DWR SERIES WIRELESS MESH ROUTER

WEB-BASED 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:

This document provides the instructions and examples for the configuration of D-LINK's DWR series wireless mesh routers through the Web-based Management Interface (WMI), and the document's scope is limited to as such. For information on DWR series' Command Line Interface (CLI) or other subjects, please refer to the CLI Configuration Guide and/or related documents.

Note: All screen shots displayed in this document are captured using an DWR-500 router and is for demonstration purposes only. The exact screen output may vary depending on the model of the router used as well as your browser and system settings.

Audience

This document is intended for system/IT or network administrator who is responsible for configuring or maintaining DWR series routers, this guide assumes the user has knowledge of wireless, wired, Layer-2, and Layer-3 networking technologies, and is comfortable with the use of an internet browser.

Related Documents

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

- DWR series CLI Configuration Guide

Chapter 2 Web Configuration Overview

The Web-based Management Interface (WMI) of DWR series offers the same configuration functions as the router's Command Line Interface (CLI) in a graphical interface accessible from most modern internet browsers, including Microsoft Interface Explorer or Mozilla Firefox. WMI allows administrators to manage a DWR series router from a remote location conveniently and efficiently.

WMI of DWR series contains the following configuration areas:

- Quick Start Configuration
- Global Settings
- Interface
- Network Settings (Routing, DHCP, NAT, Mesh Profiles)
- Services (Auto Recovery, Roaming, etc）
- Quality of Service
- Security (Wep Key Lists, MAC Address Lists)
- SNMP Settings
- Software Upgrade

The basic software requirement for the web-interface is:

- Web Browser： Internet Explorer 5.5 and above with Javascript enabled
- Optimal Resolution：1024 X 768 and above

Getting Started

This chapter introduces the basic functionality and layout of the Web-based Management Interface. It contains the following topics:

- Logging into the Web-based Management Interface
- WMI Basics

Logging into the Web-based Management Interface

To log in the web interface of a DWR series router, input the router IP address and the port address, such as 111.168.15.229 for router IP, and then input http://111.168.15.229:9080 in the web browser address. A pop-up dialog box would appear and request a username and password (see Figure).

On an un-configured DWR series router, it can connect a client PC to the router's Ethernet 0 port and the port's default IP address is 192.168.0.1.

The default username is 'root' and password is 'dlink'. After the successful authentication, the home page for WMI would appear (see Figure)

Figure 1 Logging into Web Management Interface (WMI)

Note: During the log-in process, an option such as “Remember my password” may appear. If this option is enabled, one would not be required to re-enter the username or password when accessing the WMI. Please use this option with care.

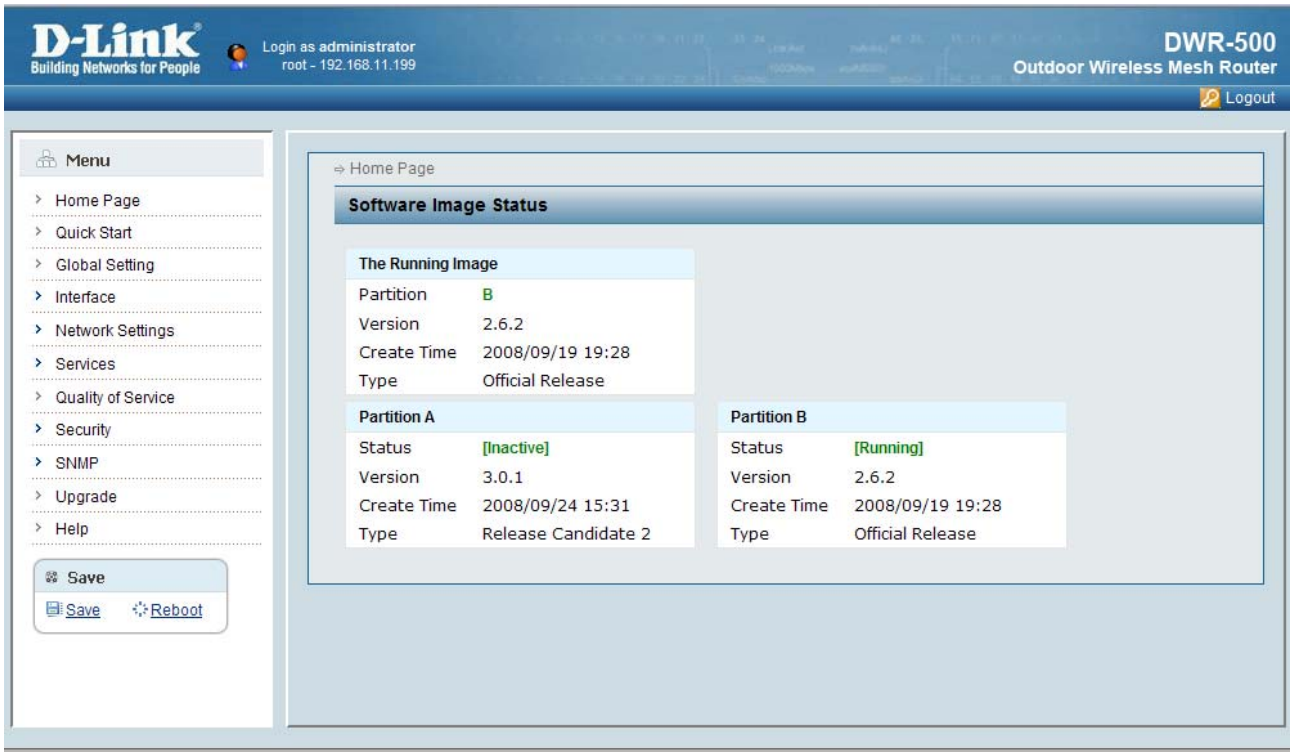


Figure 2 Web Management Interface Home Page

WMI Basics

The WMI is composed of three components: the title banner (top), the menu tree (left), the configuration area (right), and the locale selector (bottom) as shown in Figure 3. The title banner shows the router’s model name and the company Logo; the menu tree provides clear, hierarchical navigation to the various configuration areas. Clicking on one of the choices in the menu tree would cause the area on the right to

display the specific configurable settings for that menu choice. The locale selector on the bottom allows users to change the current language and locale-specific style used by the WMI. Currently, US English and PRC Chinese are supported.

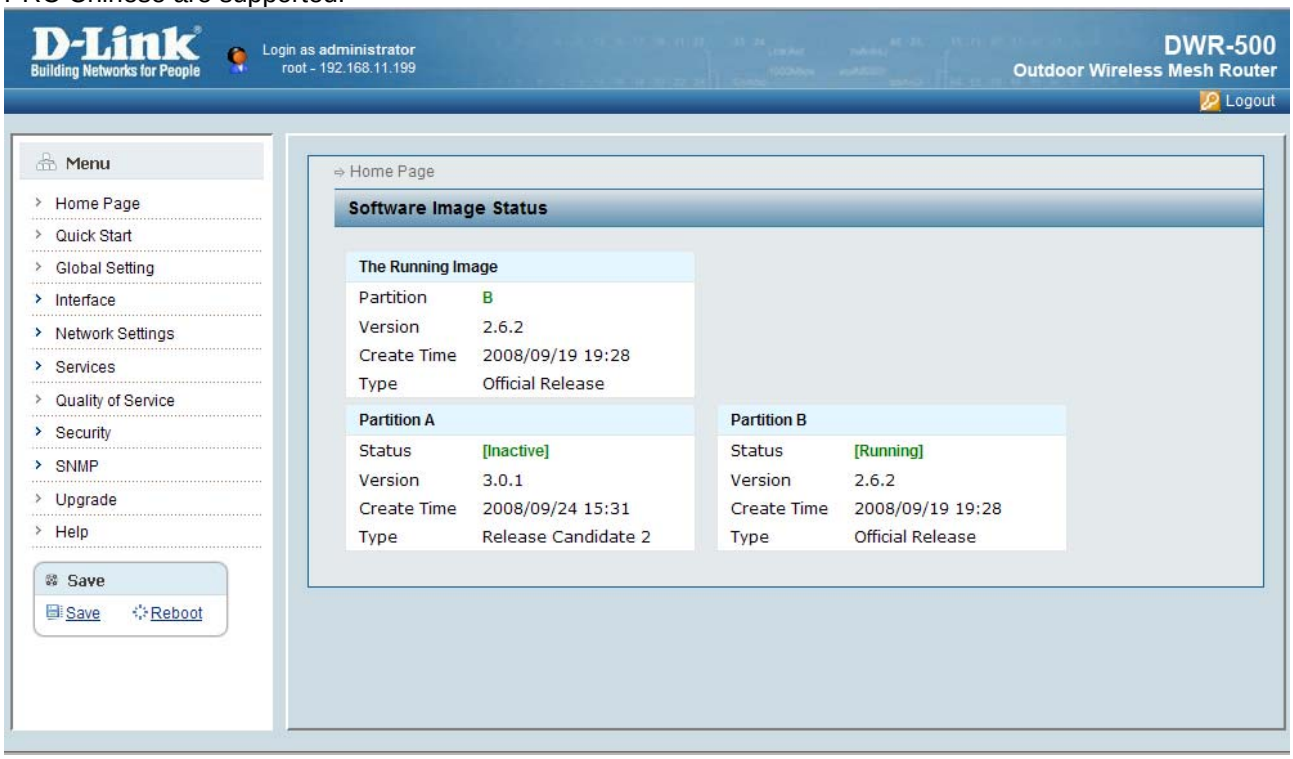


Figure 3 WMI Layout

Home page

After successfully logging into the DWR series Web Management Interface, one is lead directly to the configuration home page which displays the DWR series image status information as shown in Figure 4.

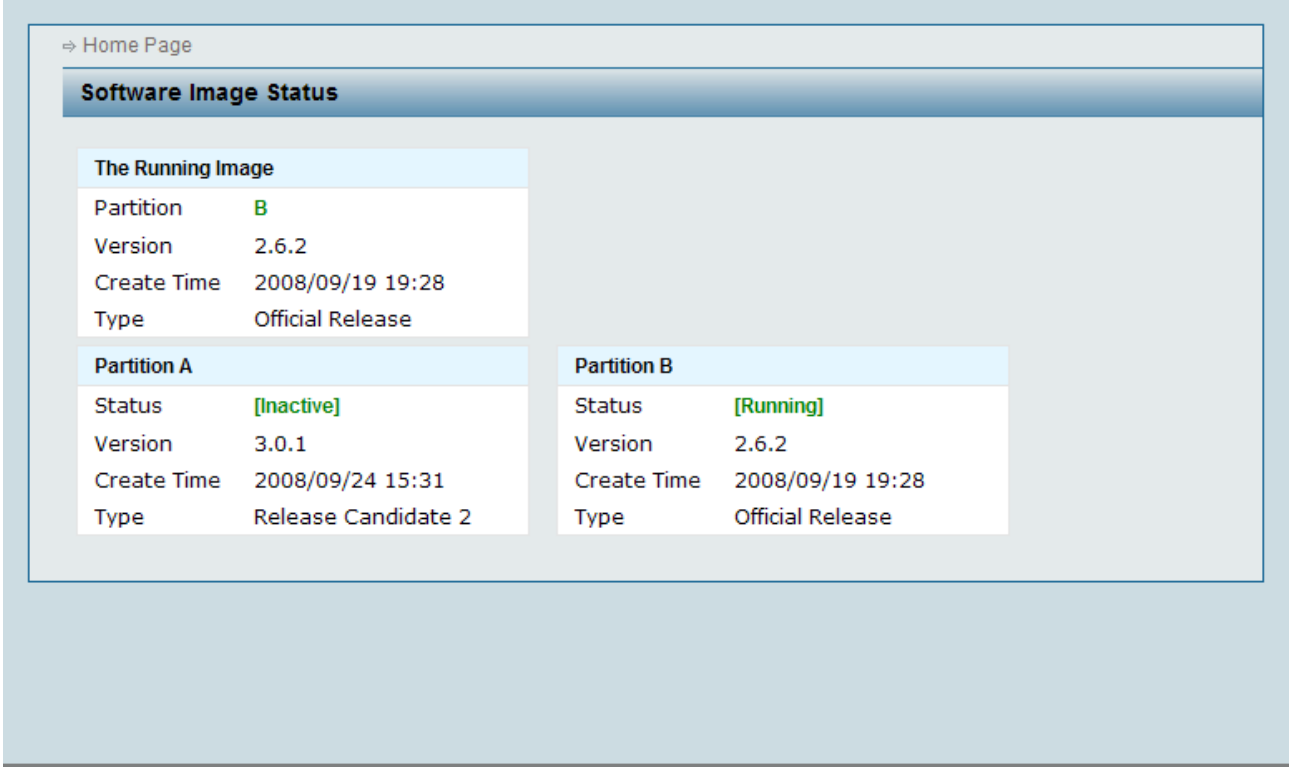


Figure 4 Software Image Status

Description of the version fields

Table 1 Software Image Version Fields

Field	Description
The Running Image	The image that is currently loaded and running
Partition A	The information that is preserved in Partition A
Partition B	The information that is preserved in Partition B

Obtaining Help

The Web-based Management Interface has a built-in on-line help page which can be accessed any time by clicking on “Help” at the bottom of the menu tree. The help text is displayed in the configuration area. An example help page is shown in Figure 5. The help page contains a variety of links to help information about specific configuration modules and items.

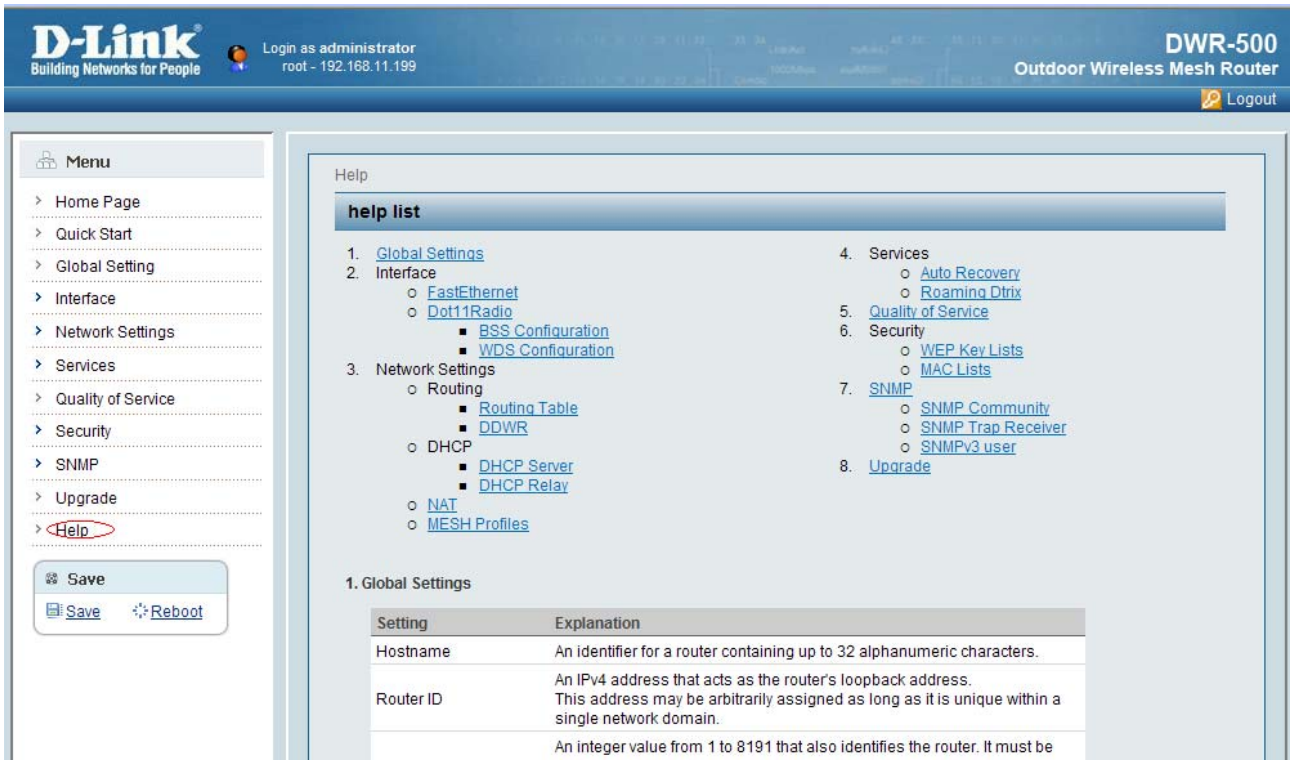


Figure 5 Sample Help Page

Chapter 3 Quick Start Configuration

Quick Start DWR series routers through WEB Installation Guide. It contains:

- Accessing the Quick Start Wizard
- Using the Quick Start Wizard

Accessing the Quick Start Wizard

To open the Quick Start Wizard, login in the home page, then click “Quick Start” link in the left-side menu tree. The Step 1 of the Quick Start Wizard appears at the right side of the web page (see Figure 6)

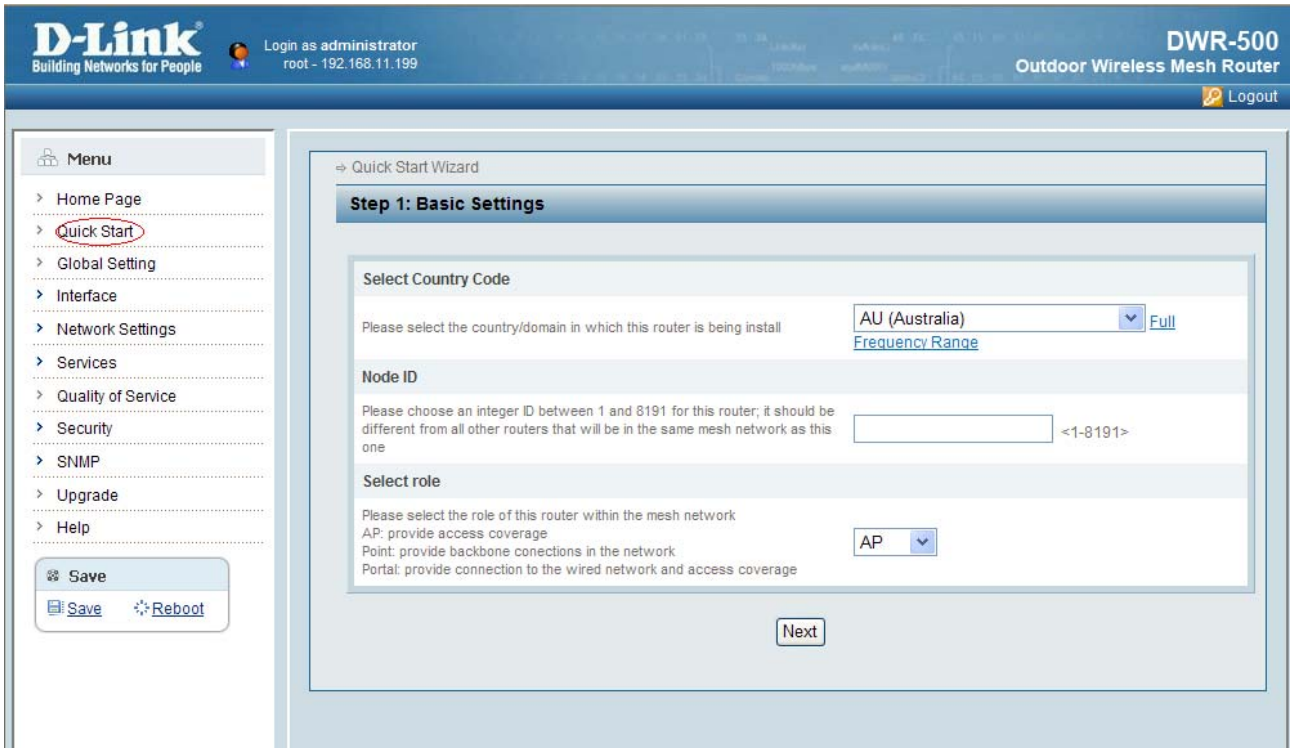


Figure 6 Web Management Interface Home Page

To open the Quick Start Wizard, click the “Quick Start” link in the left-side menu tree. The Step 1 of the Quick Start Wizard appears at the right side of the web page (see Figure 7)

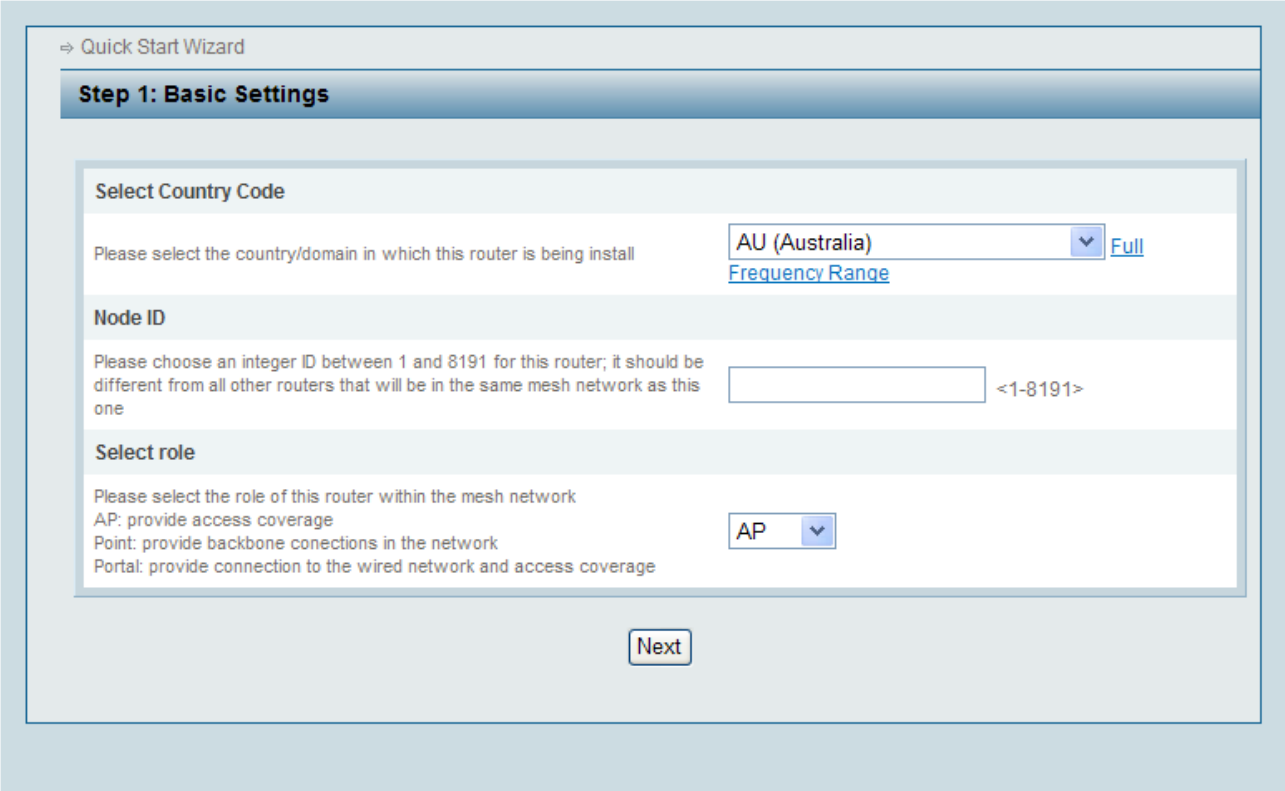


Figure 7 Web Management Interface Home Page

Using the Quick Start Wizard

To configure a node with the Quick Start Wizard, answer the questions asked during each step of the wizard. After entering the answers for all the questions at one step, click the “Next” button to go to the next step. The “Back” button could be used to return to the previous step, and clicking the “Finish” button at the end of the wizard completes the configuration.

Example Configuration 1: Portal node

The following figures show how the example portal node can be configured by answering the questions on each screen.

