DWR Series Wireless Mesh Router

CLI Configuration Guide

Version 2.6

Trademarks

Statement of Conditions
In the interest of improving internal design, operation function, and/or reliability, D-Link Corporation reserves the right to make changes to products described in this document without notice. D-Link Corporation does not assume any liability that may occur due to the use or application of the product(s) described herein.

CONTENTS

Chapter 1 About this Guide

This chapter covers the following topics:

Scope

This document provides the configuration instructions and examples for DWR series wireless mesh routers. It contains information on current features and protocols supported by DWR series.

Note: The command examples and outputs are created with an DWR-500 router and are for demonstration purposes only. The exact output of the commands may vary depending on the router model and its firmware version.

The scope of this document only includes the command-line interface of DWR series; for Web-based configuration, please see related documents.

Audience

This document is intended for system/IT or network administrator who is responsible for configuring or maintaining DWR series; this guide is also assumed the user is knowledgeable in wireless/wire Layer2 and Layer 3 networking technologies.

Related Documents

For more information about DWR series, please refer to the following documents:

- DWR series Web-based Configuration Guide

Chapter 2 Configuration Fundamentals

This section covers the following main topics:

- CLI Modes
- Basic configuration information
- Software Image Upgrade

CLI Modes

- CLI Modes
- The List Command
- CLI Navigation
- Deleting Command Lines in the Configuration
- Obtaining Help
- Entering and Editing Commands
- Filter Output

CLI Modes

The CLI is organized into multiple modes that allow navigation between different protocols and interface. Figure 1 displays the CLI modes and CLI structures that are available if you have full access to the CLI.

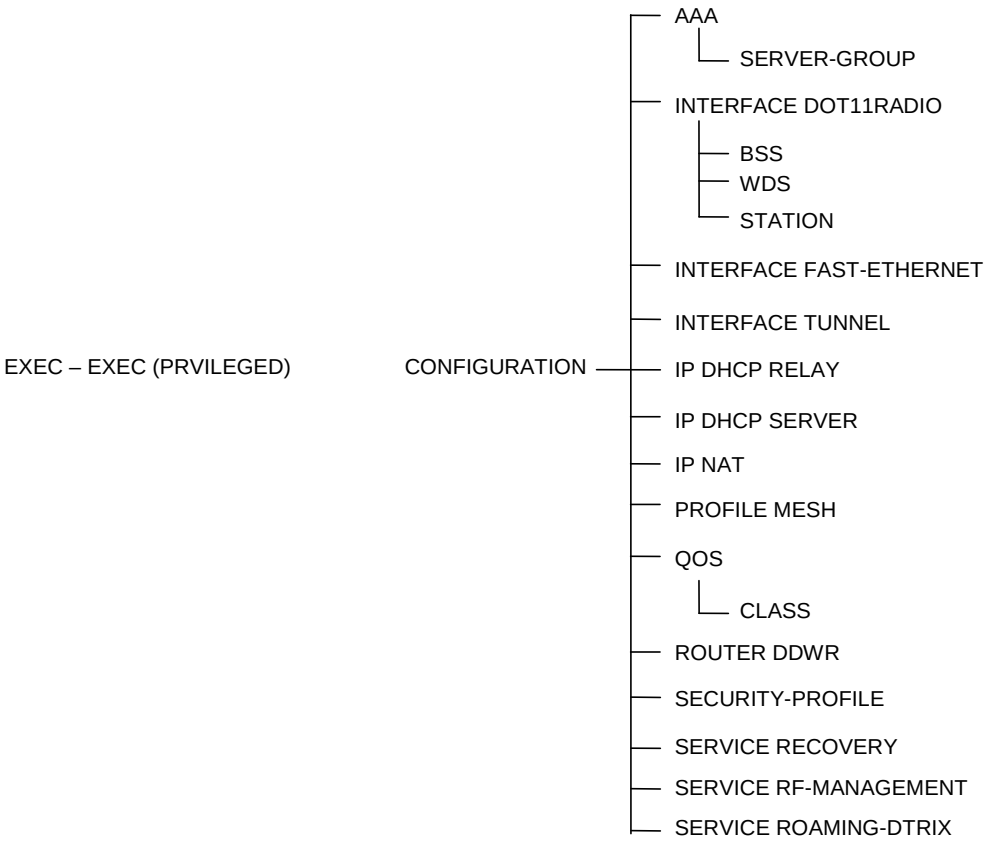


Figure 1 CLI Modes

When you login, you are in the User EXEC mode where you can enter a limited number of commands, mostly **show** commands. In this mode, you can not make or change any configuration. You can only view system information or execute limited commands. In EXEC mode, the **enable** command prompts you for your password to allow you into Privileged EXEC mode.

Privileged EXEC mode has commands to view configuration, manage configuration files, run diagnostics, enable or disable debug operations, reboot the router. By default, the privilege level is 15. To configure the router, use the **configure terminal** command to enter the CONFIGURATION mode.

CONFIGURATION mode enables you to configure security features, setup various service and SNMP functions, configure static route, and you can enter protocol, interfaces, and line CLI modes to configure setting, and save the configuration.

AAA mode enables you to configure Radius servers used by the router's security features.

INTERFACE DOT11RADIO mode enables you to configure wireless and IP-layer settings for each radio card.

INTERFACE FAST-ETHERNET mode enables you to configure layer-2 and layer-3 settings for each Ethernet port.

INTERFACE TUNNEL mode enables user to configure VPN Tunnel interface for each port.

INTERFACE VLAN mode enables user to configure vlan

IP DHCP RELAY mode enables you to configure the DHCP relay feature of the router. You may configure multiple DHCP Servers by IP address.

IP DHCP SERVER mode enables you to configure the built-in DHCP services provided by the router. You may configure the DNS, Domain name, lease time, etc.

IP NAT mode enables you to configure the NAT service for the router. You may configure choose an out-going network port to activate the NAT service on.

PROFILE MESH mode enables you to configure profiles containing mesh-specific settings. You may configure the mesh network ID in each profile.

QOS mode enables you to configure the Quality of Service (QoS) features provided by the router. You may define traffic classes and specify bandwidth control.

ROUTER DDWR mode enables you to configure the wireless routing protocol (DDWR). You may enable or disable the protocol.

SECURITY PROFILE mode enables you to configure security profiles to be used on the router. You may configure MAC, IP, and WPA2 profiles.

SERVICE RECOVERY mode enables you to configure the automatic fault recovery service provided by the router.

SERVICE RF-MANAGEMENT mode enables you to configure the intelligent radio-frequency management service provided by the router.

SERVICE ROAMING-DTRIX mode enables you to configure the Dtrix roaming service, MAC and IP address provided by the router.

VPN mode enables you to configure the PPTP client corresponding PPTP Server related configuration for DWR series routers.

OSPF mode enables you to configure the related OSPF routing services for DWR series routers.

AVT mode enables you to configure AVT services for DWR series routers.

The LIST Command

The LIST command allows a user to list all available commands for the current mode.

Table 1 List Command Information

Command Syntax	Command Mode	Purpose
List command	All **modes**	The **LIST** command lists all commands that may be entered in the current mode.

The following are examples of using the list command:

```
DWR-500(config)# interface fast-ethernet 0
DWR-500(config-if-ethernet)# list
  dhcp relay
  dhcp server POOL-NAME
  dhcp server automatic
  end
  exit
  help
  interface fast-ethernet <0-1>
  ip address A.B.C.D/M
  ip address dhcp
  list
  mode access
  mode gateway
  mode none
  mtu <256-1500>
  no dhcp
  no ip address
  no mode
  no mtu
  no shutdown
  no switchport
  quit
  show config
  show config | (grep|begin) PATTERN
  show running-config
  show running-config | (grep|begin) PATTERN
  shutdown
  switchport access vlan <1-4095>
  switchport trunk allowed-vlan WORD
  write memory
    write terminal
```

Figure 2 list Command Examples

CLI Navigation

To assist with navigation as you move among the CLI modes, the prompt changes to indicate the mode. Table 2 lists the CLI mode, its corresponding prompt, and information on how to access and exit this CLI mode.

Table 2 CLI Mode Information

CLI Command Mode	Prompt	To Enter Mode	To Exit mode
User EXEC	DWR-500>	Access the router through Telnet and successfully log in	User the **exit** commands.
PRIVILEGED EXEC	DWR-500#	From the User EXEC mode, use the **enable** command. From any other mode, use the **end** command.	Use the **exit** command.
CONFIGURATION	DWR-500(config)#	From the PRIVILEGED EXEC mode, use the **configure terminal** commands. From any other modes except the User	Use the either the **exit** or **end** command.

		EXEC and Privileged EXEC modes, use the **exit** command.	
AAA	DWR-500(config-aaa)#	From the CONFIGURATION mode, use the **aaa** command.	Use the **exit** commands to return to **CONFIGURATION** mode. Use the **end** to return to Privileged EXEC mode when in **bss, wds, station** and **class** mode.
SERVER-GROUP	DWR-500(config-aaa-server-group)#	From the AAA mode, use the **server-group** command.	
INTERFACE DOT11RADIO	DWR-500(config-if-dot11radio)#	From the CONFIGURATION mode, use the **interface dot11radoi** command.	
INTERFACE DOT11RADIO	DWR-500(config-if-dot11radio)#	From the CONFIGURATION mode, use the **interface dot11radoi** command.	
BSS	DWR-500(config-if-dot11radio-bss)#	From the INTERFACE DOT11RADIO mode, use the **bss** command.	
WDS	DWR-500(config-if-dot11radio-wds)# DWR-500(config-if-dot11radio-wds-auto)#	From the INTERFACE DOT11RADIO mode, use the **wds or wds auto** command.	
STATION	DWR-500(config-if-dot11radio-sta)#	From the INTERFACE DOT11RADIO mode, use the **station** command.	
INTERFACE FAST-ETHERNET	DWR-500(config-if-ethernet)#	From the CONFIGURATION mode, use the **interface fast-ethernet** command.	
INTERFACE TUNNEL	DWR-500(config-if-tunnel)#	From the CONFIGURATION mode, use the **ip dhcp relay** command.	
IP DHCP RELAY	DWR-500(config-dhcp-relay)#	From the CONFIGURATION mode, use the **ip dhcp server** command.	
IP DHCP SERVER	DWR-500(config-dhcp-server)#	From the CONFIGURATION mode, use the **ip nat** command.	
IP NAT	DWR-500(config-nat)#	From the CONFIGURATION mode, use the **profile mesh** command.	
PROFILE MESH	DWR-500(config-profile-mesh)#	From the CONFIGURATION mode, use the **qos** command.	
QOS	DWR-500(config-qos)#	From the QOS mode, use the **class <name>** command.	
CLASS	DWR-500(config-qos-class)#	From the QoS mode, use the **router DDWR** command.	
ROUTER DDWR	DWR-500(config-DDWR)#	From the CONFIGURATION mode, use the **security-profile** command.	
SECURITY PROFILE	DWR-500(config-security-profile)#	From the CONFIGURATION mode, use the **service recovery** command.	
SERVICE RECOVERY	DWR-500(config-recovery)#	From the CONFIGURATION mode, use the **service rf-management** command.	
SERVICE RF-MANAGEMENT	DWR-500(config-rfm)#	From the CONFIGURATION mode, use the **service roaming-Dtrix** command.	
SERVICE ROAMING-DTRIX	DWR-500(config-roaming)#	From the CONFIGURATION mode, use the **VPN PPTP Server** command.	
VPN PPTP SERVER	DWR-500 (config-pptp)#	From the CONFIGURATION mode, use the INTERFACE TUNNEL command.	
OSPF	DWR-500(config-ospf)#	From the CONFIGURATION mode, use the OSPF command.	
SERVICE AVT	DWR-500(config-avt)#	From the CONFIGURATION mode, use AVT command.	

Deleting Command Lines in the Configuration File

Each command enters a command line in the DWR series running configuration file and the “no” form of the command removes the command line form the running configuration file. To disable a command, use the “no” form of that command. The majority of the commands in the CLI have a “no” command that disables the command or re-enable a disabled function. For example, to delete a static route, use the **no** ip route *<IP destination prefix>* <*Gateway IP address*> command syntax. For both the command syntax and the “no” syntax, refer to *CLI Command Line Interface Reference.*

```
DWR-500(config)# no ip route 10.2.2.0/24 10.1.1.1
```

Figure 3 CLI Mode Information (no command)

Obtaining Help

CLI mode enables several ways for you to obtain help and list the available commands in that mode for a specific keyword.

To obtain a list of keywords and a brief functional description of those keywords at any CLI mode, do either of the following.

- Type **help** at the prompt
- Type **?** at the prompt or after a keyword.

Figure 4 illustrated the output that appears when you type **help** at any modes prompt. The output tells your how to use **?** to get help.

```
DWR-500(config)# help
When you need help,anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
 until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g. 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show me?'.)
```

Figure 4 Output of help command

Figure 5 illustrates the output that appears when you type **?** at the INTERFACE Ethernet mode prompt. All keywords are listed on the left with a brief description of the commands on the right.

```
DWR-500(config-if-ethernet)# ?
  dhcp       DHCP (Dynamic Host Configuration Protocol) method (server or relay) to assign IP addresses
  end        End current mode and return to privilege EXEC mode
  exit       Exit current mode and down to previous mode
  help       Description of the interactive help system
  interface  Select interface to operate
  ip         Interface Internet Protocol config commands
  list       Print command list
```

```
  mode       Set usage of this interface
  mtu        Set the interface's Maximum Transmission Unit (MTU)
  no         Negate a command or set its defaults
  quit       Exit current mode and down to previous mode
  show       Show running system information
  shutdown   Shutdown this interface
  write      Write running configuration to memory, network, or terminal
```

Figure 5 Example of ? command

To obtain a list of available options for a keyword or partial keyword, use the **?**. In figure 6, the keywords are listed on the left with a brief description of the commands on the right. The output is the same if you enter the **help.**

```
DWR-500(config)# snmp-server ?
  community  server read only or read write community string
  host       Set SNMP trap target ip
  v3user     Set SNMPv3 user
DWR-500(config)# snmp-server
```

Figure 6 Keyword ? Combination for the snmp-server Keyword

```
DWR-500(config)# s?          ← Enter a partial keyword, in the case "s" followed
  security-profile  Config security profile
  service           Configure a service
  show              Show running system information
  snmp-server       Set SNMP server read only or read write community string
DWR-500(config)# s
DWR-500(config)# sn?         ← Enter a partial keyword, in the case "sn" followed
  snmp-server                 immediately by a ?. All keywords that begin with
DWR-500(config)# snmp-sever   "sn" in the CONFIGURATION mode are listed.
```

Figure 7 Various Keyword Combinations

Entering and Edition Commands

- The CLI is case sensitive. All CLI commands MUST be in lower case.
- It is convenient to use the TAB key to complete keywords in commands. As long as the letters you type are unique to all available commands, it will auto-complete the commands.
- You can use the up arrow key to display the last enabled command syntax.
- You can use either the BACKSPACE key or DELETE key to erase the previous letter.

Table 3 lists the different key combinations available.

Table 3 Short-Cut Keys and their actions

Key Combinations	Action
CTRL-A	Moves the cursor to the beginning of the command line.
CTRL-B	Moves the cursor back on character.
CTRL-D	Deletes character at cursor.
CTRL-E	Moves the cursor to the end of the line.
CTRL-F	Moves the cursor forward one character.
CTRL-I	Completes a keyword.
CTRL-K	Deletes all characters form the cursor to the end of the command line.
CTRL-L	Re-enters the previous command.

CTRL-N	Return to more recent commands in the history buffer after recalling commands with CRTL-P or the up arrow key.
CTRL-P	Recalls commands, beginning with the last command.
CTRL-U	Deletes the line.
CTRL-W	Deletes the previous word.
CTRL-Z	Ends continuous scrolling of command output.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Esc D	Deletes all characters form the cursor to the end of the word.

Filter Output

Reduce outputs by configuring the filter rules. Support grey and begin mode.

- [Command] | grep mode

Output lines accord with certain mode

```
DWR-500config)# show running-config  | grep service
service recovery
service rf-management
service roaming-Dtrix
```

Figure 8 Grep Filter

- [Command] | begin mode

Output contents begin with certain mode

```
DWR-500config)# show running-config | begin qos
qos
 disable
 class DEFAULT
  maxbw 300
  minbw 50
!
```

Figure 9 Begin filter

Basic Configuration Information

This section provides information to configure your system to access the network or enable other hosts in your network after the initial system boot. Detailed feature or protocol configuration information is provided in subsequent chapters.

- System Information
- Host name configuration
- Root Password configuration
- Code Configuration
- Viewing configuration file information
- Setting CONFIGURATION mode parameters

System Information

When booting up the router, the system is pre-configured. User has to configure the router by using CLI commands to enable and manage the system.

Table 4 System Information for Initial Setup

System Information	Purpose
Hostname	Allows you to set the host name of the DWR series routers. Enter a new host name in the form of an alphanumeric string.
Router-password	Default password is **dlink**, it can be changed by using the router-password comand
Ethernet port IP address	IP address 192.168.0.1/24 is configured on FastEthernet 0 by default, and if FastEthernet 0 is configured to be the DHCP client mode, user can automatically get the address from DHCP server.
Node-id and router-id	Default node-id is 1 and router-id is 192.168.10.1; these must be set such that they are unique in a single mesh network formed by DWR series routers.
Country/Regulatory Domain Code	Default regulatory domain code is US by system. The configuration can be changed using this command

Host Name Configuration

The host name appears in the prompt. The default host name is DWR series. Names must start with a letter and end with a letter or digit. Characters within the string can be letters, digits, and hyphens.

To configure a host name, use the following command in the CONFIGUREATION mode:

Table 5 Configuring a host name

Command Syntax	Command Mode	Purpose
hostname <*name*>	CONFIGURATION	Set the host name of the DWR series. Enter a new host name in the form of a character string which must begin with the letters and the length should be no more than 32 characters.
no hostname		Remove the hostname, go back to default. Default hostname is DWR-500

Root Password Configuration

DWR series has a default password configured, the default password is dlink.

To configure the login password, configure the following command in the PRIVILEGED EXEC mode.

Table 6 Configuring login password

Command Syntax	Command Mode	Purpose
router-password root	PRIVILEGED EXEC	Change the login password for the user **root** command.

```
DWR-500# router-password root
Changing password for root
Enter new password:
```

```
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password:
Password changed.
```

Figure 10 Change the login password

Configuration Code

DWR series has setup a default country/regulatory domain code: US.
In PRIVILEGED EXEC mode, one can configure contry/regulatory domain code through the command below

Table 7 Configure Country/Regulatory Domain Code

Command Syntax	**Command Mode**	**purpose**
country-code (AU|CN|EU|IL|JP|KR|LA|NA|PS|SG|TW|US)	PRIVILEGED EXEC	Configure country/regulatory domain code manually
no country-code		Cancel the manual configured country/regularory domain code. Back to default: US

```
DWR-500(config)# country-code
 AU  Set code for Australia
  CN  Set code for China
  EU  Set code for Denmark, Germany, Iceland, Finland, Netherlands, Norway, Sweden, Poland, Slovenia, Luxembourg,
and South Africa
  IL  Set code for Israel
  JP  Set code for Japan
  KR  Set code for Korea
  LA  Set code for Latin America
  NA  Set code for North America (USA and Canada)
  PS  Set code for US Public Safety 4.9G
  SG  Set code for Singapore
  TW  Set code for Taiwan
  US  Set code for USA

DWR-500 (config)# country-code CN
% regulatory domain code will be set to 'CN' at the next router reboot.
% If any radio is configured to use a channel incompatible with the new regulatory domain code,
% it will be reset to the first legal channel of the configured mode.
```

Figure 11 Configure Regulatory Domain Code

Viewing Configuration File Information

It is highly recommended that you save your configuration often.

To save a configuration file, use either of the following commands in the Privileged EXEC mode:

Table 8 Save the running configuration to startup configuration

Command Syntax	Command Mode	Purpose
copy running-config startup-config	PRIVILEGED EXEC	Save the current running configuration to the startup-config file.
write memory	PRIVILEGED EXEC	Save the current running configuration to the startup-config file.

Use any of the following commands to display information about the configuration file:

Table 9 Display running configuration and startup configuration

Command Syntax	Command Mode	Purpose
show startup-config	PRIVILEGED EXEC	Displays the configuration information stored in the internal memory.
show running-config	PRIVILEGED EXEC	Displays current configuration information on the system.

Setting CONFIGURATION Mode Parameters

The configure command places you in the CONFIGURATION mode where you can configure interfaces and routing protocols.

From the CONFIGURATION mode, enter any of the following commands to configure protocols or interfaces:

Table 10 Some commands under configuration mode

Command Syntax	Command Mode	Purpose
node-id <1-8191>	CONFIGURATION	Set node ID, should be value between 1 and 8191.
router-id <A.B.C.D> **no router-id**	CONFIGURATION	Set router ID The format: A.B.C.D The ip address should be the loopback id of the router Generates a router-id associated with node-id.
Interface <*interface*>	CONFIGURATION	Configure a physical or logical interface on DWR series. 1.) dot11radio 2.) fast-ethernet 3.) vlan 4.) tunnel
show running-config	CONFIGURATION	Display current configuration information on the system.

Software Image Upgrade

You may upgrade the firmware or load a different version firmware installed on the routers.

Table 11 Upgrade firmware

Command Syntax	Command Mode	Purpose
upgrade{running|inactive|a|b}	PRIVILEGED EXEC	Upgrade the software image on the router

url <url> boot {running|inactive|a|b} [reboot] **upgrade** (running|inactive|a|b)ftp A.B.C.D FILENAME USERNAME PASSWORD boot (running|inactive|a|b)[reboot]		using an FTP or HTTP server. Note: If the first option is running/inactive, then the second option is also running/inactive. If the first option is A/B, then the second option is also A/B. Running: the image that is currently loaded and running Inactive: the image that is not currently loaded and running A: Represent A Partition B: Represent B partition Boot represents the booting image

For the best result, one can transfer firmware to DWR series using upgrade command.

```
DWR-500# upgrade running ftp 192.168.1.107 /tftpboot/DNOS -v2.0.5.img upimg upimg boot running
% Start downloading image
Connecting to 192.168.1.107[192.168.1.107]:21
new.img          100% |*******************************************************|  5405 KB    00:00 ETA
% Start upgrading image, this will take several minutes
Checking OK
Upgrading
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!OK
Verifying
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!OK
% Upgrade successful, please reboot the router to activate the new image


DWR-500# upgrade b url http://192.168.10.126/tftpboot/DNOS-v2.0.5.img boot b
% Start downloading image
Connecting to 192.168.10.126[192.168.10.126]:80
new.img          100% |******************************|  6347 KB    00:00 ETA
% Start upgrading image, this will take several minutes
Checking OK
Upgrading
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!OK
Verifying
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!OK
% Upgrade successful, please reboot the router to activate the new image
```

Figure 12 Output of firmware upgrade

Chapter 3 Physical Interfaces

This chapter contains information on defining and configuring and physical interfaces on the DWR series, it has the following sections:

- Interface Modes
- Configuring Fast-Ethernet Interfaces
- Configuring Dot11Radio Interfaces

Interface Modes

The wireless mesh router contains physical and logical interfaces in both Layer 2 and Layer 3 modes.

Table 12 List of Interface types and modes

Type of Interface	Mode	Dynamic Creation
fast-ethernet	Physical Layer 3	No
dot11radio	Physical Layer 2	No

Configuring Fast-ethernet Interfaces

DWR series has two physical fast-ethernet interfaces[1] that could connect the wireless mesh network with a wired network or device. Both interfaces support auto-negotiation between 10Mbps and 100Mbps as well as between half-duplex and full-duplex modes.

Table 13 Configuring Fastethernet Interface

Command Syntax	Command Mode	Purpose
interface fast-ethernet <*0-1*>	CONFIGURATION or INTERFACE FAST-ETHERNET	Configure a Fast-ethernet interface, it can be either fast-ethernet 0 or fast-ethernet 1
ip address *[ip address/mask]*	INTERFACE FAST-ETHERNET	Set IP address of fast-ethernet interface.
ip address dhcp		Set IP address to be automatically obtained by using the DHCP protocol; a DHCP server must be running on the network this fast-ethernet interface is connected to
no ip address		Remove IP address from Fast-ethernet interface
release-dhcp fast-ethernet <0-1>	PRIVILEGED EXEC	Release the fast-ethernet interface's IP address acquired from DHCP Server
renew-dhcp fast-ethernet <0-1>		Renew the fast-ethernet interface's IP address via DHCP Server
restart-dhcp fast-ethernet <0-1>		Restart DHCP client for the fast-ethernet interface
mode access	INTERFACE FAST-	Set this fast-ethernet interface as a LAN

[1] On some router models, only one Ethernet port (FastEthernet 0) is usable. It is recommended that the FastEthernet1 configuration to be left at default (disabled) for these models.

	ETHERNET	interface, for connecting with client devices
mode gateway		Set this fast-ethernet interface as a WAN interface, for connecting with a wired network.
mtu <*256-1500*>	INTERFACE FAST-ETHERNET	Set Maximum Transmission Unit (MTU)[2] size, 1500 is default ***Setting of MTU is optional and should be done with care.***
no mtu		Reset the MTU to the default value
shutdown	INTERFACE FAST-ETHERNET	Administratively shutdown the interface
no shutdown		Administratively activate the interface (Default)
exit, end, or quit	INTERFACE FAST-ETHERNET	Leave Interface mode and commit the change
dhcp server **dhcp relay**	INTERFACE FAST-ETHERNET	Configure DHCP server or relay for this Ethernet interface; for details, please refer to the chapter on DHCP and NAT.

