set level backbone
```

Configure OSPF

```
DES-7210(config)# router ospf 1
DES-7210(config-router)# redistribute rip subnets route-map redrip
% ospf redistribute rip not support match length
% ospf redistribute rip not support match route-type
% ospf redistribute rip not support set level backbone
```

33.4.2 Example of Static Route Redistribution

- **Configuration requirements**

One router exchanges route information with other routers via the RIP. In addition, there are three static routes. The RIP is only allowed to redistribute two routes: 172.16.1.0/24 and 192.168.1.0/24.

- **Configuration of the Routers**

This is a common distribution list-based route filtering configuration example in practice. Note that the metric is not specified for the routes to be redistributed in the following configuration. Since a static route will be redistributed,the RIP will automatically assign the metric. In the RIP configuration, the version must be specified and the route aggregation must be disabled for the access list allows the 172.16.1.0/24 route. To advertise the route, the RIP protocol must first support the classless route, and the route cannot be aggregated to the 172.16.0.0/16 network.

Configure the static route

```
DES-7210(config)# ip route 172.16.1.0 255.255.255.0 172.200.1.2
DES-7210(config)# ip route 192.168.1.0 255.255.255.0 172.200.1.2
DES-7210(config)# ip route 192.168.2.0 255.255.255.0 172.200.1.4
```

Configure RIP

```
DES-7210(config)# router rip
DES-7210(config-router)# version 2
DES-7210(config-router)# redistribute static
DES-7210(config-router)# network 192.168.34.0
DES-7210(config-router)# distribute-list 10 out static
DES-7210(config-router)# no auto-summary
```

Configure the extended ACL

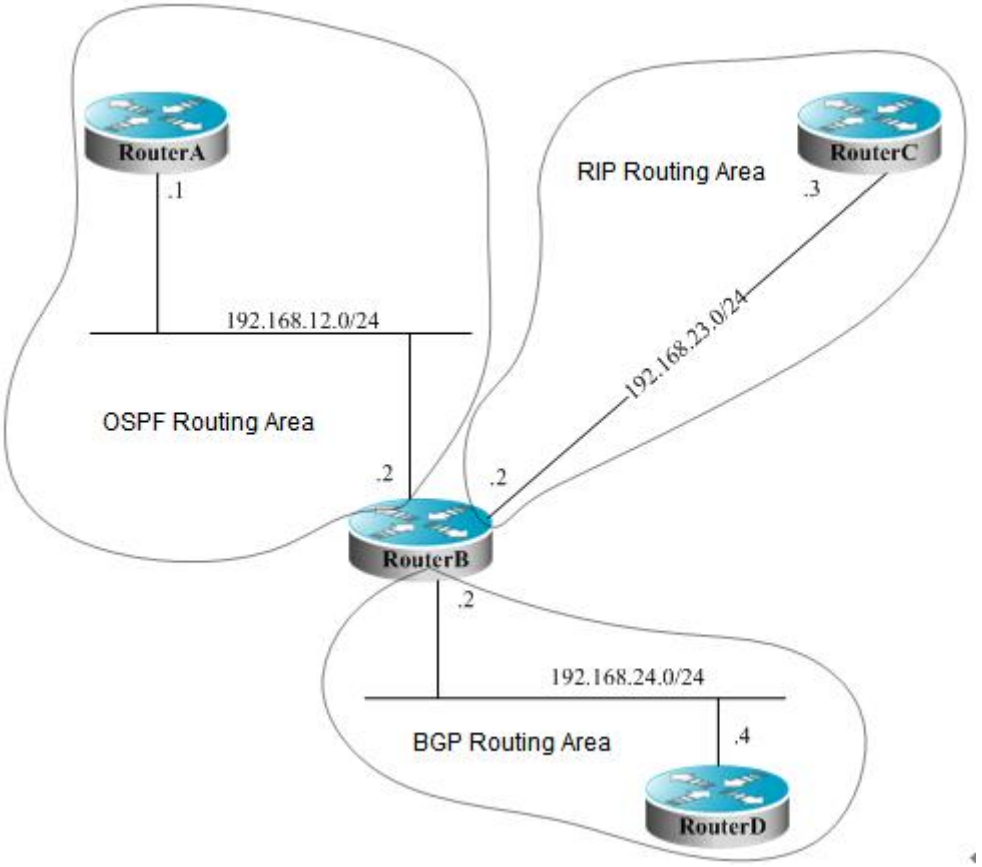
```
DES-7210(config)# access-list 10 permit 192.168.1.0
DES-7210(config)# access-list 10 permit 172.16.1.0
```

33.4.3 Example of Dynamic Route Protocol Redistribution

■ **Configuration requirements**

The connection among four routers is shown in the Figure-1. Router A belongs to the OSPF routing area, Router C belongs to the RIP routing area, Router D belongs to the BGP routing area and Router B is connected to three routing areas. Router A advertises the two routes of 192.168.10.0/24 and 192.168.100.1/32, Router C advertises the network routes of 200.168.3.0/24 and 200.168.30.0/24, and Router D advertises the network routes of 192.168.4.0/24 192.168.40.0/24.

Figure-1 Example of Dynamic Routing Protocol Redistribution



On Router B, the OSPF redistributes the RIP routes with the route Type-1, redistributes the BGP routes carrying with the community attribute 11:11. The RIP redistributes the 192.168.10.0/24 route in the OSPF routing area whose metric is 3, amd advertises a default route to the RIP routing area.

■ **The specific configuration of the routers**

When the routing protocols redistribute routes among them, the simple route filtering can be controlled by the distribution list. However, different attributes must be set for different routes, and this is not possible for the distribution list, so the route map must be configured for control. The route map provides more control functions than the distribution list, and it is more complex to configure. Therefore, do not use the route map if possible for simple configuration of the router. The following example does not use the route map.

Router A configuration:

Configure the network interface

```
DES-7210(config)# interface gigabitEthernet 0/0
```

```
DES-7210(config-if)# ip address 192.168.10.1 255.255.255.0
DES-7210(config)# interface loopback 1
DES-7210(config-if)# ip address 192.168.100.1 255.255.255.0
DES-7210(config-if)# no ip directed-broadcast
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# ip address 192.168.12.55 255.255.255.0
```

Configure the OSPF

```
DES-7210(config)# router ospf 12
DES-7210(config-router)# network 192.168.10.0 0.0.0.255 area 0
DES-7210(config-router)# network 192.168.12.0 0.0.0.255 area 0
DES-7210(config-router)# network 192.168.100.0 0.0.0.255 area 0
```

Router B configuration:

Configure the network interface

```
DES-7210(config)# interface gigabitEthernet 0/0
DES-7210(config-if)# ip address 192.168.12.5 255.255.255.0
DES-7210(config)# interface Serial 1/0
DES-7210(config-if)# ip address 192.168.23.2 255.255.255.0
```

#Configure the OSPF and set the redistribution route type

```
DES-7210(config)# router ospf 12
DES-7210(config-router)# redistribute rip metric 100 metric-type 1 subnets
DES-7210(config-router)# network 192.168.12.0 0.0.0.255 area 0
```

#Configure the RIP and use the distribution list to filter the redistributed routes

```
DES-7210(config)# router rip
DES-7210(config-router)# redistribute ospf 12 metric 2
DES-7210(config-router)# network 192.168.23.0
DES-7210(config-router)# distribute-list 10 out ospf
DES-7210(config-router)# no auto-summary
```

Configure the BGP

```
DES-7210(config)# router bgp 2
DES-7210(config-router)# neighbor 192.168.24.4 remote-as 4
DES-7210(config-router)# address-family ipv4
DES-7210(config-router-af)# neighbor 192.168.24.4 activate
DES-7210(config-router-af)# neighbor 192.168.24.4 send-community
```

Configure the route-map

```
DES-7210(config)# route-map ospfrm
DES-7210(config-route-map)# match community cl_110
```

Define the access list

```
DES-7210(config)# access-list 10 permit 192.168.10.0
```

Define the community list

```
DES-7210(config)# ip community-list standard cl_110 permit 11:11
```

Router C configuration:

Configure the network interface

```
DES-7210(config)# interface gigabitEthernet 0/0
DES-7210(config-if)# ip address 192.168.30.1 255.255.255.0
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# ip address 192.168.3.1 255.255.255.0
DES-7210(config)# interface serial 1/0
DES-7210(config-if)# ip address 192.168.23.3 255.255.255.0
```

Configure the RIP

```
DES-7210(config)# router rip
DES-7210(config-router)# network 192.168.23.0
DES-7210(config-router)# network 192.168.3.0
DES-7210(config-router)# network 192.168.30.0
```

Router D configuration:

Configure the network interface

```
DES-7210(config)# interface gigabitEthernet 0/0
DES-7210(config-if)# ip address 192.168.40.1 255.255.255.0
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# ip address 192.168.4.1 255.255.255.0
DES-7210(config)# interface serial 1/0
DES-7210(config-if)# ip address 192.168.24.4 255.255.255.0
```

Configure the BGP

```
DES-7210(config)# router bgp 4
DES-7210(config-router)# neighbor 192.168.24.2 remote-as 2
DES-7210(config-router)# redistribute connected route-map bgprm
DES-7210(config-router)# address-family ipv4
DES-7210(config-router-af)# neighbor 192.168.24.2 activate
DES-7210(config-router-af)# neighbor 192.168.24.2 send-community
```

Configure the route-map

```
DES-7210(config)# route-map bgprm
DES-7210(config-route-map)# match community 22:22
```

OSPF routes found on router A:

```
O E1 192.168.30.0/24 [110/101] via 192.168.12.5, 00:04:07, FastEthernet0/1
O E1 192.168.3.0/24 [110/101] via 192.168.12.5, 00:04:07, FastEthernet0/1
```

RIP routes found on Router C:

```
R    192.168.10.0/24 [120/2] via 200.168.23.2, 00:00:00, Serial1/0
R    192.168.10.0/24 [120/2] via 200.168.23.2, 00:00:00, Serial1/0
```

34 Policy-Based Routing Configuration

Policy-based routing provides a packet forwarding mechanism more flexible than destination-IP-address-based routing. Policy-based routing on an interface allows the router to determine how to process the packets from the interface to be routed according to the route map.

To use the policy-based routing, you must specify and create the route map for it use. A route map consists of multiple policies, each of which defines one or multiple matching rules and corresponding operations. After policy-based routing is applied to an interface, the router checks the packets, and then forwards the packets not matching against any policy in the route map by the general rule. For the packets that match a policy in the route map, it processes them according to the operation defined in the policy. For the configuration of the route map, refer to Protocol-independent Command Configuration Guide.

To configure policy-based routing, perform the following steps:

1. Define the route map. A route map consists of many policies in the order of their sequence numbers. The router will search the route map until it finds a matched policy.

   To define the route map, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **route-map** *route-map-name* [**permit** | **deny**] *sequence*	Define the route map.
DES-7210(config)# **no route-map** *route-map-name* {[**permit** | **deny**] *sequence*}	Delete the route map.

2. Define the matching rule for eacy policy of the route map;

   To define the matching rule for a policy, execute the following commands in the route map configuration mode:

Command	Function
DES-7210(config-route-map)# **match ip address** *access-list-number*	Match the IP address in the access list.
DES-7210(config-route-map)# **match length** *min max*	Match the length of the packet.

3. Define the operation performed if the match rule is met.

   To define the operation after matching, execute the following commands in the route map configuration mode:

Command	Function
DES-7210(config-route-map)# **set ip default next-hop** *ip-address*[*weight*][*ip-address*[*weight*]]	Set the next-hop IP address of the packets without any definite routes in the routing table.

Command	Function
DES-7210(config-route-map)# **set ip next-hop** *ip-address* [*weight*][*ip-address*[*weight*]]	Set the next-hop IP address of the packets.
DES-7210(config-route-map)# **set interface** *intf_name*	Set the out interface.
DES-7210(config-route-map)#**set default interface** *intf_name*	Set the default interface.
DES-7210(config-route-map)# **set ip precedence**	Modify the precedence of the IP pacekt.
DES-7210(config-route-map)# **set ip tos**	Modify the value of TOS domain in IP packet.
DES-7210(config-route-map)# **set ip dscp**	Modify the value of DSCP domain in IP packet.

4. Apply the route map to the specified interface.

   To apply a policy-based routing to the interface, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip policy route-map** *name*	Use the specified route-map for filtering on the interface.
DES-7210(config-if)# **no ip policy route-map**	Cancel the route-map applied to the interface.

5. Configure the policy-based routing for the local packets.

Command	Function
DES-7210(config-if)# **ip local policy route-map** *name*	Use the specified route-map for filtering the local packets.
DES-7210(config-if)# **no ip local policy route-map**	Cancel the route-map applied to the local packets.

For example:

Configure policy-based routing on interface GigabitEthernet 4/1 so that all incoming packets are forwarded to the device whose next hop is 192.168.5.5.

```
DES-7210(config)# access-list 1 permit any
DES-7210(config)# route-map name
DES-7210(config-route-map)# match ip address 1
DES-7210(config-route-map)# set ip next-hop 192.168.5.5
DES-7210(config-route-map)# exit
DES-7210(config)# interface gigabitEthernet 4/1
DES-7210(config-if)# ip policy route-map name
```

To configure load-balancing or redundancy backup for the policy-based routing, execute the following command in the global configuration mode:

Command	Function
DES-7210(config)# **ip policy** {**load-balance** | **redundance**}	Set the load-balancing or redundancy for the policy-based routing.
DES-7210(config)# **no ip policy**	Restore the load allocation mode for the policy-based routing.

The WCMP(Weighted Cost Multiple Path) supports up to 4 next hops and the ECMP(Equal Cost Multiple Path) supports up to 32 next hops when load balancing is configured for the policy-based routing.

When the default policy-based routing is configured, the WCMP supports up to 4 next hops and the ECMP supports up to 32 next hops.

For the route-map configuration command, see the *Protocol-independent Command Configuration Guide*.

Supported commands for the switch:

1. **[no] ip policy route-map**
2. **match ip address**
3. **set ip next-hop**
4. **set ip default next-hop**
5. **set ip tos**
6. **set ip dscp**
7. **set ip precedence**

Supported commands for the router:

1. **[no] ip policy route-map**
2. **ip local policy route-map**
3. **match ip address**
4. **match length**
5. **set ip next-hop**
6. **set ip default next-hop**
7. **set interface**
8. **set default interface**
9. **set ip tos**
10. **set ip dscp**
11. **set ip precedence**

1. On DES-7210 products, one interface can be configured with up to one route map. When multiple route maps are configured on an interface, they will overwrite each other and the policy-based routing only uses the first ACL configured in the route-map sequence. Therefore, when you use the policy-based routing, you are recommended to configure only one ACL for each route-map sequence.

2. If the configured route-map sequence has only the next hop without the ACL, this indicates all packets are matched. If the route-map sequence has only the ACL without the next hop, the matched packets are forwarded in the ordinary way. If the route-map sequence has neither the ACL nor the next hop, it indicates all the matched packets are forwarded in the ordinary way.

3. Policy-based routing only supports ACL number configuration, but not ACL name configuration. If the ACL number is configured but the ACL does not exist, this indicates all the packets are matched. If the ACL is configured but there is no ACE in it, the route-map sequence is skipped and the matching starts from the ACL of the next route-map sequence.

Caution

4. On the switch, if IP packets match with “deny” ACE, all the packets are forwarded in the ordinary way. If IP packets match with “deny any any” ACE(At the end of every ACL, it always be a default “deny any any” ACE), it skips to the next route submap to match again. On the router, if IP packets match with “deny” ACE and the route submap has other ACLs, it skips to the next ACL of this route submap to match. If the route submap has no ACL, then it skips to the ACL of the next route routemap to match. In that way, in the end it matches the “permit” ACE and then apply the corresponding set rule of route submap. If all ACLs of the routemap are not matched, all the packets will be forwarded in the ordinary way.

5. If you do not want to apply any policy-based routing to the incoming packets, you should add the ACE of “deny device IP address” at the beginning of the ACL in the PBR rule.

6. Under the redundant backup mode, the first resolved nexthop takes effect. If all the nexthops are not resolved, packets will be dropped. The first nexthop will also take effect as long as it is reachable, even though it is not resolved at the first time.

7. The routers do not support the PBR configuration on the dial port.

35 IPv6 Configuration

35.1 IPv6 Overview

As the Internet is growing rapidly and the IPv4 address space is exhausting, the limitation of the IPv4 is more obvious. The research and practice of the next generation of the Internet Protocol becomes popular. Furthermore, the IPng workgroup of the IETF determines the protocol specification of IPng referred to as IPv6. Refer to RFC2460 for details.

Key Features of Ipv6:

- More Address Space

The length of address will be extended to 128 bits from the 32 bits of Ipv4. Namely, there are 2^128-1 addresses for IPv6. The IPv6 adopts the hierarchical address mode and supports multiple-level IP address assignment, for example, from the Internet backbone network to the internal subnet of enterprises.

- Simplified Format of Packet Header

The design principle of new IPv6 packet header is to minimize the overhead. For this reason, some non-critical fields and optional fields are removed from the packet header and placed into the extended packet header. The length of the IPv6 address is 4 times of IPv4 address; its packet header is only 2 times of IPv4. The improved IPv6 packet header is more efficient for forwarding, for instance, there is no checksum in the IPv6 packet header and it is not necessary for the IPv6 router to process the fragment during forwarding (the fragment is completed by the originator).

- High-efficient hierarchical Addressing and Routing Structure

The IPv6 adopts the aggregation mechanism and defines flexible hierarchical addressing and routing structure, and several networks at the same level is presented as a unified network prefix at the higher level of routers. So it obviously reduces the entries that the router must maintain and greatly minimizes the routing and storage overhead.

- Simple Management: Plug and Play

Simplify the management and maintenance of the network node by the implementation of a series of auto-discovery and auto-configuration functions. Such as the Neighbor Discovery, the MTU Discovery, the Router Advertisement, the Router Solicitation and the Auto-configuration technologies provide related service for the plug and play. It should be mentioned that the IPv6 supports such address configuration methods as the stateful and the stateless. In the IPv4, the dynamical host configuration protocol (DHCP) implements the automatic setting of the host IP address and related configuration, while the IPv6 inherits this auto-configuration service of the IPv4 and refers to it as the Stateful Auto-configuration. Furthermore, the IPv6 also adopts an auto-configuration service, referred to as the Stateless Auto-configuration. During the stateless auto-configuration, the host obtains the local address of the link, the address prefix of local device and some other related configuration information automatically.

- Security

The IPSec is an optional extended protocol of the IPv4, while it is only a component of the IPv6 used to provide security. At present, the IPv6 implements the Authentication Header (AH) and Encapsulated Security Payload (ESP) mechanisms. Where, the former authenticates the integrity

of the data and the source of the IP packet to ensure that the packet does come from the node marked by the source address, while the latter provides the data encryption function to implement the end-to-end encryption.

- More Excellent QoS Support

The new field in the IPv6 packet header defines how to identify and process the data flow. The Flow Label field in the IPv6 packet header is used to identify the data flow ID, by which the IPv6 allows users to put forward the requirement for the QoS of communication. The router can identify all packets of some specified data flow by this field and provide special processing for these packet on demand.

- Neighbor Nodes Interaction-specific New Protocol

The Neighbor Discovery Protocol of the IPv6 uses a series of IPv6 control information message (ICMPv6) to carry out the interactive management of the neighbor nodes (the nodes of the same link). The Neighbor Discovery Protocol and high-efficient multicast and unicast Neighbor Discovery message replace previous broadcast-based address resolution protocol (ARP) and the ICMPv4 router discovery message.

- Extensibility

The IPv6 provides powerful extensibility and the new features can be added to the extended packet header after the IPv6 packet header. Unlike the IPv4, the packet header can only support the option of up to 40 bytes, while the size of the IPv6 extended packet header is only limited by the maximum bytes of the whole IPv6 packet.

The IPv6 supports the following features:

- IPv6 Protocol
- IPv6 Address Format
- Type of IPv6 Address
- ICMPv6
- IPv6 Neighbor Discovery
- Path MTU Discovery
- ICMPv6 Redirection
- Address Conflict Detection
- IPv6 Stateless Auto-configuration
- IPv6 Address Configuration
- IPv6 Route Forwarding (supporting static route configuration)
- Configuration of various IPv6 parameters
- Diagnosis Tool **Ping IPv6**

35.1.1 IPv6 Address Format

The basic format of an IPv6 address is X : X : X : X : X : X : X : X, where X is a 4 hex integers (16 bits). Each digit contains 4 bits of information, each integer contains 4 hex digits and each address contains 8 integers, so it is total for 128 bits. Some legal IPv6 addresses are as follows:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800 : 0 : 0 :0 : 0 : 0 : 0 : 1

1080 : 0 : 0 : 0 : 8 : 800 : 200C : 417A

These integers are hex integers, where A to F denote 10 to 15 respectively. Each integer in the address must be denoted and the starting 0 needs not be denoted. Some IPv6 address may contain a series of 0s (such as the examples 2 and 3). Once this condition occurs, the “: :” is allowed to denote this series of 0s. Namely, the address 800:0:0:0:0:0:0:1 can be denoted as: 800 :: 1

These two colons denote that this address can be extended to the complete 128-bit address. In this way, the 16-bit group can be replaced with two colons only when they are all 0s and the two colons can only present for one time.

In the mixture environment of IPv4 and IPv6, there is a mixture denotation method.The lowest 32 bits in an IPv6 address can be used to denote an IPv4 address. The address can be expressed in a mixture mode, i.e., X: X : X : X : X : X : d . d . d . d. Where, the X denotes a 16-bit integer, while d denotes an 8-bit decimal integer. For instance, the address 0 : 0 : 0 : 0 : 0 : 0 : 192 .168 . 20 : 1 is a legal IPv6 address. After the abbreviated expression method is used, this address can be denoted as follows: : : 192 .168 . 20 . 1

For the IPv6 address is divided into two parts such as the subnet prefix and the interface identifier, it can be denoted as an address with additional numeric value by the method like the CIDR address. Where, this numeric value indicates how many bits represent the network part (the network prefix). Namely the IPv6 node address indicates the length of the prefix, and the length is differentiated from the IPv6 address by the slash. For instance: 12AB::CD30:0:0:0:0/60,The length of the prefix used for routing in this address is 60 bits.

35.1.2 Type of IPv6 Address

In RFC2373, there are the following three defined types of IPv6 addresses:

- Unicast: Identifier of a single interface. The packet to be sent to a unicast address will be transmitted to the interface identified by this address.
- Anycast: Identifiers of a set of interfaces. The packet to be sent to an anycast address will be transmitted to one of the interfaces identified by this address (select the nearest one according to the routing protocol).
- Multicast: Identifiers of a set of interfaces (In general, they are of different nodes). The packet to be sent to a Multicast address will be transmitted to all the interfaces which are added to this multicast address.

Caution

The broadcast address is not defined in the IPv6.

The following will introduce these types of addresses one-by-one:

35.1.2.1 Unicast Addresses

IPv6 unicast addresses include the following types:

- Aggregateable Global Addresses
- Link-level Local Addresses
- Site-level Local Addresses
- IPv6 of IPv4 Addresses

1. Aggregateable Global Addresses

The format of the aggregateable global unicast addresses is shown as follows:

| 3 | 13 | 8 | 24 | 16 | 64 bits |

+--+-----+---+--------+--------+--------------------------------+

|FP| TLA |RES| NLA | SLA | Interface ID |

| | ID | | ID | ID | |

+--+-----+-----+------------+-------------+--- +

Above figure contains the following fields:

- FP field (Format Prefix):

The format prefix in an IPv6 address, 3 bits long, is used to indicate the type of the address in the IPv6 address space. 0 0 1 indicates an aggregateable global unicast address.

- TLA ID field (Top-Level Aggregation Identifier):

Top-Level Aggregation Identifier, containing toppest address routing information. It refers to the maximum route information in networking. It is 13 bits long and can provide up to 8192 different top level routes.

- RES field (Reserved for future use):

Reservation field, 8 bits. It will possibly be used to expand the top level or the next level aggregation identifier field.

- NLA ID field (Next-Level Aggregation Identifier):

Next-Level Aggregation Identifier, 24 bits. This identifier is used to control the top-level aggregation to arrange the address space by some institutions. In other word, these institutions (such as the large-sized ISP) can separate the 24-bit field according to the addressing level structure themselves. For instance, a large-sized ISP can separate it into 4 internal top-level routes by 2 bits, other 22 bits of the address space is assigned to other entities (such as the small-sized local ISP). If these entities obtain enough address space, the same measure can be taken to subdivide the space assigned to them.

- SLA ID field (Site-Level Aggregation Identifier):

Site-Level Aggregation Identifier, used to arrange internal network structures by some institutions. Each institution can use the same way as that in the IPv4 to create the hierarchical network structure themselves. If the 16 bits are taken as the plane address space, there are up to 65535 different subnets. If the former 8 bits are taken as the higher-level of routes within this organization, 255 large-scale subnets are allowed. Furthermore, each large-scale subnet can be subdivided into up to 255 small-scale subnets.

- Interface Identifier field (Interface Identifier):

It is 64 bits long and contains the 64 bit value of IEEE EUI-64 interface identifiers.

2. Link Local Addresses

The format of the link-level local addresses is shown as follows:

| 10 |

| bits | 54 bits | 64 bits |
+----------+----------+----------+

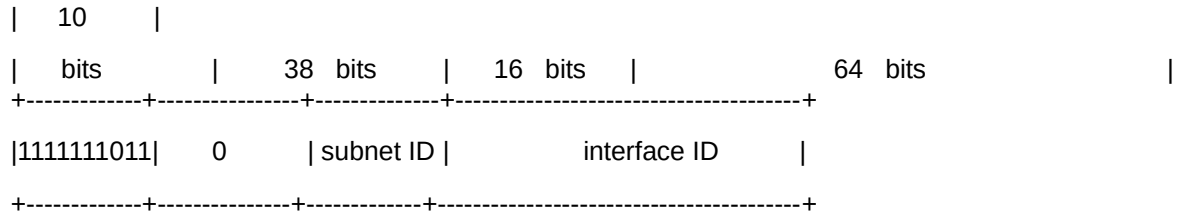
|1111111010| 0 | interface ID |

+----------+----------+----------+

The link-level local address is used to number the host on the single network link. The address of former 10-bit identification for the prefix is the link-level local address. The router will not forward the message of the source address of the destination address with the link-level local address forever. The intermediate 54-bit of this address is 0. The latter 64 indicates the interface identifier, this part allows the single network to connect to up to 2^{64}-1 hosts.

3. Site-level Local Addresses

The format of the site-level local addresses is shown as follows:

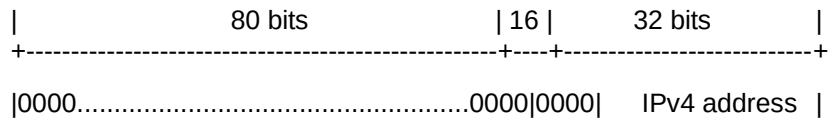


The site-level local address can be taken to transmit the data within the site, and the router will not forward the message of the source address of the destination address with the site-level local address to Internet. Namely, such packet route can only be forwarded within the site, but cannot be forwarded to out of the site. The former 10-bit prefix of the site-level local address is slightly different of that of the link-level local address, whose intermediate 38 bits are 0s, the subnet identifier of the site-level local address is 16 bits, while the latter 64 bits also indicate the interface identifier, usually for the EUI-64 address of IEEE.

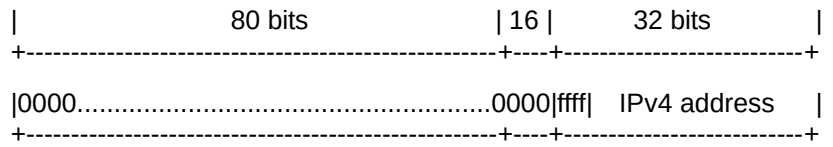
4. IPv6 of IPv4 Addresses

The RFC2373 also defines 2 types of special IPv6 addresses embedded with IPv4 addresses:

- IPv4-compatible IPv6 address



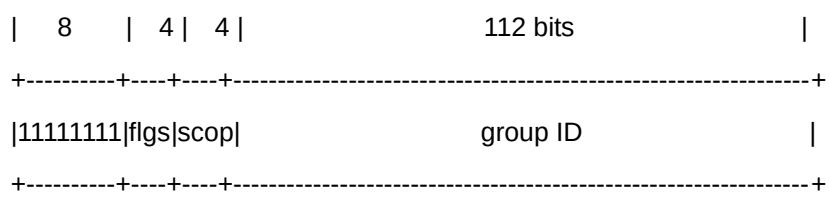
- IPv4-mapped IPv6 address



The IPv4-compatible IPv6 address is mainly used to the automatic tunneling, which supports both the IPv4 and IPv6. The IPv4-compatible IPv6 address will transmit the IPv6 packet via the IPv4 router in the tunneling way. The IPv6 address of an IPv4 mapping is used to access the nodes that only support IPv4 by IP6 nodes. For example, when one IPv6 application of the IPv4/IPv6 host requests the resolution of a host name (the host only supports IPv4), the name server will internally generate the IPv6 addresses of the IPv4 mapping dynamically and return them to the IPv6 application.

35.1.2.2 Multicast Addresses

The format of the IPv6 multicast address is shown as follows:



The first byte of the address format is full 1, which denote a multicast address.

- Flag field:

It consists of 4 bits.At present, only the fourth bit is specified. The bit is used to indicate whether the address is a known multicast address specified by Internet Number Constitution or a temporary

multicast address used in a specific condition. If this flag bit is 0, it indicates this address is a known multicast address. If this bit is 1, it indicates that this address is a temporary one. Other 3 flag bits are reserved for future use.

- Range field:

Composed of 4 bits and used to denote the range of multicast. Namely, whether the multicast group contains the local node, the local link and the local site or any position nodes in the IPv6 global address space.

- Group Identifier field:

112 bits long and used to identify a multicast group. Depending on whether a multicast address is temporary or known and the range of the address, a multicast identifier can denote different groups.

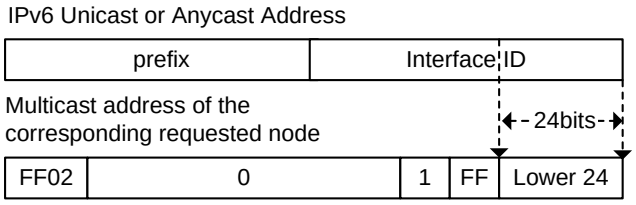
The multicast address of the IPv6 is this type of address taking FF00::/8 as the prefix One multicast address of an IPv6 usually identifies the interfaces of a serial of different nodes. When one message is sent to one multicast address, this message will be distributed to the interfaces of each node with this multicast address. One node (host or router) should add the following multicast:

- The multicast address of all nodes for the local link is FF02::1
- The prefix of the multicast address for the solicited node is FF02:0:0:0:0:1:FF00:0000/104

If they are routers, it is necessary to add the multicast address FF02::2 of all routers for the local link.

The multicast address of the solicited node corresponds to the IPv6 unicast and anycast address, so it is necessary for the IPv6 node to add corresponding multicast address of the solicited node for each configured unicast address and anycast address. The prefix of the multicast address for the solicited node is FF02:0:0:0:0:1:FF00:0000/104, another 24 bits are comprised of the unicast address or the lower 24 bits of the anycast address, for instance, the multicast address of the solicited node corresponding to the FE80::2AA:FF:FE21:1234 is FF02::1:FF21:1234,

The multicast address of solicited node is usually used to the neighbor solicitation (NS) message. The format of the solicited node is shown as follows:



35.1.2.3 Anycast Addresses

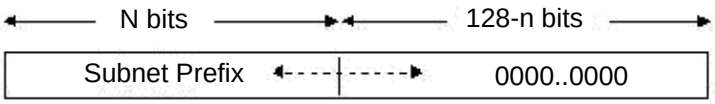
The anycast address is similar with the multicast address as more than one node shares an anycast address. The difference is that only one node expects to receive the data packet of the anycast address, while all nodes of the multicast address members expect to receive all packets sending to this address. The anycast address is assigned to normal IPv6 unicast address space, so the anycast address cannot be differentiated from the unicast address from the style. For this reason, each member of all anycast addresses has to be configured explicitly to identify the anycast address.

Caution The anycast address can only be assigned to the router, but cannot be assigned to the host. Furthermore, the anycast address cannot be taken as the source address of the message.

The RFC2373 predefines an anycast address, referred to as the anycast address of the subnet router. The following diagram shows the anycast address format of the subnet router, which consists of the subnet prefix followed by a series of 0s (as the interface identifier).

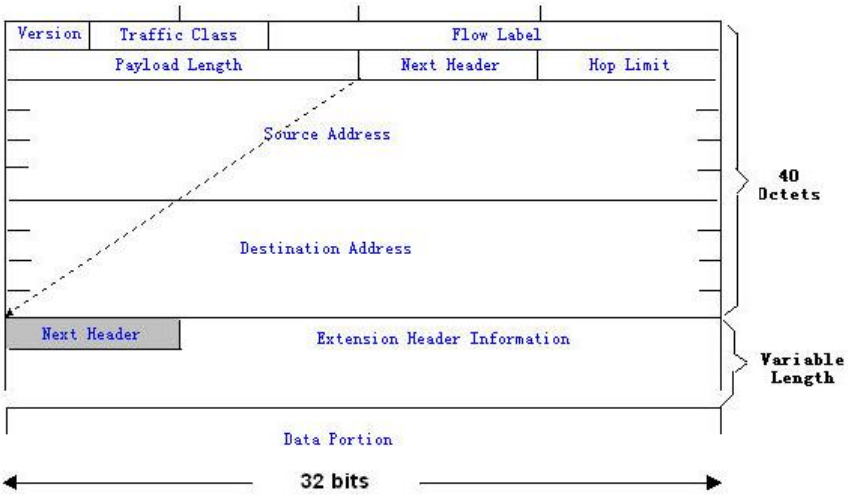
Where, the subnet prefix identifies a specified link (subnet) and the packet to be sent to the anycast address of the subnet router will be distributed to a router of this subnet. The anycast address of the subnet router is usually used for some node which needs to communicate with one router of the remote subnet.

Anycast Address Format of Subnet Router



35.1.3 IPv6 Packet Header Structure

The format of the IPv6 packet header is shown as the figure below:



The IPv4 packet header takes 4 bytes as the unit; the IPv6 packet header takes 8 bytes as the unit and the total length of the packet header is 40 bytes. In the IPv6 packet header, the following fields are defined:

- Version:

The length is 4 bits. For IPv6, the field must be 6.

- Traffic Class:

The length is 8 bits. It indicates a type of service provided to the packey and is equal to the “TOS” in the IPv4.

- Flow Label:

The length is 20 bits used to identify the packets of the same service flow. One node can be taken as the sending source of several service flows. Flow label and source node IP address identify a service flow uniquely.

- Payload Length:

The length is 16 bits, including the byte length of payload and the length of various IPv6 extension options (if any). In other words, it includes the length of an IPv6 packet except for the IPv6 header itself.

- Next Header:

This field indicates the protocol type in the header field following the IPv6 header. Similar to the IPv4 protocol field, the Next Header field can be used to indicate whether the upper level is TCP or UDP. It can also be used to indicate whether an extended IPv6 header exists.

- Hop Limit:

The length is 8 bits. When one router forwards the packet for one time, this field will reduce 1. If this field is 0, this packet will be discarded. It is similar to the life span field in the IPv4 packet header.

- Source Address (Source Address):

The length is 128 bits. It indicates the sender address of an IPv6 packet.

- Destination Address (Destination Address):

The length is 128 bits. It indicates the receiver address of an IPv6 packet.

At present, the following extended headers are defined for the IPv6:

- Hop-by-Hop Options:

This extended header must directly follow an IPv6 header. It contains the option data that must be checked by each node along the path.

- Routing Header (Routing (Type 0)):

This extended header indicates the nodes that a packet will go through before reaching the destination. It contains the address table of various nodes that the packet goes through. The initial destination address of the IPv6 header is the first one of a series of addresses in the route header, other than the final destination address of the packet. After receiving this packet, the node of this address will process the IPv6 header and the routing header, and send the packet to the second address of the routing header list. It repeats this step until the packet reaches the final destination.

- Fragment Header (Fragment):

This extended header is used to fragment the packets longer than the MTU of the path between the source node and destination node.

- Destination Option Header (Destination Options):

This extended header replaces the IPv4 option field. At present, the only defined destination option is to fill the option with an integer multiple of 64 bits (8 bytes) when necessary. This extended header can be used to carry the information checked by the destination node.

- Upper-layer Extended Header (Upper-layer header):

It indicates the the upper layer transmission protocol, such as TCP(6) and UDP(17).

Furthermore, the extended header of the Authentication and the Encapsulating Security Payload will be described in the IPSec section. At present, the IPv6 implemented by us cannot support the IPSec.

35.1.4 IPv6 Path MTU Discovery

As with the path MTU discovery of the IPv4, the path MTU discovery of the IPv6 allows one host to discover and adjust the size of the MTU in the data transmission path.

Furthermore, when the data packet to be sent is larger than the MTU of the data transmission path, the host will fragment the packets by itself. This behavior makes it not necessary for the router to process the fragment, and thus save resources and improve the efficiency of the IPv6 network.

Caution

The minimum link MTU is 68 bytes in the IPv4, indicating that the links along the path over which the packets are transmitted should support at least the link MTU of 68 bytes. The minimum link MTU is 1280 bytes in the IPv6. It is strongly recommended to use the link MTU of 1500 bytes for the link in the IPv6.

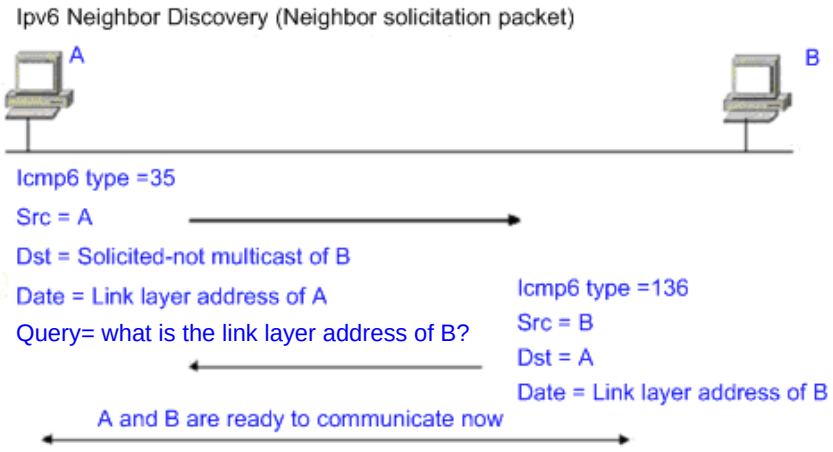
35.1.5 IPv6 Neighbor Discovery

The IPv6 neighbor discovery makes use of the ICMPv6 packet and the multicast addresses of the solicited neighbor to obtain the link layer address of the neighbors at the same link, and verify the reachability of the neighbors as well as maintain their status. These types of messages are briefly described respectively below.

35.1.5.1 Neighbor Solicitation

A node must get the link layer address of another node before communicating with it. At this time, it should send the neighbor solicitation (NS) message to the solicitated multicast address of the IPv6 address of the destination node. The NS message also contains the link layer address of itself. After receiving this NS message, the destination node responds with a message, referred to as neighbor advertisement (NA), with its link layer address. After receiving the response message, the source node can communicate with the destination node.

The following is the neighbor solicitation procedure:



The neighbor solicitation message can also be used to detect the reachability of the neighbor (for instance, the existing neighbor). At this time, the destination address of the neighbor solicitation message is the unicast address of this neighbor.

When the link layer address of one node changes, the neighbor advertisement will be sent actively to the addresses of all nodes on this link.

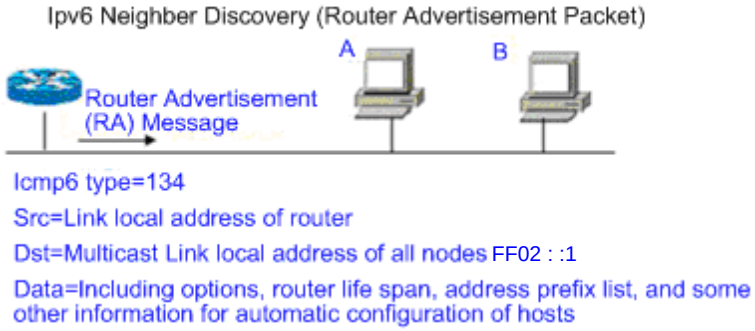
When one neighbor is considered that the reachable time is expired, the Neighbor Unreachability Detection (NUD) will be enable. This occurs only for unicast messages rather than mulicast messages destined to the neighbor.

Furthermore, the neighbor solicitation message in the stateless address auto-configuration can also be used to detect the uniqueness of the address, namely the address conflict detection. At this time, the source address of the message is unassigned address (: :).

35.1.5.2 Router Advertisement

The router sends the Router Advertisement (RA) to all the local nodes of the link periodically.

The following figure shows the process of sending the Router Advertisement (RA):



In general, the Router Advertisement (RA) contains the contents below:

- One or more IPv6 address prefixes used for the host to carry out the address auto-configuration.
- Effective period of the IPv6 address prefix.
- Usage of the host auto-configuration (Stateful or stateless).
- Information for the default router (namely, determine whether this router is taken as the default router. If yes, it will announce the time as the default router itself).
- Other information for configuration such as the hop limit, the MTU and the neighbor solicitation retransmission interval.

The Router Advertisement (RA) is also used to respond to the Router Solicitation (RS) message sent by the host. The Router Solicitation (RS) message allows the host to obtain the auto-configuration information immediately without waiting for the router to send the Router Advertisement (RA). If there is no unicast address when the host is activated, the Router Solicitation (RS) message sent by the host will use the unassigned address (0:0:0:0:0:0:0:0) as the source address of the solicitation message. Otherwise, the existing unicast address is taken as the source address, while the Router Solicitation (RS) message uses the multicast address (FF02::2) of all routers for the local link as the destination address. As the response router solicitation (RS) message, the Router Advertisement (RA) message will use the source address of the solicitation message as the destination address (if the source address is the unassigned address, it will use the multicast address FF02::1) of all nodes for the local link.

The following parameters can be configured in the Router Advertisement (RA) message:

Ra-interval: Interval of sending the Router Advertisement (RA).

Ra-lifetime: Router lifetime, namely whether the device is acted as the default router of the local link and the time as this role.

Prefix: IPv6 address prefix of the local link, which can be used to carry out the auto-configuration by the host, including the configuration of other parameters for the prefix.

Rs-initerval: Interval of sending the neighbor solicitation message.

Reachabletime: Time maintained after considering the neighbor reachable.

We configure the above parameters in the IPv6 interface property.

Caution

1. By default, no Router Advertisement (RA) message is sent actively on the interface. To do so, you can use the command **no ipv6 nd suppress-ra** in the interface configuration mode.
2. In order to make the stateless address auto-configuration of the node work normally, the length of the prefix for the router advertisement (RA) message should be 64 bits.

35.2 IPv6 Configuration

The following will introduce the configuration of various function modules of the IPv6 respectively:

35.2.1 Configuring IPv6 Address

This section describes how to configure an IPv6 address on an interface. By default, no IPv6 address is configured.

Caution

Once an interface is created and its link status is UP, the system will automatically generate the local link address for the interface. At present, the IPv6 doesn't support anycast address.

For the DES-7200 series, the range of the length of the prefix of the interface IPv6 address is [0, 64] or [128, 128], for the range of the length of the routing prefix supported by the hardware forwarding table of the chip is [0, 64] or [128, 128].

To configure an IPv6 address, execute the following commands in the global configuration mode:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
ipv6 enable	Enable the IPv6 protocol on an interface. If this command is not run, the system automatically enables the IPv6 protocol when you configure an IPv6 address for an interface.
ipv6 address *ipv6-prefix/prefix-length* [**eui-64**]	Configure the IPv6 unicast address for this interface. The key word **Eui-64** indicates the generated IPv6 address consists of the configured address prefix and the 64-bit interface ID. Note: Whether the key word **eui-64** is used, it is necessary to enter the complete address format to delete an IPv6 address (Prefix & interface ID/prefix length). When you configure an IPv6 address on an interface, then the IPv6 protocol is automatically enabled on the interface. Even if you use **no ipv6**

Command	Meaning
	enable, you cannot disable the IPv6 protocol.
End	Return to the privileged EXEC mode.
show ipv6 interface vlan 1	View the interface information.
copy running-config startup-config	Save the configuration.

Use the **no ipv6 address** *ipv6-prefix*/*prefix-length* **[eui-64]** command to delete the configured IPv6 address.

The following is an example of the configuration of the IPv6 address:

```
DES-7210(config)# interface vlan 1
DES-7210(config-if)# ipv6 enable
DES-7210(config-if)# ipv6 address fec0:0:0:1::1/64
DES-7210(config-if)# end
DES-7210(config-if)# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

35.2.2 Configuring ICMPv6 Redirection

This section will describe how to configure the ICMPv6 redirection function on the interface. By default, the redirection function of the IPv6 on the interface is enabled. The router needs to send the redirection message to the source during packet forwarding in the following cases:

- The destination address of the message is not a multicast address;
- The destination address of the message is not the router itself;
- The output interface of the next hop determined by the device for this message is the same as the interface this message received, namely, the next hop and the originator is of the same link;
- The node identified by the source IP address of the packet is a neighbor of the local router. Namely, this node exists in the router's neighbor table.

Caution The router other than the host can generate the redirection message, and the router will not update its routing table when it receives the redirection message.

To enable redirection on the interface, execute the following commands in the global configuration mode:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface vlan *1*	Enter the SVI interface configuration mode.
ipv6 redirects	Enable the IPv6 redirection function.
End	Return to the privileged EXEC mode.
show ipv6 interface vlan *1*	Show the interface configuration.
copy running-config startup-config	Save the configuration.

Use the **no ipv6 redirects** command to disable the redirection function. The following is an example to configure the redirection function:

```
DES-7210(config)# interface vlan 1
DES-7210 (config-if)# ipv6 redirects
DES-7210 (config-if)# end
DES-7210 # show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

35.2.3 Configuring Static Neighbor

This section will describe how to configure a static neighbor. By default, the static neighbor is not configured. In general, a neighbor learns and maintains its status by the Neighbor Discovery Protocol (NDP) dynamically. Moreover, you can configure the static neighbor manually.

To configure the static neighbor, execute the following commands in the global configuration mode.

Command	Meaning
configure terminal	Enter the global configuration mode.
ipv6 neighbor *ipv6-address interface-id hardware-address*	Configure a static neighbor on the interface.
End	Return to the privileged EXEC mode.
show ipv6 neighbors	View the neighbor list.
copy running-config startup-config	Save the configuration.

Use the **no ipv6 neighbor** command to delete the specified neighbor. The following is an example to configure a static neighbor on SVI 1:

```
DES-7210(config)# ipv6 neighbor fec0:0:0:1::100 vlan 1 00d0.f811.1234
DES-7210 (config)# end
DES-7210# show ipv6 neighbors verbose fec0:0:0:1::100
IPv6 Address       Linklayer Addr   Interface
fec0:0:0:1::100    00d0.f811.1234   vlan 1
State: REACH/H Age: - asked: 0
```

35.2.4 Configuring Address Conflict Detection

This section describes how to configure address conflict detection times. Address conflict detection is mandatory to assign unicast addresses to interfaces. The goal is to dectect the uniqueness of an address. The address conflict detection should be carried out for the manual configuration address, the stateless auto-configuration address or the statefull auto-configuration address. However, it is not necessary to carry out the address conflict detection under the following two conditions:

- The management prohibits the address conflict detection, namely, the number of the neighbor solicitation messages sent for the address conflict detection is set to 0.
- The configured anycast address can not be applied to the address conflict detection.

Furthermore, if the address conflict detection function is not disabled on the interface, the system will enable the address conflict detection process for the configured address when the interface changes to the Up status from the Down status.

The following is the configuration procedure of the quantity of the neighbor solicitation message sent for the address conflict detection:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface vlan *1*	Enter the SVI 1 configuration mode.

Command	Meaning
ipv6 nd dad attempts *attempts*	The quantity of the neighbor solicitation message sent for the address conflict detection. When it is configured to 0, any neighbor solicitation message is denied. Enable the address conflict detection function on the interface.
End	Return to the privileged mode.
show ipv6 interface vlan *1*	View the IPv6 information of the SVI 1.
copy running-config startup-config	Save the configuration.

Use the **no ipv6 nd dad attempts** command to restore the default value. The following is an example to configure the times of the neighbor solicitation (NS) message sent for the address conflict detection on the SVI1:

```
DES-7210(config)# interface vlan 1
DES-7210(config-if)# ipv6 nd dad attempts 3
DES-7210(config-if)# end
DES-7210# show ipv6 interface vlan 1
DES-7210(config)# interface vlan 1
DES-7210(config-if)# ipv6 nd dad attempts 3
DES-7210(config-if)# end
DES-7210# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 3
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

35.2.5 Configuring Other Interface Parameters

The IPv6 parameters on an interface fall into 2 parts, one is used to control the behavior of the router itself, the other is used to control the contents of the router advertisement (RA) sent by the

router to determine what action should be taken by the host when it receives this router advertisement (RA).

The following will introduce these commands one by one:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the interface configuration mode.
ipv6 enable	Enable the IPv6 function.
ipv6 nd ns-interval *milliseconds*	(Optional) Define the retransmission interval of the neighbor solicitation message.
ipv6 nd reachable-time *milliseconds*	(Optional) Define the time when the neighbor is considered to be reachable. Note: as specified in RFC4861, the reachable time of a neighbor should be increased or decreased at random on the basis of the configured time in the range of 0.5 to 1.5 of the configured time.
ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise**]]	(Optional) Set the address prefix to be advertised in the router advertisement (RA) message.
ipv6 nd ra-lifetime *seconds*	(Optional) Set the TTL of the router in the router advertisement (RA) message, namely the time as the default router. 0, indicates that the router will not act as the default router of the direct-connected network.
ipv6 nd ra-interval *seconds*	(Optional) Set the time interval for the router to send the router advertisement (RA) message periodically.
ipv6 nd managed-config-flag	(Optional) Set the “managed address configuration” flag bit of the router advertisement (RA) message, and determine whether the host will use the stateful auto-configuration to obtain the address when it receives this router advertisement (RA).
ipv6 nd other-config-flag	(Optional) Set the “other stateful configuration” flag bit of the router advertisement (RA) message, and determine whether the host will use the stateful auto-configuration to obtain other information other than the address when it receives this router advertisement (RA).
ipv6 nd suppress-ra	(Optional) Set whether suppress the router advertisement (RA) message in this interface.
End	Return to the privileged EXEC mode.
show ipv6 interface [*interface-id*] [**ra-info**]	Show the ipv6 interface of the interface or the information of RA sent by this interface.
copy running-config startup-config	(Optional) Save the configuration.

The **no** command of above commands can be used to restore the default value. For details, refer to *IPv6 Command Reference*.

35.3 IPv6 Monitoring and Maintenance

It is mainly used to provide related command to show some internal information of the IPv6 protocol, such as the ipv6 information, the neighbor table and the route table information of the interface.

Command	Meaning
Show ipv6 interface [*interface-id*] [**ra-info**]	Show the IPv6 information of the interface.
Show ipv6 neighbors [**verbose**] [*interface-id*] [*ipv6-address*]	Show the neighbor information.
Show ipv6 route [**static**] [**local**] [**connected**]	Show the information of the IPv6 routing table.

1. View the IPv6 information of an interface.

```
DES-7210# show ipv6 interface
interface vlan 1 is Down, ifindex: 2001
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:1:1:1::1 , subnet is fec0:1:1:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

2. View the information of the router advertisement (RA) message to be sent of an interface

```
DES-7210# show ipv6 interface ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND router advertisements live for 1800 seconds
ND router advertisements are sent every 200 seconds<240--160>
```

```
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def, Auto, vltime: 2592000, pltime: 604800, flags: LA)
```

3. View the neighbor table information of the IPv6.

```
DES-7210# show ipv6 neighbors
IPv6 Address              Linklayer Addr  Interface
fe80::200:ff:fe00:1      0000.0000.0001 vlan 1
State: REACH/H Age: - asked: 0
fec0:1:1:1::1             0000.0000.0001 vlan 1
State: REACH/H Age: - asked: 0
```

36 IPv6 Tunnel Configuration

36.1 Overview

The IPv6 is designed to inherit and replace the IPv4. However, the evolution from the IPv4 to the IPv6 is a gradual process. Therefore, it is inevitable that these two protocols coexist for a period before the IPv6 completely replaces the IPv4. At the beginning of this transition stage, IPv4 networks are still main networks. IPv6 networks are similar to isolated islands in IPv4 networks. The problems about transition can be divided into the following two types:

1. Communications among isolated IPv6 networks via IPv4 networks
2. Communications between IPv6 networks and IPv4 networks

This article discusses the tunnel technology that is used to solve problem 1. The solution to problem2 is NAT-PT (Network Address Translation-Protocol Translation), which is not covered in this article.

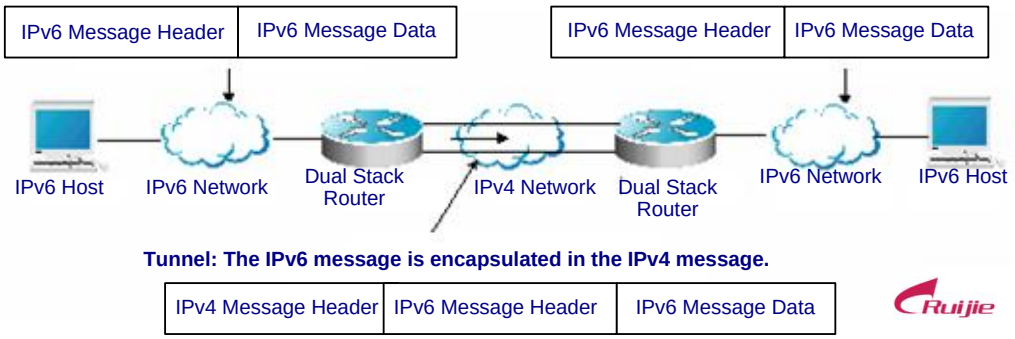
The IPv6 tunnel technology encapsulates IPv6 messages in IPv4 messages. In this way, IPv6 protocol packets can communicate with each other via IPv4 networks. Therefore, with the IPv6 tunnel technology, isolated IPv6 networks can communicate one another via existing IPv4 networks, avoiding any modification and upgrade to existing IPv4 networks. An IPv6 tunnel can be configured between Area Border Routers or between an Area Border Router and the host. However, all the nodes at the two ends of the tunnel must support the IPv4 and IPv6 protocol stacks. At present, our company supports the following tunnel technologies:

Tunnel Type	Reference
Manually Config Tunnel	RFC2893
Automatic 6to4 Tunnel	RFC3056
Intra-Site Automatic Tunnel Addressing Protocol(ISATAP)	draft-ietf-ngtrans-isatap-22

Caution

Interconnecting the isolated IPv6 networks through the IPv6 tunnel technology is not the ultimate IPv6 network architecture. Instead, it is a transitional technology.

The model using the tunnel technology is shown in the following figure:



The features of various tunnels are respectively introduced below.

36.1.1 Manually Configured IPv6 Tunnel

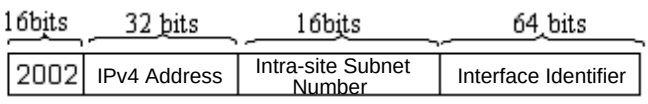
One manually configured tunnel is similar to one permanent link set up between two IPv6 domains via the backbone network of the IPv4. It is applicable for the relatively fixed connections that have a higher demand on security between two Area Border Routers or between an Area Border Router and a host.

On a tunnel interface, you must manually configure the IPv6 address, source IPv4 address (tunnel source) and destination IPv4 address (tunnel destination) of the tunnel. The nodes at the two end of the tunnel must support the IPv6 and IPv4 protocol stacks. In practical application, tunnels are always manually configured in pairs. You can think it as a point-to-point tunnel.

36.1.2 Automatic 6to4 Tunnel

The automatic 6to4 tunnel technology allows isolated IPv6 networks to be interconnected via IPv4 networks. The difference between the automatic 6to4 tunnel and manually configured tunnel technologies is that the manual configured tunnel is a point-to-point tunnel, while a 6to4 tunnel is a point -to-multipoint tunnel.

The 6to4 tunnel takes an IPv4 network as a Nonbroadcast multi-access (NBMA) link. Therefore, the routers of 6to4 need not be configured in pairs. The IPv4 addresses embedded in an IPv6 address will be used to look for the other end of the automatic tunnel. The 6to4 tunnel can be taken as a point -to-multipoint tunnel. The automatic 6to4 tunnel can be configured on an Area Border Router of one isolated IPv6 network. For each message, it will automatically build a tunnel connecting to an Area Border Router in another IPv6 network. The destination address of a tunnel is the IPv4 address of an Area Border Router in the IPv6 network at the other end. The IPv4 address will be extracted from the destination IPv6 address of the message. The destination IPv6 address starts at the prefix 2002::/16 in the following form:



IPv6 6to4 Address Format

The 6to4 address is an address for automatic 6to4 tunnel technology. The IPv4 address embedded in it are usually the global IPv4 address of the egress of the area border router in the site. When the

automatic tunnel is built, the address is used as the IPv4 address for tunnel message encapsulation. All the routers at the two ends of the 6ot4 tunnel must also support the IPv6 and IPv4 protocol stacks. A 6to4 tunnel is usually configured between Area Border Routers.

For example, the global IPv4 address of the egress of the area border router in the site is 211.1.1.1 (D301:0101 in hex), a subnet number in the site is 1 and the interface identifier is 2e0:ddff:fee0:e0e1, then the corresponding 6to4 address can be denoted as follows:

2002: D301:0101:1: 2e0:ddff:fee0:e0e1

Caution

The IPv4 address embedded in the 6to4 address cannot be a private IPv4 address (i.e., the address of the network interface segment 10.0.0.0/8, 172.16.0.0/12 or 192.168.0.0/16) and must be the global IPv4 address.

Common application models of 6to4 tunnels:

- Simple application models

The simplest and most common application of 6to4 tunnels is used to interconnect multiple IPv6 sites. Each of the sites must have one connection to one of their shared IPv4 networks at least. This IPv4 network can be an Internet network or a internal backbone network of an organization. The key is that each site must have a unique global IPv4 address. The 6to4 tunnel will use the address to form the IPv6 prefix of 6to4/48: 2002:IPV4 address/48.

- Mixture application models

Based on the application described above, other 6to4 networks access the pure IPv6 network. by 6to4 relay devices at the edge. The router used to implement the function is called 6to4 Relay Router.

36.1.3 ISATAP Automatic unnel

Intra-site Automatic Tunnel Addressing Protocol (ISATAP) is a type of IPv6 tunnel technology by which an intra-site IPv6 architecture takes an IPv4 network as one nonbroadcast multi-access (NBMA) link layer, namely taking an IPv4 network as the virtual link layer of the IPv6.

ISATAP is applicable for the case where the pure IPv6 network inside a site is not ready for use yet and an IPv6 message need be transferred internally in the site. For example, a few of IPv6 hosts for test need communicate one another inside the site. By an ISATAP tunnel, the IPv4/IPv6 dual stack hosts on a same virtual link can communicate one another inside the site.

On the ISATAP site, the ISATAP router provides standard router advertisement message, allowing the ISATAP host to be automatically configured inside the site. At the same time, the ISATAP router performs the function that an intra-site ISATAP host and external IPv6 host forward messages.

The IPv6 address prefix used by ISATAP can be any legal 64-bit prefix for IPv6 unicast, including the global address prefix, local link prefix and local site prefix. The IPv4 address is placed as the ending 32 bits of the IPv6 address, allowing a tunnel to be automatically built.

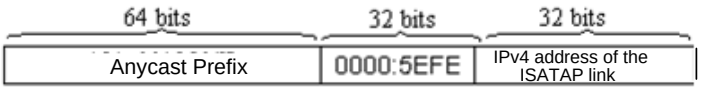
It is very possible that ISATAP is used with other transition technologies. Especially when used with the 6to4 tunnel technology, it can make the dual stack host of an internal network access an IPv6 backbone network very easily.

- ISATAP interface identifier

The unicast address used by ISATAP is in the form of a 64-bit IPv6 prefix plus a 64-bit interface identifier. The 64-bit interface identifier is generated in the revised EUI-64 address form. Where, the value of the first 32 bits of the interface identifier is **0000:5EFE**, an interface identifier of ISATAP.

- ISATAP address structure

An ISATAP address refers to the unicast address containing an ISATAP interface identifier in its interface identifier. An ISATAP address structure is shown in the following figure:



IPv6 ISATAP Address Format

The above figure shows that the interface identifier contains an IPv4 address. The address is the IPv4 address of a dual stack host and will be used when an automatic tunnel is automatically built.

For example, the IPv6 prefix is 2001::/64 and the embedded IPv4 address is 192.168.1.1. In the ISATAP address, the IPv4 address is denoted as the hexadecimal numeral of C0A8:0101. Therefore, its corresponding ISATAP address is as follows:

2001::0000:5EFE:C0A8:0101

36.2 IPv6 Tunnel Configuration

36.2.1 Manually Configuring IPv6 Tunnels

This section explains how to configure tunnels manually.

To configure a tunnel manually, configure an IPv6 address on the tunnel interface and manually configure the IPv4 addresses of the source port and destination port of the tunnel. Then, configure the hosts or routers at the two ends of the tunnel to ensure that they support the dual stacks (the IPv6 and IPv4 protocol stacks).

Caution Do not configure tunnels manually with the same Tunnel Source and Tunnel Destination.

Brief steps

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip
ipv6 enable
tunnel source {ip-address | type num}
tunnel destination ip-address
end
```

To configure an IPv6 tunnel manually, execute the following commands in the global configuration mode:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface tunnel *tunnel-num*	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.
tunnel mode ipv6ip	Set the tunnel type to manually configured tunnel.
ipv6 enable	Enable the IPv6 function on the interface. You can also configure the IPv6 address to directly enable the IPv6 function on the interface.

Command	Meaning
tunnel source {*ip-address* | *type num*	Specify the IPv4 source address or referenced source interface number of a tunnel. Note: If you specify an interface, then the IPv4 address must have been configured on the interface.
tunnel destination *ip address*	Specify the destination address of a tunnel.
end	Return to the privileged mode.
copy running-config startup-config	Save the configuration.

Refer to the section *Verifying and Mmonitoring IPv6 Tunnel Configuration* to check the operation of the tunnel.

36.2.2 Configuring 6to4 Tunnel

This section introduces how to configure a 6to4 tunnel.

The destination address of a 6to4 tunnel is determined by the IPv4 address which is extracted from the 6to4 IPv6 address. The routers at the two end of the 6to4 tunnel must support the dual stacks, namely, the IPv4 and IPv6 protocol stacks.

Caution

A device supports only one 6to4 tunnel. The encapsulation source address (IPv4 address) used by the 6to4 tunnel must be a global routable address. Otherwise, the 6to4 tunnel will not work normally.

Brief steps

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source {ip-address | type num}
exit
ipv6 route 2002::/16 tunnel tunnel-number
end
```

To configure a 6to4 tunnel, execute the following commands in the global configuration mode:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface tunnel *tunnel-num*	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.
tunnel mode ipv6ip 6to4	Set the tunnel type to 6to4 tunnel.
ipv6 enable	Enable the IPv6 function of the interface. You can also configure the IPv6 address to directly enable the IPv6 function of the interface.
tunnel source {*ip-address* | *type num*	Specify the encapsulation source address or referenced source interface number of a tunnel. Note: The IPv4 address must have been configured on the referenced interface. The used IPv4 address must be a global routable address.
Exit	Return to the global configuration mode.

Command	Meaning
ipv6 route *2002::/16* **tunnel** *tunnel-number*	Configure a static route for the IPv6 6to4 prefix 2002::/16 and associate the output interface to the tunnel interface, i.e., the tunnel interface specified in the above Step 2.
End	Return to the privileged EXEC mode.
copy running-config startup-config	Save the configuration.

Refer to the section *Verifying and Mmonitoring IPv6 Tunnel Configuration* to check the operation of the tunnel.

36.2.3 Configuring ISATAP Tunnel

This section introduces how to configure an ISATAP device.

On an ISATAP tunnel interface, the configuration of an ISATAP IPv6 address and the advertisement configuration of a prefix is same to that of a normal IPv6 interface. However, the address configured for an ISATAP tunnel interface must be a revised EUI-64 address. The reason is that the last 32 bits of the interface identifier in the IPv6 address are composed of the IPv4 address of the interface referenced by the tunnel source address. Refer to the above chapters and sections for the information about ISATAP address formats.

Caution

A device supports multiple ISATAP tunnels. However, the source of each ISATAP tunnel must be different.

Otherwise, there is no way to know which ISATAP tunnel a received ISATAP tunnel message belongs to.

Brief steps

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip isatap
ipv6 address ipv6-prefix/prefix-length eui-64
tunnel source interface-type num
no ipv6 nd suppress-ra
end
```

To configure an ISATAP tunnel, execute the following commands in the global configuration mode:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface tunnel *tunnel-num*	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.
tunnel mode ipv6ip isatap	Set the tunnel type to ISATAP tunnel.
ipv6 address ipv6-prefix/prefix-length eui-64	Configure the IPv6 ISATAP address. Be sure to specify to use the **eui-64** keyword. In this way, the ISATAP address will be automatically generated. The address configured on an ISATAP interface must be an ISATAP address.
tunnel source type *num*	Specify the source interface number referenced by a tunnel. On the referenced interface, the IPv4 address must have been configured.

Command	Meaning
no ipv6 nd suppress-ra	By default, it is disabled to send router advertisement messages on an interface. Use the command to enable the function, allowing the ISATAP host to be automatically configured.
End	Return to the privileged EXEC mode.
copy running-config startup-config	Save the configuration.

Refer to the section *Verifying and Mmonitoring IPv6 Tunnel Configuration* to check the operation of the tunnel.

36.3 Verifying and Monitoring IPv6 Tunnel Configuration

This section introduces how to verify the configuration and operation of an IPv6 tunnel.

Brief steps

```
enable
show interface tunnel number
show ipv6 interface tunnel mumber
ping protocol destination
show ip route
show ipv6 route
```

To verify the configuration and operation of a tunnel, execute the following commands in the privileged mode:

Command	Meaning
enable	Enter the privileged configuration mode.
show interface tunnel *tunnel-num*	View the information of a tunnel interface.
show ipv6 interface tunnel *tunnel-num*	View the IPv6 information of a tunnel interface.
ping protocol destination	Check the basic connectivity of a network.
show ip route	View the IPv4 routing table.
show ipv6 route	View the IPv6 router table.

1. View the information of a tunnel interface.

```
DES-7210# show interface tunnel 1
Tunnel 1 is up, line protocol is Up
Hardware is Tunnel, Encapsulation TUNNEL
Tunnel source 192.168.5.215  ,  destination 192.168.5.204
Tunnel protocol/transport IPv6/IP
Tunnel TTL is 9
Tunnel source do conformance check set
Tunnel source do ingress filter set
Tunnel destination do safety check not set
Tunnel disable receive packet not set
```

2. View the IPv6 information of a tunnel interface.

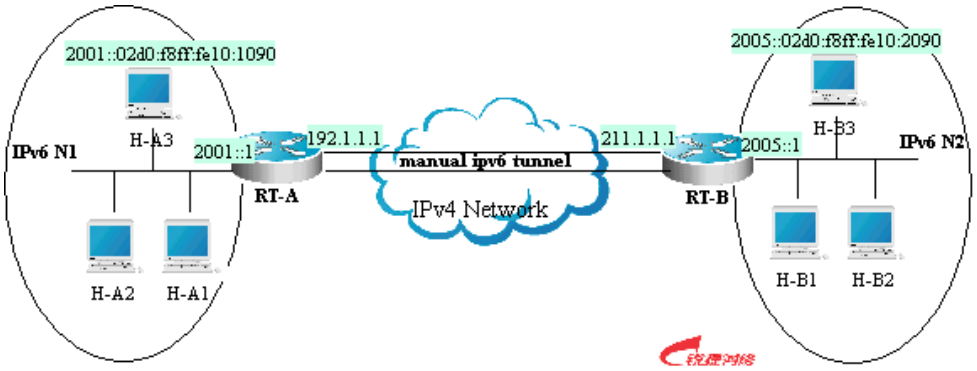
```
DES-7210# show ipv6 interface tunnel 1
interface Tunnel 1 is Up, ifindex: 6354
address(es):
Mac Address: N/A
INET6: fe80::3d9a:1601 , subnet is fe80::/64
Joined group address(es):
ff02::2
ff01::1
ff02::1
ff02::1:ff9a:1601
INET6: 3ffe:4:0:1::1 , subnet is 3ffe:4:0:1::/64
Joined group address(es):
ff02::2
ff01::1
ff02::1
ff02::1:ff00:1
MTU is 1480 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

36.4 IPv6 Tunnel Configuration Instances

The following sections introduce IPv6 tunnel configuration instances.

- Manual IPv6 Tunnel Configuration
- 6to4 Tunnel Configuration
- ISATAP Tunnel Configuration
- ISATAP and 6to4 Tunnels Configuration

36.4.1 Manual IPv6 Tunnel Configuration



As shown in the above figure, IPv6 networks N1 and N2 are isolated by the IPv4 network. Now, the two networks are interconnected by configuring a tunnel manually. For example, the H-A3 host in N1 can access the H-B3 host in N2.

In the figure, RT-A and RT-B are routers that support the IPv4 and IPv6 protocol stacks. Tunnel configuration occurs on the Area Border Routers (RT-A and RT-B) in N1 and N2. Note that the tunnel must be configured manually in pairs, that is, on RT-A and RT-B.

The following presents the tunnel configuration on routers:

Prerequisite: Suppose the routes of IPv4 are connected. In the following content, no more route configuration condition about IPv4 is listed.

RT-A configuration

#Connect the interfaces of the IPv4 network

```
interface FastEthernet 2/1
no switchport
ip address 192.1.1.1 255.255.255.0
```

#Connect the interfaces of the IPv6 network

```
interface FastEthernet 2/2
no switchport
ipv6 address 2001::1/64
no ipv6 nd suppress-ra  (optional)
```

#Configure manual tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip
ipv6 enable
tunnel source FastEthernet 2/1
tunnel destination 211.1.1.1
```

#Configure the route to the tunnel

```
ipv6 route 2005::/64 tunnel 1
```

RT-B configuration

#Connect the interfaces of the IPv4 network

```
interface FastEthernet 2/1
no switchport
ip address 211.1.1.1 255.255.255.0
```

Connect the interfaces of the IPv6 network

```
interface FastEthernet 2/2
no switchport
ipv6 address 2005::1/64
no ipv6 nd suppress-ra  (optional)
```

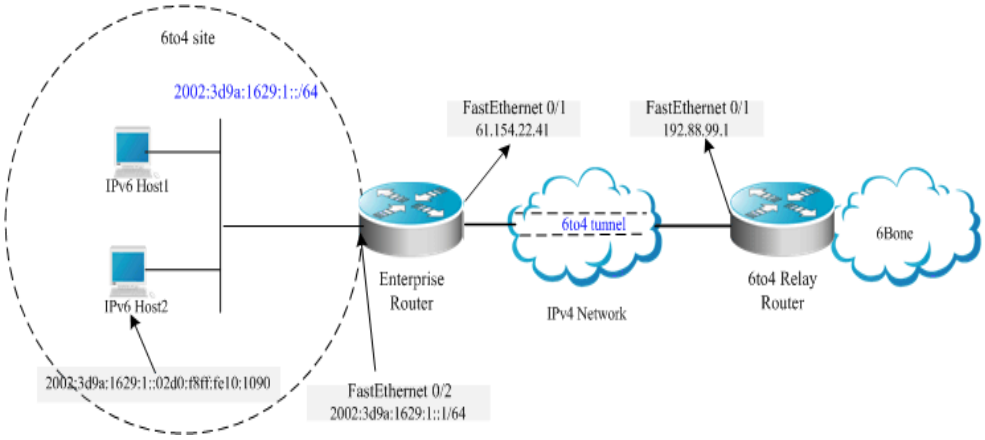
#Configure the manual tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip
ipv6 enable
tunnel source FastEthernet 2/1
tunnel destination 192.1.1.1
```

#Configure the route to the tunnel

```
ipv6 route 2001::/64 tunnel 1
```

36.4.2 6to4 Tunnel Configuration



As shown in the above figure, an IPv6 network (6to4 site) uses a 6to4 tunnel to access the IPv6 backbone network (6bone) via the 6to4 relay router.

As introduced above, the 6to4 tunnel technology is used to interconnect isolated IPv6 networks and they can access the IPv6 backbone network via the 6to4 relay router very easily. The 6to4 tunnel is an automatic tunnel and the IPv4 address embeded in the IPv6 address will be used to look for the other end of the automatic tunnel. Therefore, you need not configure the destination end for the 6to4 tunnel. Additionally, unsimilar to a manual tunnel, the 6to4 tunnel need not be configured in pairs.

61.154.22.41 is 3d9a:1629 in the hex form.

192.88.99.1 is c058:6301 in the hex form.

Caution

When configuring a 6to4 tunnel on an Area Border Router, be sure to use a routable global IPv4 address. Otherwise, the 6to4 tunnel will not work normally.

The following is the configuration of the two routers in the figure (Suppose IPv4 routes are connected. Ignore the configuration of IPv4 routes.):

Enterprise router configuration

Connect the interfaces of the IPv4 network

```
interface FastEthernet 0/1
no switchport
ip address 61.154.22.41 255.255.255.128
```

Connect the interfaces of the IPv6 network

```
interface FastEthernet 0/2
no switchport
ipv6 address 2002:3d9a:1629:1::1/64
no ipv6 nd suppress-ra
```

Configure the 6to4 tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source FastEthernet 0/1
```

Configure the route to the tunnel

```
ipv6 route 2002::/16 Tunnel 1
```

Configure the route to the 6to4 relay router to access 6bone

```
ipv6 route ::/0 2002:c058:6301::1
```

ISP 6to4 Relay Router configuration

Connect the interface of the IPv4 network

```
interface FastEthernet 0/1
no switchport
ip address 192.88.99.1 255.255.255.0
```

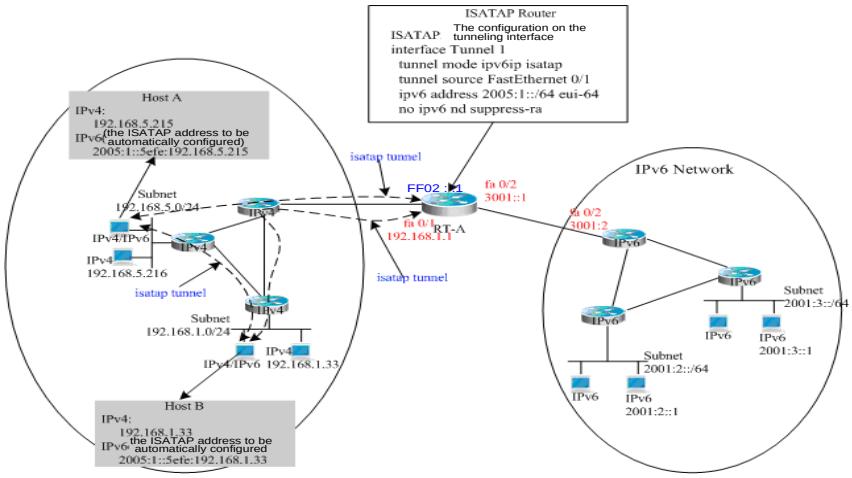
Configure the 6to4 tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source FastEthernet 0/1
```

Configure the route to the tunnel

```
ipv6 route 2002::/16 Tunnel 1
```

36.4.3 ISATAP Tunnel Configuration



The above figure is one typical topology using an ISATAP tunnel. The ISATAP tunnel is used to communicate between isolated IPv4/IPv6 dual stack hosts inside the IPv4 site. The ISATAP router has the two following functions inside the ISATAP site:

- Receive a router request message from the ISATAP host inside the site and then respond with a router advertisement message for the ISATAP host inside the site to be automatically configured.
- Be responsible for the message forwarding function of the ISATAP host inside the site and the IPv6 host outside the site.

In the above figure, when Host A and Host B send the router solicitation message to ISATAP Router, ISATAP Router will respond with a router advertisement message. After receiving the message, the hosts will automatically perform self-configuration and generate their own ISATAP addresses respectively. Then, the IPv6 communication between Host A and Host B will be done via the ISATAP tunnel. When Host A or Host B need communicate with the IPv6 host outside the site, Host A sends the message to the ISATAP router RT-A via the ISATAP tunnel and then RT-A forwards the message to the IPv6 network.

In the above figure, ISATAP Router (RT-A) is configured as follows:

Connect the interfaces of the IPv4 network

```
interface FastEthernet 0/1
no switchport
ip address 192.168.1.1 255.255.255.0
```

Configure the ISATAP tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2005:1::/64 eui-64
no ipv6 nd suppress-ra
```

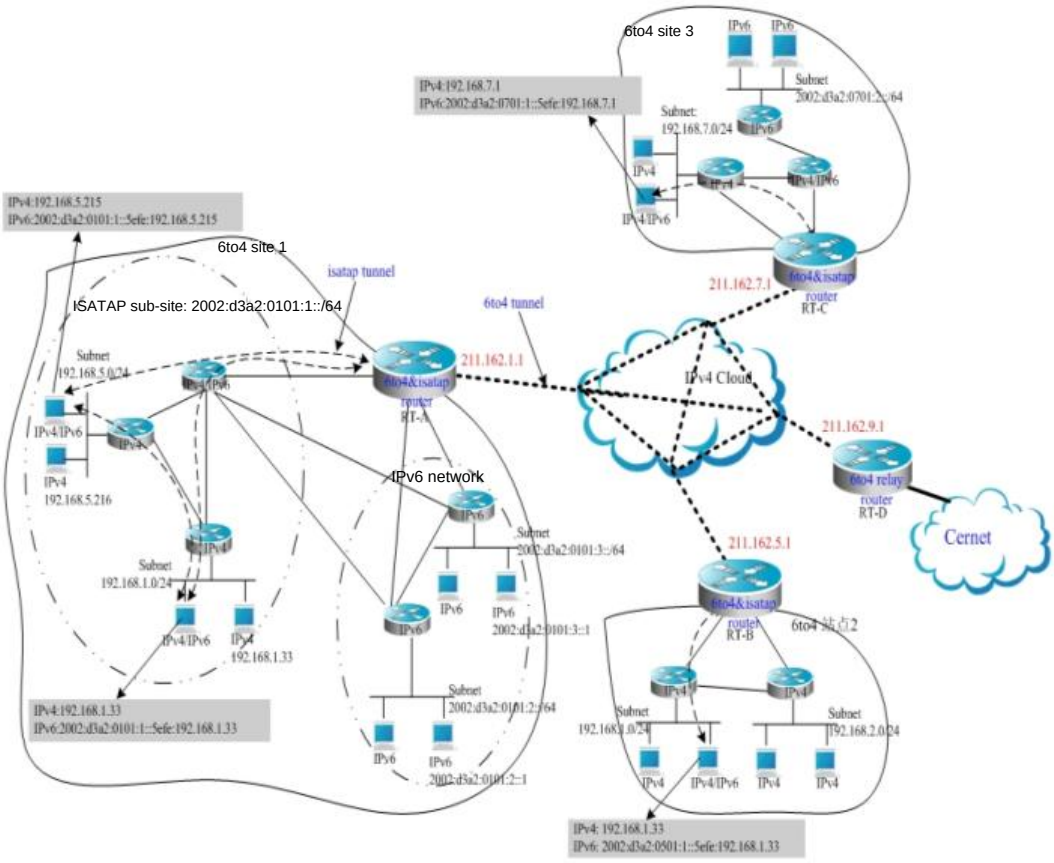
Connect the interfaces of the IPv6 network

```
interface FastEthernet  0/2
no switchport
ipv6 address 3001::1/64
```

Configure the route to the IPv6 network

```
ipv6 route 2001::/64 3001::2
```

36.4.4 ISATAP and 6to4 Tunnels Configuration



Note

In the above figure, it is an instance about composite application of 6to4 tunnel and ISATAP tunnel. By use of the 6to4 tunnel technology, various 6to4 sites are interconnected and the 6to4 site accesses the Cernet network via the **6to4 relay router**. At the same time, by use of the ISATAP tunnel technology inside the 6to4 site, the IPv6 hosts isolated by IPv4 inside the site perform IPv6 communication via the ISATAP tunnel.

Caution

In the above figure, the used global IP address containing the address of the 6to4 Relay router is only for convenience. When actually planning topologies, we should use a true global IP address and the address of the 6to4 Relay. At present, many organizations provide the addresses of open and free 6to4 Relay routers address.

The configurations of Area Border Routers in the 6to4 site shown in the above figure are introduced respectively below. Note that only main related configurations are listed here.

RT-A Configuration:

Connect the interfaces of the Internet network

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.1.1 255.255.255.0
```

Connect the interfaces of the IPv4 network inside the siteinterface FastEthernet 0/1

```
no switchport
ip address 192.168.0.1 255.255.255.0
```

Configure the ISATAP tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2002:d3a2:0101:1::/64 eui-64
no ipv6 nd suppress-ra
```

Connect interface 1 of the IPv6 network

```
interface FastEthernet 0/2
no switchport
2002:d3a2:0101:10::1/64
```

Connect interface 2 of the IPv6 network

```
interface FastEthernet  0/2
no switchport
2002:d3a2:0101:20::1/64
```

Configure the 6to4 tunnel interface

```
interface Tunnel 2
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source GigabitEthernet 0/1
```

Configure the route to the 6to4 tunnel

```
ipv6 route 2002::/16 Tunnel 2
```

Configure the route to the 6to4 relay router RT-D to access the Cernet network

```
ipv6 route ::/0 2002:d3a2::0901::1
```

RT-B configuration:

Connect the interfaces of the Internet network

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.5.1 255.255.255.0
```

Connect interface 1 of the IPv4 network inside the site

```
interface FastEthernet  0/1
no switchport
ip address 192.168.10.1 255.255.255.0
```

Connect interface 2 of the IPv4 network inside the site

```
interface FastEthernet  0/2
no switchport
```

```
ip address 192.168.20.1 255.255.255.0
```

Configure ISATAP tunnel interface

```
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2002:d3a2:0501:1::/64 eui-64
no ipv6 nd suppress-ra
```

Configure 6to4 tunnel interface

```
interface Tunnel 2
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source GigabitEthernet 0/1
```

Configure the route to the 6to4 tunnel

```
ipv6 route 2002::/16 Tunnel 2
```

Configure the route to the 6to4 relay router RT-D to access the Cernet network

```
ipv6 route ::/0 2002:d3a2::0901::1
```

RT-C configuration:

Connect the interfaces of the Internet network

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.7.1 255.255.255.0
```

Connect the interfaces of the IPv4 network inside the site

```
interface FastEthernet 0/1
no switchport
ip address 192.168.0.1 255.255.255.0
```

Configuer the ISATAP tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2002:d3a2:0701:1::/64 eui-64
no ipv6 nd suppress-ra
```

Connect the interfaces of the IPv6 network

```
interface FastEthernet 0/2
no switchport
2002:d3a2:0701:10::1/64
```

Configure the 6to4 tunnel interface

```
interface Tunnel 2
tunnel mode ipv6ip 6to4
ipv6 enable
tunnel source GigabitEthernet 0/1
```

Configure the route to the 6to4 tunnel

```
ipv6 route 2002::/16 Tunnel 2
```

#Configure the route to the 6to4 relay router RT-D to access the Cernet network

```
ipv6 route ::/0 2002:d3a2::0901::1
```

RT-D(6to4 Relay) configuration:

Connect the interfaces of the Internet network

```
interface GigabitEthernet 0/1
no switchport
ip address 211.162.9.1 255.255.255.0
```

Connect the interfaces of the IPv6 network

```
interface FastEthernet 0/1
no switchport
2001::1/64
no ipv6 nd suppress-ra
```

Configure the 6to4 tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip 6to4
ipv6 address 2002:d3a2::0901::1/64
tunnel source GigabitEthernet 0/1
```

#Configure the route to the 6to4 tunnel

```
ipv6 route 2002::/16 Tunnel 1
```

37 OSPFv3 Configuration

OSPFV2 (RFC2328) runs under the IPv4. The RFC2740 describes OSPFV3, the extension of OSPFv2 that provides support for IPv6 routes. This document briefly describes the OSPFv3 protocol and its configuration.

Caution

Before learning this document, you must know the OSPFv2 protocol and related configuration.

The OSPFv3 protocol extends the OSPFv2 protocol with the same operation mechanisms and most configurations as the OSPFv2.

37.1 Overview

As an Interior Gateway Protocol (IGP), the OSPF runs among the layer 3 devices in a same Autonomous System (AS).

Unlike a vector distance protocol, the OSPF is a link-state protocol. By exchanging various types of link-state advertisements (LSAs) recording link state between devices, it synchronizes link state information between devices and then calculates OSPF route entries through the Dijkstra algorithm.

The OSPFv3 is described in the RFC2740 and supports the IPv6. This section describes the different implementation than OSPFv2.

37.1.1 LSA Association Change

Just as described above, the OSPF is a link-state protocol and its implementation is based on LSAs. Through LSAs, we can know the topologies of networks and address information. In contrast to the IPv4, the IPv6 uses a 128-bit IP address. The design of LSAs is modified accordingly. The types of LSAs are described as follows:

- Router-LSAs (Type 1)

Each device generates this type of LSAs by itself. They describe the states of its links in specified areas and the cost spent on reaching the links.In contrast to the OSPFv2, the Router-LSAs of the OSPFv3 only indicate the state information of links. They do not record the information about the network addresses connected to routers. The information will be acquired by newly added types of LSAs. Additionaly, in the OSPFv2, only one Router-LSA is allowed to be generated for each device in each area. While in the OSPFv3, multiple Router-LSAs are allowed to be generated. Thus, when performing the SPF calculation, we must consider all the Router-LSAs generated by the device. Router-LSAs and Network-LSAs describe the link topology of areas together.

Caution

Through the flag bits on Router-LSAs, we can know whether the routers are Area Border Routers (ABR), AS boundary routers (ASBR) or those at one end of a virtual link.

- Network-LSAs (Type 2)

Network-LSAs only exist in broadcast networks or NBMA networks and are generated by DRs (Designated Routers) in a network. They describe the information about all the routers connected in specified areas on a network. Like Router-LSAs, Network-LSAs also only indicate link-state information and do not record network address information. Network-LSAs and Router-LSAs describe the link topology of areas together.

- Inter-Area-Prefix-LSAs (Type 3)

Generated for an area by the ABRs in the area and used to describe the network information about reaching other areas. They replace type 3 summary-LSAs in OSPFv2. In contrast to the OSPFv2, they use a prefix structure to describe destination network information.

- Inter-Area-Router-LSAs (Type 4)

Generated for an area by the ABRs in the area, used to describe the path information about reaching the ASBRs in other areas, and replacing type 4 summary-LSAs in the OSPFv2.

- AS-external-LSAs (Type 5)

This type of LSAs are generated by ASBRs and used to describe the network information about reaching outside AS. Usually, the network information is generated through other route protocols. In contrast to the OSPFv2, it uses a prefix structure to describe destination network information.

- NSSA-LSA (Type 7)

Their function is same to that of type 5 AS-external-LSAs. However, they are generated by ASBRs in the NSSA area.

- Link-LSAs (Type 8)

In the OSPFv3, the newly added LSA type is generated by each device for each connected link and describes the local link address of the device in the current link and all set IPv6 address prefix information.

- Intra-Area-Prefix-LSAs (Type 9)

In the OSPFv3, the newly added LSA type provides additional address information for Router-LSAs or Network-LSAs. Therefore, it has two effects:

1 Associate network-LSAs and record the prefix information of a transit network.

2 Associate router-LSAs and record the prefix information on all Loopback interfaces, point-to-point links, point-to-multipoint links, virtual links and stub networks of the router in the current area.

Other main change of LSA association:

- LSA flooding scope

In the OSPFv2, the LSA flooding occurs inside areas and ASs. In the OSPFv3, flooding occurs in local link. Type 8 Link-LSAs is the type that can flood only inside a locla link.

- Handling an unknown LSA type

This is an improvement made by the OSPFv3 based on the OSPFv2.

In the OSPFv2, database synchronization is necessary in the initial establishment of adjacency relationship. If there is an unrecognizable LSA type in the database description message, this relationship cannot be established properly. If there is an unrecognizable LSA type in a link-state updating message, then the type of LSAs will be discarded.

In the OSPFv3, it is allowed to receive an unknown LSA type. By using the information recorded in the LSA header, we can determine how to handle the received unrecognizable LSA type.

37.1.1.1 Interface Configuration

In the OSPFv3, the change based on interface configuration is as follows:

1. In order for an interface to run OSPFv3, enable the OSPFv3 directly in the interface

configuration mode. For OSPFv2, however, run the Network command in the OSPF route configuration mode.

2. If an interface runs OSPFv3, all the addresses on the interface will run IPv6. In the OSPFv2,however, all the addresses are enabled via a **network** command.
3. In the environment where the OSPFv3 runs, a link can support multiple OSPF entities and different devices connecting this link can run one of these OSPF entities. The OSPFv2 does not support this function.

37.1.1.2 Router ID Configuration

Each device running the OSPFv3 process must be identified with a router ID in the IPv4 address format.

Unlike the OSPFv2 that automatically gets an IPv4 address as a rotuer ID, to enable OSPFv3, you need use the **router-id** command to configure a router ID for the OSPFv3.

37.1.1.3 Authentication Mechanism Configuration

The OSPFv2 itself supports two authentication modes: plain text authentication and key authentication based on MD5. The OSPFv3 itself does not provide any authentication. Instead, it use the IPSec authentication mechanism. In future, we will support the IPSec authentication mechanism.

37.1.2 Basic OSPFv3 Configuration

The OSPFv3 protocol of DES-7210 Network has the following features:

- Supports multi-instance OSPF;
- Supports network type setting;
- Supports virtual link;
- Supports passive interfaces;
- Supports an interface to select a participant OSPF entity;
- Supports stub area;
- Supports route redistribution;
- Supports route aggregation;
- Supports timer setting;

To be implemented:

- Supports NSSA areas;
- Supports authentication. The OSPFv3 will use the IPSec authentication mechanism.

Default OSPFv3 configuration:

Router ID		Undefined
Interface Configuration	Interface type	Broadcast network
	Interface cost	Undefined
	Hello message sending interval	10 seconds
	Dead interval of adjacent device	4 times the hello interval.
	LSA sending delay	1 seconds
	LSA retransmit interval	5 seconds
	Priority	1
	MTU check of database description messages	Enabled
Virtual Link	Virtual Link	Undefined

Router ID		Undefined
	Hello message sending interval	10 seconds
	Dead interval of adjacent device	4 times the hello interval.
	LSA sending delay	1 seconds
	LSA retransmit interval.	5 seconds
Area Configuration	Area	Undefined
	Default router cost for stub and NSSA area	1
Route Information Aggregation	Inter-area route aggregation	Off
	External route aggregation	Off
Management Distance	Intra-area route	110
	Inter-area route	110
	External route	110
Auto cost		Enabled The default cost reference is 100 Mbps.
Changing LSAs Group Pacing		240 seconds
Shortest path first (SPF) timer		Time from receiving the topology change to running SPF at the next time :5 seconds The least interval between two calculations:
Route redistribution		Off
Route filtering		Off
Passive interface		Off

To run the OSPFv3, execute the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
ipv6 router ospf *process-id*	Start the OSPFv3 route process and enter the OSPFv3 configuration mode.
router-id *router-id*	Configure the Router ID for running the OSPFv3.
interface interface-type interface-id	Enter the interface configuration mode.
ipv6 ospf *process-id* **area** *area-id* **[instance-id** *instance-id***]**	Enable the OSPFv3 on an interface. *instance-id:* The OSPFv3 entity number that the interface participates in. The interfaces of different devices connecting a network select to participate in different OSPFv3 entities.
copy running-config startup-config	Save the configuration.