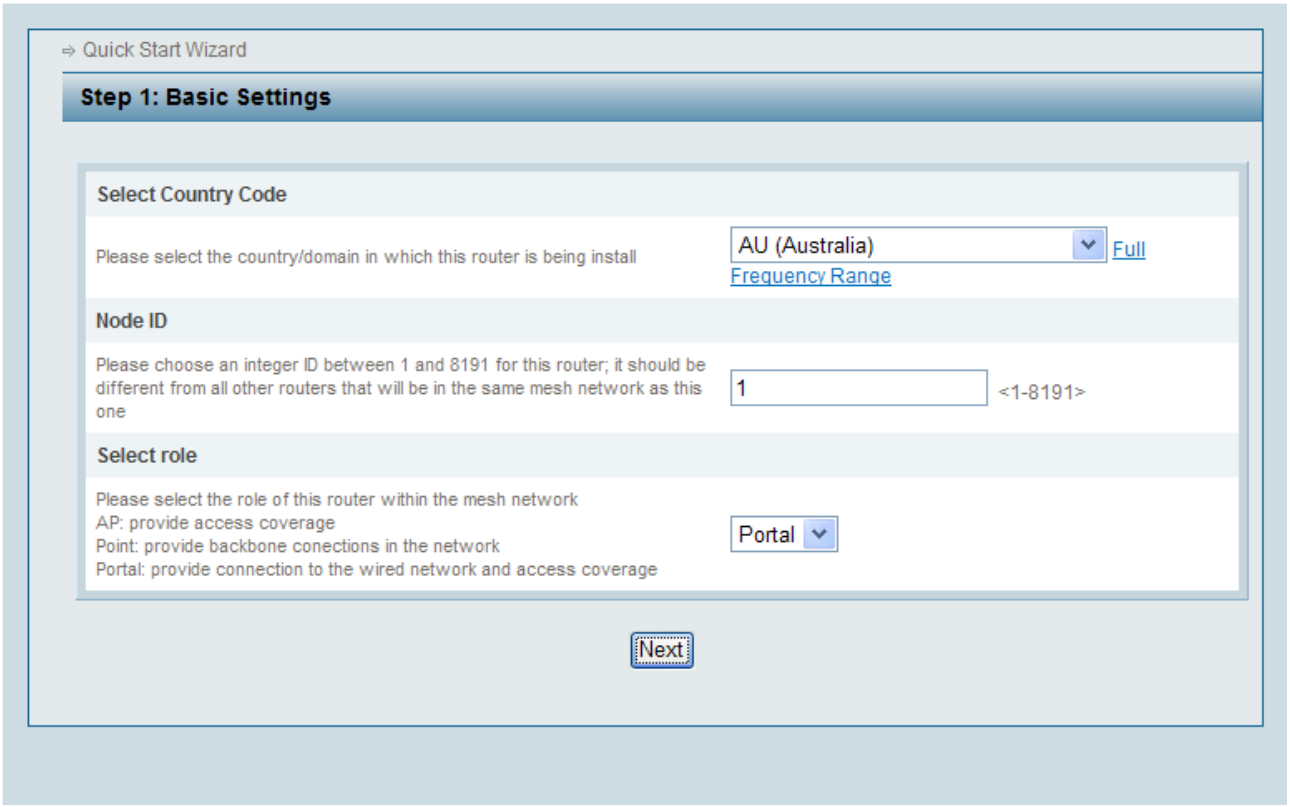


Figure 8 Configuring the portal node, step 1

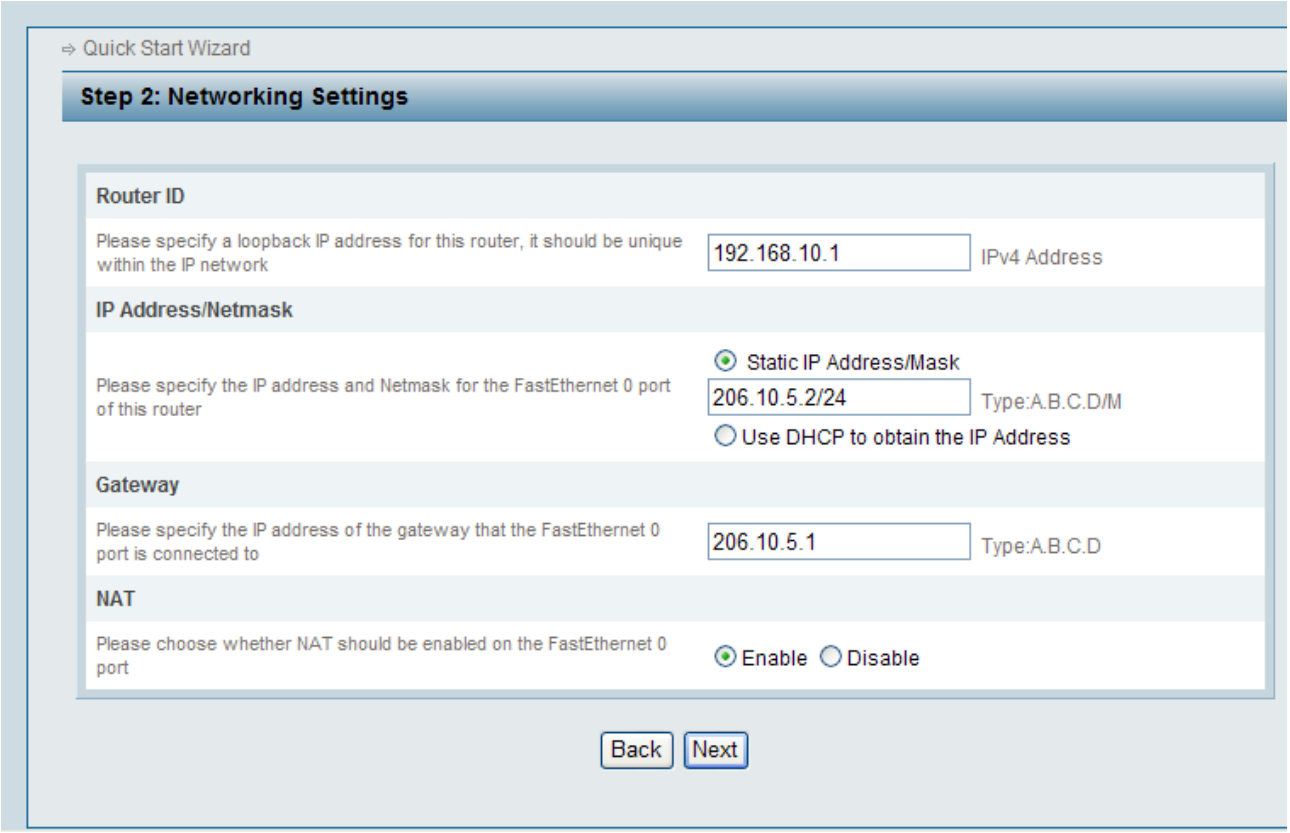


Figure 9 Configuring the portal node, step 2

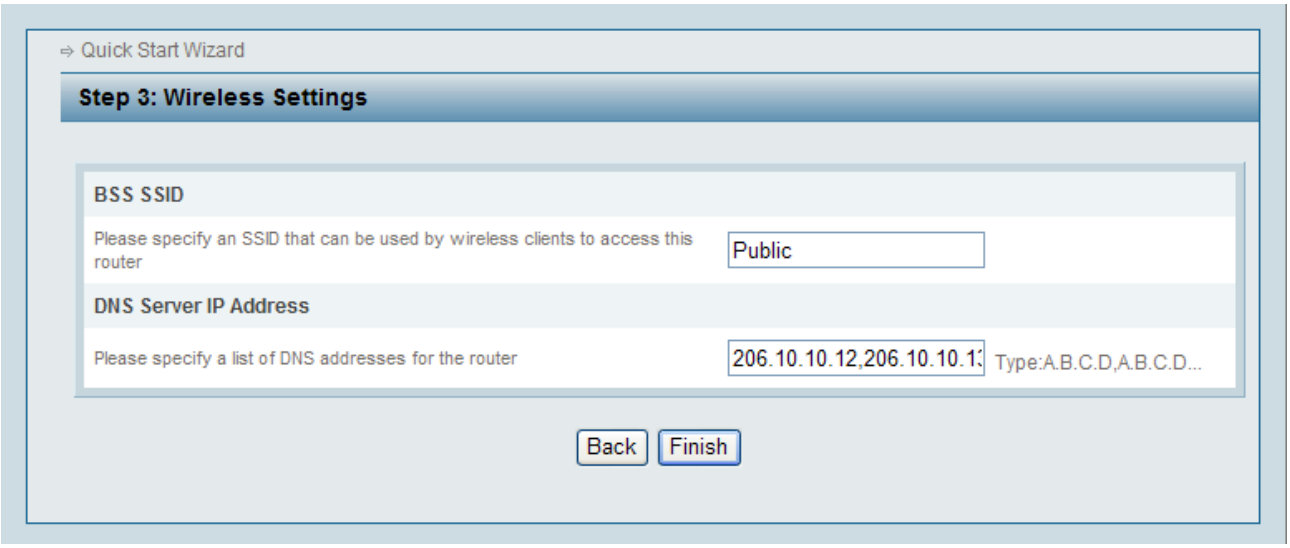


Figure 10 Configuring the portal node, step 3

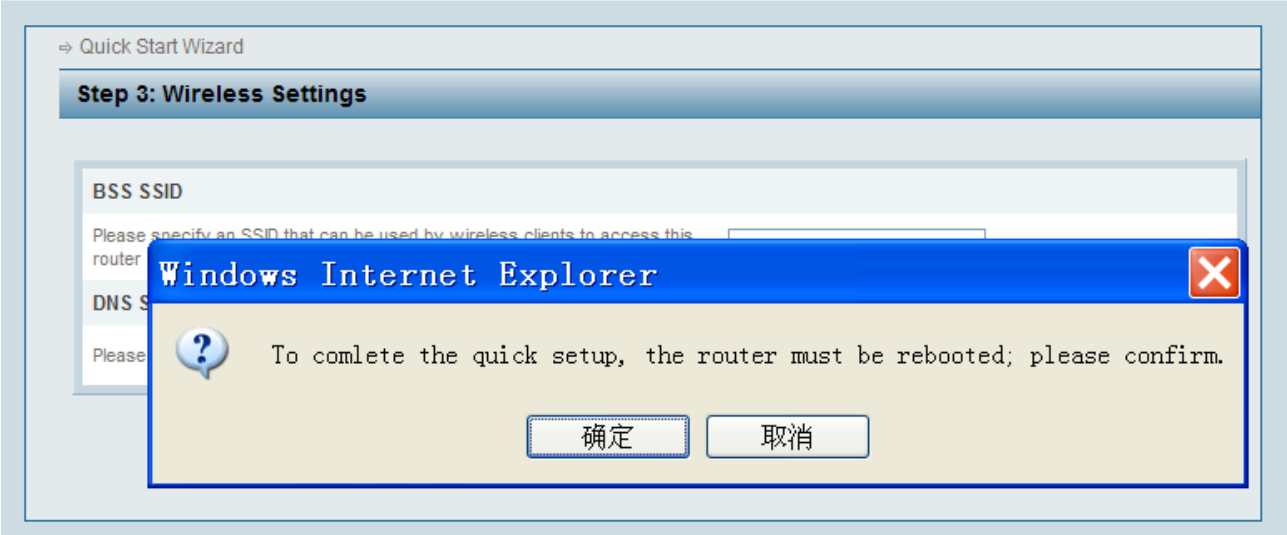


Figure 11 Configuring the portal node, step 4

After the last step of confirming the reboot is performed, the web interface would stop responding for a few seconds while the router reboots itself. Note that since the Quick Start changes the IP address of the Ethernet 0 port on the router, you may need to re-open the web interface using the new IP address if you were using Ethernet 0 to connect to the router.

Example Configuration 2: Point node

The following figures show how the example point node can be configured by answering the questions on each screen.

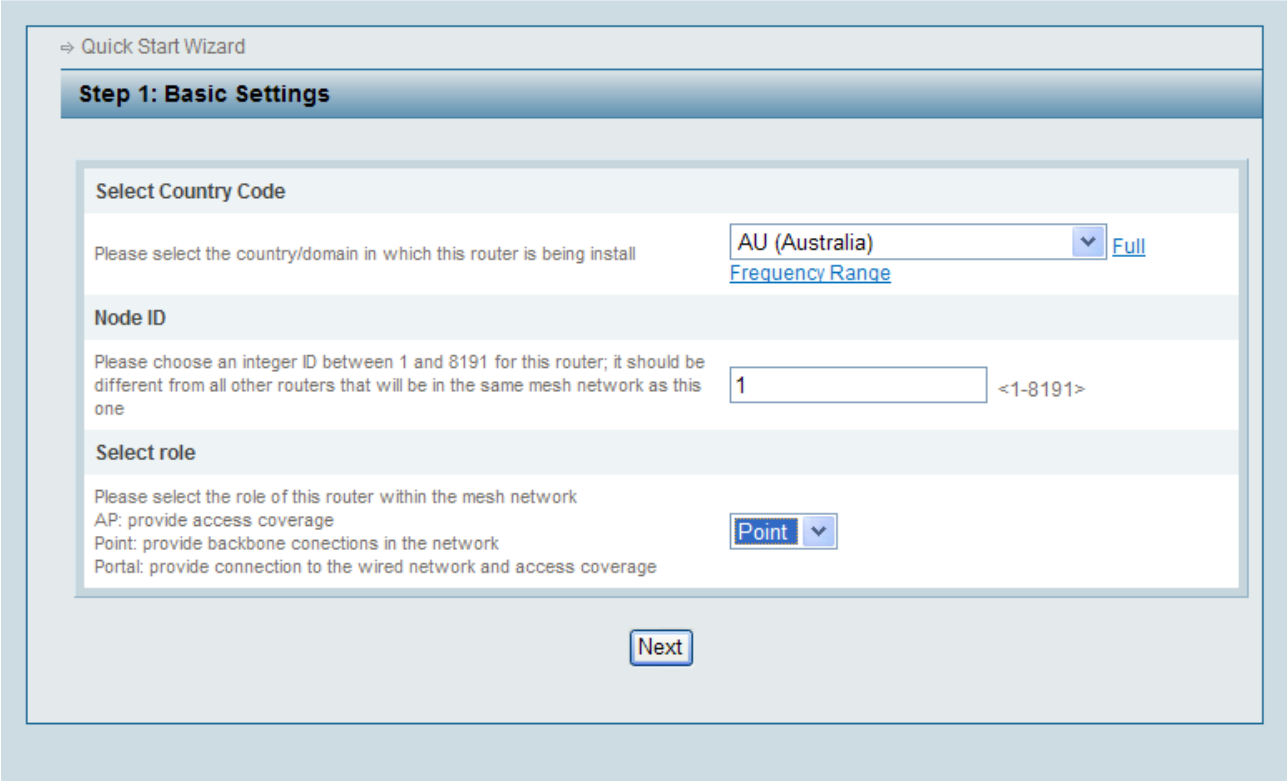


Figure 12 Configuring the point node, step 1

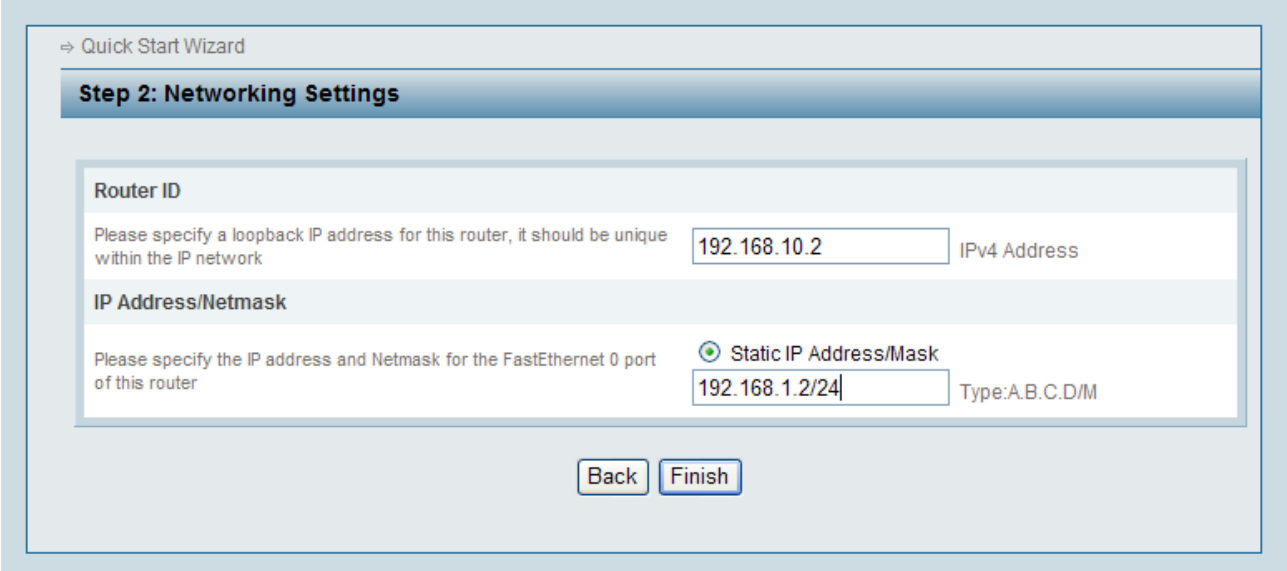


Figure 13 Configuring the point node, step 2

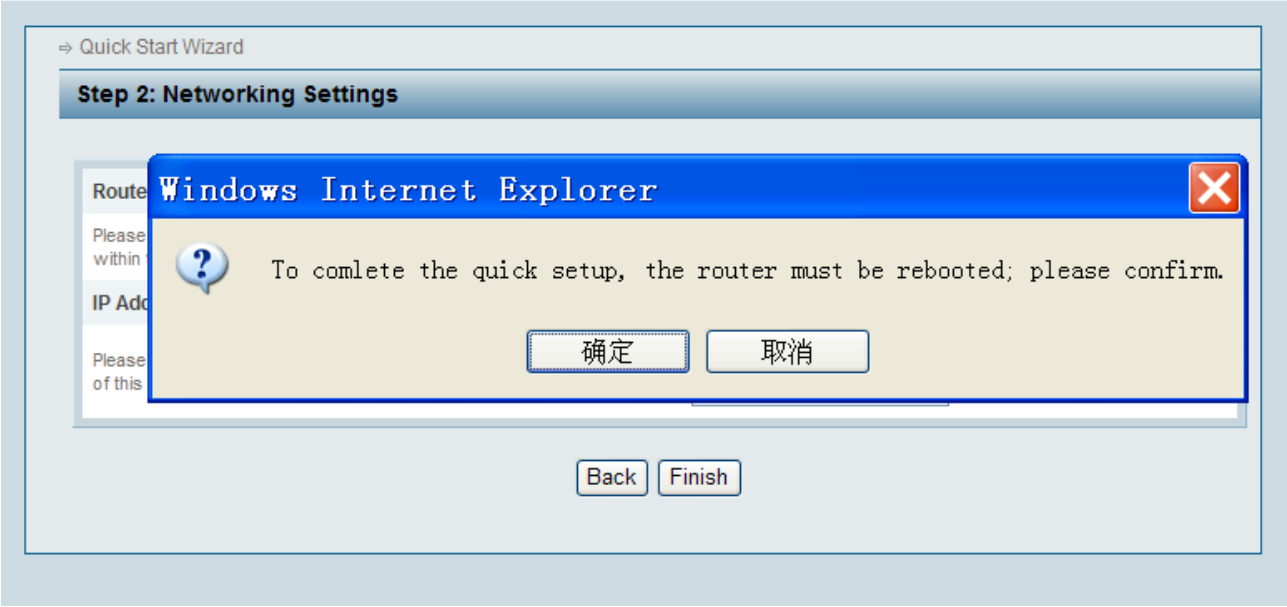


Figure 14 Configuring the point node, step 3

Example Configuration 3: AP node

The following figures show how the example AP node can be configured by answering the questions on each screen.

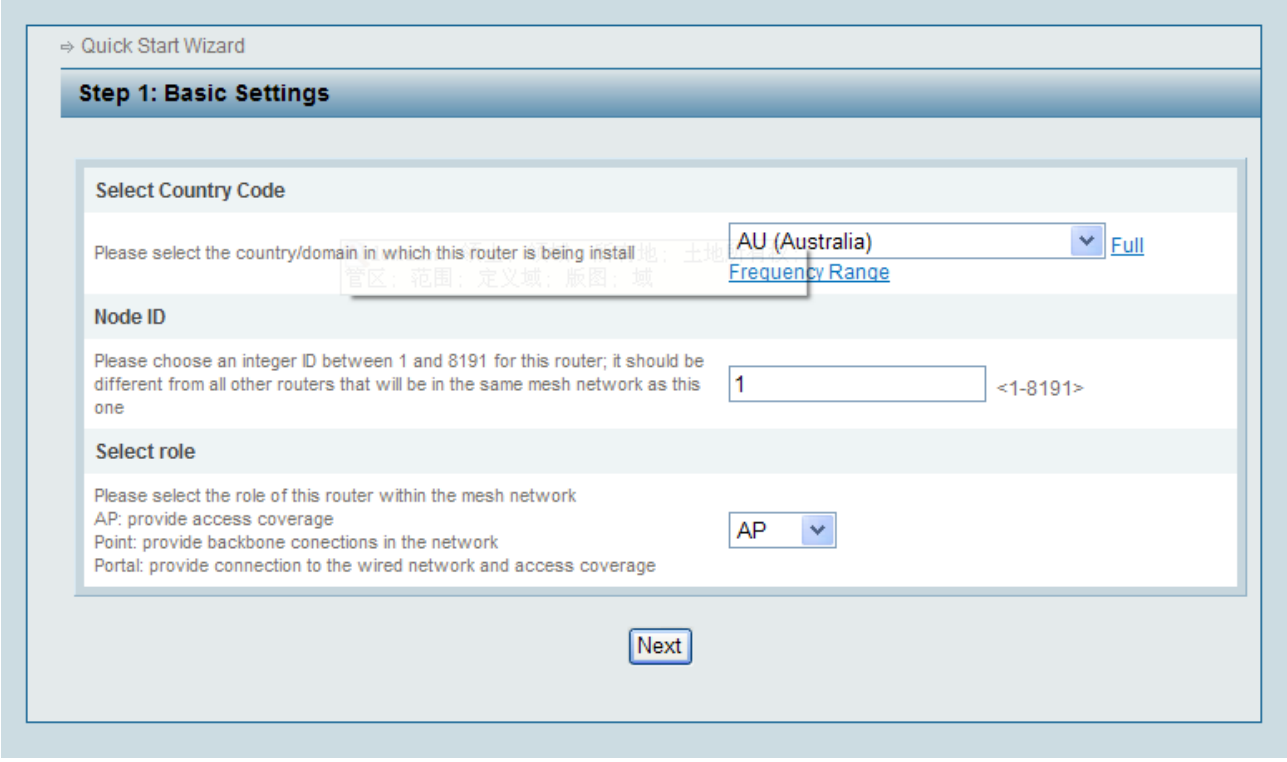


Figure 15 Configuring the AP node, step 1

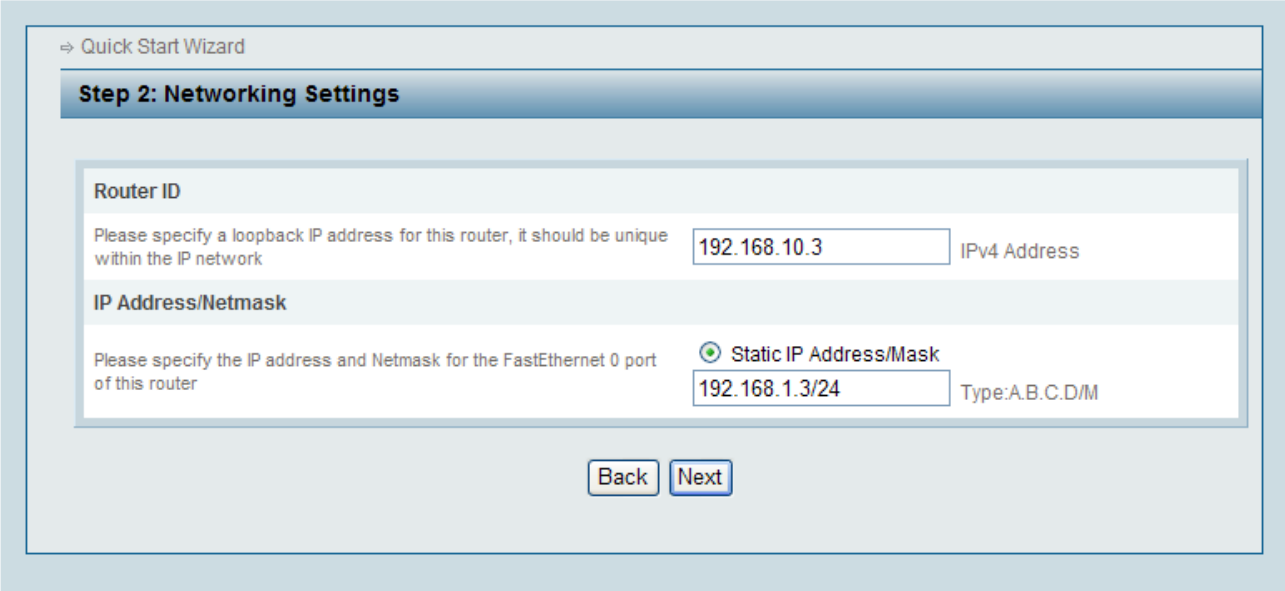


Figure 16 Configuring the AP node, step 2

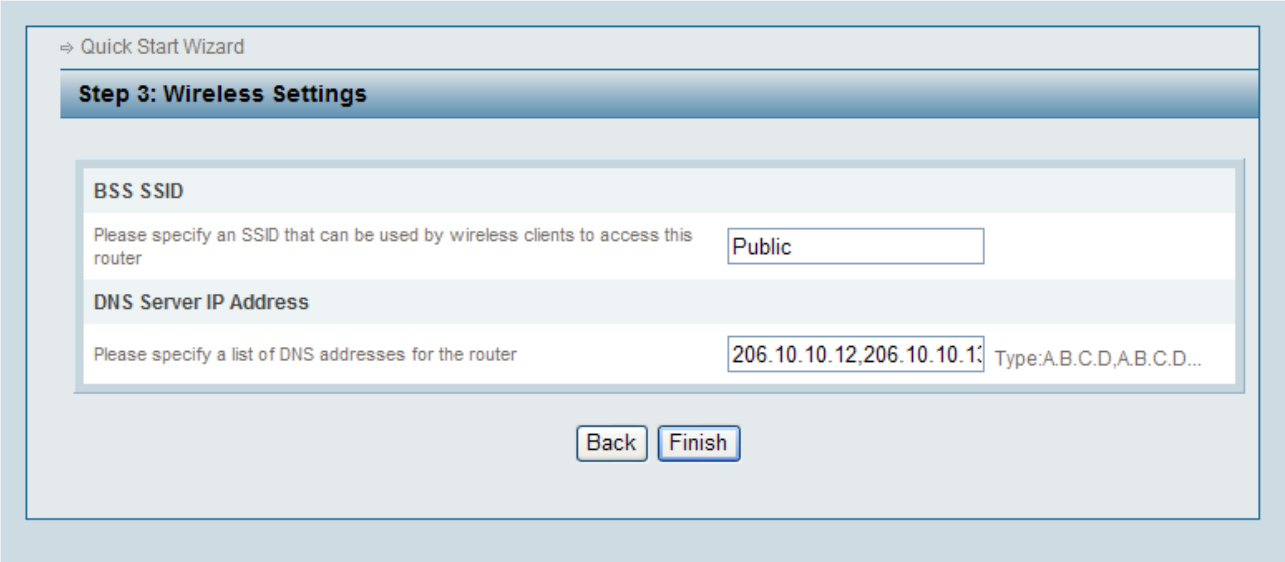


Figure 17 Configuring the AP node, step 3

Chapter 4 Global Settings

This chapter describes the settings that apply globally across a single DWR series router. It contains these topics:

- Accessing Global Settings
- Configuring Global Settings
- Performing Changes

Accessing Global Settings

Clicking on the menu item “Global Settings" leads the user to the global settings area; this area allows the user to retrieve and edit configuration settings which take effect globally across the DWR series router. An example screen is shown in Figure 18

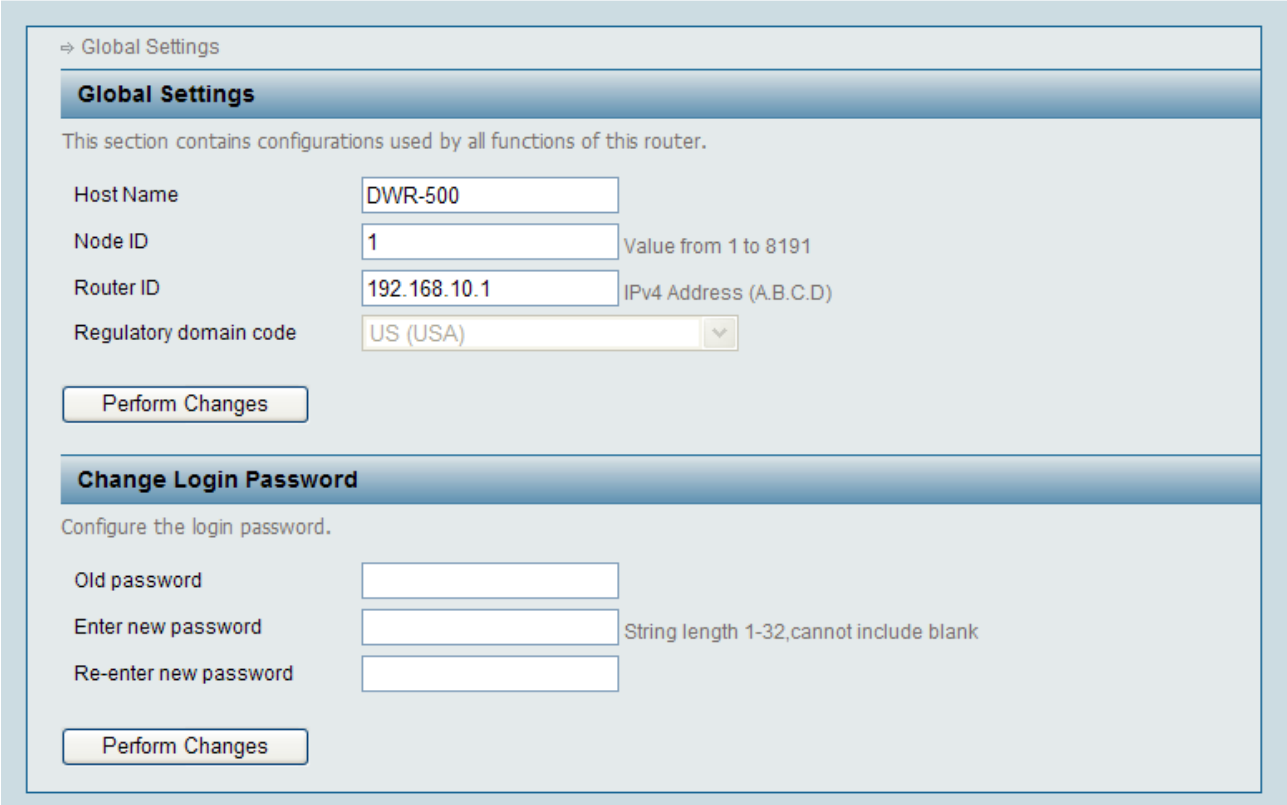


Figure 18 Global Configuration Screen

Frequency Regulations and Standards

Frequency Regulations and Standards

Abbreviation	Domain Code	2.4 GHz	4.9 GHz Frequency Band	4.9 GHz Channel	5 Ghz Frequency Band	5 Ghz Channel
NA	North America(USA,Canada)	Ch 1 ~ 11			5.15 ~ 5.35G 5.725 ~ 5.85G	36, 40, 44, 48, 52, 56, 60, 64; 149, 153, 157, 161,165
CN	China	Ch 1 ~ 13			5.725 ~ 5.850G	149, 153, 157, 161, 165
SG	Singapore	Ch 1 ~ 13			5.15 ~ 5.25G 5.725 ~ 5.85G	36, 40, 44, 48, 52, 56, 60, 64; 149, 153,157, 161, 165
TW	Taiwan	Ch 1 ~ 13			5.25 ~ 5.35G 5.725 ~ 5.825G	56, 60, 64; 149, 153, 157, 161
EU	Denmark, Germany, Iceland, Finland, Netherlands, Norway, Sweden, Poland, Slovenia, Luxembourg, South Africa, UK, Ireland	Ch 1 ~ 13			5.15 ~ 5.35G 5.47 ~ 5.725G	36, 40, 44, 48, 52, 56, 60, 64; 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
JP	Japan	Ch 1 ~ 14	5.04 ~ 5.08G 4.92 ~ 4.98G	8, 12, 16; 240, 244, 248, 252	5.15 ~ 5.35G	36, 40, 44, 48, 52, 56, 60, 64
AU	Australia	Ch 1 ~ 13			5.15 ~ 5.35G 5.725 ~ 5.825G	36, 40, 44, 48, 52, 56, 60, 64; 149, 153, 157, 161, 165
LA	Latin America	Ch 1 ~ 11			5.725 ~ 5.825G	149, 153, 157, 161
KR	Korea	Ch 1 ~ 13			5.725 ~ 5.825G	149, 153, 157, 161
IL	Isreal	Ch 1 ~ 13				
US	USA	Ch 1 ~ 11			5.15 ~ 5.35G 5.725 ~ 5.825G	36, 40, 44, 48, 52, 56, 60, 64; 149, 153, 157, 161, 165
PS	US Public Safety 4.9G	Ch 1 ~ 11	4.950 ~ 4.985G	246, 247, 248, 249, 250 ,251, 252, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309,310, 311, 312, 313, 314, 315, 316, 317, 318		

Global Settings Configuration

The global settings are described in Table 2.