Viewing fast-ethernet Interface information

The fast-ethernet interface information may be viewed using the 'show' command. The "show run" command displays the intended configuration of the interface, while the "show interface fast-ethernet" command displays the current state of the interface.

```
DWR-500# show running-config
...
!
interface fast-ethernet 0
 ip address 192.168.1.162/24
 mode gateway!
...
DWR-500# show interface fast-ethernet 0
Interface FastEthernet0
  mode: gateway
  admin status: up  physical status: up
  DHCP: disabled  DHCP client: disabled
  index 1 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:17:7b:18:18:30
  inet 192.168.1.162/24 broadcast 192.168.1.255
    input packets 52320, bytes 4810521, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 23738, bytes 3268042, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

Figure 13 Output of Fast-Ethernet

2 MTU (Maximum Transmission Unit) is the threshold at which single layer-3 IP packets become fragmented into multiple, smaller-size packets.

Configuring Dot11Radio Interfaces (Layer 2 Interfaces)

The sections describe the default interface configuration and the optional features that you can configure on the physical interfaces:

Radio Operation Mode

Radio Interface supports three operation modes, Access, Backhaul and Client. When configured for Access mode, 802.11 client devices such as personal computers, PDAs, and WiFi-phones are able to associate with the BSSs configured on the radio interface. When configured for Backhaul mode, other routers are able to connect to the radio interface through manually or automatically created WDS links. When configured for Client mode, the router can connect as a WiFi client to other APs within the range. There are commands that only take effect in one mode but not the others.

An operation mode must be configured on a radio before it could operate in a mesh network.

Table 14 Configure dot11radio interface

Command Syntax	Command Mode	Purpose
Interface dot11radio <*0-1*> Notes: DWR4000 wireless port： <0-3>	CONFIGURATION	Configure one of the dot11radio interfaces
mode access	INTERFACE DOT11RADIO	Configure radio interface for client access, allowing BSS association The default configuration: radio 0 works as the access.
mode backhaul **mode backhaul** <Mesh Profile>		Configure radio interface for backhaul operation, allowing connection with other DWR series routers. If <Mesh Profile> is specified, then the mesh settings in that profile are used for this backhaul radio; otherwise, the backhaul radio uses default mesh settings. See the later section on mesh profiles for details.
mode client		Configure radio interface to work as an 802.11 client, allowing connection with a generic 802.11 Access Point including BSSs provided by other DWR series routers. A router may only have one radio in client mode.

WPA2 over WDS

WPA2 can use ccmp to enhance network security under backhaul mode. ccmp (Counter Mode with CBC-MAC) is developed by IEEE based on Advanced Encryption Standard (AES) block cipher.

Currently WPA-PSK (TKIP) encryption is supported in backhaul mode, and TKIP still use RC4 cipher. But D-Link uses WPA2 (ccmp, AES) enhanced encryption in backhaul mode.

When WDS use WPA-PSK as the security mode, two types of encryption can be chosen: tkip (RC4 encryption algorithm) and ccmp (AES encryption algorithm), and ccmp has higher security. When

creating WDS links with multiple WPA on one radio, all the WDS have to use the same encryption algorithm, choosing tkip or ccmp.

Table 15 Configure WPA2 on WDS

Command Syntax	Command Mode	Purpose
wds-cipher-type <tkip|ccmp>	INTERFACE DOT11RADIO	Choose tkip or ccmp as WDS encryption
no wds-cipher-type		Restore the WDS encryption to default configuration (tkip)

Note: ccmp has higher security than tkip. All the WDS on one radio have to use the same WPA-PSK encryption, i.e. tkip alone or ccmp alone.

Common settings

Radio Interface supports three types of hard-ware mode: 802.11a, 802.11b (legacy mode), and 802.11g (can be configured to be backward-compatible with 802.11b). Each mode is associated with country codes and specific radio channels. The channel settings on the wireless device correspond to the frequencies available in the regulatory domain.

The following table outlines the physical, layer-2 settings that may configured on each radio interface. These settings apply in both access and backhaul modes.

Table 16 Wireless radio configuration

Command Syntax	Command Mode	Purpose
wireless-mode *<mode>* *<channel>*	INTERFACE DOT11RADIO	Configure the physical wireless settings of this radio interface manually. mode: a, b, g or g-only a: Use 802.11a b: Use 802.11b g: Use 802.11g; compatible with 802.11b in some configurations trunka: Use 802.11a trunka trunkg: Use 802.11g trunkg g-only: Use 802.11 g-only Note: g-only mode is uncompatible with the 802.11b mode. channel: A channel number, must be allowed by the router's country/regulatory domain code. If not configured, the system will choose the first legal channel number of the country/regulatory domain code.
no wireless -mode		Remove the wireless configuration manually configured. Restore default wireless mode
shutdown	INTERFACE DOT11RADIO	Administratively shutdown this radio; all existing operations on this radio will stop

no shutdown		Activate the interface
antenna <*0-2*>	INTERFACE DOT11RADIO	Configure this radio interface to use one of the two antennas connected to the physical radio card
antenna 0		Automatically choose the best antenna (default for indoor models)
antenna 1		Always use antenna 1 (default for outdoor models)
antenna 2		Always use antenna 2
no antenna		Restore default antenna setting. ***Setting of antenna is optional and should be done with care.***
packet-loss-ratio	INTERFACE DOT11RADIO	Choose the packet loss ratio of the current environment; the **force-rate-control-algorithm** rate algorithm will adjust based on the packet loss ratio value.
packet-loss-ratio low		The packet loss ratio is high under the current environment.
packet-loss-ratio very-low		The packet loss ratio is common under the current environment.
packet-loss-ratio lowest		The packet loss ratio is low under the current environment.
no packet-loss-ratio		Back to the default value of common packet loss ratio.
force-rate-control-algorithm [data|video]	INTERFACE DOT11RADIO	Enforce a particular algorithm, no auto configuration.
force-rate-control-algorithm data		Enforce the data transmission algorithm.
force-rate-control-algorithm video		Enforce the video transmission algorithm
no force-rate-control - algorithm		Select a rate algorithm automatically according to the QoS.
cts-protection <*0-3*>	INTERFACE DOT11RADIO	Enable or disable CTS protection on this radio interface.

cts-protection 0 **no cts-protection** **cts-protection 1** **cts-protection 2** **cts-protection 3**		0: Automatically enable/disable CTS using OLBC detection[3] (Default) Always enable CTS protection Always disable CTS protection Automatically enable/disable CTS without using OLBC detection[4] ***Setting of cts-protection is optional and should be done with care.***
mtu <*256-2274*> **no mtu**	INTERFACE DOT11RADIO	Set the layer-3 MTU of this radio interface. Reset the MTU to the default value ***Setting of radio MTU is not recommended and should be done with extreme caution.***
retry <1-32> <1-32> **retry** 4 7 **no retry**	INTERFACE DOT11RADIO	Sets the 802.11 MAC layer's packet retransmission limit. The first argument is the short retry limit and the second is the long retry limit. Reset retry to default (short retry of 4, long retry of 7)
tx-power-reduction *<0-65535>* **no tx-power-reduction**	INTERFACE DOT11RADIO	Set the reduced output value of the radio interface transmitting power, it decreased in 0.1dBm. For example, when it is set to 10, the reduced power can be reached 1dBm. The largest paramters configured is related to the radio interface rated transmitter power. The largest radio interface parameter of transmitting power is 200, which means the largest reduced power output can be 20dBm; the largest paramters of 400mW transmitting power can be 260, which means the power can reduce 26dBm the largest. Reset the power reduction to the default value. ***Transmission power settings should only be changed with extreme caution.***

A note regarding CTS protection:

IEEE 802.11g uses CTS frames to allow IEEE 802.11b clients notice frames sent at higher rates. This

[3] This setting will enable CTS protection when there are both 802.11g and 802.11b clients associated on one of the BSSs of the current radio or when Overlapping Legacy BSS Condition (OLBC) is detected

[4] This setting will enable CTS protection when there are both 802.11g and 802.11b clients using the current radio, but not when OLBC is detected

is useful in mixed mode networks consisting of both 802.11b and 802.11g stations. It is disabled automatically if there are no 802.11b stations associated to the AP. This behavior can be changed to enable CTS protection on IEEE 802.11g AP only, if there are IEEE 802.11b stations on the same channel using another AP. In addition, disabling this even when IEEE 802.11b stations are present can improve performance, if most traffic is between IEEE 802.11g devices.

Long-distance transmission

802.11 MAC layer protocol is specially designed for the short distance LAN data transmission (tens to hundreds of meters). Therefore, when the 802.11 protocol is applied to the long-distance transmission, it will not achieved because of the parameters of MAC layer. In order to achieve the long-distance transmission, it must enable the distance order to modify the MAC layer parameters, so as to achieve the effect of long-distance transmission.

1. Analysis and diagnosis for the long-distance transmission problems
   a) Analysis
      i. When the distance has been configured, the throughput is still not high or even can not ping successfully:
         1) Check whether the antenna has been aligned and the RSSI value.
         2) Check whether the distance at both ends be the same setting
         3) Check whether the order show interface dot11radio 0 info has been restored to the defaulted value.
      ii When the distance has been configured, the RSSI value checked is high, but the throughput is still not high.
         4) Scan whether the neighbor same frequency interface is strong
   b) Diagnose
      i. Show interface dot11radio [radioindex] can display the current distance setting.
      ii. Show interface dot11radio 0 info

Bandwidth Optimization

Bandwidth optimization is designed to provide the high-performance bandwidth. It is a series of intelligent mechanism that engages when additional bandwidth is available and/or needed. It enables the actual high bandwidth performance through the improvement of certain technology based on the existing standard such as the transmission of physical layer, data link layer and network layer.

These features include (1) compression, (2) rapid frame, and (3) static channel bonding. These capabilities operate independently to enhance the throughput of a network in different ways as follows:

Static channel bonding：Each channel occupied a fixed 20 MHz bandwidth in the 802.11 standard. The static channel bonding capability operates by bonding two 20 MHz channels into a separate one to transmission data which enhance the transmitting performance bacuse of the high bandwidth capability.

Rapid frame：Bandwidth optimization further provides throughput benefits through rapid frame, which allows for more information per frame to be transmitted. Rapid frame enhances data throughput by increasing the number of bits sent per data frame via bundling two data frames into a single wireless LAN frame, thereby eliminating the extra wireless network overhead associated with sending the second frame. Typically, frames transmitted over the wireless medium are bridged to or from

Ethernet. And therefore are generally restricted to the maximum Ethernet size of 1500 bytes. Rapid frame operate by changing the algorithm that may up to 4096 bytes.

Compression：In addition, link-level hardware compression more efficiently utilizes the wireless connection to further maximize bandwidth. This compression is implemented on a per frame basis and affects only data frames. It increases the data throughput of the compressed link, just as throughput is increased when a zipped file is attached to a message.

Bandwidth optimization configuration command

Table 17 Bandwidth Optimization Configuration Command

Command Syntax	Command Mode	Purpose
supermode	INTERFACE DOT11RADIO	Enable supermode, and enable the rapid frame and hardware compression to increase transmission rate
no supermode	INTERFACE DOT11RADIO	Disable supermode

Note: The above command table only includes enabling and disabling the rapid frame and hardware compression functions. The configuration of static channel bonding function please refer to the configuration of wireless¬-mode trunka/trunkg of radio interface.

Note:

1. All the commands must be configured under manual wds of backhaul mode. Bandwidth optimization is disabled under access, client or auto wds mode.
2. Both ends of wds need to configure the same bandwidth optimization command; otherwise wds can not link naturally.
3. Pay attention to avoid the same frequency interference when in trunk mode.

Backhaul mode Configuration

This section describes settings that only take affect in ***backhaul*** operation mode: The backhaul mode is used to create backhaul wireless links to other mesh routers.

Mesh Profiles and Settings

Each backhaul radio interface on the DWR series router must participate in a single wireless mesh network. Because each mesh network has its unique characteristics, mesh profiles can be created to specify unique settings for each mesh network.

The following table outlines the mesh profile-related commands:

Table 18 Mesh Command

Command Syntax	Command Mode	Purpose
profile mesh <NAME>	CONFIGURATION	Configure a new or existing mesh profile with the specified name on this router.
no profile mesh <NAME>		Remove an existing mesh profile

		configuration on this router.
mesh-id <WORD> **no mesh-id**	PROFILE MESH	Specify the mesh ID for this mesh profile; all mesh routers that forms the single mesh network should use the same mesh ID. Remove the mesh ID from this mesh profile.
mode backhaul <Mesh Profile>	INTERFACE DOT11RADIO	Set a radio interface for backhaul operation and use the settings in the specified mesh profile.

Backhaul radio settings

The following table outlines settings that only take affect in ***backhaul*** operation mode:

Table 19 Configuration that take effect under Backhaul mode

Command Syntax	Command Mode	Purpose
wds <*0-5*> **no wds** <*0-5*>	INTERFACE DOT11RADIO	Configure a new or existing manual WDS interface on this radio; this command is mutually exclusive with the wds auto command below[5]; Remove an existing manual WDS interface from this radio
wds auto **no wds auto**	INTERFACE DOT11RADIO	Enable automatic WDS provisioning on this radio interface and enter the auto WDS configuration mode; this command is mutually exclusive with the wds <0-5> command.[6] Disable auto WDS on this radio interface.
wds-unicast-rate [*rate*] **no wds-unicast-rate**	INTERFACE DOT11RADIO	Set the forced unicast rate of this radio interface's WDS links; once set, WDS links will attempt to consistently use the specified transmission rate. The rate is specified in units of 100kbps; the available rates are: 10, 20, 55, 110, 60, 90, 120, 180, 240, 360, 480, 540 **(Example: if choose 20, then RATE=20*100kbps=2Mbps)** Disables unicast rate setting; WDS links will automatically select the transmission rate and may dynamically vary depending on link quality (default setting)

[5] Please see the next chapter on WDS interfaces for more information.
[6] Please see chapter 7, Radio Frequency Management, for more information about auto WDS discovery and provisioning.

Access mode settings

The following table outlines settings that only take affect in ***access*** operation mode:

Table 20 Configuration that take effect under Access mode

Command Syntax	Command Mode	Purpose
bss <*SSID*> **no bss** <*SSID*>	INTERFACE DOT11RADIO	Configure a new or existing BSS on this radio interface[7] Remove an existing BSS from this radio interface SSID: The 802.11 Service Set ID (SSID) that identifies a BSS on this radio interface
station-isolation **no station-isolation**	INTERFACE DOT11RADIO	Disable the internal bridge for the client's data packets; this prevents the layer-2 broadcast traffic from one client to reach another. Broadcasts from the AP can still reach all clients. Enable the internal bridge for client's data packets; allows clients to communicate with each other through layer-2 broadcasting (default) ***It is highly recommended that station-isolation be enabled for security reasons. For example, it can prevent clients on the same AP from discovering each other through Microsoft Windows' Network Neighborhood feature.***

Client mode settings

The following table outlines settings that only take affect in ***client*** operation mode:

Table 21 Configuration that take effect under Client mode

Command Syntax	Command Mode	Purpose
station <station name> **no station <station name>**	INTERFACE DOT11RADIO	Configure a 802.11 client station on this radio interface[8] Remove 802.11 client station setting from this radio interface Note: currently only one station is allowed on each router

[7] Please see the later chapter on BSS for more information.
[8] Please see the later chapter on client mode for more information.

Viewing the dot11radio interface information

The “show run” command displays the intended configuration of the dot11radio interface, while the “show interface dot11radio” command displays the current state of the interface.

```
DWR-500# show running-config
...
 hostname DWR-500
 node-id 1
 router-id 192.168.10.1
country-code US

interface dot11radio 0
wireless-mode a 149
 antenna 0
 cts-protection 2
 mode backhaul
...
DWR-500# show interface dot11radio 0
Interface Dot11Radio0
  operation_mode:backhaul,mesh id:D-LinkMesh, country code:US, channel policy:0,
  antenna:0, cts protection:2,
  distance:0, short retry:7, long retry:4, wds up rssi limit:0, down limit:0, interference threshold:1500,
  admin status: up  physical status: up
  index 35 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWmode: a, channel: 149, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:17:7b:18:18:38
    input packets 3517383, bytes 627088483, dropped 0, multicast packets 0
    input errors 637111, length 0, overrun 0, CRC 0, frame 12, fifo 0, missed 0
    output packets 254080, bytes 35293576, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

Figure 14 Output of 802.11 radio interface

Chapter 4 Logical Interfaces (WDS)

- WDS introduction
- Typical case configuration

WDS Introduction

Wireless Distribution System (WDS) is the underlying technology that allows DWR series routers to communicate each other wirelessly and form the backhaul links of the mesh network. A WDS link is formed between two routers by creating logical WDS interfaces on each router, either through manual configuration or automatic discovery[9]. Each logical WDS interface is bound to a physical Dot11Radio interface. Therefore, WDS interface configuration commands are placed within the 'interface dot11radio' mode. Because WDS is used to form backhaul links, its configuration only takes effect on radio interfaces configured for backhaul mode.

Note: The DWR series can only form backhaul links with the radios on other DWR series routers that have the same mesh-ID configured. Please ensure all the routers in your wireless mesh network use the same mesh-ID and different networks use different IDs. The section on "Mesh Profiles" in the previous chapter describes how mesh profiles and IDs are configured.

Configuring Manual WDS

Manual WDS is to create WDS between two neighbouring routers via static configuration on wireless routers and then expand wireless mesh network.

On one radio, maximumly 6 manual WDS can be created.

The status of manual WDS link is managed by RFM and informs the up-level interface. Details refer to Chapter 8 Radio Frequency Management.

Table 22 Configuring Manual WDS Interface

Command Syntax	Command Mode	Purpose
wds <0-5>	INTERFACE DOT11RADIO	Configure a manual WDS
ip address *[ip address/mask]* **no ip address**	INTERFACE DOT11RADIO WDS	Configure IP address of WDS interface. Remove IP address from WDS interface
mtu <*256-2274*> **no mtu**	INTERFACE DOT11RADIO WDS	Configure MTU size of WDS interface Restore default MTU size (1500) ***Setting of MTU is optional and should be done with care.***
qos class <*class*> **no qos class**	INTERFACE DOT11RADIO WDS	Specify the Quality of Service (QoS) class policy[10] that should be applied for this WDS interface Disable QoS on this interface (default)
remote mac	INTERFACE DOT11RADIO WDS	Specify the MAC address of the remote

[9] Please see chapter 5 for more information about automatic discovery of WDS links
[10] Please see chapter 9, Quality of Service (QoS), for more information.

<*HH:HH:HH:HH:HH:HH***>** **remote node** *<1-8191> <0-N>*		radio on the other router that this WDS interface will establish a link with Specify the node ID and the index of the radio on the remote router that this WDS interface will establish a link with 1-8191: The node ID of the other router 0-N: The index of the radio on the other router that will form the link.
role <ap | station|auto> **no role**	INTERFACE DOT11RADIO WDS	Specify the role of this WDS interface in the link; each link requires a WDS interface as an ap and the other as station. Remove the specified role configuration (default, recommended setting)
shutdown **no shutdown**	INTERFACE DOT11RADIO WDS	Administratively shutdown this WDS interface; stops the operation of the WDS link Activate this WDS interface so it may establish a link with another router

Configuring Auto WDS

Auto WDS is to create WDS by RFM auto scanning and finding neighbour routers. When the router's radio interface is configured as Auto WDS mode, it automatically scans all the available channels and intercept and record the result of neighbour routers. According to the configured auto WDS link setting-up rules, it will create WDS.

On one radio, maximumly 6 auto WDS can be created.

The status of auto WDS link is managed by RFM and informs the up-level interface. Details refer to Chapter 8 Radio Frequency Management.

Table 22 Configuring Auto WDS Interface

Command Syntax	Command Mode	Purpose
max-auto-wds *<1-6>*	WDS AUTO	Set the maximum number of auto WDS interfaces that could be created on this radio by RFM[11]
wds auto **no wds auto**	INTERFACE DOT11RADIO	Enable Auto WDS on radio and enter Auto WDS mode. This function is mutually exclusive with Manual WDS Disable Auto WDS on radio
allowed-frequency-range a **allowed-frequency-range a 4.9**	WDS AUTO	Allow to set up auto WDS link on A-mode frequency (Default) Allow to set up auto WDS link on A-mode 4.9G frequency

[11] This setting is related to the automatic WDS link discovery feature of RFM. Please refer to chapter 5 for details.

allowed-frequency-range a 5 **allowed-frequency-range bg** **allowed-frequency-range abg**		Allow to set up auto WDS link on A-mode 5G frequency Allow to set up auto WDS link on BG-mode frequency Allow to set up auto WDS link on A-mode or BG-mode frequency

Configuring WDS Security

The 802.11 security standard defines a suite of wireless security protocols. The DWR series products' WDS support 802.11 WEP, WPA and WPA2 mode. Refer to the chapter on 802.11 Security for more information. When configuring security WDS, each WDS interface can use different 802.11 security policy, but must use the same security policy, such as TKIP or CCMP.

Manual security configuration parameters:

Command Syntax	Command Mode	Purpose
wds-cipher-type tkip **wds-cipher-type ccmp**	INTERFACE DOT11RADIO	Use WPA security configuration Use WPA2 security configuration
ssid <NAME> **no ssid**	INTERFACE DOT11RADIO WDS	Specify the SSID of this WDS link (required for WPA and WPA2) Do not use a SSID (default)
authentication open **no authentication** **authentication open key-management wpa <wpa-profile-name>** **authentication open key-management wpa2 <wpa2-profile-name>** **authentication shared wep <wep-profile-name> default-key <1-4>**	INTERFACE DOT11RADIO WDS	Allow all compatible mesh routers to form WDS links with this radio interface. Enable WPA security for the WDS; only allow mesh routers with correct WPA authentication and encryption settings to form WDS links. Designate encryption keys when WDS configuring WPA2 authentication. Only the router with correct WPA2 encryption keys can connect with WDS link. Enable WEP authentication for this WDS; only allow routers with the correct WEP key settings to form WDS links.

When configuring auto WDS, each radio should be configured the same security policy. At the same time, the neighbouring radios that may set up auto WDS should also be configured the same security policy.

Auto security configuration parameters:

Command Syntax	Command Mode	Purpose
wds-cipher-type tkip **wds-cipher-type ccmp**	INTERFACE DOT11RADIO	Use WPA security configuration Use WPA2 security configuration

authentication open key-management wpa <WPA-PROFILE-NAME>	WDS AUTO	Set auto WDS security policy to WPA
authentication open key-management wpa2 <WPA2-PROFILE-NAME>	WDS AUTO	Set auto WDS security policy to WPA2
authentication shared wep <WEP-PROFILE-NAME>	WDS AUTO	Set auto WDS security policy to share key
no authentication	WDS AUTO	Set auto WDS security policy to none

Viewing a list of all interfaces

The "show interface brief" command can be used to display a list of all interfaces on the router that includes both physical and logical interfaces.

```
DWR-500# show interface brief
Name            IP address          State
Dot11Radio0       unassigned          up
Dot11Radio1       unassigned          up
Radio0AWds0        10.0.103.1/24        up
Radio1MWds0        10.4.6.1/28          up
Radio1MWds1        10.5.6.1/28          up
FastEthernet0     192.168.1.136/24     up
FastEthernet1     unassigned          administratively down
```

Figure 15 Display the router interface status

In the above list, two physical radio interfaces and two physical fast-ethernet interfaces were included. In addition, one auto WDS[12] logical interface is bound to Dot11Radio0 (Radio0AWds0), two manual WDS interfaces are bound to Dot11Radio0 (Radio0MWds0-1), and two manual WDS interfaces bound to Dot11Radio1 (Radio1MWds0-1) were displayed. The prefix of the WDS interface name indicates the radio that the WDS interface used.

Viewing WDS Interface Information

```
DWR-500# show interface dot11radio 0 wds 0
Interface Radio0MWds0
  neighbor specified using: mac address
  remote mac address: 00:17:7b:0e:f8:50, remote node: 101, remote radio: 3
  admin status: up  physical status: up  neighbor ip: 10.3.101.2
  rssi: 26, snr: 26, link quality: 53%, unicast rate: 12Mbps
  role:auto, physical interface:0, qos class:DEFAULT,
  index 20 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  Operating HWmode: a, channel: 157, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:17:7b:00:0c:98
  inet 10.3.101.1/24 broadcast 10.3.101.255
    input packets 5751, bytes 660723, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    input rate 5.14 Kb/s
    output packets 7450, bytes 1278416, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    output rate 11.38 Kb/s
    collision 0
```

[12] See the next chapter on RFM for information on auto WDS link discovery.

Figure 16 WDS Interface Information

Chapter 5 Access and BSS Configuration

When a Dot11Radio interface is put into Access mode, a BSS configured for that interface becomes a virtual AP that client devices may associate with. Each BSS is bound to a physical dot11radio interface; therefore, BSS is configured within the 'interface dot11radio' mode. The DWR series router supports up to four BSSs on each radio interface.

Basic BSS configuration

The following table outlines the basic settings for each BSS.

Table 23 Configuring Basic BSS

Command Syntax	Command Mode	Purpose
bss <SSID> **no bss** <SSID>	INTERFACE DOT11RADIO	Configure a new or existing BSS on this radio interface Remove an existing BSS from this radio interface SSID: The 802.11 Service Set ID (SSID) that identifies a BSS on this radio interface
ip address A.B.C.D/M **no ip adress**	INTERFACE DOT11RADIO BSS	Configure IP Address for the BSS Remove IP address of this BSS
authentication open **no authentication** **authentication open wep <wep-profile-name> default-key <1-4>** **authentication open key-management wpa <wpa-profile-name>** **authentication open key-management wpa2 <wpa2-profile-name>** **authentication shared wep <wep-profile-name> default-key <1-4>**	INTERFACE DOT11RADIO BSS	Allow all clients to associate with this BSS Enable open WEP encryption for this BSS using the key settings in the WEP profile and the specified default key index Enable WPA security for this BSS; only allow clients with correct WPA authentication and encryption settings to associate with this BSS. Enable WPA2 security for this BSS; only allow clients with correct WPA2 authentication and encryption settings to associate with this BSS. Enable shared WEP authentication and encryption for this BSS using the key settings in the WEP profile and the specified default key index
mac-address accept <mac-list-name> **mac-address deny <mac-**	INTERFACE DOT11RADIO BSS	Only accept clients with MAC addresses in the specified list; deny all other clients Only deny clients with MAC addresses in

list-name> **mac-address accept-all** **no mac-address**		the specified list; allow all other clients. Restore to default configuration (accept all MAC addresses)
ignore-broadcast-ssid **no ignore-broadcast-ssid**	INTERFACE DOT11RADIO BSS	Disable broadcasting of this BSS's SSID Enable broadcasting of this BSS's SSID (Default)
max-rate <rate> **no max-rate**	INTERFACE DOT11RADIO BSS	Select the maximum allowed transmission rate for this BSS in units of 100kbps. Available rates: 10, 20, 55, 110, 60, 90, 120, 180, 240, 360, 480, 540. Allow the maximum transmission rate supported by the client and radio hardware (Default)
max-station-allowed <0-240> **max-station-allowed 240** **no max-station-allowed**	INTERFACE DOT11RADIO BSS	Configure the maximum number of stations allowed to associate with this BSS Allow up to 240 stations to associate with this BSS (default).
station-inactivity-limit <1-65535**>** **station-inactivity-limit 300** **no station-inactivity-limit**	BSS	Configure the maximum amount of time (in seconds) a station is allowed to be inactive before the action specified by the inactivity-policy (see next) is taken Set the inactivity limit to the default value of 300 seconds
station-inactivity-policy <0-1> **station-inactivity-policy 0** **no station-inactivity-policy** **station-inactivity-policy 1**	INTERFACE DOT11RADIO BSS	Configure the action taken when a station exceeds the inactivity limit. Poll the station to judge the activity of terminals. Use the exceed time to judge the activity of terminals
unicast-rate <rate> **no unicast-rate**	INTERFACE DOT11RADIO BSS	Set the unicast rate of this BSS; once set, the radio interface will attempt to consistently use the specified transmission rate for stations associated with this BSS. Setting this option will also prevent stations that do not support the specified rate from associating with the BSS. The rate is specified in units of 100kbps; the available rates are: 10, 20, 55, 110, 60, 90, 120, 180, 240, 360, 480, 540

		Disables unicast rate setting for this BSS; radio interfaces will automatically select transmission rates (default setting)
dhcp server **dhcp relay** **no dhcp**	INTERFACE DOT11RADIO BSS	Configure DHCP server or relay for this BSS; for details, please refer to the chapter on DHCP and NAT. Separate the DHCP server from the current BSS
switchport access vlan <1-4094> **no switchport**	INTERFACE DOT11RADIO BSS	Configure the BSS to VLAN access port Remove the BSS VLAN access port

Interference Detection & Avoidance

Activate interference avoidance, if the current channel that AP works is interfered by radar or the consecutive non-WiFi or WiFi, then select and switch the channel according to the following priciples:

1） No radar interference
2） The minimum interference factor
3） The channel which farest from the current interference channel

Interference detection & avoidance command:

:

Table 24 Interference Detection and Avoidance

Command Syntax	Command Mode	Purpose
interference avoidance **no interference avoidance**	INTERFACE DOT11RADIO	Enable the interference avoidance(Default disabled) Disable the interface avoidance
debug dot11radio INDEX noise_detection	PRIVILEGED EXEC	Collect the interference information of all the channels by radio
debug dot11radio INDEX noise_detection physical (a|b|g)	PRIVILEGED EXEC	Interference information of all the channels in specified mode
debug dot11radio INDEX noise_detection physical (a|b|g) N	PRIVILEGED EXEC	Interference information of one channel in some specified mode
show interface dot11radio INDEX interference-status	PRIVILEGED EXEC	Show the interference information of all the channels that radio collects.
show interface dot11radaio INDEX interference-status physical (a|b|g) N	PRIVILEGED EXEC	Show the interference information of one channel in the specified mode.

Enable WME

Wi-Fi Multi-Media QOS (Quality of Service) ensures the service quality in wireless networks for multimedia applications.

Table 25 WME command

Command Syntax	Command Mode	Purpose
force-sta-wme	INTERFACE DOT11RADIO BSS	STA that do not support WME are not allowed to link with this BSS
no force-sta-wme		Remove the limitation that STA do not support WME are not allowed to ink with this BSS

Multi-SSID

Each SSID, just like a switch virtual port, can assign a vlan ID. Users can connect to this SSID but will not be able to communicate with the layer 2 devices (even in the same BSS). 3 multi-ssid is the maximum allowed configuration for each BSS.

Table 26 Configuring Multi-SSID

Command Syntax	Command Mode	Purpose
ssid <SSID>	INTERFACE DOT11RADIO BSS	Configure a new or existing SSID on this BSS
no ssid<SSID>		Remove an existing SSID from this BSS SSID: 802.11 Service Set ID (SSID) that identifies a BSS on this radio interface.
ip address A.B.C.D/M	INTERFACE DOT11RADIO BSS SSID	Configure IP address for the Multi-ssid
no ip address		Delete the IP address for the Multi-ssid
authentication open **no authentication**	INTERFACE DOT11RADIO BSS SSID	Allow all users to associate with this SSID without authentication
authentication open wep <wep-profile-name> default-key <1-4>		Enable open WEP encryption for this SSID using the key settings in the WEP profile and the specified default key
authentication open key-management wpa <wpa-profile-name>		Enable WPA security for this SSID; only allow clients with correct WPA authentication and encryption settings to associate with this SSID.
authentication open key-management wpa2 <wpa2-profile-name>		Enable WPA2 security for this SSID; only allow clients with correct WPA2 authentication and encryption settings to associate with this SSID.

authentication shared wep <wep-profile-name> default-key <1-4>		Enable shared WEP authentication and encryption for this SSID using the key settings in the WEP profile and the specified default key
dhcp server POOL-NAME **no dhcp**	INTERFACE DOT11RADIO BSS SSID	Configure DHCP server for SSID, currently multi-ssid only support manual DHCP server. For details, please refer to the chapter on DHCP and NAT. Separate the DHCP service from the current multi-ssid
switchport access vlan <1-4094> **no switchport**	INTERFACE DOT11RADIO BSS SSID	Configure SSID to VLAN access port Remove multi-ssid VLAN access port

Note:

1. Only the ssid configured in bss can be broadcast in beacon, other multi-ssid will not list on the client's wireless network, which requiring the user manual configuration.
2. The current multi-ssid encryption should be consistent with the main bss except the encryption documents and key which can be inconsistent with the main bss.
3. The current multi-ssid only supports manual dhcp server or static IP.

Map BSSID to DSCP

Each BSS (BSSID) has its mapped DSCP value via four categories (bk, be, vi and vo). The corresponding relationship is as follows:

Category	DSCP
bk	16
be	0
vi	32
vo	56

When a station (no matter it supports 802.11e or not) connects to a particular BSS, all frames that contain BSS will have the corresponding DSCP value. The frame with high DSCP has the high priority to be sent.

Table 27 BSSID Mapping Command

Command Syntax	Command Mode	Purpose
access-category *<bk|be|vi|vo>* **no access-category**	INTERFACE DOT11RADIO BSS	Set 802.11e mapping priority on BSS Remove the priority setting on BSS

802.11 Security Configuration

The 802.11 security standard defines a suite of wireless security protocols and implementations. It provides open and shared key authentication, is compatible with WPA /WPA2, and interoperates with 802.1x.

The mesh router allows each BSS to use a different 802.11 security profile. Please refer to the chapter on 802.11 Security for more information.

Viewing BSS of dot11radio interface information.

```
DWR-500# show running-config
...
interface dot11radio 0
...
 bss demo
  station-inactivity-policy 1
  station-inactivity-limit 300
  max-rate 60
  authentication open wep test-supplicant default-key 1
  mac-address accept AAA
...
!
security-profile wep test-supplicant
 wep-key 1 hex 1234567890
 wep-key 2 ascii 12345
 wep-key 3 hex 3456789012
 wep-key 4 ascii 4567890123456
!
mac-list AAA
 mac-addr 22:22:22:bc:22:44
 mac-addr 22:22:22:bc:22:45
 mac-addr 22:22:22:bc:22:08
...
!
DWR-500# show interface dot11radio 0 bss demo
BSS:demo

  ignore broadcast ssid:disable, maxium station allowed:240,
  transmission fail percentage:0, transmission fail check interval:0,
  station inactivity policy:1, station inactivity limit:300,
  maxium rate control rate:60, authentication:open wep test-supplicant default-key 1,mac authentication:accept AAA,
    HWaddr: 00:17:7b:18:18:40
```

Figure 17 Output of BSS under dot11radio interface

Chapter 6 Client Mode Configuration

When a Dot11Radio interface is configured for client mode, an 802.11 client station configured under that interface can associate to any matching 802.11 access points as any other 802.11 client. The access point can be BSSs provided by other DWR series or an AP from another vendor. On each DWR series router, only one radio interface can operate in client mode.

Basic Client Mode configuration

The following table outlines the basic settings for a client station

Table 28 Configuring Basic Client Mode

Command Syntax	Command Mode	Purpose
station <station name> **no station <station name>**	INTERFACE DOT11RADIO	Configure a 802.11 client station on this radio interface Remove 802.11 client station setting from this radio interface ***Note: only one client can be created on a radio interface***
ip address *[ip address/mask]* **ip address dhcp** **no ip address**	INTERFACE DOT11RADIO STATION	Set IP address of this client station. Set IP address to be automatically obtained by using the DHCP protocol; a DHCP server must be running on the network this station associates to. Remove IP address from this client station.
client-authentication open wep <wep-profile-name> default-key <1-4> **client-authentication open key-management wpa client-8021x <client-8021x-profile-name>** **client-authentication open key-management wpa2 client-8021x <client-8021x-profile-name>** **client-authentication open key-management wpa-psk hex <string>**	INTERFACE DOT11RADIO STATION	Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key Enable WPA security for this client; using the authentication settings in the client-8021x profile Enable WPA2 security for this client; using the authentication settings in the client-8021x profile Enable WPA PSK on client and configure pre-shared key using hexadecimal format.

client-authentication open key-management wpa-psk ascii <string>		Enable WPA PSK on client and configure pre-shared key using ascii format.
client-authentication open key-management wpa2-psk hex <string>		Enable WPA2 PSK on client and configure pre-shared key using hexadecimal format.
client-authentication open key-management wpa2-psk ascii <string>		Enable WPA2 PSK on client and configure pre-shared key using ascii format.
client-authentication shared wep <wep-profile-name> default-key <1-4>		Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key
no client-authentication		Disable authentication for this client interface.
access-point ssid <SSID>	INTERFACE DOT11RADIO STATION	SSID of the access point that this client station wants to associate with. Default is no SSID.
no access-point ssid		Remove access-point SSID configuration. SSID: 802.11 Service Set ID
access-point bssid <*HH:HH:HH:HH:HH:HH***>**	INTERFACE DOT11RADIO STATION	BSSID of the access point that this client station wants to associate with. Default has no BSSID specified.
no access-point bssid		Remove the setting of BSSID for an access point.
access-point bssid-filter acceptable prefix <*HH:HH:HH:HH:HH:HH***> <***HH:HH:HH:HH:HH:HH***>**	INTERFACE DOT11RADIO STATION	This command provides a filter when the client is selecting an Access Point during scanning. The first MAC address is the prefix of BSSID you allow the client to associate with. The second MAC address is a mask of the prefix. If configured, only an access point with matching BSSID will be selected. For example, if you want the client to only connect to DWR series routers, you can specify a prefix of 00:17:7b:00:00:00 with mask of ff:ff:ff:00:00:00 Multiple filters can be configured if you want to allow multiple BSSID prefix choices. Default allows all BSSIDs.
no access-point bssid-filter acceptable prefix <*HH:HH:HH:HH:HH:HH***>**		Remove a certain BSSID filter

<HH:HH:HH:HH:HH:HH> **no access-point bssid-filter acceptable-prefix**		Remove all the BSSID filters
scanning hardware-modes <mode string> **scanning hardware-modes <mode string> channel-list <channel list>** **no scanning hardware-modes**	INTERFACE DOT11RADIO STATION	Configure the hardware modes that you allow the client to stay in when doing access point scanning. <mode string>: a, g, ag It means do scanning only in 802.11a mode, 802.11g mode or in both modes. Default value is both 802.11a and 802.11g Channel-list is optionally provided to permit you specifying which channels the client will scan in. Only one channel list is allowed. Default has no channel list and it scans in all legal channels of the configured hardware modes. <channel-list>: a list of comma separated channel numbers, no space in between Remove the hardware scanning mode and channel-list setting and return to default.
scanning minimum-interval <seconds> **no scanning minimum-interval**	INTERFACE DOT11RADIOSTATION	Configure the minimum allowed time interval between two consecutive scans. <seconds>: a number between 1 and 300, the unit is second. Default value is 60 seconds. Restore default setting of minimum scan interval
scanning threshold rssi <rssi value> **no scanning threshold rssi**	INTERFACE DOT11RADIO STATION	Configure the RSSI value threshold to trigger a new scan. If the current RSSI is lower than configured threshold, the client will start a new scan. <rssi value>: a number between 0 and 100. 0 means no such trigger. Default value is 15. RSSI stands for Received Signal Strength Index Restore the default RSSI threshold value.
release-dhcp dot11radio <0-N> station <station name> **renew-dhcp dot11radio <0-N> station <station name>**	PRIVILEGED EXEC	Release the station's IP address acquired from DHCP server Renew the station's IP address via DHCP server

restart-dhcp dot11radio <0-N> station <station name>		Restart DHCP client for the station

Subsidiary Connecting Device IP Address List (Client Station)

When radio of DWR series routers works in client mode, it can derive a variety of applications making use of the stations which access to the mesh network. For example, the router's other interfaces (Ethernet interface, radio interface) can connect up to four cable or wireless devices (such as: camera /encoder/decoder, WIFI phone, etc). The cable or wireless devices can also visit mesh networks through the station mesh network access. Moreover, the station roaming support makes the devices that connecting to the sation can also mutual visit the mesh networks in the process of moving.