Caution

In the interface configuration mode, first enable the interface to participate in OSPFv3 and then configure the OSPFv3 process. After you configure the OSPFv3 process, the interface will automatically participate in the appropriate process.

37.1.3 Configuring OSPF Parameters on the Interface

In the interface configuration mode, you can modify the OSPF parameters of an interface to meet practice application needs.

To configure OSPF parameters on the interface, execute the following commands in the interface configuration mode:

Command	Function
ipv6 ospf *process-id* **area** *area-id* **[instance-id** *instance-id***]**	Configure the interface to participate in the OSPFv3 routing process.
ipv6 ospf network {**broadcast** | **non-broadcast** | **point-to-point** | **point-to-multipoint** [**non-broadcast**]} [**instance** *instance-id*]	Set the network type of an interface. The default is the broadcast network type.
ipv6 ospf cost *cost* [**instance** *instance-id*]	(Optional) Define the cost of an interface.
ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]	(Optional) Set the time interval to send the Hello message on an interface. For all nodes in the whole network, the value must be same.
ipv6 ospf dead-interval *seconds* [**instance** *instance-id*]	(Optional) Set the adjacency dead-interval on an interface. For all nodes in the whole network, the value must be same.
ipv6 ospf transmit-delay *seconds* [**instance** *instance-id*]	(Optional) Set the interval of transmitting link state.
ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]	(Optional) Set the LSA transmit delay on an interface.
ipv6 ospf priority *number* [**instance** *instance-id*]	(Optional) Set the priority of an interface. The priority is used to select Designated Routers (DR) and Backup Designated Routers (BDR).

To remove the configuration, use the **no** form of the above commands.

Caution

You can modify the parameter setting of an interface based on actual needs. However, be sure that the settings of some parameters must be identical to those of neighbors. Otherwise, it will be impossible to establish the adjacency relationship. These parameters include the following: **instance, hello-interval and dead-interval.**

37.1.4 Configuring OSPFv3 Area Parameter

The OSPF protocol applies the concept of “hierarchical structure”, allowing a network to be divided into a group of parts connected through a “backbone” in mutual independence way. These parts are called Areas. The backbone part is called Backbone Area and always indicated by the numerical value 0 (or 0.0.0.0).

By using this hierarchical structure, each device is allowed to keep the link state database in the area where it resides and the topology inside the area is invisible to outside. In this way, the link state database of each device can be always in a reasonable size, route calculation time is not too much and the number of messages is not too big.

In the OSPF, the following types of special areas have been defined to meet actual needs:

- stub Area.

If an area is at the end part of the whole network, then we can design the area as a stub area.

A stub area cannot learn the external route information of an AS (type 5 LSAs). In practical application, external route information is very important in the linkstate database. Therefore, the devices inside a stub area will learn little route information, reducing the system resources for running the OSPF protocol.

When a device inside a stub area wants to access outside of an AS, use the default route entrie (type3 LSA) generated from the default route information published by Area Border Routers in the stub area.

- NSSA area (Not-So-Stubby Area)

NSSA extends the stub area. By preventing from flooding type 5 LSAs to the devices in the NSSA, it reduce the consumption of device resources. However, unlike a stub area, it allows a certain amount of external route information of the AS to enter an NSSA in other ways, namely, inject into the NSSA in the form of type 7 LSAs.

To configure OSPFv3 area parameters, execute the following command in the OSPFv3 configuration mode:

Command	Function
area *area-id* **stub** [**no-summary**]	Configure a stub area. no-summary: configure the area to a totally stub area, preventing the area border router in the stub area from sending type3 LSAs to the stub area.
area *area-id* **default-cost** *cost*	Configure the cost of the default route sent to a stub area or NSSA.

To remove the configuration, use the **no** form of the above commands.

Caution

After configured an area as the stub area, you can configure the default-cost parameter. If this area is changed as an ordinary area, the default-cost configuration will be deleted automatically.

37.1.5 Configurring OSPFv3 Virtual Link

In the OSPF, all areas must connect to the backbone area to ensure the communication with other areas.If some areas cannot connect to the backbone area, they must use virtual links to connect the backbone area.

To establish a virtual link, execute the following command in the OSPFv3 configuration mode:

Command	Function
area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**transmit-delay** *seconds*] [**retransmit-interval** *seconds*] [**instance** *instance-id*]	Configure a virtual link.

To remove the configuration, use the **no** form of the above commands.

Caution

1. It is not allowed to create a virtual link in the stub area and NSSA.
2. A virtual link can be taken as a special interface, so its configuration is same to that of a normal interface. You must ensure that the configurations of **instance, hello-interval** and **dead-interval** configured at the two ends of the virtual link are identical.

37.1.6 Configuring OSPFv3 Route Aggregation

Without route aggregation, every device in a network must maintain the routeing information of the whole network. By aggrgating some information together, route aggregation can alleviate the burden on the L3 equipment and network bandwidth. As the size of a network is growing, route aggregation becomes more and more important.

Layer 3 devices of DES-7210 Networks Ltd support two kinds of route aggregation: inter-area route aggregation and external route aggregation.

37.1.6.1 Configuring Inter-area Route Aggregation

The ABR in an area needs to advertise the routes in the area to other areas. If the route addresses are continuous, the ABR aggregates these routes and then advertises it.

To configure inter-area route aggregation, execute the following command in the OSPFv3 configuration mode:

Command	Function
area *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not-advertise**]	Configure inter-area route aggregation.

Use the **no area** *area-id* **range** {*ipv6-prefix* /*prefix-length*} command to disable the inter-area route aggregation.

37.1.7 Configuring Bandwidth Reference Value of OSPFv3 Interface Metric

The metric for the OSPF protocol is a bandwidth value based on an interface. The cost value of the interface is calculated based on its bandwidth.

For example, if the bandwidth reference value of an interfaces is 100 Mbps and the bandwidth of theinterfaces is 10Mbps, the automatically calculated interface cost is 100/10=10.

Currently, the interface refernece value of network interfaces of DES-7210 Networks is defaulted to 100 Mbps.

To change the bandwidth reference value, execute the following command in the OSPFv3 configuration mode:

Command	Function
auto-cost [**reference-bandwidth** *ref-bw*]	Configure the bandwidth reference value for interface metric.

Caution

You can run the **ipv6 ospf cost** *cost-value* command in the interface configuration mode to set the cost for a specified interface, which takes precedence over the one calculated based on bandwidth reference value.

37.1.8 Configuring OSPFv3 Default Route

In the OSPFv3 protocol, you can generate default route in many ways. For example, the default route represented by Type-3 LSA will be automatically generated in a stub area. For details, refer to Configuring OSPFv3 Area Parameters. In addition, you can configure a default route represented by Type 5 LSA and advertise it to the whose OSPF AS.

To configure a default rotue, execute the following commands in the OSPFv3 configuration mode:

Command	Function
default-information originate [always] [metric *metric-value***] [metric-type** *type-value***] [route-map** *map-name***]**	Configure a default route.

Execute the **no default-information originate** command to remove the generated default route.

Caution

1. This command cannot be configured on the devices in a stub area.
2. Once configured, the device automatically becomes ASBR.

37.1.9 Configuring OSPFv3 Timer

The OSPF protocol belongs to link-state protocols. When the link state changes, the OSPF process will trigger the SPF calculation. You can also use the following command to configure SPF calculation delay and the interval between two SPF calculations.

To configure OSPF timer, execute the following commands in the OSPFv3 configuration mode:

Command	Function
timers spf *delay holdtime*	Configure SPF calculation delay and the interval between two SPF calculations.

37.1.10 Configuring OSPFv3 Route Redistribution

Route redistribution allows you to redistribute the routes of one routing protocol to another routing protocol.

To configure the OSPFv3 route redistribution, execute the following commands in the OSPFv3 configuration mode:

Command	Function
redistribute *protocol* [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-tag*] [**match** [**internal** | **external** | **nssa-external** (1|2)]]]	Redistribute the routes of one routing protocol to another routing protocol. You can set the conditions of redistribution. At present, the OSPFv3 supports redistribution of static, connect, RIP, and OSPF routes. When redistributing OSPF routes, you can configure the match parameter to redistribute the OSPF routes of the specific sub type.
default-metric *number*	Configure the default metric for route redistribution.

You can use the **no redistribute** *protocol* mode to disable route redistribution.

37.1.11 Configuring OSPFv3 Passive Interface

To prevent other Layer 3 devices in the network from learning the route information of this device, you can set a network interface to a passive interface in the routing protocol configuration mode

For the OSPFv3 protocol, if a network interface is configured as a passive network interface, then this network interface will receive/send no OSPF message.

To configure an interface as a passive interface, execute the following command in thr OSPF3 configuration mode:

Command	Function
passive-interface {**default** | *interface-type interface-number* }	Configure a passive interface.

You can use the **no passive-interface** {*interface-id* | **default**} command to cancel the configuration of a passive interface.

37.1.12 Debugging and Monitoring OSPFv3

The OSPFv3 process supports plenty of debug commands and monitoring commands.

37.1.12.1 OSPFv3 Debugging Command

To debug OSPFv3, execute the following commands in the privileged configuration mode:

Command	Function
debug ipv6 ospf events	Show the OSPFv3 event information.
debug ipv6 ospf ifsm	Show the state machine events and changes of the outbounding interface.
debug ipv6 ospf lsa	Show the related OSPFv3 LSA information.
debug ipv6 ospf nfsm	Show state machine events and changes of neighbor.
debug ipv6 ospf nsm	Show the OSPFv3 NSM module related information.
debug ipv6 ospf packet	Show the OSPFv3 packet information.
debug ipv6 ospf route	Show the OSPF routing calculation and addition information.

Use the above **undebug** commands to disable the above enabled **debug** commands.

Caution

The **debug** commands are provided for technicians.

Running a **debug** command will affect the performance of the system in a certain extent. Therefore, after running **debug** commands, be sure to use **undebug** commands to protect the performance of the system.

37.1.12.2 OSPFv3 Monitoring Command

To monitor OSPFv3, execute the following commands in the privileged configuration mode:

Command	Function
show ipv6 ospf	Show the information of the OSPFv3 process.
show ipv6 ospf [*process-id*] **database** [**isa-type** [**adv-router** *router-id*]]	Show the database information of the OSPF process.
show ipv6 ospf interface *[interface-type interface-number]*	Show the interface information of the OSPFv3 process.
show ipv6 ospf [*process-id*] **neighbor** [*interface-type interface-number* [**detail**]] *[neighbor-id*] [**detail**]	Show the neighbor information of the OSPFv3 process.
show ipv6 ospf [*process-id*] **route**	Show the OSPFv3 route information.

Command	Function
show ipv6 ospf [*process-id*] **topology** [**area** *area-id*]	Show each area topology of the OSPFv3.
show ipv6 ospf [*process-id*] **virtual-links**	Show the virtual link information of the OSPFv3 process.

38 IPv4 Multicast Routing Configuration

38.1 Overview

IPv4 multicast refers to a network technology that forwards packets to more than one receiver through a multicast flow. Only the hosts joining the group can receive the packets from the specific multicast group. Multicast can save network bandwidth greatly for there is only single packet transmitting on any link of the network, no matter how many receivers are deployed.

Multicast uses Class-D network address specified by IANA. The highest bits of Class-D network address are 1110. So, the Class-D network address is in the range of 224.0.0.0 to 239.255.255.255. However, not all addresses in this range can be used by users. The addresses in the range 224.0.0.1 to 224.0.0.255 are reserved for protocols. For instance, 224.0.0.1 indicates all multicast host addresses and 224.0.0.2 indicates all multicast device addresses.

Multicast packets are UDP packets with best effort service. It does not provide reliable transmission and error control as TCP.

The multicast environment consists of senders and receivers. The sender sends multicast packets with a multicast group address used to distinguish different multicast flows. However, only the members of a group can receive the message destined to this group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. If necessary, a host can be a member of more than one multicast group at a time. Therefore, the active status of a group and the number of group members vary from time to time.

Devices run a multicast routing protocol (such as PIM-DM, PIM-SM, etc.) to maintain their routing tables to forward multicast messages, and use the IGMP to learn the status of the members within a group on their directly attached subnets. A host can join or leave an IGMP group by sending corresponding IGMP Report messages.

IP multicast is ideal for “one-to-multiple” multimedia applications.

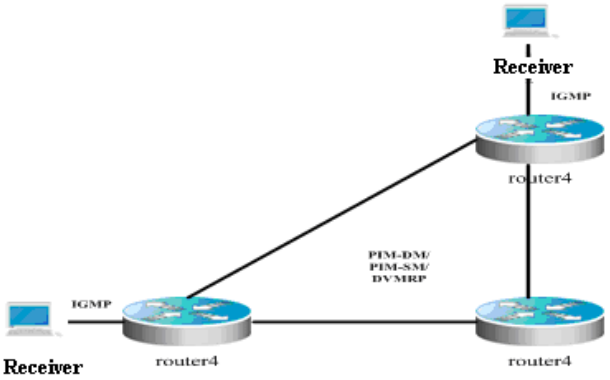
38.1.1.1 IP Multicast Routing Implementation

There are the following multicast routing protocols:

- IGMP: Runs between the routers and the hosts in a LAN to track the membership of a group and learn the relation among members.
- PIM-DM: A multicast routing protocol in dense mode, which runs between multicast devices to establish the multicast routing table for forwarding.
- PIM-SM: A multicast routing protocol in sparse mode, which runs between multicast devices to establish the multicast routing table for forwarding.
- DVMRP: Distance Vector Multicast Routing Protocol, which runs between multicast devices to establish the multicast routing table for forwarding.

The following figure shows the multicast routing protocols used in the IPv4 multicast environment:

Figure-1 IP Multicast Routing Protocols within the IP Multicast Environment



38.1.2 IGMP Overview

To enable IPv4 multicast, multicast hosts and devices must support IGMP. This protocol is used by the host to notify the multicast device of the multicast membership of the network they connect to determine how to forward multicast traffic. By using the information obtained from the IGMP, the device can maintain an interface and group-based multicast member list. The multicast member list is activated only when at least one host of an interface is a member of the group.

IGMPv1, IGMPv2 and IGMPv3 are supported at present. On the basis of IGMPv1, IGMPv2 has the leaving message so that the host can actively request to leave a multicast group. IGMP activities fall into two parts: host activity and device activity.

38.1.2.1 IGMPV1

There are only two types of messages defined in IGMP Version 1: Membership query and Membership report.

A host sends a report packet to join a group, and the router sends the query packet at periodical intervals to ensure that a group has at least one host. When a group contains no host, the router will delete that group.

38.1.2.2 IGMPV2

In Version 2, there are only four types of packets:

- Membership query
- Version 1 membership report
- Version 2 membership report
- Leave group

IGMPv2 is basically the same as IGMPv1, except that the leave mechanism of the host has been improved. For V2, the host can send a leave message to notify the device, which then sends a query to verify if there is a host in the multicast group. This makes joining and leaving a group more efficiently.

In the multicast network that runs IGMP, there is a dedicated query multicast device, which is responsible for sending IGMP query messages. This de querier is chosen through an election process. At the beginning, all the devices are queriers. When a device receives a query message, it compares the source IP address of the message. For IGMPv1, the device of the highest IP address is elected as the querier. However, for IGMPv2/v3, the one of the lowest IP address is selected as

the querier. Moreover, for the IGMP query messages with different versions, the one sending the IGMP query message of the lowest version is elected as the querier.

If the querier fails, the querier is elected again. The non-querier devices maintain the interval timers of other queriers. Every time when a device receives a membership query packet, it resets the timer. If the timer expires, the device considers itself is the querier and starts to send query messages. The querier election starts again.

The querier must send the membership query request periodically to ensure that other devices in the network know that the querier still works. For this purpose, the querier maintains one query interval timer. When it sends the membership query message, this timer will be reset. When the interval timer times out, the querier sends another membership query.

When the device appears for the first time, that is, a new device is added, it sends a series of general query messages to see which multicast groups will be received on the hosts of which interfaces for rapid convergence. The number of common query packets sent is based on the start query count configured. The querying interval between the initial general query messages is defined through the startup query interval.

When a querier receives a leave packet, it must send a particular group membership query to see if the host is the last one leaving the group. Before the querier stops forwarding packets to the group, it sends a series of such packets, the number of which is equal to the last member query number. The querier sends multiple particular membership queries to ensure that there is no member in the group. Such a query is sent every other the seconds of the last-member query interval to separate the queries. When no response is received, the querier stops forwarding multicast packets to the group on the particular interface.

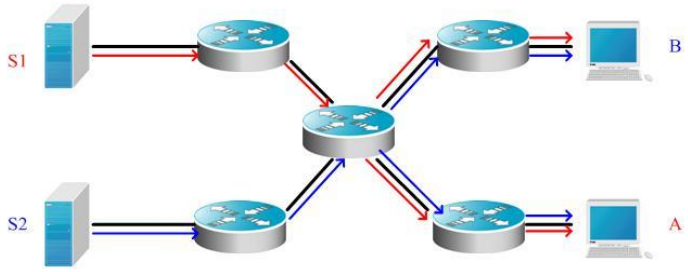
38.1.2.3 IGMPV3

In the applications of the IGMPV1 and V2, there are the following defects:

- Lack of efficient measures to control multicast sources
- Difficult to establish the multicast path due to unknown multicast source
- Difficult to find a unique multicast address. It is possible that multicast groups are using the same multicast address.

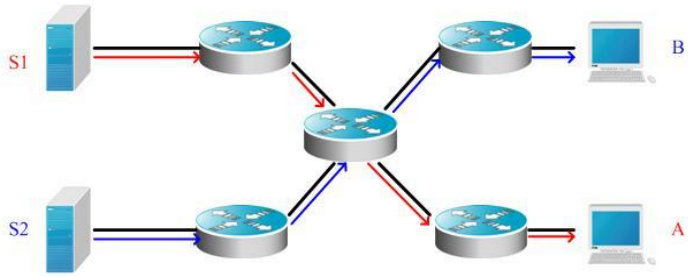
On the basis of IGMPV1/V2, IGMPV3 provides an additional source filtering multicast function. In IGMP V1/V2, the host determines to join a group and receive the multicast traffic to the group address from any source only based on the group address. On the other hand, the host running the IGMP V3 notifies this host the desired multicast group to join, and also the addresses of the multicast sources to receive. The host can indicate that it wants to receive multicast traffic from which sources through an inclusion list or an exclusion list. At the same time, another benefit of the IGMP v3 is that it saves bandwidth to avoid unnecessary, invalid multicast data traffics from occupying network bandwidth. It is particularly useful in the case where multiple multicast sources share one multicast address. The IGMPv1 and IGMPv2 can also implement “source address filter” in some sense, which, however, is performed on the end of receiving the multicast traffic. As shown in the following diagram, there are two multicast sources (S1 and S2), which send the data traffic of the same multicast address (G). The multicast flow of S1 and S2 will be sent to all hosts receiving flows from G. If host A only wants to receive multicast flows from S1, it filters flows by using the related client software.

Figure-2 Multicast route forwarding without filtering source



If the equipments in the network support IGMP v3, host A wants to receive the traffic from S1 only. It can send the IGMPv3 packet of join G include S1. If host B wants to receive the traffic from S2 only, it can send the IGMPv3 packet of join G include S2. Therefore, the traffics are forwarded as shown in the following diagram. This saves bandwidth.

Figure-3 Multicast route forwarding with filtering source



In contrast to Version 2, Version 3 defines the following two kinds of messages:

- Membership Query
- Version 3 Membership Report

There are three types of Membership Query:

- General Query: Used to query all the multicast members under the interface.
- Group-Specific Query: Used to query the members of the specified group under the interface.
- Group-and source-Specific Query: This type is the new one in the IGMPv3, which is used to query if any member under the interface needs to receive the multicast traffic of the particular group from the sources in the specified source list.

Different from the Membership Report in IGMP Version2, the Membership Report in the IGMP Version3 always has the destination address of 224.0.0.22. The Membership Report packets in IGMP Version3 include the information of multiple groups. It can carry with one or more group records, each record with group address and source address list. Below shows the types of group record:

IS_IN: Indicates INCLUDE filtering mode between the multicast group and the multicast source list, that is, only the multicast traffic from the specific multicast source list to the multicast group are received. A null multicast source list means leaving the multicast group, which is equivalent to the leave message in IGMPv2.

IS_EX: Indicates EXCLUDE filtering mode between the multicast group and the multicast source list, that is, only the multicast traffic from any multicast source except for the specific multicast source list to the multicast group are received.

TO_IN: Indicates that the filtering mode between the multicast group and the multicast source list changes from EXCLUDE to INCLUDE.

TO_EX: Indicates that the filtering mode between the multicast group and the multicast source list changes from INCLUDE to EXCLUDE.

ALLOW: Indicates receiving multicast traffic from additional multicast sources. For INCLUDE mode, it adds these multicast source to the multicast source list. For EXCLUDE mode, it removes these multicast sources from the multicast source list.

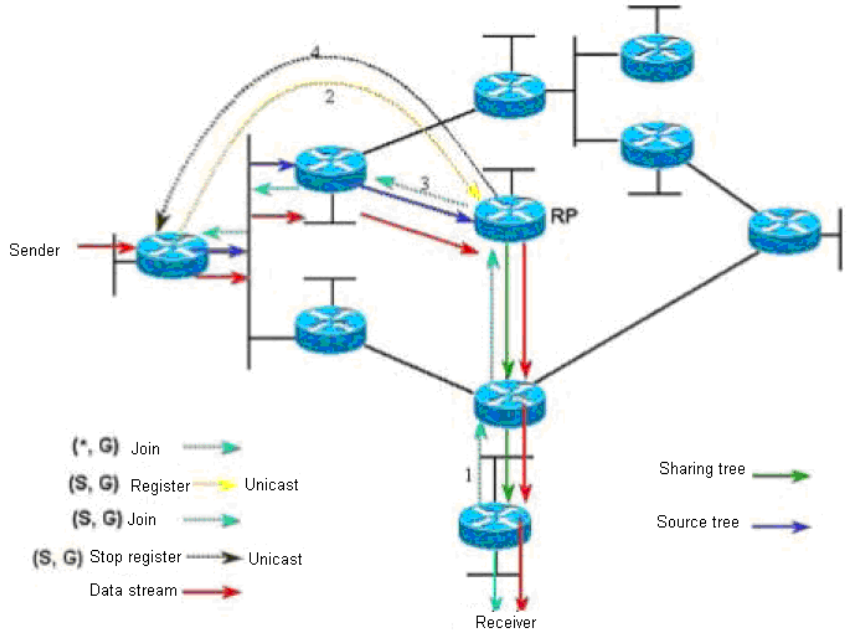
BLOCK: Indicates no longer receiving multicast traffic from some multicast sources. For INCLUDE mode, it removes these multicast source from the multicast source list. For EXCLUDE mode, it adds these multicast sources to the multicast source list.

For the sake of compatibility, IGMPv3 can identify IGMPv1/v2 packets.

38.1.3 PIM-SM Overview

The Protocol Independent Multicast Sparse Mode (PIM-SM) is a protocol independent multicast sparse mode. In a PIM-SM domain, the PIM-SM-enabled device sends the Hello message to discover adjacent PIM-SM devices and selects the designed router (DR) in a multi-access network. The DR is responsible for sending the join/prune message in the root node of the multicast distribution tree direction for the direct connection group member, or sending the data of the direct connection multicast source to the multicast distribution tree.

Join Mechanism of PIM-SM Explicitly



The PIM-SM forwards multicast data packets by establishing a multicast distribution tree. The multicast distribution tree is divided into two types: Shared Tree that takes the RP of the group G as the root and Shortest Path Tree that takes the multicast source as the root. The PIM-SM establishes and maintains the multicast distribution tree with the explicit join/prune mechanism. As shown in the above figure, when the DR receives a join request from the receiving terminal, it will multicast a (*.G) join message hop-by-hop to the RP of the group G to join the shared tree. When the source host sends multicast data to the group, the source data is encapsulated into the registration message and unicasted by the DR to the RP. Then the RP will forward the deencapsulated data packets to group members along the shared tree. The RP will send a (S, G) join message to the first hop on the source direction to join the shortest path tree of this source. In this way, the source's data packets are sent to the RP without encapsulation along its shortest path tree. When the first multicast data reaches along this tree, the RP will send the registration stop message to the DR of the source, notifying the DR of stopping registration. Consequently, the source's multicast data packets are sent to the RP along its shortest path tree rather than being registered and encapsulated. Then the RP forwards the data packets to group members along the

shared tree. When there is no need of multicast data packets, the DR multicasts a prune message to the RP of the group G hop-by-hop to prune the shared tree.

The PIM-SM also offers a mechanism of select the root point (RP). One or more Candidate-BSRs are configured in a PIM-SM domain. The PIM-SM selects a BSR by following a certain rule. There are also Candidate-RPs in a PIM-SM domain that unicast the packets including their IP addresses and available multicast groups to the BSR. The BSR will periodically generate a BSR message which includes a system candidate RP and the corresponding multicast group address. The BSR messages are sent hop-by-hop within the whole domain. The device receives and saves these BSR messages. If the DR receives a report on the member relationship of a multicast group from its directly connected host but has no route entries of the multicast group, the DR will use one Hash algorithm to map the multicast group address to a candidate RP that can serve this group. Then, the DR multicasts the Join/Prune message to the RP hop-by-hop. If the DR receives multicast data packets from its directly connected host but has no route entries of the multicast group, the DR will use one Hash algorithm to map the multicast group address to a candidate RP that can serve this group. Then the DR encapsulates multicast data packets into the registration message and unicasts it to the RP.

The main difference between the PIM-SM and the broadcast/prune model-based PIM-DM is that the PIM-SM is based on the explicit join model. In other words, the receiver sends the join message to the RP, while the router only forwards the packets of that multicast group on the outbound interface that has joined a multicast group. The PIM-SM uses the shared tree to forward multicast packets. Each group has a Rendezvous Point (RP). The multicast source sends the data to the RP along the shortest path, and then the RP sends the data to the receivers along the shortest path. This is similar to the CBT, but the PIM-SM does not use the concept of core. One of the major advantages of the PIM-SM is that it not only receives multicast messages through the shared tree but also provides a shared tree-to-SPT conversion mechanism. Such conversion reduces network delay and possible congestion on the RP, but it consumes enormous router resources. So it is suitable for the case where there are only a few multicast data sources and network groups.

The PIM-SM uses the shared tree and SPT to distribute multicast frames. At this time, it is assumed that other devices don't want to receive these multicasts unless otherwise stated definitely. When a host joins a group, the equipment connected to the host must notify the root (or the RP) by using the PIM join message. This join message is transferred one after another through the routers to create a shared tree structure. Therefore, the RP records the transfer path and also the registration message from the first hop router (DR) of the multicast source, and improves the shared tree upon these two messages. The branch/leaf messages are updated by periodically querying messages. With the shared tree, the multicast source first sends multicast packets to the RP, guaranteeing that all the receivers can receive them.

The PIMv2 BSR is a method of distributing the group-to-RP message to all devices without the need of setting the RP for them. The BSR uses the hop-by-hop broadcast BSR message to distribute the mapping message. At first, the BSR is selected among routers in the same process as selecting a root bridge based on priority level among layer 2 bridges. Each BSR checks the BSR messages and only forwards those having a priority higher than or equal to its own (higher IP address). The selected BSR sends its BSR message to the all-PIM-routers multicast group (224.0.0.13), where TTL is 1. After the adjacent PIMv2 router receives the message, it multicasts it while setting the TTL to 1. In this way, the BSR message is received by all devices hop-by-hop. Since the message contains the IP address of the BSR, the candidate BSR can know which router is the current RP based on this message. The candidate RPs send candidate RP advertisements to announce in which address ranges they can become an RP. The BSR stores them in its local candidate RP cache. The BSP notifies all PIM routers of its local candidate RPs periodically. These messages reach various devices hop-by-hop in the same way.

38.1.4 PIM-DM Overview

PIM-DM (Protocol Independent Multicast-Dense Mode), a multicast routing protocol in dense mode, is suitable for the environments of small network size and centralized multicast members. Since

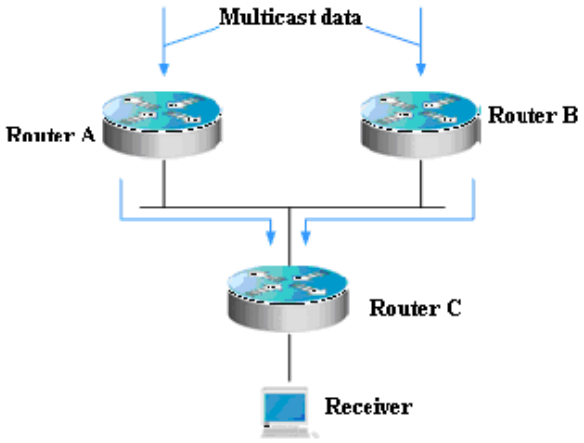
PIM-DM does not rely on any specific unicast routing protocol, it is called protocol independent multicast routing protocol. PIM-DM is defined in RFC 3973.

PIM-DM devices discover neighbors through Hello messages. After start, a PIM-DM device sends a Hello message to the PIM-DM-enabled interface periodically. The Hello message has a field called Hello Hold Time, which defines the period that a neighbor waits for the next message. If the neighbor has not received the next Hello message from the sender within this period, it announces the device's death.

PIM-DM sets up a multicast tree through flood and prune. Assume that when a multicast source begins to send a multicast packet, all the systems in the network need to receive this packet. As a result, this packet is forwarded to every system. The reverse path forwarding check is done for the packets received from the upstream interface. Those packets who fail to pass the check will be dropped. For the packets passing the check, the egress is calculated based on the (S, G) pair of the packets, or source address and group address. If the egress exists, an egress entry is set up fro the (S, G) pair and the multicast packet is forwarded through this egress. If the calculated egress is null, a prune message is sent to RPF, informing the upstream neighbor not to forward the multicast packets from the (S, G) pair to this egress. Upon receiving the prune message, the upstream interface marks the sending interface as pruned status, and set a pruned state timer. In this way, a multicast forwarding tree at the root of multicast source is set up.

PIM-DM utilizes the Assert mechanism to eliminate redundant routes.

Figure-4 Figure 4 PIM-DM's Assert mechanism



As shown in the above figure, the multicast data arrives at Router A and B at the same time, which forward the data to Router C. In this case, Router C receives two copies of the data. This is not allowed. So there must be a mechanism to select Router A or B to forward the multicast data to Router C. This is the Assert mechanism of PIM-DM.

PIM-DM uses the state refresh message to update network state. The device directly connecting to the multicast source sends the state refresh message to the downstream devices periodically to inform topology change. The devices receiving the message add their topology state to the state refresh message by modifying some fields, and then send to the downstream devices. When the refresh message arrives the leaf devices, the whole network state is updated.

PIM-DM utilizes the Graft mechanism to reestablish the connection with upstream devices. If the network topology of a downstream device in pruned state changes and needs to receive multicast data from a (S, G) pair, it sends the graft message to the upstream device. Upon receiving the graft message, the upstream device responds with a Graft-Ack message and forwards the multicast data to the downstream device again.

38.1.5 DVMRP Overview

DVMRP (Distance Vector Multicast Routing Protocol) is the earliest widely-used multicast routing protocol in the Internet, and also in the dense mode. Similar to PIM-DM, DVMRP also uses the reverse path multicast mechanism to build the distribution tree to forward the multicast packets. The difference of PIM-DM and DVMRP mainly lies in that PIM-DM is independent from the detailed unicast routing protocol, while DVMRP depends on the RIP.

DVMRP device advertises itself, learns the neighbor address and builds the adjacency relation by sending the Probe packets. If the received Probe packets sent from the neighbor include the IP address for DVMRP device, the adjacency relation is built.

DVMRP neighbors exchange the source routing information, including the source network mask and hops, by periodically sending Report packets. Those routing information are stored in a DVMRP routing table separated from the unicast routing table, and used to the RPF check in the process of establishing the source tree.

DVMRP is also a dense mode multicast routing protocols, creating the multicast forwarding tree for each multicast source. The initial multicast data are forwarded along the entire multicast forwarding tree, but the redundant paths are not forwarded. For the specified multicast forwarding tree, the device will send a Prune packet to the upstream if it is no need for the device to receive the multicast data. The device determines whether it is necessary to receive the specified multicast data by confirming the existence of the downstream neighbor or multicast member information. Once the pruning timeouts, the multicast data will be re-spread.

In addition, to enable multicast receivers to quickly join the multicast forwarding tree, DVMRP also supports grafte and grafte confirm mechanism. The grafte confirm mechanism is used to avoid the graft information loss due to the network congestion.

38.2 Basic Multicast Routing Configuration

Basic multicast configuration includes:

- Enable multicast routing forwarding (Mandatory)
- Enable multicast routing protocol (Mandatory)

38.2.1 Enabling Multicast Routing Forwarding

The multicast protocol can receive and process multicast packets and protocol packets only when the multicast routing forwarding function is enabled.

In the global configuration mode, execute the following command to enable the multicast routing forwarding function:

Command	Function
DES-7210 (config) # **ip multicast-routing**	Enable multicast routing forwarding.
DES-7210 (config) # **no ip multicast-routing**	Disable multicast routing forwarding.


Caution

For DES-7206 DES-7210, the multicast routing forwarding function and SVGL mode&IVGL-SVGL mode of IGMP SNOOPING are mutually exclusive. Before enabling the multicast routing forwarding function, please make sure that SVGL mode&IVGL-SVGL mode of IGMP SNOOPING have been disabled. Or it will prompt: `ip multicast-routing conflicts with SVGL mode of IGMP SNOOPING!` he multicast routing forwarding function can be co-used with IVGL mode of IGMP SNOOPING. The source IP check funciton of IGMP SNOOPING can not be enabled.

38.2.2 Enabling Multicast Routing Protocol

In the interface configuration mode, execute the following commands to enable the multicast routing protocols:

Command	Function
DES-7210 (config-if) # **ip pim dense-mode**	Enable PIM-DM multicast routing protocol in the interface configuration mode. This command must be configured on the Layer3 interface.
DES-7210 (config-if) # **ip pim sparse-mode**	Enable PIM-SM multicast routing protocol in the interface configuration mode. This command must be configured on the Layer3 interface.
DES-7210 (config-if) # **ip dvmrp enable**	Enable DVMRP multicast routing protocol in the interface configuration mode. This command must be configured on the Layer3 interface.

The following example shows how to configure the PIM-SM mode on the interface GabitEthernet 0/3:

```
DES-7210(config)# ip multicast-routing
DES-7210(config)# interface  gabitEthernet 0/3
DES-7210(config-if)# ip address 192.168.194.2 255.255.255.0
DES-7210(config-if)# ip pim dense-mode
```


Note

Enabling multicast routing forwarding and multicast routing protocol will enable the IGMP function on the interface at the same time.

Only one-mode multicast routing protocol can be enabled on one device.

38.2.3 Enabling IGMP

Enabling multicast routing forwarding and multicast routing protocol will enable the IGMP function on the interface at the same time.

38.2.4 Configuring the Multicast Routing RPF Check Mode

In the global configuration mode, execute the following commands to configure the multicast routing RPF check mode, the default mode is SVI mode:

Command	Function
DES-7210 (config-if) # **ip multicast-rpf** *rpf-mode*	Set the RPF-mode check on the condition that the port is routed port or SVI port.

38.3 Configuring Multicast Routing Features

Advanced IPv4 multicast routing features include:

- Configure TTL threshold (Optional)
- Limit the number of entries to be added in the IPv4 multicast route table (optional)
- Set IPv4 multicast boundary (optional)
- Configure static routes (optional)
- Monitor and maintain IPv4 multicast (optional)

38.3.1.1 Configuring TTL Threshold

You can configure TTL threshold to limit the TTL of the packets traveling through an interface.

Use the **ip multicast ttl-threshold** command to configure TTL threshold of multicast packet which is allowed to transmit through the interface in the interface configuration mode. The **no ip multicast ttl-threshold** command restores to the default value. The TTL threshold defaults to 1. 0 means the interface will not function as the outlet of packets.

Command	Purpose
DES-7210 (config-if) # **ip multicast ttl-threshold** *ttl-value*	Configure TTL threshold in the range 0 to 255.

38.3.1.2 Limiting the Number of Entries to be Added in the IPv4 Multicast Routing Table

Use the **ip multicast route-limit** *limit* [*threshold*l command to limit the number of entries to be added in the multicast routing table, and use the **no ip multicast route-limit** *limit* [*threshold*l command to restore it to the default value, or 1024.

Command	Purpose
DES-7210 (config) # **ip multicast route-limit** *limit* [*threshold*]	Limit the number of entries to be added in the multicast routing table. *limit*: Number of entries to be added in the multicast routing table in the range of 1 to 2147483647, and 1024 by default. *threshold* (optional): Number of routes triggering an alert message, 2147483647 by default. Note: As the hardware is limit for different models, the multicast packets beyond the hardware forwarding table will be forwarded by the software. This will occupy CPU and sacrifice system performance.

38.3.1.3 Configuring IPv4 Multicast Boundary

Use the **ip multicast boundary** *access-list* command to configure the interface as the multicast boundary of a specific IP group in the interface configuration mode and use the **no ip multicast boundary** command to restore the default value.

Command	Purpose
DES-7210 (config-if) # **ip multicast boundary** *access-list* {**in | out**}	Configuring the IPv4 Multicast Boundary of the specific IP group. Numerical standard ACL or name can be used to specify an IP group. Note that The ACL in this command is specific for matching destination IP address, not group IP address and source IP address.

This command filters the IGMP, PIM-SM and PIM-DM packets associated with the IP group. Multicast packets will not flow in and out from the multicast boundary.

38.3.1.4 Configuring IPv4 Multicast Static Route

It is the multicast static route that makes multicast forwarding path differ from unicast path. RPF check is always executed for forwarding multicast packets. The actual receiving port is the port expected to receive packets (the port is the next hop of unicast route reaching the sender). RPF check is reasonable if the topologies of unicast and multicast are the same. But in some cases, unicast path is expected to differ from that of multicast.

Configuring multicast static route allows for RPF check based on configuration, not the unicast routing table. Consequently, multicast packets are forwarded through tunnel. Unicast packets are not. Multicast static route is configured locally. It will not be advertised or forwarded.

In the global configuration mode, use the following command to configure multicast static route.

Command	Purpose
DES-7210 (config) # **ip mroute** *source-address mask* [**bgp** | **isis** | **ospf** | **static**] {*v4rpf-address* | *interface-type interface-number*} [*distance*]	Configure multicast static route and specify the routing protocol type. *distance*: In the range of 1 to 255

Note

To set the egress of the static multicast route not to the next hop IP address, the egress must be a point-to-point type interface.

38.3.1.5 Configuring the Flow Control of Multicast Steams on Layer 2

To enable flow control on an interface ,execute this command. More than one command, or a port that is allowed to forward can be configured for a multicast stream. Once enabled, the multicast stream can only be forwarded through these ports.

Command	Purpose
DES-7210 (config) # **ip multicast static** *source-address group-address interface-type interface-number*	Enable flow control on the interface. The static egress must be a layer 2 interface

This command controls only the forwarding of multicast streams on an interface, without direct influence on the multicast protocol's processing packets. However, as some features of some multicast protocol (for example, PIM-DM or PIM-SM) are driven by multicast streams, this may influence the activities of multicast protocols.

38.3.1.6 Monitoring and Maintenance of Multicast Routing

Execute the following command in the privileged configuration mode to show the IPv4 multicast forwarding table:

Command	Purpose
DES-7210 # **show ip mroute** [*group-address*] [*source-address*] [**dense**| **sparse**] [**summary** | **count**]}	Show the IPv4 multicast forwarding table.

Execute the following command in the privileged configuration mode to clear the IPv4 multicast forwarding table.

Command	Purpose
DES-7210 # **clear ip mroute** [*** |** *v4group-address* **|** *v4source-address*]	Delete the IPv4 multicast forwarding table.

Execute the following command in the privileged configuration mode to reset the IPv4 multicast forwarding table statistics.

Command	Purpose
DES-7210 # **clear ip mroute statistics** [*** |** *v4group-address* **|** *v4source-address*]	Reset the IPv4 multicast forwarding table statistics.

Execute the following command in the privileged configuration mode to show the RPF information of specific IPv4 source IP address.

Command	Purpose
DES-7210 # **show ip rpf** *v4source-address*	Show the RPF information of specific IPv4 source address.

Execute the following command in the privileged configuration mode to show the IPv4 multicast interface information.

Command	Purpose
DES-7210 # **show ip mvif** [*interface-type interface-number*]	Show the IPv4 multicast interface information.

Execute the following command in the privileged configuration mode to show the multicast operation.

Command	Purpose
DES-7210 # **debug nsm mcast all**	Show the multicast operation.

Execute the following command in the privileged configuration mode to show the communication between the IPv4 multicast and the routing protocol.

Command	Purpose
DES-7210 # **debug nsm mcast fib-msg**	Show the communication between the iPv4 multicast and the routing protocol.

Execute the following command in the privileged configuration mode to show the multicast operation on the interface.

Command	Purpose
DES-7210 # **debug nsm mcast vrf**	Show the multicast operation on the interface.

Execute the following command in the privileged configuration mode to show the multicast statistics.

Command	Purpose
DES-7210 # **debug nsm mcast stats**	Show the multicast statistics.

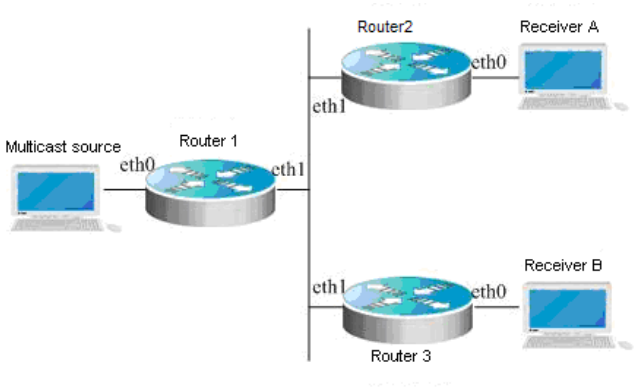
38.4 Multiple Routing Configuration Examples

38.4.1 PIM-DM Configuration Example

38.4.1.1 Configuration requirements

The network topology is shown in Figure 36-6. Device 1 and the multicast source locate in the same network, device 2 and receiver A locate in the same network, and device 3 and receiver B locate in the same network. Suppose the devices are connected with the host correctly and the IP addresses are configured.

Example of PIM-DM networking diagram



38.4.1.2 Device Configuration

Take the device 1 as an example to show how to configure PIM-DM. The steps of device 2 and 3 are similar with device 1.

Step 1: Enable multicast routing

```
DES-7210# configure terminal
DES-7210(config)# ip multicast-routing
```

Step 2: Enable PIM-DM on the interface eth0

```
DES-7210(config)# interface eth 0
DES-7210(config-if)# ip pim dense-mode
DES-7210(config-if)# exit
```

Step 3: Enable PIM-DM on the interface eth1 and return to the privileged user mode.

```
DES-7210(config)# interface eth 1
DES-7210(config-if)# ip pim dense-mode
DES-7210(config-if)# end
```

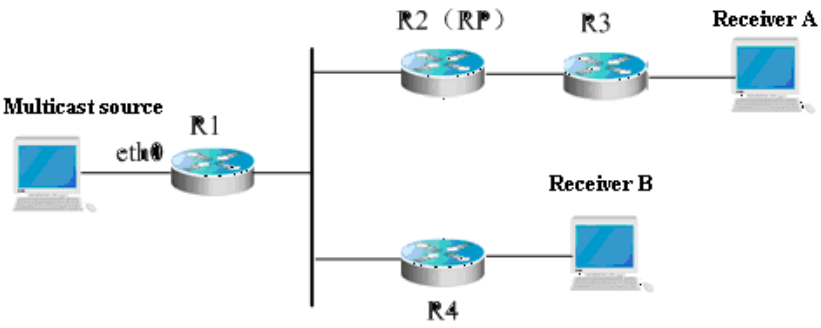
The configuration of device 2 and 3 is similar to device 1.

38.4.2 PIM-SM Configuration Example

38.4.2.1 Configuration requirements

The network topology is shown in Figure 36-7. Device 1 and the multicast source locate in the same network, device 2 and receiver A locate in the same network. Suppose the devices are connected with the host correctly; IP addresses and unicast routes are configured.

Example of PIM-SM networking diagram



38.4.2.2 Device Configuration

Take the device 1 as an example to show how to configure PIM-SM. The steps of device 2, 3 and 4 are similar with device 1.

Step 1: Enable multicast routing

```
DES-7210# configure terminal
DES-7210(config)# ip multicast-routing
```

Step 2: Enable PIM-SM on the interface eth0

```
DES-7210(config)# interface eth 0
DES-7210(config-if)# ip pim sparse-mode
DES-7210(config-if)# end
```

Step 3: Configure the candidate BSR and candidate C-RP.

Set R2's loopback1 to C-BSR and C-RP

```
DES-7210(config)# interface loopback 1
DES-7210(config-if)# ip address 100.1.1.1 255.255.255.0
DES-7210(config-if)# ip pim sparse-mode
DES-7210(config-if)# exit
DES-7210(config)# ip pim bsr-candidate loopback 1
DES-7210(config)# ip pim rp-candidate loopback 1
DES-7210(config-if)# end
```

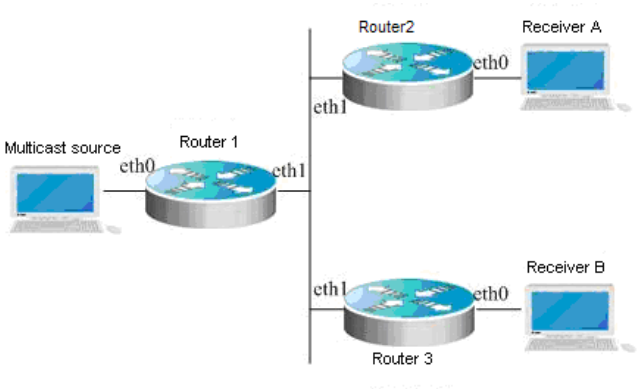
Note that once PIM-SM is enabled, IGMP is enabled on various interfaces automatically without manual configuration.

38.4.3 DVMRP Configuration Example

38.4.3.1 Configuration requirements

The network topology is shown in the following figure. Device 1 and the multicast source locate in the same network, device 2 and receiver A locate in the same network. Suppose the devices are connected with the host correctly; IP addresses and unicast routes are configured.

Example of DVMRP networking diagram



38.4.3.2 Device Configuration

Take the device 1 as an example to show how to configure DVMRP. The steps of device 2 and 3 are similar with device 1.

Step 1: Enable multicast routing

```
DES-7210# configure terminal
DES-7210(config)# ip multicast-routing
```

Step 2: Enable DVMRP on the interface eth0

```
DES-7210(config)# interface eth 0
DES-7210(config-if)# ip dvmrp enable
DES-7210(config-if)# exit
```

Step 3: Enable DVMRP on the interface eth1 and return to the privileged user mode.

```
DES-7210(config)# interface eth 1
DES-7210(config-if)# ip dvmrp enable
DES-7210(config-if)# end
```

The configuration of device 2 and 3 is similar to device 1.

Note

Once the DVMRP is enabled, IGMP is auto-enabled on every interface without manual configuration.

39 IGMP Configuration

39.1 IGMP Overview

IPv4 multicast refers to a network technology that forwards packets to more than one receiver through a multicast flow. Only the hosts joining the group can receive the packets from the specific multicast group. Multicast can save network bandwidth greatly for there is only single packet transmitting on any link of the network, no matter how many receivers are deployed.

Multicast uses Class-D network address specified by IANA. The highest bits of Class-D network address are 1110. So, the Class-D network address is in the range of 224.0.0.0 to 239.255.255.255. However, not all addresses in this range can be used by users. The addresses in the range 224.0.0.1 to 224.0.0.255 are reserved for protocols. For instance, 224.0.0.1 indicates all multicast host addresses and 224.0.0.2 indicates all multicast device addresses.

Any hosts, no matter whether they are multicast group member or not, can be the multicast source. However, only the multicast group member can receive the multicast frame. The multicast group member is able to dynamically join in or leave the group. The forwarding of multicast frame in the network is processed by the multicst device with multicast routing protocol enabled.

To enable IPv4 multicast, multicast hosts and devices must support IGMP. This protocol is used by the host to notify the multicast device of the multicast membership of the network they connect to determine how to forward multicast traffic. By using the information obtained from the IGMP, the device can maintain an interface and group-based multicast member list. The multicast member list is activated only when at least one host of an interface is a member of the group.

IGMPv1, IGMPv2 and IGMPv3 are supported at present. On the basis of IGMPv1, IGMPv2 has the leaving message so that the host can actively request to leave a multicast group. IGMP activities fall into two parts: host activity and device activity.

39.1.1 IGMPV1

There are only two types of messages defined in IGMP Version 1:

- Membership query
- Membership report

A host sends a report packet to join a group, and the router sends the query packet at periodical intervals to ensure that a group has at least one host. When a group contains no host, the router will delete that group.

39.1.2 IGMPV2

In Version 2, there are only four types of packets:

- Membership query
- Version 1 membership report
- Version 2 membership report
- Leave group

IGMPv2 is basically the same as IGMPv1, except that the leave mechanism of the host has been improved. For V2, the host can send a leave message to notify the device, which then sends a query to verify if there is a host in the multicast group. This makes joining and leaving a group more efficiently.

In the multicast network that runs IGMP, there is a dedicated query multicast device, which is responsible for sending IGMP query messages. This de querier is chosen through an election process. At the beginning, all the devices are queriers. When a device receives a query message, it compares the source IP address of the message. For IGMPv1, the device of the highest IP address is elected as the querier. However, for IGMPv2/v3, the one of the lowest IP address is selected as the querier. Moreover, for the IGMP query messages with different versions, the one sending the IGMP query message of the lowest version is elected as the querier.

If the querier fails, the querier is elected again. The non-querier devices maintain the interval timers of other queriers. Every time when a device receives a membership query packet, it resets the timer. If the timer expires, the device considers itself is the querier and starts to send query messages. The querier election starts again.

The querier must send the membership query request periodically to ensure that other devices in the network know that the querier still works. For this purpose, the querier maintains one query interval timer. When it sends the membership query message, this timer will be reset. When the interval timer times out, the querier sends another membership query.

When the device appears for the first time, that is, a new device is added, it sends a series of general query messages to see which multicast groups will be received on the hosts of which interfaces for rapid convergence. The number of common query packets sent is based on the start query count configured. The querying interval between the initial general query messages is defined through the startup query interval.

When a querier receives a leave packet, it must send a particular group membership query to see if the host is the last one leaving the group. Before the querier stops forwarding packets to the group, it sends a series of such packets, the number of which is equal to the last member query number. The querier sends multiple particular membership queries to ensure that there is no member in the group. Such a query is sent every other the seconds of the last-member query interval to separate the queries. When no response is received, the querier stops forwarding multicast packets to the group on the particular interface.

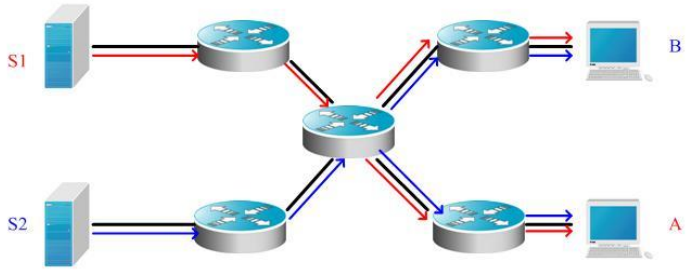
39.1.3 IGMPV3

In the applications of the IGMPV1 and V2, there are the following defects:

- Lack of efficient measures to control multicast sources
- Difficult to establish the multicast path due to unknown multicast source
- Difficult to find a unique multicast address. It is possible that multicast groups are using the same multicast address.

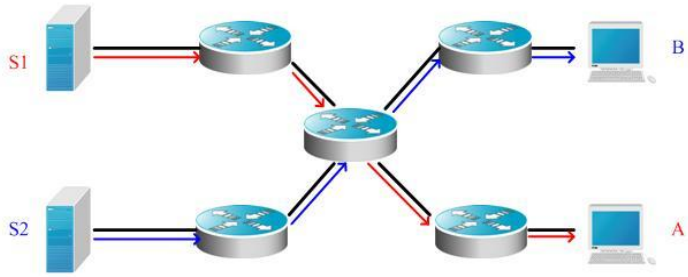
On the basis of IGMPV1/V2, IGMPV3 provides an additional source filtering multicast function. In IGMP V1/V2, the host determines to join a group and receive the multicast traffic to the group address from any source only based on the group address. On the other hand, the host running the IGMP V3 notifies this host the desired multicast group to join, and also the addresses of the multicast sources to receive. The host can indicate that it wants to receive multicast traffic from which sources through an inclusion list or an exclusion list. At the same time, another benefit of the IGMP v3 is that it saves bandwidth to avoid unnecessary, invalid multicast data traffics from occupying network bandwidth. It is particularly useful in the case where multiple multicast sources share one multicast address. The IGMPv1 and IGMPv2 can also implement “source address filter” in some sense, which, however, is performed on the end of receiving the multicast traffic. As shown in the following diagram, there are two multicast sources (S1 and S2), which send the data traffic of the same multicast address (G). The multicast flow of S1 and S2 will be sent to all hosts receiving flows from G. If host A only wants to receive multicast flows from S1, it filters flows by using the related client software.

Figure-5 Multicast route forwarding without filtering source



If the equipments in the network support IGMP v3, host A wants to receive the traffic from S1 only. It can send the IGMPv3 packet of join G include S1. If host B wants to receive the traffic from S2 only, it can send the IGMPv3 packet of join G include S2. Therefore, the traffics are forwarded as shown in the following diagram. This saves bandwidth.

Figure-6 Multicast route forwarding with filtering source



In contrast to Version 2, Version 3 defines the following two kinds of messages:

- Membership Query
- Version 3 Membership Report

There are three types of Membership Query:

- General Query: Used to query all the multicast members under the interface.
- Group-Specific Query: Used to query the members of the specified group under the interface.
- Group-and source-Specific Query: This type is the new one in the IGMPv3, which is used to query if any member under the interface needs to receive the multicast traffic of the particular group from the sources in the specified source list.

Different from the Membership Report in IGMP Version2, the Membership Report in the IGMP Version3 always has the destination address of 224.0.0.22. The Membership Report packets in IGMP Version3 include the information of multiple groups. It can carry with one or more group records, each record with group address and source address list. Below shows the types of group record:

IS_IN: Indicates INCLUDE filtering mode between the multicast group and the multicast source list, that is, only the multicast traffic from the specific multicast source list to the multicast group are received. A null multicast source list means leaving the multicast group, which is equivalent to the leave message in IGMPv2.

IS_EX: Indicates EXCLUDE filtering mode between the multicast group and the multicast source list, that is, only the multicast traffic from any multicast source except for the specific multicast source list to the multicast group are received.

TO_IN: Indicates that the filtering mode between the multicast group and the multicast source list changes from EXCLUDE to INCLUDE.

TO_EX: Indicates that the filtering mode between the multicast group and the multicast source list changes from INCLUDE to EXCLUDE.

ALLOW: Indicates receiving multicast traffic from additional multicast sources. For INCLUDE mode, it adds these multicast source to the multicast source list. For EXCLUDE mode, it removes these multicast sources from the multicast source list.

BLOCK: Indicates no longer receiving multicast traffic from some multicast sources. For INCLUDE mode, it removes these multicast source from the multicast source list. For EXCLUDE mode, it adds these multicast sources to the multicast source list.

For the sake of compatibility, IGMPv3 can identify IGMPv1/v2 packets.

39.2 IGMP Configuration Task List

IGMP configuration includes the following tasks. Only some configuration tasks are mandatory, others are optional. It should be noted that the following commands should be executed on the Layer 3 interface.

- Enable IGMP (mandatory)
- Configure IGMP version (mandatory)
- Configure query interval of last member (optional)
- Configure query count of last member (optional)
- Configure query interval of general member (optional)
- Configure the maximum response time (optional)
- Configure the timer interval of other queriers (optional)
- Configure access to multicast group (optional)
- Configure to leave the multicast group immediately (optional)
- Configure join-group (optional)
- Configure static-group (optional)
- Configure the limit of IGMP status (optional)
- Configure IGMP PROXY-Service (optional)
- Configure IGMP MROUTE-PROXY (optional)
- Enable IGMP SSM-MAP (optional)
- Configure IGMP SSM-MAP STATIC (optional)
- Clear the dynamic group member information from the response message in cache (optional)
- Clear all the information on the specific interface in cache (optional)
- Show members in the directly connected subnet (optional)
- Show the interface configuration (optional)
- Show IGMP SSM-MAP configuration (optional)
- Show IGMP debugging (optional)
- Turn on IGMP debugging (optional)

39.2.1 Configuring IGMP

39.2.1.1 Default IGMP Configuration

IGMP version	IGMPv2 is supported on all interfaces.
Query response time	10s
Query interval	125s

Access to multicast group	All multicast groups
Other querier timer	255s
Robustibility variables	2
Query interval of last member	1s
Query count of last member	2
IGMP status	Disabled

39.2.1.2 Enabling IGMP

Use the following command in the interface configuration mode to enable IGMP:

Command	Purpose
DES-7210 (config-if) # **ip pim** {**sparse-mode** | **dense-mode**}	Enable the multicast routing protocol and IGMP.
DES-7210 (config-if) # **no ip pim** {**sparse-mode** | **dense-mode**}	Disable the multicast routing protocol and IGMP.

Note

Enabling a multicast routing protocol and the multicast routing forwarding function on an interface will enable IGMP.

A device can run only one kind of multicast routing protocol.

39.2.1.3 Configuring IGMP Version

Use the following command in the interface configuration mode to configure the IGMP version.

Command	Purpose
DES-7210 (config-if) # **ip igmp version**{*1* | *2* | *3*}	Configure the IGMP version, version 2 by default.
DES-7210 (config-if) # **no ip igmp version**	Restore to the default value.

39.2.1.4 Configuring Query Interval of Last Member

After receiving the message of leaving the multicast group, the querier sends the specific membership query to verify whether there is any member in the group. If no report is received during the last member query interval period, the querier will regard the host that is leaving the group is the last member of that group, and then delete the information of the group. By default the period is 1 s.

Use the following commands in the interface configure mode to configure the query interval of last member:

Command	Function
DES-7210 (config-if) # **ip igmp last-member-query-interval** *interval*	Configure the query interval of the last member. *interval*: in the range 1 to 255 in 0.1s.
DES-7210 (config-if) # **no ip igmp last-member-query-interval** *interval*	Restore to the default value.

39.2.1.5 Configuring Query Count of Last Member

After receiving the message of leaving the multicast group, the querier device sends the specific membership query for several times to verify whether there is any member in the group. The query times should be larger than 1.

Use the following command in the interface configuration mode to configure the query count of last member:

Command	Function
DES-7210 (config-if) # **ip igmp last-member-query-count** *count*	Configure the query count of last member in the range of 2 to 7, 2 by default.
DES-7210 (config-if) # **no ip igmp last-member-query-count**	Restore to the default value.

39.2.1.6 Configuring Query Interval of General Member

The querier device sends the general member query message at intervals to all hosts to verify the current membership. The multicast IP address is 224.0.0.1, TTL is 1 and the default value is 125s.

Use the following command in the interface configuration mode to configure the query interval of general member:

Command	Function
DES-7210 (config-if) # **ip igmp query-interval** *seconds*	Configure the query interval of general member in the range of 1 to 18000 seconds, 125s by default.
DES-7210 (config-if) # **no ip igmp query-interval** *seconds*	Restore to the default value.

39.2.1.7 Configuring the Maximum Response Time

The membership query message sent by the querier device requires the maximum response time. Shorting this response time can make the device know the change of the members earlier, which will result in increase of the member reports diffusing in the network. The network administrator can consider a tradeoff between the two factors and then decide a proper value for the period, 10 seconds by default. Another consideration in configuring the response time is that it shall be shorter than the query interval.

Use the following commands in the interface configuration mode to configure the maximum response time:

Command	Function
DES-7210 (config-if) # **ip igmp query-max-response-time** *seconds*	Configure the maximum response time in the rnage1-25s.
DES-7210 (config-if) # **no ip igmp query-max-response-time** *seconds*	Restore to the default value.

39.2.1.8 Configuring the Timer of Other Querier

Once the timer times out, the querier considers that there is no other querier on the network. This is helpful for the election of querier. You can short this timer in the circumstance where the querier changes frequently to speed up response.

Use the following commands in the interface configuration mode to configure the timer of other querier:

Command	Function
DES-7210 (config-if) # **ip igmp query-timeout** *seconds*	Configure the timer of other querier in the range of 60 to 300 seconds, 255 seconds by default.
DES-7210 (config-if) # **no ip igmp query-timeout**	Restore to the default value.

39.2.1.9 Configuring Access to Multicast Groups

By default, the hosts on an interface can join any multicast group. You can restrain the multicast group range that the hosts join by configuring a standard IP ACL and applying it to the specific interface.

Use the following command in the interface configuration mode to configure access to multicast groups:

Command	Function
DES-7210 (config-if) # **config terminal**	Enter the global configuration mode.
DES-7210 (config) # **access-list** *access-list-num* **permit** *A.B.C.D A.B.C.D*	Define an ACL.
DES-7210 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210 (config-if) **# ip igmp access-group** *access-list-name*	Allow for access to the multicast groups in the ACL.
DES-7210 (config-if) # **no ip igmp access-group** *access-list-name*	Allow for access to all multicast groups.

39.2.1.10 Configuring to Leave the Multicast Group Immediately

In IGMPv2, you can execute this command to short the delay to leave a multicast group. A host leaves a multicast group as long as it sends a leave message without needing the querier to send

the specific multicast group query message. This command is available only when there is only one host on an interface.

Use the following command to configure to leave the multicast group immediately:

Command	Function
DES-7210 (config-if) # **config terminal**	Enter the global configuration mode.
DES-7210 (config) # **access-list** *access-list-num* **permit** *A.B.C.D A.B.C.D*	Define an ACL.
DES-7210 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config-if)# **ip igmp immediate-leave group-list** *access-list-name*	Leave the multicast groups in the ACL immediately.
DES-7210 (config-if) # **exit**	Enter the privileged configuration mode.

39.2.1.11 Configuring join-group

This command configures an interface of the switch with host behaviors and requires the interface to join a multicast group. In this way, the switch can learn the multicast group information.

Use this command in the interface configuration mode to add an interface into a multicast group:

Command	Function
DES-7210 (config-if) # **config terminal**	Enter the global configuration mode.
DES-7210 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config-if)# **ip igmp join-group** *group-address*	Configure the interface to join the multicast group.
DES-7210 (config-if) # **exit**	Enter the privileged configuration mode.

Use the **no ip igmp join-group** *group-address* command to leave the multicast group.

39.2.1.12 Configuring static-group

Use this command in the interface configuration mode to add an interface into a static group:

Command	Function
DES-7210 (config-if) # **config terminal**	Enter the global configuration mode.
DES-7210 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config-if)# **ip igmp static-group** *group-address*	Configure the interface to join the static group.
DES-7210 (config-if) # **exit**	Enter the privileged configuration mode.

Use the **no ip igmp static-group** *group-address* command to leave the static group.

39.2.1.13 Configuring the Limit of IGMP Group Members

This command configures the limit of IGMP group members globally. The messages of the members that exceed the limit will not be cached or forwarded.

You can configure this command on interfaces individually in interface mode or globally. The messages of the members that exceed the limit configured on an interface or globally will be ignored.

To configure the limit of IGMP group members, execute the following commands in the interface mode.

Command	Function
DES-7210(config) # **ip igmp limt** *number*	Configure the limit of IGMP members globally. The limit depends on specific products. By default, it is 65536.
DES-7210(config-if) **# ip igmp limit** *number*	Configure the limit of IGMP members on the interface. The limit depends on specific products. By default, it is 1024.

39.2.1.14 Configuring IGMP PROXY - SERVICE

This command enables service on all the downlink mroute-proxy interfaces. After you configure this command on an interface, the interface becomes the uplink interface of the corresponding mroute-proxy service. Moreover, it associates all its downlink interfaces and maintains their propagated multicast group information.

Up to 32 proxy services can be configured in this command and up to 255 downlink interfaces can be associated with per proxy-service. Upon the receipt of query message, the proxy-service interface responds accordingly based on the member information that it maintains from the interfaces with mroute-proxy configured. Consequently, configuring proxy-service on an interface equals to performing host behaviors rather than router behaviors on the interface.

To configure IGMP proxy-service, execute the following commands in the interface configuration mode.

Command	Function
DES-7210(config-if)# **ip igmp proxy-service**	Configure proxy-service on the interface.

39.2.1.15 Configuring IGMP MROUTE - PROXY

This command lets an interface to forward messages to its corresponding uplink interface.

The uplink interface can forward IGMP messages received from its members only when it is set to a proxy-service interface.

To configure IGMP mroute proxy, execute the following commands in the interface configuration mode.

Command	Function
DES-7210(config-if)# i**p igmp mroute-proxy** *interface name*	Configure mroute-proxy on the interface.

39.2.1.16 Enabling IGMP SSM-MAP

This command forcibly appends the relevant multicast source messages to the dynamically learned multicast group messages. It is usually used in conjunction with the **ip igmp ssm-map static** command.

To enable IGMP SSM-MAP, execute the following commands in the interface configuration mode.

Command	Function
DES-7210(config)# **ip igmp ssm-map enable**	Enable the SSM-MAP function.

39.2.1.17 Configuring IGMP SSM-MAP STATIC

This command is used in conjunction with the **ip igmp ssm-map enable** command. After this command is configured, the received messages whose version is earlier than version 3 will be mapped with the corresponding multicast source record.

To configure IGMP SSM-MAP STATIC, execute the following commands in the global configuration mode.

Command	Function
DES-7210(config)# **ip igmp ssm-map static** *11 192.168.2.2*	All groups matched ACL 11will be mapped with 192.168.2.2.

39.2.2 Monitoring and Maintaining IGMP State and the Group Member Information

39.2.2.1 Clearing the Dynamic Group Membership Message Obtained From the Response Message in IGMP Cache

To clear the dynamic group member messages obtained from the response message in IGMP cache, use the following command in the privileged configuration mode:

Command	Function
DES-7210# **clear ip igmp group**	Clear the dynamic group member messages obtained from the response message in the IGMP cache. Without any parameter, this command clears all the IGMP group messages.

39.2.2.2 Clearing All Information on Specified Interface in IGMP Cache

To clear all information on the specified interface in IGMP cache, use the following command in the privileged EXEC mode:

Command	Function
DES-7210# **clear ip igmp interface** *interface-type*	Clear all the information on the interface in IGMP cache.

39.2.2.3 Showing the Status of IGMP Group Members in the Directly-Connected Subnet

Use the following command in privileged EXEC mode to show the status of IGMP group members in the directly-connected subnet:

Command	Function
DES-7210# **show ip igmp groups**	Show the status of all IGMP group members in the directly-connected subnet.
DES-7210# **show ip igmp groups detail**	Show the details of all IGMP group members in the directly-connected subnet.
DES-7210# **show ip igmp groups** *A.B.C.D*	Show the status of the specified group member in the directly-connected subnet.
DES-7210# **show ip igmp groups** *A.B.C.D* **detail**	Show the details of the specified member in the directly-connected subnets.
DES-7210# **show ip igmp interface** *interface-type*	Show the information of the specified interface in the directly-connected subnets.
DES-7210# **show ip igmp groups** *interface-type* **detail**	Show the details of the specified interface in the directly-connected subnets.
DES-7210# **show ip igmp groups** *interface-type A.B.C.D*	Show the information of the specific group of the specified interface in the directly-connected subnets.
DES-7210# **show ip igmp groups** *interface-type A.B.C.D* **detail**	Show the details of the specific group of the specified interface in the directly-connected subnets.

39.2.2.4 Showing the Configuration Information of the IGMP interface

To show the configurations of the IGMP interface, run the following command in the privileged mode:

Command	Function
DES-7210# **show ip igmp interface** [*interface-type interface-number*]	Show the configuration information of the IGMP interface.
DES-7210# **show ip igmp interface**	Show the configuration information of all the IGMP interfaces.

39.2.2.5 Show the Configuration Information of IGMP SSM-MAP

To show the configuration information of IGMP SSM-MAP, use the following command in the privileged EXEC mode:

Command	Function
DES-7210# **show ip igmp ssm-map**	Show the Configuration Information of IGMP SSM-MAP.
DES-7210# **show ip igmp ssm-map** 233.3.3.3	Shown the mapping information from IGMP SSM-MAP to the multicast group 233.3.3.3.

39.2.2.6 Showing the Status of IGMP Debugging Switch

To show the status of the IGMP debugging switch, use the following command in the privileged mode:

Command	Function
DES-7210# **show debugging**	Show the status of the IGMP debugging switch.

39.2.2.7 Turning on IGMP Debugging Switch

To turn on IGMP debugging switch, use the following command in the privileged mode:

Command	Function
DES-7210# **debug ip igmp all**	Turn on all IGMP debugging switches
DES-7210# **debug ip igmp decode**	Turn on decode debugging switch
DES-7210# **debug ip igmp encode**	Turn on encode debugging switch
DES-7210# **debug ip igmp events**	Turn on event debugging switch
DES-7210# **debug ip igmp fsm**	Turn on final-state-machine debugging switch
DES-7210# **debug igmp tib**	Turn on tree debugging switch.
DES-7210# **debug ip igmp warnning**	Turn on warning debugging switch.

40 PIM-DM Configuration

40.1 PIM-DM Overview

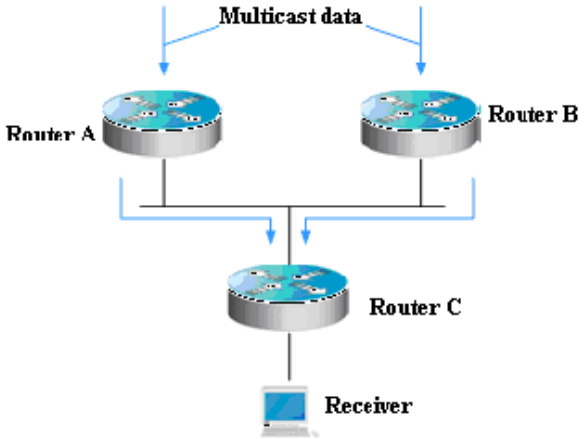
PIM-DM (Protocol Independent Multicast-Dense Mode), a multicast routing protocol in dense mode, is suitable for the environments of small network size and centralized multicast members. Since PIM-DM does not rely on any specific unicast routing protocol, it is called protocol independent multicast routing protocol. PIM-DM is defined in RFC 3973.

PIM-DM devices discover neighbors through Hello messages. After start, a PIM-DM device sends a Hello message to the PIM-DM-enabled interface periodically. The Hello message has a field called Hello Hold Time, which defines the period that a neighbor waits for the next message. If the neighbor has not received the next Hello message from the sender within this period, it announces the device's death.

PIM-DM sets up a multicast tree through flood and prune. Assume that when a multicast source begins to send a multicast packet, all the systems in the network need to receive this packet. As a result, this packet is forwarded to every system. The reverse path forwarding check is done for the packets received from the upstream interface. Those packets who fail to pass the check will be dropped. For the packets passing the check, the egress is calculated based on the (S, G) pair of the packets, or source address and group address. If the egress exists, an egress entry is set up fro the (S, G) pair and the multicast packet is forwarded through this egress. If the calculated egress is null, a prune message is sent to RPF, informing the upstream neighbor not to forward the multicast packets from the (S, G) pair to this egress. Upon receiving the prune message, the upstream interface marks the sending interface as pruned status, and set a pruned state timer. In this way, a multicast forwarding tree at the root of multicast source is set up.

PIM-DM utilizes the Assert mechanism to eliminate redundant routes.

Figure-7 Figure 4 PIM-DM's Assert mechanism



As shown in the above figure, the multicast data arrives at Router A and B at the same time, which forward the data to Router C. In this case, Router C receives two copies of the data. This is not allowed. So there must be a mechanism to select Router A or B to forward the multicast data to Router C. This is the Assert mechanism of PIM-DM.

PIM-DM uses the state refresh message to update network state. The device directly connecting to the multicast source sends the state refresh message to the downstream devices periodically to inform topology change. The devices receiving the message add their topology state to the state refresh message by modifying some fields, and then send to the downstream devices. When the refresh message arrives the leaf devices, the whole network state is updated.

PIM-DM utilizes the Graft mechanism to reestablish the connection with upstream devices. If the network topology of a downstream device in pruned state changes and needs to receive multicast data from a (S, G) pair, it sends the graft message to the upstream device. Upon receiving the graft message, the upstream device responds with a Graft-Ack message and forwards the multicast data to the downstream device again.

40.2 PIM-DM Configuration Task Lst

The PIM-DM configuration covers the following items. However, only the first and second one are mandatory, and others are optional.

- Enable Mulitcast Routing (required)
- Enable PIM-DM (required)
- Configure the interval of sending the Hello message (optional)
- Configure PIM-DM neighbor filtering (optional)
- Configure PIM-DM status refresh (optional)
- Configure the interval of sending PIM status refresh message (optional)
- Show PIM-DM status (optional)

40.2.1 Configuring PIM-DM

40.2.1.1 Enabling Multicast Routing

The multicast protocol can receive and process multicast packets and protocol packets only when the multicast routing forwarding function is enabled.

In the global configuration mode, execute the following command to enable the multicast routing forwarding function:

Command	Function
DES-7210 (config) # **ip multicast-routing**	Enable multicast routing forwarding.
DES-7210 (config) # **no ip multicast-routing**	Disable multicast routing forwarding.

40.2.1.2 Enabling PIM-DM

PIM-DM should be enabled on individual interface. Once PIM-DM is enabled on an interface of a device, the device can exchange PIM-DM control messages with other devices, maintain and update the multicast route table and forward multicast messages.

To configure PIM-DM on an interface, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip pim dense-mode**	Enable the PIM-DM protocol on the interface.
DES-7210(config-if)# **no ip pim dense-mode**	Disable the PIM-DM protocol on the interface.

The following example shows how to enable PIM-DM on GigabitEthernet 4/3.

```
DES-7210(config)# ip multicast-routing
DES-7210(config)# interface gigabitEthernet 4/3
DES-7210(config-if)# ip address 192.168.194.2 255.255.255.0
DES-7210(config-if)# ip pim dense-mode
```

Note

Enabling PIM-DM will take effect on an interface only when the multicast routing is enabled in the global configuration mode.

When this command is configured, if the “Failed to enable PIM-DM on <interface name>, resource temporarily unavailable, please try again” occurs, retry to configure this command.

When this command is configured, if the “PIM-DM Configure failed! VIF limit exceeded in NSM!!!” appears, It indicates current allowed interface configuration exceeds the upper limit of the multicast interfaces. Please remove some unnecessary PIM-SM or DVMRP interface.

It is not recommended to configure different IPv4 multicast routing protocols on different interfaces of a switch or router.

40.2.1.3 Setting the Interval of Sending the Hello Message

After the PIM-DM is enabled on an interface, the interface will send the Hello message to the interfaces of adjacent devices at an interval. You can modify the interval according to the real network circumstances.

To configure the interval of sending the Hello message, use the following command in the interface configuration mode:

Command	Function
DES-7210(config-if # **ip pimquery-interval** *interval-seconds*	Set the interval of sending the Hello message on the interface. *interval-seconds*: in the range 1 to 65535
DES-7210(config-if # **no ip pimquery-interval**	Restore the interval of sending the Hello message on the interface to the default value.

By default, the interval of sending the Hello message on the interface is 30s.

Note

When the interval of sending the Hello message is updated, the Hello hold time will be updated as 3.5 times of the Hello sending interval automatically. If the interval of sending Hello message multiplying 3.5 is larger than 65535, the Hello message hold time should be updated to 65535.

40.2.1.4 Configuring PIM Neighbor Filtering

Neighbor filtering function can be configured on the interface to enhance network security. With neighbor filtering enabled, the PIM-DM will not establish the neighborhood relationship with the neighbor or stop the currently established neighborhood relationship with the neighbor as long as a neighbor is denied by the access list.

To configure the PIM neighbor filtering function, run the following command in the interface configuration mode:

Command	Function
DES-7210(config-if #**ip pim neighbor-filter** *access-list*	Enable the PIM neighbor filtering function on the current interface.
DES-7210(config-if #**no ip pim neighbor-filter** *access-list*	Disable the PIM neighbor filtering function on the current interface.

The PIM neighbor filtering function is disabled by default on an interface.

Note

ip pim neighbor-filter command description:
When the associated ACL rule is set to permit, only the neighbor addresses in the ACL list can be considered to be the PIM neighbor of the current interface. When the associated ACL rule is set to deny, the neighbor addresses in the ACL list cannot be considered to be the PIM neighbor of the current interface.

40.2.1.5 Configuring PIM-DM Status Refresh

At administration mode, it is permitted to forward PIM-DM state refresh control message by default. For the first-hop router directly connected to the source, the interface configuration state refresh interval is the interval at which the state refresh packets are sent. In this case, it is only effective for the upstream interfaces. For subsequent routers, it is the interval at which the interfaces are allowed to receive and process the state refresh packets.

Command	Function
DES-7210(config-if #**no ip pim state-refresh disable**	Enable processing or forwarding PIM-DM status refresh messages.
DES-7210(config-if # **ip pim state-refresh disable**	Disable processing or forwarding PIM-DM status refresh message.

The PIM-DM status refresh function is enabled by default.

Caution

Disabling the status update messages may cause the re-convergence of the converged PIM-DM multicast forward tree, resulting in unnecessary bandwidth waste and routing table vibration. Therefore, it is better not to disable the status update function.

40.2.1.6 Configuring the Interval of Sending PIM Status Refresh Message

When the PIM-DM is enabled on the device, if some interface is directly connected with the multicast source, the status refresh messages will be sent to the downstream device on regular

basis, so as to refresh the statuses of the whole network. You can modify the interval of sending PIM status refresh message on an interface according to the real network circumstances.

To configure the interval of sending PIM status message on the interface, run the following command in the interface configuration mode:

Command	Function
DES-7210(config-if #**ip pim state-refresh origination-interval** *seconds*	Configure the interval of sending PIM status refresh message on the current interface as "seconds", where "seconds" is an integer within 1-100, in seconds.
DES-7210(config-if #**no ip pim state-refresh origination-interval**	Cancel the configuration of the PIM flood delay on the current interface.

By default, the interval of sending PIM status refresh message on the interface is 60 seconds.

Note

Only the devices directly connected to multicast source can periodically send the PIM status updated message to the downward interfaces. Thus, if the devices are not directly connected to the multicast source, the forwarding interval of PIM status update message configured on the downstream interface is invalid.

40.2.2 Monitoring and Maintaining PIM-DM

40.2.2.1 Viewing PIM-DM Status Information

Command	Function
DES-7210 # **show ip pim dense-mode interface** [*interface-type interface-number]* [**detail**]	Show the PIM-DM information on the interface.
DES-7210 # **show ip pim dense-mode neighbor** [*interface-type interface-number*]	Show the PIM-DM neighbor information.
DES-7210 # **show ip pim dense-mode nexthop**	Show the next hop information of PIM-DM.
DES-7210#**show ip pim dense-mode mroute** [*A.B.C.D A.B.C.D*] [**summary**]	Show the PIM-DM routing table.

For details on the use of the above command, see *PIM-DM Command References*.

Here are some examples of the commands:

show ip pim dense-mode interface detail command**:**

```
DES-7210# show ip pim dense-mode interface detail
FastEthernet 0/45 (vif-id: 3):
Address 10.10.10.10
Hello period 30 seconds, Next Hello in 15 seconds
Over-ride interval 2500 milli-seconds
Propagation-delay 500 milli-seconds
Neighbors:
10.10.10.1
VLAN 4 (vif-id: 2):
```

```
Address 50.50.50.50
Hello period 30 seconds, Next Hello in 2 seconds
Over-ride interval 2500 milli-seconds
Propagation-delay 500 milli-seconds
Neighbors:
50.50.50.1
```

In the example above, the IP address of FastEthernet 0/45 is 10.10.10.10, the Hello message sent interval 30 seconds, next Hello message to be sent in 15 seconds, and the neighbor address 10.10.10.1. The VLAN4 has similar information as FastEthernet 0/45.

show ip pim dense-mode neighbor command**:**

```
DES-7210# show ip pim dense-mode neighbor
Neighbor-Address Interface            Uptime/Expires    Ver
10.10.10.1      FastEthernet 0/45     00:19:29/00:01:21  v2
50.50.50.1      VLAN 4                00:22:09/00:01:39  v2
```

In the example above, the device has two neighbors, where neighbor 10.10.10.1 is connected with FastEthernet 0/45 and has survived for 19 minutes and 29 seconds, with neighbor survival period to expire in one minute and 21 seconds. Neighbor 50.50.50.1 is similar.

show ip pim dense-mode nexthop command:

```
DES-7210# show ip pim dense-mode nexthop
Destination  Nexthop   Nexthop      Nexthop       Metric Pref
              Num      Addr        Interface
1.1.1.111      1      50.50.50.1    VLAN 4          0     1
```

As shown in the above example, the next hop neighbor address to the multicast source 1.1.1.111 is 50.50.50.1 and the egress is VLAN4.

show ip pim dense-mode mroute command:

```
DES-7210# show ip pim dense-mode mroute
PIM-DM Multicast Routing Table
(1.1.1.111, 229.1.1.1)
MRT lifetime expires in 205 seconds
RPF Neighbor: 50.50.50.1, Nexthop: 50.50.50.1, VLAN 4
Upstream IF: VLAN 4
Upstream State: Pruned, PLT:200
Assert State: NoInfo
Downstream IF List:
FastEthernet 0/45:
Downstream State: NoInfo
Assert State: Loser, AT:170
```

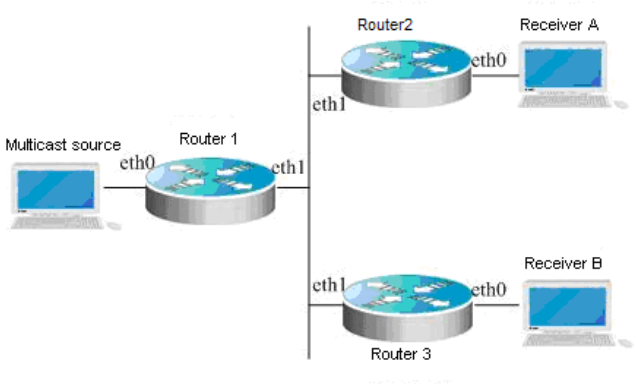
The above example shows two entries: 1.1.1.111 and 229.1.1.1, where MRG aging time is 205 seconds, RPF neighbor is 50.50.50.1, the next hop is 50.50.50.1, the egress to the next hop is VLAN 4. The upstream interface of these entries is VLAN 4 in Pruned status at present, indicating that there is no downstream forwarding egress. The downstream interface is FastEthernet 0/45 in Noinfor status. The Assert state of the interface is Loser. FastEthernet is not included in the forwarding egress.

40.3 PIM-DM Configuration Example

40.3.1 Configuration Requirements

The network topology is shown in Figure 36-6. Device 1 and the multicast source locate in the same network, device 2 and receiver A locate in the same network, and device 3 and receiver B locate in the same network. Suppose the devices are connected with the host correctly and the IP addresses are configured.

Example of PIM-DM networking diagram



40.3.2 Device Configuration

Take the device 1 as an example to show how to configure PIM-DM. The steps of device 2 and 3 are similar with device 1.

Step 1: Enable multicast routing

```
DES-7210# configure terminal
DES-7210(config)# ip multicast-routing
```

Step 2: Enable PIM-DM on the interface eth0

```
DES-7210(config)# interface eth 0
DES-7210(config-if)# ip pim dense-mode
DES-7210(config-if)# exit
```

Step 3: Enable PIM-DM on the interface eth1 and return to the privileged user mode.

```
DES-7210(config)# interface eth 1
DES-7210(config-if)# ip pim dense-mode
DES-7210(config-if)# end
```

The configuration of device 2 and 3 is similar to device 1.

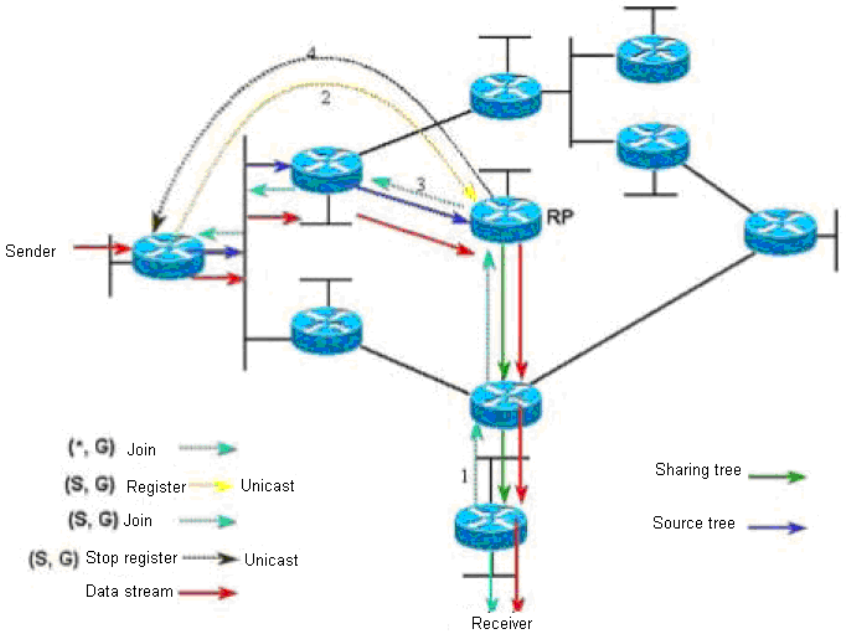
Note that once PIM-DM is enabled, IGMP is enabled on various interfaces automatically without manual configuration.

41 PIM-SM Configuration

41.1 PIM-SM Overview

The Protocol Independent Multicast Sparse Mode (PIM-SM) is a protocol independent multicast sparse mode. In a PIM-SM domain, the PIM-SM-enabled device sends the Hello message to discover adjacent PIM-SM devices and selects the designed router (DR) in a multi-access network. The DR is responsible for sending the join/prune message in the root node of the multicast distribution tree direction for the direct connection group member, or sending the data of the direct connection multicast source to the multicast distribution tree.

Join/Prune Mechanism of PIM-SM



The PIM-SM forwards multicast data packets by establishing a multicast distribution tree. The multicast distribution tree is divided into two types: Shared Tree that takes the RP of the group G as the root and Shortest Path Tree that takes the multicast source as the root. The PIM-SM establishes and maintains the multicast distribution tree with the explicit join/prune mechanism.

As shown in the above figure, when the DR receives a join request from the receiving terminal, it will multicast a (*.G) join message hop-by-hop to the RP of the group G to join the shared tree. When the source host sends multicast data to the group, the source data is encapsulated into the registration message and unicasted by the DR to the RP. Then the RP will forward the deencapsulated data packets to group members along the shared tree. The RP will send a (S, G) join message to the first hop on the source direction to join the shortest path tree of this source. In this way, the source's data packets are sent to the RP without encapsulation along its shortest path tree. When the first multicast data reaches along this tree, the RP will send the registration stop message to the DR of the source, notifying the DR of stopping registration. Consequently, the

source's multicast data packets are sent to the RP along its shortest path tree rather than being registered and encapsulated. Then the RP forwards the data packets to group members along the shared tree. When there is no need of multicast data packets, the DR multicasts a prune message to the RP of the group G hop-by-hop to prune the shared tree.

The PIM-SM also offers a mechanism of select the root point (RP). One or more Candidate-BSRs are configured in a PIM-SM domain. The PIM-SM selects a BSR by following a certain rule. There are also Candidate-RPs in a PIM-SM domain that unicast the packets including their IP addresses and available multicast groups to the BSR. The BSR will periodically generate a BSR message which includes a system candidate RP and the corresponding multicast group address. The BSR messages are sent hop-by-hop within the whole domain. The device receives and saves these BSR messages. If the DR receives a report on the member relationship of a multicast group from its directly connected host but has no route entries of the multicast group, the DR will use one Hash algorithm to map the multicast group address to a candidate RP that can serve this group. Then, the DR multicasts the Join/Prune message to the RP hop-by-hop. If the DR receives multicast data packets from its directly connected host but has no route entries of the multicast group, the DR will use one Hash algorithm to map the multicast group address to a candidate RP that can serve this group. Then the DR encapsulates multicast data packets into the registration message and unicasts it to the RP.

The main difference between the PIM-SM and the broadcast/prune model-based PIM-DM is that the PIM-SM is based on the explicit join model. In other words, the receiver sends the join message to the RP, while the router only forwards the packets of that multicast group on the outbound interface that has joined a multicast group. The PIM-SM uses the shared tree to forward multicast packets. Each group has a Rendezvous Point (RP). The multicast source sends the data to the RP along the shortest path, and then the RP sends the data to the receivers along the shortest path. This is similar to the CBT, but the PIM-SM does not use the concept of core. One of the major advantages of the PIM-SM is that it not only receives multicast messages through the shared tree but also provides a shared tree-to-SPT conversion mechanism. Such conversion reduces network delay and possible congestion on the RP, but it consumes enormous router resources. So it is suitable for the case where there are only a few multicast data sources and network groups.

The PIM-SM uses the shared tree and SPT to distribute multicast frames. At this time, it is assumed that other devices don't want to receive these multicasts unless otherwise stated definitely. When a host joins a group, the equipment connected to the host must notify the root (or the RP) by using the PIM join message. This join message is transferred one after another through the routers to create a shared tree structure. Therefore, the RP records the transfer path and also the registration message from the first hop router (DR) of the multicast source, and improves the shared tree upon these two messages. The branch/leaf messages are updated by periodically querying messages. With the shared tree, the multicast source first sends multicast packets to the RP, guaranteeing that all the receivers can receive them.

The PIMv2 BSR is a method of distributing the group-to-RP message to all devices without the need of setting the RP for them. The BSR uses the hop-by-hop broadcast BSR message to distribute the mapping message. At first, the BSR is selected among routers in the same process as selecting a root bridge based on priority level among layer 2 bridges. Each BSR checks the BSR messages and only forwards those having a priority higher than or equal to its own (higher IP address). The selected BSR sends its BSR message to the all-PIM-routers multicast group (224.0.0.13), where TTL is 1. After the adjacent PIMv2 router receives the message, it multicasts it while setting the TTL to 1. In this way, the BSR message is received by all devices hop-by-hop. Since the message contains the IP address of the BSR, the candidate BSR can know which router is the current RP based on this message. The candidate RPs send candidate RP advertisements to announce in which address ranges they can become an RP. The BSR stores them in its local candidate RP cache. The BSP notifies all PIM routers of its local candidate RPs periodically. These messages reach various devices hop-by-hop in the same way.