Table 2 Global Setting Fields

Setting	Explanation	Default
Hostname	An identifier for a DWR series router containing up to 32 alphanumeric characters.	DWR series
Router ID	An IPv4 address that acts as the router's loopback address This address may be arbitrarily assigned as long as it is unique within a single network domain.	192.168.10.1
Node ID	An integer between 1 and 8191 that also identifies the router. It must be unique with in a single DWR series wireless mesh network. Changes to the Node ID would not take effect until the router is rebooted.	1
Regulatory domain code	Select the domain code; And click every channel link viewing the channel information when configuration. Regulatory domain code changes will be active when rebooted.	US(USA)
Old password	The current password of the router; this is needed in order to specify a new password	public
New password	The new password of the router; this password will not be shown on screen and should be entered twice for verification	N/A

Tip: One could simplify management by configuring all Router IDs in a single mesh network to be located in the same subnet, for example 192.168.10.1 ~ 192.168.10.20.

Performing Changes

After editing the values for the above fields, one may save the changes by clicking the "Perform Changes" button. WMI would display whether the setting was saved successfully, as shown in Figure 19.

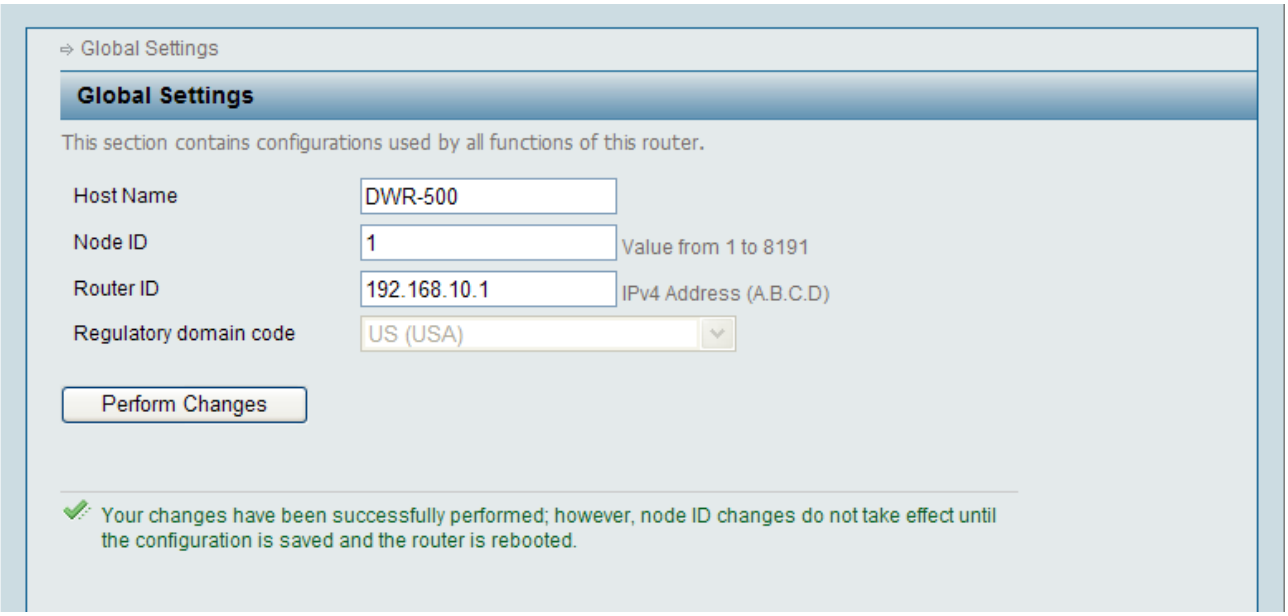


Figure 19 Successful change to global settings

Chapter 5 Configuring Router Interfaces

This chapter describes how Router Interfaces are configured using Web-based Management. It covers the following topics:

- Configuring Physical Interfaces
  - FastEthernet Interfaces
  - Dot11Radio Interfaces
- Configuring Logical WDS Interfaces
  - Create
  - Configure
  - Delete

Configuring Physical Interfaces

Each DWR-500 series router contains two physical 10/100M Ethernet interfaces1 and two physical Dot11Radio interfaces. This section describes how these interfaces are configured.

FastEthernet Interfaces

FastEthernet interfaces on the DWR series are used for connecting with Ethernet-only client devices or with a wired network. For more detailed information on how Ethernet interfaces may be used, please refer to the CLI Configuration Guide.

Accessing FastEthernet Configuration

Click the “Interface” button in the menu to expand the sub-menu for different types of router interfaces. Then, click the “FastEthernet” button in the sub-menu to enter the Ethernet interface configuration page. This page displays the physical Ethernet interfaces on the router. The basic configuration and the running status of the Ethernet interfaces are displayed in a list as shown in Figure 20.

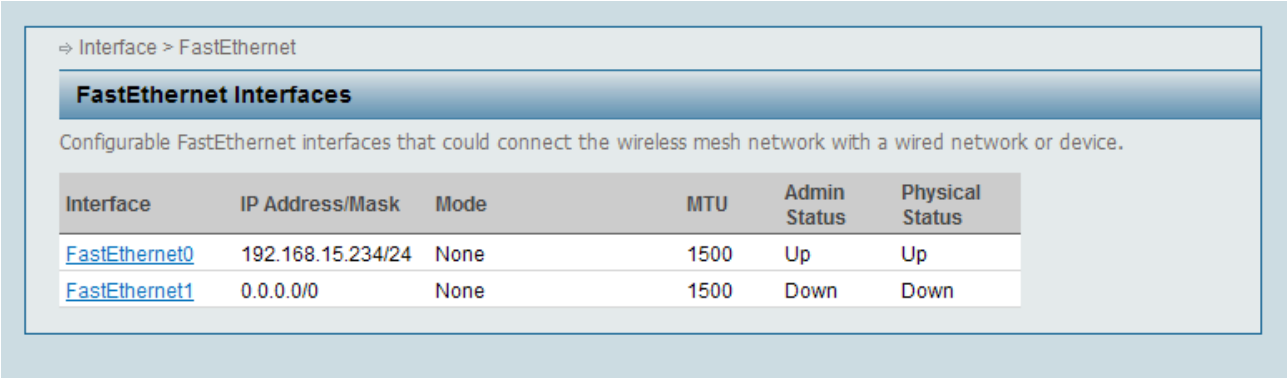


Figure 20 Fast Ethernet Interfaces Screen

Configuring FastEthernet Interface

To configure a particular Ethernet interface, click the interface name such as “FastEthernet0” in Figure to enter the edit page as shown in Figure 21.

[1] Some versions of the DWR series box may only have one Ethernet port enabled (FastEthernet 0)

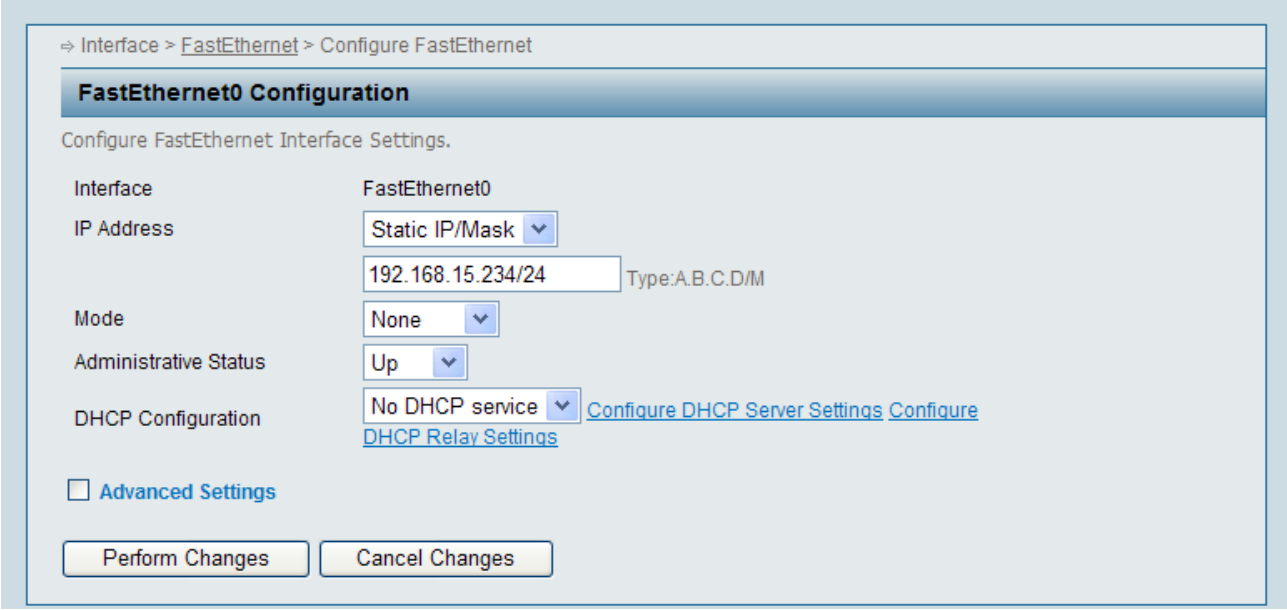


Figure 21 Fast Ethernet Interface Configuration Screen

Basic vs. Advanced Settings

Most configuration screens, including FastEthernet, have both basic settings and advanced settings. Basic settings are needed for the normal operation of the configured device, while advanced settings are used for fine-tuning by experienced administrators. Advanced settings should only be modified with extreme care, because an improper setting may prevent the configured device from functioning properly. For this reason, advanced settings are usually hidden from view. To see and configure the advanced settings, click the check box labeled “Advanced Settings” (see Figure 22).

Note: In general, advanced settings can and should be left at their default values.

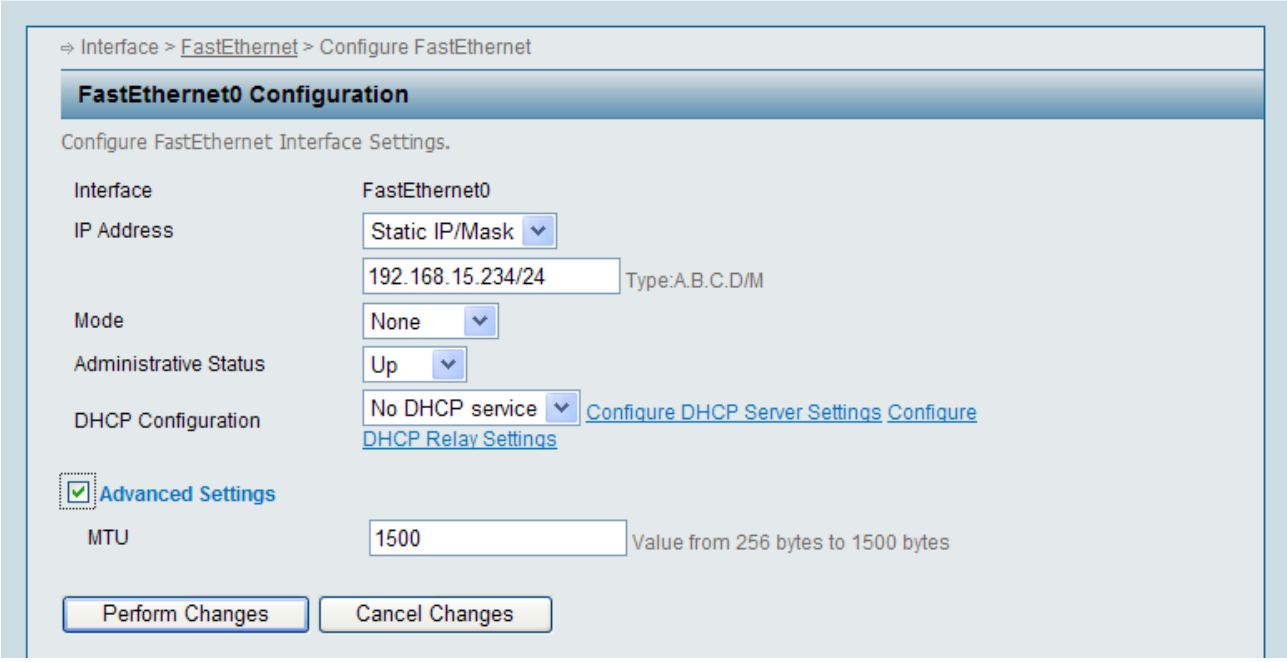


Figure 22 Configuring Advanced Settings

Table 3 below describes the settings for each FastEthernet interface.

Table 3 Fast Ethernet Configuration Fields

Setting	Explanation	Default
Basic Settings		
IP address/ netmask	Set the Ethernet interface IP address and netmask	N/A
Mode	Can be access , gateway or none Access is for connecting with Ethernet-only client devices, such as video cameras. Gateway is for connecting with internet-bound LAN routers. None is neither access nor gateway	Access Mode
Administrative Status	Can be up or down. If down, this interface would be inactive (shutdown). If up, this interface would be active, but it may not be physically working unless its physical status is also up.	Ethernet0:Up Ethernet1:Down
DHCP Pool	The type of DHCP Configuration to be used with this Ethernet port. No DHCP Service: Do not provide any DHCP service on this Ethernet port. DHCP Server: Run DHCP server on this Ethernet port, allowing connected devices to obtain IP addresses from an automatically-allocated or manually-configured DHCP pool (see next setting). DHCP server may be further configured in a separate module that is accessed via the “Configure DHCP Server Settings” link or the menu tree selection “Network Settings,” “DHCP,” “DHCP Server”. Please refer to Chapter 8 for more information. DHCP Relay: Run DHCP relay on this Ethernet port, allowing connected devices to obtain IP addresses from an external DHCP server. DHCP relay may be further configured in a separate module that is accessed via the “Configure DHCP Relay Settings” link or the menu tree selection “Network Settings,” “DHCP,” “DHCP Relay”. Please refer to Chapter 8 for more information.	Automatic
DHCP Pool	An automatic or manually-configured DHCP Pool; please refer to Chapter 8 for more information. Automatic DHCP Pools are allocated by the router software so no additional configuration is needed. ***Using an automatic DHCP Pool overrides any static IP configuration.***	Automatic
Advanced Settings		
MTU	Maximum transmission unit in bytes; controls how layer-3 packets would be fragmented when they are sent through this interface. Range: 256-1500 ***Use with extreme caution.***	1500

Saving FastEthernet Configuration

To save the configuration after editing the above settings, click the “Perform Changes” button. The browser will return to the Ethernet interface list after the configuration is successfully performed.

If the user input contains an error, the browser will report it to the user in one of two ways. The errors that could be detected without sending the configuration information to the router are shown in a pop-up dialog box. An example is shown in Figure 23

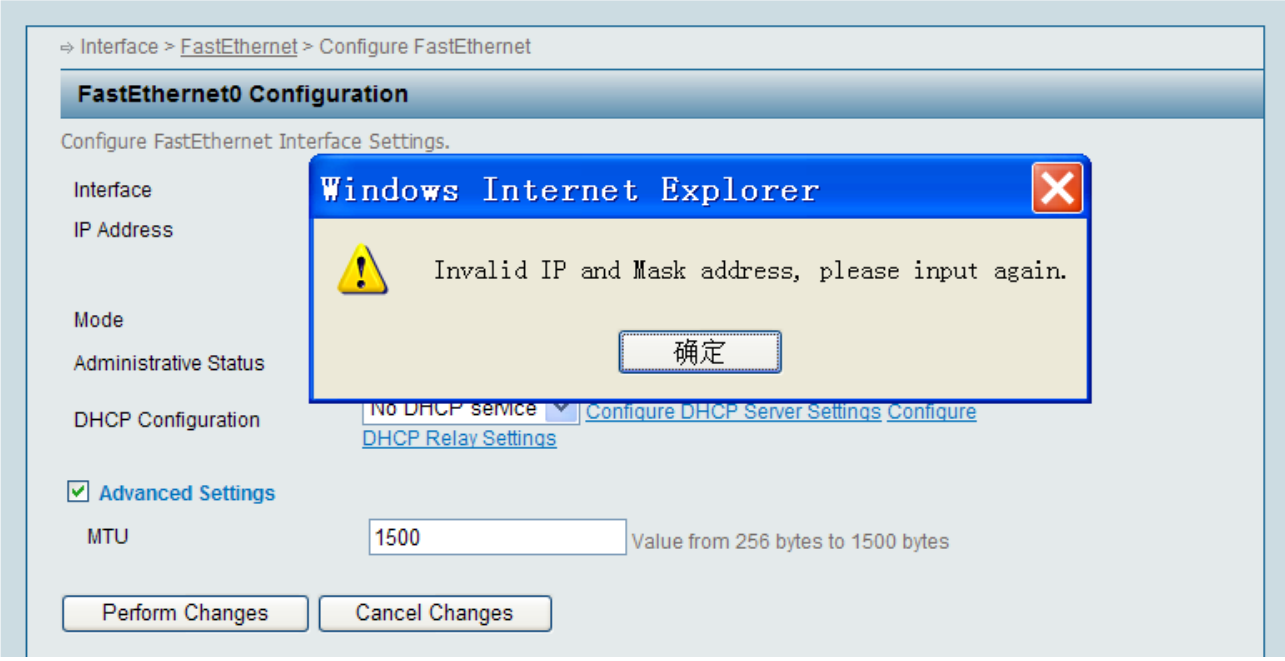


Figure 23 Error message displayed in pop-up dialog box

In the situation that errors cannot be detected until the configuration information is sent re-display the configuration page with the appropriate error message. An example error message can be found in Figure 24. Note: in this error page the advanced settings are automatically shown because the error message could be related to some of them.

To discard any changes, click the “Cancel Changes” button.

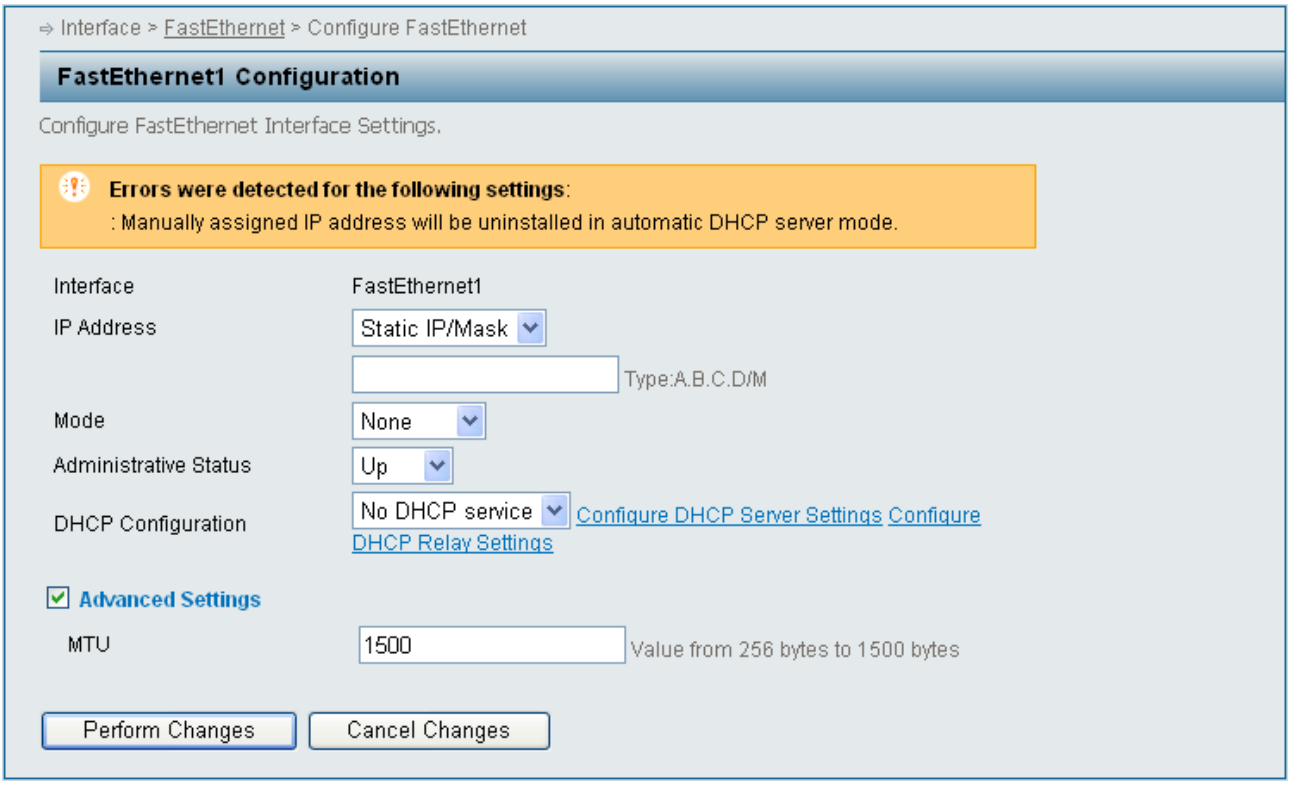


Figure 24 Error message displayed in the next page

Dot11Radio Interfaces

Dot11Radio interfaces on the DWR series are used for connecting with 802.11-compatible client devices or with other DWR series routers. For more detailed information on how Radio interfaces may be used, please refer to the CLI Configuration Guide.

Accessing Dot11Radio Configuration

Click the “Dot11Radio” item in the “Interface” sub-menu to enter the Radio interface configuration page. The resulting page displays the router’s physical radio interfaces in a list, as shown in Figure 25.

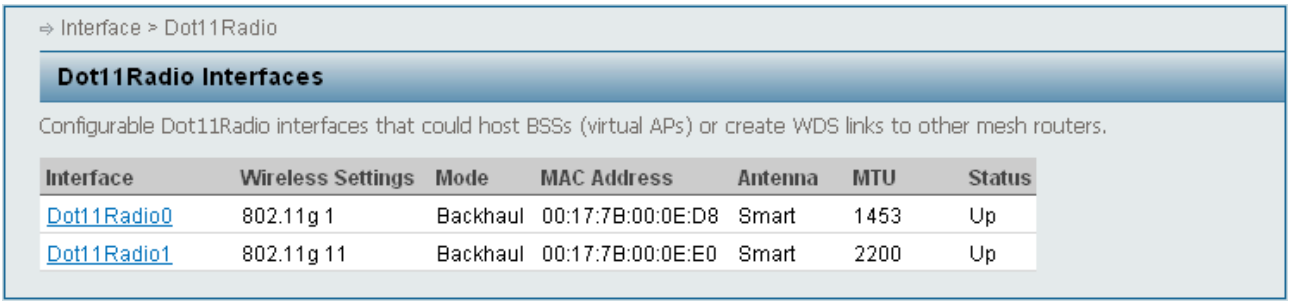


Figure 25 Dot11Radio Interfaces Screen

Configuring Dot11Radio Interface

To view or change the configuration for a particular radio, click the name of the Radio interface (i.e. “Dot11Radio0” in Figure 25). The resulting page displays the detailed configuration settings and allows them to be changed. Figure 26 shows the page with the advanced settings shown.

Note: Mode **Access** is configured under interface **dot11radio 0** by default, and Radio 1 under backhaul mode.

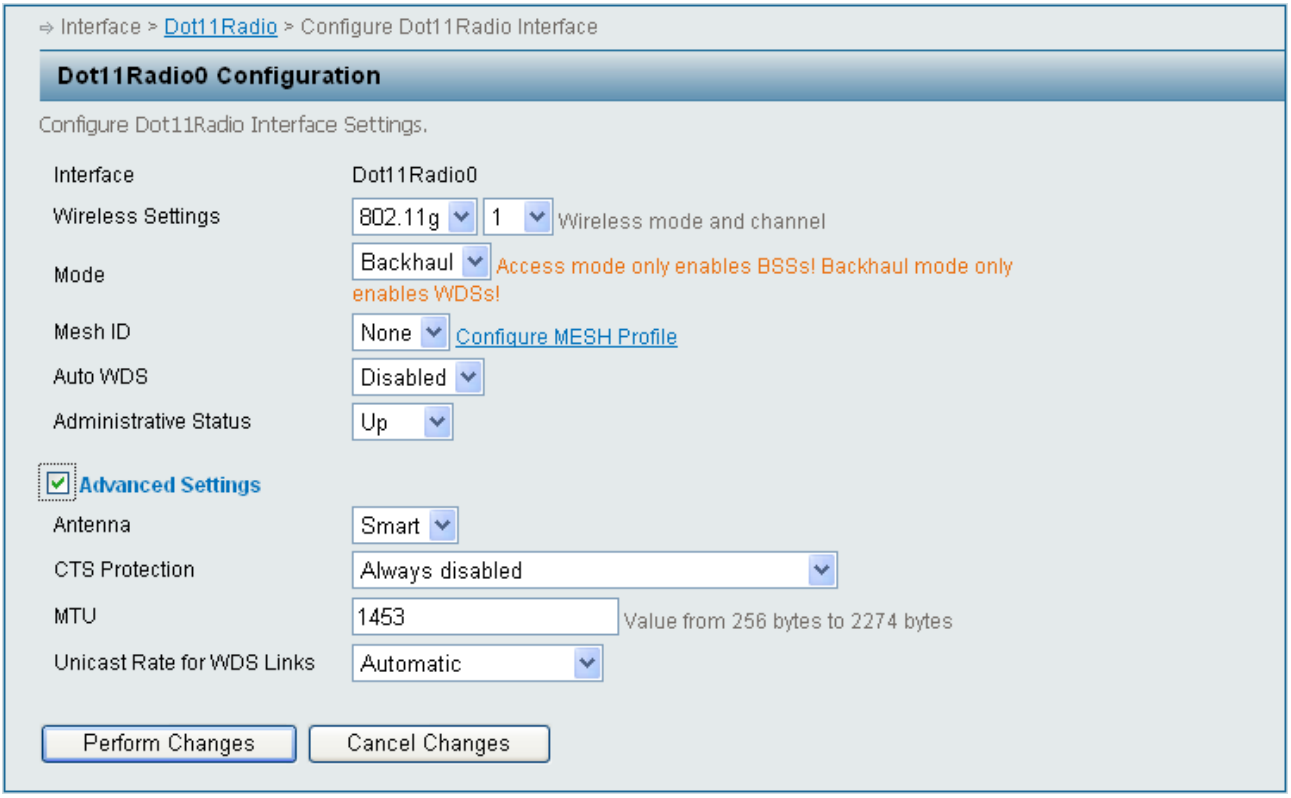


Figure 26 Dot11Radio Interface Configuration Screen

Table 4 describes the settings for each Dot11Radio interface. Detailed description of each parameter could be found in the CLI Configuration Guide.

Table 4 Dot11Radio Configuration Fields

Setting	Explanation	Default
Basic Settings		
Wireless Settings	The 802.11 mode (a/g), and channel	802.11g, 1 for Dot11Radio0 802.11a, 36 for Dot1Radio1
Mode	Can be access or backhaul[2]. Access mode allows BSS (virtual APs) to be configured on this radio interface; BSSs allow 802.11 client devices to connect to (associate with) this router. Backhaul mode allows WDS interfaces to be configured on this radio interface; WDS interfaces allow this router to form backhaul wireless links with other DWR series routers.	Access for Dot11Radio0 Backhaul for Dot11Radio1
Auto WDS	Can be enabled or disabled; this setting only applies to (and is only displayed in) backhaul mode.	Enabled for Dot11Radio1

[2] A third mode, client, can be set by the CLI but is not supported by the WMI.