The configuration and deletion of user interfaces are almost the same as that of AP, except that it only needs to modify under the client mode. MAC address: the MAC address of client mode interface; IP address: the IP address of the device which connect to the Ethernet interfaces.

Table 29 Configuring Basic Client Station-list

Command Syntax	Command Mode	Purpose
client-list *<A.B.C.D/M>*	INTERFACE DOT11RADIO STATION	Creat client-list entries for the subsidiary connecting devices that working in the client mode *<A.B.C.D/M>* Subsidiay connecting devices' IP address/mask Can creat up to 4 client-list entries
no client-list		Remove all the configured client-list entries
no client-list *<A.B.C.D/M >*		Remove the designated client-list entries. *<A.B.C.D/M>* Subsidiay connecting devices' IP address/mask

Each station can configure up to 4 client-list entries in client mode. If the station itself needs network-side management (Telnet / SSH) in the process roaming, it should use the static ip address, and the ip address of station should also be added to the station-list. In addition, according to the actual application, if the station uses the static IP address, it usually needs to manually add the default routing of station interface (ip route 0.0.0.0 / 0 station <station name> <radio index>.

802.11 Security Configuration

The 802.11 security standard defines a suite of wireless security protocols and implementations. The DWR series allows the client mode to use a specific 802.11 security profile such as WEP or WPA. Refer to the chapter on 802.11 Security for more information.

Viewing information of a station in a dot11radio interface

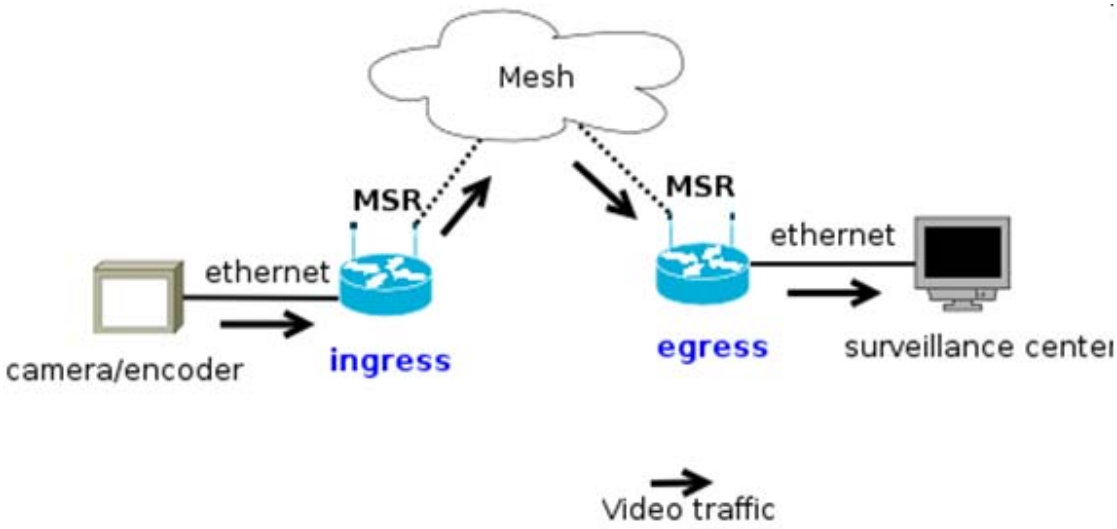
```
DWR-500# show run
...
!
interface dot11radio 0
...
 station demo
  ip address dhcp
  access-point ssid demo

...
DWR-500# sh interface dot11radio 0
  Interface Dot11Radio0
  operation mode:client, country code:US, channel policy:0, antenna:1, output power:100 mW, cts protection:2,
  distance:0, short retry:7, long retry:4, wds up rssi limit:10, wds down rssi limit:5,
  admin status: up  physical status: up
  Configured HWmode: a, channel: 36
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  Operating HWmode: g, channel: 11, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:17:7b:fc:1e:50
    input packets 1140620, bytes 220235241, dropped 0, multicast packets 0
    input errors 100757, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    input rate 161.43 Kb/s
    output packets 14288, bytes 3107981, dropped 0
    output errors 931, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    output rate 8.20 Kb/s
    collisions 0operation_mode:client, country code:US, channel policy:0, antenna:1,
  cts protection:2,
  distance:0, short retry:7, long retry:4,
  admin status: up  physical status: up
  index 35 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWmode: g, channel: 1, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:17:7b:00:27:40
    input packets 823925, bytes 96825419, dropped 0, multicast packets 0
    input errors 88069, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 457, bytes 26006, dropped 0
    output errors 2, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
  Station Information:
     Station demo
    State: Associated
    SSID: "demo", Access Point: 00:17:7b:35:e8:53 RSSI: 55
    Previous Access Point: NA
    IP Address: 172.16.21.249(DHCP acquired)
    Security: None
    Scanning threshold: RSSI 15
    Minimum scan interval: 60 seconds
    scanning in hardware modes: ag
    scanning in channels:
     mode A: 36 40 44 48 52 56 60 64 149 153 157 161 165
     mode G: 1 2 3 4 5 6 7 8 9 10 11
```

Figure 18 Output of station information under dot11radio interface

Chapter 7 Video Friendly Network

Video Friendly Network is a network transmission optimization technology specially designed by D-Link for mobile video service. It includes three parts: Active Video Transport (AVT), video friendly MAC technology and virtual video distribution layer.

AVT is a specially designed network transmission optimization technology for soft video transmission with typical application of fixed or mobile video surveillance. Through the data delay configured by users in Mesh network, AVT could effectively reduce or resolve the problems of packets loss, delivery disorder and packet jitter caused by wireless transmission, so as to provide smooth and stable multi-channel video traffic transmission. A typical application is the video surveillance. By providing in-network cache, AVT could resolve the problems that impact the quality of video transport in WMN to achieve the best transmission result.



AVT Configuration

AVT system

AVT is specially designed for point-to-point video transmission. It mainly consists of two components in structure: ingress and egress. Take the video surveillance scenario for example; the network topology is as follow:

Ingress port: DWR series routers that directly connect to video server (the left DWR in the above figure), and the video traffic enters Mesh network just from this router.

Egress port: The last DWR series router from which video traffic is out of Mesh network. Usually it is the gateway of the Mesh network with direct connection with the surveillance center.

AVT Parameter Configuration

Necessary Parameters

Parameters need to configure in ingress: Encoder: choose the type of video server. Ingress-IP: configure the IP address of video server. At present, one ingress DWR router can support four video servers at the same time.

Optional Parameters
Choose different network delay in different application to achieve the more satisfied video transmission. In general, the longer the network delay, the less the problems concur that impact video transmission, such as packet loss; the shorter the network delay, the better the real-time capability.

The network delay setting is mainly at egress router, i.e. the buffer-time at egress. It is also need to set buffer-time at ingress and its value should be no less than that of the buffer-time at egress. The default buffer time: 3 seconds for egress and 4 seconds for ingress.

CLI Command

The following commands are used to configure AVT mode and parameters

Table 30 Configuring AVT

Command Syntax	Command Mode	Purpose
service avt	CONFIGURATION	Enable AVT service configuration
enable/disable	SERVICE AVT	Enable/disable AVT service
ingress/egress **no ingress** **no egress**	SERVICE AVT	Set this router as ingress or egress Remove this router at ingress and egress
encoder <generic |tycosun|visiondigi > **no encoder**	SERVICE AVT	Set the encoder type (video server). Generic for most of the encoders (default) such as Hiklif and AVINFO; Tycosun for tycosun encoder; Visiondigi for visiondigi encoder Remove the type of encoder, get back to the default: generic
ingress-ip A.B.C.D **no ingress-ip A.B.C.D**	SERVICE AVT	Set ingress IP (up to 4) Remove the IP address of encoder at ingress
buffer-time<1-5> **no buffer-time**	SERVICE AVT	Set the buffer time as 1-5 seconds. Default second for egress is 3 Default second for ingress is 4 Remove the buffer time, restore to the default value

The following commands show AVT running status and statistics

Table 31 AVT Status and Statistics

Command Syntax	Command Mode	Purpose
show avt status	PRIVILEGED EXEC	Display the runtime statistics of AVT

show avt configuration	PRIVILEGED EXEC	Display the running configuration of AVT

Note

1. NAT is disabled between ingress and egress of AVT (including ingress), but can enable outside ingress and egress (including egress).
2. Ingress router and egress router shouldn't be the same DWR router.
3. When the wireless environment is poor, such as when in weak signal or strong interference, AVT will be limited and may not improve video transmission obviously. You can reboot AVT (disable and then enable) or close AVT and then reopen it when the wireless link gets better.

Chapter 8 Radio Frequency Management

Radio Frequency Management (RFM) is an advanced feature of DWR series that allows automatic discovery and quality monitoring of wireless mesh links. RFM automatically scans for compatible mesh routers in the neighboring area and create automatic WDS links to these routers. With RFM, multiple mesh routers can form a mesh network without any manually configured WDS interfaces. In addition, an RFM-aware routing protocol could use the link quality information from RFM to optimize the routing path in the wireless mesh network.

RFM Working Principle

When the equipment is in power or automatic WDS Link function commences, RFM module will scan all the channels to find the suitable neighbors under the set mode. It can establish the corresponding WDS Link according to the scan results and WDS link rules. RFM support two kinds of models to establish WDS links, the first is the automatic WDS links, if configured, RFM will scan the most appropriate neighbors initiately, when at least one WDS link is established, it will then enters the passive scanning, waiting for their own access to the establishment of passive automatic WDS Link. The second is the manual WDS link. When it is configured, it can only establish manual WDS link with configured nodes.

WDS Link Quality Monitoring

RFM could monitor the link quality for all WDS links present on an DWR series router, regardless of whether the link is manually configured or automatically created. The WDS interface for the link must be active[13]. The link quality is displayed in the results of the “show interface dot11radio X wds” command:

```
DWR-500# show interface dot11radio 0 wds 0
Interface Radio0MWds0
  neighbor specified using: node id
  remote mac address: 00:17:7b:00:23:30, remote node: 8103, remote radio: 0
  admin status: up  physical status: up  neighbor ip: 11.11.11.31
  rssi: 27, snr: 27, link quality: 54%, unicast rate: 18Mbps
  role:auto, physical interface:0,
  index 20 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  Operating HWmode: a, channel: 157, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:17:7b:00:23:90
  inet 11.11.11.61/24 broadcast 11.11.11.255
    input packets 17907, bytes 2008457, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    input rate 0.00 Kb/s
    output packets 97791, bytes 7900561, dropped 0
    output errors 20291, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    output rate 0.55 Kb/s
    collisions 0
```

Figure 19 Display the link quality

The link quality parameters monitored by RFM include RSSI, SNR, overall quality[14], and data rate.

[13] An active WDS interface is one that is bound to an active backhaul radio interface and not administratively shutdown.
[14] The link quality percentage measurement is based on the level of RFM control packet loss.

Auto neighbor discovery and WDS link creation

RFM discovers neighboring mesh routers using **passive-scanning**, a process that is automatically started when a backhaul radio interface is operating without any manually configured WDS interfaces. Passive-scanning automatically changes the channel of the radio interface and listens for 802.11 beacons from other mesh routers. If one or more routers are heard, RFM selectively attempts to create WDS links with these other routers. Auto WDS interfaces are automatically created and configured if the WDS connection is successfully established.

The configuration commands that controls auto-discovery is **wds auto**, which enables Auto WDS discovery for a radio interface, and **max-auto-wds**, which controls how many automatic WDS links RFM is allowed to create on that interface. If **wds auto** is not set for a radio interface, RFM will not perform any scanning or WDS interface creation on that radio.

Note: As previously mentioned in the chapter on WDS configuration, the DWR series can only form WDS links with other DWR series routers that use the same mesh ID.

Advantages of Automatic WDS link

Establish Mesh Network fast and easily without any configuration
Optimize Mesh Networks automatically according to the environmental changes and scan results

RFM related configuration commands

The following table summarizes the commands used to configure RFM's auto-discovery and link monitoring functions:

Table 32 Related RFM Command configuration

Command Syntax	Command Mode	Purpose
wds auto	INTERFACE DOT11RADIO	Enable auto WDS provisioning on this radio interface and enter the INTERFACE DOT11RADIO WDS AUTO mode for auto WDS configuration; this is mutually exclusive with the WDS command.
no wds auto		Disable auto WDS on this radio interface.
wds-rssi-limit <0-100> <0-100>	INTERFACE DOT11RADIO	Configure the minimum RSSI value of physical up WDS，the physical down cannot be changed to physical up when RSSI value of neighbor is below the configurd minimum value, and the default value is 10；Configure the maxi RSSI value that make WDS change from up to down, when WDS works in physical up and the RSSI value of neighbor is below this configured value, it must be in physical down, and the default value is 5.
debug	SERVICE RF-MANAGEMENT	Set the RFM debug log level
debug none		Disable RFM debug log
debug error		Set RFM debug log to record errors
debug state		Set RFM debug log to record errors & state

		changes
debug process		Set RFM debug log to the record network process
debug information		Set RFM debug log to the record error, state, and other detailed information
debug frame		Set RFM debug log to the record error, start, information, and RFM control packet frames
debug dump		Set RFM debug log to the recorded all RFM debug information

The following commands can be entered at the privileged EXEC prompt to display information about the RFM service:

Table 33 RFM command configuration under Privileged Mode

Command Syntax	**Command Mode**	**Purpose**
show log rf-management	PRIVILEGED EXEC	Display the log information of RFM (see debug command above)
show rf-management active-neighbors	PRIVILEGED EXEC	Display a list of neighboring DWR series routers and radios discovered by RFM
show rf-management interface	PRIVILEGED EXEC	Display a list of WDS interfaces currently monitored by RFM; may include both auto and manual WDS interfaces.
show rf-management path-info	PRIVILEGED EXEC	Display path information getting to the gateway
show rf-management reject-neighbors	PRIVILEGED EXEC	Display RFM reject Neighbors
show rf-management scan-neighbors	PRIVILEGED EXEC	Display RFM Scan Neighbors
show rf-management configuration	PRIVILEGED EXEC	Display the current configuration parameters of RFM
clear rf-management neighbor all	PRIVILEGED EXEC	Clear all the RFM active neighbors
clear rf-management neighbor mac *HH:HH:HH:HH:HH:HH*	PRIVILEGED EXEC	Clear RFM neighbor by mac
clear rf-management process	PRIVILEGED EXEC	Reset RFM process
debug rf-management errors	PRIVILEGED EXEC	Set RFM debug log to record errors
debug rf-management events	PRIVILEGED EXEC	Set RFM debug log to record link interface events
debug rf-management messages	PRIVILEGED EXEC	Set RFM debug log to record debug messages
debug rf-management packets	PRIVILEGED EXEC	Set RFM debug log to record protocol exchange packets
debug rf-management	PRIVILEGED EXEC	Display current active neighbors

active-neighbors		
debug rf-management global-variables	PRIVILEGED EXEC	Display current RFM global variables
debug rf-management ping	PRIVILEGED EXEC	Check RFM process to see if it's normal
debug rf-management radios-variables	PRIVILEGED EXEC	Display the global variables of radio interfaces
debug rf-management reject-neighbors	PRIVILEGED EXEC	Display neighbors rejected by RFM
debug rf-management scan-neighbors	PRIVILEGED EXEC	Display neighbors scanned by RFM

Typical Configuration

Typical Case of automatic WDS link:

Simulate an automatic WDS link between the three nodes according to the actual application of network environment. The three nodes are all factory defaulted before configuration.

Configure the 3 nodes separately to simulate an automatic MESH network.

Establish an automatic WDS link as the following simulated map 1:

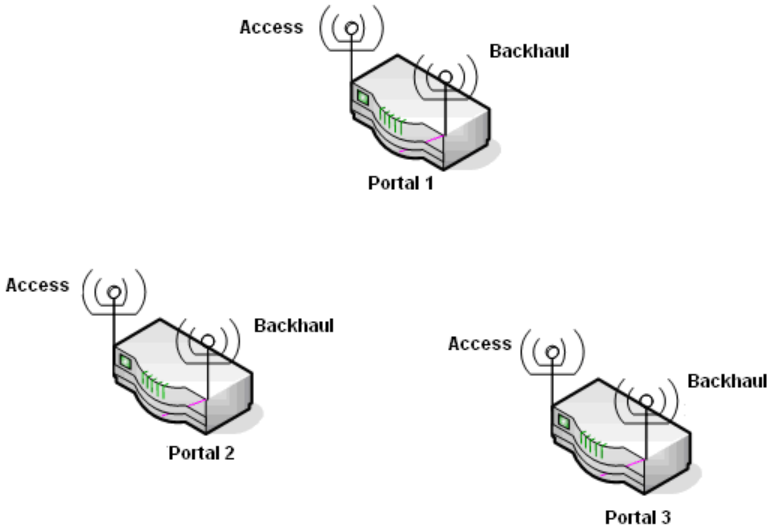


Figure 21 Simulated map 1 of automatic WDS

The simulated map after establishing an automatic WDS link:

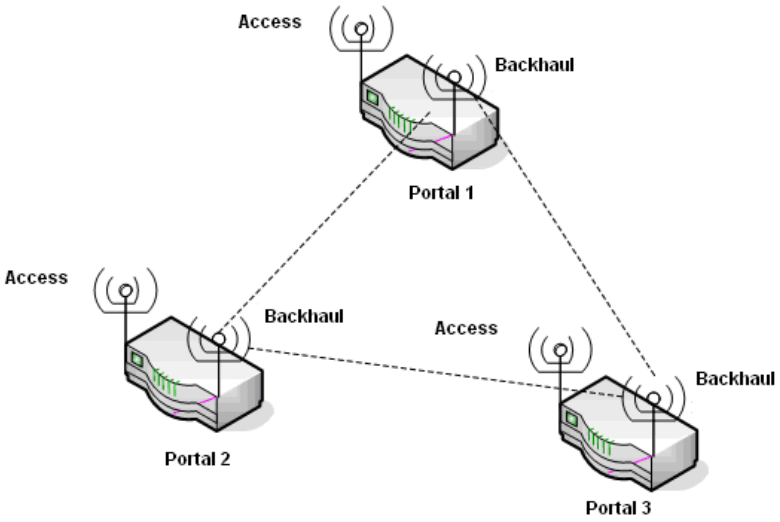


Figure 22 Simulated map 2 of automatic WDS

The three above manual WDS link information is as follows:
Node 1 and node 2: manual de-authentication WDS link
Node 1 and node 3: manual WEP authentication WDS link
Node 2 and node 3: manual WPA authentication WDS link

Configuration steps summary:

First：Node 1, node 2, node 3 all are factory configured
Second：Land on node 1 to configure the settings, please refer to the node 1 configuration step
Third：Land on node 1 to configure the settings, please refer to the node 2 configuration step
Forth：Land on node 1 to configure the settings, please refer to the node 3 configuration step
Fifth：After the configuration and reboot completed, it can view the automatic WDS link information through WDS link diagnose 15s later.

Table 34 Node configuration Summary

Node ID	Interfaces	Remote Node	Remote neighbor configuration	IP Address/Mask	Authentication Mode
Node 1	Radio 1 Wds 0	2	Remote Node and Radio	10.10.12.1/24	None
	Radio 1 Wds 1	3	Remote MAC	10.10.13.1/24	WEP
Node 2	Radio 1 Wds 0	1	Remote Node and Radio	10..10.12.2/24	None
	Radio 1 Wds 1	3	Remote Node and Radio	10.10.23.1/24	WPA
Node 3	Radio 0 Wds 0	1	Remote MAC	10.10.13.2/24	WEP
	Radio 0 Wds 1	2	Remote MAC	10.10.23.2/24	WPA

Node 1 Configuration Step:

```
Hello, Welcome to D-Link CLI

DWR-500> en
DWR-500# configure terminal
DWR-500(config)# security-profile  wep wep1
```

```
% Modifying an existing wep profile...
DWR-500(config-security-profile)# wep-key "abcde"
DWR-500(config-security-profile)# end
DWR-500# configure terminal
DWR-500(config)# interface dot11radio 1
DWR-500(config-if-dot11radio)# no wds auto
DWR-500(config-if-dot11radio)# wds 0
DWR-500(config-if-dot11radio-wds)# ip address 10.10.12.1/24
DWR-500(config-if-dot11radio-wds)# remote node 2 1
DWR-500(config-if-dot11radio-wds)# quit
DWR-500(config-if-dot11radio)# wds 1
DWR-500(config-if-dot11radio-wds)# ip address 10.10.13.1/24
DWR-500(config-if-dot11radio-wds)# remote mac 00:17:7b:00:22:88
<0-wds># authentication shared wep wep1 default-key 1
DWR-500(config-if-dot11radio-wds)# end
```

The above 00:17:7b:00:22:88 is the node 3 radio 0 physical address.

Node 2 Configuration Step:

```
DWR-500> en
DWR-500# configure terminal
DWR-500(config)# node-id 2
NOTE: node-id changes will only take effect after you save and reboot.
DWR-500(config)# router-id 10.0.0.2
DDWR routing service restarted
DWR-500(config)# end
DWR-500# configure terminal
DWR-500(config)# security-profile wpa wpa1
% Adding new wpa profile...
DWR-500(config-security-profile)# wpa-type psk ascii 1234567
%WARNING: Your key is weak. More than 20 characters will be better.
DWR-500(config-security-profile)# end
DWR-500# configure terminal
DWR-500(config)# interface dot11radio 1
DWR-500(config-if-dot11radio)# no wds auto
DWR-500(config-if-dot11radio)# wds 0
DWR-500(config-if-dot11radio-wds)# ip address 10.10.12.2/24
DWR-500(config-if-dot11radio-wds)# remote node 1 1
DWR-500(config-if-dot11radio-wds)# quit
DWR-500(config-if-dot11radio)# wds 1
DWR-500(config-if-dot11radio-wds)# ip address 10.10.23.1/24
DWR-500(config-if-dot11radio-wds)# remote node 3 0
DWR-500(config-if-dot11radio-wds)# ssid dwr
<0-wds># authentication open key-management wpa wpa1
DWR-500(config-if-dot11radio-wds)# end
DWR-500# write memory
DWR-500#
```

Node 3 Configuration Step:

```
Hello, Welcome to D-Link CLI

DWR-500> en
DWR-500# configure terminal
DWR-500(config)# node-id 3
NOTE: node-id changes will only take effect after you save and reboot.
DWR-500(config)# router-id 10.0.0.3
DDWR routing service restarted
DWR-500(config)# end
DWR-500# configure terminal
```

```
DWR-500(config)# security-profile wep wep1
% Modifying existed wep profile...
DWR-500(config-security-profile)# wep-key 1 “abcde”
DWR-500(config-security-profile)# end
DWR-500# configure terminal
DWR-500(config)# wpa-type psk ascii 1234567
%WARNING: Your key is weak. More than 20 characters will be better.
DWR-500(config-security-profile)# end
DWR-500# configure terminal
DWR-500(config)# interface dot11radio 0
DWR-500(config-if-dot11radio)# mode backhaul
DWR-500(config-if-dot11radio)# wireless-mode a 161 US
DWR-500(config-if-dot11radio)# no bss dwr
DWR-500(config-if-dot11radio)# wds 0
%WARNING: radio is currently operating on channel 6, different from configured channel 161.
DWR-500(config-if-dot11radio-wds)# ip address 10.10.13.2/24
DWR-500(config-if-dot11radio-wds)# remote mac 00:10: 7b: 00: 22:28
<0-wds># authentication shared wep wep1 default-key 1
DWR-500(config-if-dot11radio)# wds 1
DWR-500(config-if-dot11radio-wds)# ip address 10:10:23.2/24
DWR-500(config-if-dot11radio-wds)# remote mac 00:17: 7b: 00: 22: a0
DWR-500(config-if-dot11radio-wds)# ssid dwr
<0-wds># authentication open key-mangement wpa wpa1
DWR-500(config-if-dot11radio-wds)# end
DWR-500# write memory
DWR-500#
```

In the configuration above, 00:17:7b:00:22:28 is the physical address of node 1 radio 1; and 00:17:7b:00:22:a0 is the physical address of node 2. When the three nodes all are configured successfully and rebooted, it can establish the information of Figure 2 after 15 seconds.

Manual WDS Link Problems Diagnose:
Ensuring that it had been rightly configured and rebooted, but it does not establish the simulated network environment between the three nodes as the above configuration step 2.

Manual WDS Link Problem Diagnose:

Ensuring that it had been rightly configured and rebooted, but it does not establish the simulated network environment between the three nodes as the above step 2.

The common used solutions and debugging tools for potential problems.

Problem 1： No manual WDS link between the three nodes

1 First identify whether the versions of the three nodes are official or officially compatible
2 Implement show interface dot11radio 1 node-database command on one of the nodes to identify whether other nodes can be found

The simulated information map after implementing on node 3:

```
DWR-500# show interface dot11radio 1 node-database
NODE-ID RADIO MODE CHANNEL SIGNAL TYPE     MAC-ADDRESS        CAP  MESH-ID
    1     1     A     60      6   Backhaul 00:17:7b:00:00:c8    6  DWRMesh
    2     1     A     60      2   Backhaul 00:17:7b:00:29:98    6  DWRMesh
```

a) First identify whether node 1 and node 2 existing on Node-ID option, If do, it proves that other nodes can work well and can send data packets. If do not, please confirm the practical physical distance and then contact the hardware staff to identify whether there are any problems of node hardware.
b) Then check the SIGNAL option: if the data value is less than 10, it must strengthen the signal (the problem may be caused by weak signal). Manual WDS link can be established successfully when the data value above 10.
c) Finally check MESHI-ID option: Manual WDS link can be established when the option data is in line with its MESH-ID. Check its MESH-ID option data under the command of show interface dot11radio 1. Refer to the below MESH-ID data:

```
DWR-500# show interface dot11radio 1
Interface Dot11radio1
   Operation_mode: backhaul, mesh id: dwrmesh, country code: US, channel policy: 0,
   antenna: 1, cts protection: 2,
   distance: 0, short retry: 7, long retry: 4,
   admin status: up  Physical status: up
   index 35 metric 1 mtu 1500<UP, BROADCAST, RUNNING, MULTICAST>
   HWmode: a, channel:161, Fragment thr: 2346, RTS thr: 2347
   HWaddr: 00:17:7b:00:22:a8
     input packets 14087655, bytes 2371862791, droped 0, multicast packets 0
     input errors 1192848, length 0, overrun 0, CRC 0, frame 42, fifo 0, missed 0
     output packets 41294503, bytes 2528991393, dropped 0
     output errors 64127, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
     collision 0
```

Typical configuration of automatic WDS link:

Establish automatic WDS link environment between the three nodes according to the actual network application, and the three nodes all are factory default configuration. Configure the three nodes to simulate an automatic MESH network:

Establish a automatic WDS link as the following Figure 1:

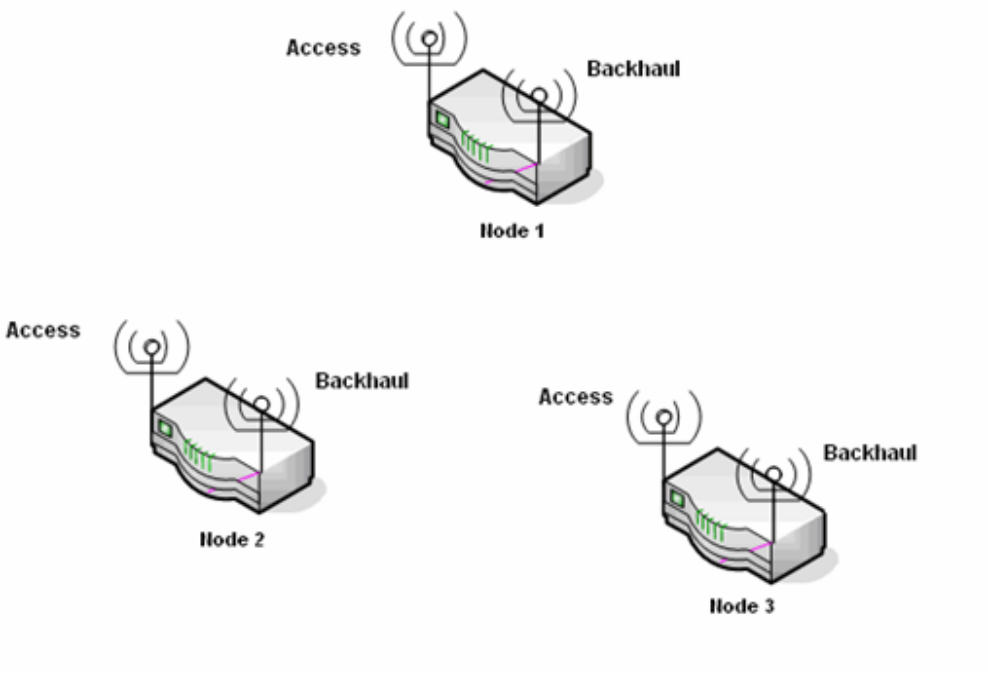


Figure 23 Simulated Auto WDS Map 1

After establishment, the auto WDS link map 2:

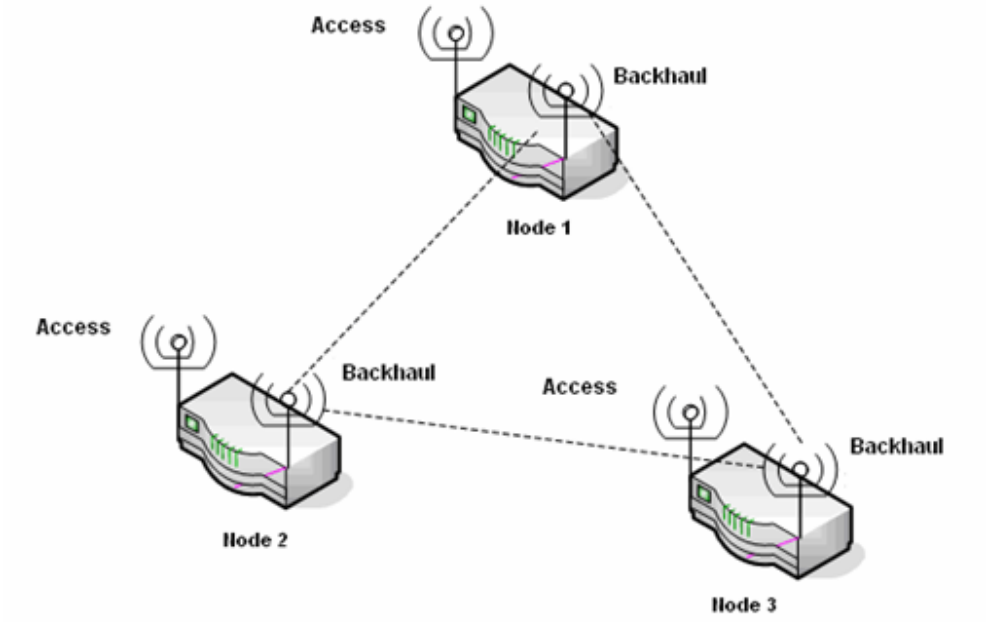


Figure 24 Simulated WDS Map 2

Configuration Steps Summary:

The first：Node 1, node 2 and node 3 all are factory defaulted

The second：Load node 1 for configuration setting. Please refer to the configuration step of node 1

The third：Load node 2 for configuration setting. Please refer to the configuration step of node 2

The forth：Load node 3 for configuration setting. Please refer to the configuration step of node 3

The fifth：When the configuration finished and be rebooted, the auto WDS link information can be viewed through WDS link diagnose command after 15 seconds.