41.2 Configuration Preparation

Before configuring the PIM-SM, you shall enable an unicast routing protocol to find the routing automatically.

41.3 PIM-SM Configuration Task List

The PIM-SM configuration covers the following items. However, only the first one is mandatory, and others are optional.

- Enable PIM-SM (mandatory)
- Configure the interval of sending the Hello message (optional)
- Configure PIM-SM neighbor filtering (optional)
- Configure the priority of DR (optional)
- Configure BSR status (optional)
- Configure static RP (optional)
- Ignore the RP priority of RP-SET(optional)
- Configure candidate RP (optional)
- Check the reachability of registered packets (optional)
- Filter RP addresses (Optional)
- Configure the speed limit on sending registered packets (optional)
- Calculate the RP checksum in Cisco way
- Configure the source address of registered packet (optional)
- Configure the RP suppression time (optional)
- Configure the time of the KAT timer (optional)
- Configure the interval of sending join/prune message (optional)
- Switch the last-hop device from shared tree to the shortest path tree (optional)
- Configure the MIB in dense mode (optional)
- Configure the specific source multicast (optional)
- Show the status of PIM-SM (optional)
- Show the internal information of PIM-SM(optional)

41.3.1 Configuring PIM-DM

41.3.1.1 Enabling PIM-SM

The PIM-SM must be enabled on every port. Only after the PIM-SM is enabled on its ports can the device exchange PIM-SM control messages with other devices, maintain and update multicast routing table, and forward multicast packets.

To enable the PIM-SM on the interface, execute the following command in the interface mode:

Command	Function
DES-7210(config-if)# **ip pim sparse-mode**	Enable the PIM-SM protocol on the interface.
DES-7210(config-if)# **no ip pim sparse-mode**	Disable the PIM-SM protocol on the interface.

Note

Enabling the PIM-SM on the interface takes effect only when the multicast routing is enabled in the global configuration mode.

When the system prompts "Failed to enable PIM-SM on <Interface Name>, resource temporarily unavailable, please try again", re-execute this command.

When the system prompts "PIM-SM Configure failed! VIF limit exceeded in NSM!!!", it indicates that the configured interfaces exceed the upper limit of the multicast interfaces. In this case, delete the unnecessary PIM-SM interfaces.

It is not recommended to configure different IPv4 multicast protocols on different interfaces of a switch/router.

41.3.1.2 Configuring the Interval of Sending the Hello Message

When the PIM-SM is enabled on the interface, the device periodically sends Hello messages to the interfaces of neighbors. You can set the interval of sending Hello messages according to real network environment.

To configure the interval of sending the Hello message, execute following commands in the interface mode:

Command	Function
DES-7210(config-if)# **ip pim query-interval** *interval-seconds*	Set the interval of sending the Hello message. *interval-seconds*: in the range of 1 to 65535 seconds
DES-7210(config-if)# **no ip pim query-interval**	Restore the interval of sending the Hello message to the default value.

The interval of sending the Hello message on the interface is 30 second by default.

Note

When the interval of sending Hello message is changed, the hold time of Hello message also changes by the following rule. The hold time becomes 3.5 times of the interval of sending Hello message. If the interval multiplying 3.5 is larger than 65535, the hold time is set to 65535.

41.3.1.3 Configuring PIM-SM Neighbor Filtering

You can filter neighbors on an interface to enhance network security. With this function enabled, when a neighbor is denied by an ACL, the PIM-SM will not establish the neighborhood relationship with that neighbor or remove the currently established neighborhood relationship with that neighbor.

To configure the PIM neighbor filtering function, run the following command in the interface mode:

Command	Function
DES-7210(config-if)# **ip pim neighbor-filter** *access-list*	Enable the PIM neighbor filtering function on the interface.
DES-7210(config-if)# **no ip pim neighbor-filter** *access-list*	Disable the PIM neighbor filtering function on the interface.

The PIM neighbor filtering function is disabled by default on an interface.

Note

Description of the **ip pim neighbor-filter** commands:

A device can become the PIM-SM neighbor of the interface only when its IP address matches an ACL. Otherwise, it will not become the neighbor of the interface.

41.3.1.4 Configuring the Priority of DR

This command is used to configure the priority of the designated router (DR), higher weight means higher priority.

To configure the priority of DR, run the following commands in the interface mode:

Command	Function
DES-7210(config-if)# **ip pim dr-priority** *priority-value*	Configure the priority in the range of 0 to 4294967294.
DES-7210(config-if)# **no ip pim dr-priority** *priority*	Restore to the default value-1.

41.3.1.5 Configuring Static RP

In a small network, you can configure static RP to use PIM-SM. This requires all the devices in the PIM-SM domain have the same static RP configuration and ensure no ambiguity of the PIM-SM multicast routes.

To configure static RP, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip pim rp-address** *rp-address* [*access-list*]	Configure static RP on the local device.
DES-7210(config)# **no ip pim rp-address** *rp-address* [*access-list*]	Remove the static RP configuration.

Caution

Attention should be attained to following points when using this command:

If both the BSR and static RP configurations take effect simultaneously, the static RP takes precedence.

The static RP address can be configured for multiple multicast groups (by ACL) or all multicast groups (not by ACL). However, a static RP address cannot be configured for several times.

If more than one static RP are configured for a multicast group, the one with the highest IP address takes effect.

Only the permitted addresses defined in the ACL are invalid multicast groups. By default, 0.0.0.0/0 refers to filter all multicast groups (224/4).

After configuration, the static RP source address is inserted into the tree of group-based static RP group. Each static multicast group maintains the link table structure of a static RP group. The link tables are ordered in descending sequence by IP addresses. When a RP is selected for a group, the first element, namely, the RP with the highest IP address is firstly selected.

Deleting a static RP address deletes the address from all groups that has this address, and one address is selected from the existing tree structure as the RP address.

41.3.1.6 Configuring the Device as the Candidate BSR

This command configures a device to be a candidate BSR to generate the globally-unique BSR in the PIM-SM domain, which will collect and distribute RPs in the domain so as to ensure the uniqueness of RP mapping in the domain.

To configure the device as the candidate BSR, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length*] [*priority-value*]	Configure the device as the candidate BSR to learn and contest the global BSR role through BSM messages. *hash-mask-length*: in the range 0 to 32, 10 by default *priority-value*: in the range 0 to 255, 64 by default
DES-7210(config)# **no ip pim bsr-candidate** *interface-type interface-number*	Remove the configuration.

41.3.1.7 Ignoring the RP Priority in RP-SET

When you compare two RPs to select one for a multicast IP address, execute this command to ignore the RP priority. Otherwise, the RP priority would be taken into account during comparison.

To ignore the RP priority, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip pim ignore-rp-set-priority**	Ignore the RP priority in the RP-Set.
DES-7210(config)# **no ip pim ignore-rp-set-priority**	Take into account the RP priority in the RP-Set.

41.3.1.8 Configuring Candidate RP

Candidate RP advertisement is sent to the BSR at intervals and then propagated to all the PIM-SM devices in the domain, and thus ensuring the uniqueness of RP mapping.

To configure the candidate RP, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip pim rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *access-list*]	Configure the device as the candidate RP. *priority-value*: in the range of 0 to 255, 192 by default *interval-seconds*: in the range 1 to 16383, 60s by default *access-list*: All multicast groups are permitted, that is 224/4
DES-7210(config)# **no ip pim rp-candidate** *interface-type interface-number*	Remove the candidate RP configuration.

Note

You can use the ACL to specify a port as the candidate RP of a particular group. It should be noted that the group calculation is based on the permit ACE only, not the deny ACE.

Caution

The source IP address of ACE is used as the specific group range for matching.

41.3.1.9 Checking the Reachability for RPs

This command detects whether the RPs sent from DR can reach the destination device.

To check the reachability of RPs, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip pim register-rp-reachability**	Check the reachability of RPs.
DES-7210(config)# **no ip pim register-rp-reachability**	Disable this function.

41.3.1.10 Filtering the Addresses of Register Packets

Execute the **ip pim accept-register list** *access list* command to filter the pair of source IP address and multicast group IP address of reached register packets. Otherwise, every reached register packet is permitted.

To filter the addresses of register packets, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip pim accept-register list** *access-list*	Filter the pair of source IP address and multicast group IP address of register packets.
DES-7210(config)# **no pim accept-register**	Remove the configuration.

41.3.1.11 Configuring the Speed Limit on Sending RPs

This command configures the speed at which the DR sends registration packets in (S, G). No speed limit is configured by default.

To configure the speed limit on sending RPs, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip pim register-rate-limit** *<1-65535>*	Set the maximum number of RP packets sent per second in the range of 1-65535.
DES-7210(config)# **no ip pim rp-candidate**	Remove the configuration.

41.3.1.12 Calculating the Checksum of Register Packets in Cisco 's Way

Execute the **ip pim cisco-register-checksum** command to calculate the checksum of register packets in Cisco's way. Otherwise, the checksum of register packets is calculated in default way specified by the protocol.

To calculate the checksum of register packets in Cisco's way, execute the following command in the global configuration mode.

Command	Function
DES-7210(config)# **ip pim cisco-register-checksum** [**group-list** *access-list*]	Calculate the checksum of register packets in Cisco's way. **group-list** *access-list*: Apply this configuration to all multicast addresses by default.
DES-7210(config)# **no ip pim cisco-register-checksum** [**group-list** *access-list*]	Remove the configuration.

41.3.1.13 Configuring the Source IP Address of RPs

This command sets the source IP address of RPs sent from DR. The **no** form of this command sets the RPF interface address as the default source address for the response when the PR sent from DR to the source host. The configured address must be reachable for the response to the correct Register-Stop information in the RP. The address is generally a loop address of the interface. It also can be other physical address. Such address must be advertised by unicast route on the DR port.

To configure the source IP address of RPs, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **ip pim register-source** { *local_address* | *Interface-type interface-number*}	Configure the source IP address used in RPs.
DES-7210(config)# **no ip pim register-source**	Set the RPF interface address as the source IP address of RPs.

41.3.1.14 Configuring the RP Suppression Time

This command configures the RP suppression time. It will modify the RP suppression time defined on the DR. If the **ip pim rp-register-kat** is not configured, defining the RP suppression time in the RP will change RP keepalive period.

To configure the RP suppression time, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config # **ip pim register-suppression** *seconds*	Configure the RP suppression time.
DES-7210(config # **no ip pim register-suppression**	Set the suppression time to 60 seconds.

41.3.1.15 Configuring KAT Timer

The KAT timer is used for monitoring PIM RP.

To configure KAT timer, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config # **ip pim rp-register-kat** *seconds*	Configure KAT timer. *seconds*: in the range of 1 to 65535.
DES-7210(config # **no ip pim rp-register-kat**	Use the default KAT value

41.3.1.16 Configuring the Interval of Sending the Join/Prune Message

By default, the Join/Prune message is sent at the interval of 60s by default. Execute this command to modify this interval.

To modify the interval of sending the Join/Prune message, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config # **ip pim jp-timer** *interval-seconds*	Set the interval of sending the Join/Prune message, in the range of 1 to 65535 seconds.
DES-7210(config # **no ip pim jp-timer** *interval-seconds*	Restore the setting to the default value, or 60s.

41.3.1.17 Allowing the Last Hop Device to Switch from the Shared Tree to the Shortest Path Tree

The last-hop device is allowed to switch from the shared tree to the shortest path tree.

When the sending speed of a source is higher than equal to the transmission speed, a PIM join message is triggered and a source tree is constructed. If the final key word is defined, all the sources in this group use the shared tree. If the transmission speed is lower than the threshold, the leaf device re-diverts to the shared tree and sends a prune packet to the source.

To allow the last hop device to switch from the shared tree to the shortest path tree, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config # **ip pim spt-threshold**	Allow the last-hop device to switch from the shared tree to the shortest path tree.
DES-7210(config # **no ip pim spt-threshold**	Disable this function.

41.3.1.18 Using the MIB of PIM-DM

Execute this command to use the MIB of PIM-DM. Otherwise, the MIB of PIM-SM will be used.

To use the MIB of PIM-DM, execute the following command in the global configuration mode:

Command	Function
DES-7210(config # **ip pim mib dense-mode**	Use the MIB of PIM-DM.
DES-7210(config # **no ip pim mib dense-mode**	Use the MIB of PIM-SM.

41.3.1.19 Configuring the Particular Multicast Source

Configuring a particular multicast source enables you directly receive multicast data packets from the source without following the RP tree. To configure a particular source multicast, run the following command.

Command	Function
DES-7210(config # **ip pim ssm {default |range** access-list]}	Configuring a particular multicast source.
DES-7210(config # **no ip pim ssm**	Remove the configuration.

41.3.2 Monitoring and Maintaining PIM-SM

41.3.2.1 Showing the Status of PIM-SM

Command	Function
DES-7210 # **show debugging**	Show the status of the debugging switch
DES-7210 # **show ip pim interface** [*interface-type interface-number*] [**detail**]	Show the PIM-SM information of the interface.
DES-7210 # **show ip pim neighbor** [*interface-type interface-number*]	Show the PIM neighbor information.
DES-7210 # **show ip sparse-mode mroute**	Show the multicast routing table information of PIM-SM
DES-7210 # **show ip pim sparse-mode bsr-router**	Use this command to show the detailed information of BSR.
DES-7210 # **show ip pim sparse-mode rp-hash** *group-address*	Use this command to show the RP information selected.
DES-7210 # **show ip pim sparse-mode rp mapping**	Show the group-RP mapping information and RP settings
DES-7210 # **show ip sparse-mode nexthop**	Show the next hop of PIM-SM from NSM.
DES-7210 # **show memory pim sparse-mode**	Show the memory statistics information of PIM-SM background program

41.3.2.2 Clearing the PIM-SM Information

The following commands are available to clear the PIM-SM information:

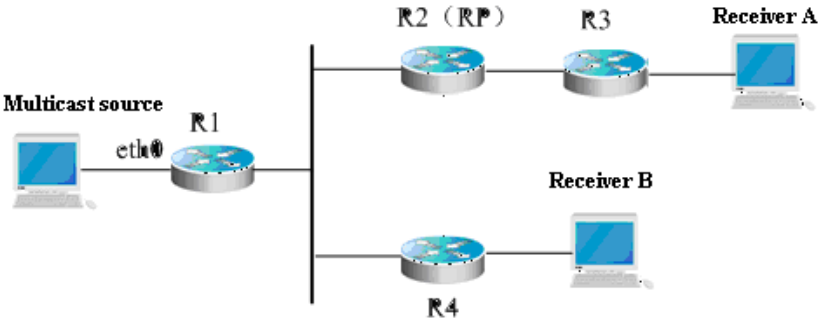
Command	Function
DES-7210# **clear ip mroute** {*** |** *group_address* [*source_address*] }	Clear multicast route entries.
DES-7210# **clear ip mroute statistics** {*** |** *group_address* [*source_address*] }	Clear the statistics of multicast route entries.
DES-7210 #**clear ip pim sparse-mode bsr rp-set ***	Clear RP-SET.

41.4 PIM-SM Configuration Example

41.4.1 Configuration Requirements

The network topology is shown in Figure 36-7. Device 1 and the multicast source locate in the same network, device 2 and receiver A locate in the same network. Suppose the devices are connected with the host correctly; IP addresses and unicast routes are configured.

Example of PIM-SM networking diagram



41.4.2 Device Configuration

Take the device 1 as an example to show how to configure PIM-SM. The steps of device 2, 3 and 4 are similar with device 1.

Step 1: Enable multicast routing

```
DES-7210# configure terminal
DES-7210(config)# ip multicast-routing
```

Step 2: Enable PIM-SM on the interface eth0

```
DES-7210(config)# interface eth 0
DES-7210(config-if)# ip pim sparse-mode
DES-7210(config-if)# end
```

Step 3: Configure the candidate BSR and candidate C-RP.

Set R2’s loopback1 to C-BSR and C-RP

```
DES-7210(config)# interface loopback 1
DES-7210(config-if)# ip address 100.1.1.1 255.255.255.0
DES-7210(config-if)# ip pim sparse-mode
DES-7210(config-if)# exit
DES-7210(config)# ip pim bsr-candidate loopback 1
DES-7210(config)# ip pim rp-candidate loopback 1
DES-7210(config-if)# end
```

Note that once PIM-SM is enabled, IGMP is enabled on various interfaces automatically without manual configuration.

42 MPLS Configuration

42.1 MPLS Overview

MPLS is the abbreviation of Multiprotocol Label Switching. Multiprotocol means that MPLS supports multiple network layer protocols, such as IP, IPv6 and IPX, and is compatible with multiple link layer technologies including ATM, frame relay, Ethernet and PPP. Label switching means that labels are attached to packets for forwarding. MPLS uses the connectionless-oriented control plane and connection-oriented data plane so that the connectionless-oriented IP network is added with the connection-oriented attribute. At the beginning, the MPLS technology is designed to improve the forwarding speed of the routers. However, as the hardware technology and network processor develop, this advantage is no longer prominent. Despite this, the inherent advantage of MPLS that integrates L2 switching and L3 routing is unmatched by other technologies in solving the important problems of the IP networks such as Virtual Private Network (VPN) and Traffic Engineering (TE). In solving enterprise interconnection and providing various services, the MPLS VPN is increasingly regarded as an important means by operators for providing value-added services. On the other hand, the MPLS TE technology also becomes a major tool for managing network traffic, reducing congestion, and ensuring the QoS of the IP network. Therefore, the MPLS technology attracts more and more attention and the application of the MPLS is gradually shifting to MPLS VPN and TE.

42.1.1 Basic Concepts

- **MPLS node**

As a node that runs MPLS, the MPLS node can identify the signaling protocols (control protocol) of MPLS and can run one or multiple L3 routing protocols (including static routing) and forward packets according to labels. Usually, a MPLS node also has the ability to forward the original L3 packet (for example, IP packet).

- **Forwarding Equivalence Class**

It is a group of data packets that are processed in any equivalent way, for example, the data packets with the same destination address prefix. The FEC can be classified in different ways depending on the specific applications. In the IP unicast routing application, the FEC can be classified according to the address prefix, that is, one route corresponds with one FEC. The packets belonging to the same FEC are processed in the same way in the MPLS network.

- **LSR (Label Switching Router)**

As the core switching of the MPLS network, the LSR provides label switching and label distribution. As described in the system document RFC3031 of MPLS, the LSR is also a MPLS node with the ability to forward original L3 packets (for example, IP packet or IPv6 packet). For the application of MPLS on IP, this means that the LSR also has the ability to forward IP packets.

- **LER (Label Switching Edge Router)**

On the edge of the MPLS network, the traffic entering the MPLS network is divided by the LER into different FECs with appropriate labels requested for them; the traffic leaving the MPLS network is

restored by the LER pop-up label into the original packets. Therefore, the LER provides the functions of traffic classification, label mapping and label removal.

- **LSP (Label Switched Path)**

A FEC traffic is assigned with specific labels at different nodes. Forwarding is enabled by switching the labels on the nodes. The path of the data traffic is known as LSP, which is a set of LSRs. The LSP can be seen as a tunnel that passes through the MPLS core network.

- **NHLFE (Next Hop Label Forwarding Entry)**

The NHLFE table is used to store the next-hop information for forwarding MPLS packets. Currently, the NHLFE table includes the following contents:

- Next hop of the data packets
- Link layer encapsulation used to forward the data packets
- Code mode used to forward the packet label stack
- Operation with the data packet label stack

  a) Using new labels to replace the labels on the top of the packet label stack
  b) Popping up the labels of the stack top
  c) Using a new label to replace the label on the top of the packet label stack and inject one or multiple new labels

- **ILM (Incoming Label Map)**

This table maps every incoming label to a series of NHLFEs (multiple NHLFEs show that there are multiple paths). The ILM is used to forward the labeled MPLS packets received by the LSR.

- **FTN (FEC-to-NHLFE)**

Unlink ILM, the FTN maps every FEC to a series of NHLFEs (multiple NHLFE show that there are multiple paths). The FTN is used to forward the unlabelled packets received by the LER by encapsulating labels to the packets before forwarding.

42.1.2 Label

A label is a short ID with fixed length and locally valid. It is locally valid in that the label is only transferred between two adjacent LSRs, thus, it's only valid between these two LSRs. The label is used to identify a FEC. When a packet reaches the ingress of the MPLS network, it is divided into different FECs according to the appropriate rule, and the label is encapsulated into the packet according to the FEC of the packet. The packet is forwarded according to the label in the MPLS network.

- **Structure of the label**

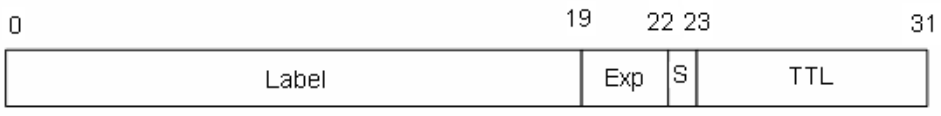


Figure 1 MPLS label coding structure

As shown in the above figure, the label consists of four domains as below:

- **Label domain**

Label value, with a length of 20 bits, is the index value of the label forwarding table. IETF defines 0 ~ 15 as reserved labels, and pre-defines the following meanings of labels:

Reserved label value	Meanings

0	IPv4 Explicit NULL Label, which can only appear at the bottom of the label stack. When a packet with this label is received, the label stack must be popped up and the packet should be forwarded according to the IPv4 header of the packet.
1	Router Alert Label, which should not occur at the bottom of the label stack. When a packet carrying this label is received, the packet must be sent to the local software module for processing, and the packet should be forwarded the label below this label. However, before the packet is forwarded, this label must be pressed into the label stack again. This option is similar to the “Router Alert Option” in the IP packet. Through this option, the LSR of every hop can be required to check this MPLS packet.
2	IPv6 Explicit NULL Label, which can only appear at the bottom of the label stack. When a packet with this label is received, the label stack must be popped up and the packet should be forwarded according to the IPv6 header of the packet.
3	Implicit NULL label, which can be distributed by the label distribution protocol, but will never appear in the label stack of the MPLS packets for transmission. When the LSR exchanges MPLS packets, if the label to be replaced on the stack top is 3, the label on the stack top will pop up without replacement. This label will be used in the “pop-up at the last but one hop” function.
4 ~ 15	Reserved by IETF for future use.

- **Exp domain**

Exp domain is of 3 bits and stores QoS information of MPLS.

- **S tag**

As the tag of the stack bottom, it has a length of one bit. When there are multiple labels, the S bit of the label at the stack bottom is set to “1”, while that of other labels are set to “0”. When there is only one label, the S bit is directly set to “1”.

- **TTL**

As the alive time, it has a length of 8 bits, similar to the TTL in the IP packet header. This value can be the TTL domain (or HopLimit of IPv6) of the IP packet header the first time when the IP packet is added with a label. At every label exchange, the TTL value of the outer layer (stack top) label is reduced by “1”. When MPLS runs on the ATM link, the label code mode differs in that it does not have the TTL domain. The RFC3032 has defined a method to handle this situation.

- **Label stack**

A MPLS packet has more than one label called label stack. The on near the header of the link layer is the top of the label stack, and the one near the IP header is the bottom of the label stack. LSR executes label switching based on the top label of the label stack. Each label is of 32 bytes in a whole. With the label stack, MPLS supports layered network architecture and LSP tunnels.

- **Label operation**

MPLS nodes perform the following operations to labels:

  - PUSH

Insert a label between the header of the link layer and the header of the network layer on the ingress LER, or insert a new label on the top of the label stack of MPLS packet on middle LSR.

- POP

Remove all the labels in the packets at the egress LER and restore to IP Packets, or remove the label on the top of the label stack .

- SWAP (Switching Label)

Replace the label on the top of the label stack according to the label forwarding table (ILM) during forwarding.

42.1.3 Label Distribution Protocol

As a new network system, MPLS also has its own signaling protocol or “routing protocol”. A fundamental concept in the MPLS system is that two LSRs agree on the label used for transmitting the traffic between them. The agreement is achieved through a series of processes, known as the Label Distribution Protocol (LDP). Through the LDP, one LSR notifies another LSR of its label binding. The MPLS system structure does not assume a single LDP. Some use the independent distribution protocol, for example, the LDP defined in the RFC3036 of IETF; some support label distribution by expanding the existing protocols through piggybacking, with typical examples like MP-BGP, OSPF, and RSVP. Different LDPs can be selected in different applications according o MPLS.

42.1.4 MPLS Network

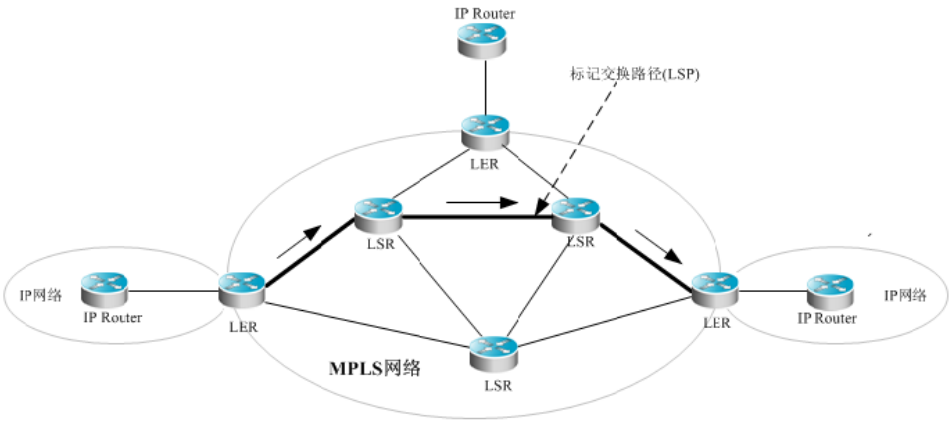


Figure 2

The MPLS network includes two basic elements: LSR and LER. The LSR is in the core of the MPLS network, running the LDP of MPLS to forward labeled packets. The LER is responsible for classifying the IP packets entering the MPLS network into FEC and adding labels to them and encapsulating them into MPLS packets for forwarding; removing the labels from the packets leaving MPLS network to restore them into the IP packets and looking up the appropriate forwarding table to forward them. In the MPLS network, the labeled packets will be forwarded along the LSP established by the LDP.

The architecture of the MPLS consists of the forwarding unit (data plane) and control unit (control plane). The forwarding unit forwards the packets by looking up the label forwarding library according to the label carried by the packet; the control unit is responsible for creating and maintaining the label forwarding information library between the connected MPLS equipment nodes. Every MPLS node must run one or multiple routing protocols (including the static route) to exchange the route information between the MPLS nodes of the MPLS network. In this case, each MPLS node is actually an IP router from the perspective of the control plane. Similar to the traditional IP routers, the routing table is also created and maintained by the unicast routing

protocol (including static route) on the MPLS node. The difference is that the traditional router uses this routing table to create the forwarding table; while for the MPLS node, this routing table can be used to exchange the label binding information between each destination subnet and the adjacent MPLS node. The protocol responsible for the label binding information exchange is referred to as the LDP (Label Distribution Protocol).

42.1.5 MPLS Forwarding Behavior

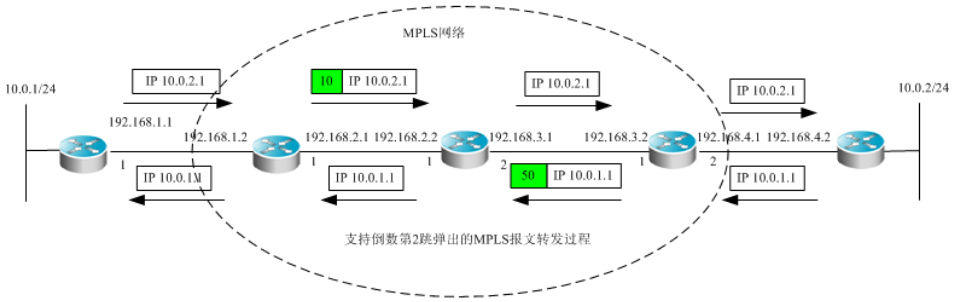


Figure 3

The MPLS forwarding process is as below:

1. All LSRs (including LER) start the traditional routing protocols (OSPF, IS-IS) to create the IP routing table in the LSR and LER.
2. The LDP creates the LSP according to the IP routing table.
3. The Ingress LER receives the IP packets, analyzes the IP header and corresponds to it with a FEC, before it adds the appropriate FEC label to the IP packet, and then sends the labeled packet to the next-hop LSR along the LSP of the label.
4. The next-hop LSR receives the label packet and looks up for the LSP according to the label at the stack top, replaces the label and then sends the packet to the next-hop LSR of the LSP.
5. The LSR on the way acts in the same way as step 4).
6. The last but one LSR receives the labeled packets and looks up the label forwarding table. If it finds that the appropriate egress label is an Implicit Null Label 3, it will pop the label and sends the original IP packet to the last-hop LSR. If the label is an Explicit Null Label, it pops the label and selects a route from the IP forwarding table according to the IP header and sends the original packet.
7. If the last but one hop pops the label, an original IP packet will be received at the last hop egress LER, and the next-hop router will be found in the IP routing table.

42.1.6 Establishment and Loop Detection of LSP

The virtual connection of MPLS refers to LSP. The data traffic of a FEC is assigned with labels at different MPLS nodes, and data forwarding is performed according to these labels. The data traffic passes the LSP, which includes a series of LSR. The data traffic of the same FEC passes the same LSP.

42.1.6.1 LSP Establishment Process

The establishment of the LSP is the process to perform the FEC and label binding, and notify the binding to the adjacent LSR. This process is performed by the LDP. The RFC3036 stipulates the protocol specification of the LDP, the interaction process between the LSR and the information format.

The LDP discovers the adjacent LSR by sending Hello messages at periodical intervals. The LDP Hello messages use the UDP encapsulation, and the destination port uses the known port 646. Its destination address is the multicast address (IP of 224.0.0.2) of all routers in the subnet. After the neighbor LSR is discovered, it triggers the establishment of the LDP session. The establishment of the LDP session involves two steps:

a) Connection setup, actually the completion of the three handshakes of the TCP connection, not involving the interaction of the LDP messages

b) Session initialization: it is the process to negotiate to determine the related parameters of the LDP session through the exchange of the mutual initialization information, for example, label distribution mode, Keepalive time and the length of largest Protocol Data Unit (PDU)

After the LDP session is established and both parties enter the OPERATIONAL status, the label information can be exchanged to allocate and manage labels for establishing the LSP.

During the LSP establishment process, the labels can be distributed in two ways: DOD Downstream on Demand and Downstream Unsolicited. In the DOD mode, the LSR only responds with the label binding information when it receives the label request of the adjacent LSR. In the DU mode, a LSR distributes label binding to its adjacent LSR when it does not receive any request.

During the LSP establishment process, there are tow label control modes: Independent and Ordered. One LSR can support two control modes by configuring options.

When independent control is used, each LSR can advertise to the adjacent device the binding between the label and the FEC at any time as needed. When working in the independent DOD mode, one LSR can immediately answer the label mapping request from the upstream without needing to wait for a label mapping from the next hop. When working in the independent DU mode, one LSR can advertise the label mapping of the FEC at any time when it is ready to perform label swap for the FEC.

When ordered control is used, one LSR can distribute the FEC bound label to the upstream only when a FEC has the next-hop label mapping or the LSR is the egress of the FEC. Otherwise, the LSR must wait for receiving the label mapping of the FEC from a downstream LSR, before the local device can bind the FEC with the label and send it to the upstream LSR. In the ordered control mode, if the label distribution mode is DU, only when it is the egress of the FEC or the label is received from the downstream LSR, it will advertise the label to its own upstream LSR. If the label distribution mode of the downstream LSR is DOD, it will transfer the request to its downstream when it receives the request information from the upstream LSR, whether it words in the DOD or DU mode.

42.1.6.2 Loop Control of LSP

During the establishment of the LSP, the loop detection mechanism must be provided to ensure that any loop of the LSP established can be detected. There are two ways to prevent the loop of the LSP: maximum hop count and path vector.

By maximum hop count, the label binding message transferred includes the number of LSRs passed. The count increases by 1 for every LSR passed. When this value exceeds the specified maximum value, it is deemed that a loop has occurred and the establishment of the LSP is terminated.

By path vector, the label binding message transferred records the IDs of the LSRs passed. When a LSR is passed, the ID of that LSR is recorded to the vector table of the message. When a LSR receives the label binding message, it checks if its ID is included in the vector table. If not, it will add its own ID to the record when distributing the message. If yes, it means that a loop has occurred, and hence the establishment of the LSP is terminated.

42.1.7 Application of MPLS

As the network develops, the forwarding advantage of the MPLS is no longer so prominent. Currently, various applications based on MPLS win increasingly more attentions, for example, VPN and QOS. The following diagram shows the applications of MPLS:

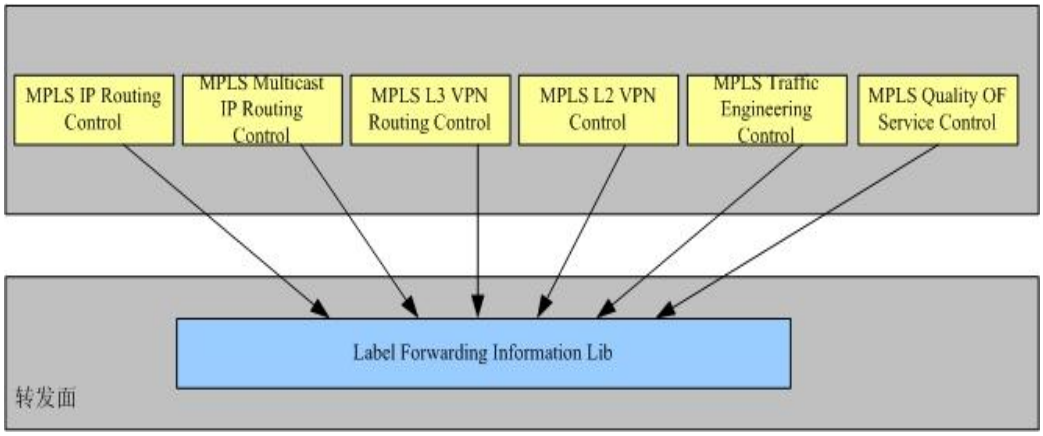


Figure 4

Same as the architecture where the MPLS system is applied to the IP unicast route, the application of every MPLS includes the following elements:

1. A database used to define FECs for the application;
2. A control protocol used to exchange FECs between LSRs;
3. A control protocol used to execute FECs label binding and directly swap the label at the LSR;

The following table describes various control protocols of different applications based on the MPLS system:

Application	FEC table	Control protocol used to create the FEC table	Control protocol used to exchange FEC and label mapping
IP Routing	Unicast routing table	IP routing protocol	LDP
L3 VPN Routing	VRF (routing table of every VPN)	PE and CE use the unicast routing protocol, and the MP-BGP is used between PEs	MP-BGPH
L2 VPN	Pwid [RFC4447]	Static configuration->Martini MP-BGP-> kompella	Martini : LDP Kompella: MP-BGP

42.2 Configuring MPLS

42.2.1 MPLS Basic Configuration Steps

To implement the basic forwarding function of MPLS,

- Enable MPLS forwarding globally (mandatory)
- Enable the LDP protocol (mandatory)

- Enable MPLS on the interface (mandatory)
- Enable LDP on the interface (mandatory)
- Configure MPLS MTU on the interface (optional)
- Configure MPLS TTL copy function (optional)

After the above configuration, the switch can provide the MPLS function.

Caution

Since the LDP protocol is based on the topology driver, the switch should enable the IPv4 routing protocol and ensure that the routing protocol is working normally in order for the MPLS network to work normally.

42.2.1.1 Enabling MPLS Forwarding Global

In the global configuration mode, use the **mpls ip** command to enable the MPLS forwarding. By default, the equipment can not enable the MPLS forwarding. After the MPLS forwarding is enabled, the equipment will use the MPLS to carry out the data forwarding firstly.

The **no mpls ip** command is used to disable the MPLS forwarding.

Note: In this version, this command is valid only for the process forwarding, but not valid for the switching chip forwarding.

Command	Meaning
mpls ip	Enable the MPLS forwarding.
no mpls ip	Disable the MPLS forwarding.

42.2.1.2 Enabling the LDP protocol

In the privileged mode, the **mpls router ldp** command is firstly used to enable the LDP protocol and enter the LDP configuration mode. When the LDP is enabled, use the **mpls router ldp** command to enter the LDP configuration mode.

Use the **no mpls router ldp** command to disable the LDP protocol.

Command	Meaning
mpls router ldp	Enable the LDP protocol and enter the LDP configuration mode
no mpls router ldp	Disable the LDP protocol.

Caution

After the LDP protocol is activated, the interface of the switch will not send and receive the LDP packets. To send and receive the LDP packets on an interface, you need to enable the LDP protocol in the interface mode.

42.2.1.3 Enabling MPLS Packet Processing Capacity of Interface

By default, the switch interface does not process the MPLS packets, but directly discards them after receiving the MPLS packets. To allow the switch interface to process the received MPLS packets, enable the MPLS function of the interface in the interface mode.

Command	Meaning

Command	Meaning
label-switching	Enable the MPLS function of the interface
no label-switching	Disable the MPLS function of the interface

Caution

After the MPLS function of the interface is enabled by the label-switching command, this interface can only process the MPLS packet with the label. It can only find common Ipv4 route table to forward for the received IP packet, but can not find the LSP forwarding of the FTN table along the MPLS. Hence, this command is not usually configured at the ingress of the IP packet for the LER. This command is specified that it needs to be configured when the MPLS multi-service card is used to carry out the MPLS service forwarding, but it doesn't need to be configured when the MPLS multi-service card is not used to carry out the MPLS service forwarding.

42.2.1.4 Enabling the LDP in the interface mode

To enable the LDP on specified interface, it is necessary to use the **mpls ip** command to activate the LDP on this interface after the global enabling of the LDP protocol, and start to send the Hello message periodically.

Command	Meaning
mpls ip	Enable the LDP function of the interface
no mpls ip	Disable the LDP function of the interface

Caution

After you enable the LDP protocol in the interface mode, the interface will not receive and send the LDP packets if you do not activate the LDP protocol by using the router ldp command in the global configuration mode.

42.2.1.5 Configuring MPLS MTU on the Interface

To configure the MPLS MTU of the interface, the MPLS label packet MTU to be transmitted on the interface is the interface MTU plus 8 bytes by default.

The **no mpls mtu command** is used to restore the MPLS MTU of the interface to the default value, the MTU of the interface plus 8 bytes.

Command	Meaning
mpls mtu bytes	Setting MPLS MTU of the Interface
no mpls mtu	Restore the MPLS MTU of the interface to the default value.

Caution

The configuration of the MPLS MTU for the interface can not exceed the actual transmitted packet capacity of the interface. This configuration does not take effect for switches, because the switch's hardware forward packets according to the MTU configured on the interface, and the one exceeding the configuration will be dropped directly. To adjust the MTU on an interface ,execute the **mtu** command.

42.2.1.6 Configuring IP TTL Copy Function of MPLS

There are two ways to process TTL for the packets after MPLS encapsulation or deencapsulation:

TTL copy: Default operation mode. When pushing a label, the system copies the TTL of an existing IP packet header or MPLS packet header to the TTL domain of the pushed label. When popping a label, the system copies the TTL of outer label to the popped label.

No TTL copy: in this mode, any TTL copy is executed. When pushing a label, the system directly sets the TTL of the label to 255. when popping a label, the system keeps the TTL of the popped IP or MPLS packet unaltered.

Use the **mpls ip ttl propagate {public | vpn}** command to control the TTL copy for the packets sent or forwarded by the local device respectively.

Command	Meaning
[no] mpls ip ttl propagate public	Enable or disable TTL copy for the packets sent by the local device.
[no] mpls ip ttl propagate VPN	Enable or disable TTL copy for the packets forwarded by the local device.

Enabling TTL copy allows you to track all the LSRs passed within the MPLS domain by suing Tracert on the CE. If you disable this function on the PE, all the LSPs passed are treated as a hop in a whole.

Caution

This command only processes the encapsulated IP packet, and it is not valid for the non-IP packet. For the switches, it indicates this configuration is invalid for the chip forwarding, and it will be carried out by the determined function of the chip.

42.2.1.7 Verifying the MPLS Information

After above configuration, the equipment can establish the LSP for MPLS forwarding. In the privileged mode, you can view the MPLS information by using the show command, and verify the configuration result.

Show MPLS Information

It will show the use information of the label space and which interface enables the MPLS function. Verify the correctness of the configuration by viewing information.

Command	Meaning
show mpls summary	Show the basic information of MPLS

- **Show MPLS Forwarding Table**

Show the contents of the FTN entries and view specific contents of the FTN entries added by the LDP protocol, for example, the FTN corresponding FEC, outgoing interface, outgoing label, and next-hop address.

Command	Meaning
show mpls forwarding-table [**detail** | **vrf name**]	Show the FTN information

- **Show the FTN table**

Show the contents of the FTN entries and view specific contents of the FTN entries added by the LDP protocol, for example, the FTN corresponding FEC, outgoing interface, outgoing label, and next-hop address. It will obtain the MPLS FTN forwarding table item information by the view.

Command	Meaning
show mpls forwarding-table ftn [**ip** | **vc** | **detail**]	Show the FTN information

- **Show the ILM table**

Show the contents of the ILM entries and view specific contents of the ILM entries added by the LDP protocol, for example, the ILM incoming interface, incoming label, outgoing label and next-hop address. It will obtain the MPLS FTN forwarding table item information by the view.

Command	Meaning
show mpls forwarding-table ilm [**ip** | **vc** | **detail**]	Show the ILM information

42.2.2 LDP Parameter Configuration

You can modify the default parameters of the LDP by using commands in the LDP configuration mode or interface configuration mode.

42.2.2.1 Configuring LDP Session Parameters

- **Configuring LDP Router ID**

The LSR ID uniquely identifies a LSR in the domain, and it uses the format of the IP address. By default, the switch uses the router id of the system as the LSR ID. The **lsr-id** command can be used to modify the LSR ID.

For the LDP uses the ldp router-id as the transport-address by default, it is necessary to ensure the ldp router-id is reachable for other LSRs.

Command	Meaning
ldp router-id ip-address	Set the LDP router ID of the LSRs.
no ldp router-id	Use the router id as the LSR ID

- **Configure the transport-address**

By default, the LSR ID is used as the global transmission address. As options, you can also choose to use the local interface address or the IP address of the specified interface or specify an IP address as the global transmission address.

When an IP address is specified as the global transmission address, you must ensure that other LSRs have routes to the transport address so that other LSRs can work with this LSR to establish connections a TCP connection for the LDP.

Command	Meaning
transport-address { **interface** |*ip-address*| *interface-name*}	Set the global transmission address
no transport-address	Use the LSR ID as the global transmission address

- **Configure the hello message interval**

The LDP discovers LDP peers by periodically sending hello messages. The default hello message interval is 5 seconds. This value can be set freely within the range of 1 ~ 65535 seconds.

Command	Meaning
mpls ldp hello-interval <*1-65535*>	Set the hello message interval
no mpls ldp hello–interval	Use the default hello message interval

- **Configure the hello message holdtime**

After the LDP discovers a LDP peer by sending hello messages at periodical intervals, it can retain the LDP peer within a certain period before it receives the hello message. If this period expires, it

deems that this LDP peer becomes invalid. This period is known as the hello message holdtime. The default hello message holdtime is 15 seconds. This value can be set freely within the range of 1 ~ 65535 seconds.

Command	Meaning
mpls ldp hello-holdtime *<1-65535>*	Set the hello message holdtime
no mpls ldp hello–holdtime	Use the default hello message holdtime

- **Configure the keepalive packet holdtime**

After the LDP discovers a LDP peer by sending hello messages and establishes the TCP session, it can retain the session within a certain period before it receives the keepalive packet. If this period expires, it deems that this LDP peer becomes invalid. This period is known as the keepalive packet holdtime. By default, the keepalive packet holdtime of the Session established by the basic discovery mechanism is 45s, and the keepalive packet holdtime of the Session established by the extended discovery mechanism is 180s. This value can be set freely within the range of 15 ~ 65535 seconds. The interval of the Keepalive packet is 1/3 of the keepalive packet holdtime.

Command	Meaning
mpls ldp keepalive –holdtime*<15-65535>*	Set the keepalive packet holdtime of the Session established by the basic discovery mechanism on the interface.
No mpls ldp keepalive–holdtime	The Session established by the basic discovery mechanism uses the default keepalive packet holdtime.
targeted-session holdtime *<15-65535>*	Set the keepalive packet holdtime of the Session established by the extended discovery mechanism on the interface in the LDP mode.
No targeted-session holdtime	The Session established by the extended discovery mechanism uses the default keepalive packet holdtime.

- **Configure the maximum times of label requests**

When the LDP requests for labels, if no label is obtained due to various reasons, the LDP will make requests again after a period of time. The default times of requests are unlimited. This value can be set freely within the range of 0 ~ 255.

Command	Meaning
mpls ldp max-label-requests*<0-255>*	Set the maximum repeating times for the LDP label requests
no mpls ldp max-label-requests	Use the default repeating times for the LDP label requests

- **Set the maximum PDU (Protocol Data Units**)

Various messages transferred between the LDP entities are included in the PDU. This size of the PDU can be set freely within the range of 255 ~ 4096 in the interface mode. The default PDU value is 4096.

Command	Meaning
mpls ldp max-pdu *<255-4096>*	Set the maximum PDU
no mpls ldp max-pdu	Use the default PDU (4096)

- **Set extended LDP discovery mechanism**

The basic LDP discovery mechanism discovers the local LDP peers, that is, establish local LDP session for the directly connected LSR. The extended discovery mechanism discovers the remote LDP peer, that is, establish LDP remote session for indirectly connected LSR.

Command	Meaning
neighbor *A. B.C. D*	Configure a remote LDP peer.

Command	Meaning
no neighbor *A. B.C. D*	Remove a remote LDP peer.

42.2.2.2 Configuring LDP Loop Detection

- **Configure Loop Detection Mode**

The LDP provides two loop detection methods: maximum hop count and path vector. By default, the loop detection is disabled for the LDP.

For the loop detection method of maximum hop count, the hot count is carried together with the labels, and the hot count increases by 1 at every hop. When the hop count exceeds the set maximum value, it deems that a loop has occurred on the LSP.

The path vector loop detection mode works by carrying the LSR ID together with the label information. At every hop, the LSR will check whether the number of LSRs in the path vector list exceeds the set maximum value. It so, a loop occurs. Otherwise, the LSR checks if its ID exists in the record. If yes, it means that a loop has occurred. If no, the LSR will add its own ID to the record.

Command	Meaning
loop-detection	Enable loop detection
no loop-detection	Disable loop detection

- **Configure the maximum hop count**

In the interface mode, you can set the maximum hop count for loop detection. By default, this value is 254. This value can be set within the range of 1 ~ 255. When loop detection is enabled, if the hop count is greater than the set value, it deems that a loop has occurred.

Command	Meaning
mpls ldp max-hop-count <*1-255*>	Set the maximum hop count for loop detection
no mpls ldp max-hop-count	Set the default maximum hop count for loop detection

- **Configure the maximum number of LSRs in the path vector list**

In the interface mode, you can set the maximum number of LSRs carried in the path vector lists. By default, this value is 254. This value can be set within the range of 1 ~ 255. When loop detection is enabled, if the LSR finds that the path vector list includes its own ID or the number of LSRs in the path vector list is greater than the set value, a loop has occurred.

Command	Meaning
mpls ldp max-path-vector <*1-255*>	Set the maximum number of LSRs in the path vector list.
No mpls ldp max-path-vector	Set the maximum number of LSRs in the path vector list to the default value

42.2.2.3 Configuring the LDP operating mode

- **Configuring the LDP label distribution control mode**

The LDP label distribution control mode indicates when the LSR notifies the binding between the label and the FEC to its neighbor. There are two label distribution control modes: independent and ordered.

When independent control is used, each LSR can advertise to the neighbor the binding between the label and the FEC at any time as needed. When ordered control is used, the LSR binds the label for the FEC and distributes to the upstream only when the FEC has the next-hop label mapping or when the LSR is the Egress LSR of the FEC.

By default, the LDP uses the ordered label distribution control mode. You can use the **lsp-control-mode** command to set the label distribution control mode of the LDP.

Command	Meaning
lsp-control-mode {*independent* | *ordered*}	Set the label distribution control mode
no lsp-control-mode	Use the default label distribution control mode (ordered)

- **Configuring the LDP label distribution mode**

The LDP label distribution mode indicates when the LSR notifies the binding between the label and the FEC to its neighbor. There are two label distribution modes: DOD and DU.

When the LSR works in the DOD mode, it only responds with the label mapping information to distribute labels when it receives the label request from the upstream LDP neighbor. When the DU node is used, it distributes labels unsolicited to the upstream LDP neighbor according to the appropriate triggering policy. If the upstream LSR and downstream LSR use different label distribution modes, the upstream and downstream LSR both use the DU mode if they are connected via Ethernet.

The LDP works in the DU mode by default. You can use the distribution-mode command in the interface mode to set the label distribution control mode of the LDP at the interface.

Command	Meaning
mpls ldp distribution-mode {*du* | *dod*}	Set the label distribution mode
no mpls ldp distribution-mode	Use the default label distribution mode (DU)

- **Configuring the LDP label retention mode**

The label retention mode indicates whether to retain the label binding learnt from the label mapping information when the received label mapping message is not from the next-hop FEC of the message, or the received label mapping message does not match not any of the existing IP route. There are two label retention modes: conservative and liberal.

When the above condition occurs, the liberal label retention mode retains the FEC label binding learnt from the neighbor, while the conservative label retention mode does not retain the FEC label binding learnt from the neighbor.

The conservative label retention mode needs to use and maintain a smaller number of labels. However, when the routes change, new labels must be obtained and so this increases the response time. On the other hand, the liberal label retention mode responds quickly to route changes, but the label mapping not used is also distributed and maintained.

By default, the LDP uses the liberal label retention mode.

You can use the label-retention-mode command to set the label retention mode.

Command	Meaning
label-retention-mode {*liberal* | *conservation*}	Set the label retention mode
no label-retention-mode	Use the default label retention mode

- **Configuring label merge**

If the LSR has bound multiple incoming labels for a specific FEC, but the same label is used to forward the packets of the FEC, it means that the LSR has the label merge function. You can enable and disable the label merge function by configuring the LDP.

By default, the LDP has enabled the label merge function.

You can enable and disable the label merge function by using the **label-merge** command.

Command	Meaning
label-merge	Enable the label merge function
no label-merge	Disable the label merge function

- **Configuring the label release information transfer mode**

When a FEC fails, the LDP will send the label release message from the downstream to the upstream to remove the label bound to the FEC. Whether each LDP on the LSP transfers the message to the downstream when it receives the label release message from the downstream depends on the label release message transfer mode set.

By default, the LDP will not transfer the message to the upstream when it receives the label release message from the downstream.

You can set the label release message transfer mode by using the **propagate-release** mode.

Command	Meaning
propagate-release	Transfer the label release message to the upstream
no propagate-release	Not transfer the label release message to the upstream

42.2.2.4 Configuring Label Distribution Policy

By default, the LDP will assign labels for all valid IGP routes, except BGP routes. In some case, you may need to assign labels for specific routes.

You can set the label release message transfer mode by using the **propagate-release** mode.

Command	Meaning
advertise-labels for host-routes	Assign labels for the routes matching 32-bit mask in the route forwarding table. By default, the mask is not limited.
advertise-labels for bgp-routes	Assign labels for BGP routes. By default, this function is disabled.

In some applications, it is not necessary to assign labels for all IGP routes to establish LSP. For example, in a MPLS network only transmitting user business like L3VPN, VPN users in different areas do business through the MPLS network. This application does not require to assign labels for every network segment in the MPLS network to establish LSP. It only needs to establish LSP between PEs. In this case, you can execute the advertise-labels for host-routes on the PEs and Ps in the MPLS network to assign labels for the routes of 32-bit mask to save label resources.

In a real network, the BGP protocol carries with more routes and generally maintains the routes from other ASs, which may be not necessary for its AS. If LDP assigns labels for these BGP routes, this will consume a lot number of label resources. By default, no label is distributed to BGP routes. If you need to distribute labels to BGP routes and advertise them to LDP neighbors, execute the **advertise-labels for bgp-routes** command.

By default, LDP distributes labels for IGP routes, not BGP routes.

42.2.2.5 Verifying the LDP information

- **Show the LDP attribute**

The **show mpls ldp parameter** command can be used to show various attribute information of the LDP, including the LSR ID, transport-address, loop detection mechanism, label distribution control mode, label retention mode, interval and keepalive of the extended peer hello message and interval and keepalive of the extended peer keepalive packet. Verify the correctness of the configuration by viewing the information.

Command	Meaning
show mpls ldp parameters	Show the LDP attribute

- **Show the LDP session information**

The **show mpls ldp session** command allows you to show the information of all LDP sessions. You can also add the IP address of the remote LDP entity in the front of the command to show the information of the specific LDP session. The information shown includes the session duration, session status, and session source address. By checking such information, you can learn the status of the session and determine if the session has been established.

Command	Meaning
show mpls ldp session	Show the LDP attribute

- **Show the binding between the FEC and the label**

The **show mpls ldp binding** command allows you to show the information of FEC and label binding. This command allows you to view the working status of the LDP, whether the LDP has normally bound the FEC, as well as the specific label value of a specific FEC binding.

Command	Meaning
show mpls ldp bindings	Show the binding between the FEC and the label

- **Show the LDP neighbor**

The **show mpls ldp neighbor** command allows you to show all LDP neighbors, including the TCP connection port between the local LDP and peer LDP, LDP status, received/sent message count, and LDP discovery party.

Command	Meaning
show mpls ldp neighbor	Show all LDP neighbors

- **Show the discovered LDP neighbors**

Show the ports on which the LDP has discovered neighbors and the information of the neighbors.

Command	Meaning
show mpls ldp discovery	Show the discovered LDP neighbors

42.2.3 Manually Configuring the LSP

To implement the basic forwarding function of MPLS, you can configure it manually instead of using the LDP. Manually configuring MPLS is to manually establish and maintain the LSP.

To manually implement the MPLS basic forwarding functions, perform the following steps:

- Enable MPLS forwarding globally (mandatory)
- Enable MPLS forwarding on the interface (mandatory)
- Configure static LSP (mandatory)

After the above configuration, the switch can provide the MPLS function.

Caution

If you manually configure the LSP, the LDP protocol is not needed, it does not need to rely on the IPv4 route. Even if there is not any IPv4 route in the network, the manual configured LSP will take effect as long as the physical network is reachable.

For the steps of enabling MPLS forwarding globally and on the interface, refer to basic MPLS configuration.

42.2.3.1 Configuring Static LSP

Manually configuring the MPLS network is mainly to manually establish the LSP. The configuration steps are the same as the case where the LDP is used. Manually establishing the LSP consists of three steps:

- Configure the FTN on the ingress LSR
- Configure the ILM on the intermediate LSR
- Configure the ILM with the outgoing label of 3 on the last but one LSR of the LSP

Label values 16 ~ 1024 are reserved for configuring static LSP.

42.2.3.2 Configuring the FTN on the ingress LSR

At the ingress of the LSP, FTN entries should be created for the FEC, that is, bind the FEC with the label.

In the global configuration mode, execute the **mpls static ftn** command to manually configure the FTN. The format of this command is as below:

Command	Meaning
mpls static ftn *A.B.C.D/M* **out-label label nexthop interface** *nexthop-ip*	Add the global FTN
no mpls static ftn *A.B.C.D/M*	Delete the global FTN

For example, to configure a global FTN where the FEC 192.168.1.0/24 is bound with the label of 16 and the next hop of the LSP is 192.168.10.10, and the outgoing interface is GigabitEthernet 2/1, execute the following command:

mpls static ftn *192.168.1.0/24* **out-label** *16* **GigabitEthernet** *2/1 192.168.10.10*

To delete the FTN entry, it is only necessary to enter the FEC, and other parameters need not to be entered.

no mpls static ftn *192.168.1.0/24*

42.2.3.3 Configuring the static ILM on the intermediate LSR

To forward the incoming labeled packets according to their labels on an intermediate LSR, set the ILM and map the incoming label to the outgoing label. In the global configuration mode, execute the mpls **static ilm in-label** command to manually configure the ILM. The format of this command is as below:

Command	Meaning
mpls static ilm in-label *in_label* **forward-action swap-label** *swap_label* **nexthop interface** *nexthop-ip* **fec** *A.B.C.D/M*	Add the global ILM
no mpls static ilm in-label *in_label*	Delete the global ILM

For example, to configure a global ILM where the incoming label 16 received from the GigabitEthernet 2/1 interface is mapped to the outgoing label 17, the next hop of the LSP is

192.168.11.11 and the outgoing interface is GigabitEthernet 2/2, the FEC of the LSP is 192.168.1.0/24, execute the following command:

mpls static ilm in-label *16* **forward-action swap-label** *17* **nexthop GigabitEthernet** *2/2 192.168.11.11* **fec** *192.168.1.0/24*

To delete the ILM, execute the following command:

no mpls static ilm in-label *16*

42.2.3.4 Configure the ILM on the last but one LSR

Since the last but one hop is to perform PHP (last but one hop pop), the ILM entry on the last but one hop must be different from the ILM entries on the other intermediate LSRs. In other words, the outgoing label of the ILM on the last but one hop LSR on the LSP must be implicit null label (with the value of 3).

Caution

For the concept of second but last hop pop, refer to the related document.

For example, to configure a global ILM on the second but one hop of the LSP, where the incoming label 17 received from the interface GigabitEthernet 2/1 is subjected to the PHP operation, the packets with label 17 popped up are sent from the interface GigabitEthernet 2/2, and the next hop address is 192.168.12.12, and the LSP corresponds with the FEC of 192.168.1.0/24, Execute the following command:

mpls static ilm in-label *17* **forward-action swap-label** *3* **nexthop GigabitEthernet** *2/2 192.168.11.11* **fec** *192.168.1.0/24*

To delete the ILM, execute the following command:

no mpls static ilm in-label *17*

42.2.4 MPLS Basic Configuration Examples

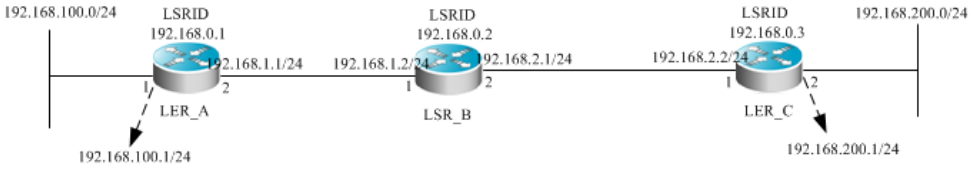


Figure 5

As shown in the above diagram, the MPLS network consists of three MPLS switches. The following sections describe how to use the LDP to establish the LSP and manually configure the LSP.

42.2.4.1 Using the LDP protocol to establish LSP

The LDP protocol needs the IPv4 route in order to work. In this case, the OSPF protocol is used to establish the IPv4 route.

LER_A configuration:

Command	Meaning
DES-7210 (config) # **mpls ip**	Enable MPLS forwarding globally.
DES-7210(config)# **mpls router ldp**	Enable the LDP protocol and enter the LDP mode.

Command	Meaning
DES-7210 (config-mpls-router)# **ldp router-id** *192.168.0.1*	Set the LSR ID.
DES-7210 (config-mpls-router)# **exit**	Exit the LDP mode and enter the global configuration mode.
DES-7210 (config)# **interface gigabitEthernet** *2/2*	Enter the interface GigabitEthernet 2/2
DES-7210 (config-if)# **mpls ip**	Enable the LDP and MPLS forwarding on the interface
DES-7210 (config-if)# **label-switching**	Enable MPLS label switching on the interface of the public network for the device using 7200-ASE3 multi-service card.
DES-7210 (config-if)# **exit**	Exit the interface mode and enter the global configuration mode
DES-7210 (config)# **router ospf** *10*	Enable the OSPF protocol and enter the OSPF mode
DES-7210 (config-router)# **network** *192.168.100.0 255.255.255.0* **area** *0* DES-7210 (config-router)# **network** *192.168.0.1 255.255.255.255* **area** *0* DES-7210 (config-router)# **network** *192.168.1.0 255.255.255.0* **area** *0*	Add the route information to OSPF
DES-7210 (config-router)# **end**	End the configuration

LER_B configuration:

Command	Meaning
DES-7210 (config) # **mpls ip**	Enable MPLS forwarding globally.
DES-7210(config)# **mpls router ldp**	Enable the LDP protocol and enter the LDP mode.
DES-7210 (config-mpls-router)# **ldp router-id** *192.168.0.2*	Set the LSR ID.
DES-7210 (config-mpls-router)# **exit**	Exit the LDP mode and enter the global configuration mode.
DES-7210 (config)# **interface gigabitEthernet** *2/1*	Enter the interface GigabitEthernet 2/1
DES-7210 (config-if)# **mpls ip**	Enable the LDP and MPLS forwarding on the interface
DES-7210 (config-if)# **label-switching**	Enable MPLS label switching on the interface of the public network for the device using 7200-ASE3 multi-service card.
DES-7210 (config-if)# **exit**	Exit the interface mode and enter the global configuration mode

Command	Meaning
DES-7210 (config)# **interface gigabitEthernet** *2/2*	Enter the interface GigabitEthernet 2/2
DES-7210 (config-if)# **mpls ip**	Enable the LDP and MPLS forwarding on the interface
DES-7210 (config-if)# **label-switching**	Enable MPLS label switching on the interface of the public network for the device using 7200-ASE3 multi-service card.
DES-7210 (config-if)# **exit**	Exit the interface mode and enter the global configuration mode
DES-7210 (config)# **router ospf** *10*	Enable the OSPF protocol and enter the OSPF mode
DES-7210 (config-router)# **network** *192.168.1.0 255.255.255.0* **area** *0* DES-7210 (config-router)# **network** *192.168.2.0 255.255.255.255* **area** *0* DES-7210 (config-router)# **network** *192.168.0.2 255.255.255.0* **area** *0*	Add the route information to OSPF
DES-7210 (config-router)# **end**	End the configuration

LER_C configuration:

Command	Meaning
DES-7210 (config) # **mpls ip**	Enable MPLS forwarding globally.
DES-7210(config)# **mpls router ldp**	Enable the LDP protocol and enter the LDP mode.
DES-7210 (config-mpls-router)# **ldp router-id** *192.168.0.3*	Set the LSR ID.
DES-7210 (config-mpls-router)# **exit**	Exit the LDP mode and enter the global configuration mode.
DES-7210 (config)# **interface gigabitEthernet** *2/1*	Enter the interface GigabitEthernet 2/1
DES-7210 (config-if)# **mpls ip**	Enable the LDP and MPLS forwarding on the interface
DES-7210 (config-if)# **label-switching**	Enable MPLS label switching on the interface of the public network for the device using 7200-ASE3 multi-service card.
DES-7210 (config-if)# **exit**	Exit the interface mode and enter the global configuration mode
DES-7210 (config)# **router ospf** *10*	Enable the OSPF protocol and enter the OSPF mode

Command	Meaning
DES-7210 (config-router)# **network** *192.168.200.0 255.255.255.0* **area** *0* DES-7210 (config-router)# **network** *192.168.0.3 255.255.255.255* **area** *0* DES-7210 (config-router)# **network** *192.168.2.0 255.255.255.0* **area** *0*	Add the route information to OSPF
DES-7210 (config-router)# **end**	End the configuration

42.2.4.2 Configuring the Static LSP

Configuring the static LSP does not need the support of the IPv4 route.

As an example, two LSPs are established between the 192.168.100.0/24 network segment connected with the interface 1 of the LER_A and the 192.168.200.0/24 network segment connected with the interface 2 of the LER_C to connect them. It is necessary to establish two LSPs for the LSP is unidirectional, there should be one LSP from LER-A to LER-C and another LSP from LER-C to LER-A.

LER_A configuration:

Command	Meaning
DES-7210 (config)# **interface gigabitEthernet** *2/2*	Enter the interface GigabitEthernet 2/2.
DES-7210(config-if)# **label-switching**	Enable MPLS label switching on the interface of the public network for the devices using 7200-ASE3 multi-service card.
DES-7210(config-if)# **exit**	Exit the interface mode and enter the global configuration mode
DES-7210 (config)# **mpls static ftn** *192.168.200.0/24* **out-label** *16* **nexthop gigabitEthernet** *2/2* *92.168.1.2*	Create a FTN to bind the 192.168.200.0/24 with label 16. Specify the next hop of the FTN as 192.168.1.2 and the outgoing interface as gigabitEthernet 2/2.
DES-7210(config-router)# **end**	End the configuration

LER_B configuration:

Command	Meaning
DES-7210(config)# **interface gigabitEthernet** *2/1*	Enter the interface GigabitEthernet 2/1
DES-7210(config-if)# **label-switching**	Enable MPLS label switching on the interface of the public network for the devices using 7200-ASE3 multi-service card.
DES-7210(config-if)# **exit**	Exit the interface mode and enter the global configuration mode
DES-7210(config)# **interface gigabitEthernet** *2/2*	Enter the interface GigabitEthernet 2/2

Command	Meaning
DES-7210(config-if)# **label-switching**	Enable MPLS label switching on the interface of the public network for the devices using 7200-ASE3 multi-service card.
DES-7210(config-if)# **exit**	Exit the interface mode and enter the global configuration mode
DES-7210(config)# **mpls static ilm in-label** *16* **forward-action swap-label** *3* **nexthop** *gi2/2 192.168.2.2* **fec** *192.168.200.0/24*	Create one ILM to map the received incoming label 16 to the outgoing label 3 (hidden empty label) of the interface gigabitEthernet 2/2. The address of the next hop is 192.168.2.2, and the FEC is 192.168.200.0/24.
DES-7210(config)# **mpls static ilm in-label** *17* **forward-action swap-label** *3* **nexthop** *gi2/1 192.168.1.1* **fec** *192.168.100.0/24*	Create one ILM to map the received incoming label 17 to the outgoing label 3 (hidden empty label) of the interface gigabitEthernet 2/1. The address of the next hop is 192.168.1.1, and the FEC is 192.168.100.0/24.
DES-7210 (config-router)# **end**	End the configuration

For LER_B is the countdown second hop of the LSP established for this FEC of 192.168.100.0/24, the outgoing label (hidden empty label) of the no.17 incoming label mapping is 3, and the outgoing interface is gi2/1.

In this way, LER_B is also the countdown second hop of the LSP established for this FEC of 192.168.200.0/24, the outgoing label (hidden empty label) of the no.16 incoming label mapping is 3, and the outgoing interface is gi2/2.

LER_C configuration:

Command	Meaning
DES-7210 (config)# **interface gigabitEthernet** *2/1*	Enter the interface GigabitEthernet 2/1
DES-7210(config-if)# **label-switching**	Enable MPLS label switching on the interface of the public network for the devices using 7200-ASE3 multi-service card.
DES-7210(config-if)# **exit**	Exit the interface mode and enter the global configuration mode
DES-7210(config)# **mpls static ftn** *192.168.100.0/24* **out-label** *17* **nexthop gigabitEthernet** *2/1 192.168.2.1*	Create a FTN to bind the 192.168.200.0/24 with label 16. Specify the next hop of the FTN as 192.168.1.2 and the outgoing interface as gigabitEthernet 2/2.
DES-7210 (config-router)# **end**	End the configuration

After the above configuration, if a packet on the LER_A has their destination addresses on the 192.168.200.0/24 network segment, the packet will be sent from the gigabitEthernet 2/2 interface of the LER_A and added with label 16. After the packets with label 16 reach the gigabitEthernet 2/1 interface of LER_B, they will be converted into IP packets, which are sent from the gigabitEthernet 2/2 interface of the LER_B. After the IP packets whose destination address is on the 192.168.200.0/24 network segment reaches the LER_C, it is routed at the LER_C according to its IP address, and is sent from the gigabitEthernet 2/1 interface in this way.

43 BGP/MPLS VPN Configuration

43.1 BGP/MPLS VPN Overview

Traditional VPNs transmit private network data traffic on the public network by using the tunnel protocols such as GRE, L2TP and PPTP. BGP/MPLS IP VPN is another form of VPN, which is a VPN of the tunnel protocol between L2 and L3. The LSP is the tunnel on the public network, except that it is established through the LDP used by MPLS. The MPLS-based VPN forms a unified network by connecting the branches of the private networks through the LSP. The MPLS-based VPN also supports the interworking between different VPNs.There are natural advantages for the MPLS to implement the VPN. For instance, for the VPN users, it can greatly reduce the workload of the VPN users, the dedicated VPN equipment is not required, and the traditional router can establish the VPN. For the operators, it can carry out the VPN expansibility by the MPLS VPN easily.

As a high effective IP backbone network technology platform, the MPLS provides the VPN with a flexible and extensible technology foundation.

The implementation of the L3VPN by using the BGP/MPLS VPN has the following characteristics:

1. The VPN tunnel is established on the network service provider PE, instead of between the user CEs. The VPN route is also transferred between the PEs, and users do not need to spend time maintaining the VPN information.
2. Directly use the existing routing protocol. The establishment of the VPN tunnel and the route distribution are dynamically implemented. This is conducive to the expansion of the VPN scale.
3. Support address overlapping to allow different VPN users to use the same address space.
4. In the service provider network, the service exchange in the VPN uses label switching instead of the traditional route distribution.
5. Achieve the same security as the user lease line.

BGP/MPLS VPN needs to implement the following functions:

1. In the backbone network, the LDP is used to establish the LSP tunnel. This process is usually performed in the network of the service provider, and is already finished when the topology is stable.
2. Data forwarding; packets are forwarded according to the label of the packets and local mapping table.
3. MP-BGP and BGP expansion attribute, used to transfer the VPN routes and bear the VPN attributes, and labels.
4. Managing the VPN routes: creating multiple routing tables and maintaining the VPN routing information

43.1.1 BGP/MPLS VPN structure

In the BGP/MPLS VPN model, there are three components, as shown in the following diagram:

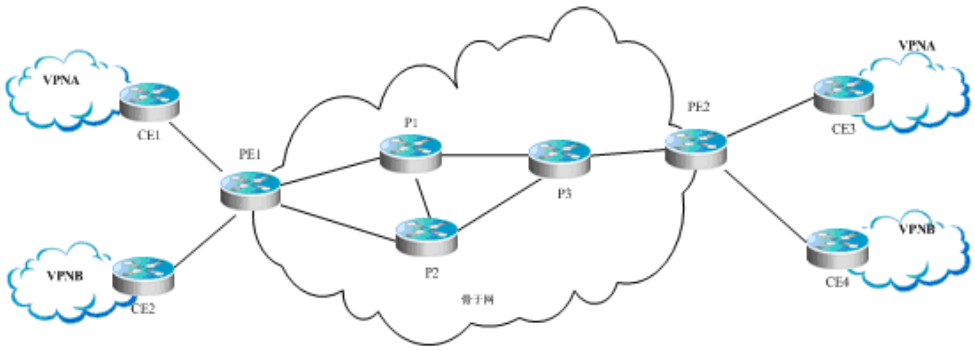


Figure 6

- **CE**

CE (Customer Edge Router), logically belonging to the VPN of the user; an interface of the CE is directly connected to the service provider router. The CE can be a host or a router, and may not support the MPLS function, for example, CE1, CE2, CE3 and CE4 as shown in the above diagram.

- **PE**

PE (Provider Edge Router), an edge device of the SP backbone network (can be a router, ATM switch or RF switch), like PE1 and PE2 shown in the diagram; logically the PE belongs to the service provider. The PE is directly connected to the CE and one PE can be connected with multiple different CEs. The PE is responsible for receiving the VPN information from the CE end, and sending the VPN information to other PEs, and receiving the VPN information from other PEs, and distributing them to the appropriate CE. The PE must support the MPLS function.

- **P**

P (Provider Router), located in the core router of the SP backbone network, as shown in P1, P2 and P3. P is not connected with the CE, and is responsible for routing and fast forwarding. P, as a router in the MPLS core backbone network, must support the MPLS function. P knows the route to any destination in the backbone network, but not that to the VPN.

43.1.2 VRF

- **VRF**

VRF (VPN Routing and Forwarding table) is mainly used to solve the local route conflict. The VPN Routing and Forwarding table is abbreviated as VRF. All connections between the PE and CE need to be associated with a VRF. There can be multiple VRFs on one PE, used to exchange route information with the CE end. Every VRF can be imagined as a “virtual router”, and each router is connected with the CE, responsible for receiving the route information from the CE end or notifying the VPN route information to the CE end. It solves the local route conflict on the PE due to that the same address spaces are used between different VPNs. The VRF includes:

A separate routing table

1. A group of interfaces belonging to this VRF
2. A group of routing protocols only used for this VRF
3. The VRF has two major attributes: RD attribute and RT attribute

- **RD**

Route Distinguisher, introduced to solve the route conflict during the transmission process. The RD can be understood as a distinguisher. If different VPNs have the same network address, the BGP is used to advertise the route information in the backbone network. The BGP decision only select the best route advertisement from these overlapped addresses, and this will cause some VPNs to fail to obtain the appropriate route information. With the RD value added, different distinguishers can be added to these overlapped addresses. The BGP decision process distinguishes the same

network addresses according to the different distinguishers carried in the VPN information. Each VPN can obtain its respective route information. The meaning of the RD is only a distinguisher to distinguish the same network addresses. If different VPNs have no overlapped addresses, it can be done without the RD value.

Usually, a unique RD is allocated for a VPN so that different VPNs have different RDs, and the route information can be transmitted normally in the backbone network. Usually, the RD value is defined as XX: XX, for example, RD 1: 100, where 1 identifies the AS number of the backbone network, and 100 is specified by the user. One VPN router can only carry one RD value.

The contents of the RD include the type field, management sub-area and distribution field. According to the value of the type field, there are the following three code formats:

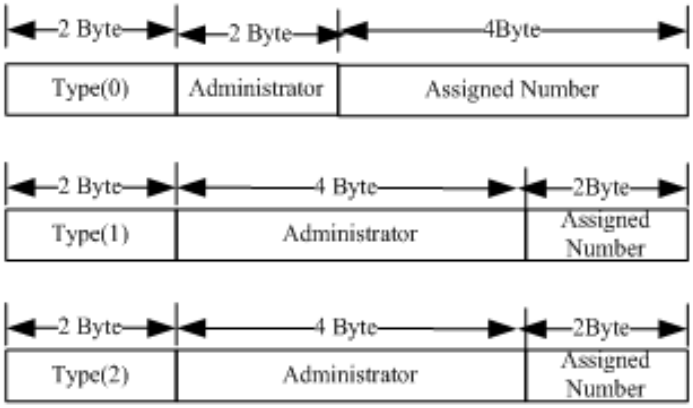


Figure 7

1. When Type = 0, the management sub-area has 2 bytes, and is identified by the AS number. It must be a public AS number. The allocation field has 4 bytes, managed by the service provider.
2. When Type = 1, the management sub-area has 4 bytes and uses the IPv4 address. The address must be the global IP address. The allocation field has 2 bytes, managed by the service provider.
3. When Type = 2, the management sub-area has 4 bytes identified by the AS number. The allocation field has 2 bytes, managed by the service provider.

- **Route-Target**

The RT attribute is used by the VRF to express how the route is handled. The RT attribute includes the “Export Route-Target” and “Import Route-Target”. The PE receives the route from the CE and adds the “Export Route-Target” attribute to these VPN route information, advertising the VPN route information to other PEs. The PE determines whether the route received from other PEs needs to be imported to the VRF according to the “Import Route-target”. One principle: When the PE receives the route information of the VPN, on if the RT attributes carried in the VPN route information at least have one attribute equal to the “Import RT” of a VRF on the local PE, the VPN information can be installed to the “VRF”. The above method can flexibly control the forwarding of the VPN route information. One piece of VPN route information can carry multiple RT values.

The expansion group attribute of the BGP defines the coding structure of the RT, as shown in the following diagram:

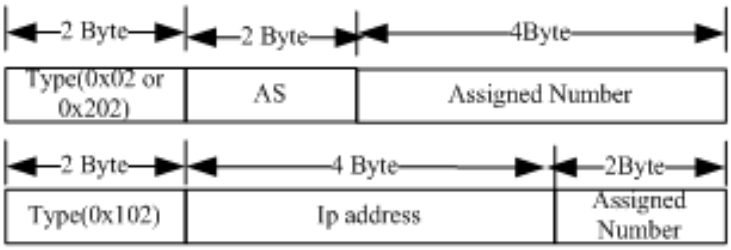


Figure 8

The RT value and RD value have similar definitions. For the type 0x02 and 0x202, the AS number must also be public. For type 0x102, the IPv4 address must be global, not private.

43.1.3 MP-BGP

The route information of the VPN is transmitted in the backbone network via BGP, and the “Export RT” attribute is carried by the expansion group attributes defined in the BGP protocol. However, as the traditional BGP4 protocol can only transmit the IPV4 route information, it cannot carry the VPN information that includes the RD, so the BGP must be expanded. The most important advantage of the BGP is its good expandability, which allows new attributes to be defined on the old basis. The MP-BGP is a new attribute introduced on the basis of the old BGP. It can support multiple protocols, known as Multi-Protocol BGP. The MP-BGP can carry the VPN information, and the VPN route can form the following form: RD + IP address prefix. When the MP-BGP transfers the VPN routes between the PE peers, the RD is added to transform the IPv4 route from the VPN user into the VPN-IPV4 router, for transfer in the backbone network.

43.1.4 Configuring BGP/MPLS VPN

BGP/MPLS VPN configuration includes:

- Configure MPLS (mandatory)
- Configure VPN route instance (mandatory)
- Configure BGP (mandatory)
- Configure PE-PE VPN route transfer (mandatory)
- Configure PE-PE route exchange (mandatory)
- Configure static L3 VPN forwarding entry (optional)
- Configure VPN label distribution method (optional)
- Configure VPN route import and export policy (optional)

43.1.5 Configuring the MPLS network

To use MPLS on the backbone network, the LDP of MPLS must be configured on the P and PE in order to establish the public network channel. This includes configuring the LDP for the appropriate router and enabling the MPLS forwarding function on each interface. The configuration steps are as below:

Command	Meaning
config terminal	
mpls router ldp	Enable the LDP protocol and enter the LDP configuration mode
Exit	Exit the LDP configuration mode
interface if-name	Enter the interface configuration mode.

Command	Meaning
label-switching	Enable the MPLS packet processing function on the interface of the public network for the devices using 7200-ASE3 multi-service card.
mpls ip	Enable LDP and MPLS on the interface
End	Return to the privileged mode
copy running-config startup-config	Save the configuration.

43.1.6 Configuring the VPN route instance

The VPN route instance is the VRF, which is configured on the PE. There is no VRF on the CE and P.

Configuring the VRF includes defining a VRF, configuring the RD and RT value for the VRF, and associating the VRF with an interface. The configuration steps are as below:

Command	Meaning
config terminal	
ip vrf *vrf_name*	Define a VRF and enter the VRF configuration mode.
rd *route-distinguish*	Define the RD value
route-target {both | export | import } *route-target-value*	Define the RT value
Exit	Exit the VRF configuration mode
interface *if-name*	Enter the interface configuration mode.
ip vrf forwarding *vrf_name*	Associate the interface with the VRF
ip address *A.B.C.D mask*	Configure the IP address
End	Return to the privileged mode
copy running-config startup-config	Save the configuration.

Caution

Once some VRF on PE defines the RD value or enables the BGP VRF function, the RD value of the VRF can not be modified or deleted.

- No two different VRFs can be defined with the same RD value on the same PE.
- Input the “ip vrf forwarding vrf_name” command. The IP address configured early for this interface will be deleted, and you need to define the IP address again in the interface mode.

43.1.7 Configuring PE-PE VPN Route Transfer

The route information is transferred between PEs via the BGP protocol. In order to transfer the VPN information to another PE, not the ordinary IPv4 route information, you need to enter the address family mode of the VPN to enable the transfer of VPN route to the peer PE. The steps are as below:

Command	Meaning
config terminal	
router bgp asn-number	Configure the BGP protocol and enter the BGP configuration mode

Command	Meaning
neighbor ip-address remote-as asn-number	Configure the PE peer
address-family vpnv4	Enter the VPN address family
neighbor ip-address activate	Enable the sending of the route information to the peer
End	Return to the privileged mode
copy running-config startup-config	Save the configuration

Caution

Options of the **neighbor update-source** command

When you use the **neighbor remote-as** command to specify the peer PE of BGP, you can specify a specific interface address of the peer to establish the TCP connection. In this case, you do not need to the **neighbor update-source** command. However, the TCP connection is established by specifying the loopback address of the other party between the peer PEs, you need to use the **neighbor update-source** command on the PE to specify its own loopback address as the TCP source address. This is often used for the IBGP neighbor. In actual configuration, you are recommended to use the Loopback address as the RouterID of PE.

43.1.8 Configuring the PE-CE Route Switching

43.1.8.1 Running the BGP protocol to transfer the route information between PE-CE

To configure the CE peer, you need to enter the VRF address family mode and configure the routing protocol for working with the CE end. The configuration steps on the PE are as below:

Command	Meaning
config terminal	
router bgp pe-asn	Configure the BGP protocol and enter the BGP configuration mode
address-family ipv4 vrf *vrf_name*	Enter the address family mode of the vrf
neighbor ip-address remote-as ce-asn	Configure the CE peer and usually specify the interface address on the CE directly connected with the PE
End	Return to the privileged mode
copy running-config startup-config	Save the configuration.

Caution

Usually, it will define the RD value of this VRF after one VRF is defined. However, if users don't define the RD value for this VRF and above command address-family ipvr vrf VRF_NAME needs to enter into the address family of specified VRF, the system will create a default RD value 0:0 for this VRF. It can no be modified or deleted after this RD value is created.

Perform the following steps on the CE to configure the PE:

Command	Meaning
config terminal	
router bgp ce-asn	Configure the BGP protocol and enter the BGP configuration mode
neighbor ip-address remote-as pe-asn	Configure the PE peer and usually specify the interface address on the PE directly connected with the CE

Command	Meaning
end	Return to the privileged mode
copy running-config startup-config	Save the configuration.

43.1.8.2 Running the OSPF protocol to transfer the route information between PE-CE

The PE and CE run the OSPF. On the PE, you must configure an OSPF instance for the corresponding VRF. Through this OSPF instance the VRF obtains the VPN route information on the CE end, and receives the VPN information from other PEs through the redistribute BGP command. At the same time, you should also enter the address family mode of the VRF and use the redistribute OSPF command to transfer the VPN information learnt from the CE end to other PE peers.

The configuration steps on the PE are as below:

Command	Meaning
config terminal	
router ospf *ospf_id vrf_name* **match internal**	Configure an OSPF instance for the VRF and enter the OSPF configuration mode
Network prefix mask area *area_id*	Configure OSPF rotues.
redistribute bgp	Redistribute the BGP
Exit	Exit the OSPF configuration mode
router bgp asn	Configure the BGP protocol and enter the BGP configuration mode
addres-family ipv4 vrf *vrf_name*	Enter the address family mode of the VRF
redistribute ospf *ospf_id*	Redistribute the OSPF in the VRF address family mode to obtain the vpn information learnt from the CE end.
End	Return to the privileged mode
copy running-config startup-config	Save the configuration.

The configuration steps on the CE are as below:

Command	Meaning
config terminal	
router ospf *ospf_id*	Configure the OSPF instance and enter the OSPF configuration mode
network *prefix mask* **area** *area_id*	Configure OSPF routes
end	Return to the privileged mode
copy running-config startup-config	Save the configuration

43.1.8.3 Transferring the route information between PE-CE through static configuration

Usually in an simple network environment, you can use the static route. The configuration process is shown as below:

Command	Meaning

Command	Meaning
config terminal	
ip route vrf *vrf_name prefix mask gateway*	Configure the static route for the VRF
router bgp *asn*	Configure the BGP protocol and enter the BGP configuration mode
address-family ipv4 vrf *vrf_name*	Enter the address family mode of the VRF
redistribute static	Redistribute the static route
end	Return to the privileged mode
copy running-config startup-config	Save the configuration.

43.1.9 Configuring Static FTN and ILM Entry of L3VPN (Optional)

In general, it is the MP-BGP to assign the label for the private network, and the public network LSP is generated by the LDP protocol running on the public network. It can also carry out the label assign of the private network route and establish the LSP tunnel by configuring the static LSP. The configuration command and step of related FTN for L3 VPN on the PE is shown as follows:

Command	Meaning
configure terminal	Enter the global configuration mode.
mpls static l3vpn-ftn vrf-name fec-prefix/fec-mask out-label out_label remote-pe ipaddr	Configure a static private network FTN, whose outgoing interface is on other PEs.. At this time, it is necessary to specify the private network label and its outgoing PE. The address of this outgoing PE will be used to match with the LSP tunnel of the public network.
mpls static l3vpn-ftn vrf-name fec-prefix/fec-mask local-forward nexthop interface nexthop-ip	Configure a static private network FTN, whose outgoing interface is the PE itself. At this time, it is necessary to specify the outgoing interface of the local PE and the next hop address (In general, its outgoing interface and next hop is on another VRF).In general, this command can be used when more than one VRF is of the same VPN on the local PE.
End	Exit to the privileged mode.
copy running-config startup-config	Save the configuration.

The configuration commands and steps of the ILM for the L3 VPN on the PE are shown as follows:

Command	Meaning
configure terminal	Enter the global configuration mode.
mpls static ilm in-label *in_label* **forward-action pop-l3vpn-nexthop** *vrf-name* **nexthop interface nexthop-ip fec** *fec*	To configure the ILM item of L3 VPN on the PE, it is necessary to specify the incoming label, the outgoing interface and the next hop address.
end	Exit to the privileged mode.
copy running-config startup-config	Save the configuration.

Caution	Above only configures the static private network FTN and ILM, and it will be valid only when corresponding public network LSP tunnel is established. To establish the LSP tunnel of the public network, see the chapter *Basic Configuration Steps of MPLS*. It can establish the public network LSP tunnel by the LDP protocol or in the static configuration way.

43.1.10 Verifying L3 VPN Configuration

This section describes how to verify the L3VPN configuration and the VPN route information by performing the following steps.

Command	Meaning
show ip vrf [*vrf_name*]	Show the VRF configuration information
show ip bgp vpnv4 {*all* | *rd route-distinguish* | *vrf vrf_name*} [*network-address*][*summary*] [*neighbor*][*label*]	Show the VPN route information
show ip bgp summary	Show the status of all BGP connections
show ip route vrf vrf_name [*A.B.C.D*|*bgp*|*connected*|*count*|*isis*|*ospf*|*rip*|*static*|*weight*]	Show the related VRF route information

43.2 BGP/MPLS VPN Configuration Example

43.2.1 Intranet Configuration Example

Requirements: There are two VPN users, VPNA and VPNB. VPNA have its own sites in Fuzhou and Shanghai, and VPNB have its own sites in Beijing and Shanghai. Now the users in VPNA should be able to access the resources in Fuzhou and Shanghai, and those in VPNB can access the resources in Beijing and Shanghai. No mutual access is allowed between the two VPNs. See the figure below.

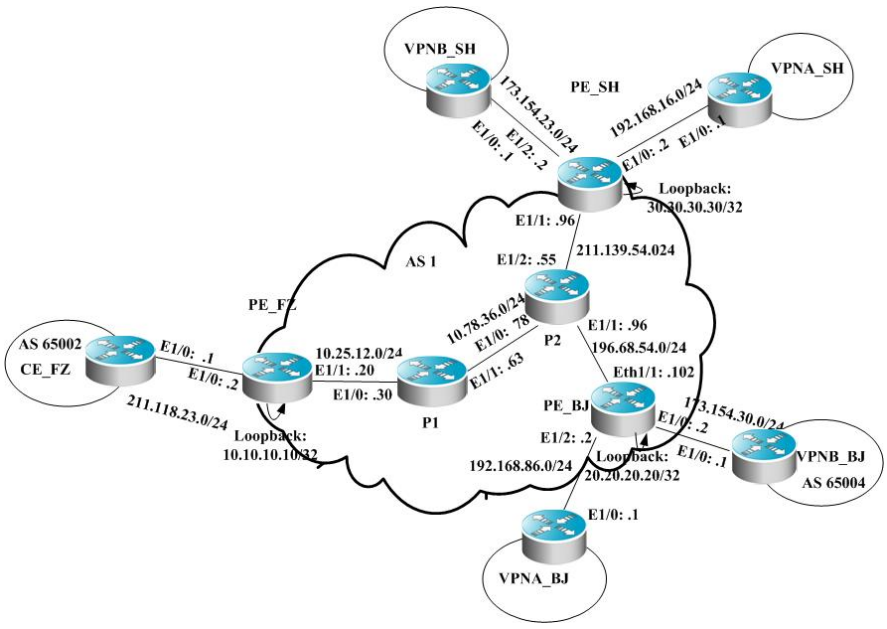


Figure 9

Configuration procedure:

1) Configuration of PE

Now take PE_SH as an example:

- **Configure the VRF**

  Define two VRFs on PE_SH, such as VRFA_SH and VRFB_SH, and define the R value and RT value. For two VRF definitions respectively, associate the VRF with corresponding interface.

#Define the VRF

```
ip vrf VRFA_SH
rd 1:100
route-target both 1:100
!
ip vrf VRFB_SH
rd 1:200
route-target both 1:200
```

#Associate the VRF with the interface

```
interface Ethernet 1/0
ip vrf forwarding VRFA_SH
ip address 192.168.16.2 255.255.255.0
!
interface Ethernet 1/2
ip vrf forwarding VRFB_SH
ip address 173.154.23.2 255.255.255.0
```

- **Configure the BGP protocol**

#Configure the PE peer

```
router bgp 1
neighbor 10.10.10.10 remote-as 1
neighbor 10.10.10.10 update-source loopback 0
!
neighbor 20.20.20.20 remote-as 1
neighbor 20.20.20.20 update-source loopback 0
!
address-family vpnv4 unicast
neighbor 10.10.10.10 activate
neighbor 20.20.20.20 activate
exit-address-family
```

#Configure the CE peer through the EBGP

```
address-family ipv4 vrf VRFA_SH
neighbor 192.168.16.1 remote-as 65003
neighbor 192.168.16.1 update-source eth1/0
exit-address-family
!
address-family ipv4 vrf VRFB_SH
neighbor 173.154.23.1 remote-as 65002
```

```
neighbor 173.154.23.1 update-source eth1/2
exit-address-family
```

- **Configure the backbone network routing protocol**

#Run the OSPF on the backbone network to transfer the route information

```
router ospf 10
network 10.25.12.0 0.0.0.255 area 0
network 10.10.10.10 0.0.0.0 area 0
```

#Configure the MPLS

```
mpls router ldp
interface Ethernet 1/1
ip address 211.139.54.96 255.255.255.0
label-switching
mpls ip
```

The PE_FZ and PE_BJ can be configured in similar ways as above.

2) Configure the CE

VPNB_SH is taken as an example:

- **Configure the BGP**

Configure the PE peer

```
router bgp 65002
neighbor 173.254.23.2 remote-as 1
neighbor 173.254.23.2 update-source eth1/0
redistribute ospf
```

The CE can be configured on the VPNA_SH, VPNA_FZ and VPNB_BJ in a similar way to that of VPNB_SH.