	Enabling auto WDS allows routers to use this radio for automatic neighbor discovery and link establishment. Established links become auto WDS interfaces for this radio interface. When auto WDS is enabled on a radio, one cannot configure manual WDS interfaces on the same radio (see next section on manual WDS interface configuration) Disabling auto WDS allows users to configure manual WDS on this radio interface (see next section on manual WDS interface configuration)	
Maximum Auto WDS	Set the maximum auto wds numbers that established under radio interface. Can be 1-6; this setting only applies for backhaul mode with auto WDS enabled. Sets the maximum number of auto WDS neighbors that could be established automatically on this radio interface.	6
Mesh ID	Selects the Mesh ID for this Radio, which determines which mesh network this backhaul radio would participate in. All wireless routers in a single backhaul network should use the same mesh ID. The Mesh IDs are defined in mesh profiles; you may configure mesh profiles by clicking the "Configure Mesh Profile" link or via the menu item "Network Settings" > "Mesh Profiles" For detailed information about mesh profiles or mesh IDs, please refer to the CLI Configuration Guide.	N/A
Administrative Status	Can be up or down. If down, this interface would be inactive (shutdown). If up, this interface would be active, but it may not be physically working unless its physical status is also up.	Up
Advanced Settings		
Antenna	Can be Smart, 1, or 2. Smart: automatically choose one of the two antennas (default setting). 1: Always use antenna 1 2: Always use antenna 2 ***This parameter is usually set at deployment time and rarely needs to change.***	For indoor models: Smart For outdoor models: 1
CTS Protection	Enable/disable CTS protection for handling of a mix of 802.11b and g clients. For more information, refer to the CLI Configuration Guide. ***This parameter is usually set at deployment time and rarely needs to change***	Disabled
MTU	Maximum transmission unit; controls how layer-3 packets would be fragmented when they are sent through this interface ***Use with extreme caution.***	1500

Unicast Rate for WDS Links	Can be Automatic or a specific rate. Automatic setting allows transmission rate of WDS interfaces to be automatically determined. Specific rate setting forces all WDS interfaces on this radio to use the selected rate.	Automatic

Saving Dot11Radio Configuration

To save the configuration after editing the above settings, click the “Save Settings” button. The browser will return to the higher-level page after the configuration is successfully saved. To discard any changes and return to the previous page, click the “Cancel Changes” button.

Configuring WDS Interfaces

Wireless Distribution System (WDS) is the fundamental technology used by DWR series to establish backhaul wireless links with other mesh routers. Unlike physical interfaces, WDS is a logical, point-to-point interface that may be dynamically created or deleted. WDS interfaces may also be automatically discovered and established by the built-in software intelligence of the mesh router. The WDS interfaces configured by the user are named “Manual WDS Interfaces” while WDS interfaces established automatically are named “Auto WDS Interfaces”. For more background information on WDS interfaces, please refer to the CLI Configuration Guide.

This chapter describes how manual WDS interfaces can be created, deleted, and configured using the Web-based Management Interface.

Accessing WDS interface Configuration

Click “Interface”->”Dot11Radio”->”WDS” in the main menu to enter the WDS interface configuration page, which contains the configuration information and state of WDS interfaces (see Figure 27)

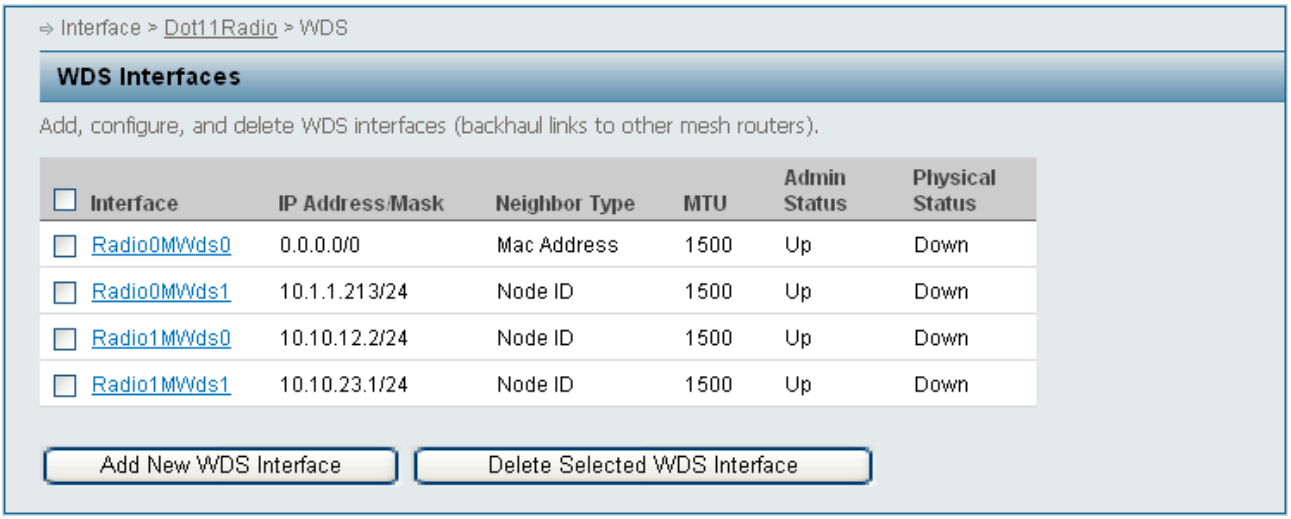


Figure 27 WDS Interface Configuration Page

From this page, one may create a manual WDS interface, configure an existing manual WDS interface, or delete a manual WDS interface.

Note: The WDS Configuration page also lists the Auto WDS interfaces created by the router. Because Auto WDS interfaces are automatically managed by the router's RF Management feature, users are not allowed to edit or delete Auto WDS interfaces. For more information about Auto WDS and RF Management, please refer to the CLI Configuration Guide.

Creating a New Manual WDS Interface

To add a manual WDS interface, click the "Add New WDS Interface" button in the WDS Interface Configuration Page. The Add WDS Interface page appears (see Figure 28 with the advanced settings shown)

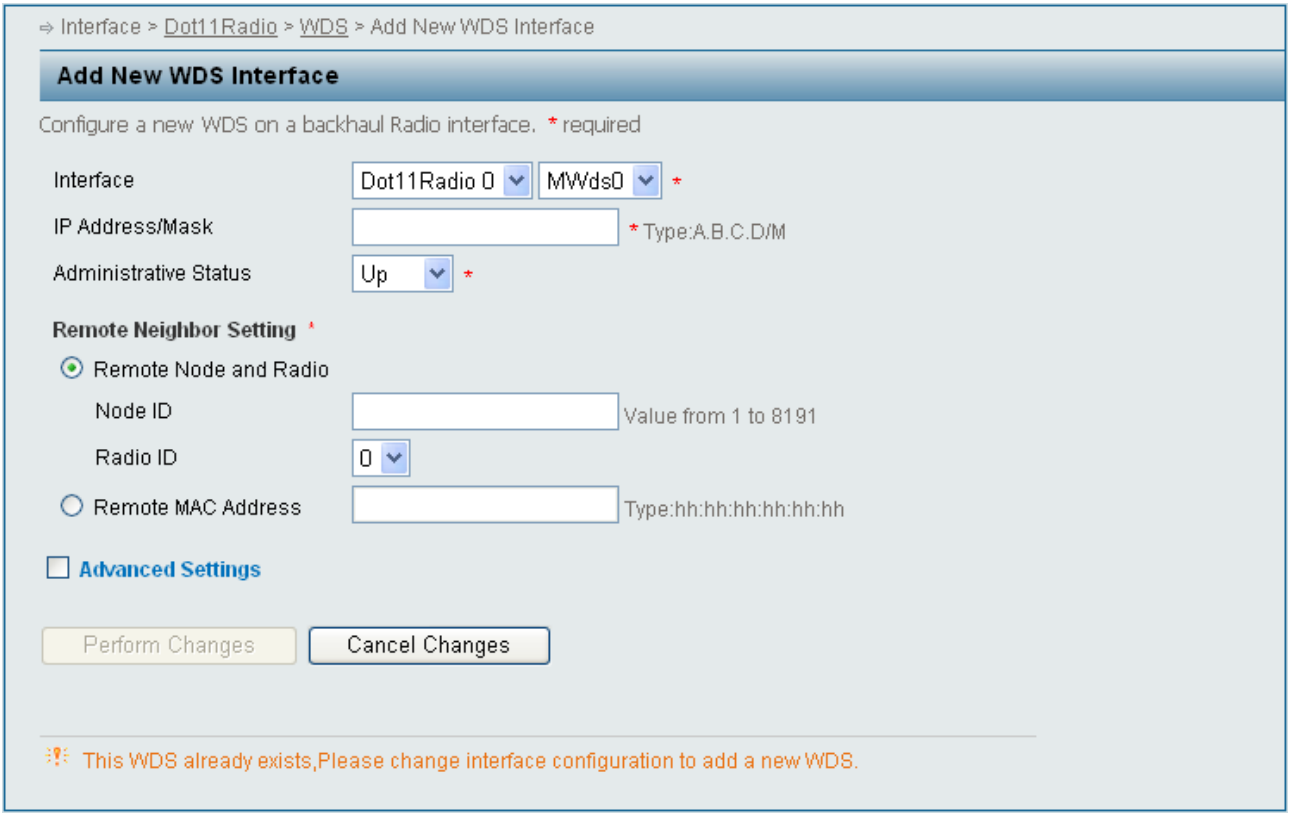


Figure 28 Add Manual WDS Interface Page

Table 5 describes the new WDS interface settings in this page.

Table 5 New WDS Interface Configuration Fields

Setting	Explanation	Default
	Basic Settings	
Interface	The name of the interface in the form Radio X MWds Y, where X represents the index of the Radio interface that will host this WDS interface and Y denotes the sub-index of the WDS interface. Each Dot11Radio interface could support six WDS interfaces. ***One may not use a WDS name that duplicates an existing WDS interface, and the name may not be changed after creation.***	Dot11Radio0 MWds0
IP Address/ Mask	The IP address and the length of the netmask for a WDS interface; typical mask lengths are 24 (mask 255.255.255.0), 16 (mask 255.255.0.0), and 8 (mask 255.0.0.0)	N/A

	Example: 10.5.6.2/24 ***This field is required.***	
Administrative Status	Can be up or down. If down, this interface would be inactive (shutdown). If up, this interface would be active, but it may not be physically working unless the physical status is also up.	Up
Remote Node/Radio and Remote MAC Address	Information about the remote WDS interface in the logic link. May be specified with the combination of remote node id and radio id, or with a single remote MAC address. ***This field is required, please see Chapter 11***	Node ID and Radio ID
Remote Node ID/Radio ID	The Radio interface index (0 or 1) and Node ID (1-8191) of the remote neighbor	Radio ID: 0
Remote MAC Address	The MAC Address of the remote neighbor	N/A

Advanced Settings		
MTU	Maximum transmission unit; controls how layer-3 packets would be fragmented when they are sent through this interface ***This setting rarely needs to be changed and should be modified with extreme caution.***	1500
QoS Class	The QoS Class for which configuration would be applied to this WDS interface. QoS Classes are configured in a separate module that could be accessed via the link “Configure QoS Classes” or via the menu tree selection “Quality of Service” ***For more information, please see Chapter 11***	None

Notes:

- Because WDS is point-to-point, the interfaces at the two ends of a WDS link should have IP addresses from the same subnet.
- To complete the addition of the new interface, click “Perform Changes”
- To discard the new interface, click “Cancel Changes”
- After configuration, the user is brought back to the page with the WDS Interfaces List.

Configuring an existing Manual WDS Interface

Click on the name of an existing WDS interface (for example WDS interface “Radio0Mwds0”) in the WDS Interface Configuration page (Figure 27) to change the WDS Interface configuration. The resulting page is depicted in Figure 29. This page allows the viewing and editing of all WDS interfaces configuration information described in the previous section except for the interface name.

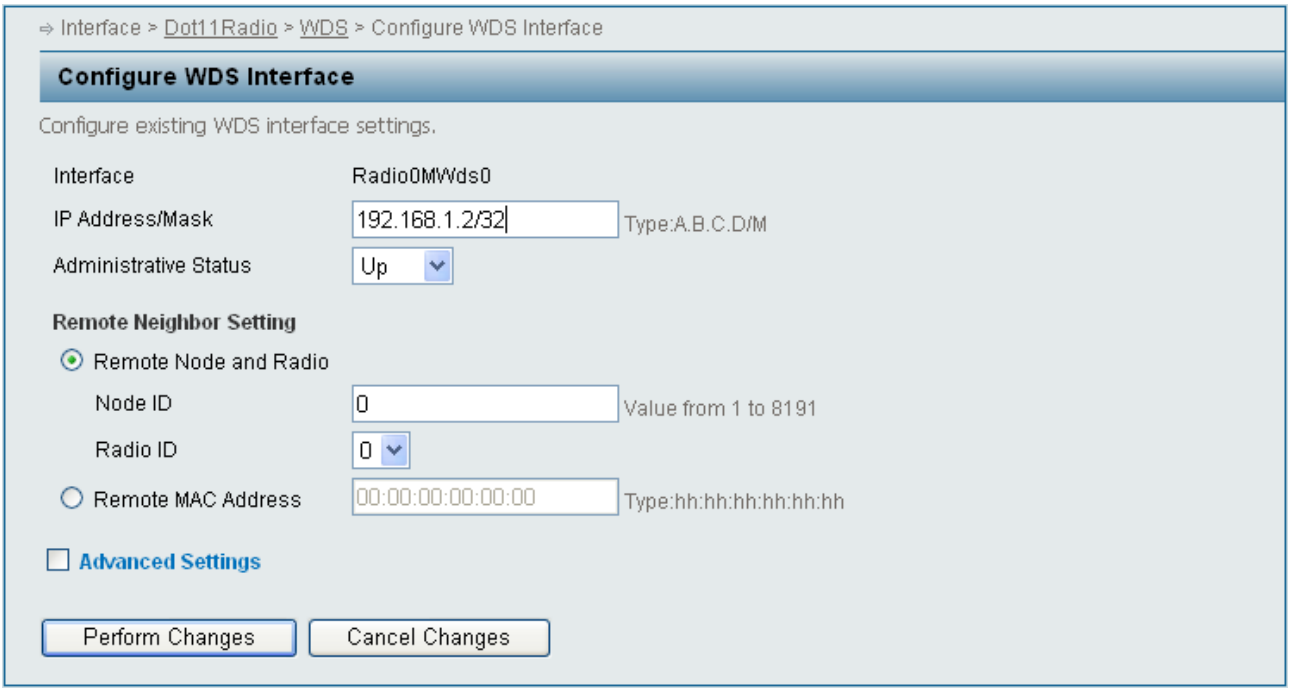


Figure 29 Manual WDS Interface Configuration Page

Deleting Manual WDS Interfaces

To delete one or more WDS Interfaces, check the boxes beside their names and click the "Delete" button. A confirmation dialog box would appear. Click "Yes" to confirm the delete, or click "No" to cancel (see Figure 30)

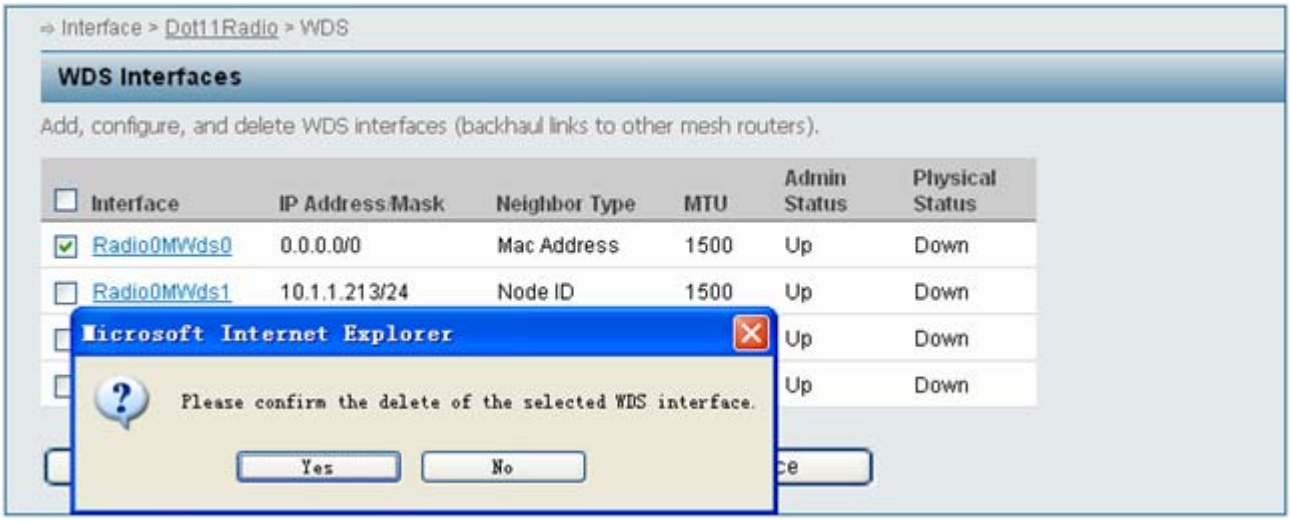


Figure 30 Deleting Manual WDS Interface

Chapter 6 BSS Configuration

Configuring 802.11 Basic Service Set (BSS) allows DWR series routers to provide Access Point (AP) for 802.11 compatible wireless clients. Each radio of DWR series routers, when configured for access mode, may support up to 4 distinct BSSs, each with its own configuration profile. For more background information on BSS, please refer to the CLI Configuration Guide.

Accessing BSS Configuration

Click “Interface” > “Dot11Radio” > “BSS” listed in the main menu tree. The resulting page shows the configuration and status of all BSSs on the router (see Figure 31).

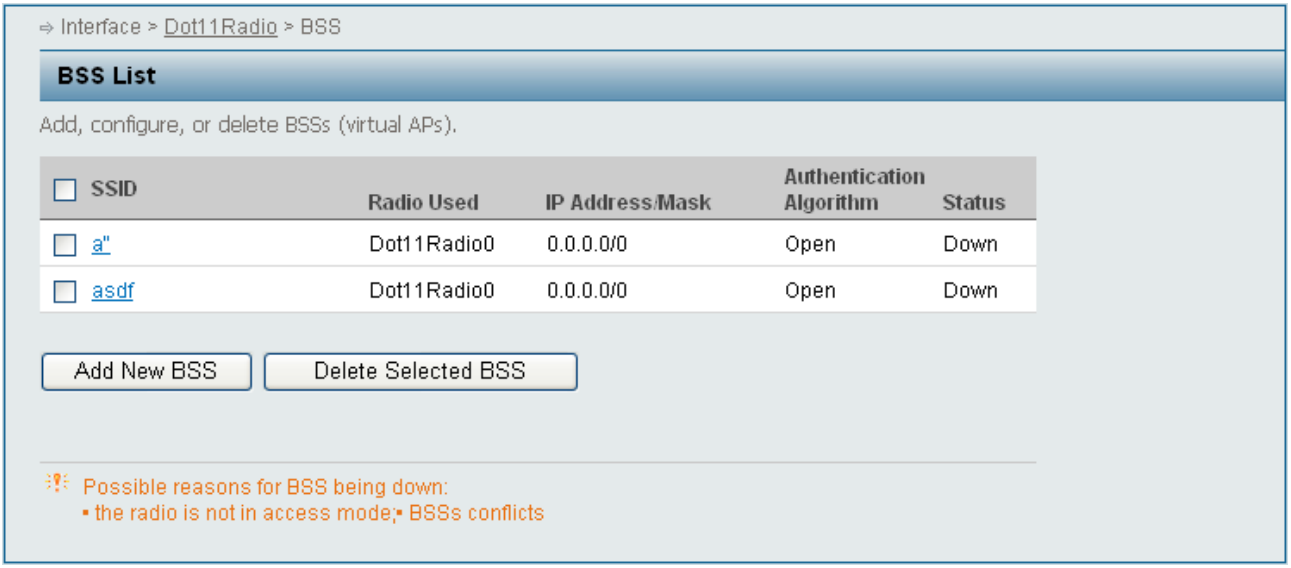


Figure 31 BSS List Page

In this page, users could create a new BSS as well as configure or delete an existing BSS.

Creating a New BSS

To create a new BSS, click the “Add New BSS” button in the BSS list page. The “Add New BSS” page appears (Figure 32)

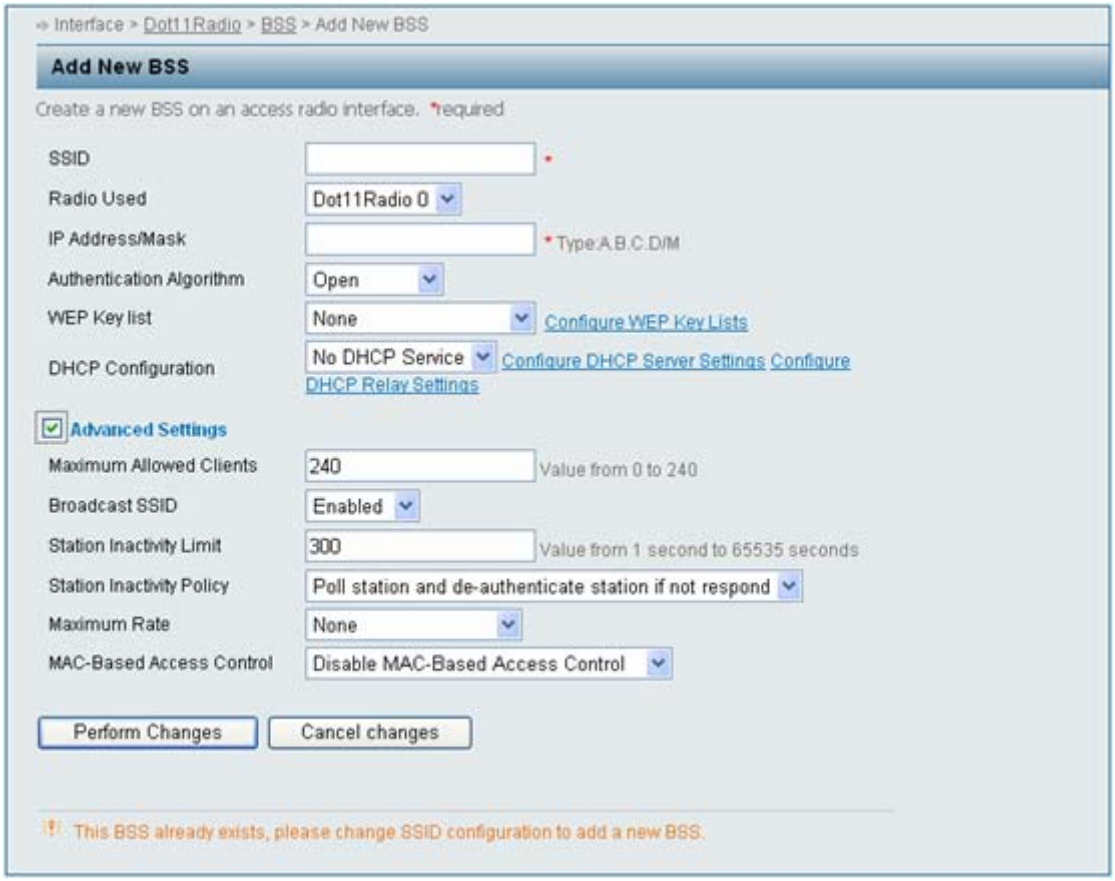


Figure 32 Add New BSS Page

Table 6 describes the BSS settings in this page.

Table 6 New BSS Configuration Fields

Setting	Explanation	Default
	Basic Settings	
SSID	The 802.11 SSID for this BSS, a string of up to 32 alphanumeric characters. Example: public Each Radio can support up to 4 BSS	N/A
Radio Used	The physical Radio interface that will host this BSS.	Dot11Radio0
IP Address/ Mask	The Static IP address and netmask for this BSS; typical mask lengths are 24 (mask 255.255.255.0), 16 (mask 255.255.0.0), and 8 (mask 255.0.0.0) Example: 192.168.20.1/24 If BSS uses DHCP server and access the IP address automatically, DHCP server will allocate an IP address to this BSS automatically without entering of BSS IP address/mask. Currently there are maximum 4 BSS are supported to access IP address automatically. If BSS uses DHCP server and also uses manual address pool, it will be OK that the BSS IP address/mask is within this network address except the broadcasting address, For example：	N/A

	Address pool network address is 10.1.1.0/24.BSS IP address is configured to 10.1.1.1/24-10.1.1.254/24.	
Authentication Algorithm	"Open" or "Open wep" or "Shared-key" algorithm for authenticating client associations "Open" means no authentication needed, however a WEP key list may still be used for data encryption "Open wep" and "Shared-key" requires a WEP key and a default WEP key list, to be exchanged during connection; WEP key list needs to be configured under administrative status.	Open
WEP Key List	The WEP key List to be used with this BSS, or None if not using a WEP Key. The WEP key lists are configured in a separate module which could be accessed through the link "Configure WEP Key Lists" or the menu tree selection "Security" and "WEP Key Lists"; see chapter 10, Security Configuration, for more information. DWR series routers support at most 16 key lists. Each WEP Key Lists consist of four WEP Keys ***A WEP Key List is required to use "Shared-Key" authentication***	None
Default WEP Key	Specify which key in the WEP Key List is the default key. ***This setting is only applicable when a WEP Key List is selected.***	1
DHCP Configuration	The type of DHCP Configuration to be used with this BSS. No DHCP Service: Do not provide any DHCP service on this BSS. DHCP Server: Run DHCP server on this BSS, allowing associated clients to obtain IP addresses from an automatically-allocated or manually-configured DHCP pool (see next setting). DHCP server may be further configured in a separate module that is accessed via the "Configure DHCP Server Settings" link or the menu tree selection "Network Settings," "DHCP," "DHCP Server. Please refer to Chapter 8 for more information. DHCP Relay: Run DHCP relay on this BSS, allowing associated clients to obtain IP addresses from an external DHCP server. DHCP relay may be further configured in a separate module that is accessed via the "Configure DHCP Relay Settings" link or the menu tree selection "Network Settings," "DHCP," "DHCP Relay. Please refer to Chapter 8 for more information.	No DHCP Service
DHCP Pool	An automatic or manually-configured DHCP Pool; please refer to Chapter 8 for more information. Using an automatic DHCP Pool overrides any static IP configuration and manual DHCP Address pool. Using a manual DHCP Pool overrides any static IP configuration and the automatic DHCP Address pool.	

Advanced Settings		
Maximum Allowed Clients	The maximum number (0-240) of 802.11 stations or clients that would be allowed to associate with this BSS at any one time.	240
Broadcast SSID	Whether to allow SSID of this BSS to be broadcasted to the air periodically. If enabled, clients will be able to discover the SSID of this BSS through scanning. If disabled, clients will not be able to discover the SSID and must be pre-configured with the SSID to associate with this BSS.	Enabled
The Maximum Transmission Rate	The maximum transmission rate when using rate control algorism 802.11a:6,9,12,18,24,36,48,54Mbps 802.11b:1,2,5.5,11Mbps 802.11g:1,2,5,5,6,9,11,12,18,24,36,48,54Mbps For example: When using rate control, the default rate will be adjusted between 6M and 54Mbps under A mode，if configured the max-rate as 360, the rate control will be adjusted between 6M and 36Mbps	None
Station Inactivity Limit	The maximum amount of time (1-65535 seconds) a station/ (client) is allowed to be inactive before the inactivity policy takes effect.	300
Station Inactivity Policy	The action taken when a particular station (client) becomes inactive for a very long time (see Station Inactivity Limit) Policy 0: Use poll frame to detect station's activity. Before timeout expires, system will send a request control message when there is no data transmission. If it doesn't receive the reply from the remote end, the router will remove this station entry. Use election frame to detect the client activities. This strategy detect without data transmission activity. Before the client expired, the system will send a request control information, if no client response received, it will remove the this client access. Policy 1: When there is no data transmission of Client, the system will delete this client directly from the client list	0
MAC Authentication Type	Determines how the BSS will use MAC addresses to authenticate stations or clients Do not use MAC authentication: allow all client access (default) Allow only MACS in accept list: BSS will only allow the MAC addresses specified in the accept list, the other MAC are all denied. Allow all MACs not in deny list: BSS will deny the MAC address access specified in MAC list, but allows other MAC access.	Do not use MAC address access
MAC Access Control List	The MAC List to be used with Access Control. The MAC Lists are configured in a separate module which could be accessed through the link "Configure MAC Lists" or the menu tree selection "Security" and "MAC Lists"; see chapter 10, Security Configuration, for more information.	N/A

	MAC access control lists only applies to MAC authentication. DWR series routers support up to eight MAC access control lists, and each list can be configured with up to 256 MAC addresses.	

Configuring an existing BSS

To configure an existing BSS, click its SSID to enter the BSS configuration page. (Figure 33) This page allows the viewing and modification of all settings for the existing BSS.