Table 35 Node configuration summary

Node ID	1	2	3
Router ID	10.0.0.1	10.0.0.2	10.0.0.3
Radio 0	Access	Access	Access
Radio 1	Backul/wds auto/Mode a	Backul/wds auto/Mode a	Backul/wds auto/Mode a

Node 1 Cofiguration：

Default configuration

Node 2 Configuration：

```
Hello, Welcome to D-Link CLI

DWR-500> en
DWR-500# configure terminal
DWR-500(config)# node-id 2
NOTE: node-id changes will only take effect after you save and reboot.
DWR-500(config)# router-id 10.10.0.2
DDWR routing service restarted
DWR-500(config)# end
DWR-500# write memory
DWR-500# reboot
Proceed with reload? (yes/no) yes
```

Node 3 Configuration：

```
Hello, Welcome to D-Link CLI

DWR-500> en
DWR-500# configure terminal
DWR-500(config)# node-id 3
NOTE: node-id changes will only take effect after you save and reboot.
DWR-500(config)# router-id 10.10.0.3
DDWR routing service restarted
DWR-500(config)# end
DWR-500# write memory
DWR-500# reboot
Proceed with reload? (yes/no) yes
```

The three nodes being configured successfully and rebooted, it can establish the simulated map 2 topology environment after 30s.

When automatic WDS link established successfully, it can view WDS link information through WDS link diagnose order.

show interface brief : View all the equipment interface information under this order, including wireless network interface and the Ethernet interface.
show rf-management interface: View all the interface information build by RFM under this order, only wireless network interface included.
show rf-management active-neighbors: View all the candidate neighbor information that RFM model can scan under this order, every radio can display the top strongest twelve nodes information at most.

Automatic WDS Link Problem Diagnose:

Ensuring that it had been rightly configured and rebooted, but it does not establish the simulated network environment between the three nodes as the above step 2.

Problem 1： No automatic WDS link between the three nodes

1 First identify whether the versions of the three nodes are official or officially compatible
2 Implement show interface dot11radio 1 node-database command on one of the nodes to identify whether other nodes can be found.

The simulated information map after implementing on node 3:

```
MSR2000# show interface dot11radio 1 node-database
NODE-ID RADIO MODE CHANNEL SIGNAL TYPE     MAC-ADDRESS        CAP  MESH-ID
     1     1     A     60      6   Backhaul 00:17:7b:00:00:c8    6  AzaleaMesh
     2     1     A     60      2   Backhaul 00:17:7b:00:29:98    6  AzaleaMesh
```

First identify whether node 1 and node 2 existing on Node-ID option, If do, it proves that other nodes can work well and can send data packets. If do not, please confirm the practical physical distance and then contact the hardware staff to identify whether there are any problems of node hardware. Implementing on node 1 and node 2.

Then check the SIGNAL option: if the data value is less than 10, it must strengthen the signal (the problem may be caused by weak signal). Manual WDS link can be established successfully when the data value above 10.

Finally check MESHI-ID option: Manual WDS link can be established when the option data is in line with its MESH-ID. Check its MESH-ID option data under the command of show interface dot11radio 1. Refer to the below MESH-ID data:

```
MSR2000# show interface dot11radio 1
Interface Dot11Radio1
  operation_mode:backhaul,mesh id:AzaleaMesh, country code:US, channel policy:0,
  antenna:1, cts protection:2,
  distance:0, short retry:7, long retry:4,
  admin status: up  physical status: up
  index 35 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWmode: a, channel: 161, Fragment thr: 2346, RTS thr: 2347
  HWaddr: 00:17:7b:00:22:a8
    input packets 14087655, bytes 2371862791, dropped 0, multicast packets 0
    input errors 1192848, length 0, overrun 0, CRC 0, frame 42, fifo 0, missed 0
    output packets 41294503, bytes 2528991393, dropped 0
    output errors 64127, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

WDS link interactive information can also be viewed through RFM module log. The defaulted RFM debugging level is none. If automatic WDS link can not be established, please configure the level of RFM log as state or frame according to the following steps. Then use show log rf-management command to analyze RFM log, as the following map:

```
S5# configure terminal
S5(config)# service rf-management
S5(config-rfm)# debug
  dump          debug-level=5
  error         debug-level=1
  frame         debug-level=4
  information   debug-level=3
  none          debug-level=0
  state         debug-level=2
S5(config-rfm)# end
S5# configure terminal
S5(config)# service rf-management
S5(config-rfm)# debug frame
S5(config-rfm)# end
S5# write memory
S5#
```

Log steps and template:

```
Hello, Welcome to Azalea CLI

M2>
M2> en
en
M2#
M2# show log rf
show log rf
01/01/00 00:00:26.487838 RFM: New log session initiated
01/01/00 00:00:26.494793 RFM: RFM opened socket 10, 11.
01/01/00 00:00:26.551973 RFM: Handle dev_resp[0] Dot11Radio1 1
01/01/00 00:00:26.552993 RFM: rfm handle radio Dot11Radio1 UP, conf /tmp/.rfm.conf1
01/01/00 00:00:26.555913 RFM: If Dot11Radio1 set phy <0,161>
01/01/00 00:00:26.559140 RFM: Handle dev_resp[1] Radio1MWds0 1
01/01/00 00:00:26.559485 RFM: handle_admin_up from wds Radio1MWds0, mac 00:17:7b:00:24:70, IP=10.125.138.1
01/01/00 00:00:26.859749 RFM: Down Ngh 00:17:7b:00:24:70 if Radio1MWds0 sets rem IP=10.125.138.2, Nmask=255.255.255.0, Bcast=10.125.
138.255
01/01/00 00:00:27.128132 RFM: debug level has been changed from 1 to 2
01/01/00 00:00:31.455889 RFM: If Dot11Radio1 ngh 00:17:7b:00:24:70 chg ATV to MANT
01/01/00 00:00:31.759444 RFM: If Dot11Radio1 node 125 ngh 00:17:7b:00:24:70 node 138 IP 10.125.138.2 UP (1,0,15) snr=14, time_diff=0
01/01/00 00:00:31.759948 RFM: If Dot11Radio1 phy up wds Radio1MWds0, ngh 00:17:7b:00:24:70
=== End of log ===
M2#
M2#
```

Record the information time and the related transition operation of RFM status on the above log. Users need to understand the procedure for RFM establishing WDS link and the working principle before viewing the log. Analyze gradually according to the steps when RFM establish the automatic WDS link.

Problem 2： Establish the below simulated network environment between the three nodes

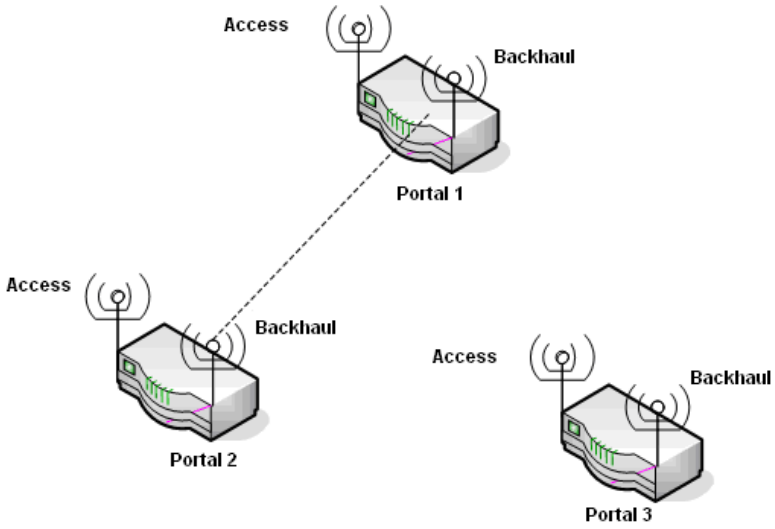


Figure 24 Simulated Network Environment between the three nodes

1 First identify whether the versions of the three nodes are official or officially compatible

2 Implement show interface dot11radio 1 node-database command to view the interactive information

```
MSR2000# show interface dot11radio 1 node-database
NODE-ID RADIO MODE CHANNEL SIGNAL TYPE     MAC-ADDRESS        CAP  MESH-ID
     1     1     A     60      6   Backhaul 00:17:7b:00:00:c8    6  AzaleaMesh
     2     1     A     60      2   Backhaul 00:17:7b:00:29:98    6  AzaleaMesh
```

First implement show interface dot11radio 1 node-database command on node 3 to identify whether node 1 and node 2 information is contained in Node-ID option. If do, it proves that node 3 can receive the data packets from other nodes correctly. If do not, please confirm the practical physical distance and then contact the hardware staff to identify whether there are any problems with node 3.
Then implement show interface dot11radio 1 node-database command on node 1 and node 2 to identify whether the information of node 3 can be discovered. If node 3 Radio works well, please contact the hardware staff to identify whether there are any problems with node 3.
Identify whether a same node 3 is existed in the NODE ID option after the above command. If does, please identify it and then close it or change the node data.
Identify whether there is a same MAC-ADDRESS data is existed that similar to node 3 Radio 1, if does, please identify the other same address and then close it or change the MAC-ADDRESS information.

Note

Router-id is unique in Mesh network；For the same Mesh Networks, it is recommended to configure the various router-IDs into a same network segment, so as to facilitate the unified management of NMS Server.
WDS link mode at both ends should be backhaul mode, rather than access or client mode.
Radio at both ends should also work in the same mode and channel.
Ensure that the Mesh-ID at both ends is the same.

Chapter 9 Configuring Routing

This chapter contains information on configuring layer-3 routing on the DWR series, it has the following sections:

Static Routing

Static routing allows the network administrator full control over the layer-3 topology and data forwarding behavior of the network. The administrator constructs the routing table for a router by specifying a route for each destination network.

A configured static route is installed in the routing table only when the route is active; that is, the route's next-hop must be bound to an operational interface. The following table summarizes the command to add/remove static route:

Table 36 Configuring Static Route

Command Syntax	Command Mode	Purpose
ip route <*A.B.C.D/M*> <*A.B.C.D*> *[<1-255>]* **no ip route** <*A.B.C.D/M*> <*A.B.C.D*>	CONFIGURATION	Add a indirect static route Remove a gateway static route A.B.C.D/M: destination network prefix/mask A.B.C.D: gateway IP address 1-255: the distance value for this route, lower is better with 255 being unreachable. (optional, default is 1)
ip route <*A.B.C.D/M*> **station** <name> <*0-N*> **no ip route** <*A.B.C.D/M*> **station** <name> <*0-N*>	CONFIGURATION	Add a directly-connected static route that binds to a client mode station Remove a directly-connected route A.B.C.D/M: destination network prefix/mask name: Station name 0-N: Index of radio interface the station belongs to.

DDWR protocol

Dynamic routing is the process through which a router learns and updates routes to the other nodes in the network. For optimal performance in a wireless mesh environment, DWR series supports the intelligent Adaptive Wireless Routing (DDWR) protocol. When DDWR is activated, each DWR series will automatically maintain a table of optimal routes to the other DWR series nodes in the network, the

clients associated to these nodes, and to the internet gateway. DDWR ensures high-performance data forwarding in a wireless mesh environment by choosing the best route in terms of cable and line quality, regardless of whether that communication is within the mesh network itself, or between a host in the network and the internet. Indicators for measuring the path quality: hops, path bandwidth, RSSI, disturbance. DDWR currently select optimal path based on the hops and Link Quality.

DDWR Introduction

DDWR working Principle

DDWR algorithm, what is known as classical distance vector algorithm, exchange router information through UDP. DDWR identify each router with router-id, which is unique in Mesh Networks.

DDWR advantages

* Adaptive, distributed and proactive routing protocol designed specific for wireless mesh network
* Works well for both mobile & fixed wireless mesh networks
* Can handle low, moderate, and high mobility rates.
* Can handle routing metrics that take radio link quality etc. into consideration.
* Well suited for large, dense mesh networks
* Can handle a variety of data traffic levels and patterns.
* Well suited for multi-radio, multi-hop wireless mesh networks
* Fast convergence enables high mobility
* Quickly adapts to both topological and link quality changes while avoiding even transient routing loops
* Low computational and communication overhead, highly scalable
* Proactive, each node knows shortest path to every other node and the wired gateway
* Support multiple gateways and load balancing
* Guarantee loop free at any instance of time
* Dynamic (link quality) metric

3-layer interface functions in DDWR

BSS/ Interface VLAN

As an access port, DDWR will inform the interface information to the neighbor networks; but can not study the DDWR router from this interface.

WDS

DDWR router can be studied when DDWR protocol message and updated message been transmitted through WDS.

Ethernet

Ethernet can be used as the access port or mesh gateway, but can not transmit DDWR protocol message in the Ethernet. When the Ethernet performs as the Mesh gateway, all the other routers in mesh will then regard this interface as the Mesh exports. DDWR also supports multi-gateway configuration.

Support Multi-gateway

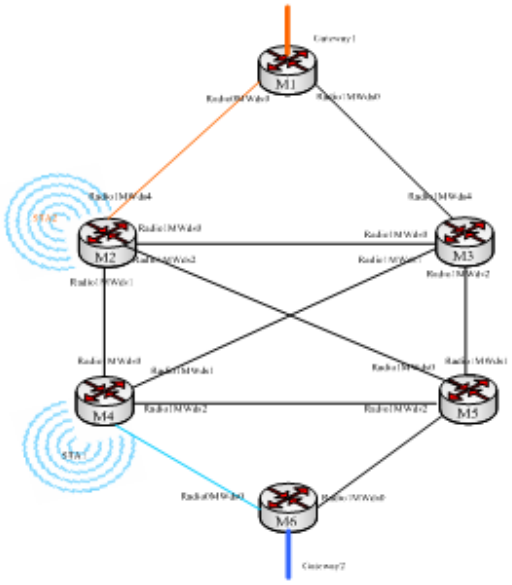


Figure 25 Multi-gateway Simulation Map

M1-M6 in the above figure all can enable DDWR protocol, and M1 and M6 works as the gateway. When the wireless terminals STA1 access to M2 and wireless terminals STA2 access to M4, STA1 will choose M1 as the gateway and STA2 corresponding to M6. The advantages for multi-gateway: When there are a number of gateway exports in the Mesh Network, choosing the nearest gateway as the export, flow shared and gateway backup in the mesh network can be done by enabling the non-gateway router in DDWR protocol.

DDWR Gateway Switchover

DDWR Primary Gateway Election (APGE) protocol is designed to support the gateway redundancy for an DDWR mesh network. APGE choose gateway according to the router-id, with only one gateway enabled, and the rest in a backup state; when the main gateway encounter problems, it can switch to the backup gateway rapidly.

DDWR command protocol：

Table 37 Configuring Static Route

Command Syntax	Command Mode	Purpose
primary-gateway-election **no primary-gateway-election**	ROUTER DDWR	Enable APGE protocol Disable APGE protocol

DDWR Enhancing Functions:

Dynamic-metric

Router algorithm enables Dynamic-metric DDWR which considers both hops and link quality comprehensively, so it can reflect the actual situation better. The reason why DDWR select transmit

rate as the link quality criterion is that the transmit rate in wireless networks depends on signal strength, interference and so on, which can reflect the wireless communications quality truly.

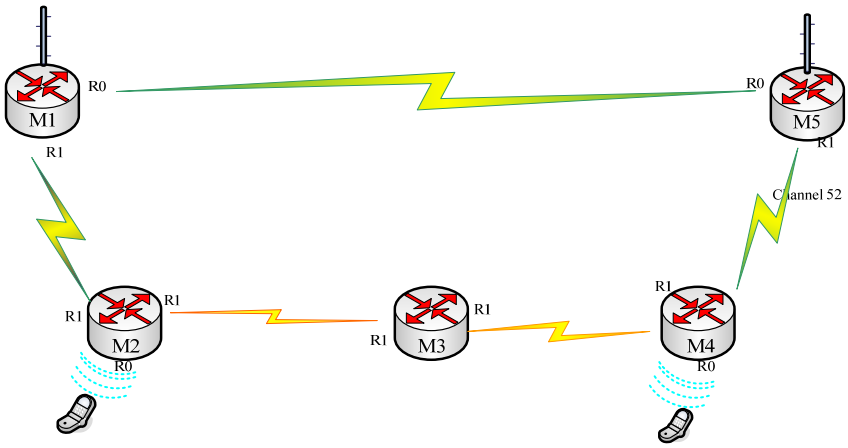


Figure 26 Dynamic-metric Simulation Map

See the road selection of the above two wireless terminals.

When Dynamic-metric enabled, the 2 wireless terminals may not choose the path of few jumps(red path), whereas, it may choose the path with the minimum value of Dynamic - metric as the final path(red or green paths)

The path dynamic-metric is the sum metric value of all the path jump interfaces, while the metric value is inversely proportional with the transmit rate of interfaces, so the more rapidly the transmit rate, the minimum Metric value.

Hello-on-wds

Enable Hello-on-wds is to open WHP（Wireless Hello Protocol）, WHP has the following functions:

1. neighbor discovery
2. neighbor failure detection
3. transmission rate algorithm of each jump

DDWR configuration commands

The following table summarizes the configuration commands that control the operation of DDWR:

Table 38 DDWR configuration command

Command Syntax	Command Mode	Purpose
router DDWR **no router DDWR**	CONFIGURATION	Start the configuration of the DDWR routing protocol Disable DDWR and remove its configuration

enable	ROUTER DDWR	Administratively activate the DDWR routing protocol[15]
disable	ROUTER DDWR	Administratively disable the DDWR routing protocol
hello-on-wds **no hello-on-wds**	ROUTER DDWR	Set WDS hello Once one router start this protocol, other routers must start to get the router Disable WDS hello
dynamic-metric **no dynamic-metric**	ROUTER DDWR	Set ddwr dynamic metrix Disable ddwr dynamic metrix
debug **debug none** **debug error** **debug state** **debug information** **debug dump**	ROUTER DDWR	Set the DDWR debug log level Disable DDWR debug log Set DDWR debug log to record errors Set DDWR debug log to record errors & state changes Log error, state, and other detailed information Log all DDWR debug information

Typical Configuration

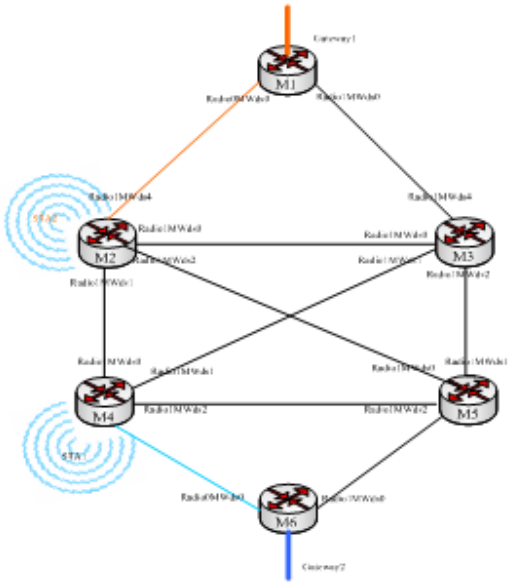


Figure 27 Simulated Configuration Map

[15] If DDWR is administratively enabled, it should be running as long as it has a valid configuration.

DDWR configuration：

```
M1：(gateway)
M1(config)#router-id 10.2.2.1
M1(config)#router DDWR
M1(config-DDWR)#enable
M1(config-DDWR)#dynamic-metric
M1(config-DDWR)#hello-on-wds
M1(config-DDWR)#exit
M1(config)#interface fast-ethernet 0
M1(config-if-ethernet)#mode gateway

M2：(non-gateway)
M2(config)#router-id 10.2.2.2
M2(config)#router DDWR
M2(config-DDWR)#enable
M2(config-DDWR)#dynamic-metric
M2(config-DDWR)#hello-on-wds
M2(config-DDWR)#exit
```

DDWR Diagnose

Displaying current routing status

The following commands can be entered at the privileged EXEC prompt to display information about the system routing table and/or the DDWR protocol state:

Table 39 Route and DDWR status configuration under PRIVILEGED EXEC

Command Syntax	Command Mode	Purpose
show ip route	PRIVILEGED EXEC	Display the current routing table
show ip forwarding	PRIVILEGED EXEC	Display the current layer-3 forwarding information
show log DDWR	PRIVILEGED EXEC	Display the debug log of DDWR (see debug command above)
show ip DDWR configuration	PRIVILEGED EXEC	Display the current DDWR configuration and status
show ip DDWR database	PRIVILEGED EXEC	Display the routing data currently tracked by the DDWR protocol
show ip DDWR neighbor	PRIVILEGED EXEC	Display the list of IP addresses of neighboring DWR series routers

Viewing routing information

```
DWR-500# show ip route
Codes: K - kernel route, C - connected, S - static, H - host,
```

```
      A - DDWR, > - selected route, * - FIB route
A>* 0.0.0.0/0 [50/267] via 10.12.1.2, Radio1MWds0, 00:00:03
A>* 10.1.1.72/32 [50/267] via 10.12.1.2, Radio1MWds0, 00:04:56
C>* 10.2.2.71/32 is directly connected, lo:2
A>* 10.2.2.73/32 [50/1335] via 10.41.1.2, Radio1MWds2, 00:00:03
A>* 10.2.2.74/32 [50/267] via 10.41.1.2, Radio1MWds2, 01:11:40
A>* 10.2.2.75/32 [50/533] via 10.41.1.2, Radio1MWds2, 01:11:40
A>* 10.2.2.76/32 [50/800] via 10.41.1.2, Radio1MWds2, 00:49:09
C>* 10.12.1.0/24 is directly connected, Radio1MWds0
H>* 10.12.1.1/32 [0/0] is directly connected, Radio1MWds0
A>* 10.37.1.0/24 [50/1335] via 10.41.1.2, Radio1MWds2, 00:00:03
C>* 10.41.1.0/24 is directly connected, Radio1MWds2
H>* 10.41.1.1/32 [0/0] is directly connected, Radio1MWds2
A>* 10.54.1.0/30 [50/267] via 10.41.1.2, Radio1MWds2, 01:11:40
A>* 10.56.1.0/24 [50/534] via 10.41.1.2, Radio1MWds2, 00:49:15
A>* 10.67.1.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:13:42
S   10.111.0.0/16 [1/0] via 10.17.1.1
A>* 172.16.75.0/24 [50/577] via 10.41.1.2, Radio1MWds2, 00:59:53
S>* 192.168.10.0/24 [1/0] via 192.168.15.1, fast-ethernet 0
C>* 192.168.15.0/24 is directly connected, fast-ethernet 0
H>* 192.168.15.71/32 [0/0] is directly connected, fast-ethernet 0
A>* 10.216.1.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:49:09
A>* 10.216.2.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:49:09
A>* 10.216.3.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:49:09
A>* 10.216.4.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:49:09
A>* 10.216.5.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:49:09
A>* 10.216.6.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:49:09
A>* 10.216.7.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:49:09
A>* 10.216.8.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:49:09


DWR-500# show ip DDWR neighbor
DDWR internal neighbor table:
Nbr 10.12.1.2       ,metric 1   ,bw   NA  Kbps, uptime 0:9:9
Nbr 10.41.1.2       ,metric 1   ,bw   NA  Kbps, uptime 1:15:56


Enable Dynamic-metric and Hello
DWR-500# show ip route
Codes: K - kernel route, C - connected, S - static, H - host,
      A - DDWR, > - selected route, * - FIB route

C>* 10.2.2.71/32 is directly connected, lo:2
A>* 10.2.2.73/32 [50/1332] via 10.41.1.2, Radio1MWds2, 00:01:41
A>* 10.2.2.74/32 [50/267] via 10.41.1.2, Radio1MWds2, 01:03:30
A>* 10.2.2.75/32 [50/533] via 10.41.1.2, Radio1MWds2, 01:03:30
A>* 10.2.2.76/32 [50/800] via 10.41.1.2, Radio1MWds2, 00:40:59
A>* 10.2.2.77/32 [50/1066] via 10.41.1.2, Radio1MWds2, 00:01:41
A>* 37.1.1.0/24 [50/1332] via 10.41.1.2, Radio1MWds2, 00:01:41
C>* 10.41.1.0/24 is directly connected, Radio1MWds2
H>* 10.41.1.1/32 [0/0] is directly connected, Radio1MWds2
A>* 10.54.1.0/30 [50/267] via 10.41.1.2, Radio1MWds2, 01:03:30
A>* 10.56.1.0/24 [50/534] via 10.41.1.2, Radio1MWds2, 00:41:05
A>* 10.67.1.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:05:32
S   10.111.0.0/16 [1/0] via 10.17.1.1
A>* 172.16.75.0/24 [50/577] via 10.41.1.2, Radio1MWds2, 00:51:43
S>* 192.168.10.0/24 [1/0] via 192.168.15.1, fast-ethernet 0
C>* 192.168.15.0/24 is directly connected, fast-ethernet 0
H>* 192.168.15.71/32 [0/0] is directly connected, fast-ethernet 0
A>* 10.216.1.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:40:59
A>* 10.216.2.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:40:59
A>* 10.216.3.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:40:59
```

```
A>* 10.216.4.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:40:59
A>* 10.216.5.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:40:59
A>* 10.216.6.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:40:59
A>* 10.216.7.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:40:59
A>* 10.216.8.0/24 [50/800] via 10.41.1.2, Radio1MWds2, 00:40:59