3) Configure the P

P1 is taken as example:

#Configuring the OSPF

```
router ospf 10
network 10.25.12.0 0.0.0.255 area 0
network 10.78.36.0 0.0.0.255 area 0
```

#Configure the MPLS

```
mpls router ldp
interface Ethernet1/0
ip address 10.25.12.24 255.255.255.0
label-switching
mpls ip
```

```
interface Ethernet1/1

ip address 10.78.36.63 255.255.255.0

label-switching

mpls ip
```

The configuration on P2 is similar to P1.

43.2.2 Extranet configuration example

Requirements: There are two VPN users, VPNA and VPNB. Mutual access should be implemented within the VPN, but is not allowed between these two. These VPNs can access some shared resources. See the figure below.

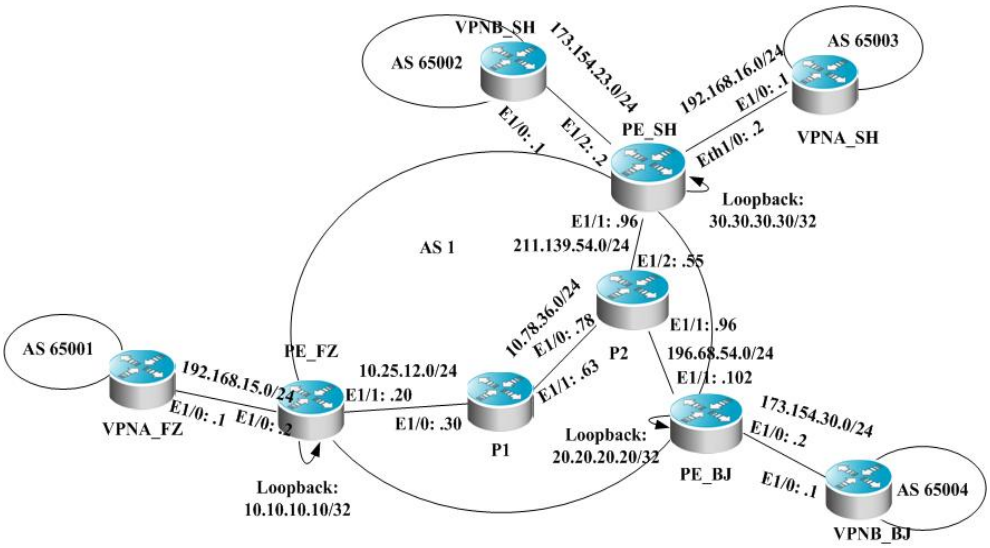


Figure 10

Configuration steps:

PE_SH:

- **Configure the VRF**

```
!

ip vrf VPNA_SH

rd 1:100

route-target both 1:100

!

ip vrf VPNB_SH

rd 1:200

route-target both 1:200
```

#Associate the VRF with the interface

```
interface Ethernet 1/0
ip vrf forwarding VRFA_SH
ip address 192.168.16.2 255.255.255.0
!
interface Ethernet 1/2
ip vrf forwarding VRFB_SH
ip address 173.154.23.2 255.255.255.0
```

- **Configure the OSPF to run between the PE and CE**

#Run the OSPF protocol between PE_SH and VPNA_SH

```
router ospf 10 VRFA_SH
network 192.168.16.0 0.0.0.255 area 10
redistribute bgp
```

#Run the OSPF protocol between PE_SH and VPNB_SH

```
router ospf 20 VRFB_SH
network 173.154.23.0 0.0.0.255 area 20
redistribute bgp
```

- **Configure the BGP**

Configure the PE peer

```
router bgp 1
neighbor 10.10.10.10 remote-as 1
neighbor 10.10.10.10 update-source Loopback 0
neighbor 20.20.20.20 remote-as 1
neighbor 20.20.20.20 update-source Loopback 0
!
address-family vpnv4 unicast
neighbor 10.10.10.10 activate
neighbor 20.20.20.20 activate
exit-address-family
```

#Receive the route information of the CE end by redistributing the OSPF

```
address-family ipv4 vrf VRFA_SH
redistribute ospf
```

```
exit-address-family
!
address-family ipv4 vrf VRFB_SH
redistribute ospf
exit-address-family
```

- **Configure the backbone network routing protocol**

#Configuring the OSPF

```
router ospf 30
network 211.139.54.0 0.0.0.255 area 0
network 30.30.30.30 0.0.0.0 area 0
```

#Configure the MPLS

```
mpls router ldp
interface Ethernet1/1
ip address 211.139.54.96 255.255.255.0
label-switching
mpls ip
PE_FZ:
```

- **Configure the VRF**

```
ip vrf VRF_FZ
rd 1:300
route-target export 1:100
route-target export 1:200
```

#Associate the VRF with the interface

```
interface Ethernet 1/0
ip vrf forwarding VRF_FZ
ip address 211.118.23.2 255.255.255.0
```

- **Configure the BGP**

Configure the PE peer

```
router bgp 1
neighbor 20.20.20.20 remote-as 1
neighbor 20.20.20.20 update-source Loopback 0
```

```
neighbor 30.30.30.30 remote-as 1

neighbor 30.30.30.30 update-source Loopback 0

!

address-family vpnv4 unicast

neighbor 20.20.20.20 activate

neighbor 30.30.30.30 activate

exit-address-family
```

#Configure the CE peer through the EBGP

```
address-family ipv4 vrf VRF_FZ

neighbor 211.118.23.1 remote-as 65002

neighbor 192.168.1.1 update-source Ethernet 1/0

exit-address-family
```

#Configure the backbone network routing protocol

```
!OSPF

router ospf 10

network 10.25.12.0 0.0.0.255 area 0

network 10.10.10.10 0.0.0.0 area 0
```

#Configure the MPLS

```
mpls router ldp

interface Ethernet1/1

ip address 12.25.12.20 255.255.255.0

label-switching

mpls ip

VPNB_SH:
```

Configuring the OSPF

```
!

router ospf 1

network 173.254.23.0 0.0.0.255 area 20
```

The VPNA_SH configuration is similar to that of PNB_SH.

The protocol between the PE_BJ and VPNA_BJ, VPNB_BJ can be the EBPG or the OSPF, RIP or other routing protocols selected to suit the practical needs.

The configuration solution of P1 and P2 is similar to that of P1 and P2 in the first configuration example.

43.2.3 Hub-and-Spoke configuration example

Requirements: The data within the VPN cannot be exchanged directly, but must be exchanged through a unified control center. Only this control center learns all the information resources in the VPN. Other users in the VPN obtain the resources in the VPN through the control center. As shown in the following diagram, the VPNB_FZ can access the resources of VPNB_BJ only through the VPNB_SH.

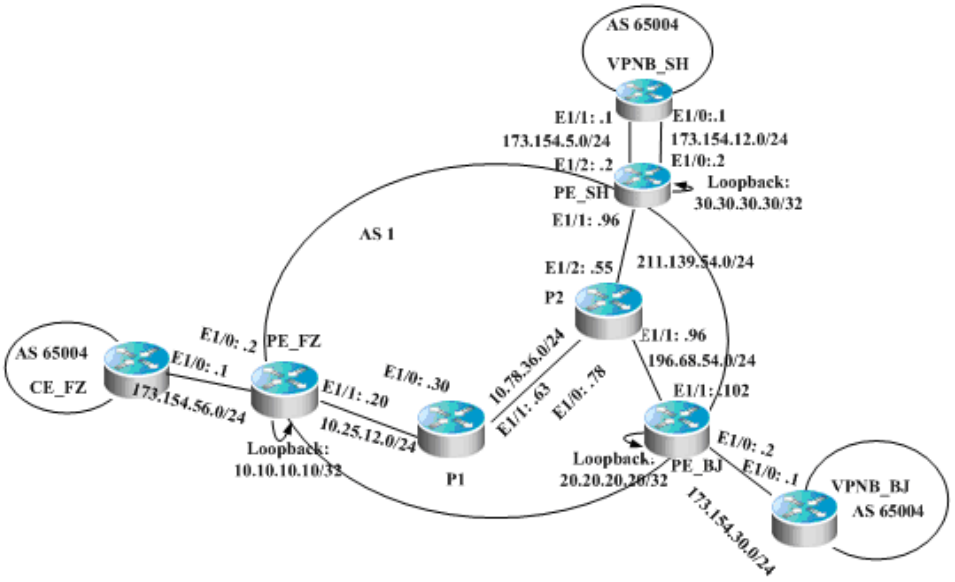


Figure 11

Configuration steps:

PE_FZ:

- **Configure the VRF**

```
!
ip vrf VRFB_FZ
rd 1:100
route-target both 1:100
!
```

#Associate the VRF with the interface

```
interface Ethernet 1/0
ip vrf forwarding VRFB_FZ
ip address 173.154.56.2 255.255.255.0
```

- **Configure the BGP**

#Configure the PE Peer

```
router bgp 1
neighbor 30.30.30.30 remote-as 1
```

```
neighbor 30.30.30.30 update-source loopback 0
!
address-family vpnv4 unicast
neighbor 30.30.30.30 activate
neighbor 30.30.30.30 allowas-in
exit-address-family
```

!

#Configure the PE Peer

```
address-family ipv4 vrf VRFB_FZ
neighbor 173.154.56.1 remote-as 65004
neighbor 173.154.56.1 update-source Ethernet 1/0
neighbor 173.154.56.1 as-override
exit-address-family
```

- **Configure the backbone network routing protocol**

```
!OSPF
router ospf 10
network 10.25.12.0 0.0.0.255 area 0
network 10.10.10.10 0.0.0.0 area 0
!MPLS
mpls router ldp
interface Ethernet1/1
ip address 10.25.12.20 255.255.255.0
label-switching
mpls ip
PE_BJ:
```

- **Configure the VRF**

```
!
ip vrf VRFB_BJ
rd 1:100
route-target both 1:200
!
```

#Associate the VRF with the interface

```
interface Ethernet 1/0
ip vrf forwarding VRFB_BJ
ip address 173.154.30.2 255.255.255.0
```

- **Configure the BGP**

#Configure the PE Peer

```
router bgp 1
neighbor 30.30.30.30 remote-as 1
neighbor 30.30.30.30 update-source loopback 0
!
address-family vpnv4 unicast
neighbor 30.30.30.30 activate
neighbor 30.30.30.30 allowas-in
exit-address-family
```

Configure the CE Peer

```
address-family ipv4 vrf VRFB_BJ
neighbor 173.154.30.1 remote-as 65004
neighbor 173.154.30.1 update-source Ethernet 1/0
neighbor 173.154.30.1 as-override
exit-address-family
```

- **Configure the backbone network routing protocol**

```
!OSPF
router ospf 10
network 196.68.54.0 0.0.0.255 area 0
network 20.20.20.20 0.0.0.0 area 0
!MPLS
mpls router ldp
interface Ethernet1/1
ip address 196.68.54.102 255.255.255.0
label-switching
mpls ip
PE_SH:
```

- **Configure the VRF**

```
!
ip vrf VRFB_SPOKE
rd 1:300
route-target import 1:100
route-target import 1:200
!
```

```
ip vrf VRFB_HUB

rd 1:400

route-target export 1:100

route-target export 1:200
```

Associate the VRF with the interface

```
interface Ethernet 1/0

ip vrf forwarding VRFB_SPOKE

ip address 173.154.12.2 255.255.255.0

!

interface Ethernet 1/2

ip vrf forwarding VRFB_HUB

ip address 173.154.5.2 255.255.255.0
```

- **Configure the BGP**

#Configure the PE Peer

```
router bgp 1

neighbor 10.10.10.10 remote-as 1

neighbor 10.10.10.10 update-source loopback 0

neighbor 20.20.20.20 remote-as 1

neighbor 20.20.20.20 update-source loopback 0

!

address-family vpnv4 unicast

neighbor 10.10.10.10 activate

neighbor 20.20.20.20 activate

exit-address-family
```

#Configure the CE Peer

```
address-family ipv4 vrf VRFB_SPOKE

neighbor 173.154.5.1 remote-as 65004

neighbor 173.154.5.1 update-source Ethernet 1/2

neighbor 173.154.5.1 as-override

exit-address-family

!

address-family ipv4 vrf VRFB_HUB

neighbor 173.154.12.1 remote-as 65004

neighbor 173.154.12.1 update-source Ethernet 1/0
```

```
neighbor 173.154.12.1 allowas-in

exit-address-family
```

- **Configure the backbone network routing protocol**

```
!OSPF

router ospf 10

network 211.139.54.0 0.0.0.255 area 0

network 30.30.30.30 0.0.0.0 area 0

!MPLS

mpls router ldp

interface Ethernet1/1

ip address 211.139.54.96 255.255.255.0

label-switching

mpls ip

VPNB_SH:
```

- **Configure the BGP**

```
router bgp 65004

neighbor 173.154.5.2 remote-as 1

neighbor 173.154.5.2 update-source Ethernet1/1

neighbor 173.154.12.2 remote-as 1

neighbor 173.154.12.2 update-source Ethernet1/0

redistribute ospf
```

The configuration of other CEs is similar to the configuration of VPNB_SH. The router configuration in the backbone network is similar to configuration example 1. You can refer to configuration example 1.

44 Port-based Flow Control Configuration

44.1 Storm Control

44.1.1 Overview

Too many broadcast, multicast or unknown unicast packets in the LAN will slow the network speed and increase the possibility of packet transmission timeout significantly. This is called LAN storm. Protocol stack implementation errors or wrong network configuration may lead to such storms.

Storm control can be conducted upon the broadcast, multicast and unknown unicast data streams respectively. When the rate of the broadcast, multicast or unknown unicast packets received by the interface exceeds the specified bandwidth throttling, the device only allows the packets within the bandwidth throttling. The packets that exceed the throttle will be discarded until the data stream becomes normal again. This prevents excessive flooding packets from entering the LAN to form a storm.

44.1.2 Configuring Storm Control

In the interface configuration mode, use the following command to configure storm control:

Command	Function
DES-7210(config-if)# **storm-control** {**broadcast** | **multicast** | **unicast**} [{ **level** *percent* | **pps** *packets* | *rate-bps*]	**broadcast**: Enable the broadcast storm control function. **multicast**: Enable the unknown multicast storm control function. **unicast**: Enable the unknown unicast storm control function. *percent:* Set according to the bandwidth percentage, for example, 20 means 20% *packets*: Set according to the pps, which means packets per second *Rate-bps*: rate allowed

In the interface configuration mode, you can disable the storm control on the appropriate interface by using the **no storm-control broadcast**, **no storm-control multicast**, or n**o storm-control unicast** command.

The following example enables the multicast storm control on GigabitEthernet 0/1 and set the allowed rate as 4M.

```
DES-7210# configure terminal
DES-7210(config)# interface GigabitEthernet 0/1
DES-7210(config-if)# storm-control multicast 4096
DES-7210(config-if)# end
```

Note

By default, for the DES-7200 series, the storm control function for broadcast, multicast and unknown unicast packets is disabled

Caution

1. The DES-7200 series does not support **storm-control action.**
2. For the DES-7200 series, the level-based storm control has certain errors for the packets in the length of more than 64 bytes. The longer the packet length is, the greater the comparable error value is. The error formula is (packet length-64)/84.
3. The reference bandwidth for the level-based storm control is the maximum bandwidth supported by the physical port, but not converted from the bandwidth of the physical port in service.
4. If you enable storm control with the **storm-control broadcast** command, the default setting or 14880PPS is used.

44.1.3 Viewing the Enable Status of Storm Control

To view the storm control status of the interface, use the following command:

Command	Function
DES-7210# **show storm-control** [*interface-id*]	Show storm control information.

The instance below shows the enabled status of the storm control function of interface Gi1/3:

```
DES-7210# show storm-control gigabitEthernet 0/3
Interface  Broadcast Control  Multicast Control  Unicast Control action
GigabitEthernet 0/3 Disabled  Disabled   Disabled    none
```

You can also view the enabling status of the storm control function of all interfaces at a time:

```
DES-7210# show storm-control
Interface  Broadcast Control  Multicast Control  Unicast Control Action
---------  ------------------ ------------------ ------- ------- ------
GigabitEthernet 0/1   Disabled   Disabled   Disabled   none
GigabitEthernet 0/2   Disabled   Disabled   Disabled   none
GigabitEthernet 0/3   Disabled   Disabled   Disabled   none
GigabitEthernet 0/4   Disabled   Disabled   Disabled   none
GigabitEthernet 0/5   Disabled   Disabled   Disabled   none
GigabitEthernet 0/6   Disabled   Disabled   Disabled   none
GigabitEthernet 0/7   Disabled   Disabled   Disabled   none
GigabitEthernet 0/8   Disabled   Disabled   Disabled   none
GigabitEthernet 0/9   Disabled   Disabled   Disabled   none
GigabitEthernet 0/10  Disabled   Disabled   Disabled   none
GigabitEthernet 0/11  Disabled   Disabled   Disabled   none
GigabitEthernet 0/12  Disabled   Disabled   Disabled   none
GigabitEthernet 0/13  Disabled   Disabled   Disabled   none
GigabitEthernet 0/14  Disabled   Disabled   Disabled   none
GigabitEthernet 0/15  Disabled   Disabled   Disabled   none
GigabitEthernet 0/16  Disabled   Disabled   Disabled   none
```

```
GigabitEthernet 0/17  Disabled   Disabled   Disabled   none
GigabitEthernet 0/18  Disabled   Disabled   Disabled   none
GigabitEthernet 0/19  Disabled   Disabled   Disabled   none
GigabitEthernet 0/20  Disabled   Disabled   Disabled   none
GigabitEthernet 0/21  Disabled   Disabled   Disabled   none
GigabitEthernet 0/22  Disabled   Disabled   Disabled   none
GigabitEthernet 0/23  Disabled   Disabled   Disabled   none
GigabitEthernet 0/24  Disabled   Disabled   Disabled   none
```

44.2 Protected Port

44.2.1 Overview

In some application environments, some ports are not required to communicate with each other on a device. In such case, frame forwarding is not allowed between the protected ports, no mattter the frames are unicast frames, broadcast frames or multicast frames. To achieve this purpose, you can set some ports as protected ports.

Once ports are set as protected ports, they cannot communicate with each other. However, protected ports can still communicate with unprotected ports.

There are two protected port modes: one is to block layer 2 forwarding between protected ports but allow layer 3 routing; the other is to block layer 2 forwarding and layer 3 routing between protected ports. The first mode is by default when both modes are supported.

When you set two protected ports as a SPAN port pair, the frames transmitted or received by the source port of SPAN are sent to the destination port of SPAN according to the SPAN setting. Therefore, it is not recommended to set the destination port of SPAN as the protected port (and you can also save system resources by doing so).

The device supports setting the Aggregated Port as the protected port. Once you do that, all the member ports of the Aggregated Port will be set as the protected port.

44.2.2 Configuring the Protected Port

Set one port as the protected port:

Command	Function
DES-7210(config-if)# **switchport protected**	Set this interface as a protected port

You can reset a port as unprotected port with the **no switchport protected** command in the interface configuration mode.

The following example describes how to set the Gigabitethernet 0/3 as the protected port.

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitethernet 0/3
DES-7210(config-if)# switchport protected
DES-7210(config-if)# end
```

44.2.3 Showing Protected Port Configuration

Command	Function
DES-7210(config-if)# **show interfaces switchport**	Show the configuration of the switching port

You can use the command of **show interfaces switchport** to view the configuration of protected port.

```
DES-7210# show interfaces gigabitethernet 0/3 switchport
Interface   Switchport  Mode   Access Native Protected   VLAN lists
---------   ----------  ----   ------ -----  --------   ----
GigabitEthernet 0/3  enabled   Trunk  1   1    Enabled    ALL
```

44.3 Port Security

44.3.1 Overview

Port security function allows the packets to enter the switch port by the source MAC address, source MAC+IP address or source IP address. You can control the packets by setting the specific MAC address statically, static IP+MAC binding or IP binding, or dynamically learning limited MAC addresses. The port with port security enabled is named as secure port. Only the packets with the source MAC address in the port security address table, or IP+MAC binding configured, or IP binding configured, or the learned MAC address, can join the switch communication, while other packets are dropped.

To enhance security, you can bind the MAC address with the IP address as the secure address. Of course you can also designate the MAC address without binding the IP address.

You can add the secure addresses on the port in the following ways:

- You can manually configure all the secure addresses of the port by using the commands in the interface configuration mode.
- You can also let this port automatically learn these addresses, which will become the secure address on this port till the total number reaches the maximum value. Note that, however, the automatically-learned secure addresses will not be bound with the IP address. On the same port, if you have configured a secure address bound with the IP address, the port cannot be added with any secure address by automatic learning.
- Manually configure some secure addresses, and let the device to learn the rest.

When a port is configured as a secure port and the maximum number of its secure addresses is reached, a security violation occurs if the port receives a packet whose source address is not one of the secure addresses on the port. When security violations occur, you can set the following methods to handle:

- **protect:** When the maximum number of secure addresses is reached, the secure port discards the packet of unknown addresses (none of which are among the secure addresses of the port).This is the default method for handling exceptions.
- **restrict:** In the case of violation, a Trap notification is sent
- **shutdown:** In the case of violation, the port is shut down and a Trap notification is sent.

44.3.2 Configuring Port Security

44.3.2.1 Default Configuration of Port Security

The table below shows the default configuration of port security:

Item	Default Configuration
Port security switch	The port security function is disabled for all the ports.
Maximum number of secure addresses	128

Item	Default Configuration
Secure address	None
Handling mode for violations	Protect

44.3.2.2 Port Security Configuration Guide

The following restrictions apply to port security configuration:

- A secure port is not an Aggregate Port.
- A secure port is not the destination port of SPAN.
- A secure port is and can only be an Access Port.

The 802.1x authentication and port security are mutually exclusive in enabling. The 802.1x authentication and port security can ensure the validity of the network users. You can enable either of them to control port access.

At the same time, the secure addresses of the IP+MAC addresses and IP addresses share with the ACLs the hardware resources of the system. Therefore, when you apply the ACLs on one secure port, the IP+MAC addresses and IP addresses on the port can be configured with less secure addresses.

The secure addresses for the same secure port must have the same format, namely either all or none of them are bound with IP addresses. If a security port includes these two types of security addresses at the same time, the secure address not bound with the IP address will fail (the secure address bound with the IP address has a high priority).

44.3.2.3 Configuration of Secure Ports and Violation Handling Modes

In the interface configuration mode, configure secure ports and violation handling modes by using the following commands:

Command	Function
DES-7210(config-if)# **switchport port-security**	Enable the port security function of this interface.
DES-7210(config-if)# **switchport port-security maximum** *value*	Set the maximum number of secure addresses on the interface. The range is between 1 and 1000 and the default value is 128.
DES-7210(config-if)# **switchport port-security violation**{**protect** | **restrict** | **shutdown**}	Set the violation handling mode: **protect**: Protected port. When the number of secure addresses if full, the security port will discard the packets from unknown address (that is, not any among the secure addresses of the port). **restrict**: In the case of violation, a Trap notification is sent **shutdown**: In the case of violation, the port is shut down and a Trap notification is sent. When a port is closed because of violation, you can recover it from the error status by using the **errdisable recovery** command in the global configuration mode.

In the interface configuration mode, you can disable the port security function of an interface with the command no switchport port-security. Use the command no switchport port-security maximum to recover to the default maximum value. Use the command no switchport port-security violation to set violation handling to the default mode.

The instance below describes how to enable the port security function on interface gigabitethernet 0/3. The maximum number of addresses to be set is 8 and the violation handling mode is set as protect.

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitethernet 0/3
DES-7210(config-if)# switchport mode access
DES-7210(config-if)# switchport port-security
DES-7210(config-if)# switchport port-security maximum 8
DES-7210(config-if)# switchport port-security violation protect
DES-7210(config-if)# end
```

Note

1. If the secure address MAC+IP has been configured on the secure port, when the number of the learned MAC address has reached and exceeded the number of secure addresses, the port violation will not occur.
2. The trap message and log prompts only when the port violation occurs for the first time.
3. The time from the occurrence of L2 port violation to the handling completion is within 1s.

Caution

For the port with secure channel configured (configure the global secure channel and non-secure channel exceptional port, or configure the port secure channel), if the port security is enabled at the same time, and the secure users are all MAC users, then the port security takes no effecet, and the non-secure user will not be dropped after the violation triggering. To this end, you shall not only configure the port security for MAC address on the port with secure channel enabled.

44.3.2.4 Configuration of Secure Addresses on the Secure Port

In the interface configuration mode, add secure addresses for secure ports by using the following commands:

Command	Function
DES-7210(config-if)# **switchport port-security mac-address** *mac-address* [**ip-address** *ip-address* | *ipv6-address*]	Manually configure the secure address on the interface. **ip-address** (optional): IP(IPv6) address bound with the secure address.

In the interface configuration mode, you can use the command **no switchport port-security mac-address** *mac-address* to delete the secure address of this interface.

The example below describes how to configure a secure address for interface gigabitethernet 0/3: 00d0.f800.073c and bind it with an IP address: 192.168.12.202.

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitethernet 0/3
DES-7210(config-if)# switchport mode access
DES-7210(config-if)# switchport port-security
DES-7210(config-if)# switchport port-security mac-address 00d0.f800.073c ip-address
192.168.12.202
DES-7210(config-if)# end
```

44.3.2.5 Configuration of Aging Time for Secure Addresses

You can configure the aging time for all the secure addresses on an interface. To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the device automatically add or delete the secure addresses on the interface.

In the interface configuration mode, configure the aging time for secure addresses by using the following command:

Command	Function
DES-7210(config-if)#**switchport port-security aging**{**static** | **time** *time* }	**Static**: When this keyword is added, the aging time will be applied to both the manually configured secure address and automatically learnt addresses. Otherwise, it is applied only to the automatically learnt addresses. **Time**: indicates the aging time for the secure address on this port. Its range is 0-1440 and unit is Minute. If you set it to be 0, the aging function actually is disabled. The aging time is the absolute time, which means that an address will be deleted automatically after the *Time* specified expires after the address becomes the secure address of the port. The default value of *Time* is 0.

In the interface configuration mode, use **no switchport port-security aging time** to disable the port security aging. Use the **no switchport port-security aging static** to apply the aging time only to dynamically learned security address.

The example below describes how to configure the port security aging time on interface Gigabitethernet 0/3. The aging time is set to 8 minutes and it is applicable to statically-configured secure addresses:

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210(config)# interface gigabitthernet 0/3
DES-7210(config-if)# switchport port-security aging time 8
DES-7210(config-if)# switchport port-security aging static
DES-7210(config-if)# end
```

44.3.3 Viewing Port Security Information

In the privileged mode, you can view the security information of a port by using the following commands.

Command	Function
DES-7210#**show port-security interface** [*interface-id*]	View the port security configuration of an interface.
DES-7210#**show port-security address**	View the secure address information.
DES-7210# **show port-security address** [*interface-id*]	Show the secure address information on an interface.
DES-7210# **show port-security**	Show the statistics of all the security ports, including the maximum number of secure addresses, the number of current addresses, and violation handling mode.

The example below shows the port security configuration on interface **gigabitethernet 0/3**:

```
DES-7210# show port-security interface gigabitethernet 0/3
Interface Gi0/3
Port Security: Enabled
Port status : down
Violation mode:Shutdown
Maximum MAC Addresses:8
Total MAC Addresses:0
Configured MAC Addresses:0
Aging time : 8 mins
SecureStatic address aging : Enabled
```

The instance below shows all the secure addresses in the system.

```
DES-7210# show port-security address
Vlan Mac Address IP Address Type Port Remaining Age(mins)
---------------------------------------- ------------------
1  00d0.f800.073c   192.168.12.202    Configured   Gi0/3     8
1  00d0.f800.3cc9   192.168.12.5      Configured   Gi0/1     7
```

You can also only show the secure address on one interface. The instance below shows the secure address on interface gigabitsethernet 0/3.

```
DES-7210# show port-security address interface gigabitethernet 0/3
Vlan Mac Address IP Address Type Port Remaining Age(mins)
---- --------------- ---------- ------ ------------------
1    00d0.f800.073c  192.168.12.202 Configured Gi0/3    8
```

The example below shows the statistic information of the secure port.

```
DES-7210# show port-security
Secure Port MaxSecureAddr(count) CurrentAddr(count) Security Action
-------- -----------------  -----------------  ------------
Gi0/1       128                 1               Restrict
Gi0/2       128                 0               Restrict
Gi0/3       8                    1              Protect
```

44.4 ARP-CHECK

44.4.1 Overview

ARP-CHECK is MAC+IP binding security function based on global or port, such as DHCP Snooping, port security or global address binding. It prevents ARP spoof effectively by discarding ARP packet of illegal user, such as preventing illegal information station from passing itself off as the IP of important network device(eg:server) and network communication disorder.

There are three modes of ARP-CHECK: enabled, disabled and auto mode. The auto mode is by default.

In the enabled mode, ARP check is enabled no matter whether there is security configuration. If there is no legal user on the port, all the arp packets from this port will be discarded.

In the disabled mode, ARP packet on the port is not checked.

In the auto mode, ARP packet is checked when there is no legal user on the port; and vice versa.

ARP-CHECK restriction:

1. Enabling ARP check of port security addresses will decrease the maximum number of the security addresses of binding IP on all the ports by half.

2. Enabling ARP check of port security addresses is not effective for the security addresses that have already existed. If you want those configured security addresses take effect, you can close and then enable them again. ARP check uses policy management module, sharing hardware resources with other modules. If the hardware resource is not enough, ARP check of part of port security addresses may not take effective.

3. When there are many MAC+IP security address entries, enabling ARP Check Cpu influences a lot on CPU performances.

44.4.2 Configuring ARP-CHECK

Use the following commands to configure ARP-CHECK in the privileged mode:

Command	Action
DES-7210# **configure t**	Enter the global configuration mode.
DES-7210(config)#**interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config-if)# **arp-check**	Enable arp check.
DES-7210(config-if)# **no arp-check**	Disable arp check.
DES-7210(config-if)#**arp-check auto**	Restore to the default configuration: enabled.

The example below shows that the ARP check is auto-enabled on the port when adding legal mac address 00d0.f822.33ab and IP address 192.168.2.5:

```
DES-7210#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# interface fastEthernet 0/5
DES-7210(config-if)# switchport port-security
DES-7210(config-if)# switchport port-security mac-address 00d0.f822.33ab ip-address
192.168.2.5
```

Thus, ARP check is auto-enabled. Use this command to disable ARP check.

```
DES-7210(config-if)# no arp-check
```

45 802.1x Configuration

This chapter describes the contents related to the AAA service configurations. The 802.1x is used to control the authentication over network access of users, and provide authorization and accounting functions for users.

This chapter includes:

- Overview
- Configuring 802.1x
- Viewing the Configuration and Current Statistics of the 802.1x
- Other Precautions for Configuring 802.1x

Note

For details about usage and descriptions of the CLI commands used in this section, please refer to *Configuring 802.1X command*.

45.1 Overview

In an IEEE 802 LAN, users can access the network device without authorization and authorization as long as they are connected to the network device. Therefore, an unauthorized user can access the network unobstructed by connecting the LAN. As the wide application of LAN technology , particularly the appearance of the operating network, it is necessary to address the safety authentication needs of the network. It has become the focus of concerns in the industry that how to provide user with the authentication on the legality of network or device access on the basis of simple and cheap Ethernet technologies. The IEEE 802.1x protocol is developed under such a context.

As a Port-Based Network Access Control standard, **the IEEE802.1x** provides LAN access point-to-point security access. Specially designed by the IEEE Standardization Commission to tackle the safety defects of Ethernet, this standard can provide a means to authenticate the devices and users connected to the LAN by utilizing the advantages of IEEE 802 LAN.

The IEEE 802.1x defines a mode based on Client-Server to restrict unauthorized users from accessing the network. Before a client can access the network, it must first pass the authentication of the authentication server.

Before the client passes the authentication, only the EAPOL (Extensible Authentication Protocol over LAN) packets can be transmitted over the network. After successful authentication, normal data streams can be transmitted over the network.

By using 802.1x, our switches provide Authentication, Authorization, and Accounting (AAA).

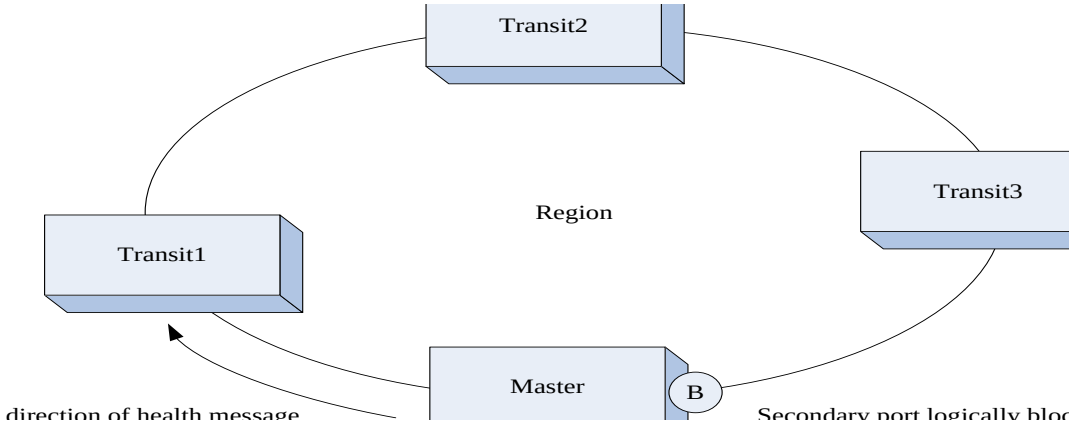
- Authentication: It is used to determine whether a user has the access, restricting illegal users.
- Authorization: It authorizes the services available to users, controlling the rights of valid users.
- Accounting: It records users' use of network resources, providing the supporting data for charging.

The 802.1x is described in the following aspects as below:

- Device Roles
- Authentication Initiation and Packet Interaction During Authentication
- States of Authorized Users and Unauthorized Users
- Topologies of Typical Applications

45.1.1 Device Roles

In the IEEE802.1x standard, there are three roles: **supplicant, authenticator, and authentication server.** In practice, they are the Client, network access server (NAS) and Radius-Server.



- Supplicant:

The **supplicant** is a role played by the end user, usually a PC. It requests for the access to network services and acknowledges the request packets from the authenticator. The supplicant must run the IEEE 802.1x client. Currently, the most popular one is the IEEE802.1x client carried by Windows XP. In addition, we have also launched the STAR Supplicant software compliant of this standard.

- Authenticator:

The **authenticator** is usually an access device like the switch. The responsibility of the device is to control the connection status between client and the network according to the current authentication status of that client. Between the client and server, this device plays the role of a mediator, which requests the client for username, verifies the authentication information from the server, and forwards it to the client. Therefore, the switch acts as both the IEEE802.1x authenticator and the RADIUS Client, so it is referred to as the network access server (NAS). It encapsulates the acknowledgement received from the client into the RADIUS format packets and forwards them to the RADIUS Server, while resolving the information received from the RADIUS Server and forwards the information to the client.

The device acting as the authenticator has two types of ports: controlled Port and uncontrolled Port. The users connected to a controlled port can only access network resources after passing the authentication, while those connected to a uncontrolled port can directly access network resources without authentication. We can control users by simply connecting them to an controlled port. On the other hand, the uncontrolled port is used to connect the authentication server, for ensuring normal communication between the server and switch.

- Authentication server:

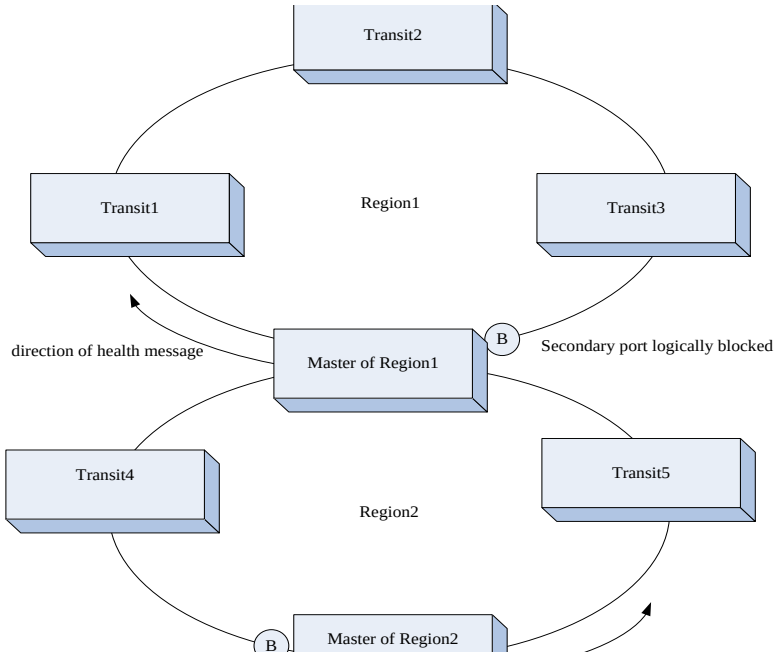
The **authentication server** is usually an **RADIUS** server, which works with the authenticator to provide users with authentication services. The authentication server saves the user name and password and related authorization information. One server can provide

authentication services for multiple authenticators, thus allowing centralized management of users. The authentication server also manages the accounting data from the authenticator. Our 802.1x device is fully compatible with the standard Radius Server, for example, the Radius Server carried on Microsoft Win2000 Server and the Free Radius Server on Linux.

45.1.2 Authentication Initiation and Packet Interaction During Authentication

The supplicant and the authenticator exchange information by EAPOL protocol, while the authenticator and authentication server exchange information by RADIUS protocol, completing the authentication process with such a conversion. The EAPOL protocol is encapsulated on the MAC layer, with the type number of 0x888E. In addition, the standard has required for an MAC address (01-80-C2-00-00-03) for the protocol for packet exchange during the initial authentication process.

The following diagram shows a typical authentication process, during which the three role devices exchange packets with one another.



This is a typical authentication process initiated by users (in some special cases, the switch can actively initiate authentication request, whose process is the same as that shown in the diagram, except that it does not contain the step where the user actively initiates the request).

45.1.3 States of Authorized Users and Unauthorized Users

The 802.1x determines whether the users on the port are allowed to access the network according to the authentication status of the port. Since we expand the 802.1X based on users, we determine whether a user is allowed to access network resources according to the authentication status of that user under a port. All users under an uncontrolled port can use network resources, while those under a controlled port can access network resources only if they are authorized. When a user just initiates an authentication request, its status is unauthorized, in which case it cannot access the network. When the authentication is passed, its status changes to be authorized, in which case it can use the network resources.

If the workstation does not support 802.1x while the machine is connected with the controlled port, when the equipment requests the username of the user, the workstation will not respond to the request due to no support. This means that the user is still unauthorized and cannot access the network resources.

On the contrary, if the client supports 802.1x, while the connected switch does not: The EAPOL-START frames from the user are not responded, and the user deems it connected port as an uncontrolled port and directly uses network resources, when the user fails to receive any response after it sends the specified number of EAPOL-START frames.

On a 802.1x-enabled device, all ports are uncontrolled ports by default. We can set a port as a controlled port, to impose authentication over all the users under that port.

When a user has passed authentication (the switch has received success packets from the RADIUS Server), the user is authorized and therefore can freely use network resources.If the user fails in the authentication and remains in the unauthenticated status, it is possible to initiate authentication once again. If the communication between the switch and the RADIUS server is faulty, the user is still unauthorized and therefore still cannot use the network.

When the user sends the EAPOL-LOGOFF packets, its status changes from authorized to unauthorized.

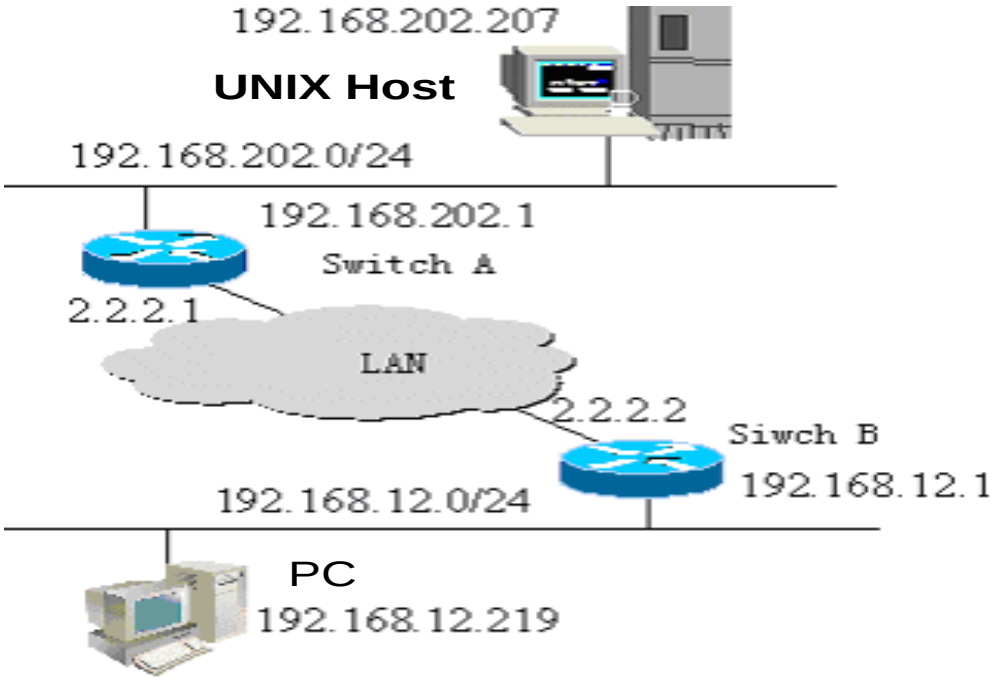
When a port of the switch changes to the LINK-DOWN status, all the users on the port change to the unauthorized status.

When the device restarts, all users on the device turn into the unauthorized status.

To force a user to pass the authentication, you can add a static MAC address.

45.1.4 Topologies of Typical Applications

A. The 802.1x-enabled device is used as the access layer device



This solution is described as below:

- Requirements of this solution:

1. The user supports 802.1x. That is, it is installed with the 802.1x client (Windows XP carried, Star-supplicant or other IEEE802.1x compliant client software).
2. The access layer device supports IEEE 802.1x.
3. One or multiple RADIUS compliant servers are available as the authentication server.

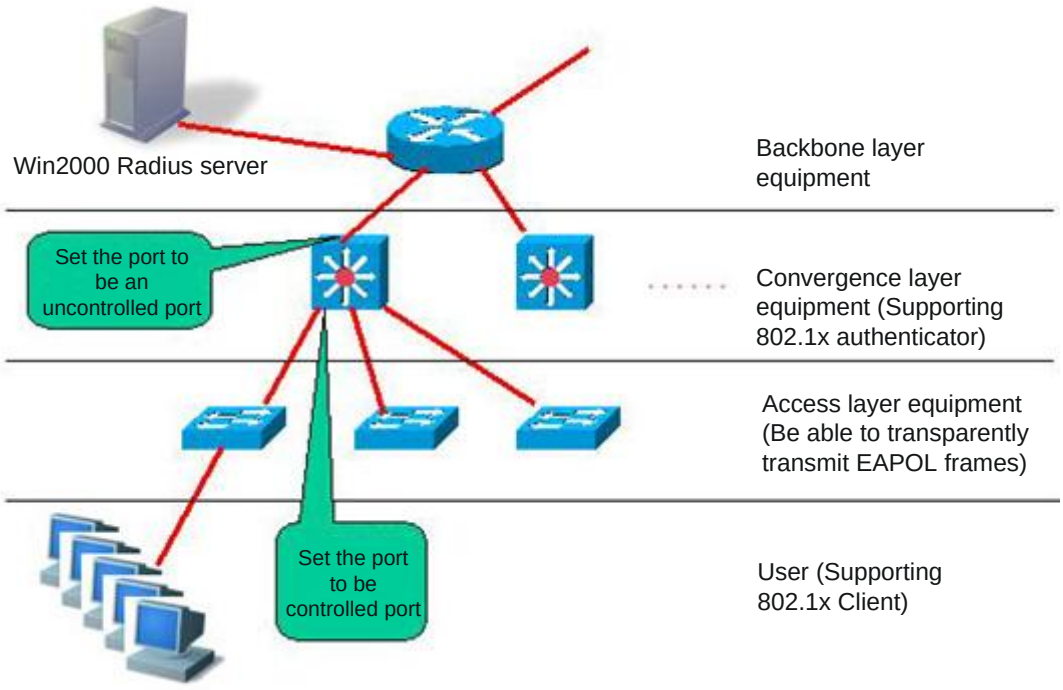
- Key points for configuration of this solution:

1. The ports connected to the Radius Server and the uplink ports are configured as **uncontrolled ports**, so that the switch can normally communicate with the server and the authorized users can access network resources through the uplink interface.
2. The ports connected to the user must be set as **controlled ports** to control the accessed users, and the users cannot access network resources unless they first pass the authentication.

- Characteristics of this solution:

1. Each 802.1x-enabled switch is responsible for a small number of clients, thus offering higher speed.The devices are mutually independent, and the restart operation of the device does not affect the users connected with other devices.
2. User management is performed on the Radius Server in a centralized manner. The administrator does not have to know which switch a user is connected to, making management much easier.
3. The administrator can manage the device on the access layer through the network.

B. The 802.1x-enabled device is used as the convergence layer device



This solution is described as below:

- Requirements of this solution:

1. The user supports 802.1x. That is, it is installed with the 802.1x client (Windows XP carried, Star-supplicant or other IEEE802.1x compliant client software).
2. The access layer device should be able to transparently transmit IEEE 802.1x. frames (EAPOL)
3. The convergence layer device supports 802.1x (playing the role of the authenticator)
4. One or multiple RADIUS compliant servers are available as the authentication server.

- Key points for configuration of this solution:

1. The ports connected to the Radius Server and the uplink ports are configured as uncontrolled ports, so that the switch can normally communicate with the server and the authorized users can access network resources through the uplink interface.
2. The ports connected to the access layer switches must be set as controlled ports to control the accessed users, and the users cannot access network resources unless they first pass the authentication.

- Characteristics of this solution:

1. The convergence layer device must be of high quality since the network is large and numerous users are connected, since any of its fault may cause the failures of many users to normally access the network.
2. User management is performed on the Radius Server in a centralized manner. The administrator does not have to know which switch a user is connected to, making management much easier.
3. The access layer device can be the less expensive non-NM switches (as long as they support transparent transmission of EAPOL frames).
4. The administrator cannot manage the device on the access layer through the network.

45.2 Configuring 802.1x

The following sections describe how to configure 802.1x.

- Default Configuration of 802.1x
- Precautions for Configuring 802.1x
- Configuring the communication between the device and Radius server
- Setting the 802.1X Authentication Switch
- Enabling/Disabling the Authentication of a Port
- Enabling Timed Re-authentication
- Changing the QUIET Time
- Setting the Packet Retransmission Interval
- Setting the Maximum Number of Requests
- Setting the Maximum Number of Re-authentications
- Setting the Server-timeout
- Configuring the device to initiate the 802.1x authentication proactively
- Configuring 802.1x Accounting
- Configuring the IP authorization mode
- Releasing Advertisement
- List of Authenticable Hosts under a Port
- Authorization
- Configuring the Authentication Mode
- Configure the backup authentication server.
- Configuring and Managing Online Users
- Implementing User-IP Binding

- Port-based Traffic Charging
- Implementing Automatic Switching and Control of VLAN
- Implementing GUEST VLAN
- Shielding Proxy Server and Dial-up
- Configuring On-line Client Probe
- Configuring the Option Flag for EAPOL Frames to Carry TAG
- Configuring Port-based User Authentication
- Configuring Port-based Single User Authentication
- Configuring Dynamic ACL Assignment

45.2.1 Default Configuration of 802.1x

The following table lists some defaults of the 802.1x

Item	Default
Authentication	DISABLE
Accounting	DISABLE
Radius Server *ServerIp *Authentication UDP port *Key	*No default *1812 *No default
Accounting Server *ServerIp *Accounting UDP port	*No default *1813
All port types	Uncontrolled port (all ports can perform communication directly without authentication)
Timed re-authentication	Off
Timed reauth_period	3,600 seconds
Interval between two authentication requests	10 seconds
Retransmission interval	3 seconds
Maximum retransmissions	3
Client timeout period	3 seconds, if within which no response is received from the client, the communication is deemed as a failure
Server timeout period	5 seconds, if within which no response is received from the server, the communication is deemed as a failure
Lists of authenticable hosts under a port	No default

45.2.2 Precautions for Configuring 802.1x

- You can perform the following configuration only to the products that support 802.1x.
- The 802.1x can run on both L2 device and L3 device.
- It is required to configure the IP address of the authentication server before the Radius-server authentication mode can operate normally.
- You cannot enable 1X authentication for ports with safety feature enabled.
- You cannot enable 1X authentication for Aggregate Port.
- If the 1x function is enabled on only one port of a switch, all the port will send the 1x protocol packets to the CPU.

45.2.3 Configuring the communication between the device and Radius server

The Radius Server maintains the information of all users: user name, password, authorization information and accounting information. All users are managed on the Radius Server in a centralized manner, without being distributed over various switches, making easier management for the administrator.

In order for the switch to normally communicate with the RADIUS SERVER, you must set the following parameters:

Radius Server end: You must register a Radius Client. At registration, you must supply the Radius Server switch's IP address, authentication UDP port (add the accounting UDP port, if needed), and the agreed key for communication between the switch and Radius Server, and select EAP support for the Client. The procedure for registering one Radius Client on the Radius Server varies with different software settings. Please refer to the appropriate document.

Device end: The following settings are necessary at the device end to ensure the communication between the device and the server: Configure the IP address of the Radius Server, authentication (accounting) UDP port and the agreed password for the communication with the server.

In the privileged mode, you can set the communication between the switch and the Radius Server via the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
Radius-server key *string*	Configure RADIUS Key.
End	Return to the privileged mode.
Write	Save the configuration.
Show radius server	Show the RADIUS server.

You can use the **no radius-server host** *ip-address* **auth-port** command to restore the authentication UDP port of the Radius Server to its default. You can use the **no radius-server key** command to delete the authentication key of the Radius Server. The following example sets the Server IP as 192.168.4.12, authentication UDP port as 600, and the key as agreed password:

```
DES-7210# configure terminal
DES-7210(config)# radius-server host 192.168.4.12
DES-7210(config)# radius-server host 192.168.4.12 auth-port 600
DES-7210(config)# radius-server key MsdadShaAdasdj878dajL6g6ga
DES-7210(config)# end
```

- The officially agreed authentication UDP port is 1812.
- The officially agreed accounting UDP port is 1813.
- No less than 16 characters are recommended for the agreed password between the device and the Radius Server.
- The port of the device to connect the Radius Server shall be configured as uncontrolled port.

45.2.4 Setting the 802.1X Authentication Switch

When the 802.1x authentication is enabled, the switch will impose authentication over the host connected to the controlled port, and the hosts that fail the authentication are not allowed to access the network.

In the privileged mode, you can enable the 1x authentication by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
Radius-server key string	Configure RADIUS Key.
aaa authentication dot1x *auth* **group radius**	Configure the dot1x authentication method list
dot1x authentication *auth*	dot1x applies authentication method list
End	Return to the privileged mode.
Write	Save the configuration.
Show running-config	Show the configuration.

The following example enables 802.1x authentication:

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
DES-7210(config)# radius-server host 192.168.217.64
DES-7210(config)# radius-server key starnet
DES-7210(config)# aaa authentication dot1x authen group radius
DES-7210(config)# dot1x authentication authen
DES-7210(config)# end
DES-7210# show running-config
!
aaa new-model
!
aaa authentication dot1x authen group radius
!
username DES-7210 password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 072d172e071c2211
!
!
!
dot1x authentication authen
!
interface VLAN 1
 ip address 192.168.217.222 255.255.255.0
 no shutdown
!
!
line con 0
```

```
line vty 0 4
!
end
```

To apply the RADIUS authentication method in the 802.1x, configure the IP address of the Radius Server and make sure normal communication between the device and the Radius Server. Without the coordination of the Radius Server, the switch cannot perform authentication. For how to set the communication between the Radius Server and the switch, please see the previous section.

45.2.5 Enabling/Disabling the Authentication of a Port

If you enable authentication for a port when the 802.1x is enabled, the port becomes a controlled port, and the users under the port must first pass authentication before they can access the network. However, the users under the uncontrolled port can directly access the network.

In the privileged mode, you can set authentication for a port by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
interface *interface*	Enter the interface configuration mode and specify the Interface to configure.
dot1x port-control auto	Set the port to be a controlled port (enable interface authentication). You can use the no option of the command to disable the authentication of the interface.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x port-control	View the authentication configuration of the 802.1x interface.

You can use the **no dot1x port-control** command to disable the authentication of the interface. The following example sets Ethernet interface 1/1 to be a controlled interface:

```
DES-7210# configure terminal
DES-7210(config)# interface f 1/1
DES-7210(config-if)# dot1x port-control auto
DES-7210(config)# end
```

When a port is set as a controlled port, only the EAP packets are allowed to pass; the packets to the CPU are also under control.

Caution

If you hope that cpu can not receive non-EAP packet from any controlled port, you can separate management VLAN from user VLAN.

45.2.6 Enabling Timed Re-authentication

The 802.1x can ask users for re-authentication at periodical intervals, to prevent authorized users from being used by other users. This can also detect disconnection, making more accurate charging. In addition to the re-authentication switch, you can also define the

re-authentication interval, which is 3600 seconds by default. In the case of charging based on duration, you should determine the re-authentication interval according to the specific network size, which should be sufficient while as accurate as possible.

In the privileged mode, you can enable/disable re-authentication and set the re-authentication interval by performing the following steps.

Command	Function
configure terminal	Enter the global configuration mode.
dot1x re-authentication	Enable timed re-authentication.
dot1x timeout re-authperiod *seconds*	Set the re-authentication interval.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x re-authentication** command to disable timed re-authentication, and use the **no dot1x timeout re-authperiod** command to restore the re-authentication interval to the default.

The following example enables re-authentication and sets the re-authentication interval as 1000 seconds.

```
DES-7210# configure terminal
DES-7210(config)# dot1x re-authentication
DES-7210(config)# dot1x timeout re-authperiod 1000
DES-7210(config)# end
DES-7210# show dot1x
802.1X Status:          Disabled
Authentication Mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Enabled
Re-authen Period:       1000 sec
Quiet Timer Period:     10 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Filter Non-RG Supp:     Disabled
Client Online Probe:    Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Disabled
```

If re-authentication is enabled, please pay attention to the reasonableness of the re-authentication interval, which must be set according to the specific network size.

45.2.7 Changing the QUIET Time

When the user authentication fails, the switch does not allow that user to re-authenticate until a specified period, which is referred to as Quiet Period.This value functions to protect the device from malicious attacks. The default interval for Quiet Period is 5 seconds.

A shorter Quiet Period may speed up re-authentication for the users.

In the privileged mode, you can set the Quiet Period by performing the following steps:

Command	Function

Command	Function
configure terminal	Enter the global configuration mode.
dot1x timeout quiet-period seconds	Set the Quiet Period.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x timeout quiet-period command to** restore the Quiet Period to its default. In the example below the QuietPeriod value is set as 500 seconds:

```
DES-7210# configure terminal
DES-7210 (config)# dot1x timeout quiet-period 500
DES-7210(config)# end
```

45.2.8 Setting the Packet Retransmission Interval

After the device sends the EAP-request/identity, it resends that message if no response is received from the user within a certain period. By default, this value is 3 seconds. You should modify this value to suit the specific network size.

In the privileged mode, you can set the packet retransmission interval by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x timeout tx-period *seconds*	Setting the Packet Retransmission Interval
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x timeout tx-period** to restore the packet re-transmission interval to its default. The following example sets the packet retransmission interval as 100 seconds:

```
DES-7210# configure terminal
DES-7210(config)# dot1x timeout tx-period 100
DES-7210(config)# end
```

45.2.9 Setting the Maximum Number of Requests

If the switch does not receive response within the ServerTimeout after it sends an authentication request to the RadiusServer, it will retransmit the packets.The maximum number of requests are the maximum retransmission requests of the device, and the authentication fails if this number is exceeded. By default, this value is 3. You should modify this value to suit the specific network size.

In the privileged mode, you can set the maximum number of retransmissions by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x max-req *count*	Set the maximum number of packet re-transmissions.
end	Return to the privileged mode.

Command	Function
write	Save the configuration.
show dot1x	Show the dot1x configurations.

```
DES-7210#show dot1x
```

You can use the **no dot1x max-req** command to restore the maximum number of packet re-transmissions to its default. The following example sets the maximum number of packet retransmissions to 5:

```
DES-7210# configure terminal
DES-7210(config)# dot1x max-req 5
DES-7210(config)# end
```

45.2.10 Setting the Maximum Number of Re-authentications

When the user authentication fails, the device attempts to perform authentication for the user once again. When the number of attempts exceeds the maximum number of authentications, the switch believes that this user is already disconnected, and ends the authentication process accordingly. By default, the number is 3. However, you can modify this value.

In the privileged mode, you can set the maximum number of re-authentications by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x reauth-max ***count***	Setting the Maximum Number of Re-authentications
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x reauth-max** command to restore the maximum number of re-authentications to its default. The following example sets the maximum number of re-authentications to 3:

```
DES-7210# configure terminal
DES-7210(config)# dot1x reauth-max 3
DES-7210(config)# end
```

45.2.11 Setting the Server-timeout

This value indicates the maximum response time of the Radius Server. If the switch does not receive the response from the Radius Server within this period, it deems the authentication as a failure.

In the privileged mode, you can set the Server-timeout and restore it to its default by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x timeout server-timeout *seconds*	Set the maximum response time of the Radius Server. You can use the no option of the command to restore it to its default.
end	Return to the privileged mode.

Command	Function
write	Save the configuration.
show dot1x	Show the dot1x configurations.

45.2.12 Configuring the device to initiate the 802.1x authentication proactively

The 802.1x is secure access authentication based on port. Users must first undergo authentication before they can access the network. In most cases, authentication is initiated by the user end through EAPOL-START packets. For the information about packet interaction during the authentication process, please see “Authentication Initiation and Packet Interaction During Authentication”.

However, authentication needs to be initiated by the switch in some cases. For example, when the switch is reset and the status of the authentication port changes from linkdown to linkup, the switch needs to automatically initiate authentication to ensure that the authenticated users can continue to use the network. In addition, if you use a 802.1x client that does not actively initiate authentication requests (for example, the Windows XP 802.1x client), the switch should be able to actively initiate authentication. The switch forcedly asks all the users under the authentication port to authenticate by sending the EAP-request/identity multicast packets.

The following section describes how to configure the switch to actively initiate 802.1x authentication and how you should configure appropriately in different application environments.

Turn on/off the switch for the proactive authentication initiation of the device

When this function is disabled, the switch can only initiate an authentication request at resetting or when the status of the authentication port is changed. This ensures that the on-line users can continue to use the network. The switch will not actively initiate an authentication request in any other cases. When this function is enabled, you can configure the times of automatic authentication initiation, authentication request interval, and whether to stop sending requests when the users pass the authentication.

In the privileged mode, you can enable automatic authentication by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auto-req	Enable automatic authentication. It is disabled by default.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

The **no** option of the command turns off the function. Only when the function is enabled, the following settings take effect. The user can set the number of proactive authentication requests initiated by the device, which can be determined according to the actual network environment.

In the privileged mode, you can set the number of automatic authentication requests by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.

Command	Function
dot1x auto-req packet-num *num*	The device proactively initiates num 802.1x authentication request messages. If num is equal to 0, the device will continually send that message. The default is 0 (infinite).
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auto-req	Show the configuration.

The **no** option of the command restores the value to its default. The following contents introduce how to configure the message sending interval.

In the privileged mode, you can set the packet sending interval by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auto-req req-interval *interval*	Setting the Packet Sending Interval
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auto-req	Show the configuration.

The **no** option of the command restores the value to its default. Since sending the authentication request multicast message will cause re-authentication for all users under the authentication interface, the sending interval shall not be too small lest the authentication efficiency is affected.

It is possible to set whether to stop sending the request messages when the user authentication passes. In some applications (only one user under a port, for example), we can stop sending authentication requests to the related port when the device finds the user authentication passes. If the user gets offline, the request is sent continually.

In the privileged mode, you can set this function by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auto-req user-detect	Stop sending the messages when there is some authentication user under the port. This function is enabled by default.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auto-req	Show the configuration.

The **no** option of the command disables the function. Before setting this function, take careful considerations on the current network application environment.

The above three commands provide you with flexible application strategies. You can select the appropriate configuration command according to the specific network application environment. To help you configure easily, the following configuration table is provided for your reference:

	Solution 1	Solution 2	Solution 3
User environment	One port for any user	One port for one user	One port for multiple users

	Solution 1	Solution 2	Solution 3
Whether the DES-7210 supplicant should be used as the authentication client	Yes	No	No
Configuration command recommended	Not necessary to enable the dot1x auto-req function	**dot1x auto-req** **dot1x auto-req packet-num** *num* **dot1x auto-req req-interval** *interval* **dot1x auto-req user-detect**	**dot1x auto-req** **dot1x auto-req packet-num** *0* **dot1x auto-req req-interval** *interval* **no dot1x auto-req user-detect**

45.2.13 Configuring 802.1x Accounting

Our 802.1x has implemented the accounting function. Accounting is based on interval. In other words, the 802.1x records the length of the period between the first successful authentication of the user and the user's logoff or when the switch detects user disconnection.

After the first successful user authentication, the switch sends an accounting start request to the server. When the user gets off-line or the switch finds that the user has got off line or when the physical connection of the user is broken, the switch sends an accounting end request to the server. The server group records this information in the database of the server group. Based on such information, the NMS can provide the basis for accounting.

Our 802.1x stresses the reliability of accounting, and it specially supports the backup accounting server to avoid failures of the accounting server. When a server can no longer provide the accounting service due to various reasons, the switch will automatically forward the accounting information to another backup server. This greatly improves the reliability of accounting.

When a user exits by itself, the accounting duration is accurate. When the connection of the user is broken by accident, the accounting accuracy depends on the re-authentication interval (the switch detects the disconnection of a user by using the re-authentication mechanism).

To enable the accounting function of the device, the following settings are necessary on the device:

1. On the Radius Server, register the switch as a Radius Client, like the authentication operation.
2. Set the IP address of the accounting server.
3. Set the accounting UDP port.
4. Enable the accounting service on the precondition that the 802.1x has been enabled.

In the privileged mode, you can set the accounting service by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable the AAA function
aaa group server radius gs	Configure the accounting server group.
server *192.168.4.12* **acct-port** *11*	Add a server to the server group.
exit	Return to the global configuration mode.

Command	Function
aaa accounting network *acct* **start-stop group** *gs*	Configure the accounting method list.
dot1x accounting *acct*	Apply the accounting method list for the 802.1X.
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

The **no aaa accounting network** command deletes the accounting method list. The **no dot1x accounting** command restores the default dot1x accounting method. The following example sets the IP address of the accounting server to 192.1.1.1, that of the backup accounting server to 192.1.1.2, and the UDP port of the accounting server to 1200, and enables 802.1x accounting:

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
DES-7210(config)# aaa group server radius acct-use
DES-7210(config-gs-radius)# server 192.168.4.12 acct-port 1200
DES-7210(config-gs-radius)# server 192.168.4.13 acct-port 1200
DES-7210(config-gs-radius)# exit
DES-7210(config)# aaa accounting network acct-list start-stop group acct-use
DES-7210(config)# dot1x accounting acct-list
DES-7210(config)# end
DES-7210# write memory
DES-7210# show running-config
```

Caution

1. The agreed accounting key must be the same as that of the Radius Server and authentication.
2. The accounting function cannot be enabled unless the AAA is enabled.
3. The accounting is impossible unless the 802.1X authentication passes.
4. By default, the accounting function of the 802.1x is disabled.
5. For the database format of accounting, see the related Radius Server documentation.

Also, the account update is supported. After the account update interval is set on the NAS device, the NAS device will send account update packets to the Radius Server at periodical intervals. On the Radius Server, you can define the number of periods before which the account update packet of a user is not received from the NAS device, the NAS or user will be regarded as off-line. Then, the Radius Server can stop the accounting of the user, and delete the user from the on-line user table.

In the privileged mode, you can set the account update function by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable the AAA function
aaa accounting update	Set the account update function.
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

You can disable the account update service by using the **no aaa accounting update** command.

```
DES-7210# configure terminal
DES-7210(config)# aaa accounting update
DES-7210(config)# end
DES-7210# write memory
DES-7210# show running-config
```

The following chapters introduce the propriety features of DES-7210's network products:

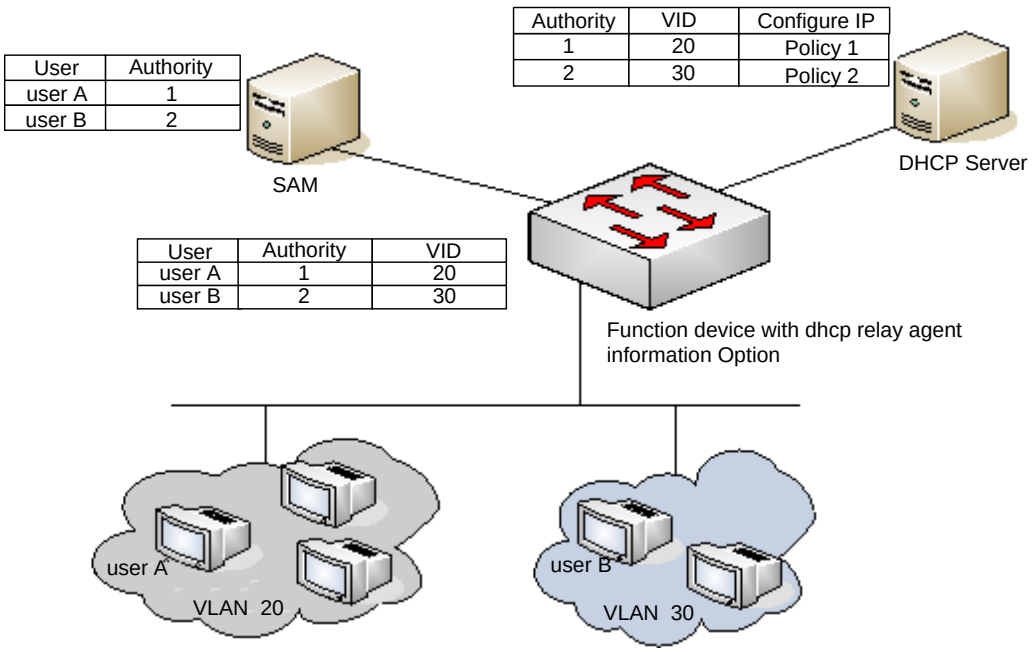
To make it easy for broadband operators and to accommodate use in special environments, our 802.1x has been expanded on the basis of the account (such expansion is completely based on the standard, and has totally compatible with IEEE 802.1x).

45.2.14 Configuring the IP authorization mode

The 802.1x implemented by DES-7210 Network can force the authenticated users to use fixed IP. By configuring the IP authorization mode, the administrator can limit the way the user gets IP address. There are four IP authorization modes: DISABLE, DHCP SERVER, RADIUS SERVER and SUPPLICANT. They are detailed below respectively:

DISABLE mode (default): The device has no limitation for the user IP, and the user only needs to pass the authentication to be able to access the network.

DHCP SERVER mode: The user IP is obtained via specified DHCP SERVER, and only the IP allocated by the specified DHCP SERVER is considered legal. For the DHCP mode, it is possible to use DHCP relay option82 to implement a more flexible IP allocation policy with the 802.1X. Here is a typical diagram for the plan:



The user initiates IP requests via the DHCP Client. The network device with dhcp relay option82 converges the user authority on the SAM server to construct the option82 field and encapsulate it in the DHCP request message. That option82 field consists of "vid + permission". The DHCP Server chooses different allocation policies by using the option82 field.

In this mode, it is required to configure the DHCP Relay and the related option82. If the DHCP relay function is enabled and the option82 policy is selected, see the DHCP Relay Configuration Guide and Command References for the configurations.

RADIUS SERVER mode: The user IP is specified by the RADIUS SERVER. The user can only use the IP specified by the RADIUS SERVER to be able to access the network.

SUPPLICANT mode: The IP bound to the user is the IP of the PC during the SUPPLICANT's authentication. After the authentication, the user can only use that IP to be able to access the network.

The application models in the four modes are as follows:

- DISABLE mode: Suitable for the environment with no limits for the users. The user can access the network once he/she passes the authentication.
- DHCP SERVER mode: The user PC gets the IP address via DHCP. The administrator configures the DHCP RELAY of the device to limit the DHCP SERVER that the users can access. In this way, only the IPs allocated by the specified DHCP SERVER are legal.
- RADIUS SERVER mode: The user PC uses fixed IP. The RADIUS SERVER is configured with <user-IP> mapping relations that are notified to the device via the Framed-IP-Address attributes of the device. The user has to use that IP to be able to access the network.
- SUPPLICANT mode: The user PC uses fixed IP. The SUPPLICANT notifies the information to the device. The user has to use the IP at authentication to be able to access the network.

Caution

When the user switches modes, it will cause all authenticated users to get offline. So, it is recommended to configure the authentication mode before the use.

In the privileged mode, configure the IP authorization mode as follows:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable the AAA function
aaa authorization ip-auth-mode {disabled | dhcp-server | radius-server | supplicant }	Configure the IP authorization mode
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

The example below configures the IP authorization mode as the RADIUS-SERVER mode:

```
DES-7210# configure terminal
DES-7210(config)# aaa authorization ip-auth-mode radius-server
DES-7210(config)# end
DES-7210# show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode radius-server
!
DES-7210# write memory
```

45.2.15 Releasing Advertisement

Our 802.1x allows you to configure the Reply-Message field on the Radius Server. When authentication succeeds, the information of the field is shown on our 802.1x client of Star-Supplicant, by which the operators can release some information.

Such information is shown at the first user authorization, but not at re-authentication. This avoids frequently disturbing the user.

The window for showing the advertisement information supports html, which converts the http://XXX.XXX.XX in the message into links capable of direct switching, for easier browsing.

Releasing of the advertising information:

1. The operator configures the Reply Message attribute on the Radius Server end.
2. Only our Star-supplicant client supports such information (free for the users of our switch), while other clients cannot see the information, which however does not affect their normal use.
3. No setting is required at the device end.

45.2.16 List of Authenticable Hosts under a Port

For enhanced security of the 802.1x, we have made expansion without affecting the IEEE 802.1x, allowing the NM to restrict the list of hosts authenticated of a port. If the list of hosts authenticated of a port is empty, any user can be authenticated. If the list is not empty, only the hosts in the list can be authenticated. The hosts that can be authenticated are identified by using the MAC addresses.

The following example adds/deletes the hosts that can be authenticated under a port.

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auth-address-table address *mac-addr* **interface** *interface*	Set the list of the hosts that can be authenticated.
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

Caution

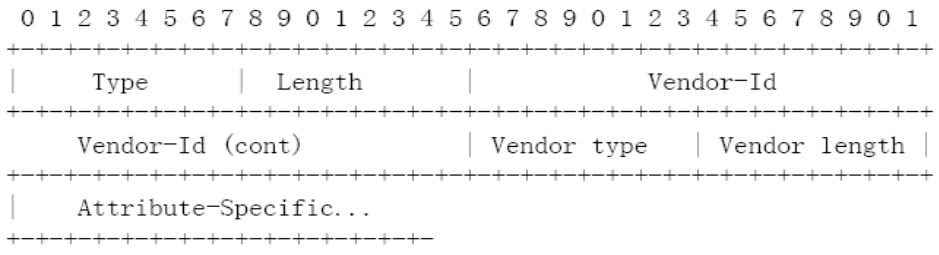
If the list of the host is empty, the port allows any host to be authenticated.

45.2.17 Authorization

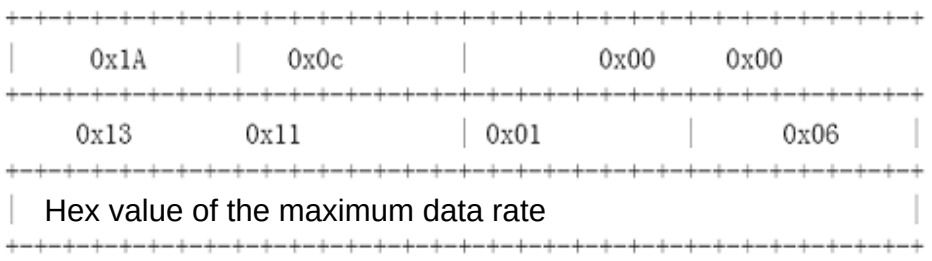
To make it easier for operators, our products can provide services of different qualities for different types of services, for example, offering different maximum bandwidths. Such information is all stored on the Radius Server, and the administrator does not need to configure every switch.

Since the Radius has no standard attribute to represent the maximum data rate, we can only transfer the authorization information by the manufacturer customized attribute.

The general format of the definition is as follows:

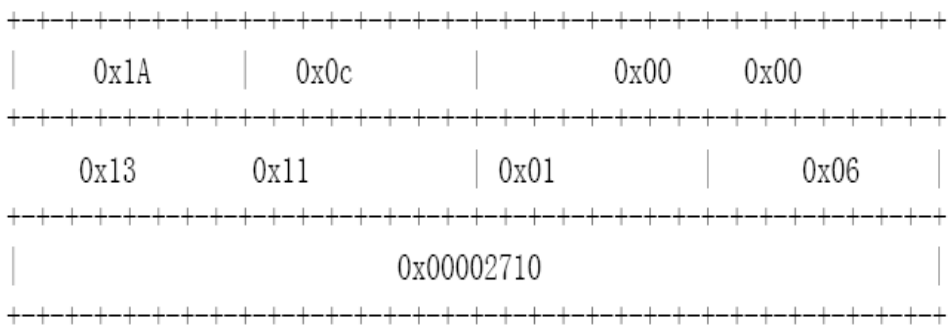


For the maximum data rate, you need to fill in the following values:



The unit of the maximum data rate is kbps.

For users with the maximum data rate of 10M, you need to fill in the following values:



For the customized header, follow those provided above. The maximum data rate is 10M, that is, 10000kbsp, and makes 0x00002710 in the Hex system. You only need to fill in the corresponding field.

This function calls for no settings on the device end, and works as long as the device end supports authorization.

45.2.18 Configuring the Authentication Mode

In the standard, the 802.1x implements authentication through the EAP-MD5. The 802.1X designed by DES-7210 can perform authentication through both the EAP-MD5 (default) mode and the CHAP and PAP mode. The advantage of the CHAP is that it reduces the communication between the switch and the RADIUS SERVER, thus alleviating the pressure on the RADIUS SERVER. Same as the CHAP mode, the communication between the PAP and RADIUS SERVER occurs only once. Although the PAP mode is not recommended for its poor security, it can meet the special needs of the user in some cases. For example, when the security server used only supports the PAP authentication mode, this mode can be selected to fully exploit the existing resources, protecting the existing investment.

In the privileged mode, you can set the authentication mode of the 802.1x by performing the following steps:

Command	Function

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auth-mode mode	Configure the authentication mode
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the configuration.

The following example configures the authentication mode to the CHAP mode:

```
DES-7210# configure terminal
DES-7210(config)# dot1x auth-mode CHAP
DES-7210(config)# end
DES-7210# show dot1x
802.1X Status:        Disabled
Authentication Mode:  CHAP
Authed User Number:   0
Re-authen Enabled:    Disabled
Re-authen Period:     3600 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Filter Non-RG Supp:   Disabled
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Group Server
```

45.2.19 Configure the backup authentication server.

Our 802.1x-based authentication system can support the backup server.When the master server is down due to various reasons, the device automatically issues a server submission authentication request to the method list server group.

In the privileged mode, you can set the backup authentication server by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa group server radius *gs-name*	Configure the server group.
server sever	Configure the server.
server server-backup	Configure the backup server.
End	Return to the privileged mode.
Write	Save the configuration.
show dot1x	Show the configuration.

The following example configures 192.168.4.12 to be the backup server:

```
DES-7210# configure terminal
DES-7210# aaa new-model
```

```
DES-7210(config)# aaa group server radius auth-11
DES-7210(config-gs-radius)# server 192.168.4.1
DES-7210(config-gs-radius)# server 192.168.4.12
DES-7210(config-gs-radius)# end
DES-7210#
```

45.2.20 Configuring and Managing Online Users

DES-7210's devices provide management for authenticated users via SNMP. The administrator can view the information of the authorized users via SNMP, and forcedly log off a user. The user forcedly logged off must pass the authentication again before it can use network resources.

This function calls for no configuration on the device.

45.2.21 Implementing User-IP Binding

With our clients and by correctly configuring the Radius Server, you can implement unique user-IP binding. A user must undergo authentication by using the IP address allocated by the administrator. Otherwise, authentication will fail.

For this function, you do not need to configure the switch. The user needs to use our client and the administrator needs to configure the Radius Server.

45.2.22 Port-based Traffic Charging

In addition to the duration-based billing, DES-7210's network devices provide the traffic-based billing function in case each port of the equipment has only one user access.

This function calls for no configuration on the device but need the support of the Radius server.

45.2.23 Implementing Automatic Switching and Control of VLAN

If the user's "down VLAN" is set on the Radius server, the Radius server will notify the device via the manufacturer customized attribution of DES-7210 Networks. DES-7210's device automatically jumps the VLAN of the port connected with the user into the VID configured on the Radius server, and the administrator need not any manual configuration on the device. You can view the real VLAN of the user by using the **show dot1x summary** command.

Caution

Our product support vlan auto-jump on the port. It is no need to enable network authorization.

Follow these steps to configure a port to allow dynamic VLAN jump or not:

Command	Function
configure terminal	Enter the global configuration mode.
interface *interface*	Enter the interface configuration mode.
[no] dot1x dynamic-vlan enable	Configure whether to allow dynamic vlan jumping, which is disabled by default.

Command	Function
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the configuration.

45.2.24 Implementing GUEST VLAN Function

If **guest vlan** is set on the switch, then when the port sends the authentication requests of certain quantity proactively but receives no corresponding reply or **eapol** packet, you can add the port to **guest vlan.** Use **show runninng-config** to view the configuration and **show valn** to check whether the port jumps to guest vlan or not .

Follow these steps to configure a port to allow **GUEST VLAN** jump or not:

Command	Function
configure terminal	Enter the global configuration mode.
interface *interface*	Enter the interface configuration mode.
dot1x dynamic-vlan enable	Allow Vlan jump on the interface.
[**no**] **dot1x guest-vlan** *vid*	Configure whether to enable guest vlan, which is disabled by default.
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

Caution

1. **Guest vlan** takes effect unless you configure **dot1x dynamic-vlan enable.**
2. It is better not to configure L2 attributes when configuring **guest vlan**, especially not to set **vlan** on the port manually.
3. Exiting **guest vlan** when there is **eapol** packet on the port and the port is **linkdown.** If you configure **guest vlan,** it will check **guest vlan** exchange conditions again when the port is **linkup.**
4. Enabling **guest vlan** on Trunk port causes the users in other vlan on this port access the network without 802.1x authentication. To this end, it is recommeded that **guest vlan** shall be enabled on the Access port.

45.2.25 Shielding Proxy Server and Dial-up

The two major potential threats to network security are: The user sets its own proxy server and the user makes dial-up to access the network after authentication. Star switches provide the function to shield proxy servers and dial-up connections.

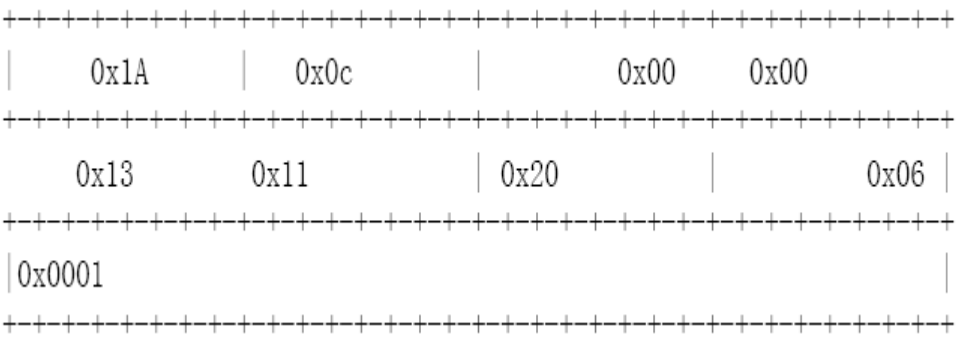
To implement this function needs no settings on the device end and needs only the corresponding attributes configured on the Radius server end. Since the Radius has no

standard attributes to indicate the maximum data rate, we can transfer the authorization information only through the manufacturer custom attributes. For the general format defined, see the Authorization section.

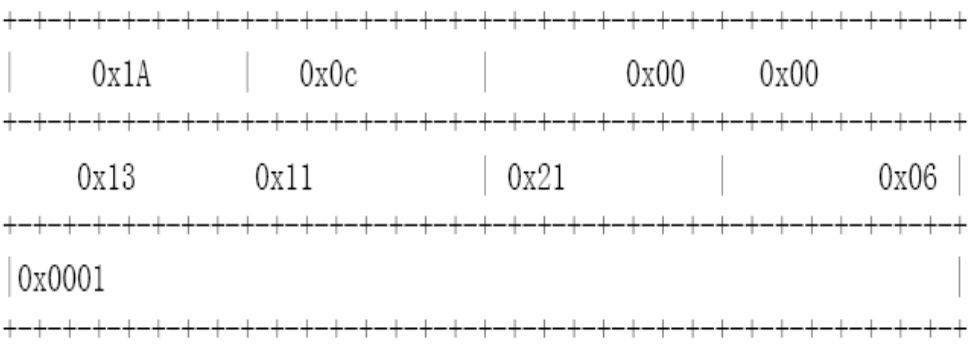
The proxy server shielding function defines the Vendor type of 0x20, and the dial-up shielding function defines the Vendor type of 0x21.

The Attribute-Specific field is a 4-byte manufacturer defined attribute, which defines the actions taken against proxy server access and dial-up access. 0x0000 means normal connection, without shielding detection. 0x0001 means shielding detection.

To shield the access via the proxy server, you should fill in the following information:



To shield the access via the dial-up connection, you should fill in the following information:



45.2.26 Configuring On-line Probe on Client End

To ensure accurate charging, an on-line probe mechanism is needed to detect whether a user is on-line within a short period. The re-authentication mechanism specified in the standard can meet such needs, but it needs the participation of the RADIUS server. Accurate user probe will occupy enormous resources of the switch and RADIUS server. To meet the need to implement accurate charging with few resources occupied, we use a new client on-line probe mechanism. Such mechanism only needs interaction between the switch and client and occupies little network traffic, and it implements minute-level charging accuracy (you can set the charging accuracy).

Caution

To implement on-line client monitoring, the client software must support this function.

The following two timers affect the performance and accuracy of on-line probe:

- Hello Interval: It is the interval at which the client sends advertisement.

- Alive Interval: Client online interval. If the device has not received the client advertisement during this interval, it actively disconnects the client and notifies the billing server. The interval must be greater than the Hello Interval.

In the privileged mode, you can configure the on-line probe function of the client by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
Dot1x client-probe enable	Enable the on-line probe function of the client
Dot1x probe-timer interval *interval*	Configure the Hello Interval
Dot1x probe-timer alive interval	Configure the Alive Interval of the device.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the configuration.

45.2.27 Configuring the Option Flag for EAPOL Frames to Carry TAG

In accordance with IEEE 802.1x, the EAPOL packets cannot be added with vlan TAG. However, based on the possible application requirements, the selection flag is provided. When the flag is turned on, tags can be outputted according to the related output rule of the trunk ports.

The typical application environment is to enable 802.1x authentication on the convergence layer. For more information, see “Topologies of Typical Applications”.

In the privileged mode, you can configure the flag for EAPOL frames to carry TAG by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x eapol-tag	Enable the flag for EAPOL frames to carry TAG. By default, the function is disabled.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the configuration.

You can disable this function by using the **no dot1x eapol-tag** command.

45.2.28 Configuring Port-based Authentication

The 802.1x controls users on the basis of their MAC addresses by default. Only the authenticated user can use the network. With port-based authentication, the port is authenticated as long as a user is authenticated on a port. Consequently, all users connecting to this port can access the network.

To configure port-based control mode, execute the following commands in the privileged mode.

Command	Function
configure terminal	Enter the global configuration mode.
interface <*interface-id*>	Enter the interface mode
dot1x port-control auto	Enable the function being controlled.

Command	Function
dot1x port-control-mode *{mac-based|port-based}*	Select the controlled mode.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x port-control	Show the configuration of port 802.1X.

You can run **no dot1x port-control-mode** to restore the settings to the default control mode.

Following example shows how to configure the authentication mode of a port.

```
DES-7210(config)#
DES-7210# configure terminal
DES-7210(config)# interface gigabitEthernet 4/5
DES-7210(config-if)# dot1x port-control-mode port-base
```

Caution

In the port-based authentication mode, a port can be connected with only one authenticated user.

Port-based authentication mode can enable or disable dynamic users to migrate among multiple authenticated ports. By default, the migration is allowed. To prohibit the migration, run the following commands one by one in the privileged mode.

Command	Function
configure terminal	Enter the global configuration mode.
dot1x stationarity enable	Disable the migration among ports.
end	Exit to the privileged mode.
write	Save the configuration.

45.2.29 Configuring Port-based Single-user Authentication

By default, 802.1x controls on the basis of user MAC. Only the authenticated users can use the network, while other users connected to the same port is not able to use the network. In the port-based control mode, the port is authenticated when there is an authenticated user on the port. All the users connected to the authenticated port are able to use the network normally.

However, in the port-based control mode, the port-based single-user authentication controls only one authenticated user. The port is authenticated when it allows only one authenticated user who is enable to use the network normally. Then, if you find other users on the port, you should clear all the users on the port and reauthenticate.

From the privileged mode, follow the steps below to configure port-based single-user control mode on the port.

Command	Function
configure terminal	Enter the global configuration mode.
interface <*interface-id*>	Enter the interface configuration mode.

dot1x port-control auto	Enable control function.
dot1x port-control-mode port-based single-host	Port-based single-user control mode.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x port-control	Show 802.1x configuration.
show running-config	Show all configurations.

You can run no dot1x port-control-mode to restore the settings to the default control mode.

Following example shows how to configure the authentication mode of a port.

```
DES-7210(config)#
DES-7210#configure terminal
DES-7210(config)#interface <interface-id>
DES-7210(config-if)#dot1x port-control-mode port-base single-host
```

Caution

In the port-based authentiction mode, every port only can receive one authentication user.

Single-host is port-based single-user 802.1x access control. Use **show dot1x port-control** to display port-based and use **show running-config** to display dot1x port-control-mode port-based single-host.

Since single-host only supports the single-user form, setting default-user-limit on the port manually does not take effect in single-host mode. If you set default-user-limit on the port after setting single-host, only one user can be permitted to use the network still.

In the port-based authentication mode, you can permit or deny dynamic users to migrate among multiple authentication ports, which is permitted by default. If you want to deny the migration of dynamic users, follow the steps below from the privileged mode.

Command	Function
configure terminal	Enters the global configuration mode.
dot1x stationarity enable	Prohibits migration between ports.
End	Returns to the privileged mode.
Write	Saves the configuration.

45.2.30 Configuring Dynamic Acl Assignment

802.1x supports ACL assignment from server and dynamic installation of the assigned ACL. Our product support installing acl by default. They will install acl dynamically on condition

that the allowed acl is set on the server and is assigned after the successful user authentication.

To implement dynamic acl assignment, you need to set the port as mac-based authentication mode or port-based single-user authentication mode. The ACL assignment is not supported in the port-based multi-user authentication mode. For the configuration, please refer to the related command configuration manual.

Caution

In single-host authentication mode, it supports to renew acl when reauthenticating. That is, acl takes effect when the authenticated user sets acl on the server and reauthenticates.

The mac-based authentication mode does not support ACL update when re-authenticating. That is to say, ACL of the authenticated user can only be assigned once. The new acl is ignored and the original acl remains if the acl changes when re-authenticating.

Supported acl type: extension type which can explain acl function on our switch.

Execute the following command if you need to support dynamic acl assignment on the server which is not authenticated by our company.

```
DES-7210#configure terminal
DES-7210(config)# radius vendor-specific extend
```

45.3 Viewing the Configuration and Current Statistics of the 802.1x

Our 802.1X provides a full range of state machine information, which is very useful for network management and can be used by the administrator to monitor user status in real time and make easy troubleshooting.

- Viewing the Radius Authentication and Accounting Configuration
- Viewing the Number of Current Users
- Viewing the List of the Addresses Authenticable
- Viewing the User Authentication Status Information
- Showing the 1x Client Probe Time Configuration

45.3.1 Viewing the Radius Authentication and Accounting Configuration

Run the **show radius server** command to check the related configuration of the Radius Sever, and run the **show aaa user** command to view the user-related information.

```
DES-7210# sh radius server
Server IP:       192.168.5.11
Accounting Port: 1813
Authen  Port:    1812
Server State:    Ready
```

45.3.2 Viewing the Number of Current Users

Our 802.1X allows you to view the numbers of two types of users: one is the number of current users, and the other is that of the authorized users. The number of current users refers to the total number of users authenticated (whether successfully or unsuccessfully), while the number of authorized users means the total number of users authorized.

In the privileged mode, run the **show dot1x** command to check the current number of users and authenticated users, 1x configuration, including the current number of users and authenticated users.

The following example shows the 802.1x configuration:

```
DES-7210# show dot1x
802.1X Status:        Disabled
Authentication Mode:  EAP-MD5
Authed User Number:   0
Re-authen Enabled:    Disabled
Re-authen Period:     3600 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Filter Non-RG Supp:   Disabled
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Disabled
```

45.3.3 Viewing the Authenticable Address Table

Our 802.1x has expanded functions that allow you to set the hosts that can be authenticated on a particular port. This function allows the administrator to view the currently available settings.

In the privileged mode, you can view the list of hosts authenticable by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auth-address-table address *mac-addr* **interface** *interface*	Set the list of the hosts that can be authenticated.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auth-address-table	Show the list of the hosts that can be authenticated.

Use the **no dot1x auth-address-table address** command to delete the specified authenticable host list. The following example shows the list of the hosts that can be authenticated.

```
DES-7210# show dot1x auth-address-table
interface:g3/1
-----------------------------------
mac addr: 00D0.F800.0001
```

45.3.4 Viewing the User Authentication Status Information

The administrator can view the authentication status of the current users of the switch for easier troubleshooting.

In the privileged mode, you can view the user authentication status information by performing the following steps:

Command	Function
show dot1x summary	Viewing the User Authentication Status Information

The following example shows the user authentication status information.

```
DES-7210# show dot1x summary

 ID   MAC       Interface  VLAN  Auth-State  Backend-State Port-Status

---- ----------- --------- ----  ----------  ------------   -----------
1   00d0f8000001 Gi3/1     1   Authenticated  IDLE       Authed
```

45.3.5 Showing the 1x Client Probe Time Configuration

In the privileged mode, you can view the 1x timer setting by performing the following steps:

Command	Function
show dot1x probe-timer	Show the 1X timer setting

The following example shows the 1.1x timer setting:

```
DES-7210# show dot1x probe-timer
Hello Interval: 20 Seconds
Hello Alive: 250 Seconds
DES-7210#
```

45.3.6 Other Precautions for Configuring 802.1x

1. When there is no IP authorization mode, each device supports 10,000 authenticated users.
2. Concurrent use of 1X and ACL

In the non-IP authorization mode, if you enable the 802.1x authentication function of a port and at the same time associate one ACL with a interface, the ACL takes effect on the basis of the MAC address. In other words, only the packets from the source MAC addresses of the authenticated users can pass ACL filtering, and the packets from other source MAC addresses will be discarded. The ACL can only work on the basis of the MAC address.