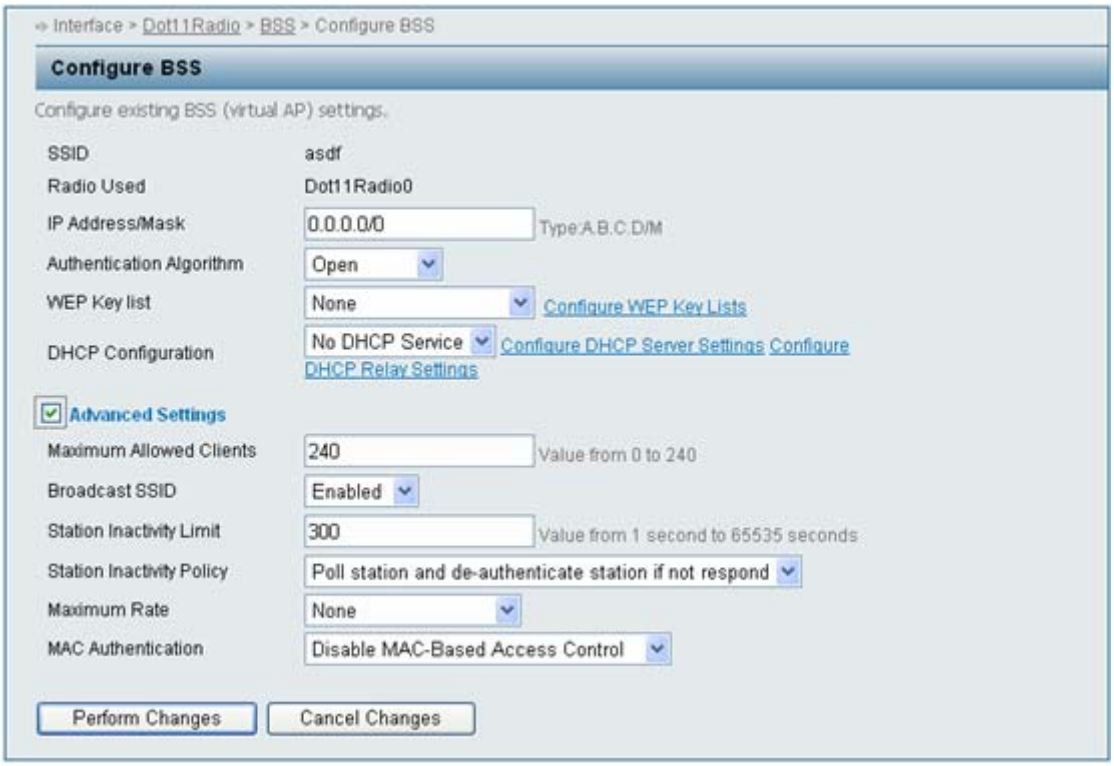


Figure 33 Establishing BSS Configuration Page

All settings are the same as those in the “Add New BSS” page, except that the SSID and the radio used settings cannot be changed.

Deleting a BSS

To delete the existing BSSs, check the boxes to be deleted beside each BSS and click the “Delete” button. A dialog will appear to ask for confirmation; click “Yes” to confirm and “No” to Cancel.

Chapter 7 Network Setting

Configuring Routing

Routing is the fundamental service provided by all routers. It is responsible for deciding where data should be sent and when it is received. There are two basic types of routing: static and dynamic. Static routes are user-configured that do not change with the network topology. Dynamic routes are automatically discovered by routing protocols according to the latest network topology. For more information about routing, please consult the CLI Configuration Guide.

Routing Table Configuration

The Routing Table is the information database used by a mesh router to track the topology of the network and to determine how each data packet would be forwarded. This chapter describes how routing table may be viewed using the DWR series' Web-based Management Interface and how static routing is configured.

Accessing Routing Table Configuration

In the menu tree, select "Network Settings" > "Routing" > "Routing Table" to bring up the Routing Table page. This page displays the current routing table in the DWR series routers and allows users to add or delete static routing. (See Figure 34 for more details)

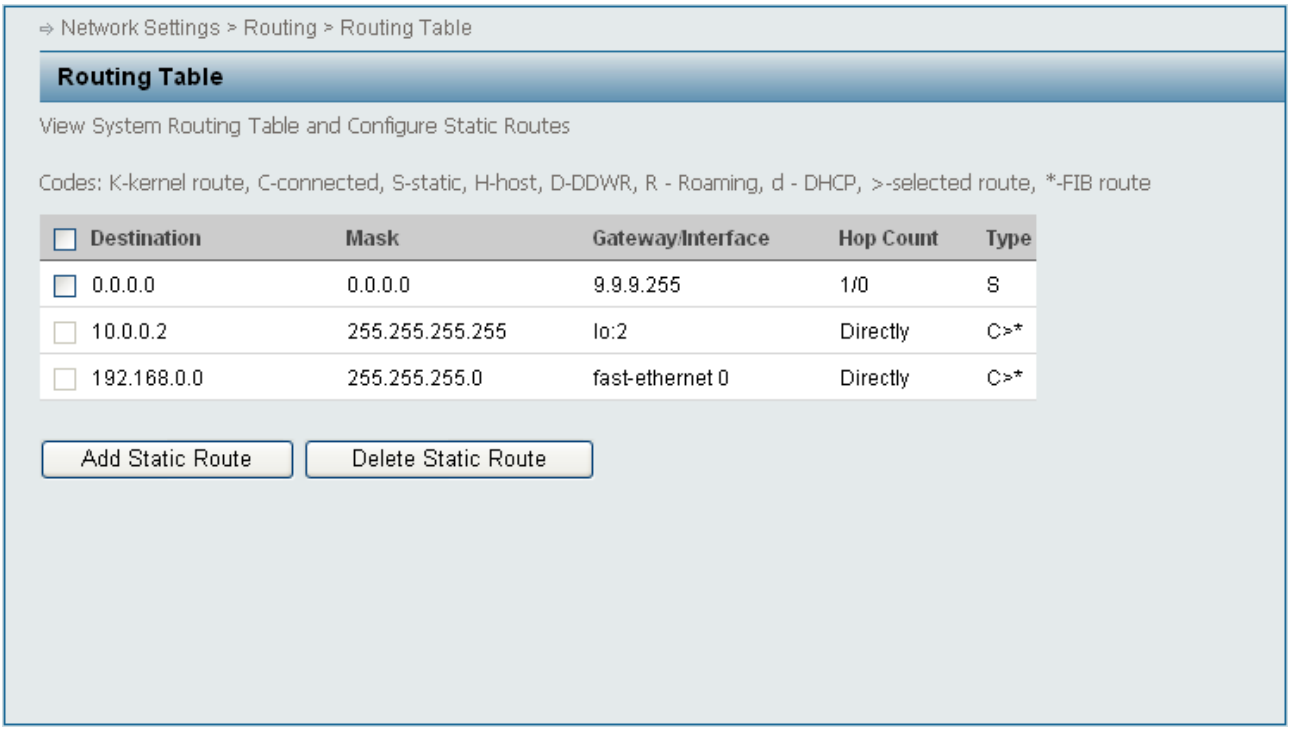


Figure 34 Network Routing Table Page

Table 7 explains the various fields in the routing table.

Table 7 Routing Table Fields

Column	Explanation
Destination	The destination network or host address.
Mask	The mask indicating the prefix for the destination; the destination and mask are used together to determine whether a packet's destination address matches a particular route
Gateway/ Interface	The gateway IP address or the router interface that this route points to. If an IP address is shown, then packets matching this route would be forwarded to this address. If an interface is shown, then packets matching this route would be forwarded using this interface.
Hop Count	In general, this field shows the number of hops between the DWR series router and the destination. However, the following special values may apply: Direct: Indicates route is for a network to which the router is directly connected. Self: Indicates a host route that points to the router itself. One may exist for each of the active interfaces (logical or physical) in the router. N/A: Indicates the hop count is either not available or not applicable for this type of route; i.e., static routes configured without any hop count information.
Type	A three-character code that indicates the type of the route. First character: K indicates a kernel route, C indicates a directly-connected route, S indicates a static route, H indicates a host route, A indicates a route learned by the DDWR protocol. Second character: '>' indicates the selected route when there are other routes with the same destination and mask. Third character: '*' indicates that the route is active in the router kernel.

Adding a Static Route

To add a new Static Route, click the "Add Static Route" button beneath the routing table to bring up the "Add Static Route" page (Figure 35)

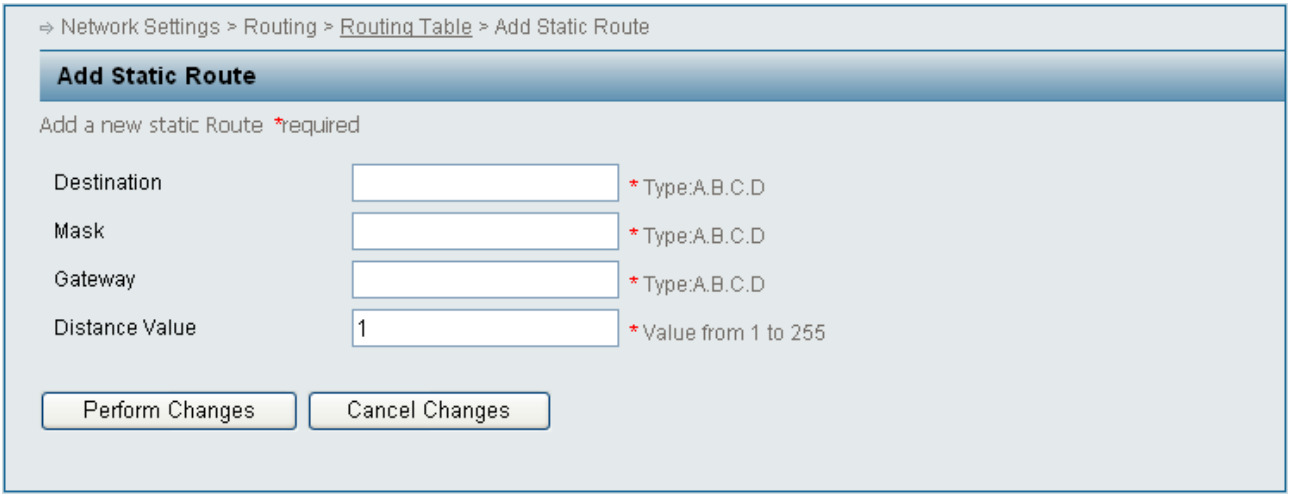


Figure 35 Add Static Route Page

Table 8 describes the settings for a static routing entry.

Table 8 Static Route Entry Fields

Setting	Explanation	Default
Destination	The destination network or host address for this route. ***This field is required; when creating a default route, use 0.0.0.0***	N/A
Mask	The mask indicating the prefix for the destination; the destination and mask are used together to determine whether a packet's destination address matches a particular route ***This field is required; when creating a default route, use 0.0.0.0***	N/A
Gateway	The gateway IP address that this route points to.	N/A
Distance Value	A value that indicates the distance of the destination network from this router; can be used to differentiate the different routes to a same network. Value Range: 1-255	1

Deleting a Static Route

To delete an existing static route, check the boxes beside the routes to be deleted and click the "Delete" button. A dialog box would appear and then ask for confirmation. Click "Yes" to confirm the delete, and click "No" to cancel.

DDWR Configuration

The DWR series routers support dynamic routing. DDWR is an adaptive, distributed wireless routing protocol specially designed for the wireless environment. DDWR reacts quickly to the rapid link changes in a wireless network and converge quickly to form the most efficient routing paths while avoiding routing loops. DDWR also uses very few computational and data communication resources. The use of DDWR dynamic routing eliminates the burden of configuring a lot of static routing, and is the recommended method to configure routing on the DWR series routers.

DDWR Configuration Page

Select "Network Settings" > "Routing" > "DDWR" from the left menu tree to open the DDWR configuration page. The DDWR Configuration Page appears (Figure 36).

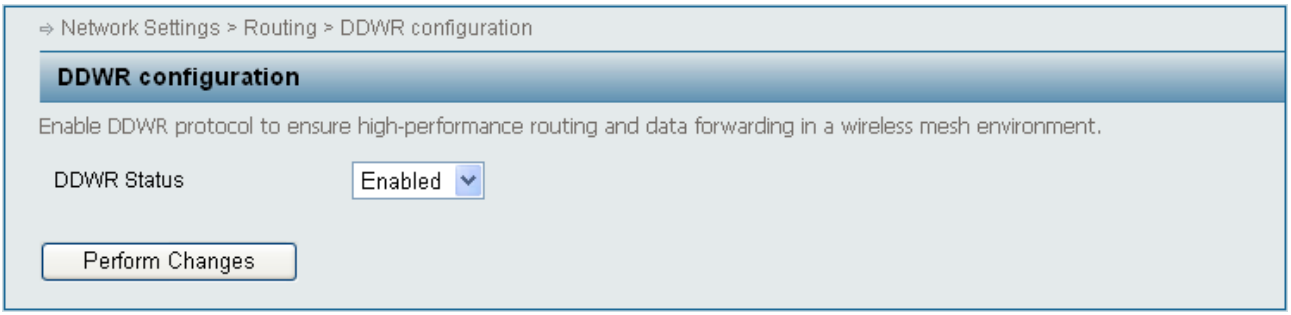


Figure 36 DDWR Configuration Page

Currently, the only setting in the DDWR Configuration Page is to enable or disable DDWR. To change this setting, simply choose the option and click the "Perform Changes" button. The resulting page would inform the users if the configuration is successful (Figure 37)

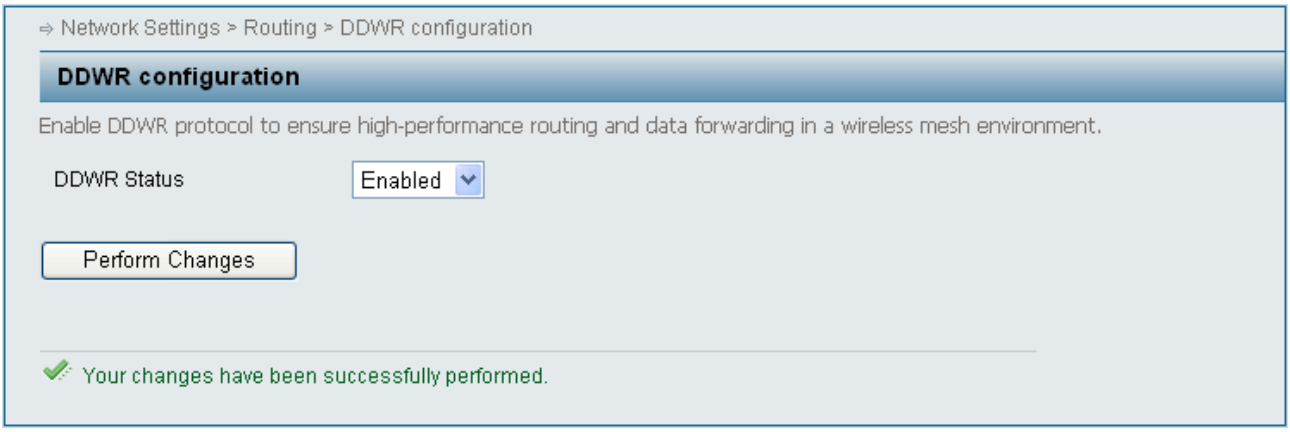


Figure 37 DDWR Configuration Success Page

Configuring DHCP

Besides routing, DHCP and NAT are also fundamental network services provided by many network devices, including DWR series Mesh Routers. This chapter describes how these basic services are configured using the Web-based Management Interface (WMI). The following sections are included:

Configuring DHCP

DHCP (Dynamic Host Configuration Protocol) is an Internet standard that allows client devices with a physical connection to a network to automatically obtain IP addresses from a DHCP server. DHCP services can be provided through the configuration of DWR BSS interface or Ethernet interface.

There are two types of DHCP services provided by the DWR series routers: DHCP Server and DHCP Relay. Using DHCP Server allows the DWR series routers to allocate IP addresses for connected clients, while using DHCP Relay causes the DWR series routers to relay any DHCP client requests to an external server that handles the IP address assignment.

For more information about DHCP service, please refer to the CLI Configuration Guide.

DHCP Server Configuration

Enter the DHCP Server configuration page, select “Network Settings” > “DHCP” > “DHCP Server” in the left-side menu tree.

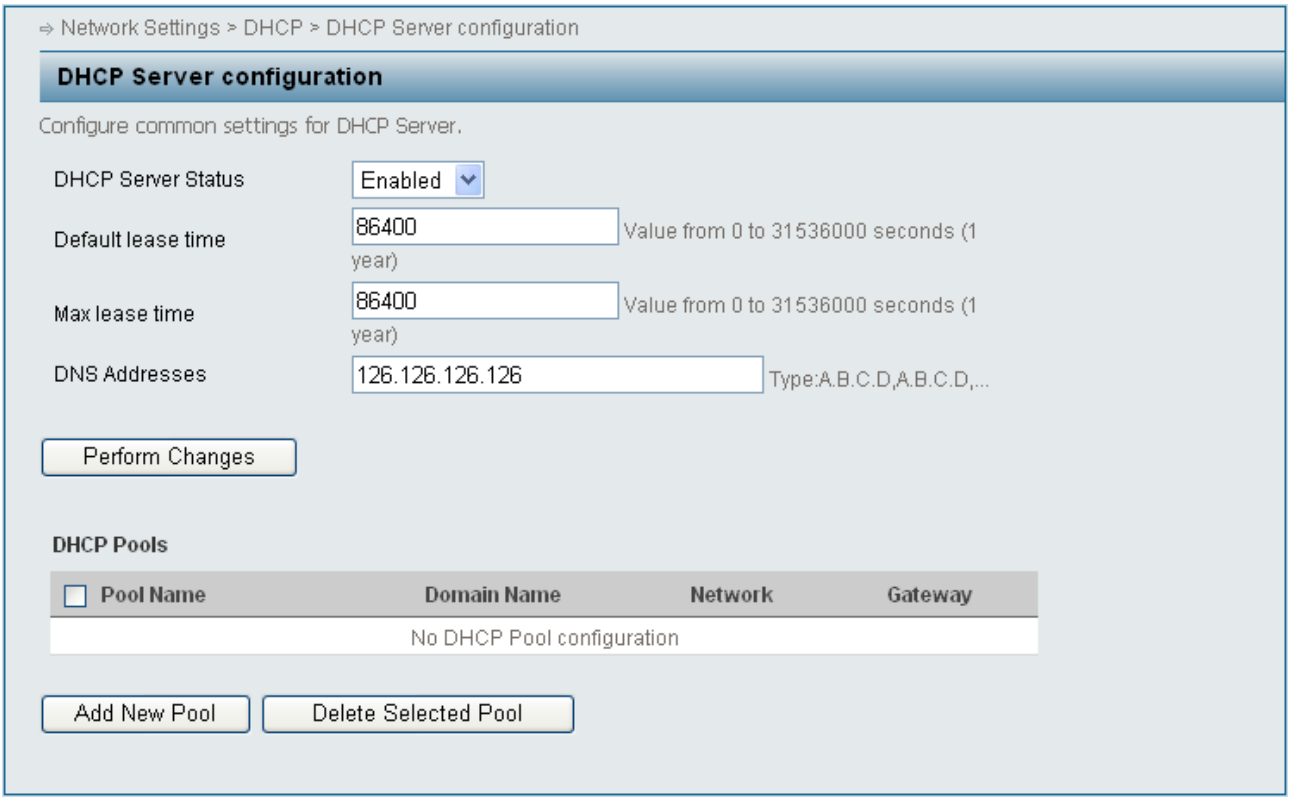


Figure 38 DHCP Server Configuration Page

In this page, the DHCP server may be enabled or disabled and server parameters such as the default lease time, max lease time, and DNS addresses can be configured.

Table 9 describes the settings for DHCP Server.

Table 9 DHCP Server Settings

Setting	Explanation	Default
DHCP Server Status	Whether the DHCP server is to be enabled or disabled	Enabled
Default lease time	The amount of time (in seconds) allowed for an IP address assignment (hereby referred to a lease) before it expires, if the client did not request for a specific lease length, it will be the default value. Value Range: 0-31536000s	86400s
Max lease time	The maximum amount of time (in seconds) allowed for a lease regardless of the client's request Value Range: 0-31536000s	86400s
DNS Addresses	A comma-separated list of DNS server addresses that would be given to clients along with the lease. Example: 206.56.44.1,206.56.33.1	N/A

After making changes in the page, click the "Perform Changes" button to confirm the configuration. The WMI would indicate to the user if the configuration is performed successfully (as in Figure 39)

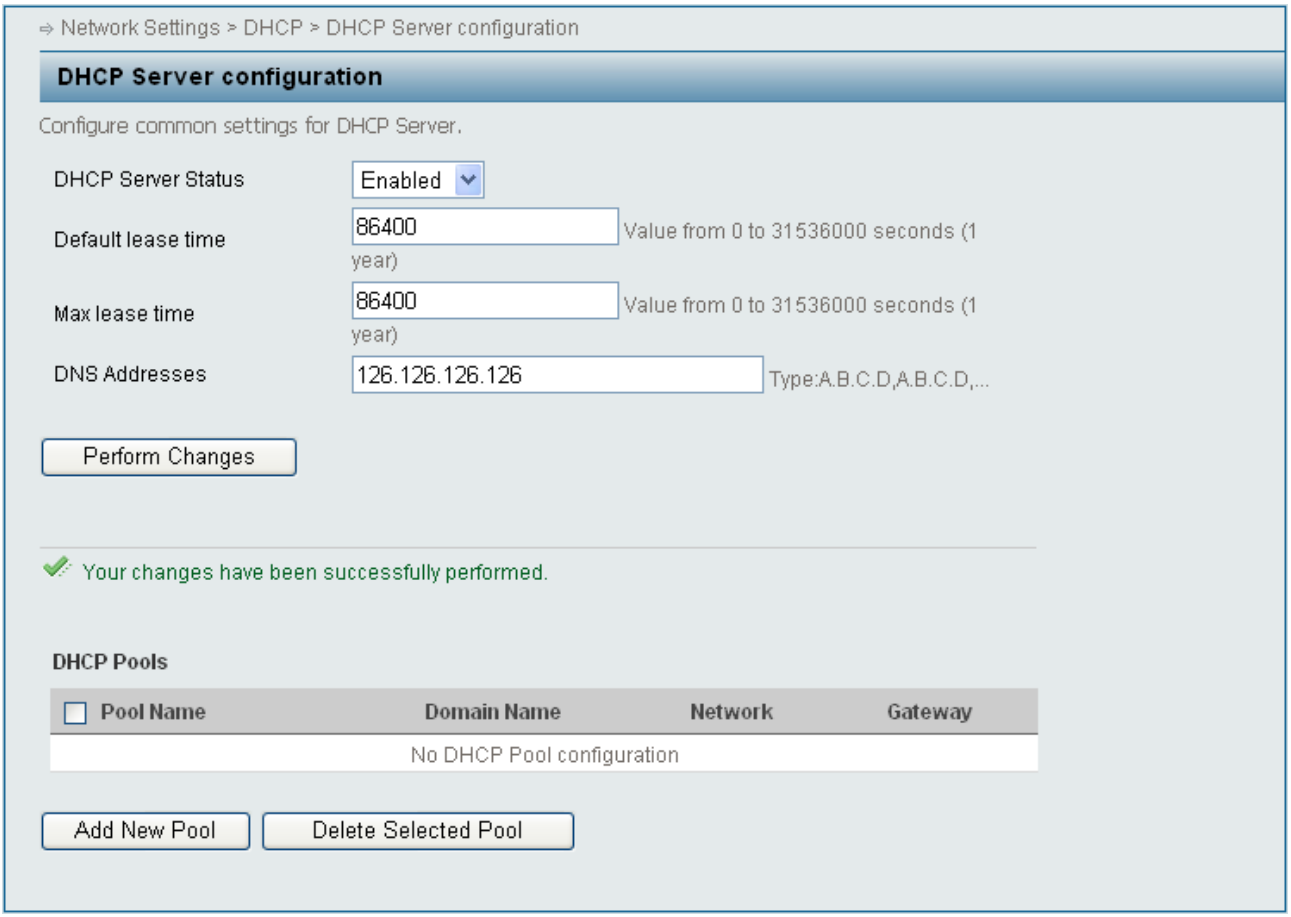


Figure 39 DHCP Server Configuration Success Page

Configuring DHCP Pools

For the proper operation of DHCP server, one or more DHCP pools must be defined. A DHCP pool defines a set of network addresses from which the DHCP server may allocate IP addresses for clients. It also includes other settings that control the behavior of the DHCP server for clients connected to different subnets served by the router. Besides allowing users to manually configure DHCP pools, DWR series mesh routers can also create DHCP pools automatically. Detailed information about the DHCP pool can be found in the configuration guide.

The currently available DHCP pools are displayed beneath the DHCP Server Settings.

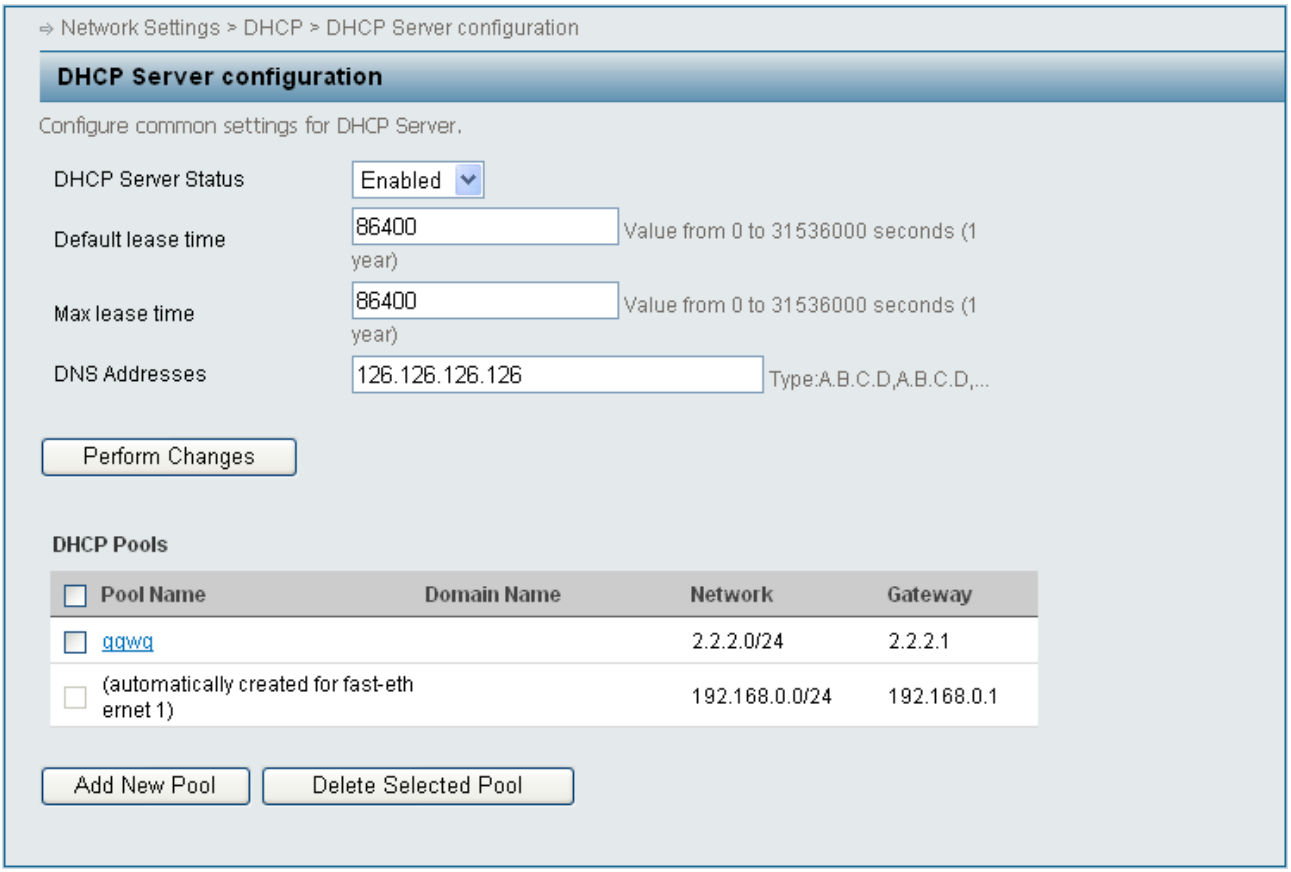


Figure 40 DHCP Pools List

The DHCP Pools list displays both automatic and manual pools on the router. It also allows users to create new pools or delete existing pools.