Enable Dynamic-metric and Hello
DWR-500# show ip DDWR neighbor
DDWR internal neighbor table:
Nbr 10.12.1.2       ,metric 266 ,bw 54000 Kbps, state 2WAY ,uptime 0:0:6
Nbr 10.41.1.2       ,metric 267 ,bw 53999 Kbps, state 2WAY ,uptime 1:3:44
```

Figure 28 Output of routing information

Fault Diagnose

When there are some problems with router study, please diagnose through the following steps:

1. Identify whether DDWR neighbor establishment is correct through order show ip DDWR neighbor. If without any neighbors, DDWR then can not study other routers routing. The possibilities for non-establishing the neighbors:
   a) If WDS interface is not in the status of UP，then enter show rf-management active-neighbor command to view the specific reason;
   b) If WDS interface is UP，but when the IP address is repeated or when the mask is different, it must revise the IP address at both ends, to ensure that the IP address is not repeated and the mask is the same.
2. Check whether router-id is unique in Mesh network
3. The Ethernet interface routing is not displayed in DDWR, please check whether Ethernet interface is set at Access mode; it can be viewed through order show running-config

OSPF

OSPF Introduction

OSPF is the abbreviation of open shortest path first which is developed by the IETF organization based on the Link State autonomy within the system routing protocol. OSPF can also collect or transmit the link status of autonomy system to discover and transmit the routing dynamicly.

Every router running OSPF protocol always describes the local network connection status (such as available interface information, reachable neighbor information, etc.) by LSA(Link Status Advertisement), and then advertise the information to the whole autonomy system. Thus, every router shall receive the LSA generated by all the autonomous systems routers, which formed the LSDB (link state database) of LSA. As each LSA is the description of the router surrounding network topology, the whole autonomy system LSDB is the true reflection of the network topology.

According to the LSDB, all the routers run SPF (Shortest Path First) algorithm. Establish a shortest path tree roots which list all the autonomy system nodes routing. "Tree" is a non-connection loop on the map, so the routing calculated by OSPF is also a non-routing loop.

In order to reduce the OSPF protocol cost, the following concepts are put forward:

(1) DR: In all kinds of multi-service network, it must designate a router if two or more routers exist in the network. "Designated router" takes charge of the synchronization of LSDB of all the routers internet. Thus two routers that are not the designated routers will no longer do the LSDB synchronization. Nonetheless, it has significant saved the same bandwidth cost.

(2) AREA: OSPF can be divided into different areas according to the autonomy system topology (AREA), thus when the area border router (ABR) send information to other regionals, it will generate the LSA summary with the network units which helps reduce the LSA numbers in the autonomy system and also reduce the complexity of routing calculation.

There are 4 types of routing with OSPF, in priority order they are:

·Intra-regional routing
·Inter-regional routing
·The first category external routing
·The second category external routing

Intra-regional and inter-regional routing describes the network structure of internal autonomy system, while external routing describes how to choose a routing to the destination of outside autonomous system. Generally, the first category external routing corresponds to the information which OSPF introduces from other internal routing protocol, the routing cost is almost the same as OSPF routing cost; The second category external routing corresponds to the information that OSPF introduces from the external routing protocol, and their own cost is more than that of OSPF routing, so it will only consider the external costs in the calculation.

OSPF Protocol Advantages

1. OSPF is the real LOOP-FREE (no-routing self central) routing protocol which derives from its own algorithm advantages.(Link state and the shortest path tree algorithm).
2. OSPF owns fast convergence, which can communicates the routing changes to the whole autonomous system in the shortest time.
3. Propose the concept area division: when the autonomous system being divided into different areas, it will reduce the required routing information that needed to transmission through the inter-routing summaries, which also makes the routing information will not expand rapidly with the expansion of the network scales.
4. Control the protocol cost to the minimum
   1) Hello message which contains the non-regular routing information is used to discover and maintain neighbors. It is very short and when contains routing information message, it must be the update trigger mechanism(send when routing changes). However, in order to enhance the robustness of the protocol, it will re-send the information every 1,800 seconds.
   2) Multicast addresses send messages(but not advertise)can reduce the interference that inflects the un-running OSPF network device.
   3) In the various multi-address access networks, through the election of DR, it makes the routing exchange number(synchronous) in the same network reduces from the number of O (N * N) to O (N).
   4) Propose the concept of STUB area: no longer spread the introducing ASE routing in the STUB area.
   5) Support routing polymerization in ABR (regional border router) to further reduce the inter-regional routing information transmission.

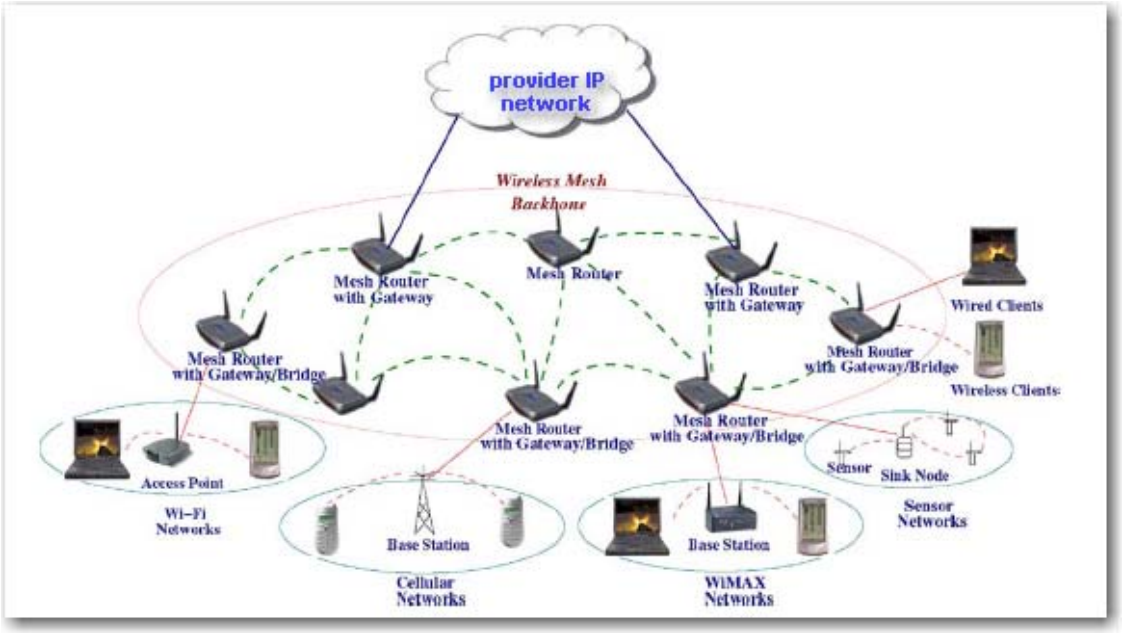
6) In point-to-point interface, through on-demand allocation of advertise properties (OSPF over On Demand Circuits), it makes OSPF no longer advertise regular hello message or updated routing information regularly. It only update information when the network topology changes.

5. Through strict division of routing (divided into four levels) to provide more credible routing.
6. Good security, ospf support proclaimation based on interface and md5 certification.
7. OSPF adapt to a variety of networks with the number up to thousands of.

OSPF Application on DWR

- DWR series router support OSPF protocol at the mesh gateway, which can be added to the OSPF domain as the internal routers to learn the internal routing. DWR series routers do not support ABR now.

The following diagram shows a typical wireless mesh network topology. Running OSPF protocol at the Mesh gateway:



- Introduce Mesh routing：OSPF at the gateway can introduce the DDWR routing and straight routing to the OSPF domain as the second external routing to achive the same network routing.

OSPF Configuration Command

- Enable OSPF
- Configure the network interface to the OSPF domain
- Introduce Mesh routing

Enable OSPF

Table 40 Enable OSPF Command

Command Syntax	Command Mode	Purpose
router ospf	CONFIGURATION	Configure OSPF

no router ospf		Close OSPF and also remove the configuration
enable	ROUTER OSPF	Enable OSPF
disable	ROUTER OSPF	Disable OSPF

Configure the network interface to the OSPF domain

Table 41 Configure the network interface to the OSPF domain

Command Syntax	Command Mode	Purpose
network *<A.B.C.D/M>* area *<area-id>* **no network *<A.B.C.D/M>* area *<area-id>***	ROUTER OSPF	Configure the designated interfaces to the OSPF domain Remode the corresponding configuration

Introduce Mesh routing

Table 42 Introduce Mesh routing

Command Syntax	Command Mode	Purpose
redistribute {DDWR | connected } **<metric-type {1|2}>** **no redistribute {DDWR | connected }**	ROUTER OSPF	Introducing DDWR or routing directly to OSPF. Default set to the first external routing introduction Remove the corresponding configuration

Typical Configuration

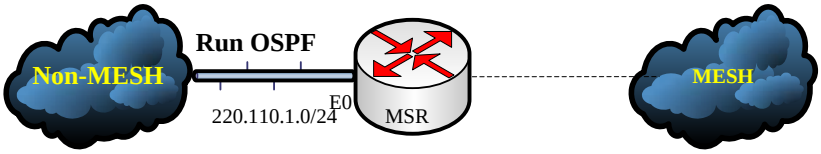


Figure 29 Typical Configuration

Running OSPF in the Mesh gateway and then add it to the AREA0, and redistribute Mesh internal routing to the non-mesh network.

OSPF Configuration:

```
DWR：(gateway)
DWR(config)#router OSPF
DWR(config-ospf)#enable
DWR(config-ospf)# network 220.110.1.0/24 area 0
DWR(config-ospf)# redistribute DDWR
DWR(config-ospf)# redistribute connected
DWR(config-ospf)# end
```

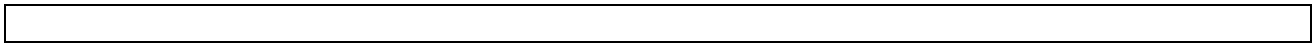


Figure 30 OSPF Configuration Information

OSPF Diagnose

Display the current Routing Status

Enter the following command at the prompt of privileged EXEC mode to display the system routing table and / or OSPF protocol status information:

Table 43 Routing and OSPF staus configuration under Privileged EXEC

Command Syntax	Command Mode	Purpose
debug {none| packet | ipc | all }	ROUTER OSPF	Set the OSPF debug log level
show ip route	PRIVILEGED EXEC	Display the current routing table
show log ospf	PRIVILEGED EXEC	Display OSPF debug log（see the previous debug command）
show ip ospf configuration	PRIVILEGED EXEC	Display the current OSPF configuration information and status
show ip ospf database	PRIVILEGED EXEC	Display the current routing data of OSPF database
show ip ospf interface	PRIVILEGED EXEC	Display the current OSPF interface information
show ip ospf neighbor	PRIVILEGED EXEC	Displaythe current OSPF neighbor routing information

View Routing Information

```
DWR-500# show ip route
Codes: K - kernel route, C - connected, S - static, H - host, O - OSPF,
       A - DDWR, R - Roaming, d - DHCP, > - selected route, * - FIB route

……
C>* 73.74.1.100/30 is directly connected, Radio0MWds3
A>* 74.135.1.0/30 [50/3] via 73.74.1.102, Radio0MWds3, 00:29:12
O>* 122.1.1.1/32 [110/11] via 192.168.15.224, fast-ethernet 0, 00:02:26
A>* 135.1.1.0/24 [50/3] via 73.74.1.102, Radio0MWds3, 00:29:12
A>* 144.2.1.0/24 [50/2] via 72.73.1.9, Radio0MWds1, 00:01:27
A>* 155.1.1.0/24 [50/2] via 72.73.1.9, Radio0MWds1, 00:01:27
S>* 192.168.10.0/24 [1/0] via 192.168.15.1, fast-ethernet 0
S>* 192.168.10.110/32 [1/0] via 72.73.1.9, Radio0MWds1
O>* 192.168.11.0/24 [110/20] via 192.168.15.232, fast-ethernet 0, 00:02:26
O>* 192.168.14.0/24 [110/20] via 192.168.15.224, fast-ethernet 0, 00:02:26
A   192.168.15.0/24 [50/2] via 73.74.1.102, Radio0MWds3, 00:01:44
O   192.168.15.0/24 [110/10] is directly connected, fast-ethernet 0, 00:49:05
C>* 192.168.15.0/24 is directly connected, fast-ethernet 0
A>* 192.168.135.135/32 [50/3] via 73.74.1.102, Radio0MWds3, 00:29:12
O>* 222.1.1.0/24 [110/20] via 192.168.15.1, fast-ethernet 0, 00:02:19
O>* 222.1.2.0/24 [110/20] via 192.168.15.1, fast-ethernet 0, 00:02:19
O>* 222.1.3.0/24 [110/20] via 192.168.15.1, fast-ethernet 0, 00:02:19
O>* 222.1.4.0/24 [110/20] via 192.168.15.1, fast-ethernet 0, 00:02:19
O>* 222.1.5.0/24 [110/20] via 192.168.15.1, fast-ethernet 0, 00:02:19
O>* 222.1.6.0/24 [110/20] via 192.168.15.1, fast-ethernet 0, 00:02:19
```

```
Display OSPF Configuration Information
DWR-500# show ip ospf configuration
 status CONFIGURED RUNNING
 enable
 debug none
 redistribute DDWR
 redistribute connected
 network 192.168.15.0/24 area 0
 network 135.1.1.0/24 area 0


Display OSPF Interface Information
DWR-500# show ip ospf interface
eth0 is up, line protocol is up
  Internet Address 192.168.15.73/24, Area 0.0.0.0
  Process ID 0, Router ID 10.2.2.73, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.15.232, Interface address 192.168.15.232
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 3, Adjacent neighbor count is 2


Display OSPF Neighbor Information
DWR-500# sho ip ospf neighbor
Neighbor ID    Pri      State        Dead Time Address        Interface Area
10.2.2.70      1      2WAY/DROTHER 00:00:33 192.168.15.70   eth0      0.0.0.0
122.1.1.1      1      FULL/BDR     00:00:36 192.168.15.224  eth0      0.0.0.0
192.168.15.232 1      FULL/DR      00:00:35 192.168.15.232  eth0      0.0.0.0


Display OSPF Database Information
DWR-500# show ip ospf database
          OSPF Router with ID (10.2.2.73) (Process ID 0)
             Router (Area 0.0.0.0)
Link ID         ADV Router       Age     Seq#         Checksum    Link count
10.2.2.70       10.2.2.70        73      0x80000156    0x2cfe         1
10.2.2.73       10.2.2.73        53      0x80000006    0xcfa1         1
122.1.1.1       122.1.1.1        947     0x80000191    0xb709         3
192.168.15.232  192.168.15.232   790     0x800001e0    0x6acc         2
             Network (Area 0.0.0.0)
Link ID         ADV Router       Age     Seq#         Checksum
192.168.15.232  192.168.15.232   59      0x80000256    0xbbd3
             Type-5 AS External
Link ID         ADV Router       Age     Seq#         Checksum  Tag
1.1.1.0         10.2.2.73        26      0x80000009    0x4715    0
10.0.70.0       10.2.2.73        26      0x80000009    0xd140    0
10.0.70.4       10.2.2.73        26      0x80000009    0xa964    0
10.2.2.70       10.2.2.73        26      0x8000000a    0xf910    0
10.2.2.71       10.2.2.73        32      0x8000000b    0xed1a    0
10.2.2.72       10.2.2.73        32      0x8000000d    0xdf25    0
10.2.2.73       10.2.2.73        58      0x80000004    0xe725    0
10.2.2.74       10.2.2.73        58      0x80000003    0xdf2d    0
10.129.24.0     10.2.2.73        26      0x8000000a    0xcbee    0
10.214.206.0    10.2.2.73        32      0x8000000d    0xebbf    0
70.71.1.0       10.2.2.73        32      0x8000000b    0x735b    0
71.72.1.0       10.2.2.73        32      0x8000000d    0x4489    0
72.73.1.8       10.2.2.73        58      0x80000004    0xecdf    0
72.74.1.12      10.2.2.73        58      0x80000007    0xb212    0
73.74.1.100     10.2.2.73        58      0x80000004    0x3836    0
74.135.1.0      10.2.2.73        58      0x80000003    0x3a5b    0
135.1.1.0       10.2.2.73        58      0x80000003    0x7e5d    0
```

```
144.2.1.0       10.2.2.73        32     0x8000000d    0xe8de    0
155.1.1.0       10.2.2.73        32     0x8000000d    0x6558    0
192.168.135.135 10.2.2.73        58     0x80000003    0xa745    0
222.1.1.0       122.1.1.1        948    0x800000cb    0x8875    0
222.1.2.0       122.1.1.1        948    0x800000cb    0x7d7f    0
…
```

Figure 31 Routing Information Status Display

Fault Diagnose

When there are problems with router learning, please diagnose through the following steps:

1. Check whether the OSPF neighbor establishment is correct using the command of show ip ospf neighbor, if no OSPF neighbors, it will not learn the routing of other routers. Possibilities of no neighbor establishment:
   a) Check whether the configuration of OSPF is correct using show ip ospf configuration command. Please check whether the Ethernet interface being configured to the corresponding OSPF domain; or OSPF domain configuration is incorrect.
   b) Please check the OSPF hello time and dead time on both ends and the retry times; DWR series router do not support these kinds of parameters now, please revise on the opposite end.
   c) Currently OSPF does not support authentication, if the OSPF authentication works in the opposite-end, please shut down.
   d) If the Ethernet interfaces of DWR series routers being configured to Mode access, this router will not run OSPF protocol.

Chapter 10 Configuring Dtrix Roaming

Dtrix Protocol Overview

Dtrix- D-Link IEEE 802.11-based 2.5 layer roaming protocol of wireless Mesh network. The 2.5-layer uses MAC layer trigger mechanism in the process of roaming, and add or delete routing in the IP layer coordinately, thus to eliminate the stratified separate roaming delay. Dtrix ensures that the IP addresses of client STA unchanged when switching between different IP subnet and the user's communications data will not be affected. Meanwhile, Dtrix has done special treatment to the unusual event in the mass Mesh Network Router and STA, which guarantees greatest the building of the new network link or the maintaining of the original network of various clients at any time, any place.

IEEE 802.11 supports Layer 2 roaming, but undefined the information exchange details between AP in the process of roaming, which poses a problem to the STA mobility of wireless site that STA can not move freely between different manufacturers' AP.

IAPP protocol aims to provide the mobile function between AP which solves the communications problem of link layer caused by mobile users. But it only guarantees that it is in the same Subnet of the different BSS. When STA roaming to different network, the original STA gateway and IP address has changed so that the user top data communication will not be able to carry on.

The layer 3 roaming solutions, represent by the mobile IP has successfully achieved the STA inter-subnet roaming. In addition, the Mobile IP technology can provide mobility in various media and in arbitrarily large geographical areas. This is the unique capability of layer 3. Using mobile IP, as long as it can be connected to the Internet, it can communicate through a fixed IP address.

But mobile IP technology also has to be improved in many aspects, especially the roaming delay. For the original Mobile IP protocol, the network layer switch delay is in average 300ms, or even several seconds. Therefore, such kind of delay thus can not meet the delay-sensitive VoIP businesses. The reason is, in the process of roaming, that Mobile IP spends a lot of time in allocating the address, detecting the unique address and the process of discovering routers. Therefore, in addition to the further improvement, the Mobile IP should also focus on the macro mobility to minimize the frequency which mobile IP supports during the STA roaming process. There are also a lot of technologies that make great contributions in micro-mobile, for example, HMIPv6, Cellular IP and Hawai, etc. These mechanisms all are based on routing technology. It avoids the tunnel cost, but at the same time increases the routing table overhead.

In addition, Mobile IP roaming trigger mechanism of layer 3 is not efficient as the layer 2 mechanism, though Mobile IP has done a lot of changes (such as ECS, HCS, FHCS), IEEE802.11 protocol framework decides that the client roaming mode switch must be hard handoff and must be forward handoff(The roaming process only refers to the interaction between client and the new AP, but not the client and the old AP). This limits the application of the improvement program of Mobile IP in the IEEE 802.11 network. In addition, the Mobile IP client itself also needs the support from clients, which further affects the market development of Mobile IP technology.

Therefore, a technology is needed which succeeds the roaming merit of layer 2 and plays the advantage of inter-subnet roaming of layer 3. Thus D-Link Dtrix comes into being.

Dtrix Configuration

This section covers the following main topics:

Dtrix-related configuration information

1) The roaming gateway

Dtrix requires the specification of a single gateway router on each access router that provides roaming support. Even when there are multiple gateways connected to the same mesh network, one of them needs to be specified as the “roaming gateway” router.

2) MAC-IP list of other BSSs

The Dtrix service also requires the IP and MAC address of every BSS (or virtual AP) within the mesh network. This information is automatically learned if the DDWR routing protocol is enabled. However, if Dtrix is to be used while DDWR is not running, then the MAC-IP mapping must be configured manually through the **mac-ip-list** command described below. Each entry in the MAC-IP list is a mapping that associates a BSS’s MAC address with its router ID.

Note: The MAC-IP list is indexed by the BSS MAC address, and each MAC address may be associated with only one IP address.

3) Static IP client list

In some applications, clients use preconfigured static IP addresses. To support such clients, only one wired-gateway router could be present in the mesh network and a station list need to be specified on each participating access router and the gateway router. The station list contains MAC-IP mappings that associate the static IP clients’ IP addresses with their MAC addresses. This information can only be configured manually.

Note:

There is only one wired gateway in the mesh network under this situation, and the roaming gateway address be configured to the wired gateway interface address(i.e. router-id).

The network segment of client static IP address should be different from all the existing mesh network address segment.

4) ISG Mode

In the ISG application, Dtrix must be enabled at first, and then configure it to the centralized mode and make the roaming gateway pointing at the ISG equipment.

Configuring Dtrix Service

The following table summarizes the configuration commands for Dtrix:

Table 44 Dtrix command configuration

Command Syntax	Command Mode	Purpose
service roaming-Dtrix	CONFIGURATION	Start configuration of the Dtrix Roaming Service
no service roaming-Dtrix		Disable Dtrix Roaming Service and remove its configuration
enable	SERVICE ROAMING-DTRIX	Activate the Dtrix roaming service[16]
disable		Shutdown the Dtrix Roaming service
gateway A.B.C.D	SERVICE ROAMING-DTRIX	Configure the IP address of the roaming gateway router
mac-ip-list *<HH:HH:HH:HH:HH:HH> <A.B.C.D>*	SERVICE ROAMING-DTRIX	Add an entry to the MAC-IP list
no mac-ip-list		Clear all entries of the MAC-IP list
no mac-ip-list *<HH:HH:HH:HH:HH:HH>*		Remove an entry from the MAC-IP list HH:HH:HH:HH:HH:HH: The MAC address of a BSS in the network
station-list *<HH:HH:HH:HH:HH:HH> <A.B.C.D/M>*	SERVICE ROAMING-DTRIX	Add an entry to the station list
no station-list		Clear all entries of the station list
no station-list *<HH:HH:HH:HH:HH:HH>*		Remove an entry from the station list HH:HH:HH:HH:HH:HH: The MAC address of a static-IP client in the network
debug	SERVICE ROAMING-DTRIX	Set the Dtrix debug log level
debug none		Disable Dtrix debug log
debug error		Set Dtrix debug log to record errors
debug information		Log errors and other important information
debug dump		Log all Dtrix debug information

[16] When enabled, Motrix should be running as long as it has a valid configuration.

centralized-control	SERVICE ROAMING-DTRIX	Configure Dtrix service to ISG mode Note: It needs to configure this mode when the current router works cooperately with the ISG.

The configuration orders contain: mac-ip-list, station-list, gateway，enable/disable。

Typical Configuration

Here summarizes the following recommended configuration according to the above orders points.
Example topology:

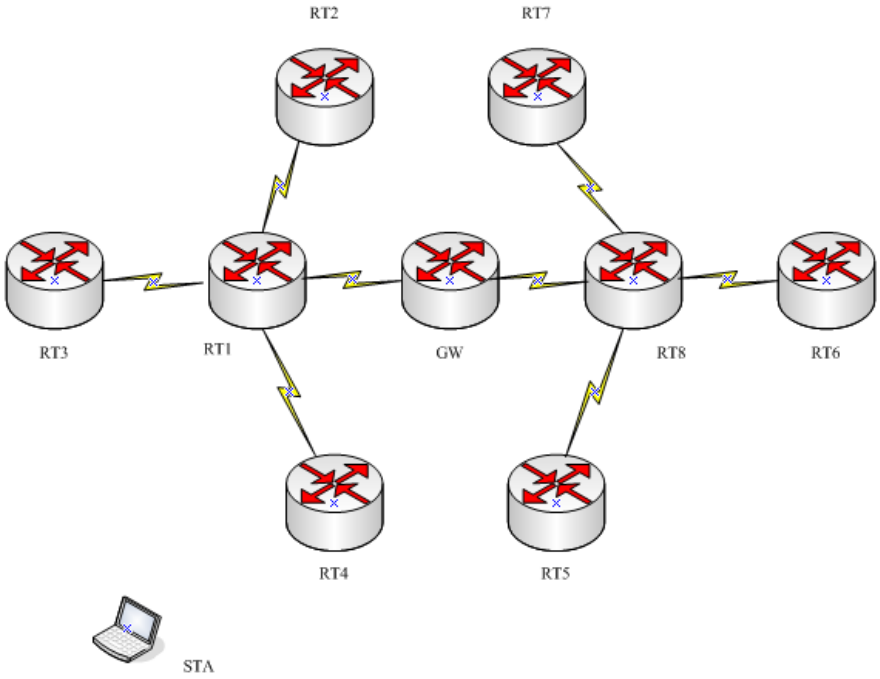


Figure 32 Typical Configuration Topology 1

STA Getting DHCP IP Address

In the practical applications, STA will get IP address by the way of DHCP. So it will be very simple for roaming configuration in such circumstances. A unified configuration will be adopted for association and reassociation clients. That is:

All routers open DDWR（RT1~RT8,GW）

All the accessing routers and gateway routers（RT2～RT7，GW） open Dtrix（non-gateway routers RT1/RT8 just for backhaul are excepted）

All the routers with access interfaces in the domain will be configured with roaming gateway(RT2~RT7) , and gateway router-id for IP address(GW)

For example：

```
DWR(config)service roaming-Dtrix
DWR (config-roaming)# enable
DWR (config-roaming)# gateway 10.19.19.5
```

STA Getting Static designated IP Address

To ensure the compatibility of all the internet client, it need to configure the static specified IP address corresponding to the client station-list on the basis of the above configuration.
For example：

```
DWR (config)#service roaming-Dtrix
DWR (config-roaming)# enable
DWR (config-roaming)# station-list 00:17:7b:00:27:40 192.168.0.222/32
DWR (config-roaming)# station-list 00:16:6f:1a:eb:80 1.1.1.0/24
DWR (config-roaming)# gateway 10.19.19.5
```

Note：
Station-list configuration does not affect the roaming process of outside station-list client; therefore, it only needs to configure client station-list on the routers which need to specify IP addresses manually. Connect to the related clients when all the routers have been configured station-list
When clients specify IP addresses, BSS can still assign DHCP address, and client gateway address can fill in the BSS interface address which will be linked to.（It has mentioned earlier that when choosing client IP address, it must ensure that the client IP address does not belong to the IP sub networks existing in the whole internet. However, there are no limitation when configuring the gateway）。If it is uncertain which BSSID will be linked firstly for client, then any BSS interface address can be filled in to configure gateway address. For example, the default gateway address of STA in topologies can be any of the BSS address of RT2 - RT7.
The network can only support one gateway router when STA using static specified IP address. Therefore, it only illustrates one gateway router in the topology. If multi-gateway exists in the mesh of the topology, then roaming can also supported in the topology. At present it is not allowed for clients to choose static IP address. In other words, it must take DHCP address. Only one portal gateway be selected as the roaming-gateway in Dtrix configuration.

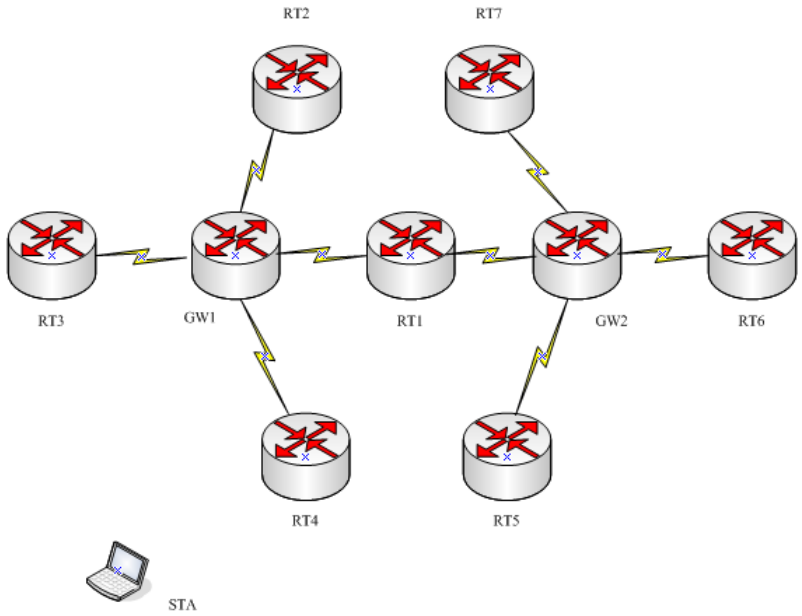


Figure 33 Typical Configuration Topology 2

Dtrix Diagnose

Displaying Dtrix Configuration and Status

Table 45 Display roaming status

Command Syntax	Command Mode	Purpose
show config	SERVICE ROAMING-DTRIX	Display the Dtrix configuration information
show log Dtrix	PRIVILEGED EXEC	Display the debug log of Dtrix (see the previous debug command)
show ip mobility Dtrix	PRIVILEGED EXEC	Display Dtrix configuration and status
show ip mobility Dtrix mac-ip-list	PRIVILEGED EXEC	Display the MAC-IP list used by Dtrix
show ip mobility Dtrix station-list	PRIVILEGED EXEC	Display the station-list information that user configured
show ip mobility Dtrix stations	PRIVILEGED EXEC	Display the clients lists that Dtrix maintains

Examples of output

View Dtrix output information：

```
DWR-500(config) # service roaming-Dtrix
DWR-500(config-roaming)# show config
!
Service roaming-Dtrix
Enable
Debug dump
Mac-ip-list 00:17:7b:fc:21:b8 10.0.0.22
Station-list 00:20:54:b1:6a:12  2.2.2.2/32
Gateway 10.0.0.19
```

View current Dtrix status information

```
DWR-500# show ip mobility Dtrix
 status RUNNING
 enable
 debug dump
 gateway ip address 10.0.0.19
```

View current routers recorded mac-ip-list

```
DWR-500# sh ip mobility Dtrix mac-ip-list
Codes: A - learned from DDWR, S - static, > - selected mapping, * - effective mapping

S>* 00:17:7b:fc:21:b8  10.0.0.22
A>* 00:17:7b:0e:f8:60  10.0.0.19
A>* 00:17:7b:0e:f8:78  10.0.0.19
A>* 00:17:7b:fc:21:e0  10.0.0.20
A>* 00:17:7b:fc:20:78  10.0.0.21
```

View the user configuration station-list

```
DWR-500# sh ip mobility Dtrix station-list
  00:20:54:b1:6a:12  2.2.2.2/32


View Dtrix maintained client list
DWR-500# sh ip mobility Dtrix stations
STATIONS:
Total number of stations: 1