For example, if the authenticated MAC address is 00d0.f800.0001, then all the packets from the source MAC address of 00d0.f800.0001 can be switched. If the port is associated with an ACL, the ACL will further filter these packets that can be switched, for example, rejecting the ICMP packets from the source MAC address of 00d0.f800.0001.

In the IP authorization mode, you are recommended not to set the ACL on the controlled interface, since the ACL has a higher priority than the authentication user, and so the authenticated IP+MAC binding will not take effect. At a port, the following users are authenticated:

User 1: mac: 00d0.f800.0001 ip: 192.168.65.100

User 2: mac: 00d0.f800.0002 ip: 192.168.65.101

Then, set one ACL on the interface as follows:

ip access-list extended ip_acl:

deny icmp any any

The original purpose is to allow the communication of authenticated users and forbid sending ICMP messages. However, the ACL has a higher priority than the authenticated IP + MAC and the last default ACE of the ACL is "**deny any any**", so the authenticated users cannot communicate.

If you add **permit any any** to IP_acl, then any authenticated users can still communicate after changing its IP address, but the IP + MAC one-to-one binding is not achieved. Therefore, IP authentication + ACL is not recommended.

3. The hardware entries for user authentication and the other applications (for example, ACL, port IP security address) share the filtering entries and filtering domain templates in the IP authentication mode. If other applications exhaust the hardware resources, the user authentication may fail in the IP authorization mode, or though success, but the users cannot communicate, for the filtering domain templates in particular, at least one should be available for user authentication in the IP authentication mode.

46 AAA Configuration

The access control is used to control which people can access the network server and which services can be accessed by the users on the network. The authentication, authorization and accounting (AAA) is a key security mechanism for access control.

46.1 Basic AAA Principles

Authentication, Authorization and Accounting (shortened as AAA) provide a consistence framework for configuring the authentication, authorization and accounting functions, which are supported by DES-7210 products.

The AAA provides the following services in a modular manner:

- Authentication: It verifies whether a user can access, where the Radius protocol or Local can be used. The authentication is the method to identify a user before his/her access to the network and network services. The AAA is configured by the definition of a naming list for authentication method and application of it on every interface. The method list defines the authentication type and execution order. Before a defined authentication is executed, the method list must be applied on a specific interface. The default method list is exceptional. If no other method list is defined, the default method list will automatically apply on all interfaces. The defined method list overwrites the default method list. All authentication methods other than the local, line password and allowing authentication must be defined with AAA.
- Authorization: This means authorizing the user with services. The AAA authorization is implemented through the definition of series attributes that describe the operations on the user by the authorization. These attributes can be stored on the network device or the RADIUS security server remotely. All authorization methods must be defined with AAA. When the AAA authorization is enabled, it is automatically applied on all interfaces of the network device.
- Accounting: This means recording the user's usage of network resources. When the AAA accounting is enabled, the network access server starts to send the user's network resource usages to the Radius security server through statistics records. Every accounting record is composed of attribute pairs and stored in the security server. These records can be read for analysis by special software to implement the accounting, statistics and tracing for the user's network resource usage. All accounting methods must be defined with AAA. When the AAA accounting is enabled, it is automatically applied on all interfaces of the network device.

Note The AAA of some products only provides the authentication function. For all problems with product specifications, contact the market or technical support personnel.

Although the AAA is the primary access control method, our product also provides simple control accesses out of the range of AAA, such as the local username authentication, line password authentication and more. The difference lies in the degree of their network protection, and the AAA provides the security protection of a higher level.

The AAA has the following advantages:

- Powerful flexibility and controllability
- Expandability
- Standardized authentication
- Multiple backup systems

46.1.1 Basic AAA Principles

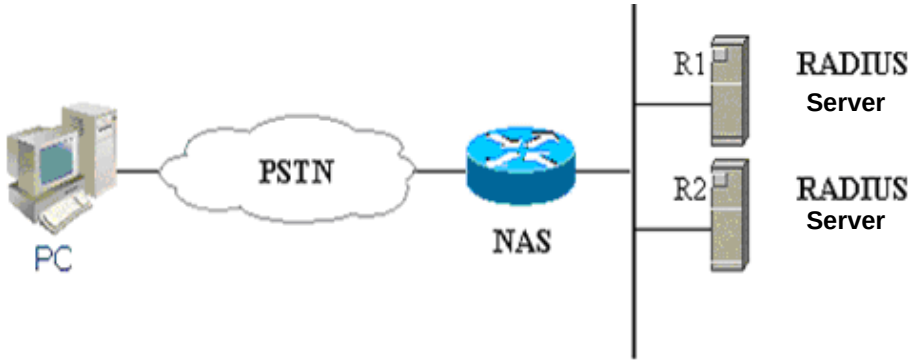
The AAA can configure dynamically authentication, authorization and accounting for a single user (line) or server. It defines the authentication, authorization and accounting by means of creating method lists and then applies them on specific services or interfaces.

46.1.2 Method List

Since the authentication for users can be implemented in a variety of ways, you need to use the method list to define the sequence of using different method to perform authentication for the users. The method list can define one or more security protocols for authentication, so that there are backup systems available for the authentication in case of the failure of the first method. Our product works with the first method in the method list for user authentication, and then selects the next method in the method list in case of no reply from that method. This process goes on till an authentication method listed successfully allows communication or all methods listed are used up. If all methods listed are used up but the communication is not allowed, it declares failure of authentication.

Caution Only when there is no reply from a method, our product will attempt the next method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

A typical AAA network configuration



The figure above illustrates a typical AAA network configuration, including two security servers: R1 and R2 are both RADIUS servers.

Supposed the system administrator has defined a method list, R1 is used first to capture the identity information, then R2, and finally the local username database on the NAS. If a remote PC user attempts to access the network via dialup, the NAS first queries the authentication information from R1. If the user passes the authentication on R1, R1 sends a SUCCESS reply to the NAS, and thus the user's access to the network is allowed. If R1 returns FAIL reply, the user's access is refused and the disconnected. If R1 has no reply, the NAS regards it as ERROR and queries authentication information from R2. This process continues for the remaining methods till the user passes the authentication, is refused or the session is terminated. If ERROR is returned for all methods, the authentication fails and the user is disconnected.

Caution The REJECT response is not the same as the TIMEOUT response. REJECT means the user fails to comply with the standard in the available authentication database and does not pass the authentication, thus the access request will be refused. TIMEOUT means there is no reply from the security server to the authentication. When an ERROR is detected, the AAA selects the next authentication method in the method list to continue the authentication process.

Note

In this chapter, take RADIUS for example of the configuration of the related authentication, authorization and accouting of the AAA security server. For the TACACS+, refer to *TACACS+ Configuration*.

46.2 Basic AAA Configuration Steps

First you shall decide to choose which security solution, evaluate the potential security risks in the specific network and select the proper measures to prevent unauthorized accesses. For the security risk evaluation and the possible security solutions, see Chapter 2, Security Overview. We recommend the use of AAA as much as possible to guarantee the network security.

46.2.1 Overview of AAA Configuration Steps

The AAA configuration may become simple when the basic operation process of AAA is understood. On the network devices, the AAA is configured through the following steps:

1. Enable AAA by using the global configuration command **aaa new-model**.
2. Configure the security protocol parameters if you decide to use the security server, such as RADIUS.
3. Define the authentication method list by using the **aaa authentication** command.
4. Apply the method list on specific interface or line, if necessary.

Caution

When the specific method list is applied, if no named method list is clearly specified, the default authentication method list will apply.

As a result, if you do not want to use the default authentication method list, you shall specify a specific method list.

For complete descriptions of the commands mentioned in this chapter, see the related chapters in the *Security Configuration Command Reference*.

46.2.2 Enabling AAA

It is required to enable AAA first to be able to use the AAA security features.

To enable AAA, execute the following command in the global configuration mode:

Command	Function
DES-7210(config)# **aaa new-model**	Enable AAA

46.2.3 Disabling AAA

To disable AAA, execute the following command in the global configuration mode:

Command	Function
DES-7210(config)# **no aaa new-model**	Disable AAA

46.2.4 Sequential Configuration Steps

After the AAA is enabled, it is time to configure the other parts related with the selected security solutions. Following table lists the possible configuration tasks and their description chapters.

Methods of AAA access control security solution

Configuration task	Step	Chapter
Configuring Local Login Authentication	3	Configuring Authentication
Defining AAA Authentication Method List	3	Configuring Authentication
Applying Method List on Specific Interface or Line	4	Configuring Authentication
Configuring Radius Security Protocol Parameters	2	Configuring Radius
Enabling Radius Authorization	5	Configuring Authorization

If you are using AAA for authentication, see *Configuring Authentication*.

46.3 Configuring Authentication

The authentication allows the user's identity verification before the user of network resources. In most cases, the authentication is implemented with the AAA security features. We recommend the use of AAA as much as possible.

46.3.1 Defining AAA Authentication Method List

To configure the AAA authentication, the first step is to define a named list of the authentication method, and then the applications use the defined list for authentication. The method list defines the authentication type and execution order. The defined authentication methods must be applied on specific interfaces before they can be executed. The default method list is exceptional.When not configured, all applications will use the default method list.

The method list is just a list to define the authentication method to be queried in turn to verify the user identity. The method list can define one or more security protocols for authentication, so that there are backup systems available for the authentication in case of the failure of the first method. Our product works with the first method in the method list for user authentication, and then selects the next method in the method list in case of no reply from that method. This process goes on till an authentication method listed successfully allows communication or all methods listed are used up. If all methods listed are used up but the communication is not allowed, it declares failure of authentication.

Caution

Only when there is no reply from a method, our product will attempt the next method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

46.3.2 Example of Method List

In a typical AAA network configuration, there are two servers: R1 and R2 are both RADIUS servers. Suppose the network administrator has chosen a security solution, and the NAS authentication uses an authentication method to authenticate the Telnet connection: First, R1 is used for the user authentication. In case of no reply, R2 will be used. In case there is no reply from both R1 and R2, the local database of the access server will perform the authentication. To configure the above authentication list, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.

Command	Function
aaa authentication login default group radius local	Configure a default authentication method list, where "default" is the name of the method list. The protocols included in this method list are listed behind the name in the order by which they will be queried. The default method list is applied on all applications.

If the system administrator hopes to apply this method list on a specific Login connection, he/she must create a named method list and then apply it on the specific connection. The example below shows how to apply the authentication method list on line 2 only.

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication login test group radius local	Define a method list named "test" in the global configuration mode.
line vty *2*	Enter the configuration layer of line 2
login authentication *test*	In the line configuration mode, apply the method list named “test” on the line.

If a remote PC user attempts to Telnet the network access server(NAS), the NAS first queries the authentication information from R1. If the user passes the authentication on R1, R1 sends a ACCEPT reply to the NAS, and thus the user's access to the network is allowed. If R1 returns the REJECT reply, the user's access is refused and then disconnected.If R1 does not respond, NAS considers TIMEOUT and queries the authentication information to R2. This process continues for the remaining methods till the user passes the authentication, is refused or the session is terminated. If all servers (R1 and R2) returns TIMEOUT, the authentication will be performed by the NAS local database.

Caution

The REJECT response is not the same as the TIMEOUT response. REJECT means the user fails to comply with the standard in the available authentication database and does not pass the authentication, thus the access request will be refused. TIMEOUT means there is no reply from the security server to the authentication. When an TIMEOUT is detected, the AAA selects the next authentication method in the method list to continue the authentication process.

46.3.3 Authentication Type

DES-7210 products support the following authentication types:

- Login Authentication -- the authentication of the user terminal logging in the NAS CLI.
- Enable Authentication -- the authentication of improving the CLI authority after the user terminal loggs in the NAS CLI.
- PPP Authentication -- the authentication of PPP dial user.
- DOT1X(IEEE802.1x) Authentication -- the authentication of the IEEE802.1x access user.

46.3.4 General Steps in Configuring AAA Authentication

The following tasks are common for the configuration of AAA authentication.

- Enable AAA by using the global configuration command **aaa new-model**.

- Configure the security protocol parameters if you decide to use the security server, such as RADIUS. See Configuring Radius for details.
- Define the authentication method list by using the **aaa authentication** command.
- Applying method list on a specific interface or line, if possible.


Caution

TACACS+ is not supported by the DOT1X authentication.

46.3.5 Configuring the AAA Login Authentication

This section deals with how to configure the AAA Login authentication methods supported by our product:


Caution

Only after the AAA is enabled through the command **aaa new-model** in the global configuration mode, the AAA security features are available for your configuration. For the details, see *AAA Overview*.

In many cases, the user needs to Telnet the network access server (NAS). Once such a connection is set up, it is possible to configure NAS remotely. To prevent unauthorized accesses to the network, it is required to perform authentication on the user identity.

The AAA security services make it easy for the network devices to perform line-based authentication. No matter which line authentication method you decide to use, you just need to execute the **aaa authentication login** command to define one or more authentication method list and apply it on the specific line that need the line authentication.

To configure the AAA PPP authentication, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable AAA.
aaa authentication login {**default** |*list-name} method1 [method2...]*	Define an accounting method list, or repeat this command to define more.
line vty *line-num*	Enter the line that needs to apply the AAA authentication.
login authentication {**default**|*list-name*}	Apply the method list on the line.

The keyword "list-name" is used to name the created authentication method list, which can be any string. The keyword "method" means the actual algorithm for authentication. Only when the current method returns ERROR (no reply), the next authentication method will be attempted. If the current method returns FAIL, no authentication method will be used any more. To make the authentication return successfully, even if no specified methods reply, it is possible to specific "none" as the last authentication method.

In the example below, it is possible to pass the identity authentication even if the Radius server returns TIMEOUT. **aaa authentication login default group radius none**


Caution

Since the keyword "**none**" enables any dialup user can pass the authentication even if the security server has no reply, it is only used as the backup authentication method. We suggest not using the "**none**" identity authentication in general cases. In special case when all possible dialup users are trustful, and no delay due to system fault is allowed for the user's work, it is possible to use "**none**" as the last identity authentication method in case the security server has no reply. And we recommend adding the local authentication method before the "**none**" authentication method.

Keyword	Description
local	Use the local username database for authentication
none	Do not perform authentication
group radius	Use Radius for authentication

The table above lists the AAA login authentication methods supported by our product.

46.3.5.1 Using the local database for Login authentication

To configure the login authentication with local database, it is required to configure the local database first. Our product supports authentication based on the local database. To establish the username authentication, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
username *name* [**password** *password*] or **username** *name* [**access-class** *number*]	Establish the username authentication using the password, or the access list.
username *name* [**privilege** *level*]	(Optional) Set the privilege level for the user.
username *name* [**autocommand** *command*]	(Optional) Set the command auto-executed after the user login.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

To define the local login authentication method list and apply it, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication login {**default** | *list-name*} **local**	Define the local method list.
end	Return to the privileged mode.
show aaa *method-list*	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode
login authentication {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

46.3.5.2 Using Radius for Login authentication

To configure the use of RADIUS authentication server for login authentication, it is required to first configure the RADIUS server. Our product supports the authentication based on the RADIUS server. To configure the RADIUS server, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
end	Return to the privileged mode.
show radius server	Show the RADIUS server.

After the RADIUS server is configured, make sure of successful communication with the RADIUS server before configuring the RADIUS for authentication. For details of the RADIUS server configurations, see *Configuring RADIUS*.

Now it is possible to configure the RADIUS server based method list. Run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication login {**default** | *list-name*} **group radius**	Define the local method list.
end	Return to the privileged mode.
show aaa *method-list*	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode
login authentication {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

46.3.6 Configuring the AAA Enable Authentication

This section deals with how to configure the AAA Enable authentication methods supported by our product:

In many cases, the user needs to Telnet the network access server (NAS). After passing the authentication, the user enters the Command Line Interface (CLI) and is assigned an initial command execution privilege (0-15 level). You can execute different commans in different levels and use the **show privilege** command to display the current level. For the details, see *using the CLI*.

After logging in the CLI, you can use the enable command to improve the privilege level if you fail to execute some commands due to low initial privilege level. To prevent the unauthorized access to the network, the identity authentication, named Enable authentication, is necessary when improving the privilege level.

To configure the AAA Enable authentication, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable AAA.
aaa authentication enable default *method1 [method2...]*	Define an enable authentication method list, for example RADIUS.

Command	Function
line vty *line-num*	Enter the line that needs to apply the AAA authentication.
login authentication {**default**|*list-name*}	Apply the method list on the line.

It can only define one enable authentication method list globally, so it is no need to define the name of the method list. The keyword "method" means the actual algorithm for authentication. Only when the current method returns ERROR(no reply), the next authentication method will be attempted. If the current method returns FAIL, no authentication method will be used any more. To make the authentication return successfully, even if no specified methods reply, it is possible to specify **none** as the last authentication method.

Once configured, the enable authentication method takes effect. When executing **enable** command in the privileged mode, it prompts to authenticate if you want to switchover a higher privilege level. It is no need to authenticate if the privilege level to be set is lower than or equal to the current one.

Caution

The current username will be recorded if the Login authentication(except for **none** method) is done when entering the CLI. At this time, if the Enable authencation processes, it will not prompt to input the username and you can use the same username of Login authentication. Note that the password input must be consistent.

The username information will not be recorded if there is no Login authentication when entering the CLI, or the **none** method is used. At this time, if the Enable authentication processes, you shall input the username again. This username will not be recorded, so you shall input it every time when the Enable authentication processes.

Some authentication methods can bind the security level. Then in the process of authentication, except for the returned response according to the security protocol, it is necessary to verify the binded security level. If the service protocol can bind the security level, the level shall be verified while authenticating. If the binded level is more than or equal to the level to be configured, the enable authentication and level switchover succeed. But if the binded level is less than the level to be configured, the enable authentication fails, prompting the error message and keeping the current level. If the service protocol fails to bind the security level, you can configure the level without verification of the binded level.

Caution

Now only RADIUS and Local authentication support to bind the securiy level. To this end, only the security levels of these two methods are checked.

46.3.6.1 Using the local username database for Enable authentication

When processing the enable authentication with local database, you can configure the user privilege level while configuring the local user. By default, the privilege level is 1. To configure the enable authentication with local database, it is required to configure the local database first and configure the privilege level. To establish the username authentication, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
username *name* [**password** *password*]	Establish the local username and set the password.

Command	Function
username *name* [**privilege** *level*]	Set the user privilege level. (Optional)
end	Return to the privileged mode.
show running-config	Confirm the configuration.

To define the local Enable authentication method list, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication enable default local	Define the local method list.
end	Return to the privileged mode.
show aaa method-list	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
show running-config	Confirm the configuration.

46.3.6.2 Using Radius for Enable authentication

The standard RADIUS server can pass the privilege level binded with the Service-Type attribute(the standard attribute number is 6), can specify the privilege with 1 or 15 level. The extened RADIUS server (for example, SAM) can configure the privilege level of the administrator(the private attribute number is 42), can specify 0-15 privilege level. For the details of the RADIUS server, see *Specifying the RADIUS Private Attribute Type* in *Configuring RADIUS*.

To configure the use of RADIUS authentication server for enable authentication, it is required to first configure the RADIUS server, then the RADIUS server-based enable authentication method list. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication enable default group radius	Define RADIUS authentication method.
end	Return to the privileged mode.
show aaa method-list	Confirm the configured method list.
show running-config	Confirm the configuration.

46.3.7 Configuring the AAA Authentication for PPP User

PPP is a link-layer protocol of carrying the network-layer datagram in the point-to-point link. In many circumstances, the user accesses to the NAS(Network Access Server) by asynchronous or ISDN dail. Once the connection has been set up, the PPP negotiation will be enabled. To prevent the unauthorized access to the network, the identity authentication is required for the dailed user in the process of PPP negotiation.

This section deals with how to configure the AAA Enable authentication methods supported by DES-7210 product. To configure the AAA Enable authentication, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable AAA.
aaa authentication ppp {default | *list-name***}** *method1 [method2...]*	Define a PPP authentication method list. RADIUS, TACACS+ remote authentication and using the local database are the supported authentication methods.
interface *interface-type interface-number*	Enter the asynchronous or ISDN interface that needs to apply the AAA authentication.
ppp authentication {**chap** | **pap**} {**default** | *list-name*}	Apply the method list on the asynchronous or ISDN interface.

For the detailed configuration method for the PPP, see the related chapter in *Configuring PPP, MP*.

46.3.8 Configuring the AAA Authentication for 802.1x User

IEEE802.1x is a standard of Port-Based Network Access Control, providing the point-to-point secure access for the LAN, and a means of the authentication of the user connecting to the LAN device.

This section deals with how to configure the 802.1x authentication methods supported by DES-7210 product. To configure the AAA Enable authentication, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable AAA.
aaa authentication dot1x {default | *list-name***}** *method1 [method2...]*	Define an IEEE802.1x authentication method list. RADIUS remote authentication and using the local database are the supported authentication methods.
dot1x authentication *list-name*	Apply the method list to 802.1x.

For the detailed configuration method for the IEEE802.1x, see the related chapter in *Configuring 802.1x*.

46.3.9 Example of Authentication Configuration

The example below illustrates show to configure the network device to use “Radius + local” for authentication.

```
DES-7210(config)# aaa new-model
DES-7210(config)# username DES-7210 password starnet
DES-7210(config)# radius-server host 192.168.217.64
DES-7210(config)# aaa authentication login test group radius local
DES-7210(config)# line vty 0
DES-7210(config-line)# login authentication test
DES-7210(config-line)# end
DES-7210# show running-config
!
aaa new-model
```

```
!
!
aaa authentication login test group radius local
username DES-7210 password 0 starnet
!
radius-server host 192.168.217.64
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
!
```

In the example above, the access server uses the Radius server (IP 192.168.217.64) to perform authentication for the login users. If the Radius server has no reply, the local database will be used for the identity authentication.

46.3.10 Example of Terminal Service Application Configuration

In the environment of the terminal service application, the terminal first connects to the asynchronous console, then offers the service accessing the network network server. However, if AAA is enabled, the Login authentication is necessary in all lines. To access the server, the terminal must pass the Login authentication and it influences the terminal service. You can separate two lines by configuration that makes the line using the terminal service directly connecting the server without the Login authentication, and ensures the device security by the Login authentication of the line connecting the device. That is to say, you can configure a login authentication list specific for the terminal service but the authentication method as **none**. Then apply the configured list to the line with terminal service enabled, while other lines connecting the local device is unchanged. Thereof the terminal can skip the local login authentication.

The example below illustrates the configuration steps:

```
DES-7210(config)# aaa new-model
DES-7210(config)# username DES-7210 password starnet
DES-7210(config)# radius-server host 192.168.217.64
DES-7210(config)# radius-server key test
DES-7210(config)# aaa authentication login test group radius local
DES-7210(config)# aaa authentication login terms none
DES-7210(config)# line tty 1 4
DES-7210(config-line)# login authentication terms
DES-7210(config-line)# exit
DES-7210(config)# line tty 5 16
DES-7210(config-line)# login authentication test
DES-7210(config-line)# exit
DES-7210(config)# line vty 0 4
DES-7210(config-line)# login authentication test
DES-7210(config-line)# end
DES-7210(config)# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
aaa authentication login terms none
```

```
username DES-7210 password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line aux 0
line tty 1 4
login authentication terms
line tty 5 16
login authentication test
line vty 0 4
login authentication test
!
!
```

In the example above, the access server uses the Radius server (IP 192.168.217.64) to perform authentication for the login users. If the Radius server has no reply, the local database will be used for the identity authentication. Login authentication is unnecessary for tty 1-4 is the used line of the terminal service, while using other tty and vty lines needs the login authentication.

46.4 Configuring Authorization

The AAA authorization enables the administrator to control the user's use of the services or the rights. After the AAA authorization service is enabled, the network device configures the user sessions by using the user configuration file stored locally or in the server. After the authorization is completed, the user can only use the services allowed in the profile or has the allowed rights.

46.4.1 Authorization Types

Our product supports the following AAA authorization methods:

- Exec authorization method – the user terminal loggs in the NAS CLI and is granted the privilege level (0-15 level).
- Command authorization method – after the user terminal loggs in the NAS CLI, the specific commands are authorized.
- Network authorization method – grant the available service to the user session in the network.

Note

Only TACACS+ supports the command authorization method. For the detailed information, please refer to *TACACS+ Configuration*.

46.4.2 Preparations for Authorization

The following tasks must be completed before the AAA authorization is configured:

- Enable the AAA server. For the details, see *AAA Overview*.
- (Optional) Configure the AAA authentication. The authorization is done after the user passes the authentication. But sole authorization can also be done without authentication. For details of the AAA authentication, see *Configuring Authentication*.
- (Optional) Configure security protocol parameters. If the security protocol is required for authorization, it is required to configure the security protocol parameters. The network authorization only supports RADIUS; the Exec authorization supports RADIUS and TACACS+. For details of the RADIUS, see *Configuring RADIUS*. For details of the TACACS+, see *Configuri*ng *TACACS+*.

- (Optional) If the local authorization is required, it is required to use the **username** command to define the user rights.

46.4.3 Configuring Authorization List

To enable AAA authorization, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authorization exec network{**default** | *list-name} method1 [method2*|…]	Define the AAA Exec authorization method.
aaa authorization network network{**default** | *list-name} method1 [method2*|…]	Define the AAA Command authorization method.

46.4.4 Configuring AAA Exec Authorization

The Exec authorization grants the privilege level of command execution for the user terminal loggs in the network access server (NAS). You can use the **show privilege** command to display the specific level after the user loggs in the NAS CLI successfully (by telnet, for example).

No matter which Exec authorization method you decide to use, you just need to execute the **aaa authorization exec** command to define one or more authorization method list and apply it to the specific line that need the Exec authorization.

To configure the AAA Exec authorization, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authorization exec network{**default** | *list-name} method1 [method2*|…]	Define the AAA Exec authorization method. If you need to define multiple methods, execute this command repeatedly.
line vty *line-num*	Enter the line to which the AAA Exec authorization method is applied.
authorization exec {**default** | *list-name*}	Apply the method to the line.

The keyword "list-name" is used to name the created authorization method list, which can be any string. The keyword "method" means the actual algorithm for authorization. Only when the current method returns ERROR (no reply), the next authorization method will be attempted. If the current method returns FAIL, no authorization method will be used any more. To make the authorization return successfully, even if no specified methods reply, it is possible to specific "none" as the last authorization method.

In the example below, it is possible to pass the Exec authorication even if the Radius server returns TIMEOUT

aaa authorization exec default group radius none

Keyword	Description
local	Use the local username database for Exec authorization.
none	Do not perform Exec authorization.

Keyword	Description
group radius	Use Radius for Exec authorization.
group tacacs+	Use Tacacs+ for Exec authorization.

The table above lists the AAA Exec authorization methods supported by our product.

Caution

The exec authorization is always used together with the login authentication, and they can be applied to the same line at the same time. But note that it is possible to have different results of the authentication and the authorization towards the same user because they can use different methods and servers. If the exec authorization fails, even though the login authentication has passed, the user can not access the CLI.

46.4.4.1 Using the local username database for exec authorization

To configure the Exec authorization with local database, it is required to configure the local database first. You can configure the user privilege level while configuring the local user. By default, the privilege level is 1. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
username *name* [**password** *password*]	Establish the local username and set the password.
username *name* [**privilege** *level*]	Set the user privilege level. (Optional)
end	Return to the privileged mode.
show running-config	Confirm the configuration.

To define the local Exec authorization method list, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authorization exec {**default** | *list-name*} **local**	Define the local method list.
end	Return to the privileged mode.
show aaa method-list	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode.
authorization exec {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

46.4.4.2 Using Radius for exec authorization

To configure the use of RADIUS server for Exec authorization, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see *Configuring RADIUS*.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication enable {**default** | *list-name*} **group radius**	Define RADIUS authentication method.
end	Return to the privileged mode.
show aaa method-list	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode.
authorization exec {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

46.4.4.3 Example of Configuring Exec Authorization

The example below illustrates how to configure exec authorization. The local login authentication and the "Radius+local" exec authorization are used when the user on the vty line 0-4 loggs in. The access server uses the Radius server with IP address 192.168.217.64 and shared keyword *test.* The local username and password are *DES-7210,* and the privilege level is *6*.

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
DES-7210(config)# radius-server host 192.168.217.64
DES-7210(config)# radius-server key test
DES-7210(config)# username DES-7210 password DES-7210
DES-7210(config)# username DES-7210 privilege 6
DES-7210(config)# aaa authentication login mlist1 local
DES-7210(config)# aaa authentication exec mlist2 group radius local
DES-7210(config)# line vty 0 4
DES-7210(config-line)# login authentication mlist1
DES-7210(config-line)# authorization exec mlist2
DES-7210(config-line)# end
DES-7210(config)# show running-config
!
aaa new-model
!
aaa authorization lexec mlist2 group radius local
aaa authentication login mlist1 local
!
username DES-7210 password DES-7210
username DES-7210 privilege 6
!
Radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
authorization exec mliat2
login authentication mlist1
```

```
!
end
```

46.4.5 Configuring AAA Network Authorization

Our product support the network authorization over the network connection including PPP, SLIP. The network authorization makes the network connection obtain the service like traffic, bandwidth, timeout, ect. The network authorization only support the RADIUS. The authorization information assigned from the server are encapsulated in the RADIUS attribute. For different network connection application, it is possible that these authorization information are different.

Caution Now the configuration does not support the 802.1X AAA authorization, while the 802.1X is implemented by using other commands. For the details of the 802.1X authorization, see *Configuring 802.1X*.

To configure the AAA network authorization, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authorization network{**default** | *list-name} method1 [method2*|*…*]	Define the AAA network authorization method. If you need to define multiple methods, execute this command repeatedly.

The keyword "list-name" is used to name the created authorization method list, which can be any string. The keyword "method" means the actual algorithm for authorization. Only when the current method returns ERROR (no reply), the next authorization method will be attempted. If the current method returns FAIL, no authorization method will be used any more. To make the authorization return successfully, even if no specified methods reply, it is possible to specific "none" as the last authorization method.

46.4.5.1 Using Radius for network authorization

To configure the use of RADIUS server for network authorization, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see *Configuring RADIUS*.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication network {**default** | *list-name*} **group radius**	Define RADIUS authentication method.

46.4.5.2 Example of Configuring Network Authorization

The example below illustrates how to configure network authorization.

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
DES-7210(config)# radius-server host 192.168.217.64
DES-7210(config)# radius-server key test
```

```
DES-7210(config)# aaa authorization network test group radius local
DES-7210(config-line)# end
DES-7210(config)# show running-config
!
aaa new-model
!
aaa authorization network test group radius none
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
```

46.5 Configuring Accounting

The AAA accounting function enables you to trace the services and network resources used by the user. After the accounting function is enabled, the network access server or router sends the user's network accesses to the Radius security server by means of attribute pair. You may use some analysis software to analyze these data to implement the billing, audition and tracing function for the user's activities.

46.5.1 Accounting Types

Our product currently supports the following accounting types:

- Exec Accounting -- record the accounting information of entering to and exiting from the CLI of the user terminal logged in the NAS CLI.
- Command Accounting – record the specific command execution information after the user terminal loggs in the NAS CLI.
- Network Accounting – records the related information on the user session in the network.

Note

Only TACACS+ supports the command accounting function. For the detailed information, please refer to *TACACS+ Configuration*.

46.5.2 Preparations for Accounting

The following tasks must be completed before the AAA accouting is configured:

- Enable the AAA server. For the details, see *AAA Overview*.
- Define the security protocol parameters. It is required to configure the security protocol parameters for accouting. The network accounting only supports RADIUS; the Exec accounting supports RADIUS and TACACS+; the Command accounting supports TACACS+ only. For details of the RADIUS, see *Configuring RADIUS*. For details of the TACACS+, see *Configuri*ng *TACACS+*.
- (Optional) Configure the AAA authentication. The accounting is done after the user passes the authentication(for example, Exec accounting). In some circumstances, the accouting can also be done without authentication. For details of the AAA authentication, see *Configuring Authentication*.

46.5.3 Configuring AAA Exec Accounting

The exec accounting records the information of entering to and exiting from the CLI of the user terminal logged in the NAS. When the user terminal loggs in and enters to the NAS CLI, it sends the accounting start information to the security server. When the user terminal exits from the CLI, it sends the accounting stop information to the server.

Caution

Only after the user terminal logged in the NAS has passed the login authentication, the exec accounting starts. If no login authentication or **none** authentication method has been configured, no exec accounting processes. For the same user terminal, if it sends no accounting start information to the security server when logging in, no accounting stop information will be sent when logging out.

To configure the AAA Exec accounting, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa accounting exec network{**default** | *list-name}* **start-stop** *method1 [method2*|…]	Define the AAA Exec accounting method list. If you need to define multiple method lists, execute this command repeatedly.
line vty *line-num*	Enter the line to which the AAA Exec accounting is applied.
accounting exec {**default** | *list-name*}	Apply the method list to the line.

The keyword "list-name" is used to name the created accounting method list, which can be any string. The keyword "method" means the actual algorithm for accounting. Only when the current method returns ERROR (no reply), the next accounting method will be attempted. If the current method returns FAIL, no accounting method will be used any more. To make the accounting return successfully, even if no specified methods reply, it is possible to specific "none" as the last accounting method.

Note

The keyword "start-stop" is used for the network access server to send the accounting information at the start and end of the network service to the security server.

46.5.3.1 Using the Radius for exec accounting

To configure the use of RADIUS server for Exec acounting, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see *Configuring RADIUS*.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa accounting exec {**default** | *list-name*} **start-stop group radius**	Define RADIUS accounting method.
end	Return to the privileged mode.
show aaa method-list	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode.
accounting exec {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

46.5.3.2 Example of Configuring Exec Accounting

The example below illustrates how to configure exec accounting. The local login authentication and the Radius exec authorization are used when the user on the vty line 0-4 loggs in. The access server uses the Radius server with IP address 192.168.217.64 and shared keyword *test.* The local username and password are *DES-7210*

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
DES-7210(config)# radius-server host 192.168.217.64
DES-7210(config)# radius-server key test
DES-7210(config)# username DES-7210 password DES-7210
DES-7210(config)# aaa authentication login auth local
DES-7210(config)# aaa accouting exec acct start-stop group radius
DES-7210(config)# line vty 0 4
DES-7210(config-line)# login authentication auth
DES-7210(config-line)# accounting exec acct
DES-7210(config-line)# end
DES-7210(config)# show running-config
!
aaa new-model
!
aaa accounting exec acct start-stop group radius
aaa authentication login auth local
!
username DES-7210 password DES-7210
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
accounting exec acct
login authentication auth
!
end
```

46.5.4 Configuring AAA Network Accounting

The network accounting provides the accounting information about user session, including the packet number, bytes, IP address and username. Now the network accounting only support RADIUS.

Note

The format of Radius accounting information varies with the Radius security server. The contents of the account records may also vary with our product version.

To configure the AAA network accounting, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.

Command	Function
aaa accounting network{**default** | *list-name}* **start-stop** *method1 [method2*|…]	Define the AAA network accounting method list. If you need to define multiple method lists, execute this command repeatedly.

The keyword "list-name" is used to name the created accounting method list, which can be any string. The keyword "method" means the actual algorithm for accounting. Only when the current method returns ERROR (no reply), the next accounting method will be attempted. If the current method returns FAIL, no accounting method will be used any more. To make the accounting return successfully, even if no specified methods reply, it is possible to specific "none" as the last accounting method.

46.5.4.1 Using Radius for network accounting

To configure the use of RADIUS server for network acounting, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see *Configuring RADIUS*.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa accounting network {**default** | *list-name*} **start-stop group radius**	Define RADIUS accounting method.

46.5.4.2 Example of Configuring Network Accounting

The example below illustrates how to configure network authorization using RADIUS.

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
DES-7210(config)# radius-server host 192.168.217.64
DES-7210(config)# radius-server key test
DES-7210(config)# aaa accounting network acct start-stop group radius
DES-7210(config-line)# end
DES-7210(config)# show running-config
!
aaa new-model
!
aaa accounting network acct start-stop group radius
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
```

46.6 Monitoring AAA user

To view the information of the current login users, run the following commands in the privileged user mode:

Command	Function
show aaa user { *id* | **all** }	View the information of the current AAA user.

46.7 Configuring VRF-supported AAA Group

Virtual Private Networks (VPNs) provides a secure method for bandwidth share on the ISP backbone network. One VPN is the collection of the sharing routes. The user station is linked with the service vendor network via one to multiple interfaces. The VPN routing table is also called VPN routing//forwarding(VRF) table. AAA can specify the VRF for each self-defined server group.

In the global configuration mode, use the following command to configure VRF for the AAA group:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa group server radius *gs_name*	Configure the RADIUS server group and enter the server group configuration mode.
ip vrf forwarding *vrf_name*	Specify the vrf for the group.

Note

It is valid for the product supporting VRF function.

46.8 Configuring Failed Authentication Lockout of Login User

To prevent login user from decoding password, use command to limit the attempt times. If you has attempted more than the limited times, you will not login during the lockout.

In the global configuration mode, use the following command to configure login parameters:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa local authentication attempts *<1-2147483647>*	Configure attempt times of login user.
aaa local authentication lockout-time*<1-2147483647>*	Configure lockout-time(hour) when the user has attempted more than the limited times.
show aaa user lockout {**all** | **user-name** <*word*>}	Display current lockout user list.
clear aaa local user lockout {**all** | **user-name** <*word*>}	Clear lockout user list.

Note

By default, login attempt times is 3 and the lockout time is restricted to be 15 hours.

47 RADIUS Configuration

47.1 Radius Overview

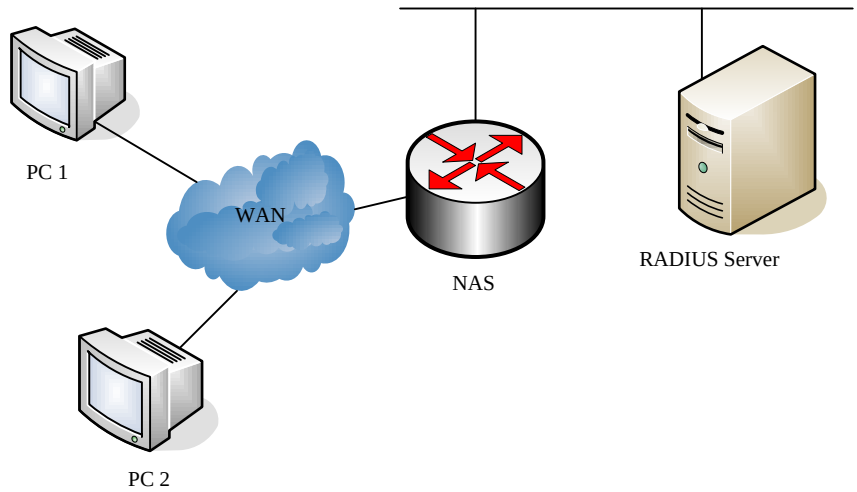
The Remote Authentication Dial-In User Service (Radius) is a distributed client/server system that works with the AAA to perform authentication for the users who are attempting to make connection and prevent unauthorized access. In the implementation of our product, the RADIUS client runs on the router or the network access server (NAS) to send the authentication requests to the central RADIUS server. The central center includes all information of user authentication and network services.

Since the RADIUS is a completely-open protocol, it has become a component and been installed in such systems as UNIX and WINDOWS 2000, so it is the security server most widely used for the time being.

The running process of the RADIUS is as follows:

- Prompt the user to enter username and password.
- The username and the encrypted password are sent to the RADIUS server via the network.
- The RADIUS returns one of the following responses:
- The user authentication passes.
- The user authentication fails and it prompts to reenter the username and password.
- The RADIUS server sends the challenge request to gather more authentication information from the user.
- The user authorization information is included in the ACCEPT response.

Here is a typical RADIUS topology:



Typical RADIUS network configuration

47.2 RADIUS Configuration Tasks

To configure Radius on the network device, perform the following tasks first:

- Enable AAA. For the details, see *AAA Overview*.
- Define the RADIUS authentication method list by using the **aaa authentication** command. For details about how to use "aaa authentication" to define the authentication method list, see *Configuring Authentication*.
- Apply the defined authentication list on the specific line; otherwise the default authentication list will be used for authentication. For more details, see *Configuring Authentication.*

After the configuration is completed, you may start to configure the RADIUS. The configuration of the RADIUS consists of the following parts:

- Configuring Radius Protocol Parameters
- Specify the RADIUS authentication.

47.2.1 Configuring Radius Protocol Parameters

Before configuring the Radius on the network device, the network communication shall operate perfectly on the Radius server. To configure RADIUS protocol parameters, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the IP address or hostname of the remote Radius security server and specify the authentication port and accounting port.
radius-server key *string*	Configure the sharing password for the communication between the device and Radius server
radius-server retransmit *retries*	Specify the times of sending requests before the router confirms Radius invalid (3 by default)
radius-server timeout *seconds*	Specify the waiting time before the router resend request (2 s by default)
radius-server deadtime *minutes*	Specify the waiting time before the server is considered dead in case of no response to the request sent by the device (5 minutes by default).

Caution To configure the RADIUS, it is necessary to configure the RADIUS Key. The sharing password on the network device and the sharing password on the Radius server must be the same.

47.2.2 Specifying the Radius Authentication

This means defining the authentication method list for the Radius after the Radius server is specified and the Radius authentication sharing password is defined. Since the RADIUS

authentication is done via AAA, it is required to execute the **aaa authentication** command to define the authentication method list and specify the authentication method as RADIUS. For more details, see AAA Configurations.

47.2.3 Specify Radius Private Attribute Type

The contents in this section enable configuring freely the type of private attributes. The default configurations are as follows:

Default configurations of our product private attribute recognition:

ID	Function	Type
1	max down-rate	1
2	qos	2
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-diractory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	16
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilige	22
23	login privilige	42
24	limit to user number	50

Extended manufacturer ID default configuration:

ID	Function	TYPE
1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8

ID	Function	TYPE
9	file-diractory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilige	22
23	login privilige	42
24	limit to user number	50

Note

Two functions cannot be configured with the same type number.

Here is an example on how to configure the private type for network device:

```
DES-7210# show radius vendor-specific
id    vendor-specific       type-value
----- --------------------  ----------
1     max down-rate         76
2     qos                   77
3     user ip               3
4     vlan id               4
5     version to client     5
6     net ip                6
7     user name             7
8     password              8
9     file-diractory        9
10    file-count            10
11    file-name-0           11
12    file-name-1           12
13    file-name-2           13
14    file-name-3           14
15    file-name-4           15
16    max up-rate           75
17    version to server     17
18    flux-max-high32       18
19    flux-max-low32        19
20    proxy-avoid           20
21    dailup-avoid          21
22    ip privilige          22
```

```
23   login privilige      42
24   limit to user number 50
DES-7210# configure
DES-7210(config)# radius attribute 24 vendor-type 67
DES-7210(config)# show radius vendor-specific
id   vendor-specific      type-value
---- -------------------- ----------
1    max down-rate        76
2    qos                  77
3    user ip              3
4    vlan id              4
5    version to client    5
6    net ip               6
7    user name            7
8    password             8
9    file-diractory       9
10   file-count           10
11   file-name-0          11
12   file-name-1          12
13   file-name-2          13
14   file-name-3          14
15   file-name-4          15
16   max up-rate          75
17   version to server    17
18   flux-max-high32      18
19   flux-max-low32       19
20   proxy-avoid          20
21   dailup-avoid         21
22   ip privilige         22
23   login privilige      42
24   limit to user number 50
DES-7210(config)#
DES-7210(config)#
```

47.3 Monitoring RADIUS

To monitor the RADIUS, execute the following commands in the privileged user mode:

Command	Function
debug radius event	Turn on the Radius debug switch to view the Radius debug information

47.4 Radius Configuration Example

In a typical Radius network configuration diagram, the RADIUS server performs authentication for the visiting users, enables the accounting function for the visiting users and records the network usage of the users.

Note

The RADIUS server can be a component that comes with the Windows 2000/2003 server (IAS) or the UNIX system, or the special server software of some manufacturers.

Here is an example on how to configure the Radius for network device:

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
DES-7210(config)# radius-server host 192.168.12.219
auth-port 1645 acct-port 1646
DES-7210(config)# radius-server key aaa
DES-7210(config)# aaa authentication login test group radius
DES-7210(config)# end
DES-7210# show radius server
Server IP:       192.168.12.219
Accounting Port: 1646
Authen  Port:    1645
Server State:    Ready
DES-7210#configure terminal
DES-7210(config)#line vty 0
DES-7210(config-line)#login authentication test
DES-7210(config-line)#end
DES-7210#show running-config
!
aaa new-model
!
!
aaa authentication login test group radius
!
username DES-7210 password 0 starnet
!
radius-server host 192.168.12.219 auth-port 1645 acct-port 1646
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

48 TACACS+ Configuration

48.1 TACACS+ Overview

TACACS+ is a security protocol with more powerful function on the basis of TACACS (RFC 1492 Terminal Access Controller Access Control System). It implements AAA function of multi-users by Client-Server mode and TACACS server communication. It needs to configure the related contents of TACACS+ server before using TACACS+ server.

TACACS+ supports user authentication, authorization and accounting analysis. That is, we can use one server to authenticate, another one to authorize and the third one to account at the same time. Each server has its own user data information, being antagonistic to authenticate, authorize and account.

The table below shows TACACS+ packet format:

4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

Figure 1

- Major Version — Major TACACS+ Version number;
- Minor Version — Minor TACACS+ Version number;
- Packet Type — the value may include:

TAC_PLUS_AUTHEN: = 0x01 (Authentication);
TAC_PLUS_AUTHOR:= 0x02 (Authorization);
TAC_PLUS_ACCT:= 0x03 (Accounting).

- Sequence Number — packet sequence number in current session. The first TACACS+ packet sequence number in the session must be 1 and every packet sequence number followed is added by 1 gradually. Therefore, the client only sends the packet with odd sequence number, while TACACS+ Daemon only sends the packet with even sequence number.
- Flags — this field includes flag with various bitmap format. The Flag value indicates whether the packet is encrypted or not.
- Session ID — ID in the TACACS+ session.
- Length —body length of TACACS+ packet (excluding head). All the packets are transmitted in the network in the encrypted form.

48.2 TACACS+ Application

The typical application of TACACS+ is the login management control of terminal users. TACACS+ client sends user name and password to TACACS+ server for authentication. After authentication and authorization, you can login to the switch for operation, which is shown as figure 2:

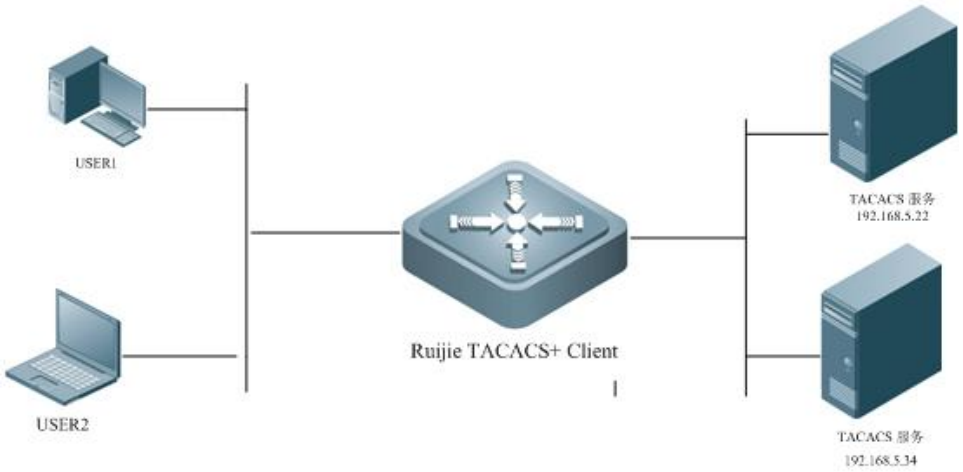


Figure 2

Figure 3 describes the interaction of the packets running in TACACS+ by login AAA:

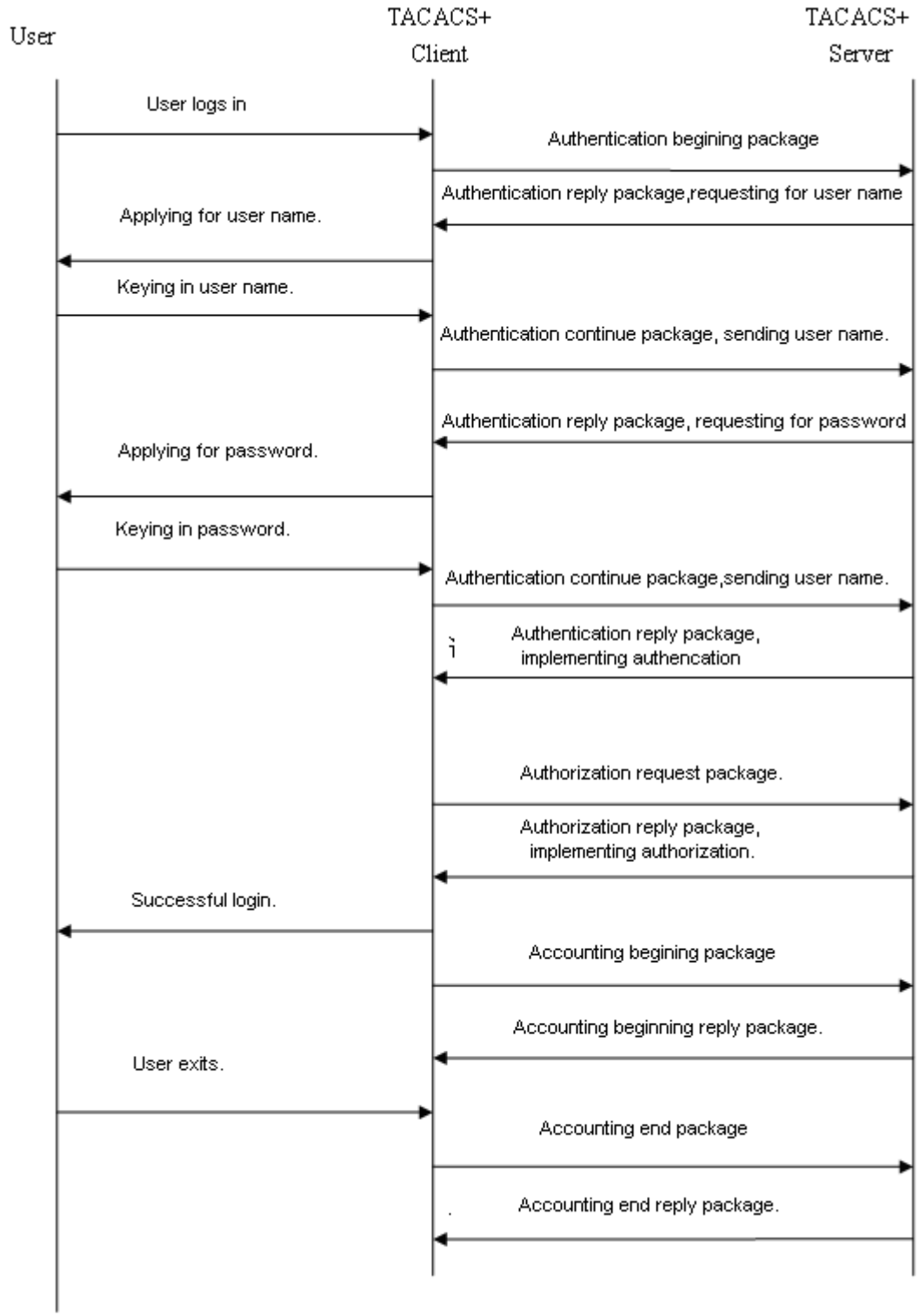


Figure 3

The whole process of basic information interaction is divided into three parts:

4. Authentication process includes:

a) User requests for logging in to the switch;

b) After receiving the request, TACACS+ Client sends the authentication beginning message to TACACS+ server;

c) TACACS+ server sends the authentication reply message, requesting for the user name;

d) TACACS+ Client asks user for user name.

e) The user keys in the login user name;

f) After receiving the user name, TACACS+ Client sends the authentication continue message including user name to TACACS+ server;

g) TACACS+ server sends authentication reply message, requesting for login password;

h) TACACS+ Client receives the login password;

i) The user keys in the login password;

j) After receiving the login password, TACACS+ Client sends authentication continue message including login password to TACACS+ server;

k) TACACS+ server sends authentication reply message, indicating that user has been authenticated.

5. Authorization process includes:

a) TACACS+ Client sends authorization request message to TACACS+ server.

b) TACACS+ server sends authorization reply message, indicating that user has been authenticated;

c) TACACS+ Client receives successful authorization reply message, outputting the configuration interface of switch to the user.

6. **Accounting process includes:**

c) TACACS+ Client sends the accounting beginning message to TACACS+ server;

d) TACACS+ server sends accounting beginning reply message, indicating that it has received the accounting beginning message;

e) The user exits;

f) TACACS+ Client sends the accounting end message to TACACS+ server;

g) TACACS+ server sends accounting end reply message, indicating that it has received the accounting end message.

48.3 TACACS+ Configuration Task

The following tasks must be executed before configuring TACACS+ on the network device:

- Use **aaa new-mode** to enable AAA. AAA must be enabled before using TACACS+; for the information how to enable **aaa new-mode**, please refer to AAA Overview.
- Use **tacacs-server host** to configure one or multiple tacacs+ servers.
- Use **tacacs-server key** to specify server and NAS shared key.
- Use **tacacs-server timeout** to specify timeout time waiting for the server reply;
- Use tacacs-server directed-request to enable the function of supporting the user to specify authentication server.
- If you need to authenticate, use **aaa authentication** to define using TACACS+ identity authentication method list. For the detailed information, please refer to authentication configuration.
- If you need to authorize, use **aaa authorization** to define using TACACS+ authorization method list. For the detailed information, please refer to authorization configuration.
- If you need to account, use **aaa accounting** to define using TACACS+ accounting method list. For the detailed information, please refer to accounting configuration.
- You shall use the defined authentication list in the specified line, or you use the list by default.

48.3.1 Configuring TACACS+ Protocol Parameter

You need to ensure that the network communication of TACACS+ server runs well before configuring TACACS+ on the network device. Use the following commands to configure TACACS+ protocol parameters:

Command	Function
configure terminal	Enter the global configuration mode.
aaa group server tacacs+ *group-name*	Configure TACACS+ group server, dividing different TACACS+ server into different groups.
server *ip-address*	Configure the server addresses in TACACS+ group server.
ip vrf forwarding *vrf-name*	Configure vrf name used in TACACS+ group server (this command exits on the device supporting VRF.)
tacacs-server host *ip-address* [**port** *integer*] [**timeout** *integer*] **key** [0 | 7] *string*	Configure IP address of remote TACACS+ security server; configures different parameters on this server by different parameter combination: ● *ip-address* :configures server address; ● **port** *intege* [optional] :determines the port used by the server; By default , the port number is 49 with the range from 1 to 65535. ● **timeout** *integer* [optional] :configures server timeout time; By default, the timeout time is 5s with the range from 1 to 1000s. ● **key** *string* [optional]:configures the key shared with the server of corresponding ip.
tacacs-server key [0 | 7] *string*	Configure the shared key used to communicate between the device and TACACS+ server. If the corresponding host does not set key by itself, you should set it globally.
tacacs-server timeout *seconds*	Specify the waiting time before the device resends request. By default, it is 5s. if the specified host does not set the specified timeout time, you should set the time globally.
tacacs-server directed-request [**restricted**] [**no-truncate**]	Configure the function of supporting the user specified authentication server. The default configuration is enabled.
Ip tacacs source-interface *interface*	Specify to send tacacs+ request to the source IP used by the server. By default, it does not specify.

Caution

You must configure TACACS+ Key before configuring TACACS+. The shared passwords on the network device and TACACS+ server must be consistent.

48.4 Using TACACS+ to Authenticate, Authorize and Account

In the typical TACACS+ network configuration figure, TACACS+ server authenticates, authorizes and accounts the access users. The following shows the examples of how to configure TACACS+ to authenticate, authorize and account by login authentication, authorization and accounting.

48.4.1 Using TACACS+ by Login Authentication

- Enables aaa first:

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
```

- Then configures tacacs+ server information:

```
DES-7210(config)# tacacs-server host 192.168.12.219
DES-7210(config)# tacacs-server key aaa
```

- Configures authentication method of using tacacs+:

```
DES-7210(config)# aaa authentication login test group tacacs+
```

- Applies the authentication method on the interface:

```
DES-7210(config)# line vty 0 4
DES-7210 (config-line)# login authentication test
```

Through the above configuration, you implement to configure login tacacs+ authentication. The configuration is shown as follows;

```
DES-7210#show running-config
!
aaa new-model
!
aaa authentication login test group tacacs+
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0
login authentication test
line vty 1 4
```

```
login authentication test
!
```

48.4.2 Using TACACS+ by Enable Authentication

8. Enables aaa first:

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
```

9. Then configures tacacs+ server information:

```
DES-7210(config)# tacacs-server host 192.168.12.219
DES-7210(config)# tacacs-server host 192.168.12.218
DES-7210(config)# tacacs-server host 192.168.12.217
DES-7210(config)# tacacs-server key aaa
```

Configures tacacs+ server group using a part of the servers in the server list:

```
DES-7210(config)# aaa group server tacacs+ tacgroup1
DES-7210(config-gs-tacacs)# server 192.168.12.219
DES-7210(config-gs-tacacs)# server 192.168.12.218
```

10. Configures authentication method of using tacgroup1:

```
DES-7210(config)# aaa authentication enable default group tacgroup1
```

Through the above configuration, you implement to configure enable authentication of some tacacs+ servers. The configuration is shown as follows;

```
DES-7210#show running-config
!
aaa new-model
!
!
aaa group server tacacs+ tacgroup1
server 192.168.12.219
server 192.168.12.218
!
aaa authentication enable default group tacgroup1
!
!
tacacs-server host 192.168.12.219
tacacs-server host 192.168.12.218
tacacs-server host 192.168.12.217
tacacs-server key aaa
!
line con 0
line vty 0
line vty 1 4
```

```
!
```

48.4.3 Using TACACS+ by Login Authorization

1. Enables aaa first:

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
```

2. Then configures tacacs+ server information:

```
DES-7210(config)# tacacs-server host 192.168.12.219
DES-7210(config)# tacacs-server key aaa
```

3. Configures the authorization method of using tacacs+:

```
DES-7210(config)# aaa authorization exex test group tacacs+
```

4. Applies the authorization on the interface:

```
DES-7210(config)# line vty 0 4
DES-7210 (config-line)# authorization exec test
```

Through the above configuration, you implement to configure to use tacacs+ by login authorization. The configuration is shown as follows:

```
DES-7210#show running-config
!
aaa new-model
!
!
aaa authorization exec test group tacacs+
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0
authorization exec test
line vty 1 4
authorization exec test
!
```

48.4.4 Using TACACS+ by Level 15 Command Audit

- Enables aaa first:

```
DES-7210# configure terminal
DES-7210(config)# aaa new-model
```

- Then configures tacacs+ server information:

```
DES-7210(config)# tacacs-server host 192.168.12.219
DES-7210(config)# tacacs-server key aaa
```

- Configures command audit method of using tacacs+:

```
DES-7210(config)# aaa accounting commands 15 default group start-stop tacacs+
```

- Applies the authorization on the interface:

```
DES-7210(config)# line vty 0 4
DES-7210 (config-line)# accounting commands 15 default
```

Through the above configuration, you implement to configure enable authentication of some tacacs+ servers. The configuration is shown as follows;

```
DES-7210# show running-config
!
aaa new-model
!
!
aaa accounting commands 15 default group tacacs+
!
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0
accounting commands 15 default
line vty 1 4
accounting commands 15 default
!
```

49 SSH Terminal Service Configuration

49.1 About SSH

SSH is the shortened form of Secure Shell. The SSH connection functions like a Telnet connection, except that all transmissions based on the connection are encrypted. When the user logs onto the device via a network environment where security cannot be guaranteed, the SSH feature provides safe information guarantee and powerful authentication function to protect the devices from IP address fraud, plain password interception and other kinds of attacks.

49.2 SSH Support Algorithms

Support algorithm	SSH1	SSH2
Signature authentication algorithm	RSA	RSA, DSA
Key exchanging algorithm	RSA public key encryption based key exchanging algorithm	KEX_DH_GEX_SHA1 KEX_DH_GRP1_SHA1 KEX_DH_GRP14_SHA1
Encryption algorithm	DES, 3DES, Blowfish	DES, 3DES, AES-128, AES-192, AES-256
User authentication algorithm	User password based authentication method	User password based authentication method
Message authentication algorithm	Not supported	MD5, SHA1, SHA1-96, MD5-96
Compression algorithm	NONE (uncompressed)	NONE (uncompressed)

49.3 SSH Supports

Caution

The DES-7200 series supports only the SSH server (compatible with the SSHv1 and SSHv2) but do not support the SSH client.

49.4 SSH Configuration

49.4.1 Default SSH Configurations

Item	Default value

Item	Default value
SSH service end status	Off
SSH version	Compatible mode (supporting versions 1 and 2)
SSH user authentication timeout period	120s
SSH user re-authentication times	3

49.4.2 User Authentication Configuration

1 For the consideration of the SSH connection security, the login without authentication is forbidden. Therefore, in the login authentication of the users, the login authentication mode must have password configured (no-authentication login allowed for telnet).

2 The username and password entered every time must have lengths greater than zero. If the current authentication mode does not need the username, the username can be entered randomly but the entry length must be greater than zero.

49.4.3 Enabling SSH Server

The SSH Server is disabled by default. To enable the SSH Server, run the **enable service ssh-server** command in the global configuration mode while generating SSH key.

Command	Description
configure terminal	Enter the global configuration mode.
enable service ssh-server	Enable SSH Server.
crypto key generate {rsa|dsa}	Generate the key

Caution

To delete the key, use the **crypto key zeroize** command rather than the **[no] crypto key generate** command.

49.4.4 Disabling SSH Server

When the SSH Server is enabled, if the public key on the server is deleted, the SSH Server is automatically closed. To delete the public key, run **no enable service ssh-server** in the global configuration mode to disable the SSH Server.

Command	Description
configure terminal	Enter the global configuration mode
no enable service ssh-server	Delete the key to disable SSH Server.

49.4.5 Configuring the Supported SSH Server Version

By default, the SSHv1 and SSHv2 are compatible. Run the following commands to configure the SSH version.

Command	Description
configure terminal	Enter the configuration mode
ip ssh version {1|2}	Configure the supported SSH version.
no ip ssh version	Restore the SSH default version.

49.4.6 Configuring SSH User Authentication Timeout

By default, the user authentication timeout period of the SSH SERVER is 120 seconds. Run the following commands to configure the SSH user authentication timeout period.

Command	Description
configure terminal	Enter the configuration mode
ip ssh time-out *time*	Configure the SSH timeout period (1-120sec)
no ip ssh time-out	Restore the SSH default user authentication timeout period 120 seconds.

49.4.7 Configuring SSH Re-authentication Times

This command is used to set the authentication attempts for SSH user requesting connections to prevent illegal actions such as malicious guesswork. The authentication attempts are 3 for the SSH Server by default. In other words, it allows the user to enter the username and password for three times to attempt the authentication. Run the following commands to configure the SSH re-authentication times:

Command	Description
configure terminal	Enter the configuration mode
ip ssh authentication-retries *retry times*	Configure SSH re-authentication times (range 0-5)
no ip ssh authentication-retries	Restore the default SSH re-authentication times as 3.

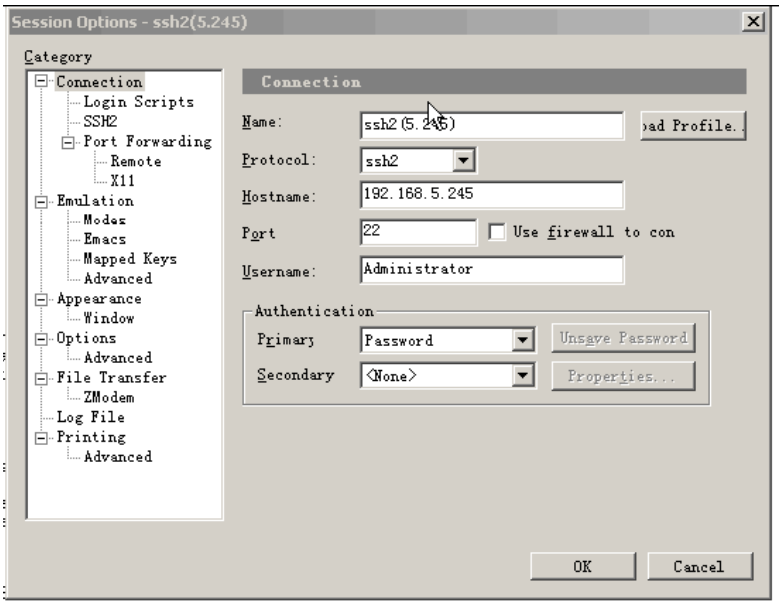
Note

For details of the above commands, see *SSH Command Reference Manual.*

49.5 Using SSH for Device Management

You may use the SSH for device management by first enabling the SSH Server function that is disabled by default. Since the Telnet that comes with the Windows does not support SSH, third-party client software has to be used. Currently, the clients with sound forward compatibility include Putty, Linux and SecureCRT. With the client software SecureCRT as an example, the SSH client configuration is described as follows (see the UI below):

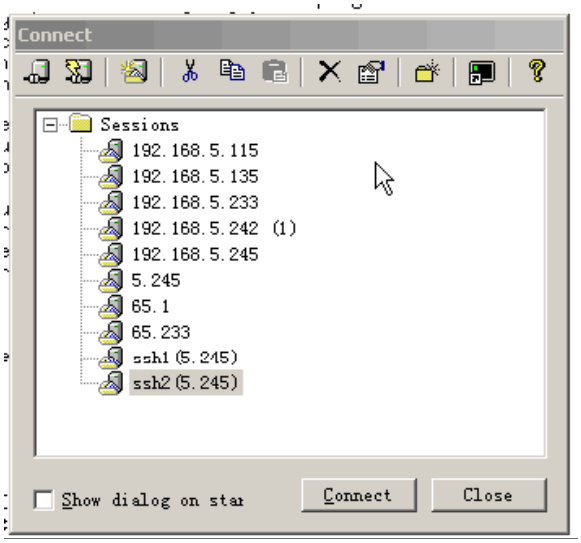
Figure-1



As shown in Figure-1, protocol 2 is used for login, so SSH2 is chosen in “Protocol”. “Hostname” indicates the IP address of the host that will log in, 192.168.5.245. Port 22 is the default number of the port for SSH listening. “Username” indicates the username, and does not take effect when the device only requires password. “Authentication” indicates the authentication mode, and the username/password authentication is supported here. The used password is the same as the Telnet password.

Click “OK” to pop up the following dialog:

Figure-2

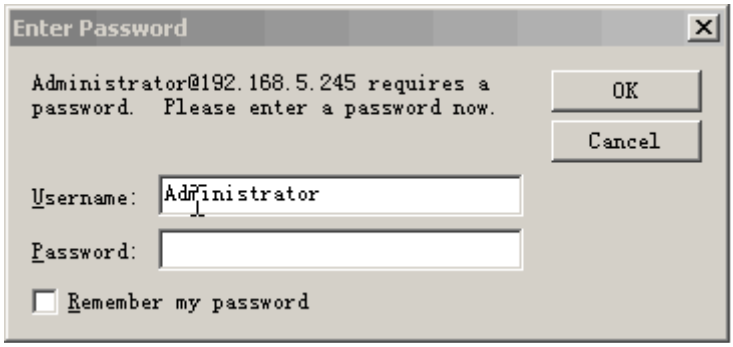


Click “Connect” to log into the host just configured, as shown below:

Figure-3

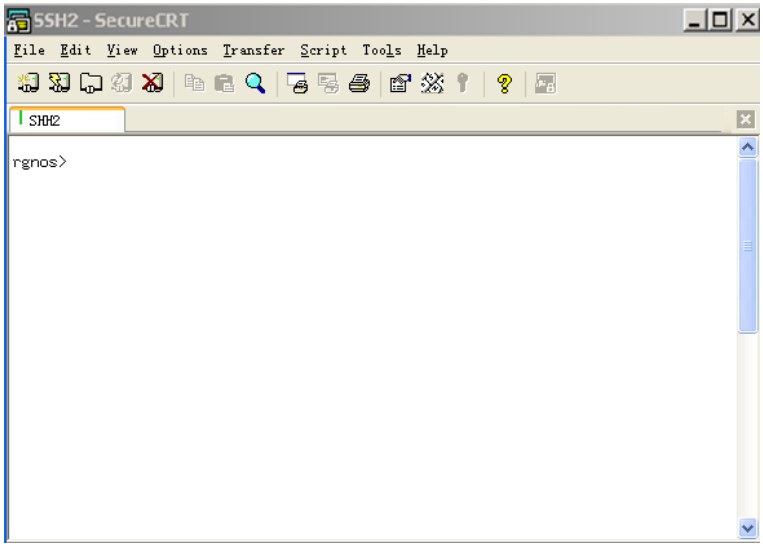
Ask the machine that is logging into the host 192.168.5.245 to see whether the key from the server end is received or not. Select “Accept & Save” or “Accept Once” to enter the password confirmation dialog box, as shown below:

Figure-4



Enter the Telnet login password to enter the UI that is the same as the Telnet. See the diagram below:

Figure-5



50 CPU Protection Configuration

50.1 Overview

50.1.1 Function of CPU Protect

Malicious attacks towards the switch CPU often occur in the network environment, and such attacks cause too high CPU utilization on the switch and abnormal operation of it. DES-7210 switch provides CPP function to reduce the CPU load and protect the normal operation.

CPP configuration helps adjust the parameters such as bandwidth, priority level, for the most detailed management.

Caution

The CPP (CPU Protect Policy) is a means to enhance switch security. With the CPP, the processor and channel bandwidth resource of the switch are protected to ensure the normal forwarding of the packets and normal running of the protocols.

50.1.2 Operating Principles of CPU Protect

The packets to be sent to the CPU of the supervisor engine are classified according to their L2, L3 and L4 information. The types of packets are different for L2 and L3 switches.

The CPU ports have eight priority queues. You can configure the queue for each type of packet and the hardware can automatically send the packets of the type to the specified queue according to your configuration. To ensure that the protocol packets with different opriority values can be sent to the CPU in time, poll scheduling algorithm is adopted. The scheduling weight of each queue are the same in the poll scheduling algorithm.

The switch provides a protection method to control the bandwidth and priority for each type of packets sent to the CPU. You can configure the maximum rate and priority for each type of packet sent to the CPU port in packets per second (PPS).

50.2 Configuring CPU Protect

The following sections describe how to configure CPU Protect.

- CPU Protect Default value
- Configuring the Bandwidth for Each Type of Packet
- Configuring the Priority for Each Type of Packet

50.2.1 CPU Protect Default value

The following lists the recommended factory settings of the maximum bandwidth and priority of each type of packet.

Type	Defaulted maximum bandwidth (pps)	Defaulted priority
TP-Guard	128	0
ARP	500	0
BPDU	128	6
DHCPS	128	0
DOT1X	128	0
GVRP	128	0
IPV6-MC	128	0
IGMP	128	3
OSPF	128	3
PIM	128	3
RERP	128	6
RIP	128	0
RLDP	128	6
VRRP	128	6
Unknown-IPMC	128	0
Err-TTL	128	0
DHCP_RELAY_CLIENT	128	0
DHCP_RELAY_SERVER	128	0
DHCP_OPTION82	128	0
UDP_HELPER	128	0

Use the command **no cpu-protected type** to restore the maximum bandwidth and priority setting of the packet to the default value.

50.2.2 Configuring the Bandwidth for Each Type of Packet

In the configuration mode, configure the bandwidth of each type of packet by performing the following steps:

Command	Function
DES-7210(config)# **cpu-protect type {arp | bpdu | dhcp | ipv6mc | igmp | rip | ospf | vrrp | pim | err-ttl | unknown-ipmc } pps** pps_vaule	Set the bandwidth for the packets in PPS, which is an integer.
DES-7210# **end**	Return to the privileged mode.

This example shows the bandwidth configuration process:

```
DES-7210(config)#cpu-protect type bpdu pps 200
Set packet type bpdu pps 100.
```

50.2.3 Configuring the Priority for Each Type of Packet

In the configuration mode, configure the priority value of each type of packet by performing the following steps:

Command	Function
DES-7210(config)# **cpu-protec type** {**arp | bpdu | dhcp | ipv6mc | igmp | rip | ospf | vrrp | pim | err-ttl | unknown-ipmc**} **pri** *pri_vaule*	Set the priority value for the packets, *pri_value* is an integer.
DES-7210# **end**	Return to the privileged mode.

This example shows the priority value configuration process:

```
DES-7210(config)# cpu-protect type bpdu pri 7
Set packet type bpdu priority 7.
```

50.3 Viewing CPU Protect information

On the switch, it is possible to view the following information about the CPU Protect:

- View the statistics of the packets received by the CPU of the supervisor engine
- View the statistics of the packets received by the CPU of the line card
- View the statistics of the packets received of a specific type

50.3.1 Showing the Statistics of the Packets Received by the CPU of the Management Board

In the privileged mode, show the CPP information of the supervisor engine by using the following commands:

Command	Function
DES-7210# **show cpu-protect mboard**	Show the statistics of the packets received by the CPU of the supervisor engine

The following example shows how to show the CPP information of the supervisor engine:

```
DES-7210#show cpu-protect mboard
 Type            Pps          Total        Drop
 ------------    ---------    ---------    ---------
 arp             500          19           0
 bpdu            200          24           0
 dhcp            0            0            0
 gvrp            0            0            0
 ipv6-mc         0            0            0
 igmp            0            0            0
 ospf            0            0            0
 pim             0            0            0
 rip             0            0            0
 vrrp            0            0            0
 unknow-ipmc     0            0            0
```

```
err-ttl          0            0            0
```

50.3.2 Showing the Statistics of the Packets Received by the CPU of the Line Card

In the privileged mode, show the statistics of the packets received by the CPU of a specific line card by using the following commands:

Command	Function
DES-7210# **show cpu-protect slot** *slot_id*	Show the packets received by the CPU of a specific line card. *slot_id*: slot ID

The following example shows the CPU protection information of the line card in slot 2.

```
DES-7210(config)# show cpu-protect slot 2
 Type            Pps         Total      Drop
 ------------    ---------   ---------  ---------
 arp             200         200        15
 bpdu            200         8          0
 dhcp            200         0          0
 gvrp            200         0          0
 ipv6-mc         200         0          0
igmp             200         0          0
 ospf            200         0          0
 pim             200         0          0
 rip             200         0          0
 vrrp            200         0          0
 unknow-ipmc     200         0          0
 err-ttl         20          3          0
```

50.3.3 Showing the Statistics of the Packets Received by a specific type

In the privileged mode, show the priority and bandwidth of each type of packet by using the following commands:

Command	Function
DES-7210# **show cpu-protect type arp | bpdu | dhcp | ipv6mc | igmp | rip | ospf | vrrp | pim | ttl1 | unknown-ipmc**	Show the statistics of the packets received by each type

The following example shows the statistics of the arp packets by using the **show cpu-protec type arp** command:

```
DES-7210(config)# show cpu-protect type arp
 Slot        Type          Pps       Total      Drop
 ---------   ------------  --------- ---------  ---------
 MainBoard   arp           200       15         0
 Slot-2      arp           200       15         0
```

Caution

1. Packet speed restriction is measured by the software, so a slight number deviation of packets is normal.
2. The actual information printed may be different from the example.

51 Anti-attack System Guard Configuration

51.1 Overview

It is known that many attacks of hackers and invasion of network virus start with scanning the hosts connecting to the network. The great amount of scanning packet consumes network bandwidth significantly and causes abnormal operation of the network communication.

For this reason, the layer 3 devices of DES-7210 Networks provide the anti-scanning function to prevent the hacker scanning and the Worm. Blaster-like attacks, and reduce the CPU load of the layer 3 devices.

At present, two types of scanning attacks are detected:

The scanning of the change for the destination IP address is referred to as the scan dest ip attack. This scanning is the most serious threaten to the network for it consumes the network bandwidth and adds the load of the switches, so it becomes the primary means of most hacker attacks.

The destination IP address doesn't exist, while a large number of packet is sent continuously, which is referred to as the same dest ip attack. This attack is mainly designed to reduce the CPU load for the devices. For the layer 3 switches, if the destination IP address exists, the packet will be forwarded directly by the switching chip and doesn't occupy the CPU resource for the switches. If the destination IP address doesn't exist, the CPU of the switches will attempt to connect periodically. Furthermore, if there are a large number of such attacks, they will consume the CPU resource. Of course, the hazard of this attack is much weaker than the first one.

For the above two kinds of attacks, it is possible to adjust the corresponding attack throttle, attack host interval of time and more parameters on the interfaces of DES-7210's device to relieve the burden of the network or devices. The administrator can tune the administration configuration of the device according to the network conditions. If the configuration of each interface is identical, administrators can set a batch of ports by the **interface range** function.

51.2 Anti-attack System Guard Configuration

The anti-attack system guard is completed in the global mode of the router. It is required to enter into the global configuration mode first to make anti-attack system guard configuration.

51.2.1 IP anti-scanning configuration task list

- Enable the anti-attack system guard function of the interface
- Set the isolation period for illegal attacking IP
- Set the threshold to judge illegal attacking IP

- Set the maximum monitored IPs
- Set exceptional IPs free from monitoring
- Clear the isolation status of isolated IPs
- View Related Information of System Guard

51.2.2 Enabling the Anti-attack System Guard on the Interface

You can enable the system guard in the interface mode. The system guard only supports physical ports.

Command	Meaning
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the configuration mode of this interface. Legal interfaces include physical interfaces.
system-guard enable	Enable the system guard function.
end	Return to the privileged mode.
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.

If you want to disable the system guard on this interface, use the **no system-guard** to set in the interface mode.

51.2.3 Setting the Isolation Period for Illegal IP Address

The isolated time of unauthorized attack IP is port-based. You may configure the isolated time of unauthorized attack user in the interface mode. This IP will restore the communication automatically after it is isolated for a period of time.

Command	Meaning
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the configuration mode of this interface. Legal interfaces include physical interfaces.
system-guard isolate-time *seconds*	Configure the Isolated Time of Unauthorized Users. Its value range is 30s – 3600s, 120s by default.
end	Return to the privileged mode.
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.

If you want to restore the default value of the isolated time, use the **no system-guard isolation-time** to set in the interface mode.

In addition, when the unauthorized user is isolated, we will send a LOG record to the log system for the query of administrators. Furthermore, it will send another LOG notification when the unauthorized isolation is released.

51.2.4 Setting the Threshold to Judge Illegal IP Address

There are two attack methods that may affect the device performance.

Scan a batch of IP network segment.

The attack to some IP that doesn't exist by sending the IP packet continuously.

Our switches carry out above limits. Among a batch of messages sent by the users, once any one of above limits exceeds the packet limit controlled by the administrator, this user will be considered to be an unauthorized attacker and be isolated. The judging threshold of illegal attacking IP is also port-based. You may configure it in the interface mode.

Command	Meaning
configure terminal	Enter the global configuration mode.
interface *interface-id*	Enter the configuration mode of this interface. Legal interfaces include physical interfaces.
system-guard same-dest-ip-attack-packets *number*	The maximum threshold of the attack that some IP which doesn't exist sends the IP packet continuously. The value range is 1 – 2000 packets per second, 20 by default. Setting to 0 indicates this attack is not monitored.
system-guard scan-dest-ip-attack-packets *number*	Configure the maximum threshold of the attack for scanning a batch of IP network segment. The value range is 1 – 1000 packets per second, 10 by default. Setting to 0 indicates this attack is not monitored.
end	Return to the privileged mode.
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.

Caution

The less the threshold is set, the poorer the accuracy of the judging for the attacked host is. It is easy to isolate the normal host online incorrectly. It is recommended that administrators to configure corresponding threshold according to the security degree of the actual network environment.

Since the hardware of the DES-7200 Series L3 switch can filter excrescent attack packet automatically, the switch can not check the second attack generally. However, Sys-Guard function still takes effect. In the extreme circumstance like full capacity hardware, when the switch can not filter the attack packets automatically, Sys-Guard function will breakthrough the second defense line of the switch, preventing switch CPU from attacking.

If you want to restore the default value of corresponding parameters, use the **no system-guard same-dest-ip-attack-packets** and **no system-guard scan-dest-ip-attack-packets** to set in the interface mode.

51.2.5 Setting the Maximum Monitored IPs

You can set the maximum quantity of the attacked hosts monitored by the devices. In general, this quantity should be maintained as the quantity of the actual operated hosts divided by 20. However, if you detect that the isolated hosts reach or approach to the maximum quantity of the monitored hosts, the quantity of the monitored hosts can be enlarged to meet the requirement for better system guard.

You can set the maximum quantity of the attacked host by the following steps:

Command	Meaning
configure terminal	Enter the global configuration mode.
system-guard detect-maxnum *number*	Set the maximum number of monitored hosts. This value is based on line card. Its value range is 1-500, 100 by default.
end	Return to the privileged mode.
show system-guard	Check the configuration entities.
copy running-config startup-config	Save the configuration.

Caution

If you change the quantity of the monitored hosts to be less than original quantity, it will clear the data of current monitored host. It may display the "chip resource full" in the isolate reason for the switch has isolated many users, which causes the hardware chip resource of the switch is full (This quantity is about 100-120 IP addresses is isolated for each port according to the actual switch operation and the ACL setting). However these users are not isolated actually, so it is necessary for administrators to take other measures to process these attackers.

If you want to restore the default value of the maximum quantity for the monitored hosts, use the "**no system-guard detect-maxnum"** in the global configuration mode.

51.2.6 Setting the Exceptional IP Addresses Free from Monitoring

You may set the exceptional IPs that is out of the monitoring. Packets that meet the exceptional IPs are allowed to be sent to the CPU.

Command	Meaning
configure terminal	Enter the global configuration mode.
system-guard exception-ip ip mask	Add the exceptional IP mask for anti-attack function. Up to 255 exceptional IP entries are supported.
end	Return to the privileged mode.
show system-guard exception-ip	Show all exceptional IP entries.
copy running-config startup-config	Save the configuration.

In the global configuration mode, the **no** option of this command deletes an exceptional IP entry. The **no** and **all-eip** options of this command will delete all exceptional IP entries.

For example, to delete all exceptional IPs:

```
DES-7210(config)# no system-guard exception-ip all-eip
```

Or to delete a single exceptional IP:

```
DES-7210(config)# no system-guard exception-ip 192.168.5.145  255.255.255.0/32
```

Caution

For the IP isolated, it will be isolated before they are aged even if it is configured as an exceptional IP. To allow the IP messages to be sent to the CPU, you may execute the **clear system-guard** command to cancel the isolation of the IP.

51.2.7 Clearing the Isolation Status of Isolated IP Addresses

The user isolated will automatically recover after a period of isolation. To clear the user manually, execute the following command in the privileged mode:

Command	Meaning
clear system-guard [interface *interface-id* **[ip-address** *ip-address***]]**	Clear Isolated Users. Where, "**clear system-guard**" indicates clearing all isolated users; "**clear system-guard interface** interface-id" indicates clearing all users under that port; "**clear system-guard interface** interface-id **ip-address** ip-address" indicates clearing the specified IP user under the interface.

51.2.8 View Related Information of System Guard

51.2.8.1 Viewing system guard information

Use **show system-guard** to view the configuration parameters of the system guard:

Command	Meaning
show system-guard [interface *interface-id***]**	View the configuration parameter of the system guard.

Let's consider an example:

```
DES-7210# show system-guard
detect-maxnum number   : 100  ------ The maximum quantity of the hosts monitored by the
device
isolated host number   : 11   ------------ The quantity of the hosts isolated by the device
interface  state   isolate time  same-attack-pkts   scan-attack-pkts
---------------------------- ----------------   ------------------
Fa 0/1    ENABLE    120            20                10
```

```
Fa 0/2    DISABLE   110            21                11
……

DES-7210# show system-guard interface Fa 0/1

detect-maxnum number   : 100  ------ The maximum quantity of the hosts monitored by the
device
isolated host number   : 11   ------------ The quantity of the hosts isolated by the device

intefacestate solate time ame-attack-pkts   scan-attack-pkts
---------------------------- ----------------
Fa 0/1     ENABLE     120         20                 10
```

51.2.8.2 Checking the information of isolated IPs for system guard

Command	Meaning
show system-guard isolate-ip [interface *interface-id***]**	Check the information of isolated IPs of the ports for anti-scanning system guard

```
DES-7210# show system-guard isolated-ip
interface ip-address    isolate reason   remain-time(second)
----------   ------------------  --------------------
Fa 0/1     192.168.5.119   scan ip attack     110
Fa 0/1     192.168.5.109   same ip attack     61
```

Above column indicates respectively the port on which the isolated IP address displays, the isolated IP address, the isolated reason and the remaining isolated time.

51.2.8.3 Viewing the IP address monitored

Command	Meaning
Show system-guard detect-ip [interface *interface-id***]**	View the IP address that is being monitored.

```
DES-7210# show system-guard detect-ip
interface ip-address ame ip attack packets  scan ip attack packets
-------------  -------------- ----------  --------  --------
Fa 0/1       192.168.5.118          0              8
Fa 0/1        192.168.5.108        12              2
```

51.2.8.4 Show exceptional IP addresses free from monitoring

To show the exceptional IPs that allow device access in the anti-attack function:

Command	Meaning
show system-guard exception-ip	Check all exceptional IPs.