Adding a new DHCP Pool

To add a new DHCP pool, click the “Add New Pool” button beneath the DHCP pools list. The “Add New DHCP Pool” page appears:

In this page, user may configure network information that is passed to the clients in the DHCP lease (e.g., Domain name, network, etc), create IP address ranges, and define fixed IP addresses for certain clients by using their MAC addresses.

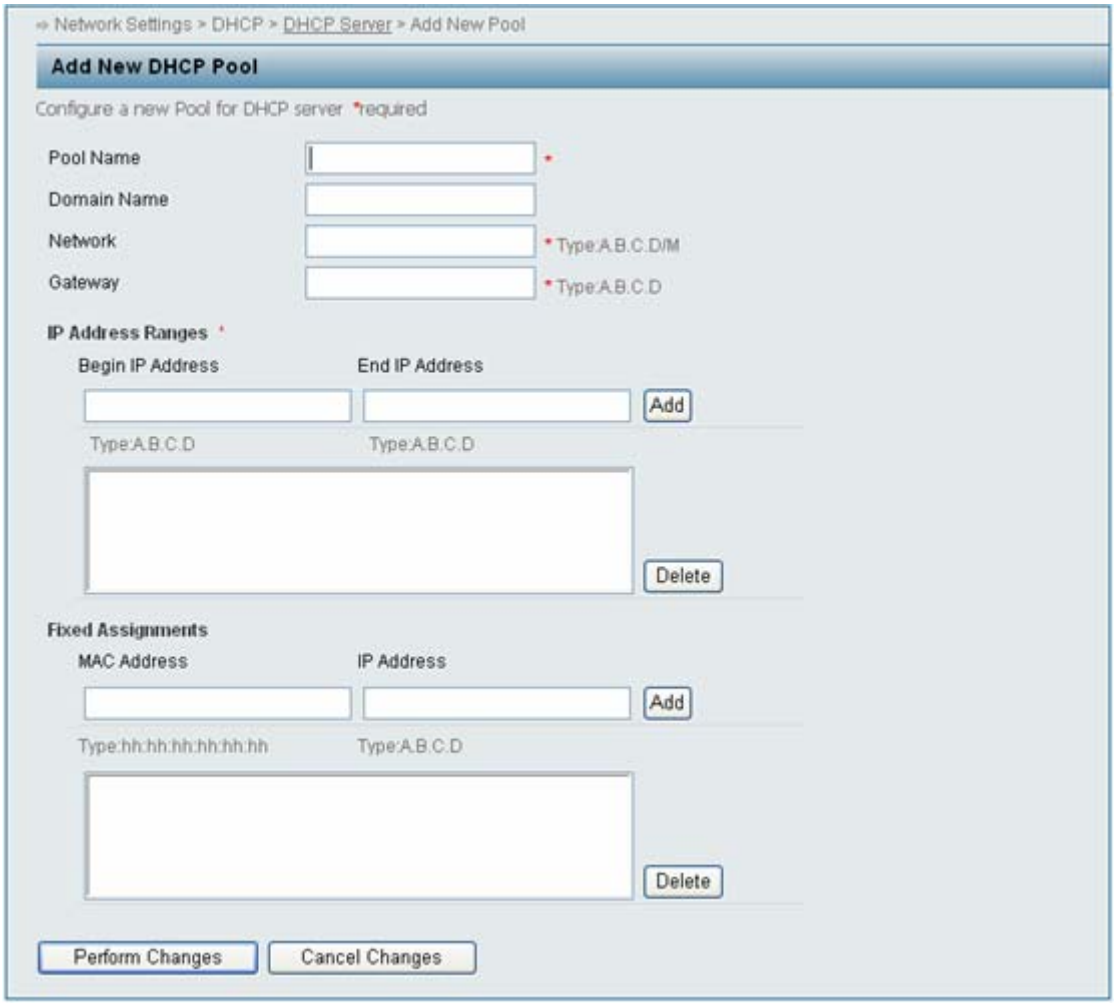


Figure 41 Add New DHCP Pool Page

The network setting for a DHCP pool is described in Table 10.

Table 10 Network Settings for DHCP Pool

Setting	Explanation	Default
Pool Name	An alphanumeric name for the pool to be created. This name must start with a letter and cannot contain any spaces. Example: pool1 ***This parameter is required and cannot be changed after the pool is created.***	N/A
Domain Name	The network domain name that will be given to DHCP clients that will use addresses from this DHCP pool. Example: dwrnet.com	N/A
Network	The network (with mask) from which the IP addresses in this DHCP pool will be part of. Example: 192.168.50.0/24	N/A
Gateway	The gateway IP address that will be given to DHCP clients that will use addresses from this DHCP pool. Example: 192.168.50.1	N/A

Defining IP Address Ranges

IP address ranges make up the available addresses in this DHCP pool. DHCP clients can only obtain IP addresses from these ranges. IP address ranges are configured beneath the network settings of the DHCP pool page.

To add a range, specify the begin IP Address and the end IP Address, then click add:

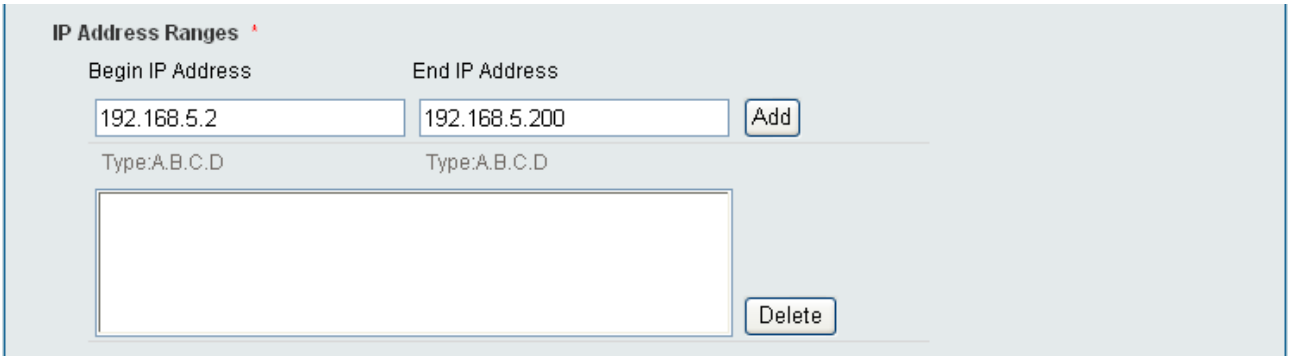


Figure 1 Adding a New IP Address Range

The IP Address range will be added to the list area. (Figure 42)

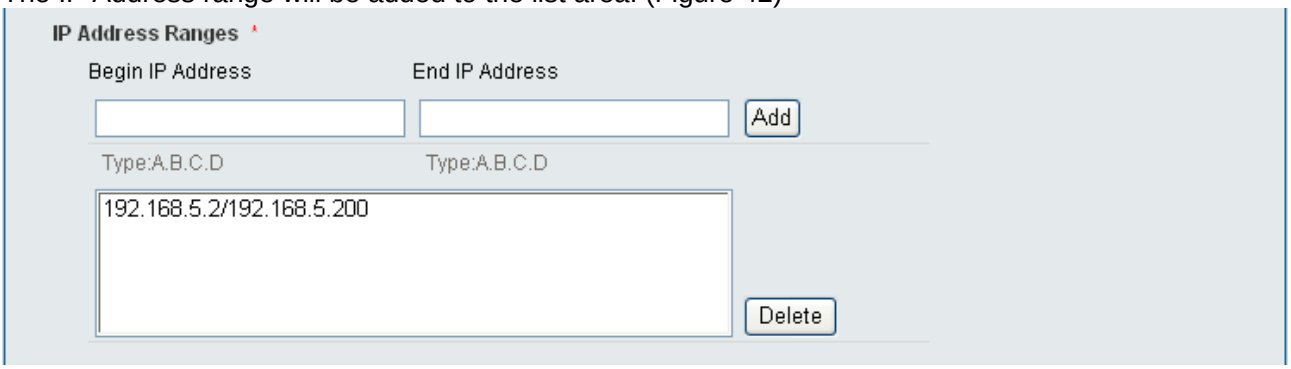


Figure 42 Adding a New IP Address Range Done

To remove an IP address range, select it and click “Delete.

Creating Fixed IP Address Assignments

In general, the DHCP protocol assigns unused addresses arbitrarily from each DHCP pool for each client. This behavior allows the number of clients that could access the network to be greater than that of the IP addresses, as long as these clients do not connect at the same time. It also, however, causes the IP address obtained by the same client to vary from session to session. Sometimes, a network administrator or client user may have the need to obtain the same IP address at all times. To satisfy this requirement, user may specify a set of fixed IP Address assignments beneath the IP Address ranges.

Fixed IP assignments are allocated based on the MAC address of each client device. To create a fixed assignment, specify the MAC Address and the desired IP address, then click Add.

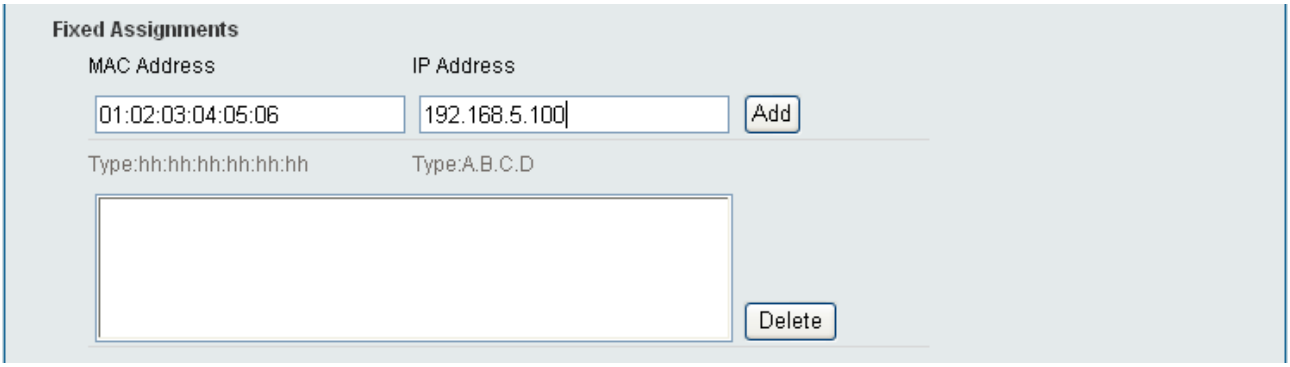


Figure 43 Adding a New Fixed IP Assignment

The fixed assignment will be added to the list area.

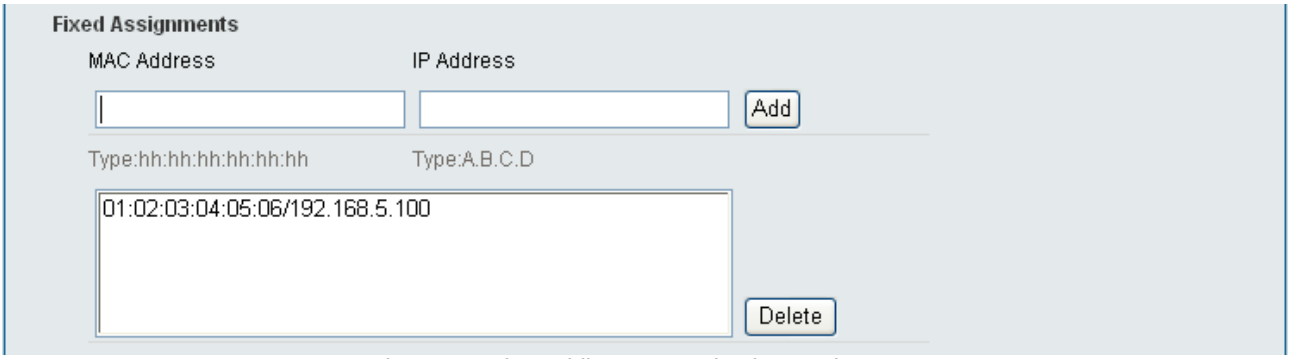


Figure 44 After Adding a New Fixed IP Assignment

To remove a fixed assignment, select it and click “Delete.”

Confirming the new DHCP Pool Settings

After the various DHCP Pool settings are configured, click “Perform Changes” to confirm the creation of a new pool, or click “Cancel Changes” to discard it. In either case, the user will be brought back to the DHCP Pool list page.

Configuring an existing DHCP Pool

To configure an existing DHCP Pool, click on its name in the DHCP Pool list. The "DHCP Pool Configuration Page" appears (Figure 45). The settings in this page are the same as the "Add New DHCP Pool Page," except that the pool name cannot be changed.

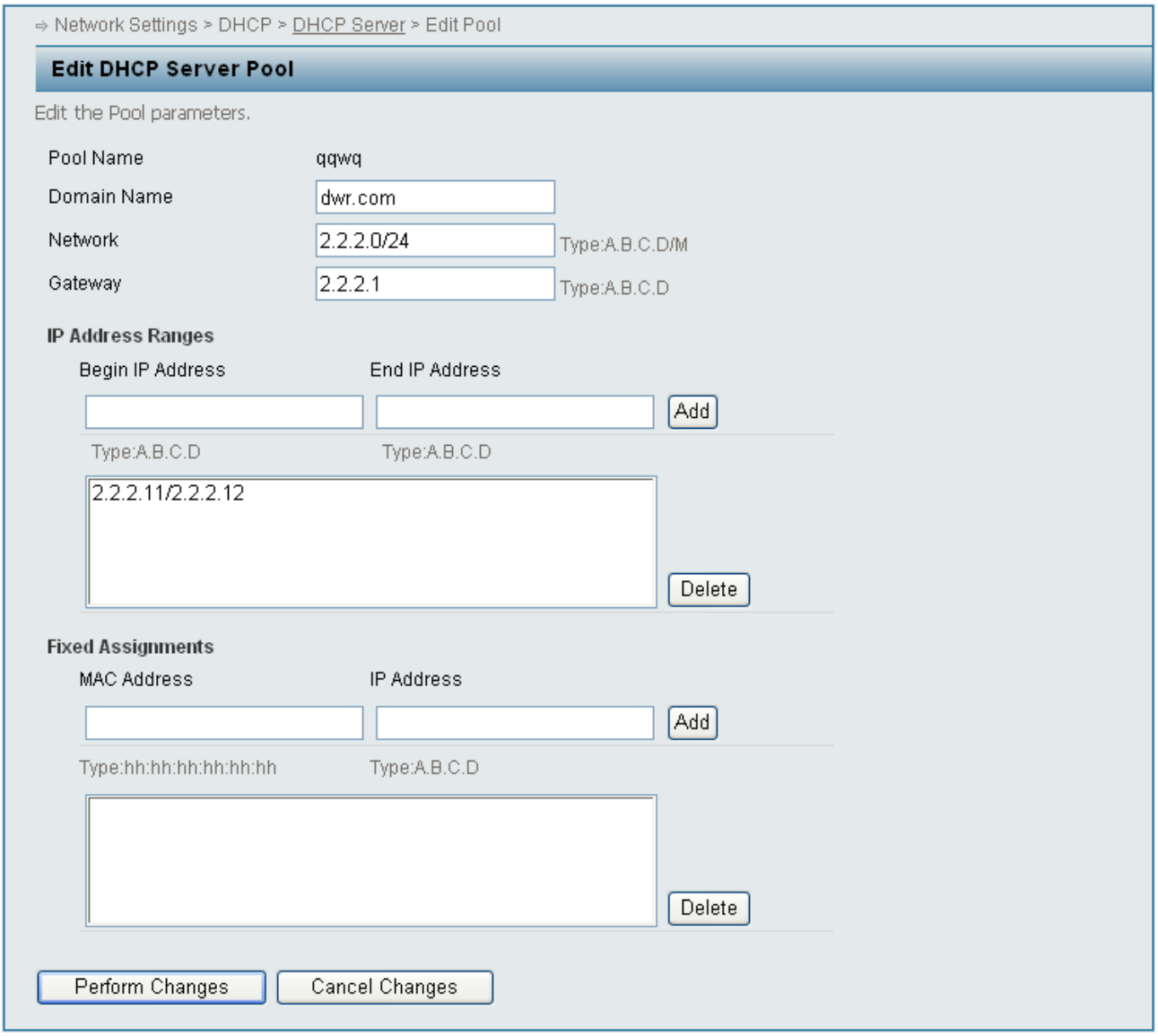


Figure 45 DHCP Pool Configuration Page

Deleting an existing DHCP Pool

To delete an existing DHCP Pool, check the box beside it and click "Delete." A confirmation dialog box will appear; click "Ok" to confirm the delete and "Cancel" to cancel.

DHCP Relay Configuration

DHCP Relay is a service provided by DWR series mesh routers that allows client devices connecting to the router to obtain IP Address from an external DHCP server. The mesh router relays both the DHCP

request from the client to the DHCP server and the reply from the server to the client. For more information about DHCP Relay, please refer to the CLI Configuration Guide.

Select “Network Settings” > “DHCP” > “DHCP Relay” in the left-side menu tree to open the DHCP server configuration page. The “DHCP Relay configuration” page appears (Figure 46).

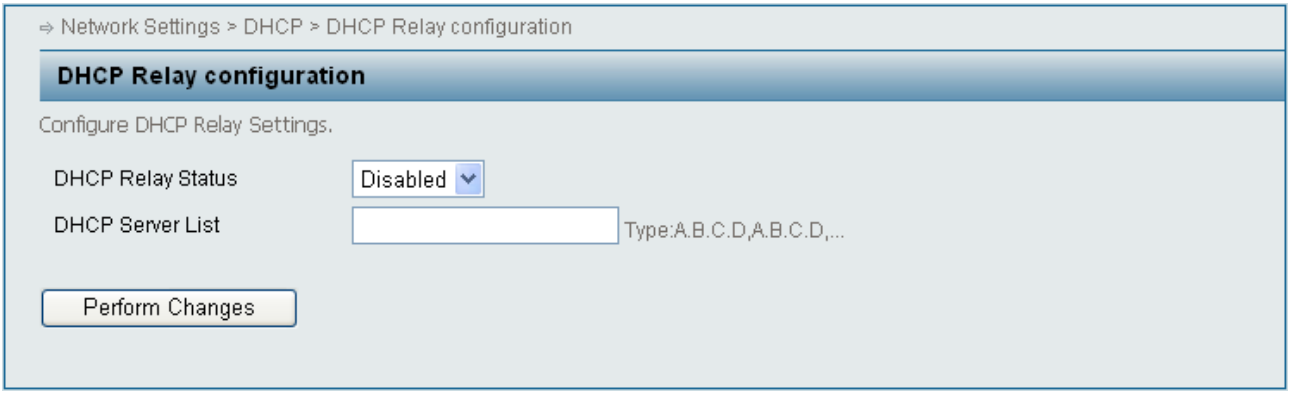


Figure 46 DHCP Relay Configuration Page

In this page, the DHCP relay service may be enabled or disabled and the external DHCP Server list can be configured.

Table 11 describes the settings for DHCP Relay.

Table 11 DHCP Relay Settings

Setting	Explanation	Default
DHCP Relay Status	Whether the DHCP relay service is to be enabled or disabled	Disabled
DHCP Server List	A comma-separated list of external DHCP server IP addresses. Example: 206.56.44.1,206.56.33.1	N/A

After making changes in the page, click the “Perform Changes” button to confirm the configuration. The WMI would indicate to the user if the configuration is performed successfully (as in Figure 47)

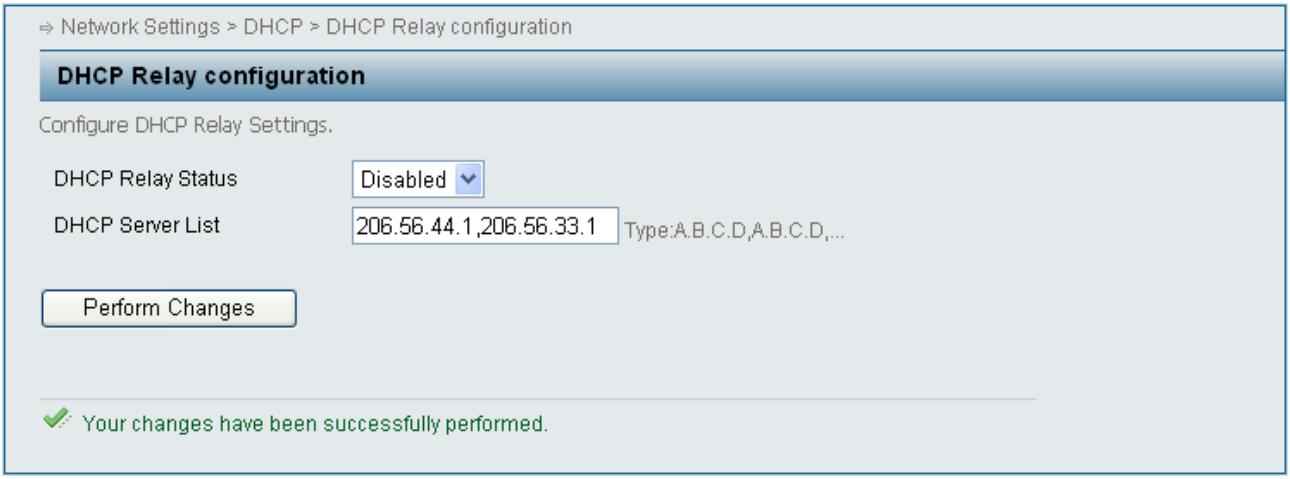


Figure 47 DHCP Relay Configuration Success Page

Configuring NAT

NAT (Network Address Transform) is an Internet standard that allows a LAN to use a set of IP addresses for internal communication and another set of addresses for external communication. The portal DWR series routers at the boundary between the wireless mesh and the wired networks could have NAT service enabled in order to achieve all the necessary IP address transform.

NAT Configuration Page

Select “Network Settings” > “NAT” in the left-side menu tree to enter the NAT configuration page. In this page (Figure 48), the NAT service may be enabled or disabled and the outgoing Ethernet interface can be selected.

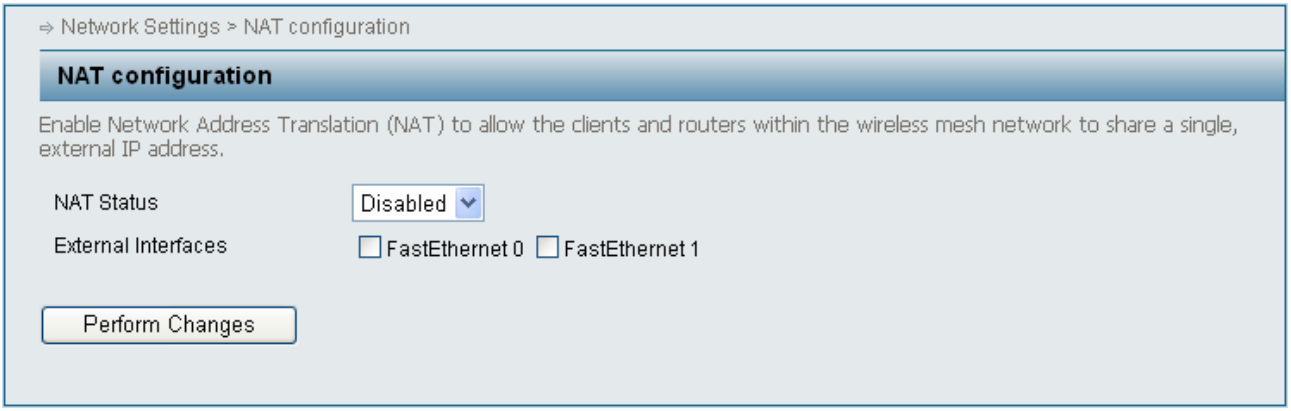


Figure 48 NAT Configuration Page

Table 12 describes the settings for NAT.

Table 12 NAT Settings

Setting	Explanation	Default
NAT Services	Whether the NAT service is to be enabled or disabled	Enabled
External Interfaces	The out-going interfaces that the NAT service would be working on. More than one interface may be selected. Only FastEthernet interfaces may be used as external interfaces.	FastEthernet 0

After the configuration is changed, click the “Confirm” button to save it. The router would indicate to the user if the configuration is saved successfully as shown in Figure 49.

Figure 49 NAT Configuration Success Page

Configure Mesh Profile

Configure the Mesh ID in mesh profile. All wireless routers in a single backhaul network should use the same mesh ID. User can configure mesh profiles by clicking the “Configure Mesh Profile” link to configure the mesh profile.

MESH Profile Configuration

To enter MESH profiles configuration, choose menu bar“Network Setting > MESH Profiles Configuration”in the menu bar. Mesh Profile can be added or deleted in this page.

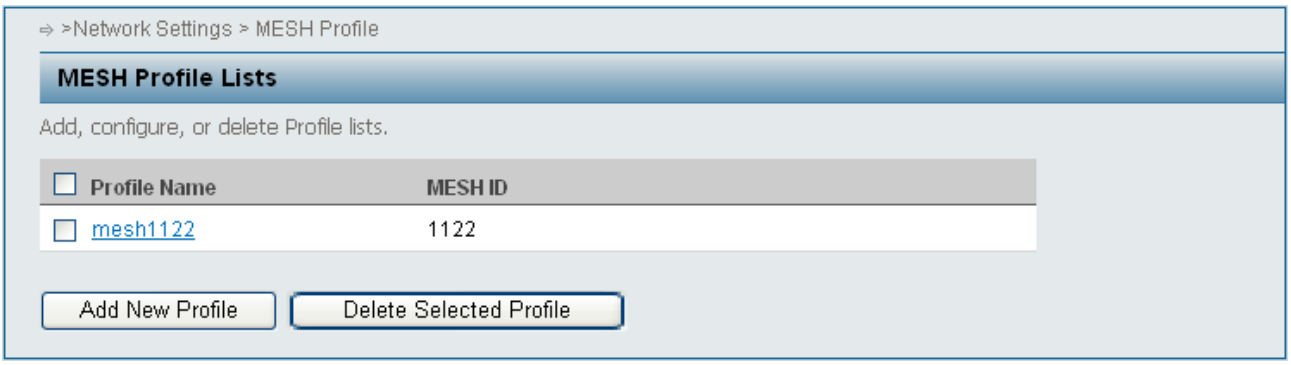


Figure 50 Mesh Profile Configuration

Click “Add New Profile” to add a new mesh ID. Enter the profile names and mesh ID, then click “perform Changes”. Note that the mesh ID number should be less than 32.

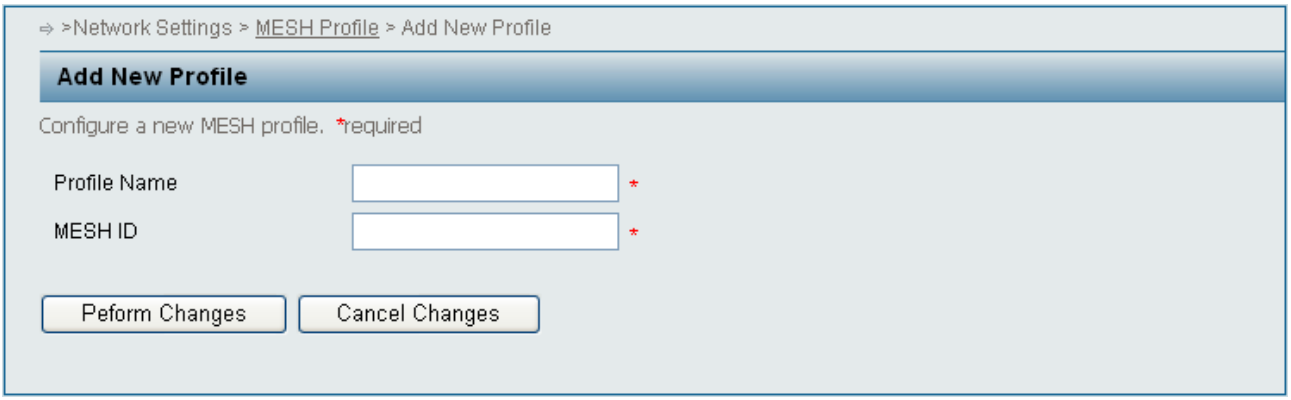


Figure 51 Add Mesh Profile

Delete MESH Profile

To delete Mesh Profile，it needs to select the profile names that want to delete, then click “delete Selected Files”.