  MAC: 00:14:78:10:76:f8
  IP: 10.128.76.249
  State: Home Associated
  Time since last (re)association: 41(s)
Previous AP: 00:00:00:00:00:00
Associated interface: Dot11Radio0(00:17:7b:0e:f8:60)
```

Figure 34 Output of Dtrix

Fault Diagnosis

The most commonly used critical testing way is to read the log files of Dtrix. The default debug level is info，generally, it can meet the demands of roaming test. If more detailed information of roaming is needed in log（such as keep alive the testing information ）, it can be set as dump. When no log record in needed. It can be set as none.

1) View Dtrix log order： show log Dtrix
2) Clear log records: clear log records.

Users can also view the current client Dtrix maintaining information and mac-ip-list and station-list. The current client data information of Dtrix, also Dtrix database, has recorded the client MAC address, IP address, status information, link time, the current linking BSSID and the previous BSSID, etc. Access routers and gateway routers all have the corresponding database records. The volume of the information and the presentation way will be different according to the role of the roaming routers and the process of the roaming.

The related command:

1) View client Dtrix station list： show roaming-Dtrix stations;
2) View current routers' mac-ip-list: show roaming-Dtrix mac-ip-list

In addition, as a supplement, the associated client linking routers can also be viewed to right correct the status of Dtrix.

1) view the associated client under a certain radio: show interface dot11radio INDEX stations
2) view the associated client under a certain BSS: show interface dot11radio INDEX bss <ssid> station

What Dtrix does is to automatic update the routing table from the overall results, to guarantee the access routing when changing client access point. By observing the changes between old and new routers and the changes of gateway router table, which helps users analyze the fault during roaming from the perspective of packets transmission.

1) view the system routers: show ip router fib

Chapter 11 DHCP and NAT

This chapter contains information on configuring the DHCP and NAT services on the DWR series, it has the following sections:

DHCP Protocol Overview

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. DHCP allows devices connecting to a network to automatically obtain an IP address.

In order to ensure that each STA can communicate with external internet and/or between each other, it should be assigned an IP address. The DWR series provides DHCP services such as DHCP server and DHCP Relay to dynamically assign such addresses.

Configuring DHCP Server

On DWR series, each BSS has its own private subnet. Each STA associated with a BSS obtains an IP address from the DHCP server.

- Configuring DHCP Server Parameters
- Configuring DHCP pools
- Attaching DHCP pools to BSSs or the Ethernet
- Showing DHCP Information and Status
- View DHCP Server Configuration

Configuring DHCP Server Parameters

DHCP configurations are performed in CONFIGURATION mode. The following table outlines the general DHCP configuration commands:

Table 46 Configuring DHCP Server

Command Syntax	Command Mode	Purpose
ip dhcp server **no ip dhcp server**	CONFIGURATION	Start configuration of DHCP server Stop the DHCP server and remove its configuration

enable	IP DHCP SERVER	Enable the DHCP server[17]
disable	IP DHCP SERVER	Temporarily disable the DHCP server
default-lease-time <*0-31536000*> **no default-lease-time**	IP DHCP SERVER	Set the time (in seconds) given to each DHCP lease request that does not specify a lease time. The maximum is 31536000 seconds (one year). Set this parameter to the default value of 86400 seconds (1 day)
dns *[DNS-list]* **no dns**	IP DHCP SERVER	Enter DNS addresses that will be included in a DHCP lease. Multiple DNS servers may be specified by separating them with commas (,). Clear the DNS list; no DNS information will be included in leases
max-lease-time <*0-31536000*> **no max-lease-time**	IP DHCP SERVER	Set the maximum allowed lease time in seconds; can be set as high as 3153600 (one year) Set this parameter to the default value of 86400 seconds (one day)
pool [NAME] **no pool [NAME]**	IP DHCP SERVER	Configure a new or existing DHCP pool (see below for details) Remove an existing DHCP pool NAME: An alphanumeric string that identifies the DHCP pool

Configuring DHCP Pools

The DWR series DHCP server supports multiple DHCP pools. Each DHCP pool is a separate IP address space that the DHCP server uses to respond to lease requests for specific pools. Each pool may be on different networks or uses different gateways and domain-names. The pool-specific configuration controls the IP address, gateway, and domain-name information the client devices would obtain through their DHCP requests.

Usually, pools are bind to specific BSSs and DHCP requests received from clients associated to these BSSs would use different DHCP pools to honor the request. DHCP pools may be configured manually on the DWR series or be automatically created. Automatical DHCP pools can use the IP address prefix “10.x.x.x, 4 IP addresses are provided now; while manual DHCP pools may use any IP address prefix.

Note: the DHCP pool IP address prefix must not duplicate any other IP addresses or networks needed by the mesh network.

The following table outlines the manual DHCP pool configuration commands:

[17] Once enabled, DHCP server will be running as long as it has a valid configuration.

Table 47 DHCP address pool configuration

Command Syntax	Command Mode	Purpose
pool [NAME] **no pool [NAME]**	IP DHCP SERVER	Configure a new or existing DHCP pool (see below for details) Remove an existing DHCP pool NAME: An alphanumeric string that identifies the DHCP pool
domain-name *[name]* **no domain-name**	IP DHCP SERVER POOL	Set the domain name to be included in DHCP leases for this pool Do not include any domain name information in DHCP leases for this pool name: A domain name such as “D-Linknete.com”
gateway <*A.B.C.D*> **no gateway** <*A.B.C.D*>	IP DHCP SERVER POOL	Set the gateway IP to be included in DHCP leases for this pool Do not include gateway in DHCP leases A.B.C.D: A gateway IP address that should conform to an IPv4 unicast address, where A is 1-223, B & C is 0-254, and D is 1-254.
host <*HH:HH:HH:HH:HH:HH*> <*A.B.C.D*> **no host** <*HH:HH:HH:HH:HH:HH*>	IP DHCP SERVER POOL	Add a fixed DHCP IP address entry for a client host Remove a fixed DHCP IP address entry HH:HH:HH:HH:HH:HH: MAC address of the client host A.B.C.D: Fixed IP address to be assigned to the host
network <A.B.C.D/M>	IP DHCP SERVER POOL	Determine the sub-network that DHCP address pool belongs A.B.C.D/M: Address/sub-network mask i.e. 10.1.1.0/24 or 10.1.1.0 255.255.255.0
network *{<A.B.C.D Mask>* | <*A.B.C.D/M>}*	IP DHCP SERVER POOL	Specify the subnet that this pool belongs to <A.B.C.D Mask>: Address and mask of the subnet, e.g. 10.1.1.0 255.255.255.0 A.B.C.D/M: Address/mask of the subnet, e.g. 10.1.1.0/24

range <*begin IP*> <*end IP*> **no range** <*begin IP*> <*end IP*>	IP DHCP SERVER POOL	Add a range of IP addresses to this DHCP pool Remove a range from this DHCP pool Begin IP: The first IP address of the range End IP: The last IP address of the range. Both begin and end IP should be a valid IPv4 unicast address.

Attaching DHCP pools to Ethernet interfaces and BSSs

Different BSS can use different DHCP address pools. Users can enter the following commands to bundle DHCP address pool to BSS under BSS mode or Interface DOT11RADIO mode.

Different Ethernet ports can use different DHCP address pools. Users can enter the following commands to bundle DHCP address pool to Ethernet port under Ethernet port or Interface Fast-Ethernet mode.

Note: a client/clients behind Ethernet interface won't be able to get IP addresses from DHCP on the DWR.

Table 48 DHCP address pool bind command configuration

Command Syntax	Command Mode	Purpose
dhcp server <*POOL-NAME*> **dhcp server automatic** **no dhcp**	INTERFACE DOT11RADIO BSS	Bundle a manual DHCP address pool to the current BSS[18] Bundle an automatic DHCP address pool to the current BSS Separate the DHCP service from the current BSS
ip address *[ip address/mask]* **no ip address**	INTERFACE DOT11RADIO BSS	Configure the IP address of BSS, it is necessary to configure when using manual DHCP address pool. Remove the IP address of the BSS
dhcp server <*POOL-NAME*> **dhcp server automatic** **no dhcp**	INTERFACE FAST-ETHERNET	Bundle a manual DHCP address pool to the current Ethernet port Bundle an automatic DHCP address pool to the current Ethernet port Separate the DHCP service from the current Ethernet port
ip address *[ip address/mask]*	INTERFACE FAST-	Configure the IP address of Ethernet port, it

[18] Either DHCP address pool or DHCP delay can be used in a BSS. So if DHCP delay is enabled in a BSS, the DHCP address pool then will be disabled.

no ip address	ETHERNET	is necessary to configure when using manual DHCP address pool. Remove the IP address of Ethernet port

Show DHCP Server Information and Status

You can use the following commands to show current configuration about DHCP server.

Table 49 Display DHCP Server Information

Command Syntax	Command Mode	Purpose
show dhcp server all	PRIVILEGED EXEC	Show all DHCP server information
show dhcp server default-lease-time	PRIVILEGED EXEC	Show the current value of default lease time
show dhcp server dns	PRIVILEGED EXEC	Show the current dns value
show dhcp server lease	PRIVILEGED EXEC	Show the current lease information
show dhcp server max-lease-time	PRIVILEGED EXEC	Show the current value of maximal lease time
show dhcp server pool	PRIVILEGED EXEC	Show the current DHCP pools

Viewing DHCP Server configuration

```
DWR-500# show dhcp server all
domain-name: D-Linknet.com
DNS servers: 10.13.28.12,10.13.31.12
default-lease-time: 86400 (unit: seconds)
max-lease-time: 100000 (unit: seconds)
!
!
DWR-500# show dhcp server default-lease-time
default-lease-time: 86400 (unit: seconds)
!
!
DWR-500# show dhcp server dns
DNS servers: 10.13.28.12,10.13.31.12
!
!
DWR-500# show dhcp server max-lease-time
max-lease-time: 86400 (unit: seconds)
!
```

Figure 36 Output of DHCP Server configuration

Configure DHCP Relay

DHCP relay transponder for the DHCP request client initiated from the DHCP client and the DHCP response from the server. It allows BSS with terminals connected to the DWR series routers to get IP address from the DHCP address pool defined by outside DHCP server.

- Configure DHCP Relay Parameters
- Enable DHCP relay on a specified BSS or Ethernet port
- Display DHCP relay information

Configure DHCP Relay Parameters

Configuring DHCP relay parameters should be under the mode of CONFIGURATION. The following table lists the commands for configuring DHCP relay:

Table 50 Configure DHCP Relay

Command Syntax	Command Mode	Purpose
ip dhcp relay **no ip dhcp relay**	CONFIGURATION	Confiugre DHCP relay Stop DHCP relay services, and remove the configuration
enable	IP DHCP RELAY	Enable DHCP relay service
disable	IP DHCP RELAY	Stop DHCP relay service
dhcp-servers *[SERVER-list]* **no dhcp-servers**	IP DHCP RELAY	Configure DHCP target server list. Use a comma "," to separate and designate multiple servers Remove DHCP service lists
debug none **debug error** **debug state** **debug information** **debug dump**	IP DHCP RELAY	Stop dhcp relay debug log Record dhcp relay error debug information into log Record the uodating dhcp relay debug error information and status into log Record dhcp relay debug erroe, status and other detail information into log Record all the dhcp relay debug information into log

Open DHCP relay on specific BSS or Ethernet port

Not all BSS or Ethernet port must use DHCP relay, some BSS can use DHCP address pool or simply not use DHCP services. Using the following command open the DHCP relay under BSS mode or Ethernet ports.

Table 51 DHCP relay configuration under BSS or Ethernet port

Command Syntax	Command Mode	Purpose

dhcp relay **no dhcp**	INTERFACE DOT11RADIO BSS	Open BSS on DHCP relay[19] Close the current BSS DHCP service
dhcp relay **no dhcp**	INTERFACE FAST-ETHERNET	Open DHCP relay on Ethernet port[20] Close the current Ethernet port DHCP service

Display DHCP Relay Information

Users can view the DHCP relay configuration through the following commands.
Note that it must be in the mode of ENABLE.

Table 52 Display DHCP Relay Information

Comand Syntax	Command Mode	Purpose
show dhcp relay	PRIVILEGED EXEC	Display DHCP relay status
show dhcp relay dhcp-servers	PRIVILEGED EXEC	Display the DHCP service address used by DHCP relay
show log dhcp-relay	PRIVILEGED EXEC	Display dhcp relay debug log (see previous debug command)

To view DHCP Relay Configuration

```
DWR-500# show dhcp relay dhcp-servers
dhcp-servers: 192.168.1.1 192.168.1.2
!
```

Figure 35 Output of DHCP Relay Configuration

Configure DHCP Relay Agent

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently.

Relay Agent Information Option

Automatic DHCP address allocation is typically based on an IP address, whether it be the gateway IP address (giaddr field of the DHCP packet) or the incoming interface IP address. In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using the relay agent information option (option 82), the Cisco IOS relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server.

[19]Either DHCPaddress pool or DHCPrelay can be used on the same BSS, if DHCP address pool is enabled on the BSS (see the previous chapter), then the DHCP relay will be disabled.
[20]Either DHCPaddress pool or DHCPrelay can be used on the same Ethernet port, if DHCP address pool is enabled on the BSS (see the previous chapter), then the DHCP relay will be disabled.

D-Link DNOS supports this functionality by using the ip dhcp relay information option command. The relay agent will automatically add the circuit identifier suboption and the remote ID suboption to the relay agent information option and forward them to the DHCP server. The DHCP server can use this information to assign IP addresses, perform access control, and set quality of service (QoS) and security policies (or other parameter-assignment policies) for each subscriber of a service provider network.

Specifying the packet forwarding Address

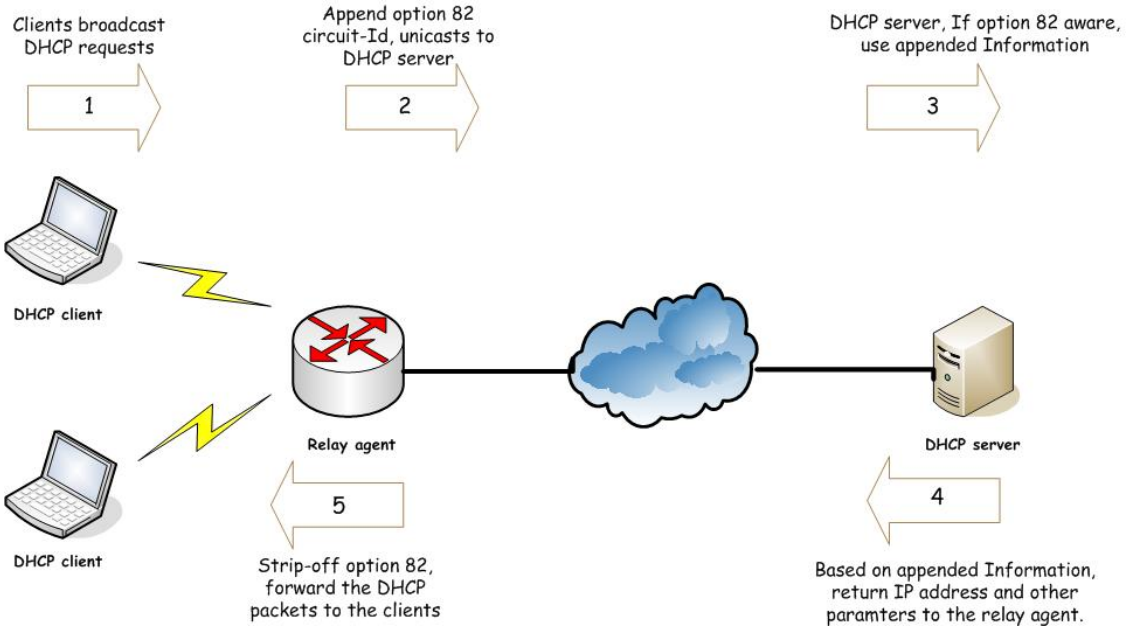
Perform this task to configure the DHCP relay agent to forward packets to a DHCP server.

DHCP clients need to use User Datagram Protocol (UDP) broadcasts to send their initial DHCPDISCOVER messages because they don't have information about the network to which they are attached. If the client is on a network segment that does not include a server, UDP broadcasts normally are not forwarded because most routers are configured to not forward broadcast traffic.

You can remedy this situation by configuring the interface of your router that is receiving the broadcasts to forward certain classes of broadcasts to a helper address. You can use more than one helper address per interface.

The following figure shows how the relay agent information option is inserted into the DHCP packet as follows:

1. The DHCP client generates a DHCP request and broadcasts it on the network.
2. The DHCP relay agent intercepts the broadcast DHCP request packet and inserts the relay agent information option (option 82) in the packet. The relay agent information option contains the related suboptions.
3. The DHCP relay agent unicasts the DHCP packet to the DHCP server.
4. The DHCP server receives the packet and uses the suboptions to assign IP addresses and other configuration parameters and forwards them back to the client.
5. The suboption fields are stripped off of the packet by the relay agent while forwarding to the client.



Configuring DHCP relay option 82 command:

Table 53 Configure DHCP Relay

Command Syntax	Command Mode	Purpose
dhcp relay option circuit-id WORD **no dhcp**	INTERFACE DOT11RADIO BSS	Configure the dhcp relay circuit-id option for the bss interface Remove the related DHCP configuration for the bss interface.
max-hop-count <1-255>	IP DHCP RELAY	Configure the max relay hop count

Note:

1. Enable option 82 relay in the BSS interface but not in Vlan, Multi-BSSID and Ethernet interfaces.
2. D-Link DNOS support Agent Circuit ID suboption and adjustable “max hop count” for DHCP relay packet.

Configuring NAT

Network Address Translation (NAT) is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations. This chapter contains the information of configuring NAT on the DWR series.

The service NAT runs only in the mesh gateway. You can use the following commands to configure the NAT service:

Table 54 Configuring NAT

Command Syntax	Command Mode	Purpose
ip nat **no ip nat**	CONFIGURATION	Enter NAT configuration mode Disable NAT and remove NAT configuration
Enable	IP NAT	Enable NAT service
Disable	IP NAT	Disable NAT service temporarily
mapping static A.B.C.D/M A.B.C.D **no mapping static A.B.C.D/M** **no mapping static all**	IP NAT	Mapping rules to a certain IP address Disable mapping rules and IP address Disable all mapping rules and IP address
out-interface fast-ethernet <0-1> **out-interface dot11radio <0-N> station <name>** **no out-interface fast-ethernet <0-1>** **no out-interface dot11radio <0-N> station <name>**	IP NAT	Add a FastEthernet interface as external NAT interface Add a client station as external NAT interface. Remove a FastEthernet as the NAT interface. Remove a client station as the NAT interface.

Show the configuration of NAT

You can use the following commands to show current configuration about NAT.

Table 55 Display NAT interface and NAT table

Command Syntax	Command Mode	Purpose
show nat out-interface	PRIVILEGED EXEC	Display NAT outside interface
show nat table	PRIVILEGED EXEC	Display NAT Table
show nat mapping static	PRIVILEGED EXEC	Display the router mapping rules
show nat configuration	PRIVILEGED EXEC	Display NAT configure info and status

Viewing NAT configuration

```
DWR-500#show nat configuration
 status RUNNING
 enable
 static mapping rule(s):
  10.1.1.0 255.255.255.0->192.168.1.2
 out-interface(s):
  fast-ethernet 1
```

```
DWR-500#show nat mapping static
 static mapping rule(s):
  10.1.1.0 255.255.255.0->192.168.1.2

DWR-500#show nat out-interface
 out-interface(s):
  fast-ethernet 1

DWR-500#show nat table
Chain POSTROUTING (policy ACCEPT 24 packets, 6296 bytes)
 pkts bytes target     prot opt in     out     source               destination
        0     0 SNAT       all  --  any    any     10.1.1.0/24          anywhere            to:192.168.1.2
        0     0 MASQUERADE  all --  any    eth1    anywhere  anywhere
```

Figure 36 NAT configuration display

Chapter 12 VLAN Configuration

This chapter describes how to configure VLAN on the DWR series router. It contains the following sections:

VLAN Overview

A VLAN is a switched network that is logically segmented on an organizational basis, by functions, project teams, or applications rather than on a physical or geographical basis. The primary protocol currently used in configuring virtual LANs is IEEE 802.1Q standard.

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. None of the switches within the defined group will bridge any frames, not even broadcast frames, between two VLANs.

VLAN working Principle

VLAN can be identified through the 4 bytes of 802.1Q label head which has been added to the normal data packet, as illustrated in Figure 37 and Figure 38.

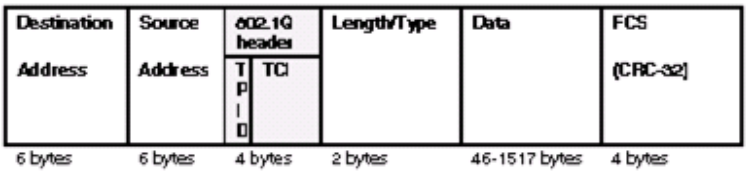


Figure 37 Ethernet frame with 802.1Q

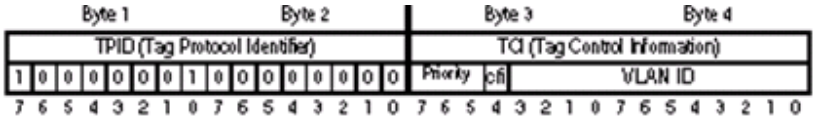


Figure 38 802.1Q label Head

The four bytes 802.1Q label head contains two bytes of tag labels protocol (Tag Protocol Identifier and its value is 0x8100), and 2 bytes of label control information TCI (Tag Control Information).

TCI contains：

1）VLAN ID: 12 domain specifies the VLAN ID,DWR series products can support 1-4094

2）CFI(Canonical Format Indicator): 1bit，used for the bus Ethernet and FDDI, frame format when token ring network exchanges data

3）Priority: 3bits，the priority of specified frame, 8 levels total，it is specially designed for the priority data transmission when the data obstructed.

VLAN Ports

The port can be divided into two categories in the divided VLAN switch: access ports and trunk ports

VLAN Access Link
In the context of VLAN, access refers to host-to-switch link. Generally speaking, the hosts do not belong to a particular VLAN, and the host's hardware do not always support frames tagged by VLAN. The required frames sent and received by host are not tagged.

Access belongs to a special port which must be connected to only a VLAN. This port can not receive other VLAN information or sent out information to other VLANS. Different VLAN information must firstly be processed with 3-layer router then can be sent to other ports.

VLAN trunk Link

In the context of VLANs, the term "trunk" denotes a network link carrying multiple VLANs, which are identified by labels inserted into their packets. Generally trunk links are often switch-to-switch or switch-to-router links or host-to-switch links and routers which support 802.1Q standard.

The VLAN ID enables VLAN switching devices to make intelligent forwarding decisions based on the embedded VLAN ID. Packets originating and contained within a particular VLAN carry the identifier that uniquely defines that VLAN (by the VLAN ID)，and then will be selectively forwarded to the ports with the same VLAN ID.

Depending on the network configuration, we configure the permitting VLAN. DO not forwarding to all the VLANS: For each packet sent from the trunk port will be forwarded to all the indicated VLAN ports. If transferred to all the VLANS, the packets then will be forwarded to the external VLAN besides internal VLAN. One port on the switch must be configured as a trunk port, otherwise it will waste time and bandwidth.

VLAN Application on the DWR

In the DWR series products, BSS and Fast-Ethernet can be configured with access port，and WDS and Fast-Ethernet can be configured with trunk port.
2. Support 3-layer VLAN interface, so can achieve the communication between different VLAN.

VLAN Configuration

BSS and Fast-ethernet of DWR can be configured to access ports, and WDS and Fast-ethernet can be configured to trunk ports.

Configuration Command about VLAN access port and trunck port

Table 56 VLAN Access port and Trunk port configuration

Command Syntax	Command Mode	Purpose

bss <*SSID*>	INTERFACE DOT11RADIO	Configure a new or exsiting BSS on the radio
ssid WORD	INTERFACE DOT11RADIO BSS	Configure multi-ssid under BSS.
switchport access vlan <1-4094> **no switchport**	INTERFACE DOT11RADIO BSS	Confiugre BSS or multi-ssid to VLAN access port Delete VLAN access port
wds < *auto*|*0-5*>	INTERFACE DOT11RADIO	Configure a new or exsiting WDS on the radio or auto WDS
switchport trunk allowed-vlan <1-4094> **no switchport**	INTERFACE DOT11RADIO WDS	Configure WDS to VLAN trunk port Delete VLAN trunk port
interface fast-ethernet <*0-1*>	CONFIGURATION	Configure Ethernet 0 or Ethernet 1
switchport access vlan <1-4094> **no switchport**	INTERFACE FAST-ETHERNET	Configure the Ethernet to VLAN access port Delete VLAN access port
switchport trunk allowed-vlan <1-4094> **no switchport**	INTERFACE FAST-ETHERNET	Configure the Ethernet to VLAN trunk port Delete VLAN trunk port

VLAN Interface Configuration Command

Table 57 VLAN Interface Configuration

Command Syntax	**Command Mode**	**Purpose**
interface vlan <1-4094> **no interface vlan** <1-4094>	CONFIGURATION	Configure VLAN Close VLAN configuration, and delete it
dhcp relay **dhcp server POOL-NAME** **no dhcp**	INTERFACE VLAN	Confiugre DHCP relay Configure DHCPserver Disable DHCP server
ip address A.B.C.D/M **no ip address**	INTERFACE VLAN	Configure VLAN Interface IP address manually Delete VLAN Interface IP address manually
ip forwarding **no ip forwarding**	INTERFACE VLAN	Open VLAN Interface and configure IP transmission function Delete VLAN Interface IP tranmssion function

VLAN applications in the two-layer

Typical Topology

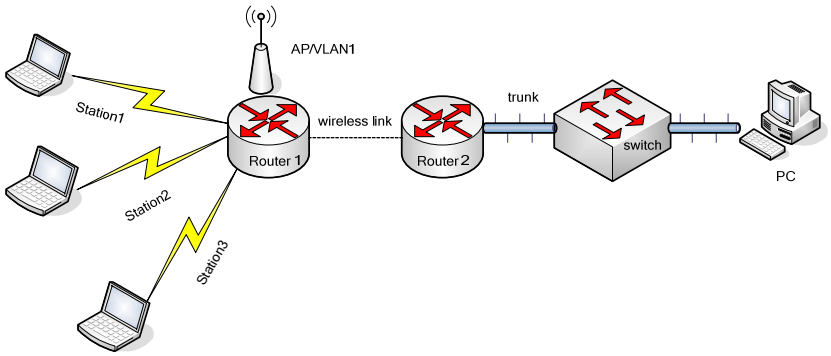


Figure 39 Typical topology of VLAN application on layer 2

Configuration Note:

Router1: Configure an AP on radio0, and then assign it into VLAN1. Wireless client station1, station2 station3 will be labeled with VLAN1 after AP being accessed. Router1 can link with Router2 through WDS, and the trunk port of WDS can be identified by VLAN1.

Router2: can link to router1 through WDS, and the trunk port of WDS can be identified by VLAN1, and the trunk port which connecting the switch Fast-Ethernet 0 should also be identified by VLAN1.

Switch : the port which link to router2 Fast-Ethernet0 is the trunk port. As PC can not recognize the label VLAN1, it has removed the VLAN1 label of the switch; the port which link to the Ethernet is the access port.

PC: Ethernet can link with the access port of switch, and the IP address should exist in the same network with the wireless client IP address.

station1/station2/station3: all can be linked to the AP, and the IP address should within the same network with the PC IP network.

Typical Configuration

Router1:

```
M128 # configure terminal
M128(config) # interface dot11radio 0
M128(config-if-dot11radio) # bss max
% Added new BSS
M128(config-if-dot11radio-bss) # switchport access vlan 1
M128(config-if-dot11radio-bss) # write memory
M128(config-if-dot11radio-bss) # end

M128 # configure terminal
M128(config) # interface dot11radio 1
M128(config-if-dot11radio) # wds 0
M128(config-if-dot11radio-bss) # switchport trunk allowed vlan 1
M128(config-if-dot11radio-bss) # write memory
M128(config-if-dot11radio-bss) # end
```

Router2:

```
M2 # configure terminal
M2(config) # interface dot11radio 1
```

```
M2(config-if-dot11radio) # wds 0
M2(config-if-dot11radio-wds) # switchport trunk allowed-vlan 1
M2(config-if-dot11radio-wds) # write memory
M2(config-if-dot11radio-wds) # end


M2 # configure terminal
M2(config) # interface fast-ethernet 0
M2 ( config-if-ethernet) # switchport trunk allowed-vlan 1
M2 ( config-if-ethernet) # write memory
M2 ( config-if-ethernet) # end
```

Figure 40 Typical Router Configuration Display

Wireless Client Communications between different VLAN

Configure VLAN bind

BSS and Ethernet of DWR can be configured to access ports, and WDS and Ethernet can be configured to trunk ports.

Topology

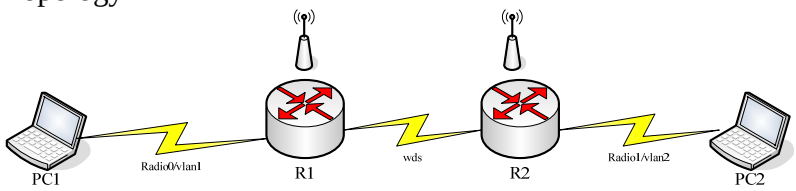


Figure 41 Typical topology of VLAN bind

Configuration Note

Router1 : Configure an AP1 on radio0, and then assign it into VLAN1, and wireless client access AP1 of station1. Router1 can connect router2 through WDS.

Router2 : Configure an AP2 on radio0, and then assign it to VLAN2, and the wireless Client access to the AP2 of station2. Router2 can link with router1 through WDS.

Staion1: It will be labeled with VLAN1 after been access to AP1. And it can also get IP address from Vlan1 interface. As station1 and station2 belong to different VLAN; therefore, data packet can be transmitted from VLAN1 interface without the labels of VLAN1.

Station2 : It will be labeled with VLAN2 after been access to AP2. As station1 and station2 belong to different VLAN; therefore, data packet can be transmitted from VLAN2 interface without the labels of VLAN2.

The data packets which transmitted through VLAN interfaces is out of 802.1Q label head. DDWR learns the dual-achiveable routers to get the mutual communication between VLAN1 and VLAN2. Note: Enable the IP forwarding function of VLAN1 and VLAN2.

If the WDS link be replaced by the Ethernet, in order to achieve the mutual communication between VLAN1 and VLAN2, it must add two static routers which can achieve each other. Similarly, it also need to enable the IP forwarding function of VLAN1 and VLAN2 interfaces.

Typical Configuration

router1:

```
M79 # configure terminal
M79(config) # interface dot11radio 0
M79(config-if-dot11radio) # mode access
M79(config-if-dot11radio) # bss a 1
% Added new BSS
M79(config-if-dot11radio-bss) # switchport access vlan 1
M79(config-if-dot11radio-bss) # write memory
M79(config-if-dot11radio-bss) # end

M79 # configure terminal
M79(config) # interface dot11radio 1
M79(config-if-dot11radio) # mode backhaul
M79(config-if-dot11radio) # wds 1
M79(config-if-dot11radio-wds) # remote node 57  1
M79(config-if-dot11radio-wds) # ip address 10.10.1.1/24
M79(config-if-dot11radio-wds) # write memory
M79(config-if-dot11radio-wds) # end

M79 # configure terminal
M79(config) # ip dhcp server
M79(config-dhcp-server) # pool 1
M79(config-dhcp-server-pool) # network 192.168.1.0/24
M79(config-dhcp-server-pool) # gateway192.168.1. 1
M79(config-dhcp-server-pool) # range 192.168.1.10  192.168.1.100
M79(config-dhcp-server-pool) # write memory
M79(config-dhcp-server-pool) # end
%  DHCP server started successfully

M79 # configure terminal
M79(config) # interface vlan 1
M79( config-if-vlan) # ip forwarding
M79( config-if-vlan) # ip address 192.168.1.1/24
M79( config-if-vlan) # dhcp server 1
M79( config-if-vlan) # write memory
M79( config-if-vlan) # end
```

router2:

```
M57 # configure terminal
M57(config) # interface dot11radio 0
M57(config-if-dot11radio) # mode access
M57(config-if-dot11radio) # bss a2
% Added new BSS
M57(config-if-dot11radio-bss) # switchport access vlan 2
M57(config-if-dot11radio-bss) # write memory
M57(config-if-dot11radio-bss) # end

M57 # configure terminal
M57(config) # interface dot11radio 1
M57(config-if-dot11radio) # mode backhaul
M57(config-if-dot11radio) # wds 1
M57(config-if-dot11radio-wds) # remote node 79 1
M57(config-if-dot11radio-wds) # ip address 10.10.1.2/24
M57(config-if-dot11radio-wds) # write memory
M57(config-if-dot11radio-wds) # end
```

```
M57 # configure terminal
M57(config) # ip dhcp server
M57(config-dhcp-server) # pool 2
M57(config-dhcp-server-pool) # network 192.168.5.0/24
M57(config-dhcp-server-pool) # gateway 192.168.5.1
M57(config-dhcp-server-pool) # range 192.168.5.10  192.168.5.100
M57(config-dhcp-server-pool) # write memory
M57(config-dhcp-server-pool) # end
% dhcp server started successfully

M57 # configure terminal
M57(config) # interface vlan 2
M57(config-if-vlan) # ip forwarding
M57(config-if-vlan) # ip address 192.168.5.1/24
M57(config-if-vlan) # dhcp server 2
M57(config-if-vlan) # write memory
M57(config-if-vlan) # end
```

Figure 42 Router typical Configuration

VLAN Diagnose

Display the current VLAN status

In the prompt of privileged EXEC mode, entering the following commands to display the current VLAN information:

Table 58 Display VLAN Configuration Order

Command Syntax	**Command Mode**	**purpose**
show interface vlan <1-4094>	PRIVILEGED EXEC	Display the specified VLAN Interface information
show vlan	PRIVILEGED EXEC	Display all the VLAN information

View VLAN related information

```
M79 # show interface vlan 1
Interface vlan 1
  Admin status: up   physicalstatus: up
  DHCP: manual pool    pool name:  1
  IP forwarding: disabled
  index 535 metric 1 mtu 1500 <UP, BROADCAST, RUNNING, MULTICAST>
  inet 192.168.1.1/24  broadcast  192.168.1.255
    input packet 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    input rate 4294967295  bytes/s
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    output rate 4294967295  bytes/s
```