```
DES-7210# show system-guard exception-ip
Exception IP Address    Exception Mask
```

```
 --------------------   ---------------
192.168.5.145            255.255.255.0
192.168.4.11             255.255.255.0
```

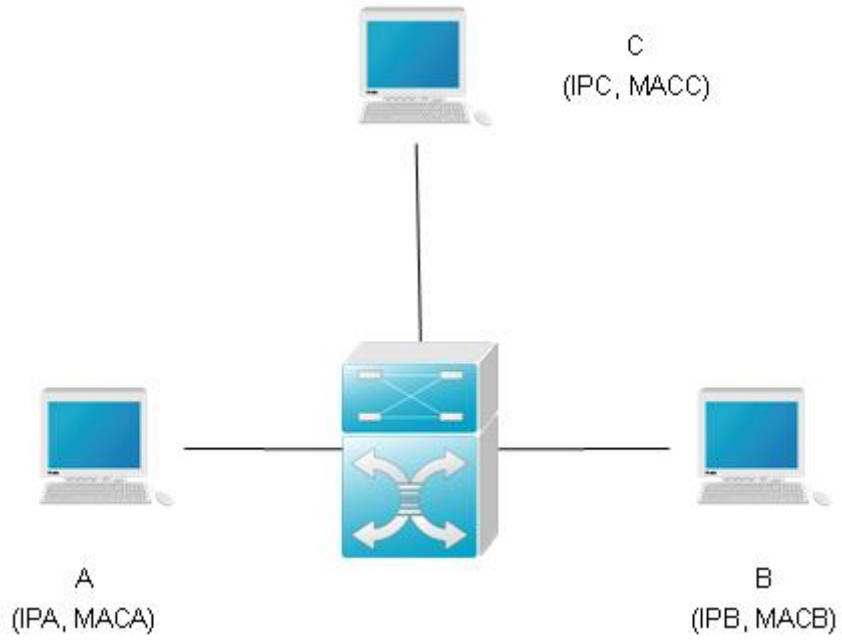
52 Dynamic ARP Inspection Configuration

52.1 Overview

DAI, an acronym of Dynamic ARP Inspection, refers to inspect the validity of received ARP packets. Illegal ARP packets will be discarded.

52.1.1 Understanding ARP Spoofing Attack

ARP itself does not check the validity of incoming ARP packets, a drawback of ARP. In this way, attackers can launch ARP spoofing attacks easily by exploiting the drawback of the protocol. The most typical one is the man in the middle attack, which is described as follows:



As shown in the diagram, devices A, B and C are connected to DES-7210 device and located in the same subnet. Their IP and MAC addresses are respectively represented by (IPA, MACA), (IPB, MACB) and (IPC, MACC). When device A needs to communicate with device B in the network layer, device A broadcasts an ARP request in the subnet to query the MAC value of device B. Upon receiving this ARP request packet, device B updates its ARP buffer using IPA and MACA, and sends an ARP response. Upon receiving this response, device A updates its ARP buffer using IPB and MACB.

With this model, device C will cause the corresponding relationship of ARP entries in device A and device B incorrect. The policy is to broadcast ARP response to the network

continuously. The IP address in this response is IPA/IPB, and the MAC address is MACC. Then, ARP entries (IPB and MACC) will exist in device A, and ARP entries (IPA and MACC) exist in device B. Communication between device A and device B is changed to communication with device C, which is unknown to devices A and B. Device C acts as an intermediary and it just modifies the received packets appropriately and forwards to another device. This is the well-known man in the middle attack.

52.1.2 Understanding DAI and ARP Spoofing Attacks

DAI ensures that only legal ARP packets are forwarded by the device. It mainly performs the following operations:

- Intercept all the ARP request and response packets at the untrusted port that corresponds to VLAN with the DAI inspection function enabled.
- Check the validity of the intercepted ARP packets according to the setting of DHCP database before further processing.
- Release the packets that do not pass the inspection.
- Appropriately process the packets that pass the inspection and send them to the destinations.

According to the DHCP snooping binding database, whether ARP packets is valid or not can be checked . For details, refer to *DHCP Snooping Configuration*.

52.1.3 Interface Trust Status and Network Security

ARP packets are checked according to the trust status of each port on the device. DAI check is ignored for the packets that are received through trust ports and are considered as legal ARP packets. DAI check will be performed strictly for the ARP packets that are received through untrusted ports.

In a typical network configuration, layer 2 port connected to the network device should be set as a trust port, and layer 2 port connected to the host device should be set as an untrusted port.

Note

Incorrectly configuring a layer 2 port as an untrusted port may affect normal communication of the network.

For specific configuration commands, refer to *ip arp inspection trust, show ip arp inspection interface.*

52.1.4 Limiting the Rate of ARP Packets

Checking DAI validity will consume a certain CPU resources. Limiting the rate of ARP packets, namely the number of ARP packets received per second, can efficiently prevent the DAI-specific DoS attack. By default, 15 ARP packets are received on an untrusted port per second. This limit does not apply to a trusted port. You can configure rate limit with the **ip arp inspection limit-rate** command on the Layer 2 interface configuration mode.

For details, refer to **ip arp inspection limit-rate** and **show ip arp inspection interface.**

52.2 Configuring DAI

DAI is an **ARP**-based security filtering technology. A series of filtering policies are configured, so that validity of ARP packets that pass the device is checked more effectively.

To use the functions of DAI, selectively perform the following tasks:

- Enabling DAI Packet Check Function for Specified VLAN (required)
- Set Trust Status of Port (optional)
- Set the Maximum Rate of Receiving ARP Packets on the Port(Optional)
- Related Configuration of DHCP Snooping Database (optional)

52.2.1 Enabling DAI Packet Check Function for Specified VLAN

By default, the DAI packet check function is disabled for all VLANs.

If no DAI packet check function has enabled VLAN vid, DAI-related security check will be skipped for the ARP packets with vlan-id = vid (ARP packet rate restriction is not skipped).

Use the **show ip arp inspection vlan** command to check whether the DAI packet check function has been enabled for all VLANs.

To configure the DAI packet check function for VLAN, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config)# **ip arp inspection vlan** *vlan-id*	Turn on the DAI packet check function switch for VLAN *vlan-id*
DES-7210(config)# **no ip arp Inspection vlan** [*vlan-id*]	Turn off the DAI packet check function switch for VLAN *vlan-id* Disable the DAI packet check function for all VLANs if *vlan-id* is ignored

52.2.2 Setting the Trust Status of Port

This command is used in the layer 2 interface configuration mode, and this layer 2 interface is a member port of SVI.

All the layer 2 ports are untrusted by default.

If the port is trusted, ARP packets will not be check further. Otherwise, the validity of the current ARP packet will be checked using information in the DHCP snooping database.

To set the trust status of a port, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip arp inspection trust**	Set the port as a trust port.
DES-7210(config-if)# **no ip arp inspection trust**	Set the port as an untrusted port.

52.2.3 Setting the Maximum Rate of Receiving the ARP Packets on the Port

This command is unavailable for the devices supporting NFPP for the NFPP implements this function automatically.

This command is used in the L2 interface configuration mode, and the L2 interface is a member port of the SVI.

By default, each untrusted switching port receives 15 ARP packets per second, and there is no limitation for the trusted switching port.

If the number of ARP packets received on the interface within 1 second exceeds the limit, the packets received consequently will be discarded.

Use the **show ip arp inspection interface** command to view the rate limit of each L2 interface.

To set the maximum rate of receiving the ARP packets on the port, execute the following commands in the interface configuration mode:

Command	Function
DES-7210(config-if)# **ip arp inspection limit-rate** { *<1-2048>* | **none**}	Set the maximum rate of receiving the ARP packets on the port, in pps. **none**: no limitation
DES-7210(config-if)# no ip arp inspection trust	Restore to the default value.

52.2.4 Related Configuration of DHCP Snooping Database

Refer to *DHCP Snooping Configuration*.

If DHCP Snooping database is not configured, all the ARP packets pass inspection.

52.3 Showing DAI Configuration

52.3.1 Showing Whether DAI Function Is Enabled for VLAN

To show the enabling status of VLAN, execute the following command in the global configuration mode:

Command	Function
DES-7210(config)# **show ip arp inspection vlan**	Show the enabling status of each VLAN

52.3.2 Showing DAI Configuration Status of Each Layer 2 Interface

To show the DAI configuration status of each layer 2 interface, execute the following command in the global configuration mode:

Command	Function

Command	Function
DES-7210(config)# **show ip arp inspection interface**	Show the DAI configuration of each layer 2 interface (including trust status and rate restriction)

For the products supporting NFPP, rate limit is done by NFPP, not DAI. Consequently, this command shows only the trust status of an interface.

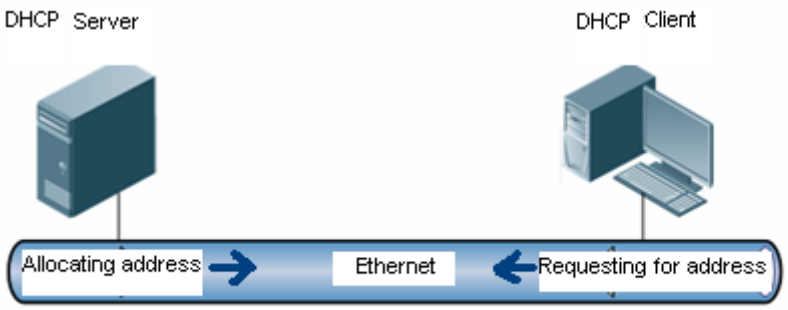
53 IP Source Guard Configuration

53.1 Brief Introduction of IP Source Guard

53.1.1 Understanding DHCP

In the typical DHCP-enabled network, the DHCP server is responsible for managing and allocating addresses for hosts. The hosts apply for legal network addresses from the DHCP server. DHCP is helpful for administrators to manage network addresses and avoid address conflict.

Figure 1 Normal DHCP Address Allocation



However, the server/client mode can not guarantee the efficiency and security of network address management. The traditional DHCP mode is required to have higher security characters because of the illegal packets or even attack packets from the clients (as shown in Figure 3) and various feigned servers (as shown in Figure 2)in the network.

DHCP Snooping solves the problem. The security problem of traditional DHCP mode can be solved by enabling DHCP Snooping on the device connecting the DHCP server with the DHCP clients. DHCP Snooping divides the network into two parts: untrusted network that shields all the DHCP Server response packets in the network and checks the security of the request from the client; trusted network that forwards the request received from legal client to the server in that trusted network which allocates and manages addresses.

Figure 2 Network with feigned DHCP server

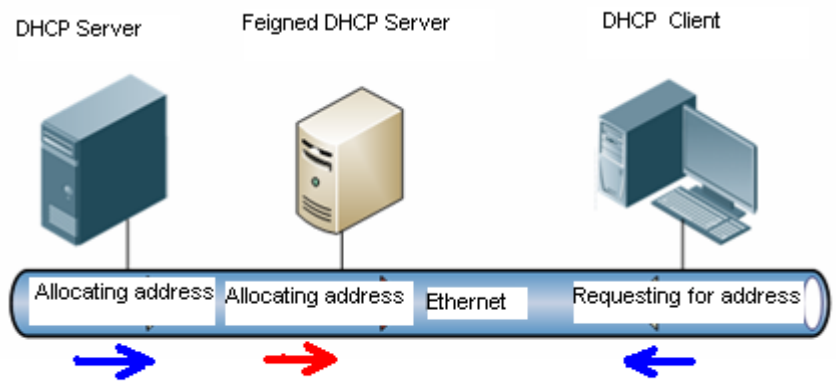


Figure 3 Network with feigned DHCP client attack

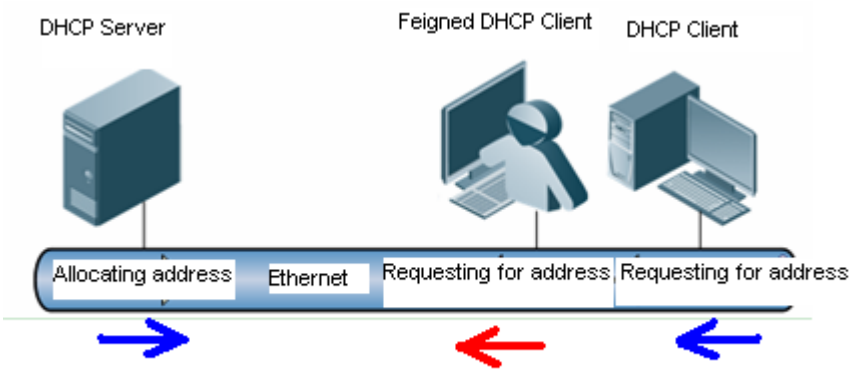
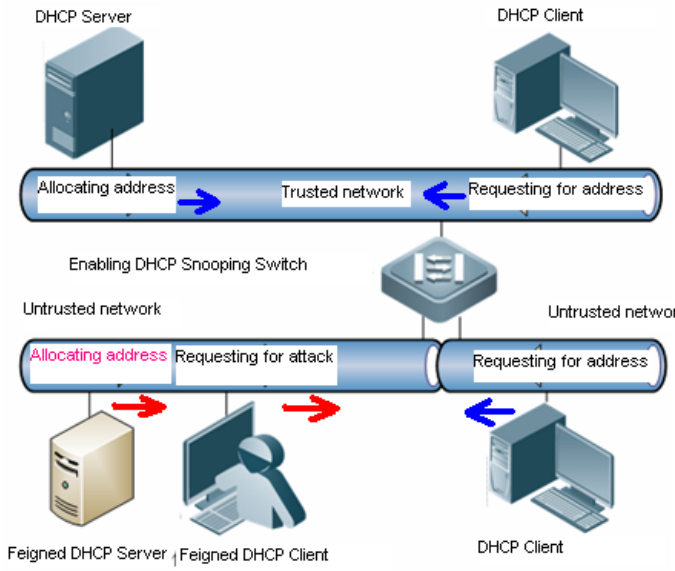


Figure 4 Network protected by DHCP Snooping



By filtering DHCP packets, DHCP Snooping shields feigned servers and block the attacks from the clients. However, it cannot control the users assign IP addresses privately. Those users easily lead to conflict of network addresses and be harm to the management of network addresses. To prevent the clients from assigning addresses privately in the DHCP network, enable IP Source Guard on the device connecting the DHCP server to the DHCP clients. DHCP Snooping-based IP Source Guard ensures that DHCP clients access network resources properly and block the users who assign addresses privately to access.

53.1.2 Understanding IP Source Guard

IP Source Guard maintains a hardware-based IP packet filtering database to filter packets, guaranteeing that only the users matching the database can access network resources.

The hardware-based IP packet filtering database is the key for IP Source Guard to enable efficient security control in DHCP applications. This database is on the basis of DHCP Snooping database. After IP Source Guard is enabled, the DHCP Snooping database is synchronized with the hardware-based IP packet filtering database. In this way, IP Source Guard can strictly filter IP packets from clients on the device with DHCP Snooping enabled.

By default, once IP Source Guard is enabled on a port, all the IP packets traveling through the port (except for DHCP packets) will be checked on the port. Only the users attaining IP addresses through DHCP and the configured static binding users can access the network.

IP Source Guard supports source MAC- and source IP-based filtering or source IP-based filtering. In the former case, IP Source Guard will check the source MAC and source IP addresses of all packets and only allow those packets matching the hardware-based IP packet filtering database to pass through. In the latter case, IP Source Guard checks the source IP addresses of IP packets.

53.1.3 Other Precautions of Configuring IP Source Guard

IP Source Guard is based on DHCP Snooping, namely port-based IP Source Guard takes effect only on the untrusted port under the control of DHCP Snooping, not on the trusted port or the interfaces in the VLAN not controlled by DHCP Snooping.

53.2 IP Source Guard Configuration

53.2.1 Configuring IP Source Guard on the Interface

By default, IP Source Guard is disabled on the interface and all the users connecting to the interface can use the network. After enabling IP Source Guard on the interface, it will filter the IP packets of the users connecting to the interface according to the hardware-based IP packet filtering database.

Command	Description
DES-7210(config)# **interface** ***interface-id***	Enter the interface configuration mode.
DES-7210(config)# [**no**] **ip verify source** [*port-security*]	Enable IP Source Guard on the interface. Use port-security to set MAC-based filtering.

The following example shows how to enable IP Source Guard on interface1:

```
DES-7210(config)# interface FastEthernet 0/1
DES-7210(config-if)# ip verify source
DES-7210(config-if)# end
```

Caution

The application of IP Source Guard is combined with DHCP Snooping. That is to say, port-based IP Source Guard only takes effect on untrusted port under the control of DHCP Snooping.

53.2.2 Configuring Static IP Source Address Binding User

By default, static binding user is not existent. In some application environment, you may need to use static IP address to access networks, which can be implemented by configuring static binding users.

Command	Description
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# [**no**] **ip source binding** *mac-addrees* **vlan** *vlan_id ip-address* **interface** *interface-id*	Configure static binding user.

The following example shows how to add a static binding user:

```
DES-7210# configure terminal
DES-7210(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface
FastEthernet 0/9

DES-7210(config)# end
```

53.3 Showing IP Source Guard Configuration

53.3.1 Showing IP Source Guard Filtering Entry

Use this command to show IP Source Guard filtering entry.

Command	escription
DES-7210# **show ip verify source** [**interface** *interface*]	Show IP Source Guard filtering entry.

For example:

```
DES-7210 # show ip verify source
Interface  Filter-type Filter-mode Ip-address  Mac-address    VLAN
-------------------- ----------- ----------- --------------- -------------- --------
FastEthernet    0/1    ip    active     192.168.4.243    00d0.f801.0101 1
```

53.3.2 Showing Hardware-based IP Packet Filtering Database

Use this command to show the related information of hardware-based IP packet filtering database.

Command	Description

DES-7210# **show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]	Show the hardware-based IP packet filtering database.

For example:

```
DES-7210# show ip source binding
MacAddress    IpAddress   Lease(sec)   Type   VLAN
Interface
------------------ --------------- ------------ ------------- ----- --------------------
00d0.f801.0101  192.168.4.243  infinite   static   1
FastEthernet  0/1
Total number of bindings: 1
```

53.3.3 IP Source Guard Debugging

Use this command to turn on the IP Source Guard debugging switch.

Command	Description
DES-7210# **debug ip source binding**	Turn on the IP Source Guard debugging switch.

For example:

```
DES-7210# debug ip source binding
```

54 NFPP Configuration

54.1 NFPP Overview

NFPP is the abbreviation of Network Foundation Protection Policy.

In the network, some malicious attacks put too much burden on the switch. When the packet traffic bandwidth or the packet percent exceeds the limit, it leads to the CPU over-utilization and abnormal operation of the switch.

DES-7210 products protect the switch and improve the switch anti-attack capacity by means of dividing the packets into three types: manage, route and protocol.

For NFPP, the detailed practices of the ARP protocol is ARP-guard, which deals with ARP DoS attack, rate-limit of the ARP packet and attack source isolation.

Caution

Network Foundation Protection Policy, abbreviated as NFPP, is a way of enhancing the switch security, protecting the switch processor and channel bandwidth resources, and ensures the normal forwarding of the packet and normal operation of the protocol.

In order to make full use of the NFPP function, you can modify the rate-limit value of each packet in CPU Protect Policy according to specified network environment, you can also use the recommended value displayed after executing the **show cpu-protect summary** command.

The packets sent to the CPU are classified into three types(manage, route and protocol) according to the application platform of each packet.

1. By configuring the packet traffic bandwidth limit, you can control the packet traffic bandwidth value and discard the packets which exceed the limit.

2. By configuring the packet percent, you can limit the packet count and discard the packets which exceed the packet percent.

54.2 Configuring NFPP

This section describes how to configure the CPU Protect.

- Default NFPP configuration.
- Configuring the packet traffic bandwidth.
- Configuring the packet percent.

54.2.1 Default NFPP Configuration

The default configurations of NFPP are as follows:

Packet type	Default traffic bandwidth	Default packet percent
Manage	3000	30

Packet type	Default traffic bandwidth	Default packet percent
Route	3000	25
Protocol	3000	45

54.2.2 Configuring the packet traffic bandwidth

This section describes how to configure the packet traffic bandwidth:

Command	Function
DES-7210(config)# **cpu-protect sub-interface** {**manage|protocol|route**} **pps** *pps_vaule*	Configure the traffic bandwidth threshold of the corresponding packet, in pps, ranging from 1 to 8192, in integer.

For example:

```
DES-7210(config)# cpu-protect sub-interface manage pps 200
DES-7210(config)# end
```

54.2.3 Configuring the packet percent

This section describes how to configure the packet percent:

Command	Function
DES-7210(config)# **cpu-protect sub-interface** {**manage|protocol|route**} **percent** *percent_vaule*	Configure the packet percent. *percent_value*: ranging from 1 to 100, in integer.

For example:

```
DES-7210(config)# cpu-protect sub-interface manage percent 60
DES-7210(config)# end
```

Caution

The valid percent value of one packet must be less than 100% minus the percent value of other two types of packets

54.3 ARP-guard

54.3.1 Overview

The IP address is translated into the MAC address by ARP protocol in the local area network(LAN). ARP protocol plays an important role in the network security. ARP DoS attack sends a large amount of illegal ARP packets to the gateway, preventing the gateway from providing the services. To deal with this attack, on one hand, you can configure the rate-limit of the ARP packet, on the other hand, you can detect and isolate the attack source.

The ARP attack detection could be user-based or port-based. User-based ARP attack detection could be classified into the following two types again: source IP address/VID/port-based and source MAC address/VID/port-based. For each attack

detection, you can configure the rate-limit threshold and warning threshold. The ARP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ARP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The user-based attack detection can isolate the attack source.

Besides, ARP-guard is able to detect the ARP scan. ARP scan is that the source MAC address on link layer is fixed while the source IP address is changing, or the source MAC address and source IP address are fixed while the destination IP address is changing. DES-7210 products only support to detect the first ARP scan(the source MAC address on link layer is fixed while the source IP address is changing).

It is worth mentioning that ARP-guard is only for the ARP DoS attack, rather than ARP fraud.

ARP-guard configuration commands include:

- Configuring the isolated time
- User-based rate-limit and attack detection
- Port-based rate-limit and attack detection
- Clearing the isolated users
- Showing arp-guard

54.3.2 Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration mode. By default, the isolated time is configured in the global configuration mode.

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **arp-guard isolate timeout** [*seconds* | *permanent*]	Configure the global isolated time, ranging 0s, 180-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.
DES-7210(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7210(config-if)# **arp-guard isolate timeout** [*seconds* | *permanent*]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
DES-7210(config-if)# **show arp-guard configuration**	Show the arp-guard parameter settings.

To restore the global isolated time to the default value, use the **no arp-guard isolation-time** command in the global configuration mode. If the isolated time has been configured on a port, you can use the **no arp-guard isolation-time** command to remove the port-based isolated time configuration in the interface configuration mode.

54.3.3 User-based rate-limit and attack detection

For the user-based attack detection, it can be classified into the following two types: source IP address/VID/port-based and source MAC address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called

warning threshold). The ARP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ARP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message.

ARP-guard supports to detect the ARP scan, which is in 10s, 15s by default. If 15 or more than 15 ARP packets have been received within 10s, and the source MAC address on link layer is fixed while the source IP address is changing, or the source MAC address and source IP address are fixed while the destination IP address is changing, ARP scan is detected and recorded in the syslog and the TRAP messages are sent.

It prompts the following message if the ARP DoS attack was detected:

```
*Dec 27 15:34:16: %ARPGUARD-4-DOS_DETECTED: ARP DoS attack was detected.
```

This message only inform the administrator of the ARP DoS attack detection without the information of user attributes. For the detailed information about the attack, the administrator can use the **show arp-guard users** command. Note that it is not recommended to set the isolated time to 0s, for the reason that “no isolation can not write the attacker attributes to the isolated user table”.

The following example shows the TRAP packet information when the isolated time has been configured to 0s and the attack action has been detected (if VLAN=0, it is a route port):

```
ARP DoS attack from user<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> detected.
```

The following message shows the TRAP packet information when the isolated time has been configured to the value except for 0 and the hardware isolation has been succeeded:

```
User<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> is isolated.
```

The following message shows the TRAP packet information when the hardware isolation failed due to shortage of memory or hardware resources:

```
Failed to isolate user<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>.
```

It prompts the following message when the ARP scan was detected:

```
*Dec 27 15:34:16: %ARPGUARD-4-SCAN: ARP scan was detected.
```

It prompts the following message when the ARP scan was detected:

For the detailed information, the administrator can use the **show arp-guard scan** command. It saves the latest 256 pieces of records in the ARP scan table. When the ARP scan table is full, it prompts:

```
*Dec 27 15:34:16: %ARPGUARD-4-SCAN_TABLE_FULL: ARP scan table is full.
```

The following is additional information of the sent TRAP packet :

```
ARP scan from user< MAC=0000.0000.0004,port=Gi4/1,VLAN=1> detected.
```

Caution

- When the hardware isolated user number exceeds 127, it slows down to learn the legal ARP packet if there are a lot of attack packets in the network.
- The upper limit of the user list memory is 1MB. When the limit has been exceeded, it prompts the message like "%ARPGUARD-4-MEM_LIMIT:user table's size reached limit 1MB." to inform the administrator.
- It sets a policy to the hardware when isolating the attackers. When the hardware resources have been exhausted, it prompts the message like " %ARPGUARD-4-ISOLATE_FAILED: failed to isolate ARP DoS attacker." to inform the administrator.
- When it fails to allocate the memory to the detected attackers, it prompts the message like " %ARPGUARD-4-NO_MEMORY: failed to alloc memory." to inform the administrator.
- It contains only the latest 256 pieces of the records in the ARP scan table. When the ARP scan table is full, the newest record will overwrite the oldest one.
- To prevent the CPU resource exhaustion due to frequent message print, you can limit the message print rate at the interval of 30s. No print rate limit for the TRAP packet message.

This section shows how to configure the user-based rate-limit and attack detection:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **arp-guard rate-limit** *pps* {**per-src-ip | per-src-mac**}	Configure the arp-guard rate-limit, ranging from 1 to 0xFFFFFFFF, 4 by default. **per-src-ip**: detect the users based on the source IP address/VID/port; **per-src-mac**: detect the users based on the source MAC address/VID/port.
DES-7210(config)# **arp-guard attack-threshold** *pps* {**per-src-ip | per-src-mac**}	Configure the arp-guard attack threshold, ranging from 1 to 0xFFFFFFFF, 8 by default. When the ARP packet number sent from a user exceeds the attack threshold, the attack is detected and ARP-guard isolates the user, records the message and sends the TRAP packet. **per-src-ip**: detect the users based on the source IP address/VID/port; **per-src-mac**: detect the users based on the source MAC address/VID/port.
DES-7210(config)# **arp-guard scan-threshold** *pkt-cnt*	Configure the arp-guard scan threshold, in 10s, ranging from 1 to 0xFFFFFFFF, 15 by default. If 15 or more than 15 ARP packets have been received within 10s, and the source MAC address on link layer is fixed while the source IP address is changing, or the source MAC address and source IP address are fixed while the destination IP address is changing, ARP scan is detected and recorded in the syslog and the TRAP messages are sent.
DES-7210(config-if)# **show arp-guard configuration**	Show the arp-guard parameter settings.

54.3.4 Port-based rate-limit and attack detection

You can configure the arp-guard rate limt and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the ARP packet rate on a port exceeds the limit, the ARP packets are dropped. When the ARP packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the ARP DoS attack was detected on a port:

```
*Dec 27 15:34:16: %ARPGUARD-4-PORT_ATTACKED: ARP DoS attack was detected on port Gi4/1.
```

The following is additional information of the sent TRAP packet :

```
ARP DoS attack was detected on port Gi4/1.
```

This section shows how to configure the port-based rate-limit and attack detection:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **arp-guard rate-limit** *pps* **per-port**	Configure the arp-guard rate-limit of the ARP packet on the port, ranging from 1 to 0xFFFFFFFF, 100 by default.
DES-7210(config)# **arp-guard attack-threshold** *pps* **per-port**	Configure the arp-guard attack threshold, ranging from 1 to 0xFFFFFFFF, 200 by default. When the ARP packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
DES-7210(config-if)# **show arp-guard configuration**	Show the arp-guard parameter settings.

Caution

MAC address-based rate limit takes precedence over IP address-based rate limit. IP address-based rate limit takes precedence over port-based rate limit.

The following steps explains how arp-guard function processes when the ARP packets are received:

1. Add 1 to the source MAC address statistics. The ARP packets are dropped if the rate limit has been exceeded. It prompts the attack warning message if the attack threshold has been exceeded. Execute step 2 if the rate limit has not been exceeded.
2. Add 1 to the source IP address statistics. The ARP packets are dropped if the rate limit has been exceeded. It prompts the attack warning message if the attack threshold has been exceeded. Execute step 3 if the rate limit has not been exceeded.
3. Add 1 to the port statistics. The ARP packets are dropped if the rate limit has been exceeded. It prompts the attack warning message if the attack threshold has been exceeded.

From the above description, it concludes that the rate limit can not be more than the scan threshold. Port configuration actually limit the user count.

When configuring the rate limit on the port, you can refer to the user count on this port. For example, if 500 users exist on a port, you can set the rate limit on this port to 500.

54.3.5 Clearing the isolated users

The isolated users can be recovered automatically after a period of the time. You can use the following command to clear the isolated users manually.

Command	Function
DES-7210# **clear arp-guard users** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]	**clear arp-guard users:** Clear all isolated users. **clear arp-guard users vlan** *vid*: Clear all isolated users in a VLAN. **clear arp-guard users** [**vlan** *vid*] [**interface** *interface-id*]: Clear all isolated users on a interface in a VLAN. **clear arp-guard users** [**vlan** *vid*] [**interface** *interface-id*] [**ip-address** | **mac-address**]: An isolated users has been cleared.Use the IP address of the MAC address to identify the users.

54.3.6 Clearing the ARP san table

You can use the following command to clear the ARP scan table manually.

Command	Function
DES-7210# **clear arp-guard scan**	Clear the ARP scan table.

54.3.7 Showing arp-guard

54.3.7.1 show arp-guard configuration

Use this command to show the arp-guard configurations.

Command	Function
DES-7210# **show arp-guard configuration**	Show the arp-guard configurations.

For example,

```
DES-7210#show arp-guard configuration

Rate limit: 1 pps per-src-ip, 1 pps per-src-mac, 100 pps per-port

Attack threshold:8 pps per-src-ip, 8 pps per-src-mac, 200 pps per-port

Scan threshold:15 packets per 10 seconds

Global isolate timeout:0 second (0 means auto recovery is disabled)
Local isolate timeout(second):

Gi0/1          300

Gi0/2          400
```

54.3.7.2 show the isolated users

Command	Function
DES-7210# **show arp-guard users statistics**	Show the arp-guard users statistics, including total user amount, isolated user amount and non-isolated user amount.
DES-7210#**show arp-guard users** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]	Show the isolated users information. **show arp-guard users vlan** *vid*: Show the isolated users in a VLAN. **show arp-guard users** [**vlan** *vid*] [**interface** *interface-id*]: Show the isolated users on a interface in a VLAN. **show arp-guard users** [**vlan** *vid*] [**interface** *interface-id*] [**ip-address** | **mac-address**]: Show the isolated users. Use the IP address or the MAC address to identify the users.

For example,

```
DES-7210#show arp-guard users statistics
Success:  100
Fail:    1
----------------
Total:   101

DES-7210#show arp-guard users
If column 1 shows '*', it means "hardware failed to isolate user".
VLAN   interface      IP address   MAC address   remain-time(seconds)
1           Gi0/1              1.1.1.1            -
110
2           Gi0/1               1.1.2.1          -
61
*3         Gi0/1                -          0000.0000.1111
110
4           Gi0/1                -         0000.0000.2222  61
Total  4 users

DES-7210#show arp-guard users vlan 1 interface g 0/1 1.1.1.1
If column 1 shows '*', it means "hardware failed to isolate user".
VLAN   interface      IP address   MAC address remain-time(seconds)
1          Gi0/1         1.1.1.1        -    110
Total  1 user
```

If the IP address columm shows “-”, it means “the user is identified by the IP address”;

If the MAC address columm shows “-”, it means “the user is identified by the MAC address”.

54.3.7.3 show the ARP scan table

Command	Function
DES-7210# **show arp-guard scan statistics**	Show the arp-guard scan statistics.
DES-7210#**show arp-guard scan** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]	Show the arp-guard scan information. **show arp-guard scan vlan** *vid*: Show the arp-guard scan information in a VLAN. **show arp-guard users** [**vlan** *vid*] [**interface** *interface-id*]: Show the arp-guard scan information on a interface in a VLAN. **show arp-guard users** [**vlan** *vid*] [**interface** *interface-id*] [**mac-address**]: Show the arp-guard scan information for a MAC address on a interface in a VLAN.

For example,

```
DES-7210#show arp-guard scan statistics
ARP scan table has 4 record(s).

DES-7210#show arp-guard scan
VLAN    interface      MAC address    timestamp
1         Gi0/1      0000.0000.0001  2008-01-23 16:23:10
2         Gi0/2      0000.0000.0002  2008-01-23 16:24:10
3         Gi0/3      0000.0000.0003  2008-01-23 16:25:10
4         Gi0/4      0000.0000.0004  2008-01-23 16:26:10
Total  4 record(s)
```

"timestamp" represents the time when the ARP scan was detected. For example, "2008-01-23 16:23:10" represents that the ARP scan was detected at 16:23:10, Jan 23, 2008.

```
DES-7210#show arp-guard users vlan 1 interface g 0/1 0000.0000.0001
VLAN    interface      MAC address    timestamp
1         Gi0/1      0000.0000.0001  2008-01-23 16:23:10
Total  1 record(s)
```

54.4 Configuration Examples

54.4.1 ARP-guard configuration example

1. When the ARP attacks occur in the network frequently, you can detect those attacks by configuring user-based source MAC address/VID/port, user-based source IP address/VID/port and port-based rate-limit and attack detection.

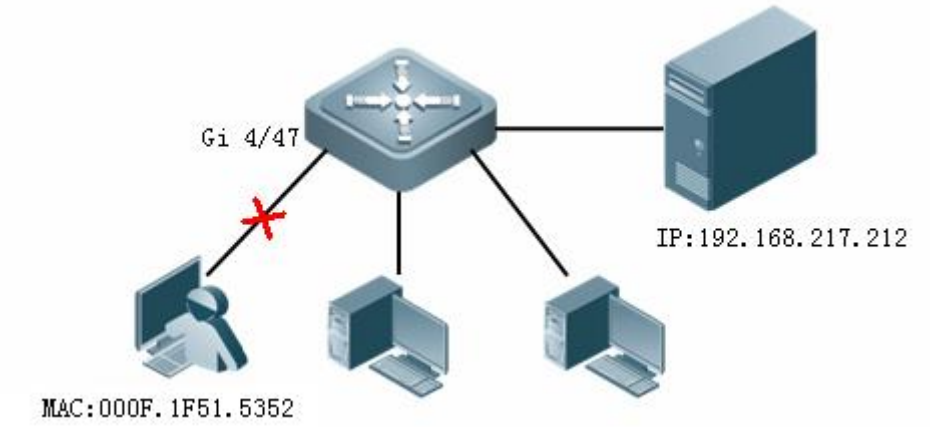
2. You can configure the rate limit and attack threshold manually.

3. The detected attackers can be isolated by configuring the isolation time.

4. If the ARP packet rate exceeds the attack threshold, arp-guard will isolate the attack, the CLI prompts and TRAP messages are sent. The SNMP server configuration, which is used to receive and resolve the SNMP TRAP packets when attacks occur, and SYSLOG MONITOR tool enables the administrator to receive the syslogs at any time.

5. The administrator can clear the isolation configuration manually.

54.4.1.1 Network Topology



54.4.1.2 Configuration Steps

By default, arp-guard function is enabled. The following lists the default configuations:

```
DES-7210# show arp-guard configuration
Rate limit: 1 pps per-src-ip, 1 pps per-src-mac, 100 pps per-port
Attack threshold:8 pps per-src-ip, 8 pps per-src-mac, 200 pps per-port
Scan threshold:15 packets per 10 seconds
Global isolate timeout:0 second(0 means don't isolate)
Local isolate timeout(second):
```

Enter the global configuration mode. Configure the source MAC address/VID/port-based attack detection, rate limit 4 pps, attack threshold 10pps:

```
DES-7210# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# arp-guard rate-limit 2 per-src-mac
DES-7210(config)# arp-guard attack-threshold 10 per-src-mac
```

Configure the source IP address/VID/port-based attack detection, rate limit 4 pps, attack threshold 10pps:

```
DES-7210(config)# arp-guard rate-limit 4 per-src-ip
DES-7210(config)# arp-guard attack-threshold 10 per-src-ip
```

Configure the port-based attack detection, rate limit 150 pps, attack threshold 300pps:

```
DES-7210(config)# arp-guard rate-limit 150 per-port
```

```
DES-7210(config)# arp-guard attack-threshold 300 per-port
```

Configure the permanent isolation in the global configuration mode:

```
DES-7210(config)# arp-guard isolate timeout permanent
```

Show the arp-guard configuration:

```
DES-7210(config)# show arp-guard configuration
Rate limit: 4 pps per-src-ip, 4 pps per-src-mac, 150 pps per-port
Attack threshold:10 pps per-src-ip, 10 pps per-src-mac, 300 pps per-port
Scan threshold:15 packets per 10 seconds
Global isolate timeout:permanent
Local isolate timeout(second):
```

Configure the SNMP server IP address 192.168.217.212. When the switch detects the attack, TRAP packets are sent to the SNMP server.

```
DES-7210(config)# snmp-server host 192.168.217.212 traps DES-7210
```

Enable the SNMP server to send the TRAP packets:

```
DES-7210(config)# snmp-server enable traps nfpp
```

Enable the syslog function, sending the syslog to the server:

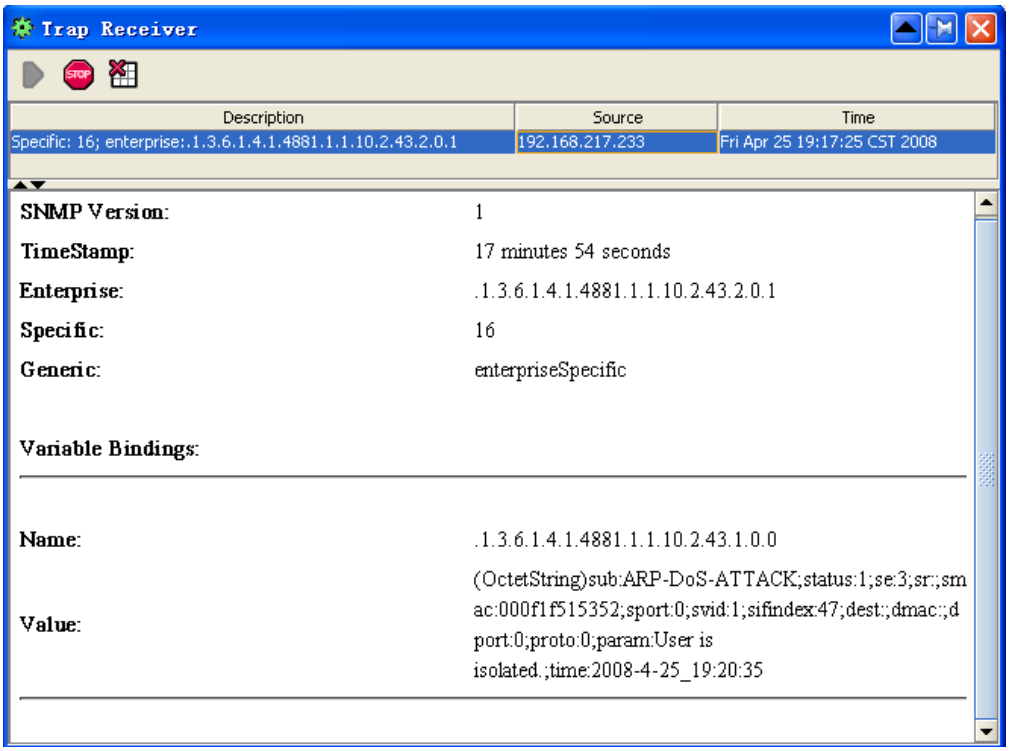
```
DES-7210(config)# logging on
DES-7210(config)# logging server 192.168.217.212
```

It prompts the following syslog when the switch receives the ARP DoS attack:

```
*Apr 25 19:20:35: %ARPGUARD-4-DOS_DETECTED: ARP DoS attack was detected.
```

You can also use theSYSLOG MONITRO tool to view the detailed syslog:

The following are the TRAP messages received from the software MIB-BROWSER:



Show the arp-guard users information:

```
DES-7210(config)# show arp-guard users
If column 1 shows '*', it means "hardware failed to isolate user".
 VLAN    interface      IP address     MAC address    remain-time(seconds)
 1       Gi4/47         -              000f.1f51.5352  -
Total: 1 user
```

Clear the arp-guard users manually :

```
DES-7210# clear arp-guard users 000f.1f51.5352
ARPGUARD:1 user is cleared.
DES-7210# show arp-guard users
If column 1 shows '*', it means "hardware failed to isolate user".
 VLAN    interface      IP address     MAC address    remain-time(seconds)
Total: 0 user
```

55 Access Control List Configuration

55.1 Overview

As part of our security solution, ACL is used to provide a powerful data flow filtering function. At present, our product supports the following access lists:

- Standard IP access control list
- Extended IP access control list
- MAC access control list
- MAC extended access control list
- Expert extended access control list
- IPV6 extended access control list

Depending on the conditions of networks, you can choose different access control lists to control data flows.

55.1.1 Access Control List Introduction

ACLs is the shortened form of Access Control Lists, or Access Lists. It is also popularly called firewall, or packet filtering in some documentation. ACL controls the messages on the device interface by defining some rules: Permit or Deny. According to usage ranges, they can be divided into ACLs and QoS ACLs.

By filtering the data streams, you can restrict the communication data types in the network and restrict the users of the network and the device they can use. When data streams pass the switch, ACLs classify and filter them, that is, check the data streams input from the specified interface and determine whether to permit or deny them according to the matching conditions.

To sum up, the security ACL is used to control which dataflow is allowed to pass through the network device. The QoS policy performs priority classification and processing for the dataflow.

ACLs consist of a series of entries, known as Access Control Entry (ACE). Each entry specifies its matching condition and behavior.

Access list rules can be about the source addresses, destination addresses, upper layer protocols, time-ranges or other information of data flows.

55.1.2 Why to Configure Access Lists

There are many reasons why we need configure access lists. Some of them are as follows:

- Restrict route updating: Control where to send and receive the route updating information.

- Restrict network access: To ensure network security, by defining rules, make users unable to access some services. (When a user only need access the WWW and E-mail services, then other services like TELNET are disabled). Or, allow users to access services only during a given period or only allow some hosts to access networks.

Figure 1 is a case. In the case, only host A is allowed to access Finance Network, while Host B is disallowed to do so. See Figure 1.

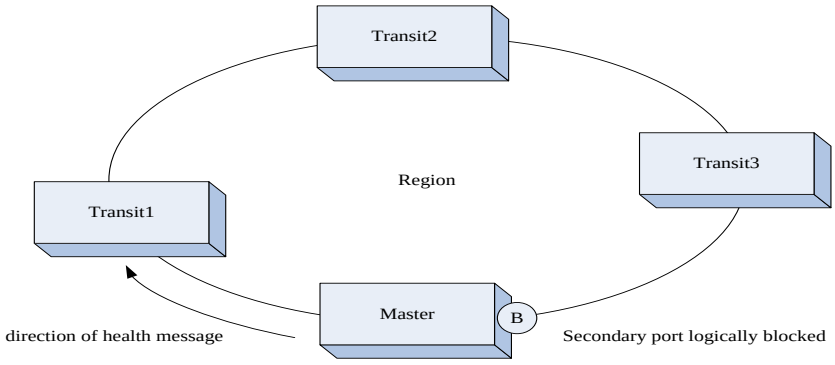


Figure 1 Using Access List to Control Network Access

55.1.3 When to Configure Access Lists

Depending on your requirements, you can select the basic access list or dynamic access list. In general, the basic access list can meet the security requirement.However, experienced hackers may use some software spoof source address and cheat the devices so as to gain accesses. Before the user can access the network, the dynamic access list requires the pass of authentication so that the hackers are difficult to invade the network. So, in some sensitive areas the dynamic access list can be used to ensure the network security.

Note

A inherent problem of all access lists is electric spoofing, the behavior of providing spoof source addresses to deceive switches Even you use the dynamic list, a spoofing problem occurs. During the valid access period of an authenticated user, a hacker may use a counterfeit user address and accesses the network. There are two methods to resolve the problem. One method is to set free time for a user to access the network as little as possible, making it hard for a hacker to attack the network. Another method is to use the IPSEC encryption protocol to encrypt network data, ensuring that all the data entering switches are encrypted.

Access lists are usually configured in the following locations of network devices:

- Devices between the inside network and outside network (such as the Internet)
- Devices at the borders of two parts in a network
- Devices on the access control port

The execution of the ACL statements must follow the order in the table strictly. Starting from the first statement, once the header of a packet matches a conditional judge statement in the table, the sequential statements are ignored.

55.1.4 Input/Output ACL, Filtering Domain Template and Rule

When a device interface receives a message, the input ACL checks whether the message matches an ACE of the ACL input on the interface. When a device interface is ready to output a message, the output ACL checks whether the message matches an ACE of the ACL output on the interface.

When detailed filtering rules are formulated, all or some of the above eight items may be used. As long as the message matches one ACE, the ACL processes the message as the ACE defined (permit or deny). The ACE of an ACL identifies Ethernet messages according to some fields of Ethernet messages. The fields include the following:

Layer-2 fields:

- 48-bit source MAC address (all the 48 bits must be declared)
- 48-bit destination MAC address (all the 48 bits must be declared)
- 16-bit layer-2 type field

Layer 3 fields:

- Source IP address field (you can specify all the 32 bits of the IP address, or specify a type of streams of the defined subnet)
- Destination IP address field (you can specify all the 32 bits of the IP address, or specify a type of streams of the defined subnet)
- Protocol type fields

Layer-4 fields:

- You can specify one UDP source port, destination port, or both
- You can specify one UDP source port, destination port, or both

The filtering domain consists of the fields in the packets based on which the packets are identified and classified when you create an ACE. A filtering domain template is the definition formed by these fields. For example, when one ACE is generated, you want to identify and classify messages according to the destination IP field of a message. When another ACE is generated, you want to identify and classify messages according to the source IP address field of a message and the source port field of UDP. In this way, these two ACEs use different filtering domain templates.

Rules refer to the values of the ACE mask. For example, one ACE is:

permit tcp host *192.168.12.2* **any eq telnet**

In this ACE, the filtering domain template is a collection of the following fields: Source IP Address Fields, IP Protocol Fields and Destination TCP Port Fields. Corresponding values (rules) are respectively as follows: Source IP Address=host 192.168.12.2; IP Protocol=tcp; TCP Destination Port=telnet.

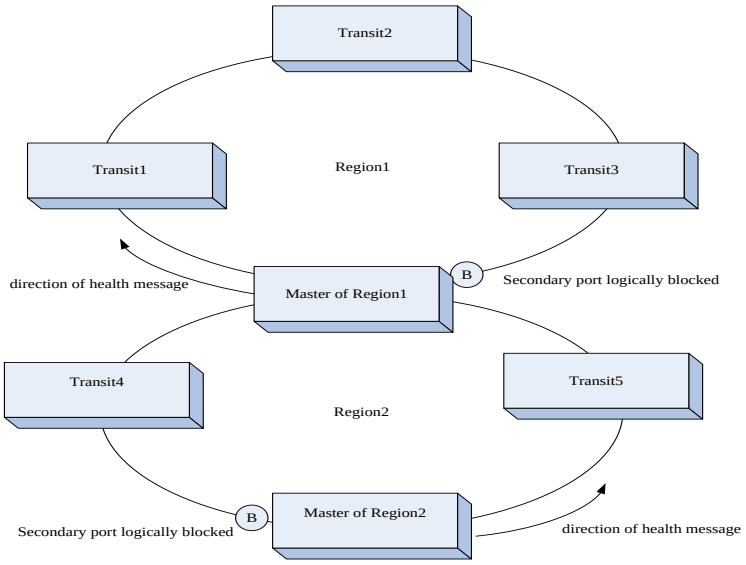


Figure 2 Analysis of the ACE permit tcp host 192.168.12.2 any eq telnet

Note

A filtering domain template can be the collection of L3 fields (Layer 3 Field) and L4 fields (Layer 4 Field) or the collection of multiple L2 fields (Layer 2 Field). However, the filtering domain templates of a standard and extended ACL cannot be the collection of L2 and L3, L2 and 4, L2 and L3, or L4 fields. To user the combination of L2, L3 and L4 fields, it is possible to apply the Expert ACLs.

55.2 Configuring IP Access List

To configure access lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol. The following table lists the protocols that can use numbers to specify access lists and the number ranges of access lists that can be used by each protocol.

Protocol	Number Range
Standard IP	1-99, 1300 - 1999
Extended IP	100-199, 2000 - 2699

55.2.1 Guide to configure IP Access List

When you create an access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

Basic Access Lists include standard access lists and extended access lists. The typical rules defined in access lists are the following:

- Source address
- Destination address
- Upper layer protocol
- Time range

Standard IP access lists (1 – 99, 1300 – 1999) forward or block packets according to source addresses. Extended IP access lists (100 – 199, 2000 – 2699) use the above four combinations to

forward or block packets. Other types of access lists forward or block packets according to related codes.

A single access list can use multiple separate access list sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list. However, the more the used sentences are, the more difficult to read and understand an access list.

55.2.1.1 Implicating "Deny Any Data Flow" Rule Sentence

The ending part of each access list implicates a "Deny any data flow" rule sentence. Therefore, if a packet matches no rule, then it is denied, as shown in the following example:

```
access-list 1 permit host 192.168.4.12
```

This list allows only the message of host 192.168.4.12 and denies any other host. This is because the list contains the following rule statement at the end: **access-list 1 deny any**

Here is another example:

```
access-list 1 deny host 192.168.4.12
```

If the list contains the only statement above, the messages from any host will be denied on the port.

Caution

It is required to consider the routing update message when defining the access list. Since the end of the access list "denies all dataflow", this may cause all routing update messages blocked.

55.2.1.2 Order to Input Rule Sentences

Each added rule is appended to the access list. If a sentence is created, then you cannot delete it separately and can only delete the whole access list. Therefore, the order of access list sentences is very important. When deciding whether to forward or block packets, a switch compares packets and sentences in the order of sentence creation. After finding a matching sentence, it will not check other rule sentences.

If you have created a sentence and it allows all data flows to pass, then the following sentences will not be checked, as shown in the following example:

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

Because the first rule sentence denies all IP messages, the host telnet message of the 192.168.12.0/24 network will be denied. Because the switch discover that the messages match the first rule sentence, it will not check other rule sentences.

55.2.2 Configuring IP Access List

The configuration of the basic access list includes the following steps:

1. Define a basic access list

2. Apply the access list to a specific interface.

There are two methods to configure a basic access list.

Method 1: Run the following command in the global configuration mode:

Command	Function

Command	Function
DES-7210(config)# **access-list id** {**deny** | **permit**} {**src** *src-wildcard* | **host src** | **any** | *interface idx*} [**time-range** *tm-rng-name*]	Define an access list
DES-7210(config)# **interface** *interface*	Select the interface to which the access list is to be applied.
DES-7210(config-if)# **ip access-group** id { **in** | **out** } **[unreflect]**	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
DES-7210(config)# **ip access-list** { **standard** | **extended** } { *id* | *name* }	Enter the access list configuration mode
DES-7210 (config-xxx-nacl)# [**sn**] { **permit** | **deny** } {**src** *src-wildcard* | **host src** | **any** } [**time-range** *tm-rng-name*]	Add table entries for ACL. For details, please see command reference.
DES-7210(config-xxx-nacl)# **exit** DES-7210(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7210(config-if)# **ip access-group** *id* { **in** | **out** } **[unreflect]**	Apply the access list to the specific interface

Note

Method 1 only configures the numerical value ACL. Method 2 can configure names and numerical value ACL and specify the priorities of table entries (in the devices that support ACE priority levels).

By default, the reflected ACL is enabled on the IP ACL port. Use the **unreflect** command to disable the reflected ACL.

(The following introduces the operation principle of the reflected ACL:

a. Router auto-generates a temporary access list according to the L3, L4 information of the beginning traffic in the internal network based on the principles of protocol is constant, the source and destination IP addresses, and the source and destination ports are rigidly exchanged.

b. Routers allows the traffic to flow into the internal network only when the L3, L4 information of returned traffic is matched with the one in the temporary access list previously created based on the outputting traffic.)

55.2.3 Showing IP ACL

To monitor access lists, run the following command the in privileged user mode:

```
DES-7210# show access-lists [ id | name ]
```

This command can be used to view the basic access list.

55.2.4 IP ACL Example

- **Configuration requirements:**

There are two devices Switch A and Switch B, as shown in Figure 3:

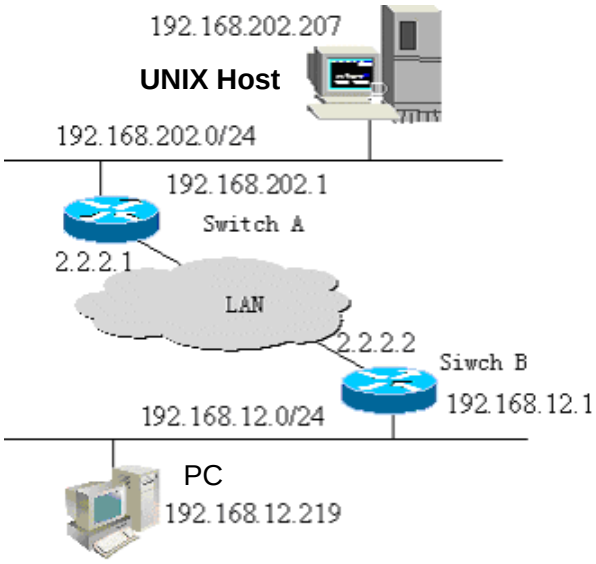


Figure-3 Basic Access List Example

It is required to implement the following security functions by configuring access lists on Switch B.

1. Hosts at the 192.168.12.0/24 network section can only access the remote UNIX host TELNET service during the normal working time period and deny the PING service.
2. On the Switch B console, access to any of the services of hosts at the 192.168.202.0/24 network section is denied.

Note The above case simplifies the application in the bank system. Namely, it only allows the hosts on the Local Area Network of branches or savings agencies to access the central host and disallows accessing the central host on the device.

■ Equipment Configuration

Switch B configuration:

```
DES-7210(config)# interface GigabitEthernet 0/1
DES-7210(config-if)# ip address 192.168.12.1 255.255.255.0
DES-7210(config-if)# exit
DES-7210(config)# interface GigabitEthernet 0/2
DES-7210(config-if)# ip address 2.2.2.2 255.255.255.0
DES-7210(config-if)# ip access-group 101 in
DES-7210(config-if)# ip access-group 101 out
```

According to requirements, configure an extended access list numbered 101

```
access-list 101 permit tcp 192.168.12.0 0.0.0.255 any eq telnet time-range check
DES-7210(config)# access-list 101 deny icmp 192.168.12.0 0.0.0.255 any
DES-7210(config)# access-list 101 deny ip 2.2.2.0 0.0.0.255 any
DES-7210(config)# access-list 101 deny ip any any
```

Configure the time range

```
DES-7210(config)# time-range check
DES-7210(config-time-range)# periodic weekdays 8:30 to 17:30
```

Note

For access list 101. the lat rule sentence ”access-list 101 deny ip any any” is not needed, for the ending part of the access list implicates a “deny any” rule sentence.

For the DES-7200 series, the extended IP ACL does not support the neq matching of TCP/UDP at L4 port.

Switch A configuration:

```
DES-7210(config)# hostname DES-7210
DES-7210(config)# interface GigabitEthernet 0/1
DES-7210(config-if)# ip address 192.168.202.1 255.255.255.0
DES-7210(config)# interface GigabitEthernet 0/2
DES-7210(config-if)# ip address 2.2.2.1 255.255.255.0
```

55.3 Configuring Extended MAC Address-based Access Control List

To configure MAC address-based access control lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol. The following table lists the range of the numbers that can be used to specify MAC access lists.

Protocol	Number Range
Extended MAC Access List	700-799

Caution

Extended MAC access list can not support REF.

55.3.1 Configuration Guide of Extended MAC Address-based Access Control List

When you create an expert access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

The typical rules defined in MAC access lists are the following:

- Source MAC address
- Destination MAC address
- Ethernet protocol type
- Time-range

The MAC extended access list (number 700 – 799) forwards or blocks the packets based on the source and destination MAC addresses, and can also match the Ethernet protocol type.

A single MAC access list can use multiple separate access list sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list.

55.3.2 Configuring Extended MAC Address-based Access Control List

The configuration of an MAC access list includes the following steps:

1. Define an MAC access list
2. Apply the access list to a specific interface

There are two methods to configure an MAC access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **access-list** id {**deny** | **permit**}{**any** | **host** *src-mac-addr*} {**any** | **host** dst-mac-addr} [*ethernet-type*] [**cos** *cos*]	Define an access list. For details about commands, please see command reference.
DES-7210(config)# **interface** *interface*	Select the interface to which the access list is to be applied.
DES-7210(config-if)# **mac access-group** *id* { **in** | **out** }	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
DES-7210(config)# **mac access-list extended** {*id* | *name*}	Enter the access list configuration mode
DES-7210 (config-mac-nacl)# [sn] { **permit** | **deny** }{**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos*]	Add table entries for ACL. For details about commands, please see command reference.
DES-7210(config-mac-nacl)# **exit** DES-7210(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7210(config-if)# **mac access-group** {*id* | *name*} { **in** | **out**}	Apply the access list to the specific interface

Note

Method 1 only configures the numerical value ACL. Method 2 can configure names and numerical value ACL and specify the priorities of table entries (they support priority ACE products and are supported on the DES-7200 series switches).

55.3.3 Showing Configuration of MAC Extended Access List

To monitor access lists, please run the following command the in privileged mode:

```
DES-7210# show access-lists [ id | name]
```

You can view basic access lists

55.3.4 MAC Extended Access List Example

It is required to implement the following security functions by configuring MAC access lists:

1. The 0013.2049.8272 host using the ipx protocol cannot access the giga 0/1 port of a device.
2. It can access other ports.

Configure an Ethernet port, apply the access list 101 on the Ethernet port and check all the messages passing in and out on the port.

```
DES-7210> enable
DES-7210# configure terminal
DES-7210(config)# mac access-list extended mac-list
DES-7210(config-mac-nacl)# deny host 0013.2049.8272 any ipx
DES-7210(config-mac-nacl)# permit any any
DES-7210(config-mac-nacl)# exit
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# mac access-group mac-list in
DES-7210(config-if)# end
DES-7210# show access-lists
mac access-list extended mac-list
deny host 0013.2049.8272 any ipx
permit any any
DES-7210#
```

Note

For access lists, ”permit any any” cannot be discarded, for the ending part of an access list implicates a “deny any” rule sentence.

55.4 Configuring Expert Extended Access List

To configure expert extended access lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol.The table below lists the number range of the Expert access list.

Protocol	Number Range
Expert extended access list	2700-2899

Caution

Expert MAC access list can not support REF.

55.4.1 Configuration Guide of Expert Extended Access List

When you create an expert extended access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

The typical rules defined in expert access lists are the following:

All information in basic access lists and MAC extended access lists

VLAN ID

Expert extended access lists (2700 – 2899) are the syntheses of basic access lists and MAC extended access lists and can filter VLAN IDs.

A single expert access list can use multiple separate access list sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list.

55.4.2 Configuring Extended Expert ACL

The configuration of an expert access list includes the following steps:

1. Define an expert access list
2. Apply the access list to a specific interface (application particular case)

There are two methods to configure an expert access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
DES-7210 (config)# **access-list** *id* {**deny** | **permit**} [*prot* | {[*ethernet-type*] [**cos** *cos*]}] [**VID** *vid*] {**src** *src-wildcard* | **host** *src* | **interface** *idx*} {**host** *src-mac-addr* | **any**} {**dst** *dst-wildcard* | **host** *dst* | **any**}{**host** *dst-mac-addr* | **any**}] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragment**] [**time-range** *tm-rng-name*]	Define an access list. For details about commands, please see command reference.
DES-7210(config)# **interface** *interface*	Select the interface to which the access list is to be applied.
DES-7210(config-if)# **expert access-group** *id* {**in** | **out** } **[unreflect]**	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
DES-7210(config)# **expert access-list extended** {*id*|*name*}	Enter the access list configuration mode
DES-7210 (config-exp-nacl)# [*sn*]{ **permit** | **deny** }[*prot* | {[*ethernet-type*] [**cos** *cos*]}] [**VID** *vid*] {**src** *src-wildcard* | **host** *src* | **interface** *idx*}{**host** *src-mac-addr* | **any**} {**dst** *dst-wildcard* | **host** *dst* | **any**} {**host** *dst-mac-addr* | **any**}][**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragment**] [**time-range** *tm-rng-name*]	Add table entries for ACL. For details about commands, please see command reference.
DES-7210(config-exp-nacl)# **exit** DES-7210(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7210(config-if)# **expert access-group** {*id*|*name*} {**in**|**out**} **[unreflect]**	Apply the access list to the specific interface

Note

Method 1 only configures the numerical value ACL. Method 2 can configure names and the numerical value ACL. In a version supporting priority table entries, method 2 can also specify the priorities of table entries (the [*sn*] option in a command).

For the DES-7200 series, the extended Expert ACL does not support the neq matching of TCP/UDP at L4 port.

For R10.3(4), when you apply an ACL with VLAN ID rule on the QinQ tunnel interface, the ACL matches the VLAN ID of the native VLAN on the tunnel port. To match the VLAN ID of the original packet tag, use the **inner** keyword before the VID.

For the DES-7200 series equipped with V2.0 card and 7200-24GE, when you apply the expert ACL with IP and Ethernet fields configured on the outbounding direction, the ACE of matching Ethernet will not take effect.

By default, the reflected ACL is enabled on the extended IP ACL port. Use the **unreflect** command to disable the reflected ACL.

55.4.3 Showing Configuration of Extended Expert ACL

To monitor access lists, please run the following command the in privileged user mode:

```
DES-7210 # show access-lists [id | name]
```

You can view expert access lists

55.4.4 Expert Extended Access List Example

It is required to implement the following security functions by configuring expert access lists:

The 0013.2049.8272 host using vlan 20 cannot access the giga 0/1 port of a device.

It cannot access other ports.

```
DES-7210> enable
DES-7210# config terminal
DES-7210(config)# expert access-list extended expert-list
DES-7210(config-exp-nacl)# permit ip vid 20 any host 0013.2049.8272 any any
DES-7210(config-exp-nacl)# deny any any any any
DES-7210(config-exp-nacl)# exit
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# expert access-group expert-list in
DES-7210(config-if)# end
DES-7210# show access-lists
expert access-list extended expert-list
petmit ip vid 20 any host 0013.2049.8272 any any
deny any any
```

55.5 Configuring IPv6-based Extended Access List

55.5.1 Configuring IPv6 Extended Access List

The configuration of an IPv6-based access list includes the following steps:

1. Define an IPv6 access list

2. Apply the access list to a specific interface (application particular case)

There is the following method to configure a basic access list. Run the following command in the ACL configuration mode:

Command	Function
DES-7210(config)# **ipv6 access-list** *name*	Enter the access list configuration mode
DES-7210 (config-ipv6-nacl)# [sn] **{permit | deny** }prot {src-ipv6-prefix/prefix-len | **host** *src-ipv6-addr* | **any**} *{dst-ipv6-pfix/pfix-len* | **any | host** *dst-ipv6-addr*} [**dscp** *dscp*] [**flow-label** *flow-labe*l] [**time-range** *tm-rng-name*]	Add table entries for ACL. For details about commands, please see command reference.
DES-7210(config-exp-nacl)# **exit** DES-7210(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7210(config-if)# **ipv6 traffic-filter** *name* {**in** | **out**}	Apply the access list to the specific interface

55.5.2 Showing Configuration of IPv6Extended Access List

To monitor access lists, please run the following command the in privileged user mode:

```
DES-7210# show access-lists [name]
```

This command can be used to view the basic access list.

55.5.3 IPv6 Extended Access List Example

It is required to implement the following security functions by configuring access lists:

The 192.168.4.12 host can access the gi 0/1 port of a device.

It cannot access other ports.

```
DES-7210> enable
DES-7210# config terminal
DES-7210(config)# ipv6 access-list v6-list
DES-7210(config-ipv6-nacl)# permit ipv6 ::192:68:4:12/24 any
DES-7210(config-ipv6-nacl)# deny ipv6 any any
DES-7210(config-ipv6-nacl)# exit
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# ipv6 traffic-filter v6-list in
DES-7210(config-if)# end
DES-7210# show access-lists
ipv6 access-list extended v6-list
permit ipv6 ::192.168.4.12 any
deny any any
DES-7210#
```

Caution

For the DES-7200 series, IPv6 ACL supports the following matching areas:

Protocol, sip, l4_src,dip, l4_dst, dip, dscp, flow_label.

An IPv6 ACL supports any one of the following three matching areas:

1. sip, dip
2. protocol, sip, l4_src, l4_dst, dscp, flow_label
3. protocol, dip, l4_src, l4_dst, dscp, flow_label

An ACL cannot match all the above areas. Besides, the IPv6 ACL does not support the fragment matching.

Besides, when an ACL match sip and dip at the same time, it can not support the matching of type code of icmp or source and destination port.

55.6 Configuring ACL80

The ACL80 is also call the custom access list, which means matching the first 80 bytes of the message to filter the messages. A message consists of a series of byte flows. The ACL80 enables the user to perform match filtering by bits in the specified 16 bytes of the first 80 bytes in the message.

Note

The randomly specified 16 bytes does not contain the following fields:

Packet SMAC, DMAC,SIP, DIP,ETYPE,PROTOCOL,L4_SPORT, L4_DPORT,VID.

In other words, you can select to match the above fields or other 16 bytes.

For any 16-byte field, it is possible to compare or not the configured value by bits. In other words, it allows setting any bit of those 16 bytes as 0 or 1. There are two factors in filtering any byte: filtering rule and filter domain template. The bits of the both are one-to-one corresponding. The filtering rule specifies the value of the field to be filtered. The filter domain template specifies whether to filter the related fields in the filtering rule (“1” indicates matching the bit in the corresponding filtering rule, 0 for not). Therefore, when it is time to match a bit, it is required to set 1 for the corresponding bit in the filter domain template. If the filter domain template bit is set as 0, no match will be done no matter what the corresponding bit is in the filtering rule.

For example,

```
DES-7210(config)# expert access-list advanced name
DES-7210(config-exp-dacl)# permit 00d0f8123456 ffffffffffff 0
DES-7210(config-exp-dacl)# deny 00d0f8654321 ffffffffffff 6
```

The user custom access control list matches any byte of the first 80 bytes in the layer-2 data frames according to the user definitions, and then performs corresponding processing for the messages. To use the user custom access control list correctly, it is necessary to have in-depth knowledge about the structure of layer-2 data frame. The following illustrates the first 64 bytes in a layer-2 data frame (each letter indicates a hexadecimal number, and each two letters indicate a byte).

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD

DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM

NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT

UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

In the figure above, the meaning of each letter and the value of offset are shown below:

Letter	Meaning	Offset	Letter	Meaning	Offset

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol ID	35
C	VLAN tag field	12	Q	IP checksum	36
D	Data frame length field	14	R	Source IP address	38
E	DSAP field	18	S	Destination IP address	42
F	SSAP field	19	T	TCP source port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequential number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version No.	26	XY	IP header length and reservation bits	58
K	TOS field	27	Z	Reservation bit and flags bit	59
L	IP packet length	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

As shown in the above table, the offset of each field is it offset in the SNAP+tag 802.3 data frame. In the user custom access control list, the user can use two parameters, the rule mask and offset, to abstract any byte from the first 80 bytes of the data frame, and then compare it with the user defined rule to filter the matched data frame for corresponding processing. The user defined rule can be some fixed attributes of the data. For example, the user wants to filter all the TCP messages by defining the rule as “06”, rule mask as “FF” and offset as 35. Here, the rule mask and offset work together to abstract the contents of the TCP protocol ID field in the received data frame, and compare it with the rule to filter all TCP messages.

An ACL rule takes effect for only ARP packets only when the rule matches the encapsulation data type (ether type) field of 0x0806. The offsets of various fields of an ARP packet are different from an IP packet. The following figure shows the first 53 bytes of an ARP packet, with each letter being a hex numerical and each two letters being a byte:

AA AA AA AA AA AA BB BB BB BBBB BB CC CC DD DD

DD DD EE FF GG HH HH HH II II JJ JJ KK KK LL MM NN NN

OO OO OO OO OO OO PP PP PP PP

QQ QQ QQ QQ QQ QQ RR RR RR RR

The following table shows the meanings and offsets of various letters:

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	Sender MAC address	34
B	Source MAC	6	P	Sender IP address	40
C	VLAN tag field	12	Q	Receiver MAC address	44
D	Data frame length field	14	R	Receiver IP address	50
E	DSAP field	18			
F	SSAP field	19			
G	Ctrl field	20			
H	Org Code field	21			
I	Encapsulated data type	24			
J	Hardware type	26			

Letter	Meaning	Offset	Letter	Meaning	Offset
K	Protocol type	28			
L	Hardware address length	30			
M	Protocol address length	31			
N	Operation type	32			

The offsets appearing in the above table are the ones of 802.3 frame of the tag of SNAP packets.

ACL80 is supported on the DES-7200 series.

The DES-7200 series supports ACL80, including matching against Ethernet packets, 803.3 SNAP packets, and 802.311c packets. If the value for matching DSAP to the cnt1 field is set to AAAA03, it indicates to match the 803.3 SNAP packets. If the value is set to E0E003, it indicates to match the 803.311c packets. This field cannot be set to match Ethernet packets.

Note:

For the DES-7200 series, 3 bytes of AAAA03 must be configured to match the 803.3snap packets(other bytes of AAAA03 shall not be configured). Besides, when using the non-24SFP line card to configure the matched snap packets, if the first byte of the org code filed of the packet is 0, the packet will be dropped. Only if the first byte of the org code is not 0, the packet can be matched. You shall pay special attention to that using this function.

Note

Configuration note:

The ACL180 has only 16 bytes for matching. If the 16 bytes are used, no fields other than the 16 bytes can be matched. For example:

```
DES-7210(config)# expert access-list advanced name
DES-7210(config-exp-dacl)# permit 11223344556677889900aabbccd
deeff ffffffffffffffffffffffffffffff 50
```

If you use the following command to add another ACE:

```
DES-7210(config-exp-dacl)#permit 11223344556677889900aabbccd
deeff ffffffffffffffffffffffffffffff 54
```

The configuration will fail because the 16 bytes are used by the first ACE. To match the second ACE, you must firstly delete the first ACE.

55.7 Configuring TCP Flag Filtering Control

The TCP Flag filtering feature provides a flexible mechanism. At present, TCP Flag filtering control supports the match-all option. Namely, when the TCP Flags in a received message exactly match those defined in the ACL table entry, the message will be checked by the ACL rule. A user can define any combination of TCP Flags to filter some messages with specific TCP Flags.

For example,

```
permit tcp any any match-all rst
```

Allow the messages with a TCP Flag RST set and 0 in other positions to pass

Note

When the protocol number of the naming ACL and numerical value configuration is TCP, you can select to configure this filtering feature. MAC extended and IP standard ones do not have this function.

Please configure a TCP Flag by following these steps:

Command	Function
DES-7210(config)# **ip access-list extended** { id | *name* }	Enter the access list configuration mode
DES-7210(config-ext-nacl)# [*sn*] [**permit** | **deny**] **tcp source** *source-wildcard* [**operator port** *[port]*] **destination** *destination-wildcard* [**operator port** *[port]*] [**match-all** *flag-name*][**precedence** *precedence*]	Add table entries for ACL. For details about commands, please see command reference.
DES-7210(config-exp-nacl)# **exit** DES-7210(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7210(config-if)# **ip access-group** {*id* | *name*} {**in** | **out**}	Apply the access list to the specific interface

The following example explains how to configure a TCP Flag

Enable permission and password

```
DES-7210> enable
DES-7210#
```

Enter the global configuration mode.

```
DES-7210# configure terminal
```

Enter the ACL configuration mode.

```
DES-7210(config)# ip access-list extended test-tcp-flag
```

Add an ACL entry

```
DES-7210(config-ext-nacl)# permit tcp any any match-all rst
```

Add a deny entry

```
DES-7210(config-ext-nacl)# deny tcp any any match-all fin
```

Adding/delete entries repeatedly.

end

```
DES-7210(config-ext-nacl)# end
```

Show

```
DES-7210# show access-list test-tcp-flag
ip access-lists extended test-tcp-flag
10 permit tcp any any match-all rst
20 deny tcp any any match-all fin
```

55.8 Configuring ACL Entries by Priority

To embody the ACE priority, there are standards for each ACL to normalize the ACE arranging method under the ACL by using the numbered start point – increment mode, as detailed below:

- ACE is sorted in the ascend order in the chain table by the sequential numbers.
- Starting from the start point number, if no number is specified, it increases by step on the basis of the previous ACE number.
- To specify number, the ACE is inserted in sorting mode, and the increment ensures new ACE can be inserted between two adjacent ACEs.

- The ACL specifies the start point number and the number increment.

The **ip access-list resequence** {*acl-id*| *acl-name*} *sn-start sn-inc* command is available, with details in the related command reference.

Whenever the above command is run, the ACEs will be re-sorted under the ACL list. For example, the ACE numbers under the ACL named tst_acl is as follows:

In the beginning

```
ace1: 10
ace2: 20
ace3: 30
```

The ACE numbers are as follows after "**ip access-list resequence** *tst_acl 100 3*" is run:

```
DES-7210(config)# ip access-list resequence tst_acl 100 3
ace1: 100
ace2: 103
ace3: 106
```

When adding ace4 without entering sn-num, the numbers are as follows:

```
DES-7210(config-std-nacl)# permit …
ace1: 100
ace2: 103
ace3: 106
ace4: 109
```

When adding ace5 by entering seq-num = 105, the numbers are as follows:

```
DES-7210(config-std-nacl)# 105 permit …
ace1: 100
ace2: 103
ace5: 105
ace3: 106
ace4: 109
```

The reference of the numbers is to implement the priority adding ace mode in step 4.

Delete ACE

```
DES-7210(config-std-nacl)# no 106
ace1: 100
ace2: 103
ace5: 105
ace4: 109
The above numbers can also facilitate deleting ACE.
```

55.9 Configuring ACL Based on Time-range

You can run the ACLs based on time, for example, make the ACL take effect during certain periods in a week. For this purpose, you must first set a Time-Range.

Time-Range implementation depends on the system clock. If you want to use this function, you must assure that the system has a reliable clock.

In the privileged configuration mode, you can create a time-range by performing the following steps:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **time-range** *time-range-name*	Identify a time-range by using a meaningful display character string as its name
DES-7210(config-time-range)# **absolute** [**start time** *date*] **end time** *date*	Set the absolute time range (optional). For details, see the configuration guide of time-range.
DES-7210(config-time-range)# **periodic day-of-the-week time to** [*day-of-the-week*] **time**	Set the periodic time range (optional). For details, see the configuration guide of time-range.
DES-7210# **show time-range**	Verify the configurations.
DES-7210# **copy running-config startup-config**	Save the configuration.
DES-7210(config)# **ip access-list extended** *101*	Enter the ACL configuration mode.
DES-7210(config-ext-nacl)# **permit ip any any time-range** *time-range-name*	Configure the ACE of a time-range.

Note

The length of the name should be 1-32 characters, which should not include any space.

You can set one absolute time range at most. The application based on time-ranges will be valid only in this time range.

You can set one or more periodic intervals. If you have already set a running time range for the **time-range**, the application takes effect at periodic intervals in that time range.

The following example shows how to deny HTTP data streams during the working hours in a week by using the ACLs as example:

```
DES-7210(config)# time-range no-http
DES-7210(config-time-range)# periodic weekdays 8:00 to 18:00
DES-7210(config)# end
DES-7210(config)# ip access-list extended limit-udp
DES-7210(config-ext-nacl)# deny tcp any any eq www time-range no-http
DES-7210(config-ext-nacl)# exit
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# ip access-group no-http in
DES-7210(config)# end
```

Example of displaying time range:

```
DES-7210# show time-range
time-range entry: no-http(inactive)
periodic Weekdays 8:00 to 18:00
time-range entry: no-udp
periodic Tuesday 15:30 to 16:30
```

55.10 Configuring Security Tunnel

Applying a secure ACL globally means that the ACL is a security tunnel. A general ACL is installed on a port or port map; a security tunnel is installed on an interface or globally. The difference between them arises in priority. The security tunnel takes precedence over port security (that is the

IP binding under port security), 802.1x and secure ACL. The global security tunnel takes effect for all ports, unless you set a port as an exception port.

Note

1. A security tunnel supports permit and deny rules.
2. The global security tunnel takes no effect for an exception port.
3. The security tunnel policies enabled on an interface take precedence over the global security tunnel.
4. Without IP authorization, using a security tunnel in 802.1x will reduce the permitted authentication number at large extent, which is in accordance with the one under IP authorization.
5. It is strongly recommended to configure a security tunnel before authentication, so as to avoid the case that resource exhaustion causes the authenticated users cannot access the Interface due to the configuration of security tunnel midway.
6. If MAC-IP binding and MAC related binding under port security are enabled on the DES-7200 series, the related IP and MAC policies configured on other ports do not function.

You can use an exist ACL to configure a security tunnel

In the privileged configuration mode, execute the following commands to configure a global security tunnel:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210(config)# **security global access-group** *acl-name*	Configure a global security tunnel.

In the privileged configuration mode, execute the following commands to set an exception port:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config)# **security uplink enable**	Set the interface as an exception port..

If a security tunnel is configured under the interface, remove the security tunnel and then set the interface as the exception port.

In the privileged configuration mode, execute the following commands to configure a security tunnel on the interface:

Command	Function
DES-7210# **configure terminal**	Enter the global configuration mode.
DES-7210# **interface** *interface-id*	Enter the interface configuration mode.
DES-7210(config)# **security access-group** *acl-name*	Configure a security tunnel on the interface.

If the interface is set as an exception port, remove the setting and then configure the security tunnel on the interface.

The following example configures a security tunnel.

Set port 4 as security port and bind IP address and MAC address

```
DES-7210(config)#interface FastEthernet 0/4

DES-7210(config-if)#switchport port-security

DES-7210(config-if)#switchport port-security mac-address 0000.0000.0011 ip-address
192.168.6.3
```

Only the packets whose source IP address is 192.168.6.3 and MAC address is 0000.0000.0011 can flow in the switch from port 4. To receive IPX packets, set a security tunnel as follows:

```
DES-7210 #configure
DES-7210 (config)#expert access-list extended safe_channel
DES-7210 (config-exp-nacl)#permit ipx any any
DES-7210 (config-exp-nacl)#exit
DES-7210 (config)#security global access-group safe_channel
```

Or configure a security tunnel on the interface:

```
DES-7210 #configure
DES-7210 (config)#expert access-list extended safe_channel
DES-7210 (config-exp-nacl)#permit ipx any any
DES-7210 (config-exp-nacl)#exit
DES-7210(config)#interface FastEthernet 0/4
DES-7210 (config-if)#security access-group safe_channel
```

55.11 Configuration Examples

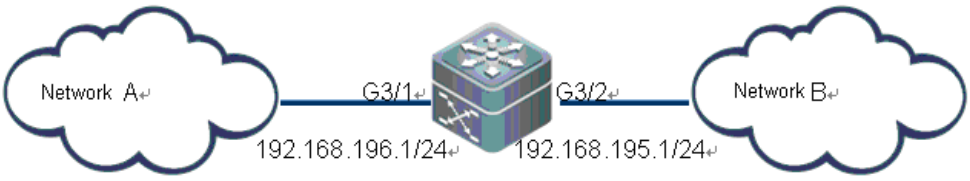
55.11.1 Configuring Unidirectional TCP Connection

Configure TCP Flag filtering to enable unidirectional ACL.

Configuration Requirements

For the security of network A, the hosts in network A are allowed to originate the TCP connection request to the hosts in network B. However, the hosts of network B are not allowed to originate the TCP communication requests to network A.

Topology View



As shown in the above figure, two networks are connected through a layer 3 switch. Network A connects to the G3/1 port of the switch and network B connects to the G3/2 port of the switch.

Analysis

By filtering the packets of TCP connection request originated by network B on the G3/2 port of the switch, you can block the TCP connection request from hosts in network B to network A. Accoding to the analysis of TCP connection, the SYN of the flag field in the TCP header of the initial TCP request packet is reset and the ACK is set to 0. Therefore, to enable network A to access network B in the one-way direction, configure the Match-all option of the extended ACL to set the SYN of the TCP header to 1 and ACK to 0 on the inbounding direction of theG3/2 port.

Configuration Procedure

1 Define an Access Control List (ACL)

Enter the configuration mode of the switch

```
DES-7210# configure terminal
```

Create the extended ACL101 in the configuration mode

```
DES-7210(config)# ip access-list extended 101
```

Deny the packets whose SYN is 1 and permit other packets whose SYN is 0 (including ACK)

```
DES-7210(config-ext-nacl)# deny tcp any any match-all SYN
```

Permit other IP packets

```
DES-7210(config-ext-nacl)# permit ip any any
```

2 Apply the ACL at the interface

Exit ACL mode

```
DES-7210(config-ext-nacl)# exit
DES-7210(config)# interface vlan 1
DES-7210(config)# ip address 1.1.1.1 255.255.255.0
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)#ip access-group ifaddr in
```

Enter the G3/2 port on which the ACL is applied

```
DES-7210(config)# interface gigabitEthernet 3/2
```

Apply ACL 101 to the packet filtering at the inlet of G3/2

```
DES-7210(config-if)# ip access-group 101 in
```

3 Show the configuration of ACL

In the privileged mode, use the **Show** command to display related configuration of ACL

```
DES-7210# show access-lists 101
ip access-list extended 101
 10 deny tcp any any match-all syn
 20 permit ip any any
```

55.12 Acl Configuration of Different Line Cards

The following description is applicable for DES-7200 R10.3(1) and later.

7200-24GE or other enhanced line cards can provide 3838 entries for acl in incoming direction and 512 entries for acl in outgoing direction since their hardware resources have been increased.

Acl out has two processing methods:

When all the line cards online are 7200-24GE or other enhanced line cards, acl out can associate the outgoing port and takes effect for any packet, supporting associating svi, l3ap and router port with the outgoing port.

When there are other line cards among the line cards online, which are not 7200-24GE or other enhanced line cards, acl out takes effect only for known unicast packets and does not support router port and l3ap on L3. This principle is also appropriate for hot plugging/unplugging line cards, which prompts the users to reset line cards.

Note that when the non-E line cards are inserted in the chassis, ACL out association at the outbounding direction on ACCESS port is valid for the known unicast packets forwarded in Layer2 only, but invalid for the broadcast packets and packets forwarded in Layer3.

If acl out is implemented on the exit port, then ip extension acl and expert acl will not support port matching. Besides, expert acl only supports ip packet matching, not other L2 packets, IPV6 does not support flow_label, dscp and fragment matching.

If acl out is processed in the original way, then associating acl out with svi has lots of restrictions:

- Changes the priority of in and out direction; the acl used in out direction is higher than that used in in direction.
- When associating acl with svi in out direction, there is no **deny any any** option by default. But there is **deny any any** option in other acl application.
- Associating acl with svi in Out direction can support ip standard, ip extension, mac extension, acl application of expert extension.
- There are some restrictions for matching destination ip and destination mac in acl when associating acl with svi in Out direction. If you want to match destination mac in mac extension and expert acl and applicate the acl in out direction of svi, the entry will be set and not take effect.
- The set acl will not take effect if you want to match destination ip, which is not within the subnet ip range of associated svi, in ip standard, ip extension and expert acl . For example, the address of vlan 1 is 192.168.64.1 255.255.255.0. And now, if you create an ip extended acl with ace deny udp any 192.168.65.1 0.0.0.255 eq 255, it will not take effect when applicating this acl to the exit port of vlan 1, for the destination ip is not within the subnet ip range of vlan 1; but it will take effenct if the ace is deny udp any 192.168.64.1 0.0.0.255 eq 255, for the destination ip is up to sepecification.
- The priority of associating acl with svi in out direction is higher than that of all the other acl application.
- Acl out does not support user-defined acl type.

56 VACL Configuration

56.1 Overview

The implementation method of ACL is directly applying ACL on port SVI in VLAN, which is the same as applying ACL on physical port. While VLAN Access Control(VACL), which is also named as VLAN Access Mapping List, has different implementation method. VACL is used for inter- and intra VLAN communications. Moreover, it supports ETHERTYPE-based and MAC-based filtering and prevents unauthorized data flow from entering VLAN. There are three actions supporting VACL: forward, drop and redirect.

56.2 VACL Configuration

56.2.1 Creating VLAN Access Map

In the global configuration mode, use the following commands to create VLAN access map:

Command	Function
DES-7210(config)# **vlan access-map** *map_name* [*map_sn*]	Create a submap with map_sn range from 0 to 65535.
DES-7210(config)# **no vlan access-map** *map_name* [*map_sn*]	Delete a submap with map_sn range from 0 to 65535.
DES-7210(config)# **no vlan access-map** *map_name*	Delete a hostmap.

It will enter the **config-access-map** mode after creating **vlan access map** successfully.

Caution

Vlan access map has 2 keywords. *map_name* is the major keyword and indispensable, while *map_sn* is the minor one which can be omitted. We define the collection of one or multiple submap(s) with the same name as hostmap.

1. In fact, creating **vlan access map** is creating a submap. When *map_sn* is not specified, it will add 10 before the submap and on the basis of *map_sn* of the submap which belongs to the same hostmap.

2. When *map_sn* is not specified, deleting **vlan access map,** all *Map_nam*e with the same *map_name* will be deleted, that is to say, the hostmap is deleted.

3. When *map_sn* is not specified, deleting **vlan access map** will delete the specified submap. When the hostmap to which the specified submap belongs does not includes submaps, then the hostmap will be deleted automatically; and vice versa.

4. One hostmap includes 6553 submaps at most.

56.2.2 Configuring match Content of vlan access map

Execute the following commands in the access map configuration mode:

Command	Function
DES-7210(config-access-map)# **match ip address** {*1 –199* | *1300 – 2699* | *acl_name* }	Associate ip acl with specified submap.
DES-7210(config-access-map)# **match mac** address {*700 –799* | *acl_name* }	Associate mac acl with specified submap.
DES-7210(config-access-map)# **no match ip address** {*1 –199* | *1300 – 2699* | *acl_name* }	Remove the association between ip acl and specified submap.
DES-7210(config-access-map)# **no match mac address** {*700 –799* | *acl_name* }	Remove the association between mac acl and specified submap.

Caution

1. Now, a submap can only be associated with ip acl or map acl. You can not associate a submap with both ip acl and map acl.

2. One submap can only be associated with at most 8 acls.

3. One submap can not be associated with an inexistent acl.

4. One submap can not be associated with acl without ace, which is null acl.

5. When a submap has been associated with ip acl (mac acl), you need to configure to associate ip acl (mac acl) again. And ip acl (mac acl) later configured is after the one first configured.

6. When a submap has been associated with ip acl (mac acl), you need to configure to associate mac acl (ip acl) again and delete the configured ip acl (MAC acl) automatically first and then configure MAC acl (ip acl).

56.2.3 Configuring actions Content of vlan access map

Execute the following commands in the access map configuration mode(or in VACL mode):

Command	Function
DES-7210(config-access-map)# **action drop**	Configure drop action of the specified submap.
DES-7210(config-access-map)# **action** forward	Configure forward action of the specified submap.
DES-7210(config-access-map)# **action redirect** {**gigabitEthernet** | **aggregateport** } { *port_number*}	Configure redirect action of the specified submap.
DES-7210(config-access-map)# **no action drop**	Delete drop action of the specified submap.
DES-7210(config-access-map)#**no action forward**	Delete forward action of the specified submap.
DES-7210(config-access-map)# **no action redirect** {**gigabitEthernet** | **aggregateport** }{ *port_number*}	Delete redirect action of the specified submap.

Caution

1. One submap only has one action. That is, you choose one action from drop, forward and redirect;
2. Redirect action specifies only one port to redirect;
3. By default, the action is **forward** if the submap is not onfigured;
4. When a submap is associated with ip acl, the default action for the Layer 2 packet is **forward**. But for the Layer 3 packet matched with no ip acl, the default action is **drop**.
5. When a submap is associated with mac acl, the default action for the Layer 3 packet is **forward**. But for the Layer 3 packet matched with no ip acl, the default action is **drop**.

56.2.4 Application of Vlan Access Map

In the global configuration mode, execute the following commands to create VLAN access map:

Command	Function
DES-7210(config)#**vlan filter** *map-name* **vlan-list** *vlan_id*	Apply VLAN access map in the specified VLAN .
DES-7210(config)# **no vlan filter** *map-name* **vlan-list** *vlan_id*	Delete the application of VLAN access map in the specified VLAN.

Caution

1. Hostmap is the unit of VLAN access map application. In other words, map-sn can not be input;
2. A VLAN access map can be applied to more than one VLAN separated with comma. You can also input a VLAN range, for instance, **vlan filter** *aa* **vlan-list** *1-33*, which means applying the map to VLAN 1 to VLAN 33.

56.2.5 Displaying Vlan Access Map

Command	Function
DES-7210# **show vlan access-map** [*map_name*]	Show the information of vlan access map.
DES-7210# **show vlan filter**	Show the application of all vlan access maps in vlan.
DES-7210# **show vlan filter access-map** *map_name*	Show the application of the specified vlan access map in vlan.
DES-7210# **show vlan filter vlan** *vlan_id*	Show the application of vlan access map in the specified vlan.

57 QoS Configuration

57.1 QoS Overview

The fast development of the Internet results in more and more demands for multimedia streams. Generally, people have different service quality requirements for different multimedia, which requires the network to be able to allocate and dispatch resources according to the user demands. As a result, the traditional "best effort" forwarding mechanism cannot meet the user demands. So the QoS emerges.

The QoS (Quality of Service) is used to evaluate the ability for the service provider to meet the customer demands. In the Internet, the QoS mechanism is introduced to improve the network service quality, where the QoS is used to evaluate the ability of the network to deliver packets. The commonly-mentioned QoS is an evaluation on the service ability for the delay, jitter, packet loss and more core demands.

57.1.1 Basic Framework of QoS

The devices that have no QoS function cannot provide the capability of transmission quality service, and will not ensure special forwarding priority for certain dataflow. When bandwidth is abundant, all the traffic can be well processed. But when congestion occurs, all traffic could be discarded. This kind of forwarding policy is otherwise called the service of best effect, since the device now is exerting its performance of data forwarding and the use of its switching bandwidth is maximized.

The device of this module features the QoS function to provide transmission quality service. This makes it possible to select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. The network environment with QoS configured is added with predictability of network performance and allocates network bandwidth more effectively to maximize the use of network resources.

The QoS of this device is based on the DiffServ (Differentiated Serve Mode) of the IETF Internet Engineering Task Force. According to the definitions in the DiffServ architecture, every transmission message is classified into a category in the network, and the classification information is included in the IP packet header. The first 6 bits in the ToS (Type of Service) field for IPv4 packet header or the Traffic Class field for Ipv6 packet header carry the classification information of the message. The classification information can also be carried in the Link layer packet header. Below shows the special bits in the packet:

- Carried by the first 3 bits in the Tag Control Information of 802.1Q frame header, which contains the priority information of one of the 8 categories. These three bits are generally called User Priority bits.
- Carried by the first 3 bits of the ToS field for IPv4 packet header or Traffic Class field for IPv6 packet header, called IP precedence value; or carried by the first 6 bits of the ToS field for IPv4 packet header or Traffic Class field for IPv6 packet header, called Differentiated Services Code Point (DSCP) value.

In a DiffServ-compliant network, every device has the same transmission service policy for the messages with the same classification information, and vice versa. The class information in the

packet can be assigned by all the systems along the way, such as hosts, devices, or other network devices. It's based on a policy set by a manager, or contents in the packet, or both. The assignment of class information in order to identify packets usually consumes enormous resources of the network device. To reduce the processing overhead on the backbone network, such assignment is often used on the network edge. Based on the class information, the devices can provide different priorities for different traffic, or limit the amount of resources allocated per traffic class, or appropriately discard the packets of less important, or perform other operations as appropriate. This behavior of these independent devices is call per-hop behavior in the DiffServ architecture.

If all devices in the network are providing consistent per-hop behavior, this network forms the end-to-end QoS solution for the DiffServ architecture.

57.1.2 QoS processing flow

57.1.2.1 Classifying

The process of classifying involves putting the messages to the dataflow indicated with CoS value according to the trust policy or the analysis of the message contents. As a result, the core task of classifying is to determine the CoS value of a message. It happens when the port is receiving the inbound messages. When a port is associated with a policy-map that represents a QoS policy, the classification will take effect and be applied on all the messages input through that port.

For general non-IP messages, the switch classifies the messages according to the following criteria:

- If the message itself does not contain any QoS information, which means the layer-2 packet header has no User Priority bits, it gets the QoS information of the message by using the default CoS value of the message input port. Like the User Priority bits of the message, the default CoS value of the port ranges 0~7.
- If the message itself contains QoS information, which means the layer-2 packet header has User Priority bits, it gets the CoS information directly from the message.

Note

The above criteria take effect only when the QoS trust mode of the port is enabled. Enabling the QoS trust mode of a port does not mean getting the QoS information directly from the message or the input port of the message without analyzing the message contents.

- If the policy-map associated with the port is using the ACL classifying based on the MAC access-list extended, the associated ACLs will be matched by getting the source MAC address, destination MAC address and Ethertype domain of the message on that port, to determine the DSCP value of the message. Note that, if a port is associated with a policy-map but has no DSCP value set for it, the switch will assign the priority for the messages of this classification by performing the default behavior: following the priority information contained in the layer-2 packet header of the message or the default priority of the port.

Note

The above three criteria may apply simultaneously on the same port. In this case, they will take effect according to the sequence 3, then 2 and then 1. In other words, the ACLs work first for the classifying operation. When it fails, the criteria 2 will be used, and so on. Here, if the QoS trust mode of the port is enabled, criteria 2 and 1 will be used to get the QoS information directly from the message or the port; otherwise, default DSCP value 0 will be assigned for the messages failing the classifying operation.

For IP messages, the switch classifies the messages according to the following criteria:

- If the port trust mode is Trust ip-precedence, it extracts from the ip precedence field (3 bits) of the IP message and fills the CoS field (3 bits) of the output message.

- If the port trust mode is Trust cos, it extracts directly the CoS field (3 bits) of the message and overwrite the ip precedence field (3 bits) of the message. There are the following two cases. Case 1 is that the layer-2 packet header does not contain User Priority bits, and now the CoS value is got from the default CoS value of the message input port. Case 2 is that the layer-2 packet header contains User Priority bits, and now the CoS is got directly from the packet header.
- If the Policy-map associated with the port is using the ACLs classifying based on the ip access-list (extended), the associated ACLs will be matched by getting the source IP address, destination IP address, Protocol field and layer-4 TCP/UDP port field of the message, to determine the DSCP value of the message, and the CoS value is determined according to the mapping from DSCP to CoS. Note that, if a port is associated with a policy-map but has no DSCP value set for it, the switch will use the above criteria 1 and 2 to determine the priority.

Just like the criteria for non-IP message classifying, the above classifying criteria can apply on the same port at the same time. In this case, they will take effect according to the sequence 3, then 2 and then 1.

For the details of the CoS-to-DSCP map and IP-precedence-to-DSCP map, see the descriptions below.

57.1.2.2 Policing

The Policing action happens after the data classifying is completed. It is used to constrain the transmission bandwidth occupied by the classified dataflow. The Policing action will check every message in the classified dataflow. If the message is occupying more bandwidth as allowed by the police that applies on that dataflow, the message will be treated specially, either to be discarded or assigned with another DSCP value.

In the QoS processing flow, the Policing action is optional. If no Policing action is enabled, the DSCP value of messages in the classified dataflow will remain unchanged, and no message will be discarded before the message is sent for the Marking action.

57.1.2.3 Marking

After the Classifying and Policing actions, the Marking action will write the QoS information for the message to ensure the DSCP value of the classified message can be transferred to the next hop device in the network. Here, the QoS ACLs can be used to change the QoS information of the message, or the QoS information is reserved in the Trust mode. For example, the Trust DSCP can be selected to reserve the DSCP information in the IP packet header.

57.1.2.4 Queuing

The Queuing action is responsible for transferring the messages in the dataflow to an output queue of the port. The messages in different output queues will have transmission service policies of different levels and qualities.

Each port has 8 output queues. The two mapping tables DSCP-to-CoS Map and Cos-to-Queue Map configured on the switch convert the DSCP value of the message into output queue number so as to determine which output queue to transfer the messages into.

57.1.2.5 Scheduling

The Scheduling action is the last cycle in the QoS process. After the messages are transferring into different output queues of the port, the switch works with WRR or another algorithm to transmit the messages in those 8 queues.

It is possible to set the weight in the WRR algorithm to configure the amount of messages to be transmitted in every cycle of message output, thus affecting the transmission bandwidth. Alternatively, it is possible to set the weight in the DRR algorithm to configure the amount of message bytes to be transmitted in every cycle of message output, thus affecting the transmission bandwidth.

57.1.3 QoS Logic Interface Group

A series of interface, which could be APs, or the physical ports, can be specified as one QoS logic interface group, and association the logic interface group with Policy-map for the QoS processing. Take the rate-limit for example, the packets that correspond to the rate-limit condition share the bandwidth value limited by Policy-map on all ports within the same logic interface group.

Note

The member ports join the logic interface group must be physical ports or Aggregate Port.

For the DES-7200 series, the member of the logic interface group must be in the same line card. If there are 48 ports in the line card, all member ports must be distributed in the former 24 ports or the latter 24 ports.

The supported logic interface group number is up to 128.

57.2 QoS Configuration

57.2.1 Default QoS configuration

Make clear the following points of QoS before starting the configuration:

- One interface can be associated with at most one policy-map.
- One policy-map can have multiple class-maps.
- One class-map can be associated at most one ACL, and all ACEs in that ACL must have the same filter domain template.
- The amount of ACEs associated with one interface meets the constraint described in the section "Configuring secure ACL".

By default, the QoS function is disabled. That is, the device treats all messages equally. When you associate a Policy Map with a port and set the trust mode of the port, the QoS function of that port is enabled. To disable the QoS function of a port, you may remove the Policy Map setting and set the trust mode of the port as Off. Below is the default QoS configuration:

Default CoS value	0
Number of Queues	8
Queue Scheduling	WRR
QueueWeight	1:1:1:1:1:1:1:1
WRR Weight Range	1:15
DRR Weight Range	1:15
Trust mode	No Trust

Default mapping table from CoS value to queue

CoS Value	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Default mapping table from CoS to DSCP

CoS Value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

Default mapping table from IP-Precedence to DSC

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Default mapping table from DSCP to CoS

DSCP	0	8	16	24	32	40	48	56
CoS	0	1	2	3	4	5	6	7

57.2.2 Configure the QoS trust mode of the interface

By default, the QoS trust mode of an interface is disabled.

Command	Description
configure terminal	Enter the configuration mode
interface interface	Enter the interface configuration mode.
mls qos trust {cos | ip-precedence | dscp}	Configure the QoS trust mode of the interface CoS, dscp or ip-precedence
no mls qos trust	Restore the QoS trust mode of the interface to default

The command below set the trust mode of interface gigabitEthernet 0/4 to DSCP:

```
DES-7210(config)# interface gigabitEthernet 0/4
DES-7210(config-if)# mls qos trust dscp
DES-7210(config-if)# end
DES-7210# show mls qos interface g0/4
Interface GigabitEthernet 0/4
Attached input  policy-map:
Default COS: trust dscp
Default COS: 0
DES-7210#
```

57.2.3 Configuring the Default CoS Value of an Interface

You may configure the default CoS value for every interface through the following steps.

By default, the CoS value of an interface 0.

Command	Description
configure terminal	Enter the configuration mode
interface interface	Enter the interface configuration mode.
mls qos cos default-cos	Configure the default CoS value of the interface, where default-cos is the desired default CoS value, ranging 0~7.

Command	Description
no mls qos cos	Restore to the default CoS value.

The example below set the default CoS value of interface g0/4 to 6:

```
DES-7210# configure terminal
DES-7210(config)# interface g 0/4
DES-7210(config-if)# mls qos cos 6
DES-7210(config-if)# end
DES-7210# show mls qos interface g 0/4
Interface GigabitEthernet 0/4
Attached input  policy-map:
Default COS: trust dscp
Default COS: 6
DES-7210#
```

57.2.4 Configuring the Logic Interface Group

To configure the logic interface group, run the following command in the interface configuration mode:

Command	Description
DES-7210(config-if)#**virtual-group** *virtual-group-number*	Add an interface to the logic interface group. *virtual-group-number:* the goup number of the logic interfaces.

Use the **no virtual-group** *virtual-group-number* command to make a physical port to exit from the logic interface group.

The example below set the interface g0/1 to the member of logic interface group 5:

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# virtual-group 5
DES-7210(config-if-range)# end
```

57.2.5 Configuring Class Maps

You may create and configure Class Maps through the following steps:

Command	Description
configure terminal	Enter the configuration mode
ip access-list extended{*id*|*name*} … **ip access-list standard** {*id*|*name*} … **mac access-list extended** {id|*name*} … **expert access-list extended{***id*|*name*} … **ipv6 access-list extended name** … **access-list id**[…]	Create ACL Please refer to the chapter of ACL

Command	Description
[no] class-map *class-map-name*	Create and enter into the class map configuration mode, where class-map-name is the name of the class map to be created. The no option will delete an existing class map
[no] match access-group {*acl-num* | *acl-name }*	Set the matching ACL, where a*cl-name* is the name of the created ACL, acl-num is the ID of the created ACL; the no option delete that match.