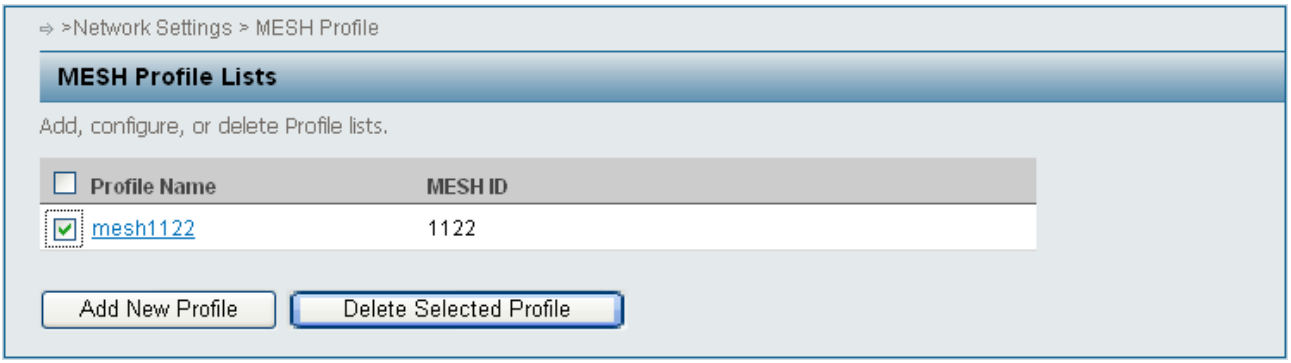


Figure 52 Delete Mesh Profile

Chapter 8 Configuring Services

This chapter describes how DWR series mesh router's advanced services such as recovery and roaming are configured; the following sections are included:

- Auto Recovery
- Roaming Dtrix

Auto Recovery

The Auto Recovery service allows the mesh router to diagnose abnormal conditions during its operation and to automatically recover from the problems. Enabling auto recovery maximizes the reliability and availability of the mesh network.

For more information about Auto Recovery, please refer to the CLI Configuration Guide.

Configuring Auto Recovery

Select "Services" > "Auto Recovery" from the left-side menu tree to enter the "Auto Recovery" configuration page. The resulting page is shown in Figure 53. It displays the status of the Auto Recovery service and the Portal IP Address List used by the service.

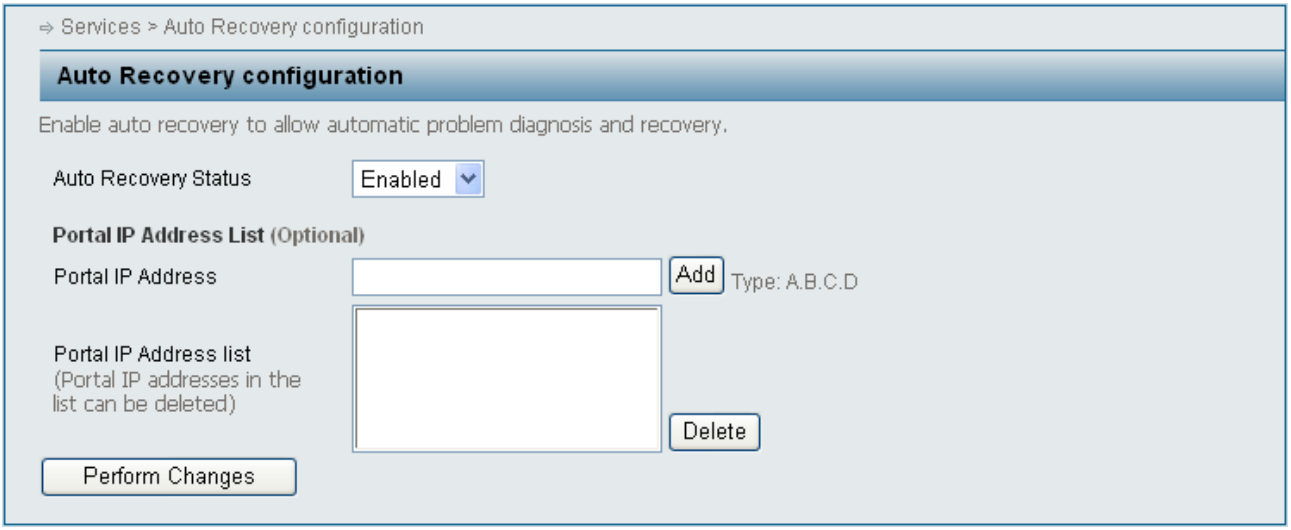


Figure 53 Auto Recovery Configuration Page

Table 13 describes the settings for Auto Recovery.

Table 13 Auto Recovery Settings

Setting	Explanation	Default
Auto Recovery Status	Whether the Auto Recovery service is to be enabled or disabled. ***For maximum reliability and availability, it is highly recommended that Auto Recovery be kept enabled.***	N/A
Portal IP Address	A list of IP Addresses for portal routers that this router would ping to determine network connectivity; details below.	N/A

A list of portal IP addresses may be provided for the auto recovery service to check network connectivity. When one or more such addresses cannot be reached, the auto recovery service may take appropriate action, such as changing configuration and/or rebooting the router. For more information about portal IP addresses, please refer to the CLI Configuration Guide.

A new IP Address can be added to the portal IP Address List can be configured by specifying the address and clicking Add, while an existing address may be deleted by selecting the address and clicking Delete.

After the configuration is changed, click the “Perform Changes” button to activate the change. The router would indicate to the user wether the configuration is saved successfully as shown in Figure 54.

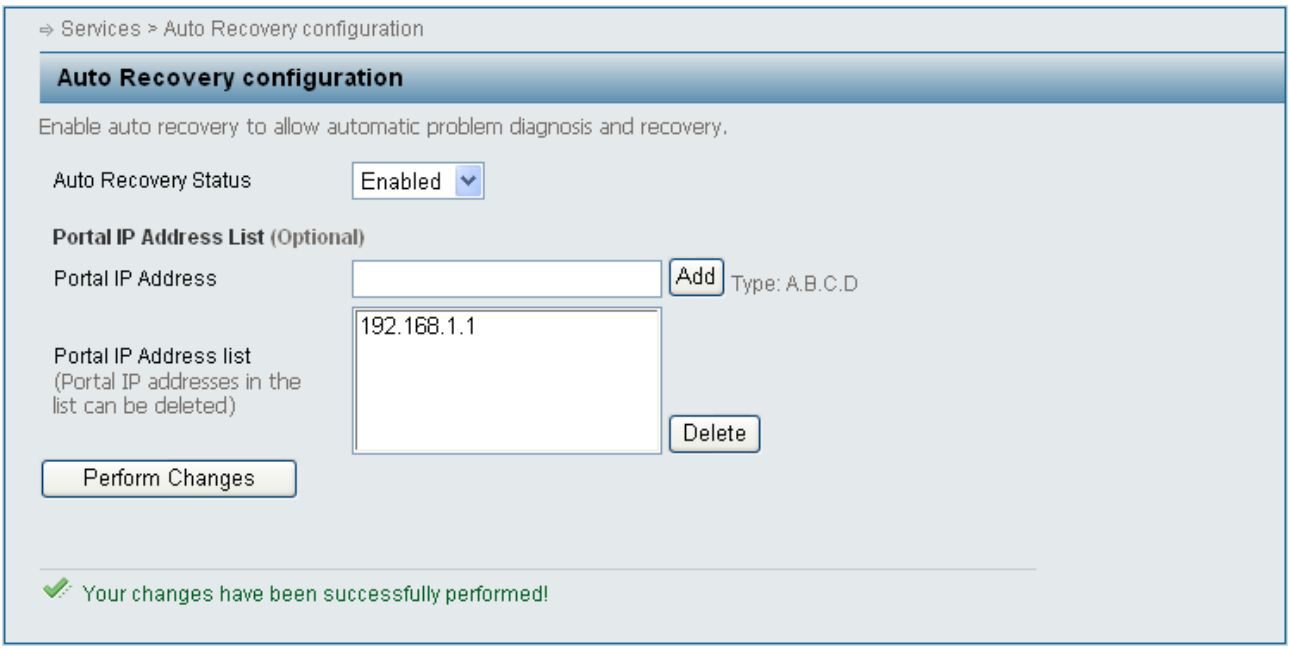


Figure 54 Auto Recovery Configuration Success Page

Roaming Dtrix Service

The Dtrix roaming service allows clients to roam freely without interference within a BSS network switching from a BSS to another BSS, and the IP address remains unchanged. To support client roaming, Dtrix needs to be enabled on all DWR routers providing BSS services.

For more information about Dtrix, please refer to the CLI Configuration Guide.

Configuring Dtrix

Enter the “Dtrix” configuration page, select “Services” > “Dtrix Roaming” from the left-side menu tree. The resulting page is shown in Figure 55.

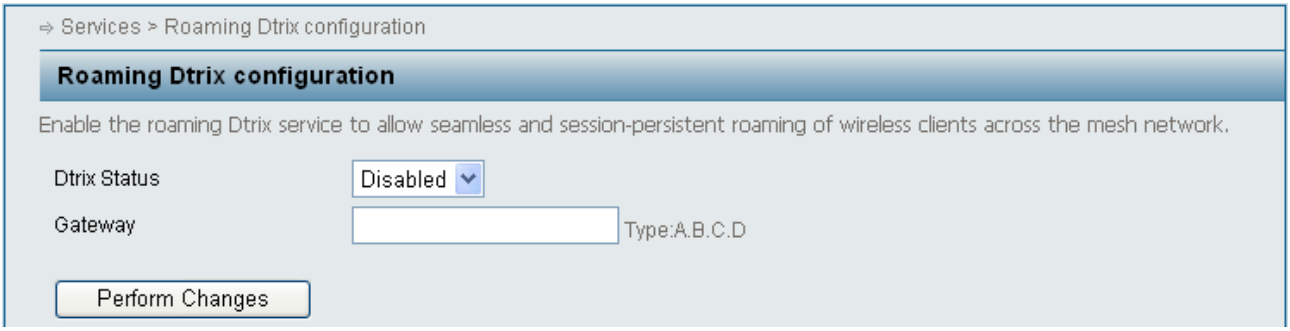


Figure 55 Dtrix Roaming Configuration Page

Similar to DDWR, Dtrix can be enabled or disabled by directly changing the “Dtrix Status” field. Select the required status and click the “Perform Changes” button, the system will prompt if the configuration is performed successfully as shown in Figure 56.

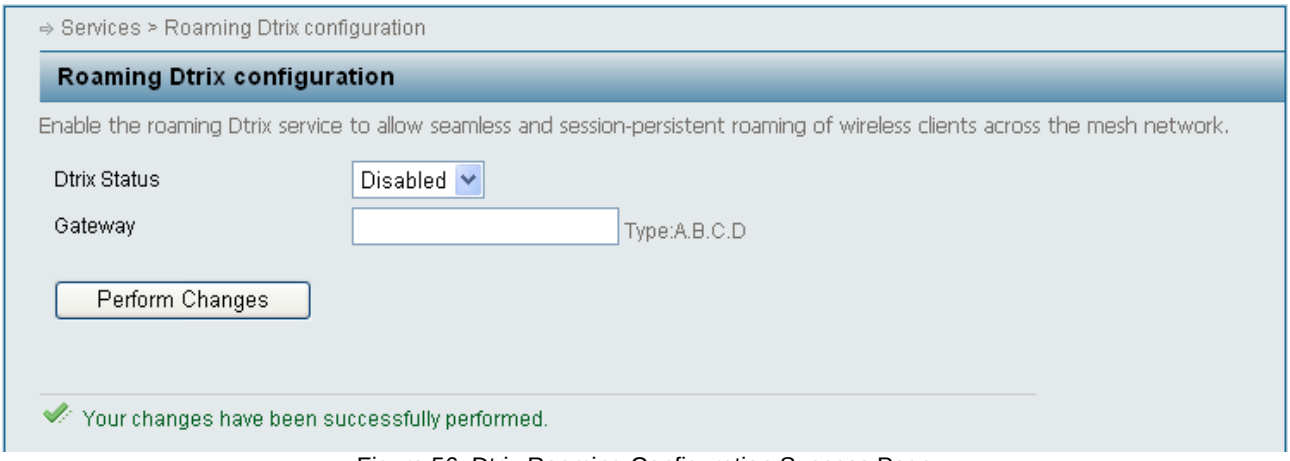


Figure 56 Dtrix Roaming Configuration Success Page

The following table summaries the Dtrix configuration:

Table 14 Dtrix Configuration

Configuration	Explanation	Default
Dtrix Status	Dtrix service enabled or disabled	Enabled
Gateways	Configure the router IP address of Dtrix gateway	N/A

Configuring MAC-IP Mapping

Beneath the Dtrix Roaming settings is the “Peer AP MAC-IP Mappings” table.

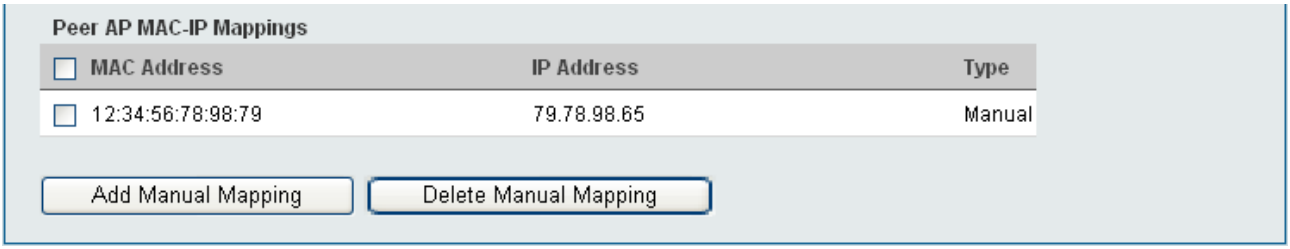


Figure 57 Peer AP MAC-IP Mappings Table

MAC-IP Mappings table records the mapping of MAC address of a BSS to an IP address in a roaming domain (ESS). Accurate data in this list is required for proper roaming.

MAC-IP mapping can be automatically configured if DDWR is enabled, or through the user manual configuration (senior). At the same time, manual configuration can coexist with the automatically configured DDWR MAC-IP mapping table and complement each other, but when the same MAC-IP configuration entries of BSSID exist in the same list, it will take the manual configured mapping relation as the standard. Users, however, may only delete manually configured MAC-IP entries and not the DDWR generated mapping entries.

Table 15 summarizes the information columns of the MAC-IP mapping table.

Table 15 MAC-IP Mapping Table Columns

Setting	Explanation
MAC Address	BSSID of routers.
IP Address	The corresponding IP Address of the peer AP.
Type	Automatic or manual. Automatic: The mapping entry is automatically made by DDWR. Manual: The mapping entry is manually configured.

Adding a Manual MAC-IP Mapping

To add an MAC-IP address mapping manually, click the “Add Manual Mapping” button in the page to bring up the “Add MAC-IP address mappings” page as shown in Figure 58.

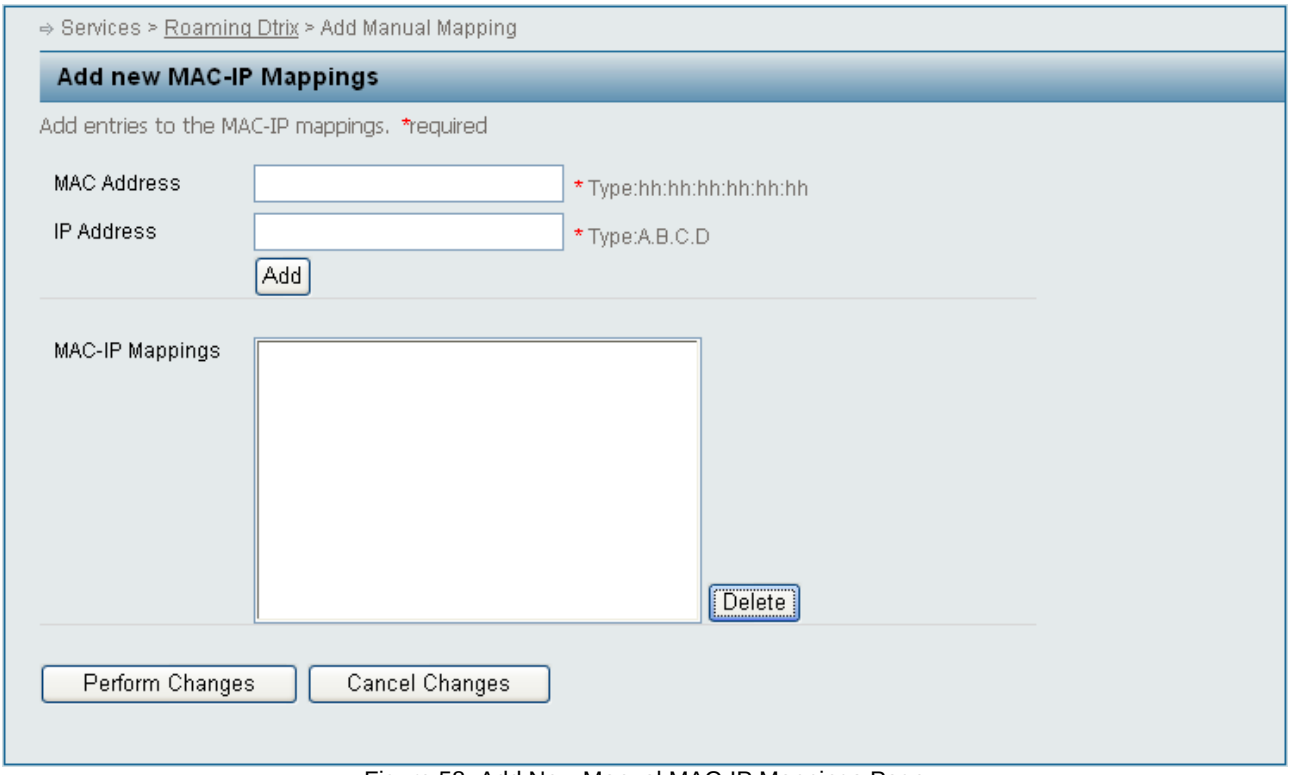


Figure 58 Add New Manual MAC-IP Mappings Page

Specify the MAC and IP address of a BSS and click “Add” to add it to the list. Multiple addresses may be added in this page. (Figure 59) Once finished, click “Perform Changes” adding the new entries to the MAC-IP mappings table and return to the Dtrix Configuration page.

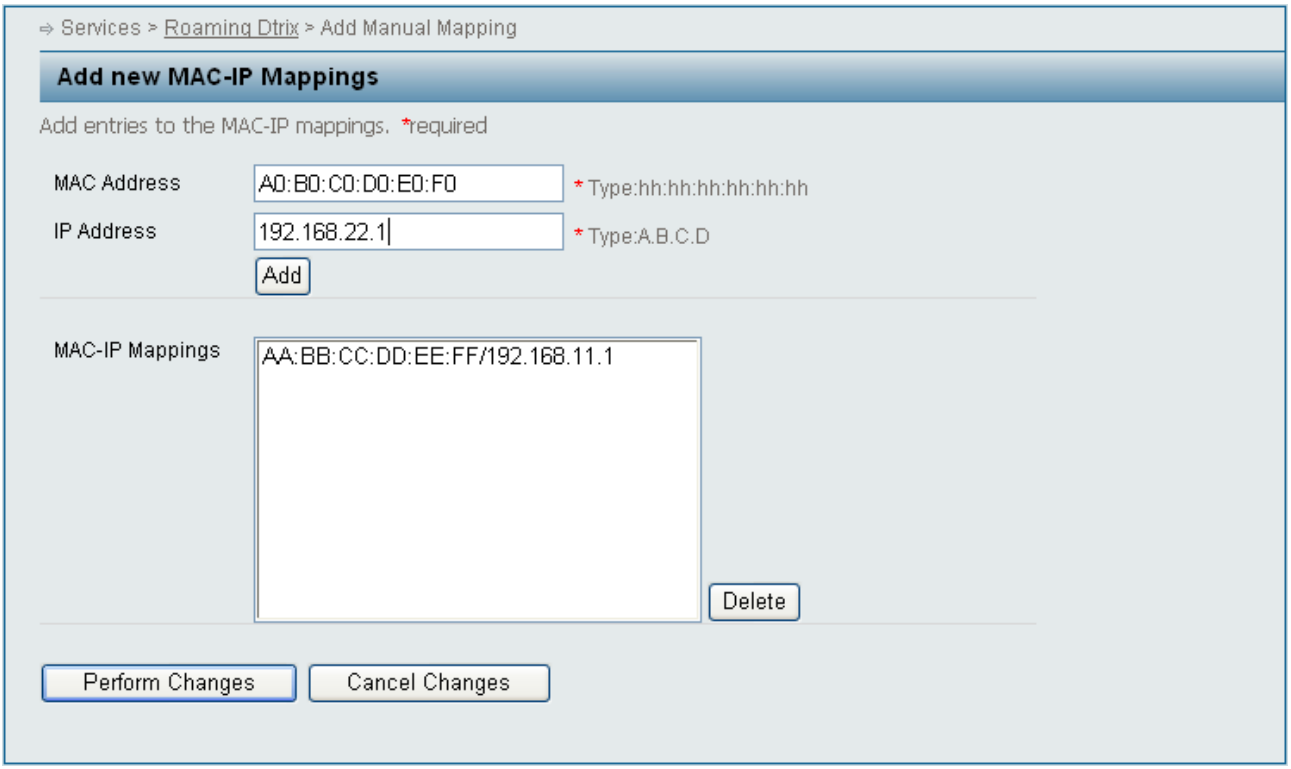


Figure 59 Adding Manual MAC-IP Mappings

Deleting a Manual MAC-IP Mapping

To delete a manually configured MAP-IP address mapping, check the boxes beside each entry to be deleted, and click the “Delete” button. A confirmation dialog would appear. Click “Ok” to perform the deletion, and click “Cancel” to cancel.

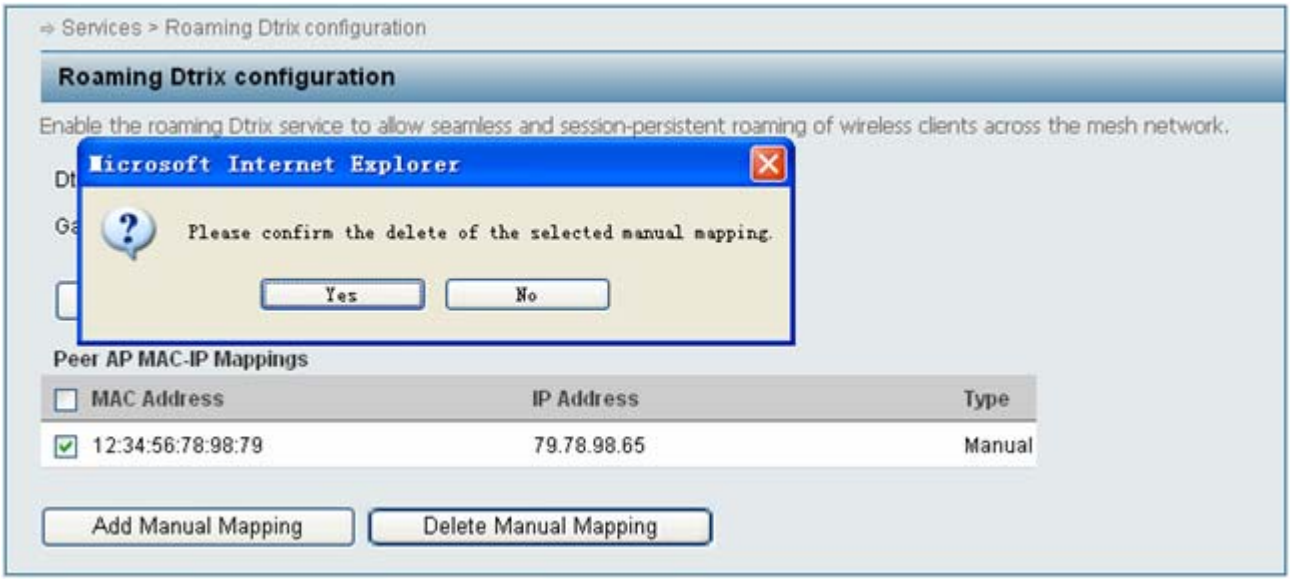


Figure 60 Deleting Manual MAC-IP Mapping

Chapter 9 Security Configuration

DWR series mesh routers provide security features such as access control and encryption for both backhaul and access connections. This chapter describes the security features that may be configured by the Web-based Management Interface. For full information about security, including some features that cannot be configured using the WMI, please refer to the CLI Configuration Guide.

The WMI supports Wired-Equivalent Privacy (WEP) and MAC-based security. WEP security use a list of shared secret keys for access control and encryption, while MAC-based security use a list of MAC addresses for access control only. Both security methods can be combined. Chapter 6, BSS Configuration, has already mentioned these lists because they are part of BSS settings.

This chapter contains the following sections:

- WEP Security
  - WEP Key List Configuration
  - Selecting a WEP Key List for a BSS
- MAC-based Security
  - MAC List Configuration
  - Selecting a MAC List for a BSS

WEP Security

Wired-Equivalent Privacy (WEP) is a standard and popular method of securing access to wireless APs. The WMI support WEP in its security configuration for BSSs.

WEP Key List Configuration

WEP security uses a list of secret keys for access control and encryption. The WEP Key Lists can be configured by selecting “Security” > “WEP Key Lists” in the menu tree. Figure 61 shows the “WEP Key Lists Configuration” page, which contains all configured WEP Key Lists. Each key list contains four keys.

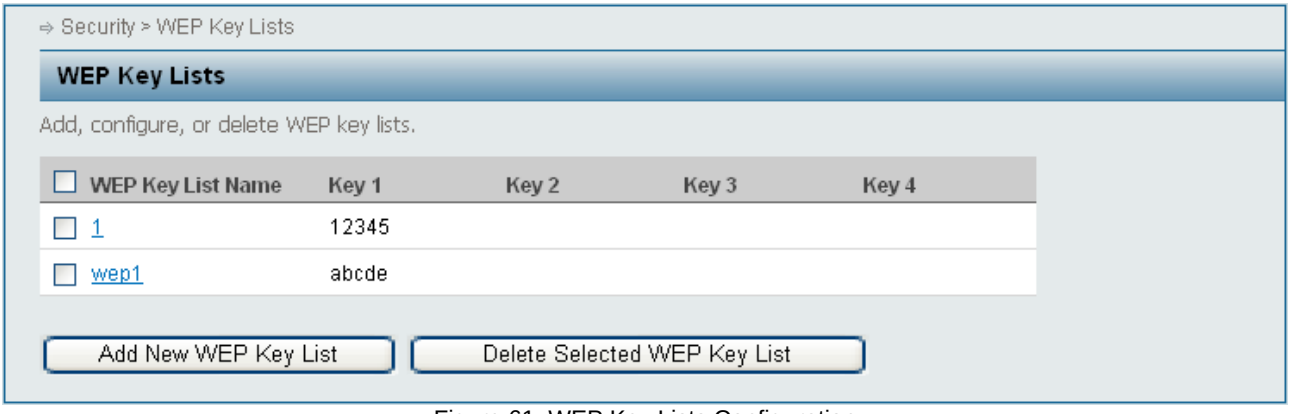


Figure 61 WEP Key Lists Configuration

Adding a New WEP Key List

To add a WEP Key List, click the “Add New WEP Key List” button at the bottom of the page. The “Add New WEP Key List” page appears:

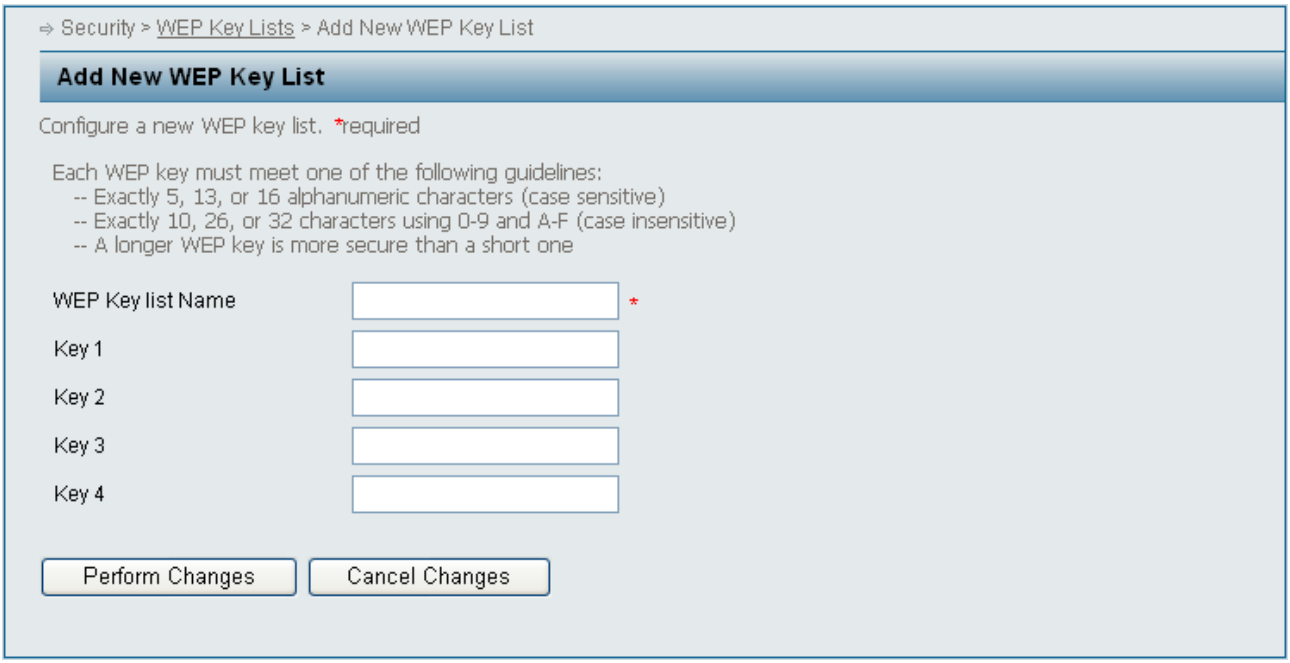


Figure 62 Add New WEP Key List Page

The required information in this page is the WEP key list name and four WEP keys. The list name should be alphanumeric, start with a letter, and contain no spaces. Each WEP key must meet one of the following guidelines:

- Exactly 5, 13, or 16 alphanumeric characters (case sensitive)
- Exactly 10, 26, or 32 characters using 0-9 and A-F (case insensitive)
- A longer WEP key is more secure than a short one

After specifying all needed settings, click “Perform Changes” at the bottom of the page to create the new WEP Key List, or click “Cancel Changes” to cancel. In either case, the user will be brought back to the WEP Key Lists page.