```
    collisions 0

M79 # show vlan
Total 2 VLANs
    VLAN 1   ports(0):
    VLAN  11   Port(0):
```

Figure 43 VLAN Related Information Display

Fault Diagnose

1. Assign the two AP to the same VLAN, access wireless client to the two separate AP, but it still can not communicate, please diagnose from the following aspects:

Whether the client IP address belong to the same network
If the two BSS connect the separate routers, then check the link flow and whether there is a trunk port that can identify the VLAN.
In mesh network, one VLAN better only allows one VLAN interface. Check whether one VLAN has assigned several VLAN interfaces which will conflict with each other when accessing IP address.

2. When different VLAN can not communicate well, please check the following aspects:

Whether there is 3-layer reachable routing through which different VLAN can communicate
If routing is OK, check whether IP forwarding function has been enabled

Note:

DWR series VLAN currently does not support STATION interface
One VLAN can only configure one VLAN interface
Interface vlan currently only support manual configuring address pool
VLAN currently does not support roaming and NAT
5. In the loop topology, all the interconnect port can not be configured into the same Vlan, which can avoid the network loop.

Chapter 13 802.11 Security

This chapter describes how to configure security policies as defined by the 802.11i standard on the DWR series router. It contains the following sections:

802.11 standard overview

The 802.11 security standard defines a suite of wireless security protocols and implementations. It provides open and shared key authentication, is compatible with WPA /WPA2, and interoperates with 802.1x.

OPEN

Open authentication allows any client authentication and tries to connect with the router.

Shared-key

a) Shared Key Authentication looks for the clients knowing sharing key or not.
b) Shared Key only applies in the WEP.
c) Does not recommend to use for many hidden safety problems.

WEP

WEP (wired equivalent privacy) is the wireless safety solutions based on the symmetric encryption using the RC4 encryption algorithm. It adopts the same way to encryption and decryption.

d) To enhance the WEP security, WEP adopts the 4 different sequence keys and enhances the key strength with: 40 bits，104bits and 128 bits.

WPA

WPA (Wifi protected access) and WPA2 can achieve the common wireless security through pre-shared key and 802.1x. The only difference between WPA and WPA2 the different encryption algorithm, WPA achieves data security using TKIP (RC4), while WPA2 through CCMP (AES).

Pre-shared key is the encryption which achieves data communications through symmetric approach.

WPA and WPA2 also combined 802.1x to strengthen the wireless data communications security.

802．1X

The basic 802.1x authentication model：

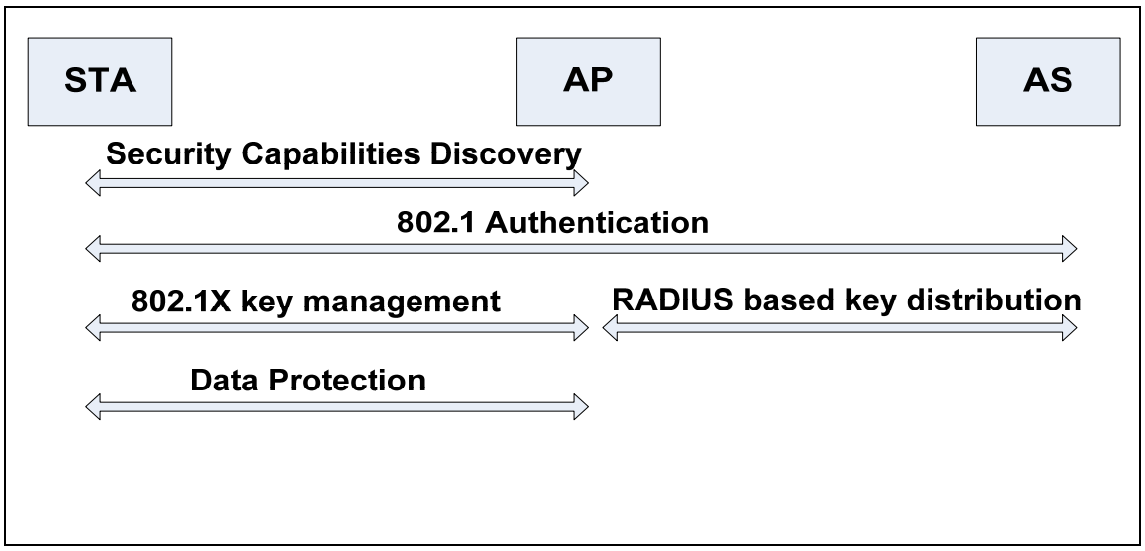


Figure 44 Model of 802.1x authentication

802.1 x-based certification process:

1. Access Point announces security suites in Beacon and Probe Response frame
2. Station choose the correct security suite and password connecting to the access point;
3. Establish a layer-2 link between Station and Access Point;
4. Use EAP for 802.1x authentication:
   a) First, station starts authentication with EAP start frams;
   b) AP enters the identification through EAP-request and station EAP-response, AP package station EAP-response to the Access-request and then transmit it to the AS;
   c) AS transmits authentication request through challenge message and AP to station, and then station reponses the the challenge message through the EAPoL-response message and change the authentication status; Station and AS have the similar PMK(Pairwise Master Key), Access point get the PMK from AS.
   d) AS transmit Access-Accept to AP, and AP change the status of Staton to authenticated and then transmit EAPoL-success to Station, when EAPoL-success frame received, Station change its status to successful authentication.
   e) Authentication success; Access Point and AS create a PTK(Pairwise Transient Key);
   f) Access Point distributes GTK (Group Transient Key) using PTK's KCK (EAPOL-Key Confirmation Key) and KEK (EAPOL-Key Encryption Key);
   g) Station and Access Point shook hands four times creating a group of key to protect data during network transmission.
5. When the Station authentication success, DHCP Discovery operates and access to 3-layer address and then adding routing, access to the Internet;
6. Station and Access Point shook hands four times perpetual creating a group of keys to protect data during transmission. Disconnect link.

MAC-based Access Control Configuration

DWR series allows MAC address-based access control. For each BSS hosted by the router, one can allow or disallow a list of client MAC addresses proper association with the AP. Creation of the MAC list and the specification of the MAC addresses are performed by the mac-list command under CONFIGURATION TERMINAL mode.

Table 58 Configuring MAC-List

Command Syntax	Command Mode	Purpose
mac-list <*listname*>	CONFIGURATION	Create or modify a MAC address list with the specified name
no mac-list <*listname*>	CONFIGURATION	Remove a MAC address list
mac-addr <*HH:HH:HH:HH:HH:HH*>	MAC-LIST	Add a MAC address to the MAC list
no mac-addr <*HH:HH:HH:HH:HH:HH*>	MAC-LIST	Remove a MAC address from MAC list

Show the configuration of MAC-List

You can use the following commands to show current configuration about MAC-List.

Table 60 Display MAC-List and information

Command Syntax	Command Mode	Purpose
show mac-list	PRIVILEGED EXEC	Show all configured MAC address list

View MAC-List configuration:

```
!
mac-list aaa
 mac-addr 00:17:7b:11:11:11
 mac-addr 00:17:7b:11:11:12
 mac-addr 00:17:7b:11:11:13
 mac-addr 00:17:7b:11:11:14
mac-list bbb
 mac-addr 00:17:7b:22:22:22
 mac-addr 00:17:7b:22:22:23
 mac-addr 00:17:7b:22:22:24
!

DWR-500# show mac-list
mac-list aaa
 mac-addr 00:17:7b:11:11:11
 mac-addr 00:17:7b:11:11:12
 mac-addr 00:17:7b:11:11:13
 mac-addr 00:17:7b:11:11:14
mac-list bbb
 mac-addr 00:17:7b:22:22:22
 mac-addr 00:17:7b:22:22:23
 mac-addr 00:17:7b:22:22:24
```

Figure 45 Output of MAC-List configuration

RADIUS AAA Configuration

This section describes how to enable and configure the RADIUS (Remote Authentication Dial-In User Service), which provide flexible administrative control over authentication and authorization processes. RADIUS is configured with the AAA mode command.

Table 61 Configuring AAA

Command Syntax	Command Mode	Purpose
aaa	CONFIGURATION	Configuring AAA parameters, including authentication and accounting servers and ports
radius-server <*A.B.C.D*> *auth-port <1-65535> key <string>* **radius server** <*A.B.C.D*> *auth-port default key <string>* **no radius-server** <*A.B.C.D*> *auth*	AAA	Add a radius authentication server using the specified port and secret key. Add a radius authentication server using the default port of 1812 and the specified secret key. Remove a radius authentication server
radius-server <*A.B.C.D*>*acct-port <1-65535> key <string>* **radius server** <*A.B.C.D*> *acct-port default key <string>* **no radius-server** <*A.B.C.D*> **acct**	AAA	Add a radius accounting server using the specified secret key and authentication port Add a radius accounting server using the default port of 1813 and the specified secret key. Remove a radius accounting server
server-group[2]	AAA	Enter server group configuration
server <*A.B.C.D*> **auth** **no server** <*A.B.C.D*> **auth** **server** <*A.B.C.D*> **acct** **no server** <*A.B.C.D*> **acct**	SERVER GROUP	Add a authentication server to server group Remove authentication server from server group Add a accounting server to server group Remove a accounting server from server group

Notes:

1. The radius-server command defines a radius server; the definition includes the ip address and port of an authentication or the ip address and port of an accounting server, Specifying a radius-server only make it available for use to the DWR series, but would not be used until included by a server

group.

2. The server-group contains the radius server information for authentication or accounting, it is the current running-configuration that allow user to configure multiple servers under the server-group. The first authentication and accounting radius server is the primary server, the second server is the backup server, and the second server takes effect only when the first server fail to communicate with DWR series.

Table 62 Display AAA configuration

Command Syntax	Command Mode	Purpose
show aaa	PRIVILEGE EXEC	Show aaa configuration, including radius server and server-group configuration

View AAA configuration:

```
!
aaa
 radius-server  192.168.10.69 auth-port 1812 key secret
 radius-server  192.168.20.234 auth-port 1812 key 123456
 server-group
  server 192.168.10.69 auth
  server 192.168.20.234 auth
!
DWR-500# show aaa
!
aaa
 radius-server  192.168.10.69 auth-port 1812 key secret
 radius-server  192.168.20.234 auth-port 1812 key 123456
 server-group
  server 192.168.10.69 auth
  server 192.168.20.234 auth
DWR-500#
```

Figure 46 Output of AAA configuration

Certificate Configuration

This section describes how to download and install certificates which are used for authenticating the DWR series as an allowed client for other 802.11 APs.

Table 63 Installing Authentication Certificates

Command Syntax	Command Mode	Purpose
install certificate ca <URL>	PRIVILEGED EXEC	Download and install the CA certificate from the provided URL
install certificate client <URL>		Download and install the client certificate from the provided URL
install client-key <URL> password <password>		Download and install the client key file from the provided URL. Install this profile may need to enter the protection password.

Table 64 Displaying Installed Certificates

Command Syntax	Command Mode	Purpose

show certificate ca	PRIVILEGED EXEC	Show the information of the installed CA certificate.
show certificate client		Show the information of the installed client certificate.

Configuration example:

```
DWR-500# install certificate ca http://192.168.1.1/certs/cert-ca.pem

DWR-500# install certificate client http://192.168.1.1/certs/cert-clt.pem

DWR-500# install client-key http://192.168.1.1/certs/cert-clt-key.pem

DWR-500# show certificate ca

DWR-500# show certificate client
```

Security-Profile Configuration

This section describes the authentication types and encryption methods that you can configure on the router. Security profile on DWR series defines all security policy supported by router software. Now router supports WEP, WPA, WPA2 and 8021X security suites. This block is only a definition of security policy, and it will take effect after attached in BSS or WDS. Users can add to delete configuration files according to the actual application, interface can switch security policy flexibly through different configuration facilities.

Table 65 Configuring Security Profiles

Command Syntax	Command Mode	Purpose
security-profile wep <wep-profile-name>	CONFIGURATION	Create or modify a WEP security profile of the given name
no security-profile wep <wep-name>		Remove a WEP profile
wep-key <1|2|3|4> <key-string>	SECURITY-PROFILE WEP	Add a WEP key to the WEP security profile
no wep-key <1|2|3|4>		Remove a WEP key from WEP security profile
security-profile wpa <wpa-profile-name>	CONFIGURATION	Create or modify a WPA security profile of the given name
no security-profile wpa <wpa-profile-name>		Remove a WPA profile
encryption-mode-cipher tkip	SECURITY-PROFILE WPA	Designate TKIP encryption mode for WPA security policy.
no encryption-mode-cipher		Remove the encryption mode configuration

wpa-type 8021x <8021x-profile-name>	SECURITY-PROFILE WPA	Designate WPA security policy using 802.1x authentication
no wpa-type 8021x		Remove 8021X authentication
wpa-type psk hex <string>	SECURITY-PROFILE WPA	Designate WPA PSK authentication on WPA policy and pre-configure hexadecimal key.
wpa-type psk ascii <string>		Designate WPA PSK and configure pre-shared key using ASCII format
no wpa-type psk		Remove WPA PSK authentication from WPA profile
security-profile wpa2 <wpa2-profile-name>	CONFIGURATION	Add a WPA2 profile
no security-profile wpa2 <wpa2-profile-name>		Remove a WPA2 profile from current configuration
encryption-mode-cipher ccmp	SECURITY-PROFILE WPA2	Designate CCMP encryption for WPA2 security policy
encryption-mode-cipher tkip		Designate TKIP encryption for WPA2 security policy
no encryption-mode-cipher		Remove WPA2 encryption type setting
wpa2-type 8021x <8021x-profile-name>	SECURITY-PROFILE WPA2	Designate 8021X authentication for WPA2 profile
no wpa2-type 8021x		Remove 8021X authentication from WPA2 profile
wpa2-type psk hex <string>	SECURITY-PROFILE WPA2	Designate WPA2 PSK for WPA2 security policy, pre-configured hex key.
wpa2-type psk ascii <string>		Designate WPA2 PSK for WPA2 sucurity policy, pre-configured ASCII code key
no wpa2-type psk		Remove WPA2 PSKauthentication setting
security-profile 8021x <8021x-profile-name>	CONFIGURATION	Add a 8021X authentication profile
no security-profile 8021x<8021x-profile-name>		Remove a 8021X authentication profile

eap-reauth-period <0-65535> **eap-reauth-period 3600** **no eap-reauth-period**	SECURITY-PROFILE 8021x	Set EAP re-authentication period Restore EAP re-authentication to default value of 3600 seconds
security-profile client-8021x <client-8021x-profile-name> **no security-profile client-8021x <client-8021x-profile-name>**	CONFIGURATION	Add 802.1 x security policy profile and client authentication profile that client mode use. Remove the 802.1x and client authentication policy profiles
eap-method peap **eap-method ttls** **eap-method tls** **no eap-method**	SECURITY-PROFILE CLIENT-8021x	Set EAP to PEAP Set EAP to TTLS Set EAP to TLS Remove EAPsetting
password <string> **no password**	SECURITY-PROFILE CLIENT-8021x	Set authentication user password Remove authentication user password setting
user-name <string> **no user-name**	SECURITY-PROFILE CLIENT-8021x	Set authentication user name Remove authentication user name

Table 66 Display configuration of security profile

Command Syntax	Command Mode	Purpose
show security-profile wep	PRIVILEGED EXEC	Show WEP profile configuration
show security-profile wpa	PRIVILEGED EXEC	Show WPA profile configuration
show security-profile wpa2	PRIVILEGED EXEC	Show WPA2 profile configuration
show security-profile 8021x	PRIVILEGED EXEC	Show 8021x profile configuration
show security-profile client-8021x	PRIVILEGED EXEC	Show client-8021x profile configuration

```
security-profile wep wep1
 wep-key 1 1234567890abcdef1234567890
```

```
 wep-key 2 "abcde"
 wep-key 3 "abcdefabcdefa"
 wep-key 4 abcdefabcdefabcdefabcdefabcdefab
security-profile wep wep2
 wep-key 1 "abcde"
 wep-key 2 "1234567890123"
 wep-key 3 "1234567890abcdef"
 wep-key 4 1234567890
security-profile wep wep3
 wep-key 3 abcdefabcdefabcdefabcdefab
security-profile wep wep4

DWR-500#  show security-profile wep
security-profile wep wep1
 wep-key 1 1234567890abcdef1234567890
 wep-key 2 "abcde"
 wep-key 3 "abcdefabcdefa"
 wep-key 4 abcdefabcdefabcdefabcdefabcdefab
security-profile wep wep2
 wep-key 1 "abcde"
 wep-key 2 "1234567890123"
 wep-key 3 "1234567890abcdef"
 wep-key 4 1234567890
security-profile wep wep3
 wep-key 3 abcdefabcdefabcdefabcdefab
security-profile wep wep4
DWR-500#
```

Figure 47 Output of WEP profile configuration

```
security-profile wpa wpa1
 encryption-mode-cipher tkip
 wpa-type psk hex 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
security-profile wpa wpa2
 encryption-mode-cipher tkip
 wpa-type 8021x 802.1xprofile
security-profile wpa wpa3
 encryption-mode-cipher tkip
```

Figure 48 Output of WPA profile configuration

```
security-profile wpa2 wpa2-pskprofile
 encryption-mode-cipher ccmp
 wpa2-type 8021x 802.1xprofile
!
```

Figure 49 Output of WPA2 profile configuration

```
!
security-profile 8021x 8021xprofile
 eap-reauth-period 3600
security-profile 8021x 8021x1

DWR-500# show security-profile 8021x
security-profile 8021x 8021xprofile
 eap-reauth-period 3600
security-profile 8021x 8021x1
DWR-500#
```

Figure 50 Output of 8021x profile configuration

```
security-profile client-8021x client-8021x1
 eap-method tls
 user-name test-tls
security-profile client-8021x client-8021x2
 eap-method peap
 user-name test-peap
 password whatever
security-profile client-8021x client-8021x3
 eap-method ttls
 user-name test-ttls
 user-name ttls
 password whatever
```

Figure 51 Output of client-8021x profile configuration

BSS Security Configuration

This section describes how to apply security profiles and MAC lists to the router's BSS configurations.

Table 67 Configuring BSS Security

Command Syntax	Command Mode	Purpose
authentication open **no authentication**	INTERFACE DOT11RADIO BSS	Allow all clients to associate with this BSS
authentication open wep <wep-profile-name> default-key <1-4>		Designate WEP encryption for BSS using the key settings in the WEP profile and specify the default transmission key series
authentication open key-management wpa <wpa-profile-name>		Designate WPA security for this BSS; only allow clients with correct WPA authentication and encryption settings to associate with this BSS.
authentication open key-management wpa2 <wpa2-profile-name>		Designate WPA2 security for this BSS; only allow clients with correct WPA2 authentication and encryption settings to associate with this BSS.
authentication shared wep <wep-profile-name> default-key <1-4>		Designate WEP authentication and encryption for BSS using the key settings in the WEP profile and specify the default transmission key series.
mac-address accept <mac-list-name>	INTERFACE DOT11RADIO BSS	Only accept clients with MAC addresses in the specified list; reject all other clients
mac-address deny <mac-list-name>		Only deny clients with MAC addresses in the specified list; allow all other clients.
mac-address accept-all **no mac-address**		Restore to default configuration (accept all MAC addresses)

Table 68 Security configuration command

Command Syntax	Command Mode	Purpose
show interface dot11radio <0|1> bss <SSID> accept-macs **show interface dot11radio <0|1> bss <SSID> deny-macs**	PRIVILEGED EXEC	Show attached accept macs address on SSID of the Radio Show attached deny macs address on SSID of the Radio
show interface dot11radio0 bss <SSID> wep-keys	PRIVILEGED EXEC	Show BSS WEP configuration

```
DWR-500# show interface dot11radio 0 bss public accept-macs
accept mac list:
00:17:7b:22:22:22, 00:17:7b:22:22:23, 00:17:7b:22:22:24,

DWR-500# show interface dot11radio 0 bss public1 deny-macs
deny mac list:
00:17:7b:11:11:11, 00:17:7b:11:11:12, 00:17:7b:11:11:13, 00:17:7b:11:11:14,


DWR-500# show interface dot11radio 0 bss public wep-keys
  <cr>
DWR-500# show interface dot11radio 0 bss public wep-keys
wep key 1=1234567890abcdef1234567890
wep key 2="abcde"
wep key 3="abcdefabcdefa"
wep key 4=abcdefabcdefabcdefabcdefabcdefab
DWR-500#
```

Figure 52 Display security configurations on BSS

WDS Security Configuration

This section describes how to apply security profiles and MAC lists to the router's manual WDS interfaces.

Table 69 Configuring WDS security

Command Syntax	Command Mode	Purpose
authentication open **no authentication**	INTERFACE DOT11RADIO WDS	Disable authentication for this WDS interface (open system).
authentication shared wep <wep-profile-name> default-key <1-4>		Designate WEP authentication and encryption for this WDS using the key list in the WEP profile and specify the default transmission key series.
authentication open key-management wpa <wpa-profile-name>		Designate WPA security for this WDS interface using the specified profile settings.
authentication open key-management wpa2 <wpa2-profile-name>		Designate WPA security for this WDS interface using the specified profile settings. Only allow the routers with correct WPA2

		encryption configuration to create WDS link with it.

Client Security Configuration

This section describes how to apply security profiles and WEP key to the router's configured clients.

Table 70 Configuring client-mode security

Command Syntax	Command Mode	Purpose
client-authentication open wep <wep-profile-name> default-key <1-4>	INTERFACE DOT11RADIO STATION	Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key
client-authentication open key-management wpa client-8021x <client-8021x-profile-name>		Enable WPA security for this CLIENT, using the authentication settings in the client-8021x profile
client-authentication open key-management wpa2 client-8021x <client-8021x-profile-name>		Enable WPA2 security for this CLIENT, using the authentication settings in the client-8021x profile
client-authentication open key-management wpa-psk hex <string>		Enable WPA PSK on client and configure pre-shared key using hexadecimal format.
client-authentication open key-management wpa-psk ascii <string>		Enable WPA PSK on client and configure pre-shared key using ascii format.
client-authentication open key-management wpa-psk hex <string>		Enable WPA2 PSK on client and configure pre-shared key using hexadecimal format.
client-authentication open key-management wpa-psk ascii <string>		Enable WPA2 PSK on client and configure pre-shared key using ascii format.
client-authentication shared wep <wep-profile-name> default-key <1-4>		Enable WEP encryption for this client using the key settings in the WEP profile and the specified default key
no client-authentication		Disable authentication for this client interface.

802.1x Typical Configuration

Network Topology:

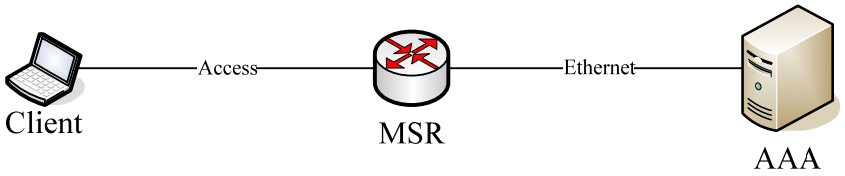


Figure 53 8021x Network Topology

Topology Note：

AAA represents Authentication Server
DWR opens WPA2+802.1x authentication
Client can be accessed to DWR，and have the right to visit AAA；

DWR Configuration：

```
。 。 。 。 。 。
aaa
 radius-server  192.168.10.69 auth-port 1812 key 123456
 server-group
  server 192.168.10.69 auth


。 。 。 。 。 。

interface dot11radio 0
 wireless-mode g 1
 antenna 1
 mode access
bss D-Link
  authentication open key-management wpa2 wpa2-8021x
  dhcp server automatic


。 。 。 。 。 。
```

Figure 54 DWR configuration display

802.11 Security Configuration Diagnose

1. Determine whether Station and Access Point having the same security strategy
2. When using WEP security strategy, note the following:
   a) The same serial key at both ends of the key list should be consistant;
   b) Whether it is the same authentication way, open or shared-key;
3. For the PSK security of WPA and WPA2
   a) If clients set the two security policy with an option, it must determine whether it uses the same encryption algorithm with the AP.
   b) When the key is HEX, and the allowed key length may not be 63, it must ensure whether the complemented key is the same.
4. For the 802.1x clients:
   a) Determine whether Access Point can communicate well with AS, and 1812 and 1813 port are

not stopped

b) Determine whether the authentication port of Access Point is in accordance with that of AS
c) Whether the clients can initiate the correct request of EAP authentication.
d) For the certificate authentication, it must install correctly and authenticate correctly by certificate.

Chapter 14 WME Configuration

WME introduction

WME, as a transitional standard, supports of 802.11e and also provides the 2-layer QoS guarantee for mesh network . When the network is overloaded or congested, QoS can ensure the critical traffic volume being not delayed or discarded so as to keep the efficient operation of network. The traditional 802.11 protocol provides service using the best effects to delivery the data traffic, which makes the real-time service operation un-guaranteed. While D-Link DWR series routers takes the Service differentiation mechanism of 802.11e to divide the data transmission queen into six priority, which can ensure the priority transmission of voice, video and other business. When WME enabled(Wireless multimedia enhanced protocol), data with different priorities will be entered into different queues. And the end-to-end QoS in the protocol ensures that the transmission and receive requests with high levels of priority will be disposed with high priority.

Basic functions of WME(802.11e):

Transmission queue (AP-to-STA traffic)

There are all 6 transmission queues in AP: 4 queues for data flow, 1 queue for the transmission of beacon frames, another for the traqnsmission of "beacon after" packet (such as management frame transmission should follow by the beacon frame). The last two queues can not be configured by users.

If 802.11 e (wme) is disabled, AP will transmit data by the default queue (make the greatest efforts to delivery).

If 802.11e (wme) is enabled, but the linking STA does not support 802.11, then AP will transmit data by the default queue (make the greatest efforts to delivery).

If 802.11 e (wme) is enabled, and the linking STA also supports 802.11e, then AP will transmit data in different queues based on the priority label of VLAN 802.11p or the DHCP of IP header.

QoS broadcast (STA-to-AP traffic)

AP can broadcast QoS parameters through beacon frame. QoS parameters can be get when 802.11 e clients are connected to AP, Which will be the basis of Client transmitting communication flow.

Quene coparison between DSCP value and TOS value:

DSCP		TOS	Priority
Decimal	Binary	Decimal	
0~7	000 000 ~ 000 111	0	Best Effect
8~15	001 000 ~ 001 111	1	Background
16~23	010 000 ~ 010 111	2	Background
24~31	011 000 ~ 011 111	3	Best Effect
32~39	100 000 ~ 100 111	4	Video
40~47	101 000 ~ 101 111	5	Video
48~55	110 000 ~ 110 111	6	Voice
56~63	111 000 ~ 111 111	7	Voice

Note: Running WME requires the both points all support WME at the same time, i.e.: If AP and station enable WME, then they both must all support WME and enable. WME is enabled under the default backhaul mode.

D-Link WME Advantages

a. Support point-to-point QoS。
b. Support different priority for different services and guarantees the business of voice and video.

WME Configuration Command

Table 71 WME command configuration

Command Syntax	Command Mode	Purpose
wme **no wme**	INTERFACE DOT11RADIO	Enable WME service Disable WME service
force-sta-wme **no force-sta-wme**	INTERFACE DOT11RADIO BSS	Only allow client access that support WME mandatory Allow client that do not support WME access

Typical Configuration

WME

```
DWR-500(config-if-dot11radio)# wme
DWR-500(config-if-dot11radio)# no wme
```

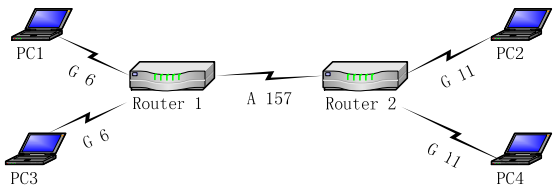


Figure 55 WME Examples

Assuming all the PC support WME, transmit high-priority voice flow from PC1 to PC2, and transmit 30M background flow from PC3 to PC4. When the WME of Router1 and Router2 is enabled, MOS value over provision that the link can support is much smaller than that when WME is disabled.

Display WME Configuration

```
DWR-500 # sh running-config
….
interface dot11radio 0
 wme
```

Fault Diagnose

When the Mesh networks need to provide high-quality multimedia services, check whether WME opened between end-to-end routers. When the background flow or voice is poor, user can enther command <show interface dot11radiorunning-config> to check whether WME is open.

Chapter 15 QoS Configuration

QoS at three layer of DWR Series routers is achieved through the bandwidth limitation. Currently, D-Link QoS bandwidth limitation mainly achieves in the WDS interface to avoid the WDS link traffic overload.

Enable/Disable QoS Service

By default, QoS doesn't take effect on DWR series. Use the following commands to start or stop the QoS in QoS mode.

Table 72 Enable/Disable QoS

Command Syntax	Command Mode	Purpose
qos	CONFIGURATION	Enter QOS configuration mode
enable	QOS	Enable QoS, start QoS service and all QoS classes attached to WDS interface will take effect. If QoS is not defined, default QoS will take effect.
disable		Disable QoS, stop QoS service and all QoS classes attached to WDS interface will be disabled

Configuring QoS over Manual WDS Interface

There are two steps to run QoS service over one ManualWDS interface: creating one QoS class and attaching it to ManualWDS interface. First, user should configure one QoS class which specifies the maximal and minimal bandwidth of this ManualWDS interface. After creating one specific QoS class, user should attach this QoS class to ManualWDS interface.

Configuring QoS Classes

The QoS class is targeted to let user specify acceptable bandwidth of one WDS link. For each QoS class, user must specify one maximal bandwidth value and one minimal bandwidth value. Use the following commands to configure QoS classes.

Table 73 Configuring QoS Classes

Command Syntax	Command Mode	Purpose
class <name>	QOS	Create/configure one QoS class. The class

no class <name>		name is unique identifier for all QoS classes. Meanwhile, user enters the CLASS configuration mode to configure the QoS class Delete the QoS class with specific name
maxbw <1-500> **no maxbw**	QOS CLASS	Specify the maximal bandwidth that this QoS class can obtain. (Unit: 100kbps) Set the max bandwidth to default value (30Mbps; if the Supermode is enabled or in the trunk channel, the default value is 60Mbps).
minbw <1-200> **no minbw**	QOS CLASS	Specify the minimal bandwidth guarantee to this class. (Unit: 100kbps) Set the minimal bandwidth to default value (5Mbps)

Attaching QoS Class to Manual WDS Interface

After configuring one preferable QoS class, user should indicate which ManualWDS interface to use this specific QoS class. Use the following commands to attached one specific QoS class to one ManualWDS interface.

Table 74 Attaching QoS Class to ManualWDS

Command Syntax	Command Mode	Purpose
qos class <*classname*> **no qos class**	INTERFACE DOT11RADIO WDS	Attach one specific QoS class with *classname* to this ManualWDS Interface. Correspondingly, start QoS service over this interface if QoS service is enabled on router. Remove QoS class from this ManualWDS interface. Furthermore, one default QoS class will take effect on this interface if enable QoS globally.

Bandwidth Limitation

```
DWR-500(config)# qos
DWR-500 (config-qos)# enable
% QoS started successfully
DWR-500 (config-qos)# class abc
DWR-500 (config-if-dot11radio-wds)# qos
DWR-500 (config-if-dot11radio-wds)# qos class abc
```

Figure 56 Bandwidth limitation display

Showing QOS Information and Status

Table 75 QoS information and status

Command Syntax	Command Mode	Purpose
show qos configuration	PRIVILEGED EXEC	Show configuration of QoS
show qos dot11radio <*Radio*> class	PRIVILEGED EXEC	Show the specific radio class rules
show qos dot11radio <*Radio*> qdisc	PRIVILEGED EXEC	Show the specific radio queue discipline rules
show qos interface	PRIVILEGED EXEC	Show the QoS class and the running status that applied on the configured interfaces

View QOS configuration