For example, the following steps creates a class-map named class1, which is associated with a ACL:acl_1. This class-map will classify all TCP messages with port 80.

```
DES-7210(config)# ip access-list extended acl_1
DES-7210(config-ext-nacl)# permit tcp any any eq 80
DES-7210(config-ext-nacl)# exit
DES-7210(config)# class-map class1
DES-7210(config-cmap)# match access-group acl_1
DES-7210(config-cmap)# end
```

57.2.6 Configuring Policy Maps

You may create and configure Policy Maps through the following steps:

Command	Description
configure terminal	Enter the configuration mode
[no] policy-map *policy-map-name*	Create and enter into the policy map configuration mode, where policy-map-name is the name of the policy map to be created. The no option will delete an existing policy map
[no] class *class-map-name*	Create and enter into the data classifying configuration mode, where class-map-name is the name of the class map to be created. The **no** option deletes that data classification
[no]set ip dscp *new-dscp*	Set new ip dscp value for the IP messages in the dataflow; it does not take effect for non-IP messages. *new-dscp* is the new DSCP value to be set, whose range varies with the specific product.
police *rate-bps burst-byte* **[exceed-action** {**drop** | **d*scp*** *dscp-value*}]**no police**	Limit the bandwidth of the dataflow and specify the action for the excessive bandwidth part, where *rate-bps* is the limited bandwidth per second (kbps), *burst-byte* is the limited burst bandwidth (Kbyte), **drop** means dropping the message of the excessive bandwidth part, **dscp** *dscp-value* means changing the DSCP value of the message in excessive bandwidth part, and *dscp-valu*e value range varies with specific products. The effective range of the burst-byte is 4 to 2097152.

For example, the following steps create a policy-map named policy1 and associate it with interface Gigabitethernet 1/1.

```
DES-7210(config)# policy-map policy1
DES-7210(config-pmap)# class class1
DES-7210(config-pmap-c)# set ip dscp 48
```

```
DES-7210(config-pmap-c)# exit
Router(config-pmap)# exit
DES-7210(config)# interface gigabitethernet 1/1
DES-7210(config-if)# switchport mode trunk
DES-7210(config-if)# mls qos trust cos
DES-7210(config-if)# service-policy input policy1
```

57.2.7 Applying Policy Maps on the Interface

You may apply the Policy Maps to a port through the following steps:

Command	Description
configure terminal	Enter the configuration mode
Interface *interface*	Enter the interface configuration mode.
[no] service-policy {**input | output** *policy-map-name}*	Apply the created policy map to the interface, where the *policy-map-name* is the name of the created policy map, **input** is the input rate limit and **output** is the output rate limit.

Note

The DES-7200 series supports applying the policy map to the out direction only for the line card 7200-24GE. Because it is necessary to associate the class map with acl, all restrictions of the acl configuration are applicable for the qos configuration. For the details, see the *ACL Configuration*.

57.2.8 Applying Policy Maps to the Logic Interface Group

To apply Policy Maps to the logic interface group, run the following commands:

Command	Description
configure terminal	Enter the configuration mode
virtual-group *virtual-group-number*	Enter the logic interface group configuration mode.
[**no**] **service-policy** {**input | output**} *policy-map-name*	Apply the created Policy Maps to the logic interface group. *policy-map-name:* the name of created policy map; input*:* the input rate-limit; output*:* the output rate-limit.

Note

This function is not supported. Because it is necessary to associate the class map with acl, all restrictions of the acl configuration are applicable for the qos configuration. For the details, see the *ACL Configuration*.

57.2.9 Configuring the Output Queue Scheduling Algorithm

You may schedule the algorithms for the output queue of a port: WRR, SP, RR and DRR. By default, the output queue algorithm is WRR (Weighted Round-Robin).

You may set the port priority queue scheduling method through the following steps. For details of the algorithm, see the overview of QoS.

Command	Description
configure terminal	Enter the configuration mode
mls qos scheduler {**sp** | **rr** | **wrr** | **drr**}	Set the port priority queue scheduling method, where **sp** is absolute priority scheduling, **rr** is round-robin, **wrr** is weighted round-robin with frame quantity, and **drr** weighted round-robin with frame length
no mls qos scheduler	Restore the default **wrr** scheduling

For example, the following steps set the port output algorithm to SP:

```
DES-7210# configure terminal
DES-7210(config)# mls qos scheduler sp
DES-7210(config)# end
DES-7210# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
DES-7210#
```

57.2.10 Configuring Output Round-Robin Weight

You may set the output round-robin weight through the following steps:

Command	Description
configure terminal	Enter the configuration mode
{**wrr-queue** | **drr-queue**} **bandwidth** *weight1...weightn*	weight1...weightn are the weight values specified for the output queues. For the count and value range, see the default QoS settings
no {**wrr-queue** | **drr-queue**} **bandwidth**	The no option restores the default weight value.

The following table lists the mapping relationship of the DES-7200 series v1.x linecard port drr output round-robin weight and bytes:

drr	0	1	2	3	4	5	6	7
bytes	0k	10k	20k	40k	80k	160k	320k	640k

drr	8	9	10	11	12	13	14	15
bytes	1280k	2560k	5120k	10M	20M	40M	80M	160M

Note

The following table lists the mapping relationship of the DES-7200 series v2.x linecard port drr output round-robin weight and bytes:

drr	0	1	2	3	4	5	6	7
bytes	0k	10k	20k	40k	80k	160k	320k	640k

drr	8	9	10	11	12	13	14	15
bytes	16k	18k	20k	22k	24k	26k	28k	30k

The example below sets the wrr scheduling weight as 1:2:3:4:5:6:7:8

```
DES-7210# configure terminal
DES-7210(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
DES-7210(config)# end
DES-7210# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
DES-7210(config)#
```

57.2.11 Configuring Cos-Map

You may set cos-map to change which queue to select for the messages in output. The default value of cos-map is provided in the default QoS configuration section.

Command	Description
configure terminal	Enter the configuration mode
priority-queue Cos-Map qid cos0 [**cos1** [**cos2** [**cos3** [**cos4** [**cos5** [**cos6** [**cos7**]]]]]]]	*qid* is the queue id; *cos0..cos7* are the CoS values associated with that queue.
no priority-queue cos-map	Restore default of cos-map

Below is the example of configuring CoS Map

```
DES-7210# configure terminal
DES-7210(config)# priority-queue Cos-Map 1 2 4 6 7 5
DES-7210(config)# end
DES-7210# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   1
3   4
4   1
5   1
6   1
7   1

wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

57.2.12 Configuring CoS-to-DSCP Map

CoS-to-DSCP Map is used to map the CoS value to internal DSCP value. You may follow these steps to set CoS-to-DSCP Map. The default value of CoS-to-DSCP is provided in the default QoS configuration section.

Command	Description
configure terminal	Enter the configuration mode
mls qos map cos-dscp *dscp1...dscp8* **no mls qos map cos-dscp**	Change the CoS-to-DSCP Map settings, where dscp1...dscp8 are the DSCP values corresponding to CoS values 0 ~ 7. The DSCP value range varies with specific products.

For Example:

```
DES-7210# configure terminal
DES-7210(config)# mls qos map cos-dscp 56 48 46 40 34 32 26 24
```

```
DES-7210(config)# end
DES-7210# show mls qos maps cos-dscp
cos dscp
--- ----
0   56
1   48
2   46
3   40
4   34
5   32
6   26
7   24
```

57.2.13 Configuring DSCP-to-CoS Map

DSCP-to-CoS is used to map internal DSCP value to CoS value so that it is possible to select output queue for messages.

The default value of DSCP-to-CoS Map is provided in the default QoS configuration section. You may follow these steps to set DSCP-to-CoS Map:

Command	Description
configure terminal	Enter the configuration mode
mls qos map dscp-cos *dscp-list* **to** *cos*	Set DSCP to COS Map, where dscp-list is the list of DSCP values to be set, DSCP values delimited by spaces, value range varying with specific products, cos means the CoS values corresponding to the DSCP values, ranging 0~7
no mls qos map dscp-cos	Restore default

For example, the following steps set the DSCP values 0, 32 and 56 to map 6:

```
DES-7210# configure terminal
DES-7210(config)# mls qos map dscp-cos 0 32 56 to 6
DES-7210(config)# show mls qos maps dscp-cos
dscp cos    dscp cos   dscp cos   dscp cos
---- ---    ---- ---   ---- ---   ---- ---
 0   6       1   0      2   0      3   0
 4   0       5   0      6   0      7   0
 8   1       9   1     10   1     11   1
12   1      13   1     14   1     15   1
16   2      17   2     18   2     19   2
20   2      21   2     22   2     23   2
24   3      25   3     26   3     27   3
28   3      29   3     30   3     31   3
32   6      33   4     34   4     35   4
36   4      37   4     38   4     39   4
40   5      41   5     42   5     43   5
44   5      45   5     46   5     47   5
48   6      49   6     50   6     51   6
52   6      53   6     54   6     55   6
56   6      57   7     58   7     59   7
60   7      61   7     62   7     63   7
```

57.2.14 Configuring Port Rate Limiting

You may follow these steps to limit the port rate:

Command	Description
configure terminal	Enter the configuration mode
interface *interface*	Enter the interface configuration mode.
rate-limit output ***bps burst-size***	Port rate limit, where output is the output rate limit, bps is the bandwidth limit per second (kbps), and burst-size is the burst bandwidth limit (Kbyte)
no rate-limit	Cancel port rate limiting

Note

The DES-7200 series does not support input rate limit on a port. Use the **buffer management qos** command in the global configuration mode to enable the global flow-control if the flow is exported from multiple ports with the output rate limit configured to the same port; or the flow congestion will influence the output rate on other ports.

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitEthernet 0/4
DES-7210(config-if)# rate-limit input 100 100
DES-7210(config-if)# end
DES-7210#
```

57.2.15 Configuring IPpre to DSCP Map

IPpre-to-Dscp is used to map the IPpre values of message to internal DSCP values. The default settings of IPpre-to-DSCP Map are provided in the default QoS configuration section. you may follow these steps to configure IPpre-to-Dscp Map:

Command	Description
configure terminal	Enter the configuration mode
mls qos map ip-precedence-dscp *dscp1...dscp8*	Modify the setting of IP-Precedence-to-Dscp Map, where dscp1...dscp8 are the DSCP values corresponding to IP-Precedence values 0~7
no mls qos map ip-prec-dscp	

For Example:

```
DES-7210# configure terminal
DES-7210(config)# mls qos map ip-precedence-dscp 56 48 46 40 34 32 26 24
DES-7210(config)# end
DES-7210# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
0     56
1     48
2     46
3     40
4     34
5     32
6     26
```

```
7     24
```

57.3 Configuring the Switch Buffer

To manage the switch buffer in the state of 802.3x flow-control or QoS, run the following commands:

Command	Description
configure terminal	Enter the configuration mode
buffer management *{fc|qos}*	Configure the buffer management mode. 13 FC: 802.3xflow-control QoS: QoS mode
no buffer management	

For Example:

```
DES-7210# configure terminal
DES-7210(config)#buffer management qos
DES-7210(config)# end
DES-7210# show buffer management
%current port's buffer management mode: qos
```

57.4 QoS Displaying

57.4.1 Showing class-map

You may show the contents of class-map through the following steps:

Command	Description
Show class-map [*class-name*]	Show the contents of the class map entity

For example,

```
DES-7210# show class-map
Class Map cc
Match access-group 1
DES-7210#
```

57.4.2 Showing policy-map

You may show the contents of policy-map through the following steps:

Command	Description
show policy-map [*policy-name* [**class** *class-name*]]	Show QoS policy map, *policy-name* is the selected name of policy map, specified as **class** Show the class map bound with the policy map in case of *class-name*

For example,

```
DES-7210# show policy-map
Policy Map pp
```

```
Class cc
DES-7210#
```

57.4.3 Showing mls qos interface

You may show the QoS information of all ports through the following steps:

Command	Description
show mls qos interface [*interface*| *policers*]	Show the QoS information of the interface, The **Policers** option shows the policy map applied on the interface.

For example,

```
DES-7210# show mls qos interface gigabitEthernet 0/4
Interface GigabitEthernet 0/4
Attached input  policy-map: pp
Default COS: trust dscp
Default COS: 6
DES-7210#show mls qos interface policers
Interface: GigabitEthernet 0/4
Attached input  policy-map: pp
DES-7210#
```

57.4.4 Showing mls qos virtual-group

You may show the QoS information on all interfaces through the following steps:

Command	Description
show mls qos virtual-group [*virtual-group-number* | **policers**]	Show the police information associated with the logic interface group. The **Policers** option displays the police associated with the logic interface group.

For example:

```
DES-7210# show mls qos virtual-group 1
Virtual-group: 1
Attached input  policy-map: pp
DES-7210# show mls qos virtual-group policers
Virtual-group: 1
Attached input  policy-map: pp
DES-7210#
```

57.4.5 Showing mls qos queueing

You may show the QoS queue information through the following steps:

Command	Description
Show mls qos queueing	Show the QoS queue information, CoS-to-queue map, wrr weight and drr weight;

For example:

```
DES-7210# show mls qos queueing
```

```
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   1
3   4
4   1
5   1
6   1
7   1
wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

57.4.6 Showing mls qos scheduler

You may show the QoS scheduling method through the following steps:

Command	Description
Show mls qos scheduler	Show the port priority queue scheduling method.

For example:

```
DES-7210# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
DES-7210#
```

57.4.7 Showing mls qos maps

You may show the MLS QoS maps table through the following steps:

Command	Description
show mls qos maps [**cos-dscp** | **dscp-cos** | **ip-prec-dscp**]	Show MLS QoS map.

For example:

```
DES-7210# show mls qos maps cos-dscp
cos dscp
--- ----
0   0
1   8
2   16
3   24
```

```
4   32
5   40
6   48
7   56
DES-7210# show mls qos maps dscp-cos
dscp cos    dscp cos    dscp cos    dscp cos
---- ---    ---- ---    ---- ---    ---- ---
 0   6       1   0       2   0       3   0
 4   0       5   0       6   0       7   0
 8   1       9   1      10   1      11   1
12   1      13   1      14   1      15   1
16   2      17   2      18   2      19   2
20   2      21   2      22   2      23   2
24   3      25   3      26   3      27   3
28   3      29   3      30   3      31   3
32   6      33   4      34   4      35   4
36   4      37   4      38   4      39   4
40   5      41   5      42   5      43   5
44   5      45   5      46   5      47   5
48   6      49   6      50   6      51   6
52   6      53   6      54   6      55   6
56   6      57   7      58   7      59   7
60   7      61   7      62   7      63   7
DES-7210# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
0     56
1     48
2     46
3     40
4     34
5     32
6     26
7     24
```

57.4.8 Showing mls qos rate-limit

You may show the port rate limiting information through the following steps:

Command	Description
show mls qos rate-limit [**interface** *interface*]	Show the rate limit of [port]

```
DES-7210# show mls qos rate-limit
Interface GigabitEthernet 0/4
rate limit input bps = 100 burst = 100
```

57.4.9 Showing show policy-map interface

You can show the configuration of port policy map by performing following steps

Command	Function
show policy-map interface *interface*	Showing the configuration of (port) policy map

```
DES-7210#show policy-map interface f0/1
FastEthernet 0/1  input (tc policy): pp
    Class cc
      set ip dscp 22
      mark count 0
```

Note The device currently does not support the statistic of mark count.

57.4.10 Showing the buffer management mode

You can show the buffer management mode by performing following steps

Command	Function
show buffer management	Showing the configuration of buffer management mode.

```
DES-7210#show buffer management
%current port's buffer management mode: qos
```

57.4.11 Showing virtual-group

You can show the virtual-group configuration by performing following steps

Command	Function
show virtual-group [*virtual-group-number* | **summary**]	Showing the logic interface group information.

```
DES-7210#show virtual-group 1
 virtual-group       member
  -------------       -------------------------
  1                   Gi0/2 Gi0/3 Gi0/4 Gi0/5
                      Gi0/6 Gi0/7 Gi0/8 Gi0/9 Gi0/10
DES-7210#show virtual-group summary
  virtual-group       member
  -------------       -------------------------
  1                   Gi0/1 Gi0/2 Gi0/3 Gi0/4
                      Gi0/5 Gi0/6 Gi0/7 Gi0/8 Gi0/9
  2                   Gi0/11 Gi0/12 Gi0/13 Gi0/14
                      Gi0/15 Gi0/16 Gi0/17 Gi0/18 Gi0/19
```

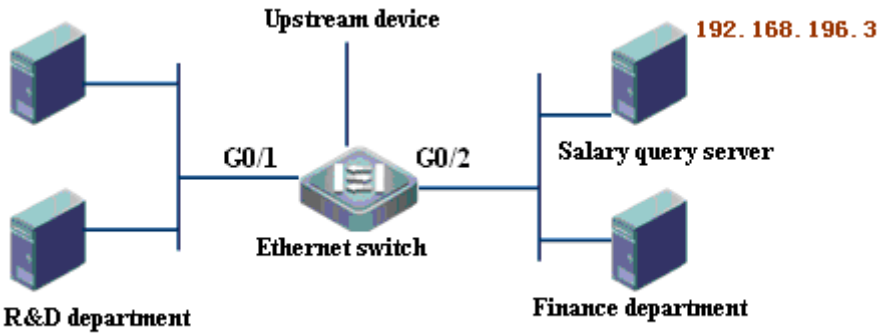
57.5 QoS Configuration Examples

57.5.1 Classified Packets-based Rate Limit

57.5.2 Configuration Requirements

Various departments are interconnected through Ethernet switches in the Intranet, where the finance department is connected through G0/2. For some reason, it is required to limit the maximum outgoing traffic from the salary query server to no more than 512Kbps. The ones exceeding the limit will be dropped.

57.5.3 Topology View



57.5.4 Configuration Procedure

Note

Below shows only the configuration commands associated with QoS ACL.

Enter the global configuration mode.

```
DES-7210# configure
Enter configuration commands, one per line. End with CNTL?Z
```

Define a standard ACL named salary_acl.

```
DES-7210(config)# ip access-list standard salary_acl
```

Define a rule to permit the traffic from the salary server.

```
DES-7210(config-std-nacl)# permit host 192.168.217.223
```

Exit to the global configuration mode.

```
DES-7210(config-std-nacl)# exit
```

Create a class map named salaryclass and enter the class-map configuration mode.

```
DES-7210(config)# class-map salaryclass
```

Define a match rule.

```
DES-7210(config-cmap)# match access-group salary acl
```

Exit to the global configuration mode.

```
DES-7210(config-std-nacl)# exit
```

Create a policy named salarypolicy and enter the policy-map configuration mode.

```
DES-7210(config)# policy-map salarypolicy
```

Set the policy to classify traffic based on salaryclass.

```
DES-7210(config-pmap)# class salaryclass
```

Limit the maximum outgoing traffic from the salary query server to 512Kbps and the burst traffic to 32Kbps, and drop the traffic exceeding this limit.

```
DES-7210(config-pmap-c)# police 512 32 exceed-action drop
```

Exit to the class-map configuration mode.

```
DES-7210(config-pmap-c)# exit
```

Exit to the global configuration mode.

```
DES-7210(config-pmap)# exit
```

Enter the G0/2 interface configuration mode.

```
DES-7210(config)# interface gigabitEthernet 0/2
```

Apply salarypolicy to the inbounding direction of the G0/2 interface.

```
DES-7210(config-if)# service-policy input salarypolicy
```

Exit to the privileged EXEC mode.

```
DES-7210(config-if)# end
```

Show the configuration.

```
DES-7210# show mls qos interface policers
Interface: GigabitEthernet 0/2
Attached input  policy-map: salarypolicy
DES-7210#show policy-map salarypolicy
 Policy Map salarypolicy
    Class salaryclass
      police 512 32 exceed-action drop
DES-7210#show class-map salaryclass
 Class Map salaryclass
   Match access-group salary_acl
DES-7210#show access-lists salary_acl
ip access-list standard salary_acl
 10 permit host 192.168.217.223
```

58 VRRP Configuration

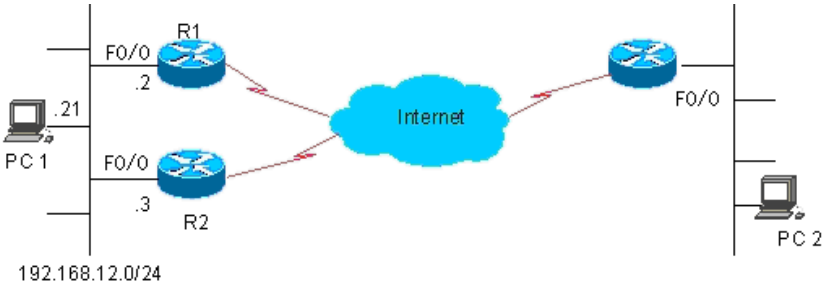
58.1 Overview

The Virtual Router Redundancy Protocol (VRRP) is designed to work in the active/standby mode to ensure that the standby router can take over the work without affecting internal and external data communication and modifying the parameters of internal networks when the master router fails. Multiple devices within a VRRP group are mapped to a virtual device. The VRRP ensures one and only one device to send packets on behalf of the virtual device at one time, while the host sends messages to that virtual device. The device that forwards packets is elected as the master device. If that device cannot work due to some reason, the one in standby status will be selected to replace it and become the active device. With VRRP, the hosts in the LAN seem to use only one router. The route connectivity is also guaranteed even when the currently-used first-hop router fails.

RFC 2338 defines the IP packet format in VRRP type and its working mechanism. The VRRP message means a kind of multicast message with specified destination address, which is sent by the master router by schedule to indicate its operation and are also used to elect the master router. The VRRP allows another router to automatically take over the operations when the router that undertaking route forwarding function in the IP LAN fails, thus implementing the hot-backup and error-tolerance of IP routing and ensuring the continuity and reliability of host communication in the LAN. Redundancy is implemented for a VRRP application group through multiple devices, but only one device acts as the master device at any time to undertake the route forwarding function. The others are in the backup roles. Inter-router switching in the VRRP application group is fully transparent for the host in the LAN. The RFC 2338 defines the router switching rules:

- The VRRP protocol adopts the preemption method to select the master router. First, it compares the VRRP priorities that are set for the interfaces of the routers a VRRP group. The one with the highest priority becomes the master router and its status will become Master. If the priority of the routers is identical, compare the master IP addresses of the network interfaces, the one with larger IP address will become the master router to forward packets.
- After the master device is elected, the others are in the standby status and monitor the status of the master device through the VRRP message sent by the master device. In normal operation, the master router sends a VRRP message at an interval, called advertised message, to notify the standby devices. The master device is in the normal working status. If the standby device within the group doesn't receive the message from the master device for a long time, it becomes the master. If more than one device within the group become master, repeat the preempt process in step 1.In this process, the device with the maximum priority will be selected as the master router to execute the VRRP backup function.

Figure-1: VRRP working principles



Once a master device is elected in a VRRP backup group, the hosts in the LAN will execute route forwarding through that master device. The communication process is illustrated in Figure-1.

As you can see, R1 and R2 are connected with LAN 192.168.12.0/24 through the VRRP-enabled Ethernet interface Fa0/0. All hosts in the LAN use the IP address of the virtual router of the VRRP group as the default gateway. The hosts in the LAN only know the virtual router of the VRRP group, while the master router in the VRRP which is implementing the forwarding function is transparent to them. For example, if host PC 1 in the LAN is communicating with host PC 2 in another network, PC 1 will use the virtual router as the default gateway to send packets to PC 2. After receiving the packets, the master router in the VRRP group forwards them to PC 2. In this communication process, PC 1 only feels the virtual device but does not know whether R1 or R2 works. The master router is elected between R1 and R2 in the VRRP group. Once the master router fails, the other router automatically becomes the master.

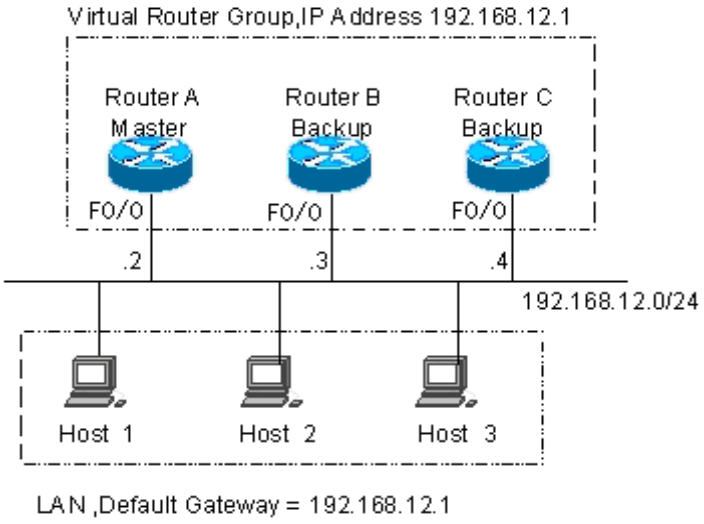
58.2 VRRP Applications

There are two VRRP application modes: basic and advanced. In basic applications, simple redundancy is implemented with a single backup group, while in advanced applications multiple backup groups are used to implement both route redundancy and load balancing.

58.2.1 Route Redundancy

The basic VRRP applications are illustrated in Figure-2.

Figure-2: Basic VRRP applications

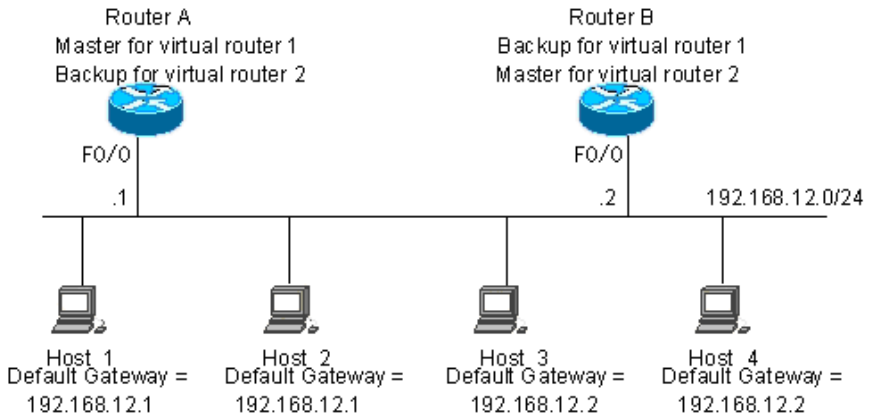


As shown in Figure-2, routers A, B and C are connected with the LAN through an VRRP-enabled Ethernet interface. They are in the same VRRP group with virtual IP address 192.168.12.1. Router A is elected as the master router of the VRRP, and routers B and C are standby routers. Hosts 1, 2 and 3 in the LAN use the IP address of the virtual router 192.168.12.1 as the gateway. The packets from the hosts in the LAN to other networks will be forwarded by the master router (router A in Figure-2). Once router A fails, the master router preempted between routers B and C undertakes the route forwarding function of the virtual device, resulting in a simply route redundancy.

58.2.2 Load Balancing

The advanced VRRP applications are illustrated in Figure-3.

Figure-3: Advanced VRRP applications



As shown in Figure-3, two virtual devices are set. For virtual router 1, router A uses the IP address of Ethernet interface Fa0/0 192.168.12.1 as the IP address of the virtual router, and thus router A becomes the master router and router B becomes the backup. For virtual router 2, router B uses the IP address of Ethernet interface Fa0/0 192.168.12.2 as the IP address of the virtual router, and thus router B becomes the master router and router A becomes the backup. In the LAN, hosts 1 and 2 use the IP address of virtual router 1 192.168.12.1 as the default gateway, while hosts 3 and 4 use the IP address of virtual router 2 192.168.12.2 as the default gateway. In this VRRP application, router A and router B provide the route redundancy to share the traffic from the LAN, that is, load balancing.

58.3 VRRP Configuration

58.3.1 VRRP Configuration Task List

The VRRP is applicable for the multicast or broadcast LANs, such as Ethernet. The configuration of the VRRP is concentrated on the Ethernet interfaces. The configuration tasks are as follows:

- Enable VRRP backup function (mandatory)
- Set the authentication string of the VRRP backup group (optional)
- Set the advertisement interval of the VRRP backup group (optional)
- Set the preemption mode of the router in the VRRP backup group (optional)
- Set the priority of the router in the VRRP backup group (optional)
- Set the interface to be monitored by the VRRP backup group (optional)
- Set the IP address to be monitored by the VRRP backup group (optional)
- Set the learning function of the VRRP advertisement timer device(optional)
- Set the description string of the router in the VRRP backup group (optional)
- Set the delay reload of the VRRP backup group(optional)

Not all of the tasks are required here. Tasks that are required for a VRRP backup group depend on user requirements.

58.3.2 Enabling VRRP Backup Function

By specifying the backup group number and virtual IP address, you may add a backup in the specified LAN network segment to enable the VRRP backup function of the related Ethernet interfaces.

Command	Purpose
DES-7210(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable VRRP.
DES-7210(config-if)# **no vrrp** *group* **ip** *ipaddress* [**secondary**]	Disable VRRP.

The backup group number is in the range of 1 to 255. If the virtual IP address *ipaddress* is not specified, the router will not participate in the VRRP backup group. If the **secondary** parameter is not used, the IP address set here will become the master IP address of the virtual router.

Note

If the virtual IP address (Primary or Secondary) of the VRRP group is the same as the IP address (Primary or Secondary) of the Ethernet interface, it is considered that the VRRP group occupies the actual IP address of the Ethernet interface, and the priority of the VRRP group is 255. If the corresponding Ethernet interface is available, the VRRP group will become the Master status automatically.

For NMX-2GEH line card, each interface supports up to 14 VRRP backup groups. It will prompt the error if the number of VRRP group exceeds 14.

58.3.3 Setting the Authentication String for the VRRP Backup Group

The VRRP supports plaintext password authentication mode and no authentication mode. When the authentication string is set for the VRRP backup group, it is also required to set the VRRP group to be in the plaintext password authentication mode. The members in the VRRP group must be in the same authentication mode for normal communication. In the plaintext authentication mode, the routers in the same VRRP group must have the same authentication password configured. The plaintext authentication password cannot provide security. It aims only to prevent/prompt the incorrect VRRP configuration.

Command	Purpose
DES-7210(config-if)# **vrrp** *group* **authentication** *string*	Set the authentication string of the VRRP.
DES-7210(config-if)# **no vrrp** *group* **authentication**	Set no authentication for VRRP.

By default, the VRRP is in the no authentication mode. For the plaintext password authentication mode, the length of the plaintext authentication mode cannot be greater than 8 bytes.

58.3.4 Setting the Advertisement Interval of the VRRP Backup Group

Command	Purpose
DES-7210(config-if)# **vrrp** *group* **timers advertise** *interval*	Set the master device VRRP advertisement interval.
DES-7210(config-if)# **no vrrp** *group* **timers advertise** [*interval*]	Restore the VRRP advertisement interval of the master device to the default value.

If the current device becomes the master in the VRRP group, it will notify its VRRP status, priority and more information by sending VRRP advertisements at the specified interval. By default, this interval is 1 second.

Note

When the VRRP timer learning function is not configured, the routers in a VRRP group should be configured with the same VRRP advertisement interval; otherwise, the routers in the standby status will drop the received VRRP advertisement

58.3.5 Setting the Preemption Mode of the Router in the VRRP Backup Group

If the VRRP group is working in the preemption mode, once it finds its priority is higher than the Master priority, it will preempt to become the master of the VRRP group. If the VRRP group is not working in the preemption mode, even if a device finds its priority is higher than the Master priority, it will not preempt to become the master of the VRRP group. In case the VRRP group is using the Ethernet interface IP address, the setting of the preemption mode does not make sense, because this VRRP group has the highest priority and thus it automatically become the master in the VRRP group.

Command	Purpose
DES-7210(config-if)# **vrrp** *group* **preempt** [**delay** *seconds*]	Set VRRP backup group to work in the preemption mode
DES-7210(config-if)# **no vrrp** *group* **preempt** [**delay**]	Set VRRP backup group to work in the preemption mode

The optional parameter **delay seconds** defines the delay for the VRRP router prepares to declare its Master identify, 0 seconds by default. Once the VRRP function is enabled, the VRRP group will work in the preemption mode by default.

58.3.6 Setting the Priority of the Router in the VRRP Backup Group

The VRRP protocol provides that the priority parameter of the device determines its position in the backup group. The device that has the highest priority in the preempt mode and has the virtual IP address becomes the active (or master) device in the backup group. Other devices of lower priority in the same group become the backup (or monitoring) devices. Once the VRRP function is enabled, the VRRP group has 100 as its default priority.

Command	Purpose
DES-7210(config-if)# **vrrp** *group* **priority** *level*	Set the priority of the VRRP backup group.
DES-7210(config-if)# **no vrrp** *group* **priority**	Restore the default of the VRRP priority

The priority level range is 1~254. If the VRRP virtual IP address is the same as the actual IP of the Ethernet interface, the priority of the corresponding VRRP group is 255. Now no matter whether the VRRP group in the preemption mode, the corresponding VRRP group will be in the Master status automatically (as long as the corresponding Ethernet interface is available).

58.3.7 Setting the Interface to be Monitored by the VRRP Backup Group

After the interface to be monitored by the VRRP backup group is configured, the system will dynamically adjust the priority of the router according to the monitored interface. Once the status of the monitored interface becomes unavailable, the priority of the router in the VRRP backup group will be decreased according to the preset value. At the same time, another router in the backup group which has a more stable interface status or higher priority will become the active (master) router of the VRRP backup group.

Command	Purpose
DES-7210(config-if)# **vrrp** group **track** *interface-type number* *[interface –priority]*	Set the interface to be monitored by the VRRP backup group
DES-7210(config-if)# **no vrrp** *group* **track** *interface-type number*	Cancel setting of the interface to be monitored by the VRRP backup group

By default, there is no interface configured to be monitored by the VRRP backup group. The parameter *interface –priority* ranges 1~255. If the parameter *interface –priority* is default, the system will use the default value 10.

Note

The monitored interface only is layer-3 routable logical interfaces (such as Routed Port, SVI, Loopback and Tunnel).

58.3.8 Setting the IP address to be Monitored by the VRRP Backup Group

After the IP address to be monitored by the VRRP backup group is configured, the system will dynamically adjust the priority of the router according to the monitored address. Once the status of the monitored IP address becomes unreachable or it is unable to ping the monitored IP address, the priority of the router in the VRRP backup group will be decreased according to the preset value. At the time, another router in the same backup group which has a higher priority will become the active (master) router of the VRRP backup group. The optional parameter *interval-value* shows the interval time of probing whether the destination address is reachable or not. The Optional parameter *timeout-value* shows the timeout time of pinging the destination address.

Command	Purpose
DES-7210(config-if)# **vrrp** *group* **track** *ip-address* [[[**interval** *interval-value*] **timeout** *timeout-value*] *priority*]	Set the IP address to be monitored by the VRRP backup group
DES-7210(config-if)# **no vrrp** *group* **track** *ip-address*	Cancel setting of the IP address to be monitored by the VRRP backup group

By default, there is no IP address configured to be monitored by the VRRP backup group. The parameter *interval–value* ranges 1~3600s. If the parameter *interval–value* is default, the system will use the default value 3s. The parameter *timeout–value* ranges 1~60s. If the parameter *timeout–value* is default, the system will use the default value 1s. Note that the timeout-value must be less than or equal to interval-value. The parameter *priority* ranges 1~255. If the parameter *priority* is default, the system will use the default value 10.

58.3.9 Setting the Learning Function of VRRP Advertisement Timer Device

Once the timer learning function is enabled, if the current router is VRRP backup router, after setting the timer learning function, the router will learn VRRP advertisement sending interval from VRRP advertisement of the master router and calculate the failure judgment interval of master router. It does not calculate by VRRP advertisement sending interval set locally. Use this command to synchronize the VRRP advertisement timer between the backup router and master router.

Command	ınction
DES-7210(config-if)# **vrrp** *group* **timers learn**	Set the timer learning function.
DES-7210(config-if)# **no vrrp** *group* **timers learn**	Delete the timer learning function.

By default, the VRRP group timer learning function is not set.


Note

In case the advertisement sending interval in VRRP advertisement received by VRRP backup router is inconsistent with the advertisement interval set locally, if the timer learning function is not configured on the VRRP backup router, the VRRP backup router will drop the VRRP advertisement; otherwise, it will receive the VRRP advertisement and calculate failure judgment interval of VRRP Master router by the advertisement interval.

58.3.10 Setting the Description String of the Router in the VRRP Backup Group

This command will set the descriptor for the VRRP group to facilitate identifying the VRRP group.

Command	Purpose
DES-7210(config-if)# **vrrp** *group* **description** *text*	Set the description string of the VRRP group.
DES-7210(config-if)# **no vrrp** *group* **description**	Cancel the description string of the VRRP group.

By default, the VRRP backup group has no description string configured. The length of the VRRP backup group description string is 80 by maximum.


Note

If blanks are contained in the description string of the VRRP backup group, quotation marks (") must be used to identify the description string.

58.3.11 Setting the Delay Reload of the VRRP Backup Group

This command will set the delay reload time of the VRRP backup group on an interface. The delay reload time has two types: the one when the system reloads and the one when the interface becomes active. You can set those two types of delay reload time separately or simultaneously.

In the non-preemption mode, when the VRRP backup group with higher priority reloads, it can not preempt the master router in the same backup group. However, even though the non-preemption mode is configured, the reloading VRRP backup group can also preempt the VRRP master router. That is because when the router reloads or the interface becomes active, the VRRP backup group on the interface fails to receive the VRRP packets sent from the master router in the same backup group in time.

At this time, you can enable the VRRP backup group to delay reload using the following command. After configuring this command, when the system reloads or the interface becomes active, the VRRP backup group on the interface can not reload immediately, but reload after the preset delay time, and the non-preemption configuration is still effective.

If the VRRP packets are received on the interface when the delay reload of VRRP backup group is configured, the delay reload configuration will be cancelled and the VRRP will be enabled immediately.

Command	Purpose
DES-7210(config-if)# **vrrp delay** { [**minimum** *min-seconds*] [**reload** *reload-seconds*] }	Set the delay reload of the VRRP group on the interface.
DES-7210(config-if)# **no vrrp delay**	Cancel the delay reload of the VRRP group.

By default, the VRRP backup group has no delay reload of VRRP backup group configured. The two types of the delay reload of the VRRP backup group ranges 0-60s.

58.4 Monitoring and Maintaining VRRP

Our products provide the **show vrrp** and **debug vrrp** commands to monitor and maintain VRRP. The **show vrrp** command is used to check the VRRP status of a local router; the **debug vrrp** command is used to check the information on the VRRP group status, received/sent VRRP advertisement and VRRP events.

58.4.1 show vrrp

Our product provides the following **show vrrp** commands to check the VRRP status of the local router.

Command	Purpose
DES-7210# **show vrrp** [**brief** | *group*]	Check the current VRRP status
DES-7210# **show vrrp interface** *type number* [**brief**]	Show the VRRP status of the specified network interface

Here are some examples of the command:

1. **show vrrp** command

```
DES-7210# show vrrp
GigabitEthernetFastEthernet 0/10 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
GigabitEthernetFastEthernet 0/20 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
```

The displayed messages above include the Ethernet name, VRRP backup group number configured on the interface, status, priority, preemption mode, VRRP advertisement interval, virtual IP address, virtual MAC address, Master router IP address, Master router priority, Master router advertisement interval, Master router failure judgment interval, current interface monitored by the VRRP backup group and corresponding priority change scale.

The current interface monitored by the VRRP backup group and the corresponding priority change metrics can be shown only after the monitoring interface function is enabled.

2. **show vrrp brief** command

```
DES-7210# show vrrp brief
Interface      Grp Pri Time Own Pre State   Master addr     Group addr
GigabitEthernet0FastEthernet0/0 1  100  3-   -   P  Backup 192.168.201.213
192.168.201.1
GigabitEthernet0FastEthernet0/0 2  120  -    -   P  Master  192.168.201.217
192.168.201.2
```

The information displayed above includes the Ethernet interface name, VRRP group number, priority, timeout period for backup turning into master, same as the interface IP address or not, preemption mode, master device IP address, and VRRP group IP address.

3. **show vrrp interface** command

```
DES-7210# show vrrp interface FastEthernet 0/1
GigabitEthernetFastEthernet 0/1 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 0/1 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
DES-7210#
```

The displayed messages above include the specified Ethernet name, VRRP backup group number configured on the interface, status, priority, preemption mode, VRRP advertisement interval, virtual IP address, virtual MAC address, Master router IP address, Master router priority, Master router advertisement interval, Master router failure judgment interval, current interface monitored by the VRRP backup group and corresponding priority change scale.

58.4.2 debug vrrp

Our produce has the following **debug vrrp** commands to provide the VRRP status debugging information of the local router.

Command	Purpose
DES-7210# **debug vrrp errors**	Turn on the VRRP error prompt debug switch

Command	Purpose
DES-7210# **no debug vrrp errors**	Turn off the VRRP error prompt debug switch
DES-7210# **debug vrrp events**	Turn on the VRRP event debug switch
DES-7210# **no debug vrrp events**	Turn off the VRRP event debug switch
DES-7210# **debug vrrp packets**	Turn on the VRRP packet Debug switch
DES-7210# **no debug vrrp packets**	Turn off the VRRP packet debug switch
DES-7210# **debug vrrp state**	Turn on the VRRP state debug switch
DES-7210# **no debug vrrp state**	Turn off the VRRP status debug switch
DES-7210# **debug vrrp**	Turn on the VRRP debug switch
DES-7210# **no debug vrrp**	Turn off the VRRP debug switch

Here are some examples of the command:

1. **debug vrrp** command

```
DES-7210# debug vrrp
DES-7210#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Event - Advert higher or equal priority
%VRRP-6-STATECHANGE: GigabitEthernetFastEthernet 0/0 Grp 1 state Master -> Backup
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address 192.168.1.1
%VRRP-6-STATECHANGE: GigabitEthernetFastEthernet 0/0 Grp 1 state Backup -> Master
DES-7210#
```

The **debug vrrp** command is equivalent to the joint execution of debug vrrp errors, debug vrrp events, `debug vrrp packets` and `debug vrrp state`.

2. **debug vrrp errors** command

```
DES-7210# debug vrrp errors
DES-7210#
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address 192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address 192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address 192.168.1.1
```

The above displayed information indicates the VRRP advertisement comes from 192.168.201.213 for VRRP group 1. The virtual IP address 192.168.1.1 in the advertisement is not in local VRRP group 1.

3. **debug vrrp events** command

```
DES-7210# debug vrrp events
DES-7210#
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
DES-7210#
```

The above displayed information indicates the priority in the VRRP advertisement received by the local VRRP group is not lower than the local priority.

4. **debug vrrp packets** command

```
DES-7210#debug vrrp packets
DES-7210#
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
```

The above displayed information indicates the local VRRP group 2 is sending VRRP advertisement, whose VRRP checksum is 0XDD4D.

```
DES-7210# debug vrrp packets
DES-7210#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
```

The above displayed information indicates the VRRP advertisement is received from 192.168.201.213 for VRRP group 1, whose priority is 120.

5. **debug vrrp state** command

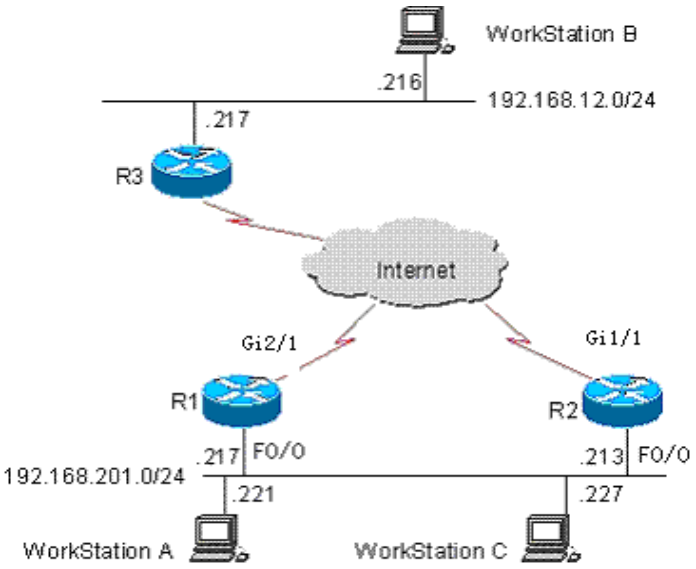
```
DES-7210# debug vrrp state
VRRP State debugging is on
DES-7210#
%VRRP-6-STATECHANGE: GigabitEthernetFastEthernet 0/0 Grp 2 state Master -> Backup
%VRRP-6-STATECHANGE: GigabitEthernetFastEthernet 0/0 Grp 2 state Backup -> Master
DES-7210# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# interface GigabitEthernetfastethernet 0/0
DES-7210(config-if)# no shutdown
DES-7210(config-if)# end
DES-7210#
%VRRP-6-STATECHANGE: GigabitEthernetFastEthernet 0/0 Grp 2 state Master -> Init
DES-7210#
```

The above displayed information indicates the VRRP group status on GigabitEthernet 0/0 is shifting among Master, Backup and Init.

58.5 Example of Typical VRRP Configuration

As shown in Figure-4, the VRRP backup group is configured on R1 and R2 to provide VRRP services for 192.168.201.0 /24. R3 is not configured with VRRP but just common routing functions. The following shows the VRRP configuration of R1 and R2.

Figure-4: Network connection with VRRP



In the configuration example below, the configurations of device R3 remain unchanged, The configuration on device R3 is shown below:

```
DES-7210# configure terminal
DES-7210(config)# !
!
hostname "R3"
!
!
!
interface gigabitEthernetFastEthernet 0/0
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.168.12.217 255.255.255.0
DES-7210(config-if)# exit
DES-7210(config)# !
interface GigabitEthernet 1/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 60.154.101.5 255.255.255.0
DES-7210(config-if)# exit!
DES-7210(config)# interface GigabitEthernet 2/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 202.101.90.61 255.255.255.0
DES-7210(config-if)# exit!
DES-7210(config)# router ospf 1
DES-7210(config-router)# network 202.101.90.0 0.0.0.255 area 10
DES-7210(config-router)# network 192.168.12.0 0.0.0.255 area 10
DES-7210(config-router)# network 60.154.101.0 0.0.0.255 area 10
DES-7210(config-router)# !
!
!
end
```

58.5.1 Example of Single VRRP Backup Group Configuration

Establish the connections according to Figure-4. In this configuration example, user workstation group (192.168.201.0/24) uses the backup group that is composed of routers R1 and R2, and points its gateway to the virtual router IP address 192.168.201.1 of the backup group. The remote user workstation group (in network 192.168.12.0 /24) is accessed via the virtual router 192.168.201.1. Here router R1 is set as the VRRP Master device. In normal cases, device R1 is the active router to function as the gateway (192.168.201.). When device R1 becomes unreachable due to power-off or failure, device R2 takes its place to function as the gateway (192.168.201.1). The configurations for devices R1 and R2 are described as follows.

Configurations on device R1:

```
DES-7210# configure terminal
!
!
hostname "R1"
!
!
interface gigabitEthernetFastEthernet 0/0
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.168.201.217 255.255.255.0
DES-7210(config-if)# vrrp 1 priority 120
DES-7210(config-if)# vrrp 1 timers advertise 3
DES-7210(config-if)# vrrp 1 ip 192.168.201.1
DES-7210(config-if)# exit!
DES-7210(config)# interface GigabitEthernet 2/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 202.101.90.63 255.255.255.0
DES-7210(config-if)# exit !
DES-7210(config)# router ospf 1
DES-7210(config-router)# network 202.101.90.0 0.0.0.255 area 10
DES-7210(config-router)# network 192.168.201.0 0.0.0.255 area 10
```

Configurations on device R2:

```
DES-7210# configure terminal
DES-7210(config)# !
```

Configurations on router device R2:

```
!
hostname "R2"
!
interface GigabitEthernetFastEthernet 0/0
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.168.201.213 255.255.255.0
DES-7210(config-if)# vrrp 1 ip 192.168.201.1
DES-7210(config-if)# vrrp 1 timers advertise 3
DES-7210(config-if)# exit
DES-7210(config)# !
interface GigabitEthernet 1/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 60.154.101.3 255.255.255.0
DES-7210(config-if)# exit!
```

```
DES-7210(config)# !
router ospf 1
DES-7210(config-router)# network 60.154.101.0 0.0.0.255 area 10
DES-7210(config-router)# network 192.168.201.0 0.0.0.255 area 10
DES-7210(config-router)# !
!
end
```

As shown above, routers R1 and R2 are in the same VRRP backup group 1, point to the same virtual router IP address (192.168.201.1) and are both in the VRRP preemption mode. Since the VRRP backup group priority of device R1 is 120 but that of R2 is the default value 100, device R1 acts as the VRRP Master in normal cases.

58.5.2 Example of configuration to monitor interface with VRRP

Establish the connections according to Figure 47-4. In this configuration example, user workstation group (192.168.201.0/24) uses the backup group that is composed of routers R1 and R2, and points its gateway to the virtual router IP address 192.168.201.1 of the backup group. The remote user workstation group (in network 192.168.12.0 /24) is accessed via the virtual router 192.168.201.1. Here router R1 is set as the VRRP Master device. Different from the above configuration example, router R1 is configured with VRRP to monitor interface GigabitEthernet 2/1. In normal cases, device R1 is the active device to function as the gateway (192.168.201.1). When device R1 becomes unreachable due to power-off or failure, device R2 takes its place to function as the gateway (which is just the virtual device address 192.168.201.1). Especially, when the WAN interface GigabitEthernet 2/1 of device R1 is unavailable, device R1 will decrease its priority in the VRRP backup group so that device R2 has the chance to become active and function as the virtual gateway (192.168.201.1). If the WAN interface GigabitEthernet 2/1 of device R1 resumes normal, device R1 restores its priority in the VRRP backup group, becomes active and functions as the virtual gateway once again. The configurations for devices R1 and R2 are described as follows.

Configurations on device R1:

```
DES-7210# configure terminal


!
!
hostname "R1"
!
!
interface gigabitEthernetFastEthernet 0/0
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.168.201.217 255.255.255.0
DES-7210(config-if)# vrrp 1 priority 120
DES-7210(config-if)# vrrp 1 timers advertise 3
DES-7210(config-if)# vrrp 1 ip 192.168.201.1
DES-7210(config-if)# vrrp 1 track GigabitEthernet 2/1 30
DES-7210(config-if)# exit
DES-7210(config)# !

interface GigabitEthernet 2/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 202.101.90.63 255.255.255.0
DES-7210(config-if)# exit !
```

```
DES-7210(config)# router ospf 1
DES-7210(config-router)# network 202.101.90.0 0.0.0.255 area 10
DES-7210(config-router)# network 192.168.201.0 0.0.0.255 area 10
DES-7210(config-router)# !
!
end
```

Configurations on device R2:

```
DES-7210# configure terminal
DES-7210(config)# !
!
hostname "R2"
!
interface gigabitEthernetFastEthernet 0/0
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.168.201.213 255.255.255.0
DES-7210(config-if)# vrrp 1 ip 192.168.201.1
DES-7210(config-if)# vrrp 1 timers advertise 3
DES-7210(config-if)# exit
DES-7210(config)# !
interface GigabitEthernet 1/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 60.154.101.3 255.255.255.0
DES-7210(config-if)# exit !
DES-7210(config)# router ospf 1
DES-7210(config-router)# network 60.154.101.0 0.0.0.255 area 10
DES-7210(config-router)# network 192.168.201.0 0.0.0.255 area 10
DES-7210(config-router)# !
!
end
```

As shown above, devices R1 and R2 are in the same VRRP backup group 1, use the same VRRP backup group authentication mode (no authentication), point to the same virtual IP address (192.168.201.1) and are both in the VRRP preemption mode. The VRRP Advertisement interval for devices R1 and R2 are 3 seconds. In normal cases, since the VRRP backup group priority of device R1 is 120 but that of R2 is the default value 100, device R1 acts as the VRRP Master in normal cases. If device R1 in the Master status finds its WAN interface GigabitEthernet 2/1 is unavailable, device R1 decreases its priority in the VRRP backup group from 90 to 30, so that device R2 can become the Master. If router R1 finds its WAN interface GigabitEthernet 2/1 becomes available later, it increases its priority in VRRP backup group from 30 to 120, so that device R1 becomes the master once again.

58.5.3 Example of Multiple VRRP Backup Groups

In addition to the single backup group, the DES-7200 series also allows multiple VRRP backup groups configured on the same Ethernet interface. There are obvious benefits for the use of multiple backup groups. It is possible to implement load balancing yet mutual backup to offer more stable and reliable network services.

Establish the connections according to Figure-4. In this configuration example, user workstation group (192.168.201.0/24) is using the backup group that is composed of routers R1 and R2. Some user workstations (such as A) point its gateway to the virtual IP address 192.168.201.1 of backup group 1, while the others (such as C) point its gateway to the virtual IP address 192.168.201.2 of backup group 2.Device 1 acts as the master in backup group 1 and standby in backup group 1;

device 2 acts as the standby in backup group 2 and master in backup group 1The configurations for devices R1 and R2 are described as follows.

Configurations on device R1:

```
DES-7210# configure terminal


!
!
hostname "R1"
!
interface gigabitEthernetFastEthernet 0/0
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.168.201.217 255.255.255.0
DES-7210(config-if)# vrrp 1 timers advertise 3
DES-7210(config-if)# vrrp 1 ip 192.168.201.1
DES-7210(config-if)# vrrp 2 priority 120
DES-7210(config-if)# vrrp 2 timers advertise 3
DES-7210(config-if)# vrrp 2 ip 192.168.201.2
DES-7210(config-if)# vrrp 2 track GigabitEthernet 2/1 30
DES-7210(config-if)# exit
DES-7210(config)# !
interface GigabitEthernet 2/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 202.101.90.63 255.255.255.0
DES-7210(config-if)# exit !
DES-7210(config-router)# router ospf
DES-7210(config-router)# network 202.101.90.0 0.0.0.255 area 10
DES-7210(config-router)# network 192.168.201.0 0.0.0.255 area 10
DES-7210(config-router)# !
!
end
```

Configurations on device R2:

```
DES-7210# configure terminal


!
!
hostname "R2"
!
!
interface Loopback 0
DES-7210(config-if)# ip address 20.20.20.5 255.255.255.0
DES-7210(config-if)# exit
DES-7210(config)# !
interface GigabitEthernetFastEthernet 0/0
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 192.168.201.213 255.255.255.0
DES-7210(config-if)# vrrp 1 ip 192.168.201.1
DES-7210(config-if)# vrrp 1 timers advertise 3
DES-7210(config-if)# vrrp 1 priority 120
DES-7210(config-if)# vrrp 2 ip 192.168.201.2
```

```
DES-7210(config-if)# vrrp 2 timers advertise 3
DES-7210(config-if)# exit!
DES-7210(config)# interface GigabitEthernet 1/1
DES-7210(config-if)# no switchport
DES-7210(config-if)# ip address 60.154.101.3 255.255.255.0
DES-7210(config-if)# exit!
DES-7210(config)# router ospf
DES-7210(config-router)# network 60.154.101.0 0.0.0.255 area 10
DES-7210(config-router)# network 192.168.201.0 0.0.0.255 area 10
DES-7210(config-router)# !
!
!
```

It is shown that devices R1 and R2 are mutual backup, and the two are acting as the master devices in VRRP backup groups 1 and 2 respectively to provide different virtual gateway functions.

58.6 Diagnosing and Troubleshooting VRRP

You can troubleshoot VRRP failures by viewing configuration and debugging information. Here is analysis of some common faults.

Symptom: Unable to ping the virtual IP address

Analysis:

- Ensure at least one router in the backup group is active.
- If it is possible to ping the virtual IP address from other network devices, the causes may be the VRRP status changing needs some time (although brief). Execute the **show vrrp** command to check the VRRP information and confirm this.
- If the local network device is in the same network segment of the virtual router, check whether ARP table of the local network device contains the APP entry for the IP virtual address. If no, check the network lines.
- If the local network device is not in the same network segment of the virtual router, make sure the local network device has a router to the virtual IP address.

Symptom: multiple master devices in the same VRRP backup group

Analysis:

- In the same VRRP backup group, the Ethernet interfaces of those routers are in different VRRP group authentication modes.
- In the same VRRP backup group, the Ethernet interfaces of those routers are in the plaintext password VRRP group authentication mode, but the authentication strings are not the same.
- In the same VRRP backup group, the cables the Ethernet interfaces of some routers may be disconnected, since the routers fail to detect that.
- In the same VRRP backup group, the VRRP advertisement interval is inconsistent and the timer learning function is not configured.
- In the same VRRP backup group, the virtual IP address for the routers are not the same.

59 RERP Configuration

59.1 RERP Overview

59.1.1 Understanding RERP

For the loop blocking and link recovery in core ring network, currently the OSPF and BGP4 are mostly used for the implementation. For complex network, the link recovery may take tens of seconds. If MSTP is used for loop blocking in the link layer, the STP needs to advertise level by level by the spanning tree, the network convergence may take rather long time in case of complicated network.

The Rapid Ethernet Ring Protection Protocol (RERP) is a special layer-2 link redundancy backup protocol designed for core Ethernet. The loop blocking and link recovery for the RERP are centrally implemented on the master device and the non-master devices directly report their link conditions to the master device without additional processing on the non-master devices; however the STP works with the spanning tree to advertise level by level by the spanning tree and determine the final link status through level-by-level calculations. So, the loop block and recovery with the RERP are faster than those with the STP. Based on the above difference, the link recovery of RERP in ideal environment may be completed in several microseconds.

The RERP involves the following key concepts: Ring, Region, Master, Backup, Transit, Primary Edge Node, Secondary Edge Node, Primary Port, Secondary Port, Shared Port and Control Vlan. They are explained through the following typical applications.

Note

As an alternative of STP in the core ring network, the RERP cannot be turned on at the same time with the STP in the actual configurations. RERP and REUP cannot share one port.

59.1.2 Typical Applications

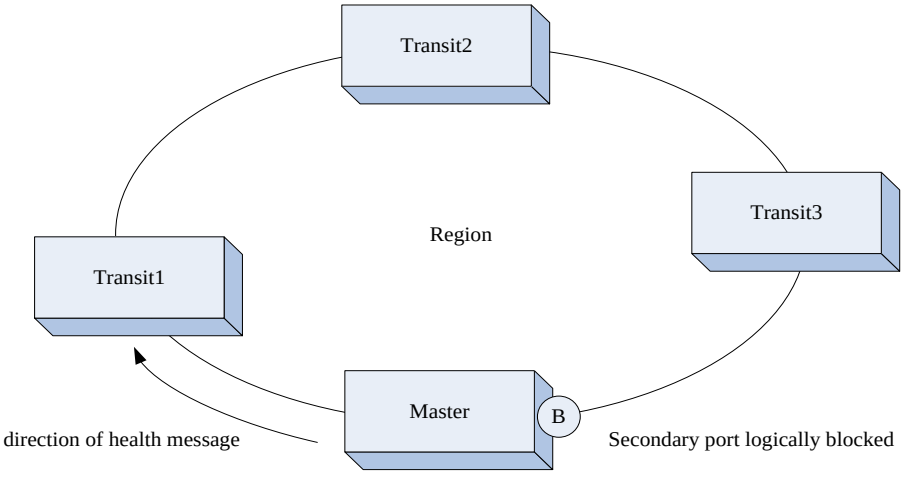


Figure-1

As shown above, the four devices are all core Ethernet devices and form a ring core network. In such a topology, each device has two and only two interface to be connected with the ring. This type of ring is called a RERP region, identified uniquely with an integer. Each RERP region can have only one Master and one Backup specified. The others are all Transit. Each device must be specified with the region and configured with the master/backup port.

Master:

The link is a TRUNK connection. The ring has an independent VLAN as the control VLAN, which is specially used to transmit various control messages defined by the RERP. The other VLANs are the data VLANs and used for the transmission of dataflow.

The two ports of the master connected to the ring are called the primary port and secondary port respectively, whether the primary port sends the Hello message outside on regular basis.

Loop blocking:

In normal cases, the master device prevents the generation of layer-2 loop in the whole ring by blocking the secondary port.

Link interruption:

When a link fails in the Ethernet ring (the link between Transit1 and Transit2 is broken, for example), both Transit1 and Transit2 may recognize this condition in the link, and advertise a LINK DOWN message via the control VLAN to the master. When the master receives it, it clears the layer-2 forwarding table information related with its data VLAN, and sends the FLUSH NOW message to notify all control devices to clear all data VLAN related layer-2 forwarding information. At the same time, the BLOCK status turns into the FORWARDING status.

Link recovery:

When the interrupted link recovers in the Ethernet (the one between Transit1 and Transit2 recovers normal, for example), Transit1 and Transit2 recognize the link recovery information, and make the ports of the recovery link ends in the BLOCK status, to forbid forwarding any messages. Then, they send the LINK UP advertisement to the master. The master receives it and turns the secondary interface in the BLOCK status, and then sends FLUSH NOW message to notify all controlled device to clear all data VLAN related layer-2 address table information. When Transit1 and Transit2 find the link recovery devices receive the FLUSH NOW message, they clear the layer-2 address table information in all data VLAN and then change the ports in BLOCK status into the FORWARDING status.

Device abnormity detection:

When the primary port of the master sends the HELLO message on regular basis (at an adjustable time interval, in 100 ms), if the secondary interface of the master does not receive the HELLO message from the primary port of the master, it considers the devices on the ring abnormal. Now, the master clears the data VLAN related layer-2 forwarding table information and sends the FLUSH NOW message to notify all controlled device to clear the DATA VLAN layer-2 forwarding table information, and then changes the BLOCK status of the secondary port into the FORWARDING status.

When the secondary port of the master receives the HELLO message from the primary interface, it immediately turns the secondary port to the BLOCK status, and then sends the FLUSH NOW message to notify the controlled devices to clear the layer-2 address table information in all data VLANs.

Master failure detection:

The user can specify a secondary device as the backup master. When the backup master does not detect the HELLO message sent from the master, it considers failure of the master and escalates itself to the master.

After the backup master switches to the master device, if it receives the message from the original master, it transfers the control to the original master and degrades again to the backup master.

The RERP supports tangent multiple rings. In other words, it allows multiple rings to share one devices. In this topology, two rings can run independently, which can be in the same domain or belong to different domains.

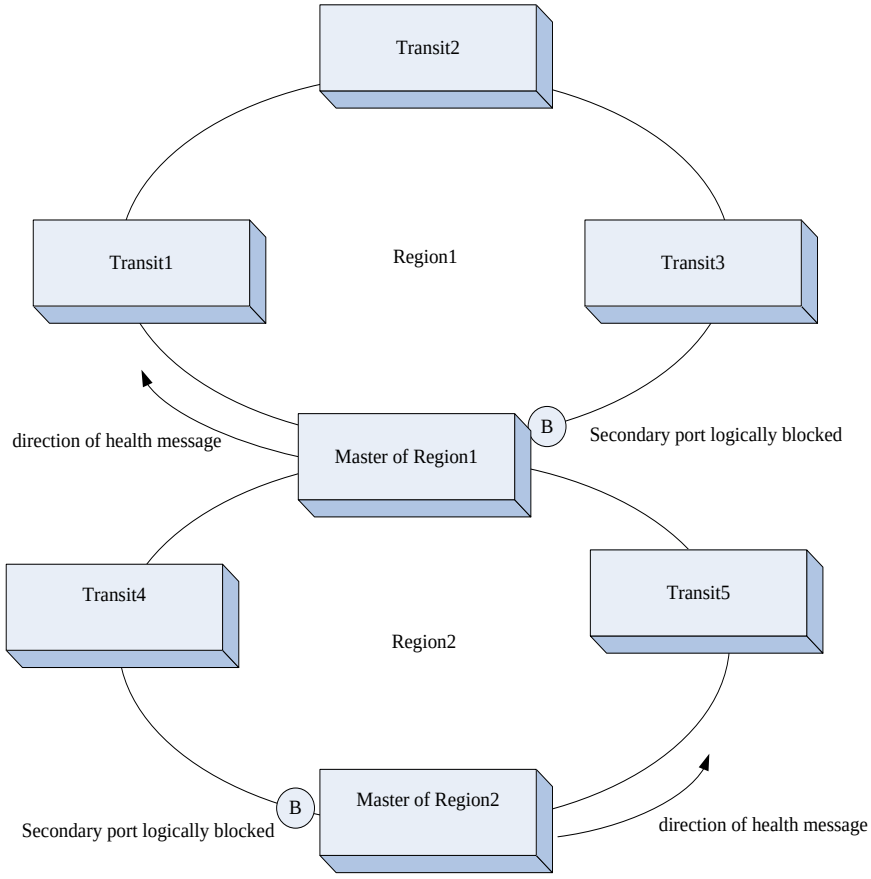


Figure-2

RERP also support the intersection of multiple rings in the single domain:

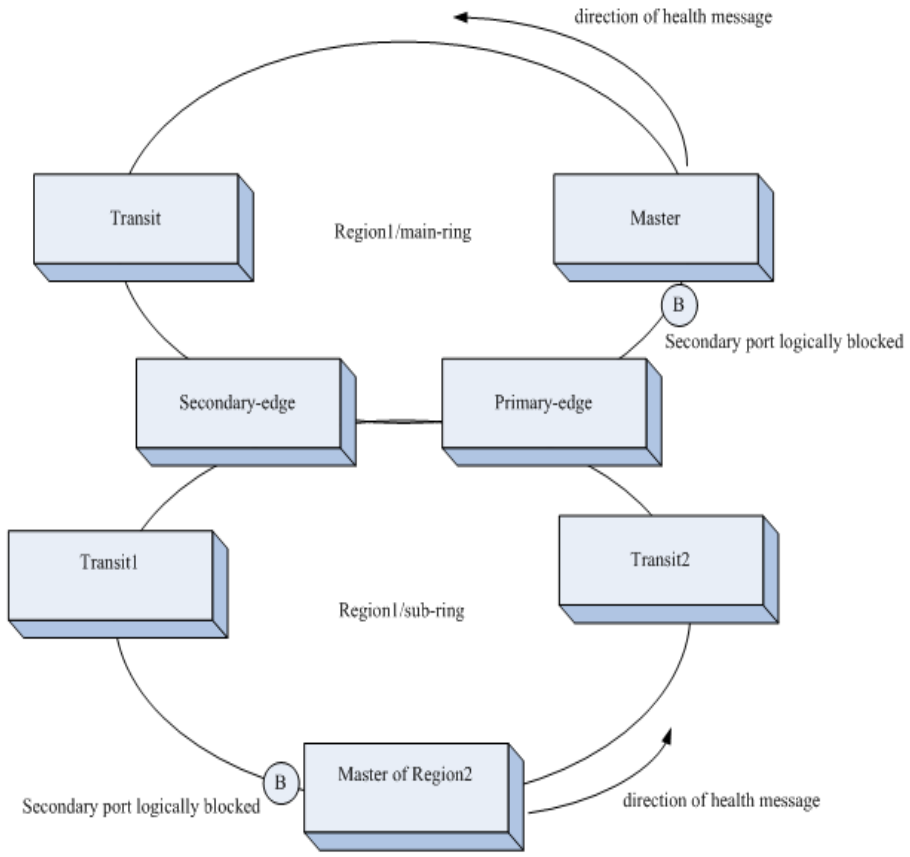


Figure-3

As shown in Figure-3, two rings are intersected in Region 1. In other words, the two rings (main-ring and sub-ring) share one link. The two intersected nodes are called Primary-edge and Secondary-edge respectively. RERP only support one sub-ring in one shared link. The connection line between Secondary-edge and Primary-edge in Figure-3 is the shared link. The characteristic of the intersected rings is that the RERP messages for the sub-ring can be controlled as the datagram in the main-ring that provides two backup links for the sub-ring. As shown in the Figure, the Secondary-edge and Primary-edge communicate through two paths. If one path is Down, no change happens for the sub-ring. While if the two paths are both Down, Secondary-edge is able to detect the failure rapidly and notify the Master in the sub-ring in time, enabling the rapid switchover of the sub-ring, rather than switchover untill the hello failure for the sub-ring. Besides, when the link between the Secondary-edge and the Primary-edge is recovered, Secondary-edge will discover and notify the Master in the sub-ring of blocking the secondary port and loop prevention. That fast processing depends on the new edge health detection mechanism between the Secondary-edge and the Primary-edge. The Secondary-edge and Primary-edge inter-detect each other in both directions of the main-ring, and the Secondary-edge is responsible for notifying the Master in the sub-ring. This ring intersection technology improves the flexibility of the RERP network topology enormously.

59.2 Configuring RERP

The following sections describe how to configure CPU Protect.

- RERP defaults
- Configure global RERP
- Configure RERP detection interval

- Configure RERP detection failure period
- Configure RERP region
- Configure RERP region role
- Configure RERP region control VLAN
- Configure RERP primary/secondary port

59.2.1 Default RERP Configuration

Global RERP status	DISABLE
RERP detection interval	1S
RERP failure time	3S

Precautions before Configuration:

- The RERP and STP are exclusive. In other words, if the RERP is configured, the STP shall be turned off.
- The refresh failure waiting time and the detection failure time are always the same and equal to the failure time.
- If the Transit and Backup do not receive the HELLO message from the Master, they will use the detection interval and detection failure interval that are configured on the local machine. If the HELLO message is received from the master, the master configurations will be used to keep consistent protocol operations on the ring network.
- The RERP control VLAN does not include vlan 1 and vlan 4094.
- Each RERP region must have one and only one master and at the same time at most one backup.
- With intersected rings configured, the failure interval of the sub-ring must be more than the one of the main-ring. It is necessary to set the failure interval of the sub-ring twice as the main-ring.
- To prevent the loop interruption during the process of configuration modification, you shall shutdown one of the RERP port in this ring and use the **no shutdown** command when modifying the RERP configurations of a ring.
- After the RERP port is enabled, it is set as the trunk port automatically, and the native VLAN is set as the control VLAN in the corresponding ring automatically. The modification of trunk and native VLAN attribute for the RERP port is prohibited. After the RERP port is disabled, it is still trunk port and the native VLAN restores to 1.
- After adding the AP port to the RERP ring, the operation of adding AP members to the AP port, removing AP members and AP port can not be implemented. The AP port shall exit from the RERP ring to execute the above operation.
- Fail to enable IGMP Snooping on the device with RERP enabled. Or the RERP cannot work normally.

59.2.2 Configuring RERP Globally

The protocol messages can be processed normally when the global RERP is enabled.

In the global configuration mode, follow these steps to enable RERP:

Command	Function
DES-7210(config)# **rerp enable**	Turn on the global RERP function switch.

Command	Function
DES-7210(config)# **end**	Return to the privileged mode.

The **no** option of the command turns off the global RERP.

Note

After setting primary and secondary ports, the port forwarding status is controlled no matter whether RERP global switch is turned on. For example, when RERP is disabled, the slave port of master will still in the blocked status to prevent the rings due to parameter configuration error.

59.2.3 Configuring RERP Detection Interval

The Master needs to send the RERP detection message on regular basis to check the health conditions of the loop. In the configuration mode, follows these steps to set the RERP detection interval:

Command	Function
DES-7210(config)# **rerp hello-interval** *interval*	Configure the detection interval within the range 1-6s, 1s by default.
DES-7210(config)# **end**	Return to the privileged mode.

The **no** option of the command restores the value to its default.

59.2.4 Configuring RERP Failure Time

If the secondary port of the master does not receive the detection message from the primary port in a certain period, it considers the fault of the loop, and then the master forces the secondary port to enter the learning forwarding status. In addition, the address refresh waiting time of the Transit and Backup is also that value.

In the global configuration mode, follow these steps to configure the RERP failure time:

Command	Function
DES-7210(config)# **rerp fail-interval** *num*	Configure the failure interval within the range 3-18s, 3 s by default.
DES-7210(config)# **end**	Return to the privileged mode.

The **no** option of the command restores the value to its default.

Note

The failure interval must be greater than or equal to three times of the detection interval.

Once an intersection ring is configured, the timeout time of the sub ring should be two times of the major ring.

59.2.5 Configuring RERP Region

An RERP region is uniquely identified with an integer, and up to 64 regions can be configured on a machine. While the RERP region is configured, it also specifies the device to support the region and enter the RERP region configuration mode.

In the privileged mode, follow these steps to configure the RERP region:

Command	Function

Command	Function
DES-7210(config)# **rerp region** *num*	Create an RERP region and enter the RERP region configuration mode. The range of *num* is 1-64.

59.2.6 Configuring RERP Ring

Each device plays only one role in a RERP ring. Only one master device and one backup device can be configured in a RERP ring.

In the global configuration mode, follow these steps to configure the RERP region role:

Command	Function
DES-7210(config)# **rerp region** *num*	Create an RERP region and enter the RERP domain configuration mode.
DES-7210 (config-rerp)# **ring** *num* **role** [**master | backup | transit**] **ctrl-vlan** *vid* **primary-port interface** *interface-id* **secondary-port interface** *interface-id*	Configure the role of the device in the RERP ring, control VLAN and primary/secondary port.

Note

When a port joins a RERP ring, it is automatically set to be a trunk port, the native VLAN is automatically set to be the control VLAN. Modifying the trunk port and native VLAN is prohibited. After the port leaves from the RERP ring, it is still a trunk port, but the native VLAN is restored to VLAN 1.

59.2.7 Configuring Edge Nodes

Two rings have two intersect nodes and share a link. The devices located in the two ends of the link are called edge nodes.

In the global configuration mode, follow these steps to configure edge nodes:

Command	Function
DES-7210(config)# edge-**ring num role** [**primary-edge**|**secondary-edge**] ctrl-vlan *vid* **shared-port interface** *interface-id* **sub-port interface** *interface-id*	Configure edge nodes

Note

The shared port must be configured in advance in a RERP ring. That is to say, a RERP ring must be configured before you configure this command.

59.2.8 Configuring the Control VLAN for the Edge Ring Supported on the Major Ring

To transmit the packets from the edge ring on the port of the major ring, set the edge ring on the major ring.

In the global configuration mode, follow these steps to configure the control VLAN for the edge ring on the major ring:

Command	Function
DES-7210(config)# **rerp region** *num*	Create an RERP region and enter the RERP domain configuration mode at the same time.
DES-7210(config-rerp)# **major-ring** *num* **edge-ring-vlan** *vid*	Set the control VLAN for the edge ring on the major ring.

Note

The major ring must have been existed.

59.3 Viewing RERP Information

The following RERP-related information can be viewed:

- View RERP configuration and status
- View RERP packet statistics

59.3.1 Viewing RERP Configuration and Status

In the privileged mode, run the following command to view the RERP configuration and status of the device:

Command	Function
DES-7210# **show rerp**	View the RERP configuration and status of the device

In the example below, the **show rerp** command is used to view the RERP configuration and status of the device.

```
DES-7210# show rerp

rerp state                      : enable

rerp admin hello interval  : 1(*1s)

rerp admin fail interval   : 3(*1s)

rerp edge interval         : 1(*300 ms)

rerp local bridge          : 001a.a902.fe0b

-----------------------------------

region 1

ring                       : 1

rerp oper hello interval   : 1

rerp oper fail  interval   : 3

ring master                    : 001a.a902.fe0b

ctrl-vlan                      : 100

edge-vlan                      :

role                       : master
```

```
primary-port                    : GigabitEthernet 0/4(forwarding)

secondary-port                  : GigabitEthernet 0/21(down)
```

59.3.2 Viewing RERP Packet Statistics

In the privileged mode, run the following command to view the RERP packet statistics:

Command	Function
DES-7210# **show rerp statistics region** *num* **ring** *ring_id*	View the RERP packet statistics
DES-7210# **clear rerp statistics**	Clear the RERP packet statistics

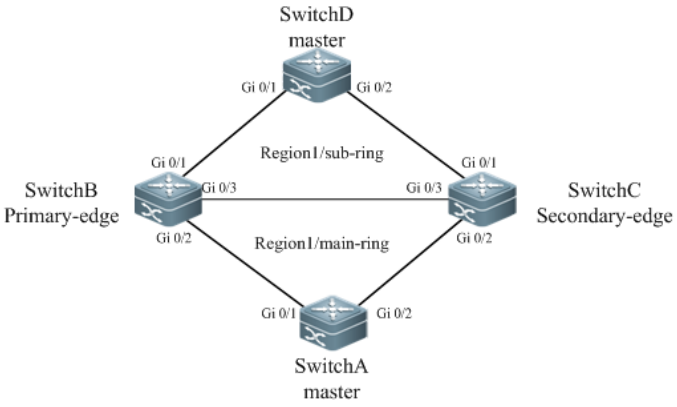
The example below shows the RERP packet statistics:

```
DES-7210# show rerp statistics region 1 ring 1
The statistics for region 1 ring 1 GigabitEthernet 0/4

TX hello packets       23   , RX hello packets         0

TX edge-hello packets   0    , RX edge-hello packets   0

TX flush packets        0    , RX flush packets        0

TX down packets        0    , RX down packets          0

TX up packets              0    , RX up packets            0

TX major fail packets   0    , RX major fail packets   0

TX major resume packets    0    , RX major resume packets 0

TX sub complete packets    0    , RX sub complete packets 0


The statistics for region 1 ring 1 GigabitEthernet 0/21

TX hello packets           0    , RX hello packets        23

TX edge-hello packets   0    , RX edge-hello packets    0

TX flush packets           0    , RX flush packets         0

TX down packets            0    , RX down packets          0

TX up packets          0    , RX up packets            0

TX major fail packets      0    , RX major fail packets    0

TX major resume packets0    , RX major resume packets  0

TX sub complete packets0    , RX sub complete packets  0
```

59.4 Configuration Examples

59.4.1 Networking Diagram

Figure 4 RERP intersect ring networking diagram



As shown in the above figure, the major ring consists of Switch A, Switch B, and Switch C, in which Switch A is the master, Switch B and Switch C are the transit. Domain ID is 1. Ring ID is 1. Control VLAN is 100. The sub ring consists of Switch B, Switch C and Switch D, in which Switch D is the master, Switch B is the primary edge, Switch C is the secondary edge. Domain ID is 1. Ring ID is 2. Control VLAN is 200.

59.4.1.1 Configuration Steps

Configure Switch A

Configure the major RERP ring as the master, control VALN to 100, primary port to Gi0/1, secondary port to Gi0/2.

```
DES-7210(config)#rerp enable

DES-7210(config)#rerp region 1

DES-7210(config-rerp)# ring 1 role master ctrl-vlan 100 primary-port interface Gi 0/1
secondary-port interface Gi 0/2
```

Configure the control VLAN for the edge ring on the major ring to 200.

```
DES-7210(config)#rerp region 1

DES-7210(config-rerp)#major-ring 1 edge-ring-vlan 200
```

Configure Switch B

Configure the major RERP ring as the transit, control VALN to 100, primary port to Gi0/2, secondary port to Gi0/3.

```
DES-7210(config)#rerp enable

DES-7210(config)#rerp region 1

DES-7210(config-rerp)# ring 1 role transit ctrl-vlan 100 primary-port interface Gi 0/2
secondary-port interface Gi 0/3
```

Configure the edge RERP ring as the primary edge, control VALN to 200, shared port to Gi0/3, sub port to Gi0/1.

```
DES-7210(config)#rerp enable

DES-7210(config)#rerp region 1

DES-7210(config-rerp)# edge-ring 2 role primary-edge ctrl-vlan 100 shared-port interface
Gi 0/3 sub-port interface Gi 0/1
```

Configure the control VLAN for the edge ring on the major ring to 200.

```
DES-7210(config)#rerp region 1

DES-7210(config-rerp)#major-ring 1 edge-ring-vlan 200
```

Configure Switch C

Configure the major RERP ring as the transit, control VALN to 100, primary port to Gi0/2, secondary port to Gi0/3.

```
DES-7210(config)#rerp enable

DES-7210(config)#rerp region 1

DES-7210(config-rerp)# ring 1 role transit ctrl-vlan 100 primary-port interface Gi 0/2
secondary-port interface Gi 0/3
```

Configure the edge RERP ring as the secondary edge, control VALN to 200, shared port to Gi0/3, sub port to Gi0/1.

```
DES-7210(config)#rerp enable

DES-7210(config)#rerp region 1

DES-7210(config-rerp)# edge-ring 2 role secondary-edge ctrl-vlan 100 shared-port
interface Gi 0/3 sub-port interface Gi 0/1
```

Configure the control VLAN for the edge ring on the major ring to 200.

```
DES-7210(config)#rerp region 1

DES-7210(config-rerp)#major-ring 1 edge-ring-vlan 200
```

Configure Switch D

Configure the edge RERP ring as the master, control VALN to 200, primary port to Gi0/1, secondary port to Gi0/2.

```
DES-7210(config)#rerp enable

DES-7210(config)#rerp region 1

DES-7210(config-rerp)# ring 2 role master ctrl-vlan 200 primary-port interface Gi 0/1
secondary-port interface Gi 0/2
```

Configure the timeout time of the edge RERP ring to be two times of the one of the major ring.

```
DES-7210(config)#rerp fail-interval 6
```

60 REUP Configuration

60.1 REUP Overview

60.1.1 Understanding REUP

The Rapid Ethernet Uplink Protection protocol(REUP) protects Ethernet uplink rapidly.

Ports are configured in pair on the ends of an uplink, with one being active and the other being standby. When two ports are up, one of them is set to be backup. For details, refer to section Configure REUP Preemption Mode and Delay.

By default, the standby port is in backup status, which cannot forward packets. When the port in forward status is down, the backup port transfers to health status and forwards packets. Moreover, the REUP advertises address update messages to upstream devices for updating MAC address, so that data interruption can be restored in 50ms in case of a link failure.

The REUP and STP are mutually exclusive on a port. In this case, the STP runs on downstream and the REUP runs on upstream for uplink backup and problem protection. The REUP offers basic link redundancy even if the STP is disabled while enabling millisecond-level fault recovery.

60.1.2 Default REUP Configuration

The following table shows default REUP configuration:

Item	Default value
REUP	Disabled
Preemption mode	Off
Preemption delay	35 seconds
Mac update transit	Disable
Mac update receive	Disabled

60.1.3 REUP Configuration Guide

Before configuring the REUP, note that:

- A port belongs to only one REUP pair. Each active link has only one standby link and vice versa. The active link and the standby link must be different ports.
- The REUP supports Layer2 physical port and Layer2 AP port, not AP member port.

- The primary port can be of different type than the secondary port. So do their rates. For example, you can set the AP port as the primary port and the physical port as the secondary port.
- The STP is disabled on the port with the REUP enabled. The port with the REUP configured does not participate in STP. BPDU penetrate transmission is supported when the STP is disabled.
- A device can be configured with up to 16 REUP pairs and 8 address update groups. Each address update group has up to four member ports. A port belongs to only one address update group.
- It is necessary to disable modifying the attributes of a port after the REUP is configured successfully on it.

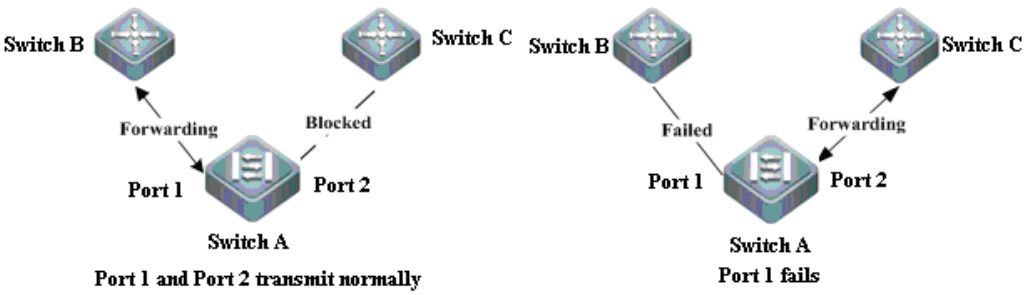
60.2 Configuring REUP

60.2.1 Configuring Dual Link Backup

You can configure a REUP pair by specifying one port as the standby port of another port. When two links are up, one is active (forwarding packets), and the other is standby (not forwarding packets). If the active link fails, the standby link becomes active and begins to forward packets. After the active link recovers from the fault, it becomes standby and does not forward any packets. Certainly, you can set the link recovered from the fault to preempt the currently active link.

As shown in Figure-1, for example, Switch A's port 1 and port 2 are connected to the upstream switches B and C. REUP is enabled on port 1 and port 2. Port 1 is active for forwarding packets; port 2 is backup. Switch C does not forward any packets from Switch A. Once port 1 fails, port 2 starts to forward packets. If port 1 recovers from the fault, it becomes backup.

Figure-1 REUP topology



In the privileged EXEC configuration mode, execute the following command to configure a REUP pair:

Command	Function
DES-7210 # **configure terminal**	Enter the global configuration mode.
DES-7210 (config) # **interface** *interface-id*	Enter the interface configuration mode.
DES-7210 (config-if) # **switchport backup interface** *interface-id*	Configure a Layer 2 physical port or a layer 2 AP port as a backup port
DES-7210(config-if)# **end**	Return to the privileged mode.

DES-7210# **show interfaces** [*interface-id*] **switchport backup** [**detail**]	Show the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

For example:

```
DES-7210# configure

Enter configuration commands, one per line.  End with CNTL/Z.