```
DWR-500# show running-config
……
interface dot11radio 0
 wireless-mode a 136 DK
 antenna 1
 mode backhaul
 max-auto-wds 5
 wds 0
  remote mac 00:0b:6b:37:a0:00
  ip address 10.53.54.2/24
  qos class band1
  no shutdown
 wds 1
  remote mac 00:0b:6b:37:a1:00
  ip address 10.52.54.2/24
  qos class band2
  no shutdown
!
……
!
qos
 enable
 class band1
  maxbw 200
  minbw 100
 class band2
  maxbw 150
  minbw 60
 class band3
  maxbw 100
  minbw 40
```

Figure 57 QoS Configuration Display

Chapter 16 Configuring SNMP

This section describes commands used to configure the Simple Network Management Protocol (SNMP) Agent on the DWR-500 for the purposes of network monitoring and management.

- Configuring SNMP Community
- Configuring SNMP trap
- Configuring SNMPv3 user

Configuring SNMP Community

To set the community string for controlling access to the Management Information Base (MIB) on the SNMP Agent, use the snmp-server community command. The no form of this command removes the specified community string.

Table 76 Configuring snmp-server community

Command Syntax	Command Mode	Purpose
snmp-server community *[community] [ro|rw]* **no snmp-server community** *[community]*	CONFIGURATION	Add an SNMP community string that identifies an access control domain for the SNMP agent. **ro:** Specifies read-only access. Authorized management stations are able to retrieve, but not modify, MIB objects. **rw:** Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects. Remove SNMP community string
show snmp-server community	PRIVILEGED EXEC	Display all configured community strings

Configuring SNMP Trap

To specify the recipient of a SNMP trap (a mechanism used to notify Network Management Servers of a change in the network device state), use the snmp-server host configuration command. To remove the specified host, use the no form of this command.

Table 77 Configuring snmp-server host

Command Syntax	Command Mode	Purpose
snmp-server host *[ip-address] [community] [udp-port] [*<v2c> <inform>*]*	CONFIGURATION	Configure IP address of SNMP host to receive traps using the specified community string and SNMP port. (If D-Link NMS is used, the port number will be 162). The fllowing TRAPs are provided here:

		V1 TRAP V2C TRAP V2C INFORM INFORM type increases the retransmission mechanism on the basis of the original TRAP, which is conducive to the event of NMS perception equipment in the wireless environment. As the complexity of the wireless environment, the traditional Trap (based on unreliable protocol) will sometimes result in the occurrence of TRAP packet loss, which in turn will lead to the result that NMS can't receive the TRAP information. INFORM will receive the NMS response when TRAP issued, which can provide more reliability compared to the traditional TRAP, so it is proposed to report event using INFORM in the wireless environment.
show snmp-server host	PRIVILEGED EXEC	Display all SNMP trap hosts with associated community strings and ports

Configuring SNMPv3 users

DWR series also supports SNMPv3, which introduces the concept of users. The following commands control the SNMPv3 user database on each DWR series router:

Table 78 Configuring SNMPv3 users

Command Syntax	Command Mode	Purpose
snmp-server v3user *<name> <ro|rw> <MD5 pass> <DES pass> <user-type>* **no snmp-server v3 user <name>**	CONFIGURATION	Configure a new or existing SNMPv3 user account. Remove an existing SNMPv3 user account name: SNMPv3 user name ro|rw: whether the user is read-only or read-write MD5 pass: Authentication password DES pass: Encryption password user-type: auth auth, no priv noauth no auth, no priv priv auth, priv
show snmp-server v3user	PRIVILEGED EXEC	Display all configured SNMP V3 user accounts

Viewing the snmp-server information

```
DWR-500# show snmp-server community
```

```
community string                access mode
public                          read-only
private                         read-write
!
DWR-500# show snmp-server host
host                            community string                port
192.168.10.55                       public                      162
192.168.10.10                       trap                        162
192.168.10.64                       trap                        162
192.168.10.130                      trap                        162
192.168.10.44                       public                      162
DWR-500# show snmp-server v3user
user            access      usm-level  auth-pass       priv-pass
read            read-only   noauth     12345678        12345678
```

Figure 58 Output of snmp-server configuration

Chapter 17 PPTP Configure

PPTP overview

Point-to-Point Tunneling Protocol (PPTP) is a network Technology that supports multi-protocol virtual private network, users can set up tunnels connecting to the external network security. PPTP is the expansion of PPP protocol providing communication ways for multi-protocol security VPN on IP network. Remote users can visit the technical network by any ISP which supports PPTP. PPTP can provide confidential communications between PPTP client and PPTP servers. PPTP client refers to the PC or terminals which runs this protocol, PPTP server refers to the server which runs this protocol.

PPTP Working Principle

Customers can access the public IP network by dial-up connections in the traditional PPTP. First of all, dial-up customers can access to the ISP's server (NAS) by conventional dial-up ways to establish a PPP connection; and then customers' secondary dial-up can establish PPTP server connectivity on that basis, which is called PPTP tunnel. As for the direct IP network customers, it does not need the first PPP dial-up connections, but can directly create a virtual pathway with the PPTP server.

PPTP Application on DWR

DWR can realize the PPTP client function which aims at building a tunnel between NMS server and Mesh gateway to improve the communication and security performance.

DWR currently provides CHAP encryption authentication.

PPTP Client Configuration Command

User name and password files for configuring PPTP

Figure 79 User name and password files for configuring PPTP

Command Syntax	Command Mode	Purpose
vpn pptp server <*word*> **no vpn pptp server** <*word*>	CONFIGURATION	Add a PPTP Server Remove PPTP Server
user <*USERNAME PASSWD*> **no user** <*USERNAME*>	VPN PPTP SERVER	Add a user name and password Remove a user name

Tunnel configure

Table 80 Tunnel configuration

Command Syntax	Command Mode	Purpose
interface tunnel *<0-3>*	CONFIGURATION	Configure tunnel
destination *[A.B.C.D]* **no destination**	INTERFACE TUNNEL	Configure PPTP Sever a destination Remove PPTP Sever destination
ip address *[A.B.C.D]* **no ip address**	INTERFACE TUNNEL	Configure interface a IP Address Remove IP Address
protocol pptp *[SERVERNAME USERNAME]* **no protocol pptp**	INTERFACE TUNNEL	Configure tunnel a PPTP Server and a user name Clear PPTP Server of tunnel
shutdown **no shutdown**	INTERFACE TUNNEL	Close Tunnel manually Boot Tunnel manually
show interface tunnel *<0-3>*	EXEC	Display all the configured Tunnel

Typical Configuration

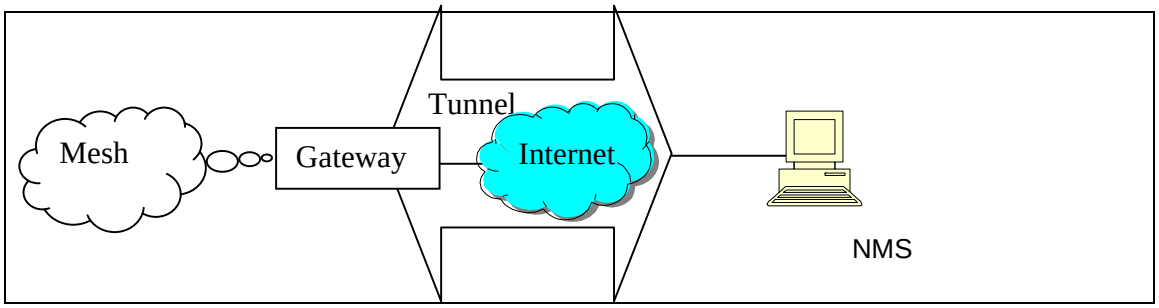


Figure 59 Tunnel typical configuration

Enable PPTP server on NMS server. The PPTP address is 192.168.10.69 and DHCP Server is also enabled, the user name and password is test and the encryption verify method is chap. Detailed information please refer to NMS manual.

Gateway Configuration：

```
DWR(config)# vpn pptp server test
DWR(config-vpn)# user test test
DWR(config-vpn)# exit
DWR(config)# interface tunnel 0
DWR(config-if-tunnel)# destination 192.168.10.69
```

```
DWR(config-if-tunnel)# protocol pptp test test
DWR(config-if-tunnel)# end
```

PPTP diagnose

Display tunnel command

Table 81 Display Tunel order

Command Syntax	Command Mode	Purpose
show interface tunnel <*0-3*>	PRIVILEGED EXEC	Display all the configured tunnels

Display tunnel interface

```
M150# show interface tunnel 0
Interface ppp0
 admin status: up  physical status: up
 protocol: pptp server name: pptpd destination: 192.168.10.69
 authentication: chap  user: hzhang
  index 536 metric 1 mtu 1500 <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
  HWaddr: f8:fc:bf:ff:f8:e8
  inet 192.168.101.2/32 pointopoint 192.168.101.1
    input packets 20, bytes 1361, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    input rate 0 bytes/s
    output packets 8, bytes 295, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    output rate 0 bytes/s
    collisions 0
```

Figure 60 Output of tunnel interface

Fault Diagnose

When the tunnel physical status displays down, please diagnose in the following ways:

1. Whether the network can be linked between PPTP client DWR and PPTP server, if not, please check the routing information and link status
2. Whether the user name and password is the same in PPTP client and the server ends
3. Whether the PPTP server encryption verified method is chap，if not，please change it to chap.

Chapter 18 Other commands and utilities

This chapter contains other commands and troubleshooting utilities on the DWR series, it has the following sections:

- Save & Reboot
- Ping & Traceroute
- Telnet Client & Server
- Auto Recovery
- Interference Detection Tool

Save & Reboot

Save

D-Link recommends that you save your configuration often.

To save a configuration file, use either of the following commands in the Privileged EXEC mode:

Table 82 Save the running configuration to startup configuration

Command Syntax	Command Mode	Purpose
copy running-config startup-config	PRIVILEGED EXEC	Save the current running configuration to the startup-config file.
write memory	PRIVILEGED EXEC	Save the current running configuration to the startup-config file.

Reboot

D-Link provides command **reboot** to hot restart DWR series. After upgraded, user can use command **reboot** to restart DWR series, then the new image takes effects.

Table 83 Reboot configuration

Command Syntax	Command Mode	Purpose
Reboot	PRIVILEGED EXEC	Restart DWR

Ping & Traceroute

Commands **ping** and **traceroute** are very helpful utilities to troubleshoot network access problems.

Ping

Command **ping** a very common method for troubleshooting the accessibility of devices. It uses a series of Internet Control Message Protocol (ICMP) Echo messages to determine:
Whether a remote host is active or inactive.
The round-trip delay in communicating with the host.
Packet loss.

Command **ping** first sends an echo request packet to an address, then waits for a reply, the reply will be recorded with latency. The default **ping** packet is 6, **Ctrl+c** can terminate **ping**.

Traceroute

Command **traceroute** is used to discover the routes that packets actually take when traveling to their destination. The network device sends out a sequence datagram of User Datagram Protocol (UDP) to an invalid port address at the remote host.

Three datagram are sent, each with a Time-To-Live (TTL) field value set to one. The TTL value of 1 causes the datagram to "timeout" as soon as it hits the first router in the path; this router then responds with an ICMP Time Exceeded Message (TEM) indicating that the datagram has expired.

Another three UDP messages are now sent, each with the TTL value set to 2, which causes the second router to return ICMP TEMs. This process continues until the packets actually reach the other destination. Since these datagram are trying to access an invalid port at the destination host, ICMP Port Unreachable Messages are returned, indicating an unreachable port; this event signals the Traceroute program that it is finished.

The purpose behind this is to record the source of each ICMP Time Exceeded Message to provide a trace of the path the packet took to reach the destination.

Table 84 Ping & traceroute configuration

Command Syntax	Command Mode	Purpose
ping { <*A.B.C.D*> | <*hostname*> }	PRIVILEGED EXEC	Detect remote device accessibility or not.
ping { <*A.B.C.D*> | <*hostname*> } count (1-6000) size (1-6000)	PRIVILEGED EXEC	Specify the number of packets and their size, and detect remote device accessibility or not.
traceroute { <*A.B.C.D*> | <*hostname*> }	PRIVILEGED EXEC	Trace the path of the packet to destination.

```
DWR-500# ping 192.168.15.126
PING 192.168.15.126 (192.168.15.126): 56 data bytes
84 bytes from 192.168.15.126: icmp_seq=0 ttl=64 time=8.7 ms
84 bytes from 192.168.15.126: icmp_seq=1 ttl=64 time=0.8 ms
84 bytes from 192.168.15.126: icmp_seq=2 ttl=64 time=1.0 ms
84 bytes from 192.168.15.126: icmp_seq=3 ttl=64 time=0.9 ms
84 bytes from 192.168.15.126: icmp_seq=4 ttl=64 time=1.0 ms
84 bytes from 192.168.15.126: icmp_seq=5 ttl=64 time=0.9 ms

--- 192.168.15.126 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.8/2.2/8.7 ms

DWR-500# ping 192.168.15.11
PING 192.168.15.11 (192.168.15.11): 56 data bytes

--- 192.168.15.11 ping statistics ---
6 packets transmitted, 0 packets received, 100% packet loss


DWR-500# traceroute 192.168.15.126
traceroute to 192.168.15.126 (192.168.15.126), 30 hops max, 40 byte packets
 1  192.168.15.126 (192.168.15.126)  7.134 ms  1.323 ms  0.821 ms
DWR-500#
```

Figure 61 Output of ping & traceroute information

Telnet Client & Server

DWR series can play role as Telnet Client and Telnet Server.

Telnet Client
When DWR series acts as Telnet client, you can use command **telnet** to access other device.

Telnet Server
When DWR series acts as Telnet server, you should use command **ip telnet server** to enable the service. Telnet Server disable by default.

Table 85 Telnet Client & Server configuration

Command Syntax	Command Mode	Purpose
telnet { *<A.B.C.D>* | *<hostname>* } [port]	PRIVILEGED EXEC	Access remote device through Telnet.
ip telnet server **no ip telnet server**	CONFIGURATION	Enable telnet server. Disable telnet server

Viewing Telnet Server configuration

```
!
ip telnet server
!
```

Auto Recovery

Auto Recovery is an advanced feature provided by DWR series, When enabled, Auto Recovery will automatically detect and recover from system fault. When configured with a portal IP, auto recovery would also monitor its connectivity with the portal node. If the connectivity is lost and auto recovery believes it is due to a local problem, it will automatically reboot the router as an attempt to restore its normal working state.

Table 86 Auto Recovery configuration

Command Syntax	Command Mode	Purpose
service recovery	CONFIGURATION	Enter Auto Recovery configuration mode
Enable	SERVICE RECOVERY	Administratively activate Auto Recovery
Disable	SERVICE RECOVERY	Administratively disable Auto Recovery
portal ip *<A.B.C.D>* **no portal ip *<A.B.C.D>***	SERVICE RECOVERY	Set an IP address for the device to check the state of wired network Delete portal IP address

Viewing Auto Recovery configuration

```
!
service recovery
 enable
```

```
!
```

Figure 62 View auto-recovery configuration

Interference Detection Tool

D-Link's interference detection tool enhances the performance of detecting interference, which can:

- Show CCA(clear channel assessment) percentage to provide the idle percentage of channel.
- Show real-time noise intensity to reflect non-WIFI interference degree in air.
- Show WIFI channel status
  - ✓ Provide channel-occupied percentage by WIFI traffic,
  - ✓ Provide different traffic types, such as multicast, unicast (to this router or other router), to display the reason for channel occupation.
  - ✓ Reflect collision status through FCS error rate.

Table 87 Interference Detection Command

Command Syntax	Command Mode	Purpose
debug dot11radio (radio_index) noise_detection physical (a|b|g|trunka|trunkg) (num)	PRIVILEGED EXEC	Detect the interference information of specified channels
debug dot11radio (radio_index) noise_detection physical (a|b|g)	PRIVILEGED EXEC	Detect the interference information of all the channels in specified mode
debug dot11radio (radio_index) noise_detection	PRIVILEGED EXEC	Detect the interference information of all channels

Chapter 19 MIBs and RFCs

Supported MIBs

The following is a list of Management Information Bases (MIBs) supported by DWR series.

Public Part:

- IF-MIB
- RFC 1213-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-USER-BASED-SM-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMP-VIEW-BASED-ACM-MIB
- TCP-MIB
- UDP-MIB

Private Part:

- D-LINK-DDWR-MIB
- D-LINK-DEVICE-INFO-MIB
- D-LINK-DOT11-BSS-MIB
- D-LINK-DOT11-QOS-MIB
- D-LINK-DOT11-SECURITY-MIB
- D-LINK-FLASH-MGMT-MIB
- D-LINK-IF-MIB
- D-LINK-NMS-COMPATIBLE
- D-LINK-REF-MIB
- D-LINK-RFM-MIB
- D-LINK-ROAMING-MIB
- D-LINK-ROUTING-IF-MIB
- D-LINK-SYSMGMT-MIB
- D-LINK-WMIMGMT-MIB

Supported RFCs

- RFC 1213 Network Management of TCP/IP-based internet: MIB-II
- RFC 1157 Simple Network Management Protocol
- RFC 1573 Interfaces Group MIB
- RFC 2012 SNMPv2 Management Information Base for the TCP
- RFC 2013 SNMPv2 Management Information Base for the User Datagram Protocol
- RFC 2271 An Architecture for Describing SNMP Management Frameworks
- RFC 1901 Introduction to Community-based SNMPv2
- RFC 1902 Structure of Management Information for Version 2 of the SNMPv2
- RFC 1903 Textual Conventions for SNMPv2
- RFC 1904 Conformance Statements for SNMPv2

- RFC 1905 Protocol Operations for SNMPv2
- RFC 1906 Transport Mappings for SNMPv2
- RFC 1907 Management Information Base for SNMPv2
- RFC 2571 Architecture for SNMP Frameworks
- RFC 2572 Message Processing and Dispatching
- RFC 2573 SNMP Applications
- RFC 2574 User-based Security Model (USM) for SNMPv3
- RFC 2575 View-based Access Control Model (VACM) for SNMP
- RFC 2578 Structure of Management Information Version 2 (SMIv2).
- RFC 2579 Textual Conventions for SMIv2
- RFC 2580 Conformance Statements for SMIv2

Chapter 20 List of Commands

	<cr>
A	aaa
	access-category <bk|be|vi|vo>
	accept-point bssid HH:HH:HH:HH:HH:HH
	access-point bssid-filter acceptable-prefix HH:HH:HH:HH:HH:HH HH:HH:HH:HH:HH:HH
	access-point ssid WORD
	allowed-frequency-range a (4.9 | 5)
	allowed-frequency-range (a | abg | bg)
	antenna {0|1|2}
	authentication open
	authentication open key-management wpa <wpa-profile-name>
	authentication open key-management wpa2 <wpa2-profile-name>
	authentication open wep <wep-profile-name> default-key <1-4>
	authentication shared wep <wep-profile-name> default-key <1-4>
B	bss WORD
C	centralized-control
	class NAME
	clear certificate ca
	clear counters interface dot11radio INDEX
	clear counters interface dot11radio INDEX (wdsauto|wdsmanu) <0-5>
	clear counters interface fast-ethernet INDEX
	clear log { DDWR|hostapd|rf-management|Dtrix|cli|station|ospf }
	clear rf-management {neighbor all| neighbor mac HH:HH:HH:HH:HH:HH | process }
	client-authentication (open|shared) wep PROFILE-NAME default-key <1-4>
	client-authentication open key-management (wpa|wpa2) client-8021x PROFILE-NAME
	client-authentication open key-management wpa-psk (hex|ascii) WORD
	client-authentication open key-management wpa2-psk (hex|ascii) WORD
	client-list A.B.C.D/M
	clock <2005-2037> <1-12> <1-31> <0-23> <0-59> <0-59>
	configure terminal
	copy running-config startup-config
	country-code (AU|CN|EU|IL|JP|KR|LA|NA|PS|SG|TW|US)
	cts-protection {0|1|2|3}
D	debug (hap|cli) { none|error|state|info|frame|dump }
	debug rf-management (events|messages|packets|errors|ping| active-neighbors| global-variables| radios-variables| reject-neighbors| scan-neighbors)
	debug dot11radio Index distance [{default<a|b|g> |timout VALUE}]
	debug dot11radio Index scan [{bssid HH:HH:HH:HH:HH:HH| physical (a|g) N | pectrum | ssid WORD }]
	debug dot11radio INDEX noise_detection
	debug dot11radio INDEX noise_detection physical (a|b|g|trunka|trunkg)
	debug dot11radio INDEX noise_detection physical (a|b|g|trunka|trunkg) N
	debug dot11radio INDEX scan
	debug dot11radio INDEX scan bssid HH:HH:HH:HH:HH:HH
	debug dot11radio INDEX scan physical (a|g|trunka|trunkg) N
	debug dot11radio INDEX scan spectrum
	debug dot11radio INDEX scan ssid WORD
	debug phm (error|info|dump)
	default-lease-time <0-31536000>
	dhcp relay

	dhcp relay option circuit-id WORD
	dhcp server
	dhcp server {<POOL-NAME> | automatic}
	dhcp-servers SERVER-list
	disable
	dns DNS-list
	domain-name NAME
	dynamic-metric
E	eap-method (peap|ttls) phase2 (md5|mschapv2|tls)
	eap-method tls
	eap-reauth-period <0-65535>
	enable
	encryption-mode-cipher {tkip|ccmp}
	end
	exit
F	force-sta-wme
	force-rate-control-algorithm (video|data)
G	gateway A.B.C.D
H	help
	hello-on-wds
	hostname WORD
	host HH:HH:HH:HH:HH A.B.C.D
I	ignore-broadcast-ssid
	interference-avoidance
	interface dot11radio Index
	interface fast-ethernet <0-1>
	interface tunnel <0-3>
	interface vlan <1-4095>
	install certificate ca URL
	install certificate client URL
	install client-key URL
	install client-key URL password PRIVATE-KEY-PASSWORD
	ip address A.B.C.D/M
	ip address dhcp
	ip forwarding
	ip dhcp {relay|server}
	ip nat
	ip route A.B.C.D/M A.B.C.D [<1-255>]
	ip route A.B.C.D/M station <name> <0-N>
	ip telnet server
L	list
M	mac-addr HH:HH:HH:HH:HH:HH
	mac-address {deny|accept} MAC-LIST-NAME
	mac-address accept-all
	mac-list WORD
	mapping static A.B.C.D/M A.B.C.D
	max-auto-wds <1-6>
	max-hop-count <1-255>
	max-lease-time <0-31536000>
	max-rate (60|90|120|180|240|360|480|540|10|20|55|110)
	max-station-allowed <0-240>
	mode {access|backhaul|client}
	mode backhaul WORD

	mode {access|gateway A.B.C.D/M|none}
	mtu <256-1500>
	mtu <256-2274>
N	network {A.B.C.D|A.B.C.D/M} network{ A.B.C.D A.B.C.D}
	no access-category
	no access-point bssid
	no access-point bssid-filter acceptable-prefix
	no access-point bssid-filter acceptable-prefix HH:HH:HH:HH:HH:HH HH:HH:HH:HH:HH:HH
	no access-point ssid
	no antenna
	no authentication
	no bss WORD
	no centralized-control
	no class NAME
	no client-authentication
	no client-list
	no client-list A.B.C.D/M
	no cts-protection
	no country-code
	no default-lease-time
	no dhcp
	no dhcp-servers
	no dns
	no domain-name
	no dynamic-metric
	no eap-method
	no eap-reauth-period
	no encryption-mode-cipher
	no force-rate-control-algorithm
	no force-sta-wme
	no gateway A.B.C.D
	no hello-on-wds
	no hostname [HOSTNAME]
	no host HH:HH:HH:HH:HH:HH
	no ignore-broadcast-ssid
	no interference-avoidance
	no interface vlan <1-4094>
	no ip address
	no ip dhcp {relay|server}
	no ip forwarding
	no ip nat
	no ip route A.B.C.D/M {A.B.C.D|station WORD Index}
	no ip telnet server
	no mac-address
	no mac-addr HH:HH:HH:HH:HH:HH
	no mac-list WORD
	no mac-ip-list
	no mac-ip-list HH:HH:HH:HH:HH:HH
	no mapping static (all|A.B.C.D/M)
	no max-lease-time
	no max-rate
	no max-station-allowed
	no mode

	no mtu
	no network prefix /prefix-length area area-id
	no out-interface dot11radio INDEX station WORD
	no out-interface fast-ethernet <0-1>
	no packet-loss-ratio
	no password
	no pool NAME
	no primary-gateway-election
	no profile mesh WORD
	no qos class
	no radius-server A.B.C.D (auth|acct)
	no range A.B.C.D A.B.C.D
	no redistribute DDWR
	no retry
	no role
	no router ospf
	no router DDWR
	no rts-threshold
	no scanning { hardware-modes| mininum-interval| threshold rssi}
	no security-profile {8021x|client-8021x|wep|wpa|wpa2} WORD
	no service roaming-Dtrix
	no server A.B.C.D
	no shutdown
	no software-retry
	no snmp-server community COMMUNITY
	no snmp-server host A.B.C.D
	no snmp-server v3user USERNAME
	no ssid <SSID>
	no station WORD
	no station-inactivity-limit
	no station-inactivity-policy
	no station-isolation
	no station-list
	no station-list HH:HH:HH:HH:HH:HH
	no supermode
	no tx-power-reduction
	no unicast-rate
	no user-name
	no wds {<0-5>|auto}
	no wds-cipher-type
	no wds-rssi-limit
	no wds-unicast-rate
	no wep-key <1-4>
	no wireless-mode
	no wme
	no wpa-type {8021x|psk}
	no wpa2-type {8021x|psk}
	no vpn pptp server WORD
	node-id <1-8191>
O	out-interface dot11radio INDEX station WORD
	out-interface fast-ethernet <0-1>
P	password PASSWORD-STRING
	packet-loss-ratio (low|very-low|lowest)

	ping WORD
	ping WORD count <1-60000> size <1-60000>
	primary-gateway-election
	pool [NAME]
	profile mesh <WORD>
Q	qos
	qos class NAME
	quit
R	radius-server A.B.C.D {auth-port {<1-65535>|default}|acct-port{<1-65535>|default} key WORD
	range A.B.C.D A.B.C.D
	reboot
	remote-mac HH:HH:HH:HH:HH:HH
	release-dhcp {dot11radio Index station WORD |fast-ethernet<0-1>}
	remote node <1-8191> INDEX
	renew-dhcp {dot11radio Index station WORD |fast-ethernet<0-1>}
	restart-dhcp {dot11radio Index station WORD| fast-ethernet<0-1>}
	retry <1-32> <1-32>
	rts-threshold <0-2347>
	role (ap|station|auto)
	router {DDWR|ospf}
	router-id A.B.C.D
	router-password root
S	scanning hardware-modes (a|g|ag) <channel-list WORD>
	scanning minimum-interval <1-300>
	scanning threshold rssi <0-100>
	security-profile {8021x|client-8021x|wep|wpa|wpa2} WORD
	server-group
	server A.B.C.D (auth|acct)
	service recovery
	service rf-management
	service roaming-Dtrix
	setup ap (AU|CN|EU|IL|JP|KR|LA|NA|PS|SG|TW|US) <1-8191> A.B.C.D A.B.C.D/M WORD WORD
	setup factory
	setup point (AU|CN|EU|IL|JP|KR|LA|NA|PS|SG|TW|US) <1-8191> A.B.C.D A.B.C.D/M
	setup portal (AU|CN|EU|IL|JP|KR|LA|NA|PS|SG|TW|US) <1-8191> A.B.C.D A.B.C.D/M WORD WORD
	setup portal (AU|CN|EU|IL|JP|KR|LA|NA|PS|SG|TW|US) <1-8191> A.B.C.D A.B.C.D/M A.B.C.D WORD WORD nat-off
	setup portal (AU|CN|EU|IL|JP|KR|LA|NA|PS|SG|TW|US) <1-8191> A.B.C.D dhcp WORD WORD
	setup portal (AU|CN|EU|IL|JP|KR|LA|NA|PS|SG|TW|US) <1-8191> A.B.C.D dhcp WORD
	WORD nat-off
	show aaa
	show arp
	show arp A.B.C.D
	show avt configuration
	show avt status
	show certificate (ca|client)
	show clock
	show country-code
	show config
	show cpu
	show dhcp relay dhcp-servers
	show dhcp server {all| default-lease-time|dns|lease|lease A.B.C.D | lease count |max-lease-time|pool|pool POOL-NAME}

	show interface dot11radio INDEX stations
	show hardware
	show hostname
	show interface brief
	show interface dot11radio INDEX[{stations|info|txpower| node-database}]
	show interface dot11radio INDEX bss WORD {accept-macs| deny-macs| stations| wep-keys}
	show interface dot11radio INDEX bss WORD ssid WORD wep-keys
	show interface dot11radio INDEX interference-status
	show interface dot11radio INDEX interference-status physical (a|b|g) N
	show interface dot11radio INDEX {wds|wdsauto} <0-5>
	show interface dot11radio INDEX bss WORD ssid [WORD|WORD wep-keys]
	show interface fast-ethernet <0-1>
	show interface tunnel <0-3>
	show interface vlan <1-4094>
	show ip DDWR {configuration|database|neighbor}
	show ip forwarding
	show ip mobility Dtrix {mac-ip-list|station-list|stations }
	show ip ospf {configuration|database|interface|neighbor}
	show ip route [{DDWR|connected|static| A.B.C.D| A.B.C.D/M| A.B.C.D/M longer-prefixes|fib|summary}]
	show log {DDWR|cli|hostapd|rf-management|Dtrix|station|phm|ospf}
	show mac-list
	show nat {out-interface|configuration|table| mapping static }
	show node-id
	show process
	show profile mesh
	show qos dot11radio Index {class|qdisc}
	show qos {configuration|interface}
	show recovery configuration
	show rf-management {active-neighbors|interface|configuration| scan-neighbors|path-info| reject-neighbors}
	show rf-management dot11radio (radio_index) chan-stats
	show rf-management dot11radio (radio_index) chan-stats physical (a|b|g) (num)
	show router id
	show running-config
	show security-profile (wep|wpa|wpa2|8021x|client-8021x)
	show snmp-server {community|host|v3user}
	show startup-config
	show uptime
	show version
	show vlan
	shutdown
	software-retry <1-10>
	snmp-server community COMMUNITY {rw|ro}
	snmp-server host A.B.C.D COMMUNITY <1-65535>
	snmp-server host A.B.C.D COMMUNITY <1-65535> v2c inform
	snmp-server v3user USERNAME {ro|rw} MD5PWD DESPWD {noauth|auth|priv}
	ssid <SSID>
	ssid WORD
	station-list HH:HH:HH:HH:HH:HH A.B.C.D/M
	station WORD
	station-inactivity-limit <1-65535>
	station-inactivity-policy {0|1}

	station-isolation
	supermode
	switchport access vlan <1-4094>
	switchport trunk allowed-vlan WORD
	switch image
T	telnet WORD [PORT]
	traceroute WORD
	tx-power-reduction <0-300>
U	unicast-rate (60|90|120|180|240|360|480|540|10|20|55|110)
	upgrade (a|b) url URL boot (a|b)
	upgrade (a|b) url URL boot (a|b) reboot
	upgrade (inactive|running) url URL boot (inactive|running)
	upgrade (inactive|running) url URL boot (inactive|running) reboot
	upgrade (inactive|running) ftp A.B.C.D FILENAME USERNAME PASSWORD boot(inactive|running)
	upgrade(inactive|running)ftp A.B.C.D FILENAME USERNAME PASSWORD boot(inactive|running){reboot}
	user-name NAME-STRING
V	verify image (a | b)
	vpn pptp server WORD
W	wds-unicast-rate (60|90|120|180|240|360|480|540|10|20|55|110)
	wep-key <1-4> (ascii|hex) WORD
	wds <0-5>
	wds auto
	wds-cipher-type <tkip|ccmp>
	wds-rssi-limit <0-100> <0-100>
	wireless-mode (a|g|b|g-only|trunka|trunkg) [CHANNEL]
	wme
	write {memory|terminal}
	wpa-type 8021x NAME
	wpa-type psk (hex|ascii) WORD
	wpa2-type 8021x NAME
	wpa2-type psk (hex|ascii) WORD