DES-7210(config)# interface gigabitEthernet 0/1

DES-7210(config-if)# switchport backup interface gigabitEthernet 0/2

DES-7210(config-if)# show interface switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State

------------------------------------------------------------

GigabitEthernet 0/1     GigabitEthernet 0/2     Active Up/Backup Down
```

60.2.2 Configuring the Preemption Mode and Delay

By configuring the preemption mode, you can determine the best available link. for bandwidth mode, the REUP will uses a link of larger bandwidth. For forced mode, the REUP will forcibly use a reliable and stable link.

To avoid frequent active-standby link switching, you can define preemption delay. After two links recover, link switching occurs after the delay.

In the privileged Exec mode, execute the following commands to configure the preemption mode and delay:

Command	Function
DES-7210 # **configure terminal**	Enter the global configuration mode.
DES-7210 (config) # **interface** *interface-id*	Enter the interface configuration mode.
DES-7210 (config-if) # **switchport backup interface** *interface-id*	Configure a Layer 2 physical port or a layer 2 AP port as a backup port.
DES-7210(config-if)# **switchport backup interface** *interface-id* **preemption mode** { **forced|bandwidth|off** }	Configure the preemption mode: Forced: The primary port always preempts the secondary port. Bandwidth: Use the port of higher bandwidth. Off: Disable preemption.
DES-7210(config-if)# **switchport backup interface** *interface-id* **preemption delay** *delay-time*	Configure preemption delay, which takes effect only in forced and bandwidth modes.
DES-7210(config-if)# **end**	Return to the privileged mode.
DES-7210# **show interfaces** [*interface-id*] **switchport backup** [**detail**]	Show the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

For example:

```
DES-7210# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210 (config) # interface gigabitEthernet 0/1
DES-7210 (config-if) # switchport backup interface gigabitEthernet 0/2 preemption mode forced
DES-7210 (config-if) # switchport backup interface gigabitEthernet 0/2 preemption delay 50
DES-7210 (config-if) # show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------
GigabitEthernet 0/1     GigabitEthernet 0/2     Active Up/Backup Down
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(10 Mbits)
```

Note

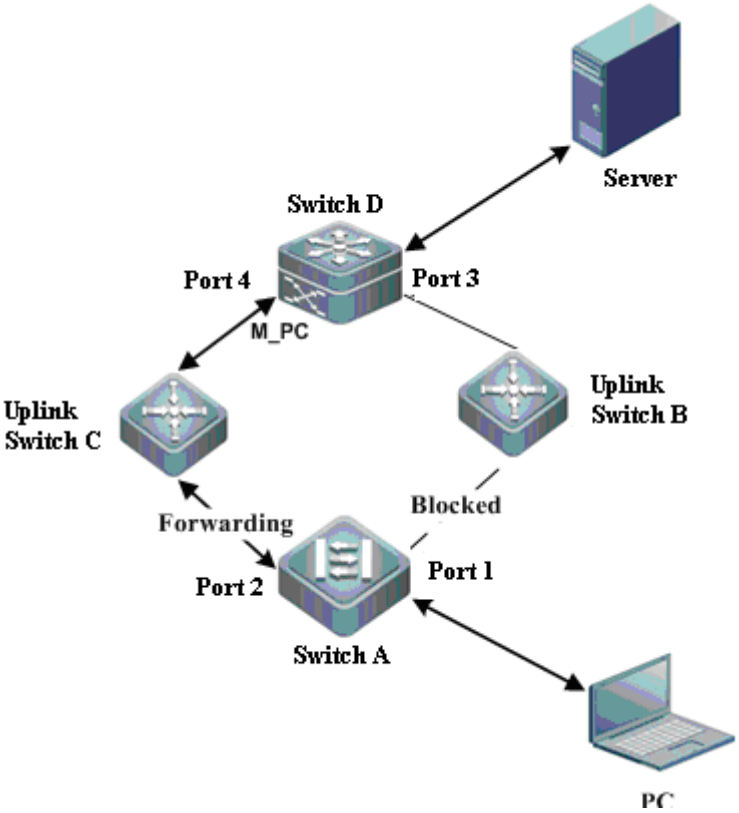
1. The bandwidth of an AP port is the number of its members whose link is up multiplying the speed of the members.
2. Once the STP is enabled on the uplink, the preemption delay should be larger than 35 seconds.

60.2.3 Configuring MAC Address Updating

60.2.3.1 Introduction to MAC Address Updating

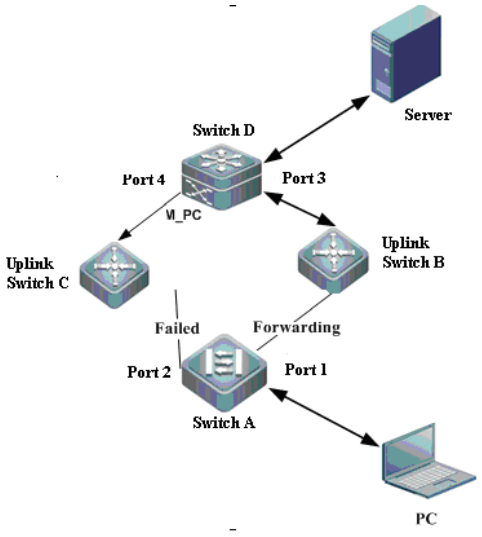
As shown in Figure-2, the REUP dual link backup is enabled on port 1 and port 2 of Switch A. Port 2 is served as the primary port. In general communication, Switch D will learn the PC's AMC address on port 4.

Figure-2 REUP operation diagram



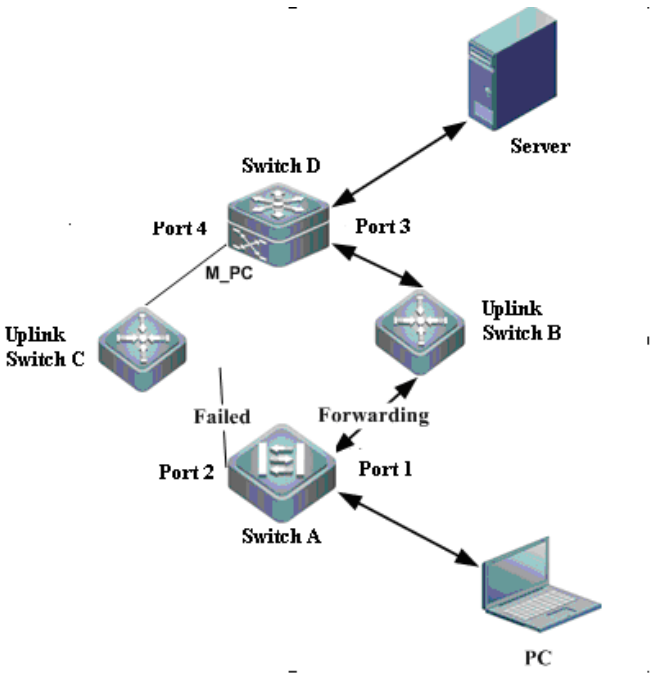
Once a fault occurs on port 2, port 1 becomes the active link. In this case, Switch D cannot learn PC's MAC address on port 3 temporarily. Switch D forwards the packets from the PC to Switch C through port 4, resulting in packet loss.

Figure-3 Error status during switching



To solve this problem, enable MAC address updating function on Switch A. When forwarding packets on port 1, Switch A will send a MAC address updating message to the port 3 of Switch D for updating its MAC address table. In this way, Switch D forwards the packets to PC to port 3, and thus speeding up the convergence of packet transmission.

Figure-4 Status after sending the MAC address updating message



To reduce the flooding influences caused by MAC address updating, a MAC address updating group is introduced. An updating group refers to assigning some ports into a group. When one of them receives the MAC address updating message, the MAC addresses on other ports of the group is also updated.

60.2.3.2 Configuring MAC Address Updating

To enable the MAC address updating function, enable the function of sending MAC address message on the switch.

In the privileged EXEC configuration mode, follow these steps to function of sending MAC address message on the switch:

Command	Function
DES-7210 # **configure terminal**	Enter the global configuration mode.
DES-7210 (config) # **mac-address-table move update transit**	Enable the function of sending the MAC address updating message.
DES-7210(config-if)# **end**	Return to the privileged mode.
DES-7210# **show mac-address-table move update**	Show the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

Enable the function of receiving the MAC address updating message on all the switches along the switching path, and add all the ports along the switching path to a MAC a MAC address updating group.

Command	Function
DES-7210 # **configure terminal**	Enter the global configuration mode.
DES-7210 (config) # **mac-address-table move update receive**	Enable the function of receiving the MAC address updating message.
DES-7210(config)# **interface** *interface-id*	Etner the interface configuration mode.

DES-7210(config-if)# **mac-address-table update group** [*number*]	Add the port to the MAC address updating group. By default, add the port to the first MAC address updating group.
DES-7210(config-if)# **end**	Return to the privileged mode.
DES-7210# **show mac-address-table update group**	Show the configuration.
DES-7210# **copy running-config startup-config**	Save the configuration.

For example, as shown in Figure-4, enable the REUP dual link backup function on port 1 and port 2.

```
DES-7210 # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210 (config)# interface gigabitEthernet 0/2
DES-7210 (config-if)# switchport backup interface gigabitEthernet 0/1
DES-7210 (config-if)# end
DES-7210 # show interface switchport backup detail
Switch Backup Interface Pairs:
Active Interface       Backup Interface       State
GigabitEthernet 0/2    GigabitEthernet 0/1    Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : off
Preemption Delay : 35 seconds
Bandwidth : 100000 Kbit (Gi0/1), 100000 Kbit (Gi0/2)
```

Enable the function of sending the MAC address updating on Switch A.

```
DES-7210 # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210 (config)# mac-address-table move update transit
DES-7210 (config)# end
DES-7210 # show mac-address-table move update
Mac address table move update status:
Transit:enable
Receive:disable
Pair: Gi0/2,Gi0/1
Members            Status    Transit Count    Last Transit Time
------------------------------------------------------------
Gi0/2              Up        0
Gi0/1              Down      0
```

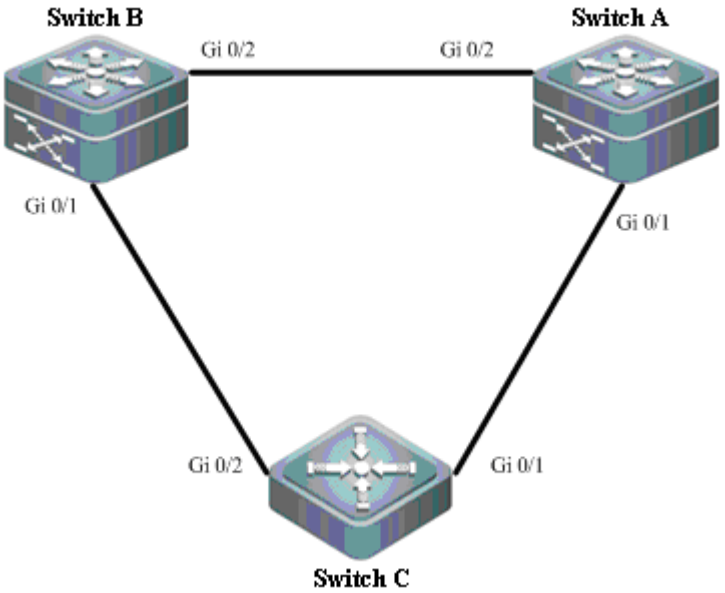
Enable the function of receiving the MAC address updating message on Switches B, C and D, and add port 3 and port 4 of Switch D to the same MAC address updating table.

```
DES-7210 # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7210 (config)# mac-address-table move update receive
```

```
DES-7210 (config)# interface range gigabitEthernet 0/3-4
DES-7210 (config-if-range)# mac-address-table update group
DES-7210 (config-if-range)# end
DES-7210 # show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member        Receive Count    Last Receive Switch-ID      Receive Time
------------------------------------------------------------
Gi0/3               0                0000.0000.0000
Gi0/4               0                0000.0000.0000
```

60.3 Typical REUP Applications

Figure-5 Typical REUP application topology



As shown in the above figure, Switch C connects to Switch A and Switch B through Gi0/1 and GI0/2. To enable rapid bi-directional convergence, enable the dual link backup function on Switch C, enable the function of receiving the MAC address updating message on Switch A and Switch B, and add the ports along the switching path to the MAC address updating group.

Configuration on Switch C:

```
DES-7210 # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# switchport backup interface gigabitEthernet 0/2
DES-7210(config-if)# exit
DES-7210(config)# mac-address-table move update transit
DES-7210(config)# end
DES-7210# show mac-address-table move update
```

```
Mac address table move update status:
Transit:enable
Receive:disable
Pair: Gi0/1,Gi0/2
Members            Status    Transit Count    Last Transit Time
-----------------------------------------------------------
Gi0/1              Standby   0
Gi0/2              Up        1                Wed Aug 20 10:51:34 2008
```

Configuration on Switch A and Switch B:

```
DES-7210 # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7210(config)# mac-address-table move update receive
DES-7210(config)# interface range gigabitEthernet 0/1 - 2
DES-7210(config-if-range)# mac-address-table update group
DES-7210(config-if-range)# end
DES-7210# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member        Receive Count    Last Receive Switch-ID      Receive Time
-----------------------------------------------------------
Gi0/1               0                0000.0000.0000
Gi0/2               0                0000.0000.0000
```

61 RLDP Configuration

61.1 RLDP Overview

61.1.1 Understanding RLDP

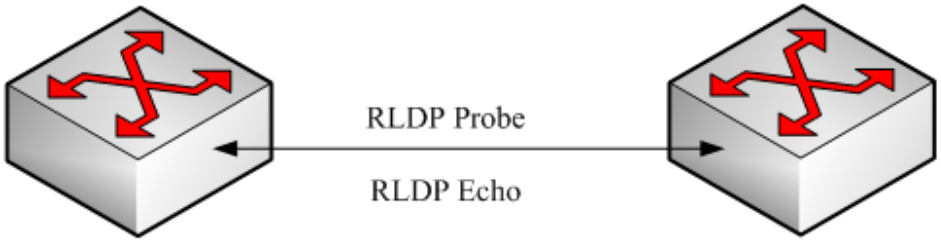
The Rapid Link Detection Protocol (RLDP) is one of DES-7210's proprietary link protocol designed to detect Ethernet link fault quickly.

General Ethernet link detection mechanism only makes use of the status of the physical connections and detects the connectivity of the link via the auto-negotiation of the physical layer. This detection mechanism has restrictions and sometimes cannot provide reliable link detection information for the user. For example, if the optical fiber receiving line pair on the optical interface is misconnected, due to the existence of the optical converter, the related port of the device is "linkup" physically but actually the corresponding layer-2 link cannot work for communications. Here is another example. There is an intermediate network between two Ethernet devices. Due to the existence of the network transmission relay devices, the same problem may occur if those relay devices are faulty.

The RLDP enables easy detection of Ethernet device link fault, including the one-way link fault, two-way link fault and loop link fault.

The RLDP implements the detection by exchanging the RLDP messages at the two ends of the link, as shown in Figure-1:

Figure-1:



The RLDP defines two protocol messages: Probe message and Echo message. The RLDP sends the Probe message of this port to the port with RLDP configured and in linkup status on regular basis, and waits for the Echo message from the neighbor port and waits for the Probe message sent by the neighbor ports. If a link is correct both physically and logically, a port shall be able to receive the Echo message of the neighbor port as well as the Probe message of the neighbor port. Otherwise, the link is considered abnormal.

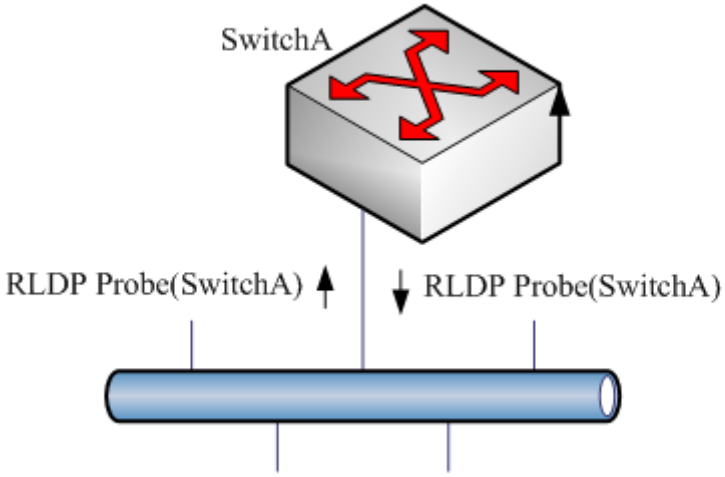
Note

To make use of the one-way detection and two-way detection functions of the RLDP, it is necessary to ensure the RLDP is enabled on the ports at both ends of the link. And, it is not allowed for a port with RLDP enabled to connect multiple neighbor ports. Otherwise, the RLDP cannot detect the health conditions of every neighbor link.

61.1.2 Typical Application

Loop detection:

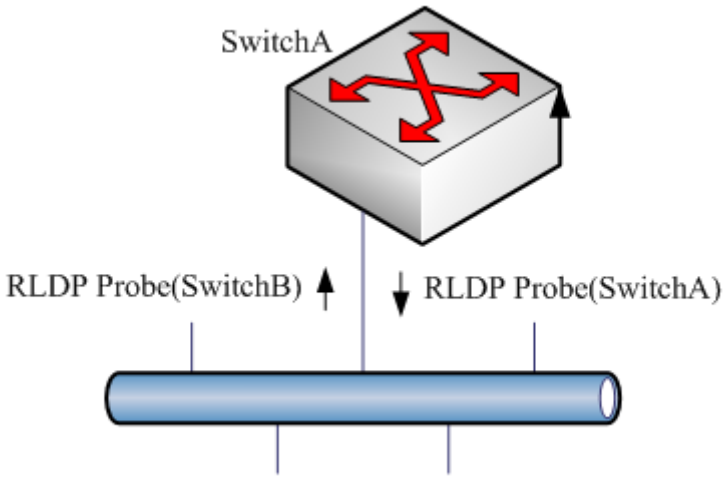
Figure-2: Loop detection



The so-called loop fault means that a loop appears on the links connected with the port. A shown above, on a port the RLDP receives the RLDP message sent from its machine, so the port is considered as loop fault. So, the RLDP deals with the fault according to the user configurations, including alarming, setting port violation, turning off the SVI with that port, turning off the port learning forwarding, and more.

One-way link detection:

Figure-3: One-way link detection

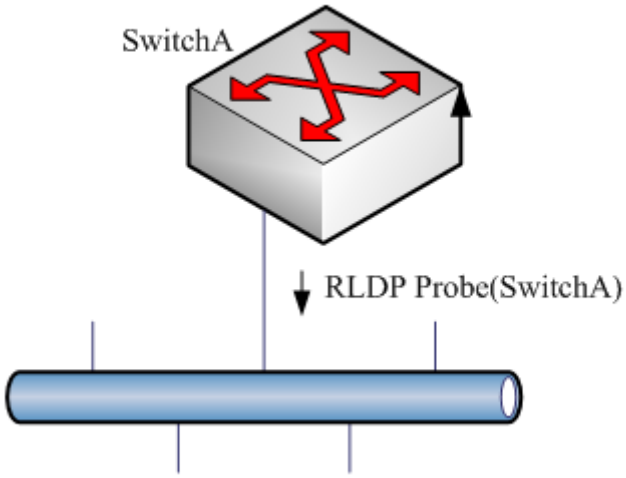


The so-called one-way link detection means the link connected with the port can receive message only or send messages only (due to misconnection of the optical receiving line pair, for example). As shown above, the RLDP only receives the detection message from the neighbor port on a port, so it is considered one-way link fault. So, the RLDP deals with the

fault accordingly according to the user configurations. In addition, if the port cannot receive any RLDP detection message, it is also considered one-way link fault.

Two-way link detection:

Figure-4 Two-way link detection



This means that fault occurs at the frame transmission/receiving at both ends of the link. As shown above, the port of the device sends the RLDP probe message but has never received the Echo message or the Probe message from the neighbors. So, it is considered two-way link fault. From the nature of the fault, the two-way fault actually includes the one-way fault.

Note

If the party at one of the two link ends has not enabled the RLDP, the diagnosis also shows two-way or one-way link fault. So, in configuring two-way link detection or one-way link detection, the administrator shall make sure that the RLDP is enabled at both ends to avoid the incorrect diagnosis information.

61.2 Configuring RLDP

The following sections describe how to configure RLDP.

- RLDP defaults
- Configure global RLDP
- Configure port RLDP
- Configure RLDP detection interval
- Configure the RLDP maximum detection times
- Restore the RLDP status of the port

61.2.1 RLDP defaults

Global RLDP status	DISABLE
Port RLDP status	DISABLE
Detection interval	2S

Maximum detection times	3

Caution

- The RLDP can be configured only on the basis of the switching interface (including AP) and the routing interface.
- All RLDP frames are untagged.
- In the RLDP fault processing type, the block function and the STP are mutually exclusive. In other words, if the fault processing type configured on the port is "block", it is recommended to disable STP; otherwise, since the STP cannot recognize one-way link, possibly the STP allows port forwarding but the RLDP is configured with port blocking.

61.2.2 Configuring RLDP Globally

The RLDP works on the port only when the global RLDP is enabled.

In the global configuration mode, follow these steps to enable RLDP:

Command	Function
DES-7210(config)# **rldp enable**	Turn on the global RLDP function switch.
DES-7210(config)# **end**	Return to the privileged mode.

The **no** option of the command turns off the global *RLDP*.

61.2.3 Configuring RLDP on the Port

The RLDP operation is port-based, so the user needs to explicitly configure which ports shall run RLDP. In configuring the port RLDP, it is required to specify the diagnosis type and the troubleshooting method for the port at the same time. The diagnosis types include unidirection-detect, bidirection-detect and loop-detect. The troubleshooting methods include warning, block, shutdown-port, and shutdown-svi.

In the configuration mode, follow these steps to configure the RLDP on the port:

Command	Function
DES-7210(config)# **interface** *interface-id*	Enter the interface mode.
DES-7210(config-if)# **rldp port** {**unidirection-detect** | **bidirection-detect** | **loop-detect** } {**warning** | **shutdown-svi** | **shutdown-port** | **block**}	Enable the RLDP on the port and configure the diagnosis type and troubleshooting method at the same time.
DES-7210(config-if)# **end**	Return to the privileged mode.

The **no** option of the command disables the RLDP on the port and the configured detection types one by one.

In the example below, the RLDP is configured on GigabitEthernet 0/5, and multiple diagnosis types and troubleshooting methods are specified:

```
DES-7210# configure terminal
DES-7210(config)# interface gigabitEthernet 0/5
DES-7210(config-if)# rldp port unidirection-detect
shutdown-svi
DES-7210(config-if)# rldp port bidirection-detect warning
DES-7210(config-if)# rldp port loop-detect block
```

```
DES-7210(config-if)# end
DES-7210# show rldp interface gigabitEthernet 0/5
port state     : normal
local bridge   : 00d0.f822.33ac
neighbor bridge : 0000.0000.0000
neighbor port  :
unidirection detect information:
action : shutdown svi
state  :  normal
bidirection detect information :
action : warnning
state  :  normal
loop detect  information    :
action : block
state  :  normal
```

Several precautions in configuring port detection:

- The routing interface does not support the shutdown-svi error handling method, so this method is not executed in case of the occurring of detection error.
- In configuring loop detection, the neighbor devices downward connected with the port cannot enable the RLDP detection; otherwise, the port cannot have correct detection.
- If the block method is configured on the aggregated port and the link detection error happens, do not change the member port relations of the aggregate port before the port reset detection; otherwise, the forwarding status of the member interface may have unexpected effects of forwarding status.
- If the RLDP detects link error, alarm information will be given. The user can send the alarm information to the log server by configuring the log function. At least 3 levels of log shall be ensured.
- You are recommended to specify the diagnosis type of the loop detection to shutdown-port for the reason that for some devices, even if the device detects the loop and specifies the block port, a large amount of packets will be sent to the CPU for the hardware chip limitation.

61.2.4 Configuring RLDP Detection Interval

The port with the RLDP function enabled will send the RLDP Probe messages on a regular basis.

In the global configuration mode, follow these steps to configure the RERP detection interval:

Command	Function
DES-7210(config)# **rldp detect-interval** interval	Configure the detection interval within the range 2-15s, 3s by default.
DES-7210(config)# **end**	Return to the privileged mode.

The **no** option of the command restores the value to its default.

61.2.5 Configuring the Maximum RLDP Detection Times

If the port with RLDP enabled cannot receive messages from neighbors in the maximum detection period (maximum detection times X detection interval), that port will be diagnosed as faulty. See the Overview for details of the fault types.

In the global configuration mode, follow these steps to configure the RERP maximum detection times:

Command	Function
DES-7210(config)# **rldp detect-max** Num	Configure the maximum detection times, num range 2-10, 2 by default.
DES-7210(config)# **end**	Return to the privileged mode.

The **no** option of the command restores the value to its default.

Note

The maximum detection times only take effect in the unidirectional link detection and bidirectional link detection, and will not take effect if only loop detection is enabled on a port.

61.2.6 Restoring the RLDP Status of the Port

The port with shutdown-port troubleshooting method configured cannot resume the RLDP detection actively after a fault occurs. If the user confirms the fault removed, run the recovery command to restart the RLDP on the shutdown port. This command sometimes may make the other ports with detection errors resume.

In the privileged mode, follow these steps to resume the RLDP detection of the port:

Command	Function
DES-7210# **rldp reset**	Make any port with RLDP detection failure resume the detection.

Note

The **errdisable recover** command can be used in the global configuration mode to restart, instantly or at fixed time, the RLDP detection of the port that is set violation by RLDP. It is worth mentioning that when there are some relay devices between rldp ports, if you use **errdisable recover interval** to restore the fault timely, you need to set the value of rldp detection time greater than that of **errdisable recover interval**, that is, the value of detect-interval* detect-max total time is greater than that of **errdisable recover interval** to prevent error judgment.

61.3 Viewing RLDP Information

The following RLDP-related information can be viewed:

- View the RLDP status of all ports
- View the RLDP status of the specified port

61.3.1 Viewing the RLDP Status of All Ports

In the privileged mode, run the following commands to view the RLDP global configuration and the port detection information with RLDP detection configured:

Command	Function
DES-7210# **show rldp**	View the RLDP global configuration and the port detection information with RLDP detection configured

In the example below, the **show rldp** command is used to view the detection information of all RLDP ports:

```
DES-7210# show rldp
rldp state            : enable
rldp hello interval   : 2
rldp max hello        : 3
rldp local bridge     : 00d0.f8a6.0134
------------------------------------------------
interface GigabitEthernet 0/1
port state:normal
neighbor bridge       : 00d0.f800.41b0
neighbor port         : GigabitEthernet 0/2
unidirection detect information:
action                : shutdown svi
state                 : normal

interface GigabitEthernet 0/24
port state:error
neighbor bridge       : 0000.0000.0000
neighbor port         :
bidirection detect information :
action                : warnning
state                 : error
```

As shown above, port GigabitEthernet 0/1 is configured with unidirection detection. No error is detected now, and the port status is normal. Port GigabitEthernet 0/24 is configured with bidirection detection, and bidirection fault is detected.

61.3.2 Viewing the RLDP Status of the Specified Port

In the privileged mode, run the following command to view the RLDP detection information of the specified port:

Command	Function
DES-7210# **show rldp interface** interface-id	View the RLDP detection information of interface-id.

In the example below, the **show rldp interface GigabitEthernet** *0/1* command is used to view the RLDP detection information of port fas0/1:

```
DES-7210# show rldp int GigabitEthernet 0/1
port state     :error
local bridge   : 00d0.f8a6.0134
neighbor bridge : 00d0.f822.57b0
```

```
neighbor port   : GigabitEthernet 0/1
unidirection detect information:
action: shutdown svi
state :  normal
bidirection detect information :
action : warnning
state :  normal
loop detect  information    :
action: shutdown svi
state :  error
```

As shown above, the port GigabitEthernet 0/1 is configured with three detection types: unidirection detection, bidirection detection and loop detection. The troubleshooting methods are shutdown-svi and warning. Error is found in loop detection so the current port status is error. Accordingly, the SVI of the port is shutdown.

62 TPP Configuration

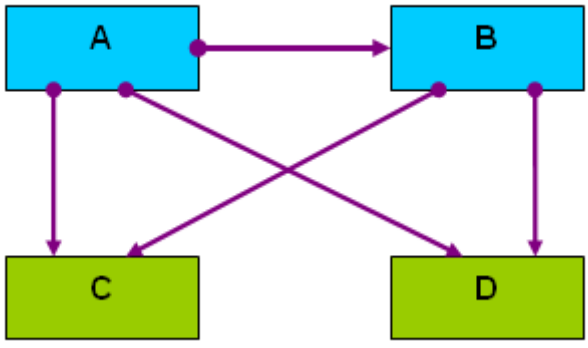
62.1 TPP Overview

The Topology Protection Protocol (TPP) is a topology stability protection protocol. The network topology is rather fragile. Illegal attacks in the network may cause abnormal CPU utilization on network devices, frame path blocked, etc. These are apt to cause network topology turbulence. The topology protection aims to stabilize the network topology by detecting the abnormalities (high CPU utilization, frame buffer abnormal, etc.) and detecting the abnormalities of neighbor devices. The interaction with neighbor devices is implemented by sending specific abnormity advertisement. This function has rather high priority and can effectively prevent network topology turbulence.

62.2 TPP Application

The topology protection is generated to address the network topology turbulence that my be caused in the MSTP or VRRP and other distributed network protocol. The MSTP, VRRP and other protocols work with the message notification mechanism to automatically maintain the network topological structure and automatically adapt to the topological change in the network. This on the other hand results in the aptness to attacks. When malicious network attacks arrive, transient interruption of timed messages may be caused due to high CPU utilization or frame path blocking, causing error fluctuation of the network topology and great harm to the normal communication in the network. The topology protection function minimizes such unnecessary fluctuations. It works with the other distributed protocols (MSTP, VRRP, etc.) to make the network more stable and reliable.

Figure-1:



As shown in the above dual-core topology, A and B are the L3 convergence devices, and C and D are the L2 access devices. A is the MSTP root bridge. The topology protection functions of all the devices are enabled.

The CPU of the L3 convergence device A is extremely busy due to network attack, resulting in that the BPDU packets cannot be sent. The topology protection function detects the exception and sends the exception advertisement packet to its neighbors. B, C, and D all receive the advertisement and adopt the anti-vibration measures.

he CPU of B is extremely busy under the attack of a large number of packets and cannot send or receive packets normally. After detecting the exception, B sends the exception advertisement to all its neighbors. A receives the exception advertisement but does not process it further because B finds the exception has not effect on B according to its source. The downstream C and D receive the exception advertisement and perform further defense activities to ensure the reliability of the network topology, because they find the exception will affect the topology calculation.

62.3 TPP Configuration

Configuring TPP involves global function configuration and port function configuration. The global function configuration is used to enable the topology protection function of the device. By default, the global topology protection function is enabled. Here, it will detect the running conditions of the local and neighbor devices and perform treatment for the abnormities that occur. However, it does not notify the local running conditions to neighbor devices. The port function configuration is used to enable the topology protection function of the port. When the topology protection function is enabled on the port, it indicates that the opposite neighbor device is concerning about the running conditions of this machine. When the local device becomes abnormal, this will be notified to the opposite neighbor device of the port. By default, the topology protection function is disabled on all ports.

Note

The topology protection function is suitable for the point-to-point link network, and adjacent network devices must enable the topology protection function. Besides, during the TPP configuration, you often need to use cpu topology-limit to configure the threshold for CPU utilization detection. When the CPU utilization exceeds the threshold, the system generates the topology protection advertisement. We suggest a middle to high value, such as 50–70, so that the TPP can judge the network conditions more accurately. If the value is too small, the network topology may not switch when it should to switch due to TPP alarm. If the value is too large, the system may be too busy to generate the TPP alarm, causing the TPP invalid.

62.3.1 Configuring Topology Protection Globally

The global topology protection function is enabled by default. The **no** option of the command disables the global topology protection.

The configuration commands are as follows:

Command	Function
DES-7210> **enable**	Enter the privileged mode.
DES-7210# **config terminal**	Enter the global configuration mode.
DES-7210(config)# **topology guard**	Enable the global topology protection
DES-7210(config)# **end**	Exit to the privileged mode.
DES-7210# **copy running-config startup-config**	Save the configuration.

The **no topology guard** command disables the global topology protection function on the device.

62.3.2 Configuring Topology Protection on the Port

The configuration commands are as follows:

Command	Function

Command	Function
DES-7210> **enable**	Enter the privileged mode.
DES-7210# **config terminal**	Enter the global configuration mode.
DES-7210(config)# **interface gi** *0/1*	Enter the interface configuration mode.
DES-7210(config-if)# **tp-guard port enable**	Enable the port topology protection function.
DES-7210(config-if)# **end**	Exit to the privileged mode.

The **no tp-guard port enable** command disables the topology protection on the port. This command is suitable only on layer-2 switching ports and routing ports.It is inapplicable to AP member ports.

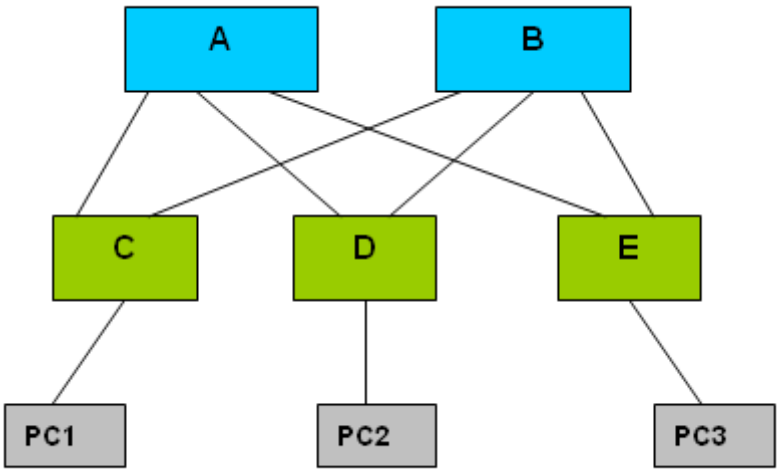
Note

The global topology protection is the global switch for the topology protection. When it is enabled, the device detects the running parameters of its own and monitors the running parameters of neighbor devices at the same time. When abnormity appears locally, it sends abnormity notification messages to the neighbor devices. When the port topology protection function is enabled, if abnormity occurs locally, it sends abnormity notification message to neighbor devices.

62.4 Typical TPP Configuration Examples

The figure below shows a dual-core networking topology:

Figure-2:



As shown in the figure, A and B are L3 convergence devices, while C, D and E are L2 access devices.

The MSTP enabled on A, B, C, D, and E, and VRRP enabled on A and B. The topology protection function enables the MSTP and VRRP to operate more reliable, avoiding unnecessary vibration of the network topology.

The global topology protection function is enabled on A, B, C, D, and E, and the topology protection function is enabled on all the ports..

62.5 View TPP information

The following TPP-related information can be viewed:

- View the TPP configuration and status of the device

62.5.1 Viewing the TPP configuration and status of the device

In the privileged mode, run the following command to view the TPP configuration and status of the device:

Command	Function
DES-7210# **show tpp**	View the TPP configuration and status of the device

```
DES-7210 #show tpp
tpp state          : enable
tpp local bridge   : 00d0.f822.35ad

      ------------------------------------
```

63 Redundancy Configuration for Supervisor Engine

This chapter describes how to configure supervisor engine redundancy to implement nonstop forwarding(NSF) and the system file management method of the supervisor engine.

This chapter includes:

1. Understanding redundant NSF of supervisor engine
2. NSF configuration method

63.1 Understanding Redundant NSF of Supervisor Engine

63.1.1 Overview

NSF means that in the network device with the structure of separating control side from forward side, the control side is planned to shut down(such as software upgrade) or not planned to shut down(such as software and hardware defect) while the forward side goes on forwarding and there is no forward halt or topology fluctuation during the reboot of control side. NSF is an important part of High Availability Architecture

Caution The DES-7200 series switch that supports hot-plugging/unplugging of supervisor engine implements NSF in the method of supervisor engine redundancy.

In the machine which is installed with dual supervisor engines, the master supervisor engine is used normally while the other backup one is slave supervisor engine which is a substitute for the master one when the master one is broken off or requires for the switchover. It not only enlarges exchanging capacity but also offers management redundancy to improve the stability of device. In the running process of the device, if the master supervisor engine does not work well, the device will switch to the slave one automatically without losing user's corresponding configuration, which ensures that the network runs well. Generally, slave supervisor engine does not join in the switch management but monitors the status of master one. These events below will trigger supervisor engine switchover:

1) System suspend or reset due to hardware fault of master supervisor engine
2) No heartbeat between two supervisor engines
3) Manual switchover

When booting dual supervisor engines at the same time or hot-plugging another when one board is enabled, they will do some batch synchronization configuration before they are in Active/Standby Hot status. At this time, if disturbance sources are configured, slave supervisor engine will reboot and the dual ones are in Active/Boot Hot status. If all disturbance sources are cleared in Active/Boot Hot status, the slave one will reboot too and the dual ones are in Active/Standby Hot status. If new disturbance sources are configured in Active/Boot Hot status, it will influence nothing and the dual ones are still in Active/Boot Hot status.

Now, the disturbance sources include the following entities:

- GVRP: GARP VLAN Registration Protocol, an application of the relationship between dynamic configuration and extended VLAN member .
- SVLAN: Super VLAN, also named as VLAN Aggregation which is a kind of management technology for optimizing IP address.

Caution

- PVLAN: Private VLAN.
- MCAST: Multicast.
- DOT1X: 802.1x, which is used to control the authentication of user network access and provide authorization and accounting function.
- PTLVLAN: Protocol VLAN, VLAN classification technology based on package protocol type. It can divide the null VLAN ID of a protocol typet to a same VLAN.

Postscript: the dual managemetn panels are in Boot Cold/Boot Cold status if the system detects the in consistency of the software version of the dual ones when starting up. In other words, they can detect the other side respectively, but they are not in Active/Standby Hot status untill the automatic upgrade is finished and the slave one is reset. Finally, the software version of the dual supervisor engines is consistent.

63.1.2 NSF Advantages and Limitation

The advantages of NSF technology implementation in network service are:

- Improving the network availability:

  NSF technology maintains the information of data forwarding and user session status in the process of device change.

- Preventing the neighbour from detecting link flap:

  The forwarding side does not reboot during the switchover, so the neighbour can not detect the link status change from Down to Up.

- Preventing routing flaps:

  The forwarding side maintains to forward and communicate during the switchover and the control side forms new forwarding list quickly without apparent substitution between the new and oil forwarding list, thus preventing routing flaps.

- User sessions will not be lost:

User sessions built before the switchover will not be lost due to the synchronization in real time.

The limitations of using NSF technology in the switch are:

- NSF works well on the premise that the software and hardware constitution of the dual supervisor engines are consistent.
- It should synchronizes the master and slave supervisor engines in batch to make them consistent, before which is the window period when NSF can not take effect.
- Not all the functions related with forwarding are synchronized. The switch function can be classified into the following types according to NSFsupporting degree:
  - High availability support function;
  - Real time synchronization of status information between master and slave supervisor engine. For example, it synchronizes the control side function directly related with L2 forwarding in real time.
  - High availability compatibility function
  - These features do not support high availability for the status datas are not synchronized. However, when enabling high availability, these functions that starts to run from initialization can still be used after switching.
  - High availability incompatibility function

Caution

These features do not support high availability for the status datas are not synchronized. When enabling high availability, these functions can not be used, or it may lead to system abnormity. When enabling these functions, the system status is changed from Standby Hot to Boot Hot and the system can only synchronize running-config, such as GRRP.

63.1.3 Key Constitution Technology of NSF

The key technologies of implementing NSF include:

- **Status synchronization**

The master supervisor engine synchronizes the running status with the slave one in order to enable the slave one to be a substitute for the master one at any time without noticeable changes.

- **Configuration synchronization**

It synchronizes the configurations of the functions that are not associated with NAF directly. The user configuration keeps consistent during the switchover by the synchronization of running-config and startup-config.

Conducting running-config when user configuration returns to the privileged mode from the global mode, while conducting startup-config synchronization when the user executes command write or copy to save the configuration.

It can not synchronize SNMP configuration automatically untill running-config synchronization is triggered by CLI configuration method.

Caution

You can configure auto-sync mode as the following steps. In the global configuration mode, execute command **redundancy** first and then **auto-sync { standard | startup-config | running-config }.** To view the current auto-sync mode, use **show redundancy auto-sync** in the privileged mode. To configure the auto-sync interval in an unit of second, execute command **redundancy** first and then **auto-sync time-period value.**

Auto-sync has three modes:

h) standard: synchronizes all the system files. In other words, it synchronizes both startup-config and running-config.

i)startup-config: synchronizes startup configuration file.

j)running-config: synchronizes configuration file of running time.

The **no** form of the command disables all the modes, making the configuration file out of auto-sync. By default , the mode of auto-sync is standard, which synchronizes both startup-config and running-config.

63.2 NSF Configuration Method

Caution

In supervisor engine redundancy constitution methods, only master supervisor engine supports all CLI commands, while slave supervisor engine supports a few commands in user EXEC and privileged EXEC mode.

63.2.1 Configuring Redundant Management

This chapter includes:

- Automatic selection of master supervisor engine
- Manual selection of master supervisor engine

63.2.1.1 Automatic selection of master supervisor engine

You can plug or unplug the supervisor engines while the switch is working. Based on the current conditions, the switch automatically selects an engine for its operation without normal data switching. In case of any conditions below during you use, the master supervisor engine will be selected accordingly:

- If only one supervisor engine is plugged when the switch is started up, the switch will select it as the master supervisor engine no matter whether it is in slot M1 or M2.

- If both supervisor engines are plugged when the switch is started up, by default, the one in slot M1 will be selected as the master and the one in slot M2 as the slave for purpose of redundancy. Related prompt message will be provided.
- If only one supervisor engine is plugged when the switch is started up, and the other supervisor engine is plugged while the switch is in normal operation, the latter will be regarded as the slave supervisor engine for purpose of redundancy, no matter whether it is slot M1 or M2. Related prompt message will be provided.
- If both supervisor engines are plugged when the switch is started up, and one of them is unplugged while the switch is in normal operation (or one becomes abnormal): if the unplugged supervisor engine is the slave before it is unplugged (or abnormal), the switch only prompts that the slave supervisor engine is unplugged (or becomes abnormal); if the unplugged supervisor engine is the master before it is unplugged (or abnormal), the other supervisor engine will turn from slave to master, and related prompt will be provided.

Caution

During the normal operation of the switch, the parameters must be saved when the configurations are done; otherwise, the configuration will be lost in case of master/salve switchover.

During the startup of the device inserted with two supervisor engines, if the main program of any supervisor engine is incomplete or absent, the switch cannot start. The symptom is that the two boards restart repeatedly or suspend during the startup process.

During the startup of the device inserted with one supervisor engine, if the supervisor engine with incomplete or absent CTRL program or main program is inserted before the success of the startup, the switch also cannot start.

In the above two case, remove the faulty supervisor engines. If the device is still abnormal, power off the switch and restart it.

During the batch backup of master and slave supervisor engine, do not unplug the master one, or it will lead to data flow breakoff due to system reset. If the software of dual supervisor engines are abnormal during the period of batch backup, it will also lead to data flow breakoff due to system reset.

Please unplug one of the dual supervisor engines quickly if you want to unplug one of them when they are working simultaneously. Slow unplugging may make the supervisor engine work abnormally. Please make sure that the supervisor engine is plugged tightly and the screw id tightened.

63.2.1.2 Manual selection of master supervisor engine

The DES-7200 series switch supports dual supervisor engines. You may select the master and slave supervisor engines by using the commands available in CLI.

In the privileged user mode, execute the following commands to forcibly switch over the master supervisor engine:

Command	Meaning
redundancy force-switchoverswitch	This command is executed immediately without the necessity for global configuration mode.

For example, the current master supervisor engine is the one in slot M1. When the following commands are executed, the supervisor engine will be switched over to the slave supervisor engine, and the one in slot M2 becomes the master.

```
DES-7210# redundancy force-switchoverswitch
```

63.2.2 Configuring the Synchronization Mode

Run the following commands to configure the configuration files to be synchronized:

Command	Function
DES-7210(config)# **redundancy**	Enter the redundancy configuration mode
DES-7210**(config-red)# auto-sync** {**standard** | **running-config** | **startup-config**}	Configure the configuration files to be synchronized.
DES-7210#**show running-config**	Confirm the hot-backup started.
DES-7210#**show redundancy state**	Show the current redundancy operation mode.

63.2.3 Configuring the Heart-beat Check Time

Run the following command to configure the heart-beat check time between the master and slave supervisor engines.

Command	Function
DES-7210(config)# **redundancy**	Enter the redundancy configuration mode
DES-7210(config-red)# **switchover timeout** *timerout-period*	Control the heart-beat check time between the master and slave boards
DES-7210#**show running-config**	Confirm the hot-backup started.
DES-7210#**show redundancy state**	Show the current redundancy operation mode.

63.2.4 Resetting the Supervisor Engine

Run the following command to reset the specified supervisor engine or both the master and salve ones.

Command	Function
DES-7210(config)#**redundancy reload {peer | shelf}**	peer: reset the slave supervisor engine only. shelf: reset both.

64 File System Configuration

64.1 Overview

The file system is an organization for storing and managing the files on the auxiliary storage devices. The switch provides the serial Flash as the auxiliary storage device to store and manage the NM operating system files and configuration files of the switch.

The file data are stored as logs on the serial Flash and each file has a file header for recording the basic information of the file. When the storage device is full with no more space for other operations, the file system will automatically de-fragment the storage device and recycle the trash. This is for providing the sufficient space for file operations. This is done in a very short period without your perception. To make full use of the limited space, the file system provides the data compression function and the data node index.

64.2 Configuring File System

The following sections describe how to configure the file system.

- Changing Directories
- Copying Files
- Showing Directories
- Formatting the System
- Creating directories
- Moving Files
- Showing the Current Working Path
- Removing Files
- Deleting Empty Directories

64.2.1 File System Configuration Guide

The command keyword is not case sensitive, while the file name is case sensitive, and the maximum size of the file name is 4096.

All the file names and paths do not support the wildcard.

It is highly recommended that the file system can not occupy over **128M** on the device with great flash storage space; otherwise, the system will slow down the boot rate evidently and the waiting time of executing command **dir** to view the file for the first time in privileged mode will be increased greatly. Therefore, it is recommended to clear some useless outdated files manually after the file system has been used for some time.

For the device with the flash storage space(excluding the storage space for the extended flash) is **32M**, when the free memory is less than **512k**, it is recommended to clear the useless outdated files manually to ensure the normal operation to the flash file system.

For example, when the USB mounts, the operation system deals with the flash file system. Therefore, when it fails to mount the USB file system and the free flash memory is less than **512k**, it is recommended to clear the timeout and useless files manually and then try again.

Note

For the device with the flash storage space(excluding the storage space for the extended flash) is **512M,** when the free memory is less than **4M**, it is recommended to clear the useless outdated files manually to ensure the normal operation to the flash file system.

For example, when the USB mounts, the operation system deals with the flash file system. Therefore, when it fails to mount the USB file system and the free flash memory is less than **4M**, it is recommended to clear the useless outdated files manually and then try again.

When the free flash memory is less than the **110%*the size of the file to be copied**, it is recommended to clear the useless outdated files manually to ensure the successful copy.

For example, when you want to copy the file in 10MB, the operation system will make use of the partly flash storage space to manage the 10MB data. Therefore, when the flash memory space is less than 11MB, it is recommended to clear the useless outdated files manually and then try again.

64.2.2 Changing Directories

This shifts from the current directory to the specified directory.

In the privileged mode, use this command by performing the following steps:

Command	Function
DES-7210# **cd** *directory*	Enter the specified directory.
DES-7210# **cd** ../	Enter the higher-level directory
DES-7210# **cd** ./	Enter the current-level directory

The following example enters the document directory in the mnt directory at the root:

```
DES-7210# cd mnt/document
```

After that, the operations will be performed in the mnt/document directory.

64.2.3 Copying Files

This copies the files to a directory or a file.

In the privileged mode, copy files to a directory or files by using the **cp** command:

Command	Function
DES-7210# **cp dest** *directoryname* **sour** *filename*	Copy the file to the specified directory
DES-7210# **cp dest** *filename* **sour** *directoryname*	Copy the file to the specified file

The following example shows how to copy a file to a directory and another file:

```
DES-7210# cp dest ../bak sour config.text
DES-7210# cp dest con_bak.txt sour config.text
```

64.2.4 Showing Directories

This shows the contents of the current working directory or specified directory:

Command	Function
DES-7210# **dir**	Show the contents in the current directory
DES-7210# **dir** *directory*	Show the contents in the specified directory

The following example shows the contents of the current directory and specified directory:

```
DES-7210# dir
DES-7210# dir ../bak
```

64.2.5 Formating the System

In the privileged mode, format the device to be managed and operated by the file system by using the following command:

Command	Function
DES-7210# **makefs dev** *devname* **fs** *fs_name*	Format the device named dev for the file system named **fs_name**

The following example formats the first MTD device in the dev directory for use by the jffs2 file system:

```
DES-7210# makefs dev /dev/mtd/mtdblock/1 fs jffs2
```

The above example formats a device in the mtdlbock directory for the jffs2 file system, clearing the data on the device for use by the file system.

64.2.6 Creating Directories

In the privileged mode, create the needed directory at the specified location by performing the following steps:

Command	Function
DES-7210# **mkdir** *directoryname*	Create directories

The following example creates a bak directory in the root directory:

```
DES-7210# mkdir bak
```

64.2.7 Moving Files

In the privileged mode, move the specified files to the specified directory:

Command	Function
DES-7210# **rename flash:** *old_filename* **flash**: *new_filename*	Name the file named as *old_filename* to *new_filename*.

64.2.8 Showing the Current Working Path

In the privileged mode, show the current working path by performing the following steps:

Command	Function
DES-7210# **pwd**	Show the current working paths

64.2.9 Removing Files

In the privileged mode, delete a file permanently by performing the following step:

Command	Function
DES-7210# **del** *filename*	Delete the specified file.

The following example deletes the temporary file named large.c in the mnt directory:

```
DES-7210# del mnt/large.c
```

64.2.10 Deleting Empty Directories

In the privileged mode, delete an empty directory permanently by performing the following step:

Command	Function
DES-7210# **rmdir** *directoryname*	Delete an empty directory

The above example deletes an empty directory named MNT.

```
DES-7210# rmdir mnt
```

65 System Memory Display Configuration

65.1 System Memory Display Configuration Task List

- Show the usage of system memory
- Configure the memory-lack exit-policy
- Show the usage of the protocol memory

65.2 Showing the Usage of System Memory

Use the **show memory** command to show the usage and status of system memory:

Command	Function
DES-7210# **show memory**	Show the usage of system memory.

By default, the switch name is DES-7210.

Below is the result of executing this command:

```
DES-7210#show memory
System Memory Statistic:
  Free pages: 13031
  watermarks : min 378, lower 756, low 1534, high 1912
  System Total Memory : 128MB, Current Free Memory : 54892KB
  Used Rate : 58%
```

The above information includes the following parts:

1. Free pages: the memory size of one free page is about 4k;

2. Watermarks(see the following table)

Parameter	Description
min	The memory resources are extremely insufficient. It can only keep the kernel running. All application modules fails to run if the minimum watermark has been reached.
lower	The memory resources are severely insufficient. One route protocol will auto-exit and release the memory if the lower watermark has been reached. For the details, see the **memory-lack exit-policy** command.

Parameter	Description
low	The memory resources are insufficient. The route protocol will be in OVERFLOW state if the low watermark has been reached. In the overflow state, the routers do not learn new routes any more. The commands are not allowed to be executed when the memory lacks.
high	A plenty of memory resources. Each route protocol attempts to restore the state from OVERFLOW to normal.

3. System total memory, current free memory and used rate.

65.3 Configuring the memory-lack exit-policy

Use the **memory-lack exit-policy** command to configure the exit policy of the route protocol if the lower watermark has been reached. The route protocol includes BGP, OSPF, RIP, PIM-SM.

memory-lack exit-policy [**bgp**|**ospf**|**pim-sm**|**rip]**

Command	Function
DES-7210(config)# **memory-lack exit-policy** [**bgp**|**ospf**|**pim-sm**|**rip**]	Configure the exit policy of the route protocol if the lower watermark has been reached.

Use the **no memory-lack exit-policy** command to restore the default configuration. By default, if the memory size reaches the lower watermark, the protocol that occupies the most memory exits.

If the system free memory decreases to the lower watermark, the system will disable one route protocol, releasing the memory resources to ensure the normal operation of other protocols.

You shall know what route protocols support the major network service. If the memory resources lack, you can disable the most unimportant protocol to ensure the normal operation of the major services.

For example, in a user network, the routes BGP learned are irrelevant to the major network service, you can use the **memory-lack exit-policy bgp** command.

Specifying the disabled route protocol as the exit policy can not help the system obtain enough memory resources.

65.4 Showing the usage of the protocol memory

Use the **show memory protocol** command to display the usage of the memory protocol.

Command	Function

Below is the result of executing this command:

```
DES-7210# show memory protocols

================================

protocol      |memory(byte)

BGP            102000000

OSPF           24000000

RIP            10000000
```

```
PIM             50000000
LDP             20000000
Total           206000000
```

Caution

Different switches support different routing protocols, including BGP OSPF RIP LDP PIM ISIS, ect.

66 System Management Configuration

66.1 System Management Configuration Task List

- Show CPU utilization
- Configure CPU logging trigger threshold

66.2 Showing CPU Utilization

Use the **show cpu** command to show the total CPU utilization and the CPU utilization per process:

Command	Function
DES-7210# **show cpu**	Show CPU utilization.

By default, the switch name is DES-7210.

Below is the result of executing this command:

```
DES-7210#show cpu
 ======================================
     CPU Using Rate Information
 CPU utilization in five seconds: 25%
 CPU utilization in one minute  : 20%
 CPU utilization in five minutes: 10%
   NO   5Sec   1Min   5Min   Process
   0     0%     0%     0%    LISR INT
   1     7%     2%     1%    HISR INT
   2     0%     0%     0%    ktimer
   3     0%     0%     0%    atimer
   4     0%     0%     0%    printk_task
   5     0%     0%     0%    waitqueue_process
   6     0%     0%     0%    tasklet_task
   7     0%     0%     0%    kevents
   8     0%     0%     0%    snmpd
   9     0%     0%     0%    snmp_trapd
  10     0%     0%     0%    mtdblock
  11     0%     0%     0%    gc_task
  12     0%     0%     0%    Context
  13     0%     0%     0%    kswapd
  14     0%     0%     0%    bdflush
  15     0%     0%     0%    kupdate
  16     0%     3%     1%    ll_mt
  17     0%     0%     0%    ll main process
  18     0%     0%     0%    bridge_relay
  19     0%     0%     0%    d1x_task
  20     0%     0%     0%    secu_policy_task
  21     0%     0%     0%    dhcpa_task
  22     0%     0%     0%    dhcpsnp_task
  23     0%     0%     0%    igmp_snp
  24     0%     0%     0%    mstp_event
```

```
25    0%    0%    0%   GVRP_EVENT
26    0%    0%    0%   rldp_task
27    0%    2%    1%   rerp_task
28    0%    0%    0%   reup_event_handler
29    0%    0%    0%   tpp_task
30    0%    0%    0%   ip6timer
31    0%    0%    0%   rtadvd
32    0%    0%    0%   tnet6
33    2%    0%    0%   tnet
34    0%    0%    0%   Tarptime
35    0%    0%    0%   gra_arp
36    0%    0%    0%   Ttcptimer
37    8%    1%    0%   ef_res
38    0%    0%    0%   ef_rcv_msg
39    0%    0%    0%   ef_inconsistent_daemon
40    0%    0%    0%   ip6_tunnel_rcv_pkt
41    0%    0%    0%   res6t
42    0%    0%    0%   tunrt6
43    0%    0%    0%   ef6_rcv_msg
44    0%    0%    0%   ef6_inconsistent_daemon
45    0%    0%    0%   imid
46    0%    0%    0%   nsmd
47    0%    0%    0%   ripd
48    0%    0%    0%   ripngd
49    0%    0%    0%   ospfd
50    0%    0%    0%   ospf6d
51    0%    0%    0%   bgpd
52    0%    0%    0%   pimd
53    0%    0%    0%   pim6d
54    0%    0%    0%   pdmd
55    0%    0%    0%   dvmrpd
56    0%    0%    0%   vty_connect
57    0%    0%    0%   aaa_task
58    0%    0%    0%   Tlogtrap
59    0%    0%    0%   dhcp6c
60    0%    0%    0%   sntp_recv_task
61    0%    0%    0%   ntp_task
62    0%    0%    0%   sla_deamon
63    0%    3%    1%   track_daemon
64    0%    0%    0%   pbr_guard
65    0%    0%    0%   vrrpd
66    0%    0%    0%   psnpd
67    0%    0%    0%   igsnpd
68    0%    0%    0%   coa_recv
69    0%    0%    0%   co_oper
70    0%    0%    0%   co_mac
71    0%    0%    0%   radius_task
72    0%    0%    0%   tac+_acct_task
73    0%    0%    0%   tac+_task
74    0%    0%    0%   dhcpd_task
75    0%    0%    0%   dhcps_task
76    0%    0%    0%   dhcpping_task
77    0%    0%    0%   dhcpc_task
78    0%    0%    0%   uart_debug_file_task
79    0%    0%    0%   ssp_init_task
80    0%    0%    0%   rl_listen
81    0%    0%    0%   ikl_msg_operate_thread
82    0%    0%    0%   bcmDPC
83    0%    0%    0%   bcmL2X.0
84    3%    3%    3%   bcmL2X.0
85    0%    0%    0%   bcmCNTR.0
86    0%    0%    0%   bcmTX
87    0%    0%    0%   bcmXGS3AsyncTX
88    0%    2%    1%   bcmLINK.0
89    0%    0%    0%   bcmRX
90    0%    0%    0%   mngpkt_rcv_thread
91    0%    0%    0%   mngpkt_recycle_thread
92    0%    0%    0%   stack_task
93    0%    0%    0%   stack_disc_task
94    0%    0%    0%   redun_sync_task
95    0%    0%    0%   conf_dispatch_task
96    0%    0%    0%   devprob_task
97    0%    0%    0%   rdp_snd_thread
98    0%    0%    0%   rdp_rcv_thread
99    0%    0%    0%   rdp_slot_change_thread
```

```
 100     4%     2%     1%    datapkt_rcv_thread
 101     0%     0%     0%    keepalive_link_notify
 102     0%     0%     0%    rerp_msg_recv_thread
 103     0%     0%     0%    ip_scan_guard_task
 104     0%     0%     0%    ssp_ipmc_hit_task
 105     0%     0%     0%    ssp_ipmc_trap_task
 106     0%     0%     0%    hw_err_snd_task
 107     0%     0%     0%    rerp_packet_send_task
 108     0%     0%     0%    idle_vlan_proc_thread
 109     0%     0%     0%    cmic_pause_detect
 110     1%     1%     1%    stat_get_and_send
 111     0%     1%     0%    rl_con
 112    75%    80%    90%    idle
```

As shown in the above, the first three lines indicate the total CPU utilization in the last 5 seconds, 1 minute and 5 minutes respectively, including LISR, HISR and task. Below detains CPU utilization, where:

- No: number
- 5Sec: CPU utilization in the last 5 seconds
- 1Min: CPU utilization in the last 1 minute
- 5Min: CPU utilization in the last 5 minutes
- Process: process name

The first two lines indicate the CPU utilization of all LISRs and the CPU utilization of all HISRs respectively. All the lines starting the third line indicate the CPU utilization of processes. The last line indicates the CPU utilization of idle process. As with System Idle Process under Windows, it indicates an idle status. The above example shows that the CPU utilization of idle processes in the last 5 seconds is 75%, meaning that 75% CPU is available.

66.3 Configuring CPU Logging Trigger Threshold

To configure the CPU logging trigger threshold, execute the following command:

Command	Function
cpu-log log-limit *low_num high_num*	Configure the CPU logging trigger threshold.

By default the upper threshold is 100% and the lower threshold is 90%.

The following example sets the lower threshold to 70% and the higher threshold to 80%:

```
DES-7210# configure terminal                    // Enter the global configuration mode

DES-7210(config)# cpu-log log-limit 70 80    // Configure the CPU logging trigger threshold
```

If the CPU utilization is higher than 80%, the system prompts:

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU utilization in one minute : 95%  Using most
cpu's task is ktimer : 94%
```

If the CPU utilization is lower than 70%, the system prompts:

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU utilization in one minute :68%  Using most cpu's
task is ktimer : 60%

Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: The CPU using rate has down!
```

67 Syslog Configuration

67.1 Overview

During the operation of a device, there are various state changes, such as the link status up/down, and various events occurring, such as receiving abnormal messages and handling abnormities. Our product provides a mechanism to generate messages of fixed format (log message) in case of status change or event occurring. These messages can be displayed in related windows (console, VTY, etc.) or recorded in related media (memory buffer, FLASH), or sent to a group of log servers in the network for the administrators to analyze and locate problems.Meanwhile, in order to make it easy for administrators to read and manage log messages, these log messages can be labeled time stamps and serial numbers, and is graded according to the priority of log information.

67.1.1 Log Message Format

The format of the our log message is as follows:

<priority> seq no: timestamp sysname: %severity

%ModuleName-severity-MNEMONIC: description

They are: <priority> Sequential number timestamp device name module name-severity – information type: abbre: information contents

Priority value = Device value *8 + Severity

For example:

```
<189> 226:Mar  5 02:09:10 DES-7210 %SYS-5-CONFIG_I: Configured from console by console
```

Caution

The priority field is not attached to the log messages that are printed in the user window. It only appears in the log messages that are sent to the syslog server.

67.2 Log Configuration

67.2.1 Log Switch

The log switch is turned on by default. If it is turned off, the device will not print log information in the user window, or send log information to the syslog server, or record the log information in the related media (memory buffer, flash).

To turn on or off the log switch, run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **logging on**	Turn on the log switch
DES-7210(config)# **no logging on**	Turn off the log switch


Caution

Do not turn off the log switch in general case. If it prints too much information, you can reduce it by setting different displaying levels for device log information.

67.2.2 Configuring the Device Displaying the Log Information

When the log switch is turned on, the log information will be displayed on the console and also sent to different displaying devices. To configure different displaying devices for receiving logs, run the following commands in the global configuration mode or privileged level:

Command	Function
DES-7210(config)# **logging buffered** [*buffer-size* | *level*]	Record log in memory buffer
DES-7210# **termninal monitor**	Allow log to be displayed on VTY window
DES-7210(config)# **logging** *host*	Send log information to the syslog sever in the network
DES-7210(config)# **logging file flash:***filename* [*max-file-size*] [*level*]	Record log on extended FLASH

Logging Buffered will record log information in the memory buffer. The memory buffer for log is used in recycled manner. That is, when it is full, the oldest information will be overwritten. To show the log information in the memory buffer, run **show logging** at the privileged user level. To clear the log information in the memory buffer, run **clear logging** at the privileged user level.

Terminal Monitor allows log information to be displayed on the current VTY (such as the telnet window).

Logging Host specifies the address of the syslog server that will receive the log information. Our product allows the configuration of at most 5 syslog servers. The log information will be sent to all the syslog servers at the same time.


Caution

To send the log information to the syslog server, it is required to turn on the timestamp switch or sequential number switch of the log information. Otherwise, log information will not be sent to the syslog server.

Logging File Flash: Record log information in FLASH. The filename for log shall not have any extension to indicate the file type. The extension of the log file is fixed as txt. Any configuration of extension for the filename will be refused.

More flash: filename command shows the contents of the log file in the flash.


Caution

Some devices support extended FLASH. If the device has extended FLASH, the log information will be recorded there. If the device has no extended FLASH, the log information will be recorded in the serial FLASH.

67.2.3 Enabling the Log Timestamp Switch of Log Information

To add or delete timestamp in log information, run the following command in the global configuration mode:

Command	Function

Command	Function
DES-7210(config)# **service timestamps** *message-type* [**uptime** | **datetime**]	Enable the timestamp in the log information
DES-7210(config)# **no service timestamps** *message-type*	Disable the timestamp in the log information

The timestamp are available in two formats: device uptime and device datetime. Select the type of timestamp appropriately.

Message type: log or debug. The "log" type means the log information with severity levels 0-6. The "debug" type means that with severity level 7.

Caution

If the current device has no RTC, the configured time is invalid, and the device automatically uses the startup time as the timestamp for the log information.

67.2.4 Enabling Switches in Log System

By default, the system name is not included in the log information. To add or remove the system name in the log information, perform the following commands in the global configuration mode.

Command	Function
DES-7210(config)# **no service sysname**	Cancel the system name in the log message.
DES-7210(config)# **service sysname**	Add the system name to the log message.

67.2.5 Enabling Log Statistics

By default, the log statistics function is disabled. To enable or disable the log statistics function, perform the following commands in the global configuration mode.

Command	Function
DES-7210(config)# **no logging count**	Disable the log statistics function and delete the statistics information
DES-7210(config)# **logging count**	Enable the log statistics function

67.2.6 Enabling the Sequential Number Switch of Log Information

By default, the log information has no sequential number. To add or delete sequential number in log information, run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **no service sequence-numbers**	Delete sequential number in the log messages
DES-7210(config)# **service sequence-numbers**	Add sequential number to the log messages

67.2.7 Configuring Synchronization Between User Input and Log Output

By default, user input is asynchronous with log output. User input is interrupted if the log is output when the user is keying in characters. Use this command to configure synchronization between user input and log output in the line configuration mode:

Command	Function
DES-7210(config-line)# **logging synchronous**	Set synchronization between user input and log output.
DES-7210(config)# **no logging synchronous**	Delete synchronization between user input and log output.

67.2.8 Configuring Log Rate Limit

By default, log rate is not limited. Use this command to configure log rate limit in the global configuration mode:

Command	Function
DES-7210(config)# **logging rate-limit** *number*	Set log rate limit.
DES-7210(config)# **no logging rate-limit**	Delete the setting of log rate limit.

67.2.9 Configuring the Log Information Displaying Level

To limit the number of log messages displayed on different devices, it is possible to set the severity level of log information that is allowed to be displayed on those devices.

To configure the log information displaying level, run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **logging console** *level*	Set the level of log information that is allowed to be displayed on the console
DES-7210(config)# **logging monitor** *level*	Set the level of log information that is allowed to be displayed on the VTY window (such as telnet window)
DES-7210(config)# **logging buffered** [*buffer-size* | *level*]	Set the level of log information that is allowed to be recorded in memory buffer
DES-7210(config)# **logging file flash:***filename* [*max-file-size*] [*level*]	Set the level of log information that is allowed to be recorded in extended flash
DES-7210(config)# **logging trap** *level*	Set the level of log information that is allowed to be sent to syslog server

The log information of our products is classified into the following 8 levels:

Level Keyword	Level	Description
Emergencies	0	Emergency case, system cannot run normally
Alerts	1	Problems that need immediate remedy
Critical	2	Critical conditions
Errors	3	Error message
Warnings	4	Alarm information
Notifications	5	Information that is normal but needs attention
Informational	6	Descriptive information

Level Keyword	Level	Description
Debugging	7	Debugging messages

Lower value indicates higher level. That is, level 0 indicates the information of the highest level.

When the level of log information that can be displayed is set for the specified device, the log information that is at or below the set level will be displayed. For example, after the command logging console 6 is executed, all log information at or below level 6 will be displayed on the console.

By default, the log information that is allowed to be displayed on the console is at level 7.

By default, the log information that is allowed to be displayed on the VTY window is at level 7.

By default, the log information that is allowed to be sent to the syslog server is at level 6.

By default, the log information that is allowed to be recorded in the memory buffer is at level 7.

By default, the log information that is allowed to be recorded in the extended flash is at level 6.

The privileged command show logging can be used to show the level of log information allowed to be displayed on different devices.

67.2.10 Configuring the log information device value

The device value is one of the parts that form the priority field in the messages sent to the syslog server, indicating the type of device that generates the information.

To configure the log information device value, run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **logging facility** *facility-type*	Configure the log information device value
DES-7210(config)# **no logging facility** *facility-type*	Restore the default of the log information device value

The meanings of various device values are described as below:

```
Numerical Code       Facility
         0           kernel messages
         1           user-level messages
         2           mail system
         3           system daemons
         4           security/authorization messages
         5           messages generated internally by syslogd
         6           line printer subsystem
         7           network news subsystem
         8           UUCP subsystem
         9           clock daemon
        10           security/authorization messages
        11           FTP daemon
        12           NTP subsystem
        13           log audit
        14           log alert
        15           clock daemon
        16           local use 0  (local0)
```

```
17          local use 1  (local1)
18          local use 2  (local2)
19          local use 3  (local3)
20          local use 4  (local4)
21          local use 5  (local5)
22          local use 6  (local6)
23          local use 7  (local7)
```

The default device value of our products is 23.

67.2.11 Configuring the Source Address of Log Messages

By default, the source address of the log messages sent to the syslog server is the address of the port that sends the messages. It is possible to fix the source address for all log messages through commands.

It is possible to directly set the source IP address of the log messages or the remote port of the log messages.

To configure the source address of the log messages, run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **logging source interface** *interface-type interface-number*	Configure the source port of log information
DES-7210(config)# **logging source ip** *A.B.C.D*	Configure the source IP address of log messages

67.2.12 Setting and Sending User Log

By default, no log is output when a user logs in or out and executes configuration commands. To output user login/logoff logs or configuration command logs, execute the following commands in the global configuration mode:

Command	Function
DES-7210(config)# **logging userinfo**	Set user login/logoff log.
DES-7210(config)# **logging userinfo command-log**	Send a log when a configuration command is executed

67.3 Log Monitoring

To monitor log information, run the following commands in the privileged user mode:

Command	Function
DES-7210# **show logging**	View the log messages in memory buffer as well as the statistical information of logs
DES-7210# **show logging count**	View the statistical information of logs in every modules
DES-7210# **clear logging**	Clear the log messages in the memory buffer
DES-7210# **more flash:***filename*	View the log files in the extended flash

Caution

The format of the timestamp in the output result of **show logging count** is the format in the latest log output.

67.3.1 Examples of Log Configurations

Here is a typical example to enable the logging function:

```
DES-7210(config)# interface gigabitEthernet 0/1
DES-7210(config-if)# ip address 192.168.200.42 255.255.255.0
DES-7210(config-if)# exit
DES-7210(config)# service sequence-numbers                //Enable sequence number
DES-7210(config)# service timestamps debug datetime     //Enable debug information timestamp,
in date format
DES-7210(config)# service timestamps log datetime        //Enable log information timestamp,
in date format
DES-7210(config)# logging 192.168.200.2                  //Specify the syslog server address
logging trap debugging                                   //The log information of all levels
will be sent to syslog server
DES-7210(config)# end
```

68 Module Hot-Plugging/ Unplugging

68.1 Overview

Caution

The DES-7200 series switches support hot-plugging/unplugging of modules. You may plug and unplug modules while the device is powered on, without affecting the normal system operation or other modules.

68.2 Module Hot-Plugging/Unplugging Configuration

This chapter includes:

- Plugging or Unplugging Modules
- Installing or Uninstalling Modules
- View module information

68.2.1 Plugging or Unplugging Modules

You may plug or unplug modules while the device is operating (hot-plugging/unplugging). The operation of the other modules will not be affected. After the module is plugged in the slot, the management software of the device attempts to install its driver.

Caution

If the slot has been installed with another module driver, it is required to delete the original driver before installing the new module. You may execute the **show version module** command to get the related information.

Please plug the module tightly in the slot and tighten the screw. The module may not work well if it is loosely plugged.

You may plug modules while the switch is operating (hot-plugging/unplugging), which will not affect the operation of the other modules. The related configuration will be reserved when the module is unplugged, and it is possible to continue the setting of the module. When the module is re-plugged, the module will be automatically activated. All the configurations take effect automatically.

68.2.2 Installing or Uninstalling Modules

In addition to automatic installation of module driver after the module is plugged, you may also install the module driver manually. After the installation, all configurations for the slot will be done for

the type of the installed module. Even if the module is unplugged, you can still configure it without loss of the configuration.

In the global configuration mode, execute the following commands to install a module manually:

Command	Meaning
configure terminal	Enter the global configuration mode.
install *slot-num moduletype*	Install the module of a specified type in a slot
end	Return to the privileged mode.

Caution

The installation of driver does not need physical presence of the module. This means that you may "pre-configure" the device. You may use the **install** command to virtualize the module of a specified type and then configure it. When the module is plugged, all configurations take effect automatically.

You can uninstall an operating module. Once uninstalled, all configurations for it will be lost, and the module is disabled. To restore that module, you may "install" its driver manually, or unplug and then plug it again.

In the global configuration mode, execute the following commands to uninstall a module manually:

Command	Meaning
configure terminal	Enter the global configuration mode.
no install *slot-num*	Uninstall the module in a slot
End	Return to the privileged mode.

68.2.3 Viewing module information

In the privileged user mode, execute the following commands to check the details of a module so as to uninstall it manually:

Command	Meaning
show version module detail	View module information

```
DES-7210# show version module detail
Device  : 1
Slot    : 1
User Status:     installed
Software Status: ok
Online Module :
       Type    : 7200-24G
       Ports   : 24
       Version : 01-01-05-02
Configured Module :
    Type    : 7200-24GE
    Ports   : 24
    Version : 01-01-05-02

Device  : 1
Slot    : 2
User Status:     installed
Software Status: ok
Online Module :
```

```
   Type    : 7200-2XG
    Ports   : 2
    Version : 01-01-05-02
Configured Module :
    Type    : 7200-2XG
    Ports   : 2
    Version : 01-01-05-02

Device  : 1
Slot    : 3
User Status:     installed
Software Status: ok
Online Module :
Type    : 7200-24
    Ports   : 24
    Version : 01-01-05-02
Configured Module :
    Type    : 7200-24
    Ports   : 24
    Version : 01-01-05-02

Device  : 1
Slot    : 4
User Status:     installed
    Software Status:  none
    Online Module :
    Type    :
    Ports   : 0
    Version :
    Configured Module :
    Type    : 7200-24
    Ports   : 24
    Version :
    Device  : 1
    Slot    : M1
    Status  : master
    Online Module :
    Type    : 7200-CM1
    Ports   : 0
    Version : 01-01-05-02
```

69 LCD Configuration

69.1 Overview

The LCD display is a visual display that features simple and easy operation with buttons. The user can know the running status of the device at a glance even if the user has no knowledge about the CLI commands. When abnormity occurs with the device operation, the displaying immediately notifies the abnormity to the users.

The state information shown by the LCD includes the switch name, duration of work, CPU utilization ratio (Supervisor Engine), memory utilization ratio (Supervisor Engine), temperature (Supervisor Engine and Line Card), fan and the working state of power supplies.

Generally, the device prints the information circularly.

A user can use keys to show desired state information. The LCD provides the following four key:

- Menu key (Menu): Show a menu.
- Selection key (Enter): Select an item.
- Page Up key (Pgup): Page up.
- Page Down key (Pgdn): Page down,

When there is an unexpected condition in a module, for example, the CPU utilization ratio is too high, and then the LCD keeps showing the warning information. The information will not disappear from the display until the user pushes the selection key (enter).

69.1.1 LCD Key Introduction

When the switch prints state information circularly, each page displays for a fixed period. If a user pushes one of the four keys, then the following condition will occur.

1. Menu: Stop the current displaying and show the main menu. Stops showing the menu and shows the state beginning at this page.
2. Selection key (enter): The key does not work.
3. Page Up key (Pgup): Shows the content of the previous screen. If the information of a state is not fully shown in one screen, then it can be shown in multiple screens. If the first screen is not currently shown, then push the key Pgup to show the previous screen of the current content. If the first screen is shown, then push the key Pgup to show the last screen of the state information.
4. Page Down key (Pgdn): Shows the content of next screen. If the information of a state is not fully shown in one screen, then it can be shown in multiple screens. If the last screen is not currently shown, then push the key Pgdn to show the next screen of the current content. If the last screen is shown, then push the key Pgdn to show the first screen of the state information.

Press Menu to show the main menu, and the selected line will be highlighted. If there is no button pressing operation, it returns to the circular displaying again and display the next screen since the previous displaying. If a key is pressed, the following condition may occur:

1. Menu: Stop the current displaying and show the main menu.

2. Selection key (enter): Select the currently selected menu item. If there is a submenu in the menu item, then the submenu is shown. If a menu item indicates the information of a state, then the state information is shown.
3. Page Up key (Pgup): Shows the content of the previous screen.

All the menu items of a menu page are circularly organized. The previous item of the first menu item is the last item. The next item of the last item is the first item. If a menu is currently shown and the selected menu is not in the first line of the screen, when you push the Pgup key, the content of the screen will not change, the selected menu item will move up a line and the selected line is still the first line.

The state information that menu items point to are also circularly organized. The previous screen of the first screen is the last screen and the next screen of the last screen is the first screen. If the content of a menu item is currently shown, then Pgup shows the content of the previous screen. When the content of a menu item is shown, push the key enter to return to the menu page.

4. Page Down key (Pgdn): Shows the content of next screen.

If a menu is currently shown and the selected menu is not in the last line of the screen, when you push the Pgdn key, the content of the screen will not change, the selected menu item will move down a line and the selected line is still the last line.

If the content of a menu item is currently shown, then Pgdn shows the content of the next screen. When the content of a menu item is shown, push the key enter to return to the menu page.

If warning messages are required to be shown in the LCD, then the display shows generated warning messages. If a warning message needs being shown in multiple screens, then the display shows the content of the warning message in screens circularly. If multiple warning messages are generated at the same time, then various warning messages are shown in turn and then the content of the newest warning message is shown circularly. The condition will not end until the user types the selection key (enter) to stop showing the warning message. If you push one of the four keys when a warning is shown, the following condition will occur:

1. Menu key (Menu): Stops showing the warning message and begins to show the main mp
2. Selection key (enter): Stops showing the current warning message. If there is no updated warning message, then returns to the circular display mode. If there is an updated warning message, the new warning message is shown.
3. Page Up key (Pgup): All the warning messages are circularly organized. The previous screen of the first screen is the last screen of the previous warning message. The next screen of the last screen is the first item of the next warning message. Pgup shows the content of the previous screen. If the first screen of the first warning message is currently shown, the shown content will not change.
4. Page Down key (Pgdn): Warning messages are circularly organized. Pgdn shows the content of the next screen. If the last screen of the last warning message is currently shown, the shown content will not change.

69.2 LCD Configuration Task List

69.2.1 Configuring Warning Information Queue Length

After a warning message is generated, the LCD keeps showing the latest warning message until a user pushes the key Enter. The user can browse history warning messages through menu items after pushing the key Enter. The command can be used to configure the length of a warning message.

The current version of our products saves 100 history warning messages by default. To configure the length of a history warning message, run the following command in the global configuration mode:

Command	Function
DES-7210(config)# **lcd trap-number** *num*	Set a new length of a warning message
DES-7210(config)# **no lcd trap-number**	Restore to the default setting

69.3 LCD Configuration Instance

Use the following command to configure the length of a history warning message:

```
lcd trap-number 200   //Configure the length of a warning message to 200
```

Use the following commands to configure the memory thresholds:

```
memory-rate rising-threshold 60
```

70 USB Configuration

70.1 Overview

This chapter introduces the use of the USB storage (mostly the USB disk). The system can recognize the FAT-partitioned USB disk only and cannot recognize the other file systems.

When a USB disk is inserted, the system automatically loads the recognized partitions to the system. The operation on the USB disk is the same as normal directories.

70.2 Inserting the Device

Just insert the USB device into the USB slot without additional operations. If the system finds the device and loads its driver, the following prompts are printed:

```
0:1:18:57 DES-7210: %5:USB Device Found ..... <USB Mass Storage Device>!

0:1:18:57 DES-7210: %5:  Auto Mount Disk Partitions:

0:1:18:57DES-7210: %5:  * /dev/uba/disc0/part1 --> /mnt/uba    size : 131072000B(125MB)
```

`<USB Mass Storage Device>` is the name of the device found. The `/dev/uba/disc0/part1` is the device file of the partition. The `/mnt/uba` is the directory for the partition. The `"size"` means the partition size. In the example above, the USB disk has free space 125MB.

70.3 Using the Device

When the partition of the USB disk is loaded to the system, the commands of the file system (dir, copy, del, etc.) can be used to operate the USB disk. The operation below copies the files in the USB disk to the flash.

```
DES-7210# cd /mnt/uba    # Enter the USB disk partition

DES-7210# copy flash: a.txt flash: /b.txt  # Copy the file a.txt from the USB disk to the root
directory of the device.
```

Now, run " dir /" to see the file b.txt added into the flash.

Similar to other file operations, the partition of the USB disk is like a directory on the file system.

70.3.1 Formatting the partition

The system may format the partition by using the **makefs** command.

Command	Function
DES-7210#**makefs dev** *dev_file* **fs** *fs_name*	Format the partition of device file dev_file into a file system named fs_name.

For the above USB disk found, run the following command:

```
DES-7210#makefs dev /dev/uba/disc0/part1 fs vfat
```

Then the partition of the USB disk is reformatting into a FAT32 partition.

Caution

A USB disk supports only to be formatted into vfat.

70.3.2 Showing USB Device Information

Command	Function
DES-7210# **show usb**	Show the USB device information of the system

In the CLI command mode, use the **show usb** command to view the USB device information of the system. The displayed information is as follows:

```
DES-7210#sh usb
Device: USB Mass Storage Device :
ID: 778
Lun 0:
ID: 0
Disk Partitions:
1: /dev/uba/disc0/part1 --> /mnt/uba
size : 131072000B(125MB)
```

As shown above, "USB Mass Storage Device" is the device name.

"778" is the ID assigned by the system to the device, which is used when the device is to be uninstalled.

"Lun" is the logical unit number of the storage. Some devices have multiple logical units. The following ID is the one assigned by the system for the logical unit.

"Disk Partitions" shows the partition information of the logical unit. In the example above, there is one partition with device name /dev/uba/disc0/part1, loaded directory /mnt/uba, and size 125MB.

70.3.3 Unplugging USB Device

Before unplugging the USB device, run the CLI command to unload it first to prevent errors when the device is in use.

Command	Function
DES-7210# **usb remove** *device_ID*	Unload the USB device with ID Device_ID

After executing the unloading command, the system prints:

```
OK, now you can poll out the device 778.

0:1:1:38 DES-7210: %5:USB Device <USB Mass Storage Device> Removed!
```

Now it is ready to unplug the USB device.

Sometimes the device cannot be unloaded temporarily since it is in use, wait for a while, execute the command and unplug the device.

Caution

Be sure to unload the device first and then unplug the device to prevent the system error.

70.4 USB Faults

Following information will be printed:

```
0:1:2:34 DES-7210: USB-3-OHCI_ERR: USB1.0 controller is not available now.
```

In this case, the USB 1.0 controller is unavailable, but the U-disk 2.0 is usable. To use the U-disk of version 1.0, you need to reset the device.

Following information will be printed:

```
0:1:3:29 DES-7210: USB-3-EHCI_ERR: USB2.0 controller is not available now.
```

In this case, the USB 2.0 controller is unavailable, but the U-disk 1.0 is usable. To use the U-disk of version 1.0, you need to reset the device.

71 POE Management Configuration

71.1 Overview

PoE (Power Over Ethernet) is a mechanism that provides 45V~-57V DC to the remote PD devices (IP Phone, WLAN AP and Network Camera) via twisted pair cables.

The PSE (Power Sourcing Equipment) can transmit both data and current at the same time via Category 3/5 twisted pair cables (1, 3, 2, 6), with a maximum distance of 100m.

The switch supporting POE can provide the statistics of the power condition each port and the entire device, which can be shown by using a query command. At the same time, it also provides overtemperature protection. When the temperature inside the switch exceeds 80 Celsius degrees, the switch will trigger protection by turning off the PoE power supply to all ports. When the temperature inside the switch is lower than 60 Celsius degrees, the switch will restore the PoE power supply for all ports.

Caution

The POE line cards include 7200-48P, 7200-24P, etc.

71.2 POE Configuration Management

This section includes:

- Remote power supply configuration
- Enable/disable the remote power supply of the port
- Set the minimum allowed voltage of the POE system
- Set the maximum allowed voltage of the POE system
- Set the power management mode of the switch
- Disconnection detection mode
- Show the port/system status

71.2.1 Remote power supply configuration

The switch supporting POE can automatically detect whether the device connected to a port is a standard PD device and supply power to the standard PD device.

You can enable or turn off the remote power supply of a port, set the minimum allowed voltage of the POE system, set the maximum allowed voltage of the POE system, set the power management mode of the switch, and set the disconnection detection mode by using the command line.

Table-1: Remote Power Supply Configuration

Device	Configuration	Default	Description

Device	Configuration	Default	Description
Switches supporting PoE	Enable/disable the PoE of the port	Disabled	-
	Set the maximum power of the power supply for the port	15.4w	-
	Set the minimum allowed voltage of the POE system	45v	-
	Set the maximum allowed voltage of the POE system	57v	-
	Power management mode of the switch	Auto	-
	Disconnection detection mode	AC	-
PD device	Correct connection with the electrical interface of the POE device	-	-

71.2.2 Enabling/Disabling the PoE of the Port

You can enable or disable the PoE feature of a port as needed by using the following commands. By default, the PoE is disabled. Please do the following configuration in the global mode.

Table-2: Enable/Disable the PoE Feature of a Port

Step 1	**Configure**	Enter the configuration mode
Step 2	**interface gigabitEthernet** *interface-id*	Select the port, enter the interface configuration mode, and specify the physical port to be configured.
Step 3	**poe enable** | **no poe enable**	Enable/disable the PoE of a port
Step 4	**End**	Return to privileged EXEC mode
Step 5	**show run**	Verify the configuration
Step 6	**copy running-config startup-config**	Save the settings into the parameter file.

For example, enable/disable the PoE of port 1 on line card 1:

```
DES-7210#
DES-7210# configure
DES-7210 (config)#interface gigabitEthernet 1/1
DES-7210(config-if)# poe enable
DES-7210(config-if)# no poe enable
DES-7210(config-if)# end
DES-7210#
```

60.2.2 Setting the Minimum Allowed Voltage of the POE System

Currently, the Ethernet port of the switch supporting POE can provide the minimum allowed voltage of 45V. You can set the minimum allowed voltage according to the actual need, within the range of 45000 mv to 47000 mv. When the output voltage is lower than the minimum allowed value due to reasons such as power faults, the equipment will automatically turn off the power supply of the devices connected to all ports.

You can use the following commands to set the minimum allowed voltage of the power supply of the port. Please do the following configuration in the global mode.

Table-3: Set the Minimum Allowed Voltage of the POE System

Step 1	**Configure**	Enter the configuration mode

Step 2	**poe-power lower** *lower* | **no poe-power lower**	Set the minimum allowed voltage of the POE system/restore the minimum allowed voltage to the default value
Step 3	**End**	Return to privileged EXEC mode
Step 4	**show run**	Verify the configuration
Step 5	**copy running-config startup-config**	Save the settings into the parameter file.

By default, the minimum output power of a port is 45v.

For example, set the minimum output power of the system to 46v.

```
DES-7210#
DES-7210# configure
DES-7210 (config)#poe-power lower 46
DES-7210 (config)# end
DES-7210#
```

60.2.3 Setting the Maximum Allowed Voltage of the POE System

The Ethernet port of the switch supporting POE can provide the maximum allowed voltage of 57V. You can set the maximum allowed voltage according to the actual need, within the range of 55000 mv~57000 mv. When the output voltage is higher than the maximum allowed value due to reasons such as power faults, the equipment will automatically turn off the power supply of the devices connected to all ports.

You can use the following commands to set the maximum allowed voltage of the power supply of the port. Please do the following configuration in the global mode.

Table-4: Set the Maximum Allowed Voltage of the POE System

Command	Description
Configure	Enter the configuration mode
poe-power upper *upper* | **no poe-power upper**	Set the maximum allowed voltage of the POE system/restore the maximum allowed voltage to the default value
End	Return to privileged EXEC mode
show run	Verify the configuration
copy running-config startup-config	Save the settings into the parameter file.

By default, the maximum output power of a port is 57v.

For example, set the maximum output power of the system to 56v.

```
DES-7210#
DES-7210# configure
DES-7210 (config)#poe-power upper 56
DES-7210(config-if)# end
DES-7210#
```

60.2.4 Setting the Power Management Mode of the Switch

The power management mode of the switch is used to allocate the power to the PD devices. When one PD device is connected to the equipment if the current power allocated has not exceeded the

no_connect limit, the equipment will allocate power to the external PD device according to the power supply management mode. (POE has one limit: no_connect. When the power allocated from the equipment exceeds the no_connect limit, the equipment will not supply power to any new PD devices.)

Currently, the PoE device uses the auto power management mode.

In the Auto mode, the power is allocated according to the detected port PD type. In the Auto mode, the equipment allocates power to classes 1~3 PD devices as follows: class1~4W, class2~7W, class3~15.4W and class0~15.4W.

This configuration is automatically performed by the switch without any user intervention.

60.2.5 Disconnect Detection Mode

The equipment supporting POE checks whether a previously connected device has been disconnected by using disconnect detection. The equipment supports two detection modes: AC and DC. AC detection mode deems that the connected PD device is disconnected when the current of a port is smaller than a fixed value for the specified period. DC detection mode works by detecting the voltage feature of the port.

You can use the following command to set the disconnect detection mode. Please make the following configuration in the global mode. You can also set this mode for a particular device.

Table-5: Disconnect Detection Mode

Command	Description
Configure	Enter the configuration mode
Poe disconnect-mode {**ac** | **dc**} | **no poe disconnect-mode**	Set the disconnect detection mode/restore the disconnect detection mode to the default value
End	Return to privileged EXEC mode
show run	Verify the configuration
copy running-config startup-config	Save the settings into the parameter file.

By default, the disconnection detection mode is the AC mode.

For example, set the disconnect detection mode to DC:

```
DES-7210#
DES-7210# configure
DES-7210 (config)#poe-disconnect-mode dc
DES-7210(config-if)# end
DES-7210#
```

60.2.6 Showing the Power Supply Status of the Port/System

The equipment supporting POE will scan the ports and the status of the entire POE system at periodical intervals, and save all the status information. You may view interface status by using **show** in privileged EXEC mode.

Command	Description
show poe interfaces gigabitEthernet [*interface-id*]	Show the power supply status of the specified port
show poe interfaces	Show the power supply status of all POE ports (the 24 ports depending on the power supply of the POE system)

Command	Description
show poe powersupply	Show the power supply status of the entire POE system
show running-config interface [*interface-id*]	Show the configuration of the current running interface.

For example, show the power status of the gigabitethernet 0/2 port:

```
Interface : Gi0/2
Port power enabled : ENABLE
Port connect status : OFF
Port PD Class : no PD devices
Port max power : 15.4W
Port current power : 0 mW
Port peak power : 0 mW
Port current : 0 mA
Port voltage : 48V
Port trouble cause : normal
```

Note: Port trouble cause means the power-off cause, as below:

Port trouble cause	Description
Normal	Normal power supply (LED green); AC/DC detects that the equipment is disconnected (LED off), Disable (LED off)
Overload during start-up	Power supply start-up, finding that the current is too large or is disconnected (LED orange)
port off due to overload event	PD device is disconnected due to overload (LED orange)
short circuit event	PD device is disconnected due to short circuit (LED red)
voltage is out of established bounds	Output voltage is turned off due to out of bounds (LED red)
temperature rise too high	Turned off due to high-temperature protection (LED red)
power overload	Turned off due to power management (LED orange)

The following example shows the power supply status of the POE system:

```
DES-7210#show poe powersupply

PSE Total Power :1200.0 W
PSE Total Power Consumption : 0 W
PSE Available Power : 1200.0 W
PSE Peak Value : 0 W
PSE Min Allow Voltage : 45 V
PSE Max Allow Voltage : 57 V
PSE Disconnect Sense Mode : ac
```