Configuring an existing WEP Key List

To configure an existing WEP Key List, click on its name in the WEP Key List configuration page. The “Configure WEP Key List” page appears (Figure 63). The settings in this page are the same as the “Add New WEP Key List” page, except that the list name cannot be changed.

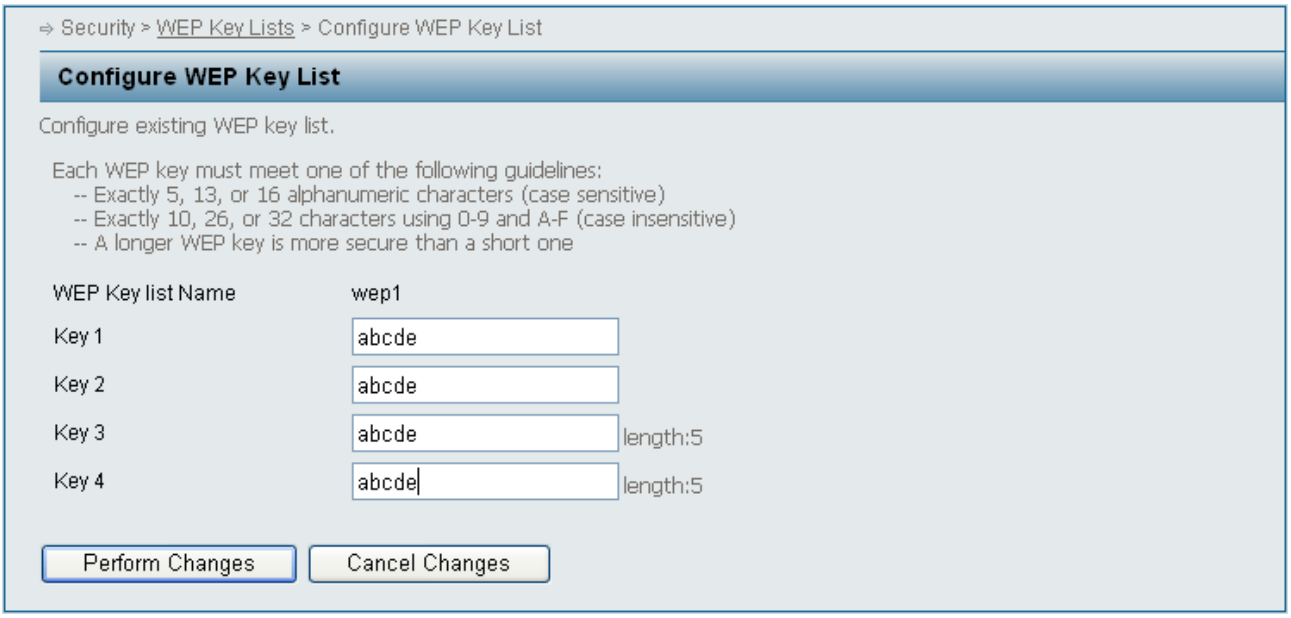


Figure 63 Configure WEP Key List Page

Deleting a WEP Key List

To delete a WEP Key List, check the boxes beside each list to be deleted, and click the “Delete” button. A confirmation dialog would appear. Click “Ok” to perform the deletion or click “Cancel” to cancel.

Figure 64 Deleting a WEP Key List

Selecting a WEP Key List for a BSS

After the WEP Key Lists are configured, one must select a WEP Key List for each BSS that needs to use WEP-based security. To do, open the BSS configuration page (**Error! Reference source not found.**65) and specify the name of the WEP Key List and a default WEP Key.

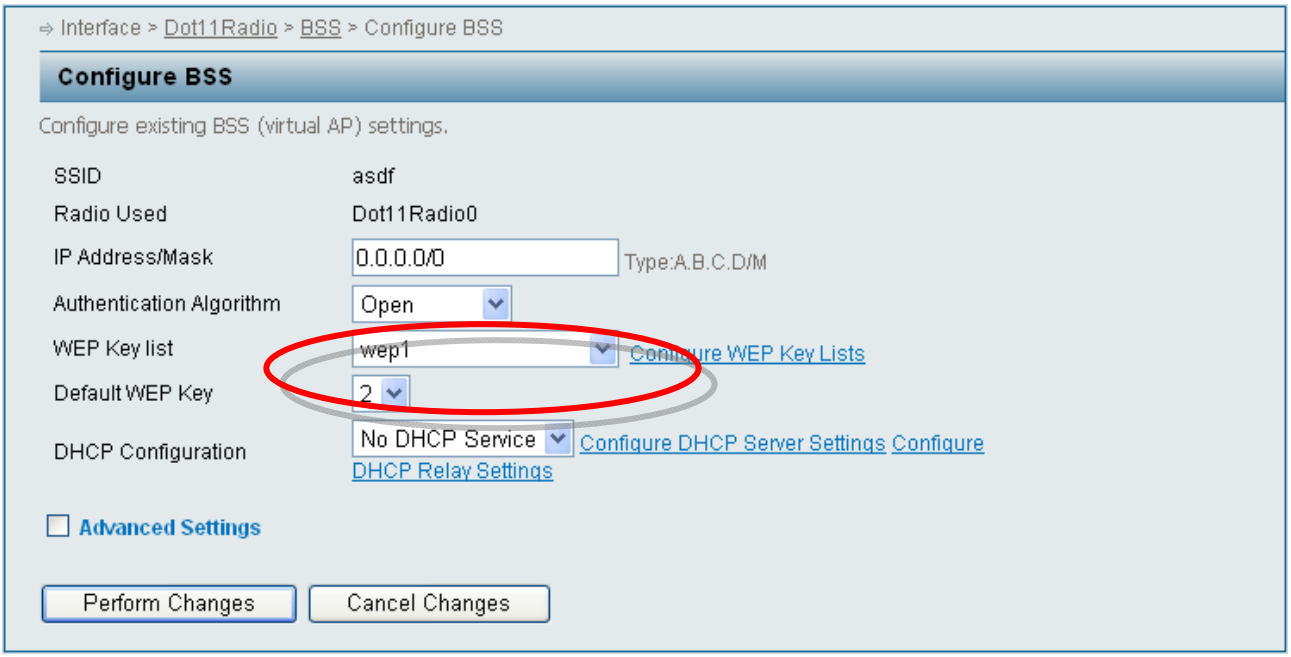


Figure 65 Selecting a WEP Key List for a BSS

MAC-based Security

MAC-based security is also a popular method of controlling access to wireless APs. DWR series products support MAC-based access control in addition to WEP. Both mechanisms can be active at the same time, and only clients that satisfy both security requirements would gain access to the BSS.

MAC List Configuration

MAC-based security uses a list of client MAC addresses for access control. The MAC List can be configured by selecting “Security” > “MAC Lists” in the menu tree. Figure 66 shows the “MAC Lists Configuration” page, which contains all configured MAC Lists.

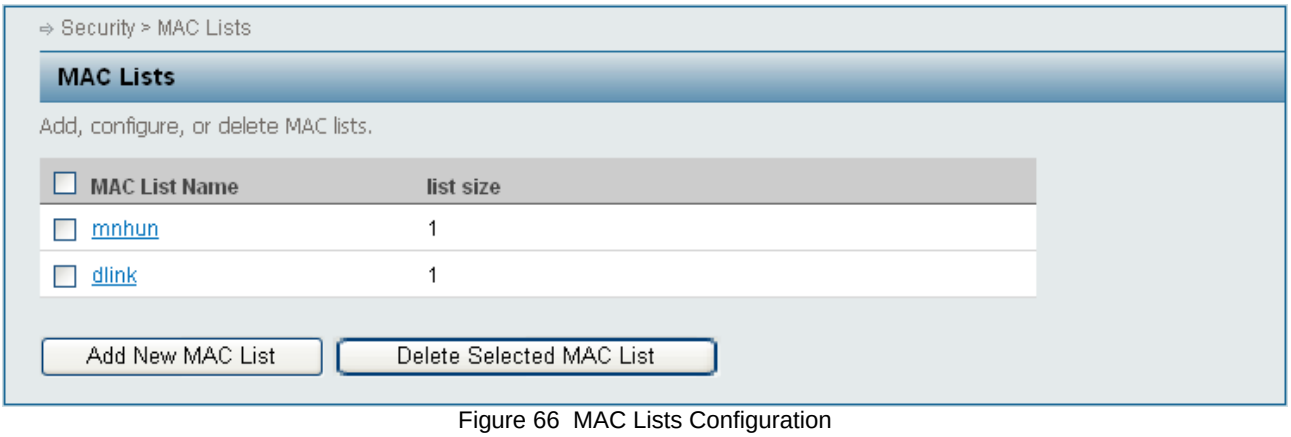


Figure 66 MAC Lists Configuration

Adding a New MAC List

To add a MAC List, click the “Add New MAC List” button at the bottom of the page. The “Add New MAC List” page appears (Figure 67)

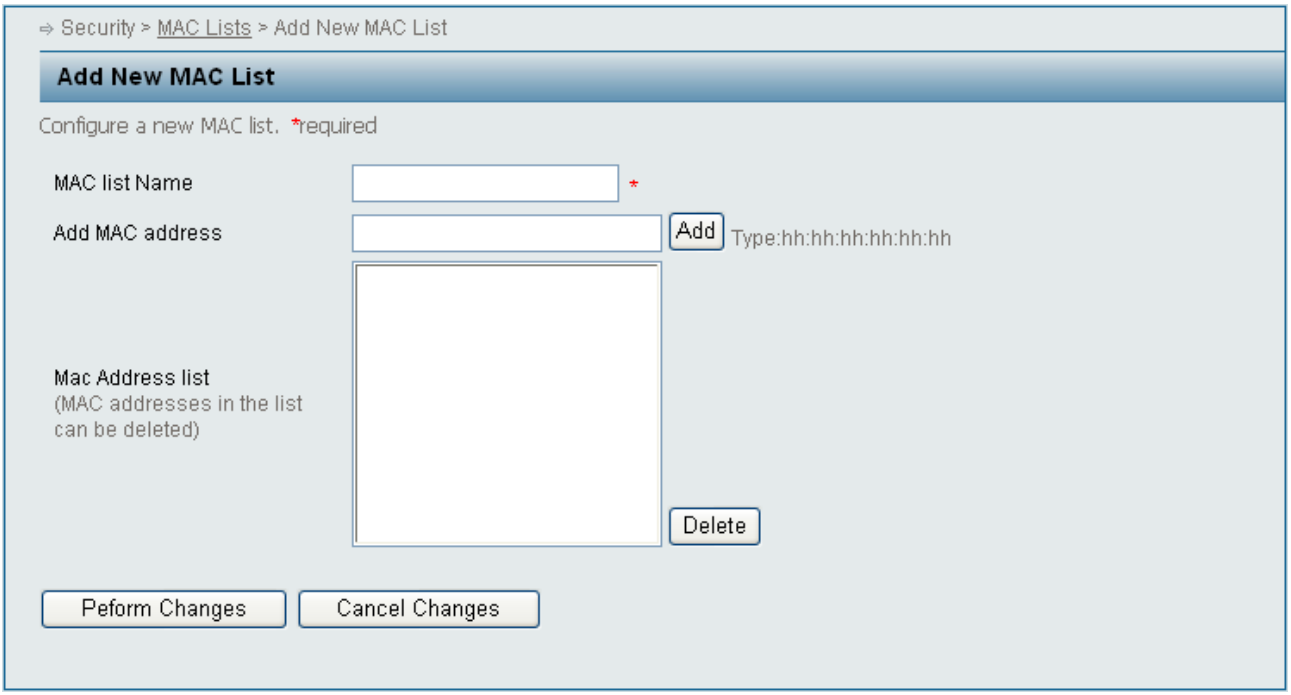


Figure 67 Add New MAC List Page

First, enter a name for the new MAC list. The name should be alphanumeric, start with a letter, and contains no spaces.

To add an MAC address to the list, specify the MAC and click Add (Figure 68).

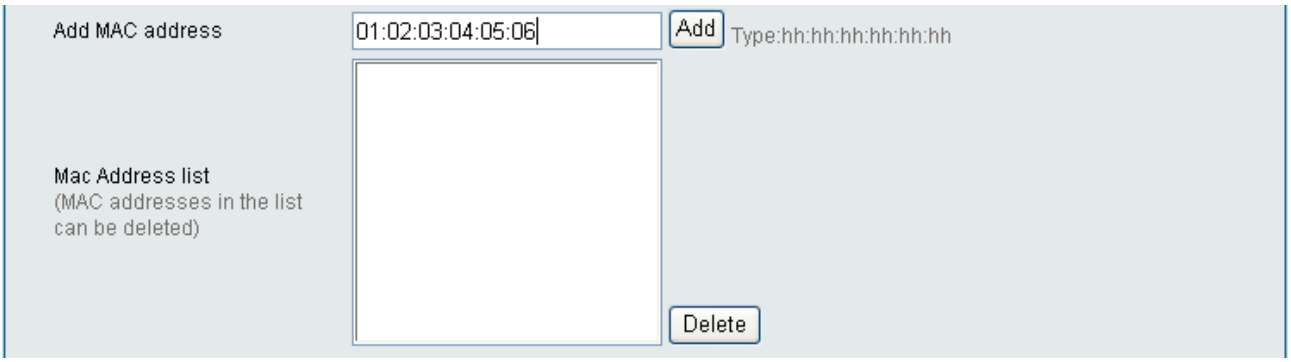


Figure 68 Adding an MAC address to the MAC List

The MAC address will be added to the list area.

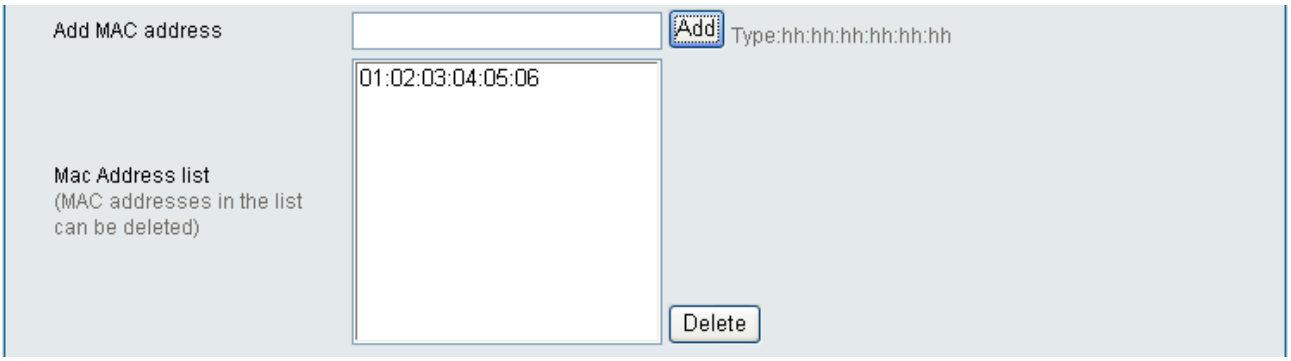


Figure 69 After Adding an MAC address

To remove an address, select and click “Delete.”

After specifying the name and the MAC addresses for the list, click “Perform Changes” at the bottom of the page to create a new MAC list, or click “Cancel Changes” to cancel. In either case, the user will be brought back to the MAC Lists page.

Configuring an existing MAC List

To configure an existing MAC List, click on its name in the MAC List configuration page. The “Configure WEP Key List” page appears (

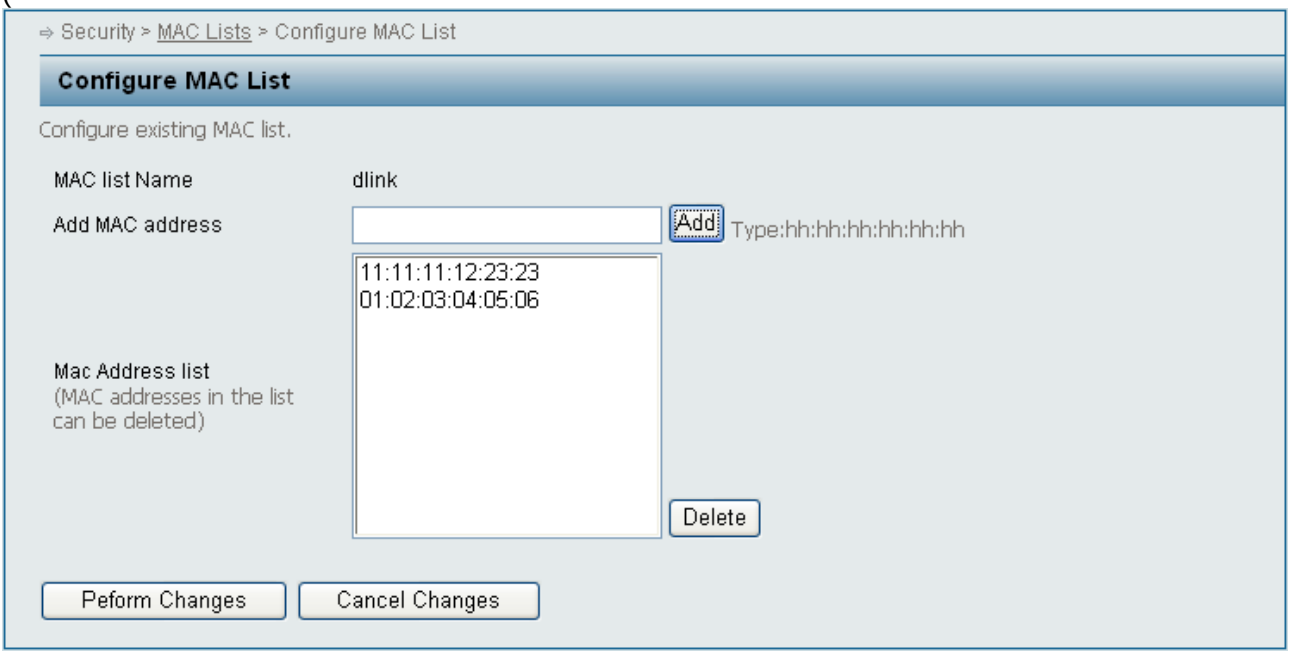


Figure 70). The settings in this page are the same as the “Add New MAC List” page, except that the list name cannot be changed.

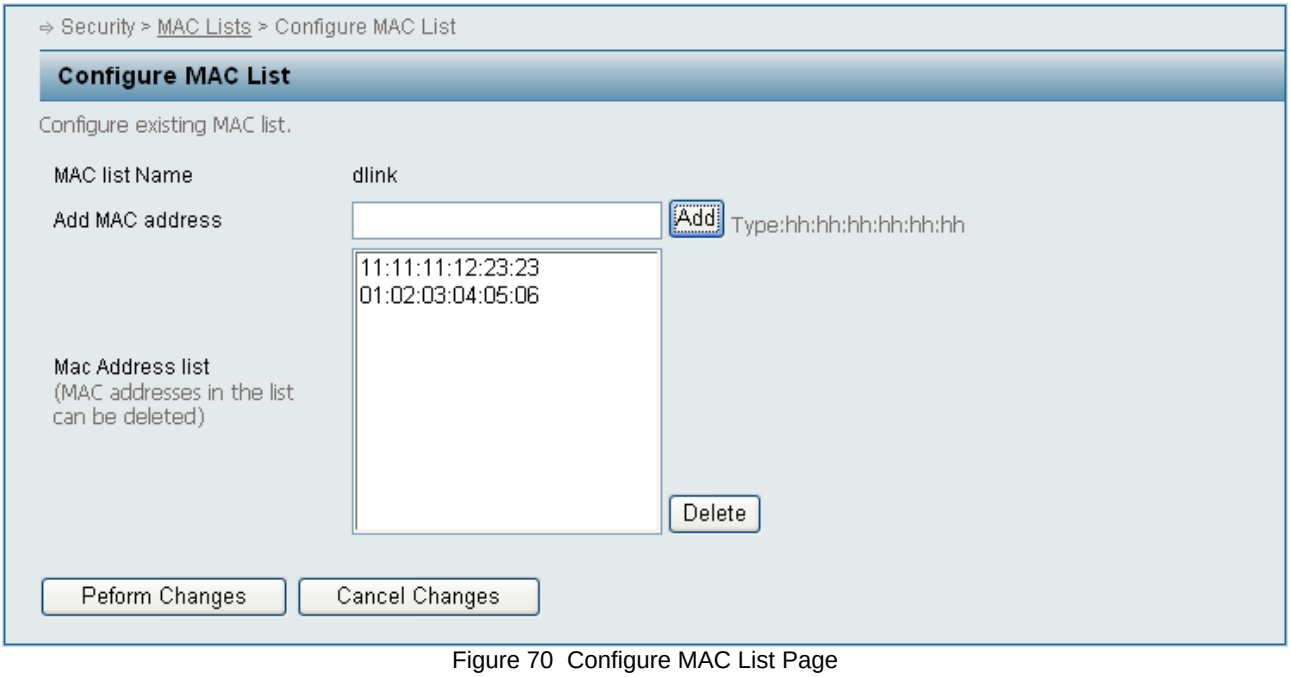


Figure 70 Configure MAC List Page

Deleting a MAC List

To delete a MAC list, check the box beside each list to be deleted, and click the “Delete” button. A confirmation dialog would appear. Click “Ok” to perform the deletion or click “Cancel” to cancel.

Figure 71 Deleting a MAC List

Selecting a MAC List for a BSS

After the MAC Lists are configured, one must select a MAC List for each BSS that needs to use MAC-based security. To perform this function, open the BSS configuration page and select "Advanced Settings" (**Error! Reference source not found.**72). In this page, specify the method of MAC-based access control and the name of the MAC List.

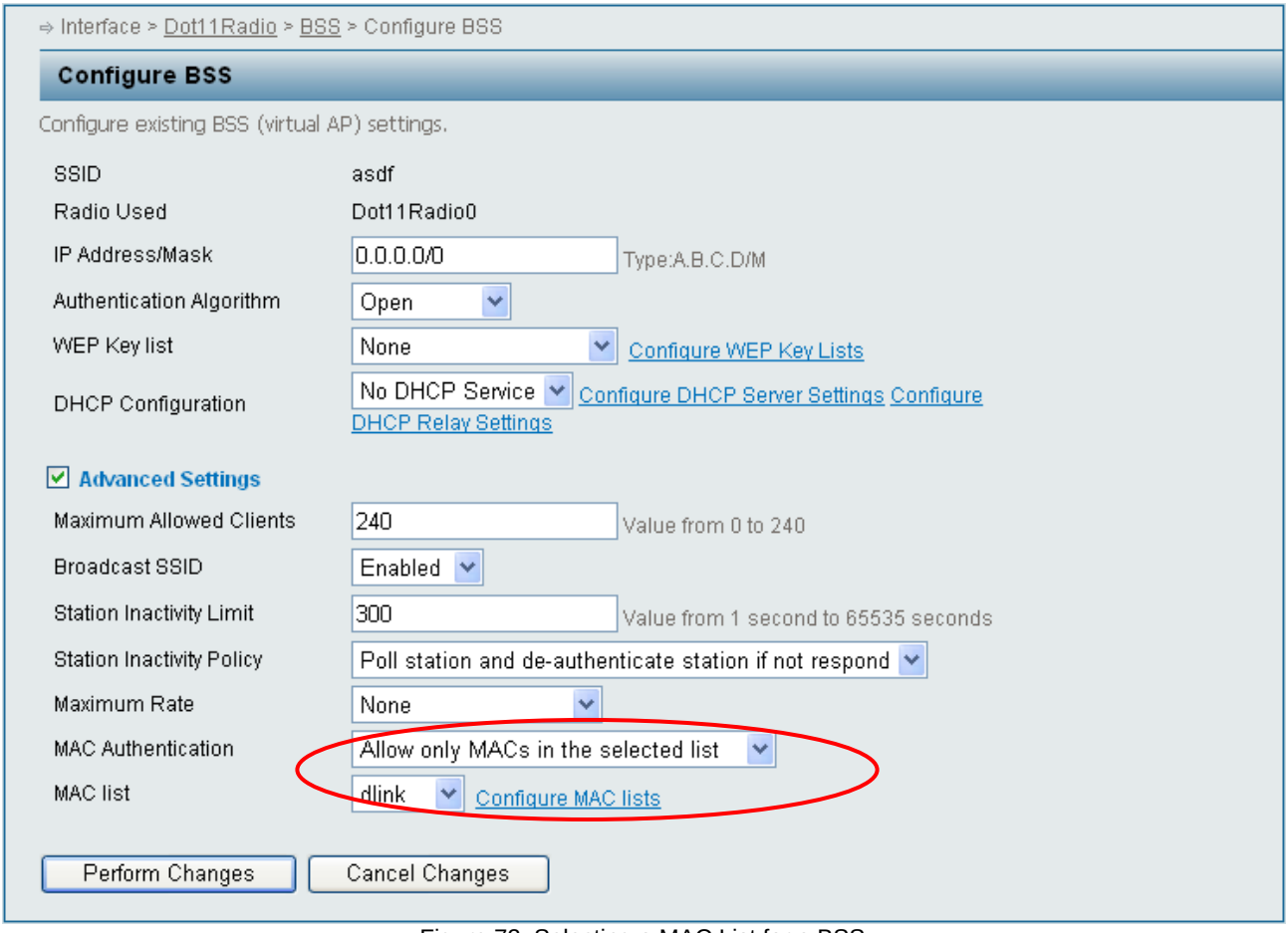


Figure 72 Selecting a MAC List for a BSS

There are two methods of using the MAC list:

- Allow only MACs in the selected list: this method would allow clients with MAC addresses that have been specified in the selected MAC list, while denying all other clients; i.e., use the MAC-list as an "accept list."

- Allow all MACs that are not in the selected list: this method would allow all clients except those that have been specified in the selected MAC list; i.e., use the MAC list as a “deny list”

Chapter 10 QoS Configuration

Quality of Service (QoS) is the advanced data traffic engineering and bandwidth control feature provided by DWR series mesh routers. This chapter describes how QoS can be configured using the Web-based Management Interface. For full information on QoS, please refer to the CLI Configuration Guide.

This chapter contains the following sections:

- QoS Configuration
- QoS Classes Configuration
- The Association of QoS Class and WDS

Configuring QoS

To enter the "QoS" configuration page, select "Quality of Service" from the left-side menu tree. The resulting page is shown in Figure 73

Figure 73 QoS Configuration Page

Similar to DDWR, QoS can be enabled or disabled by directly changing the "QoS Status" field. Select the required status and click the "Perform Changes" button, the system will prompt if the configuration is performed successfully as shown in Figure 74.

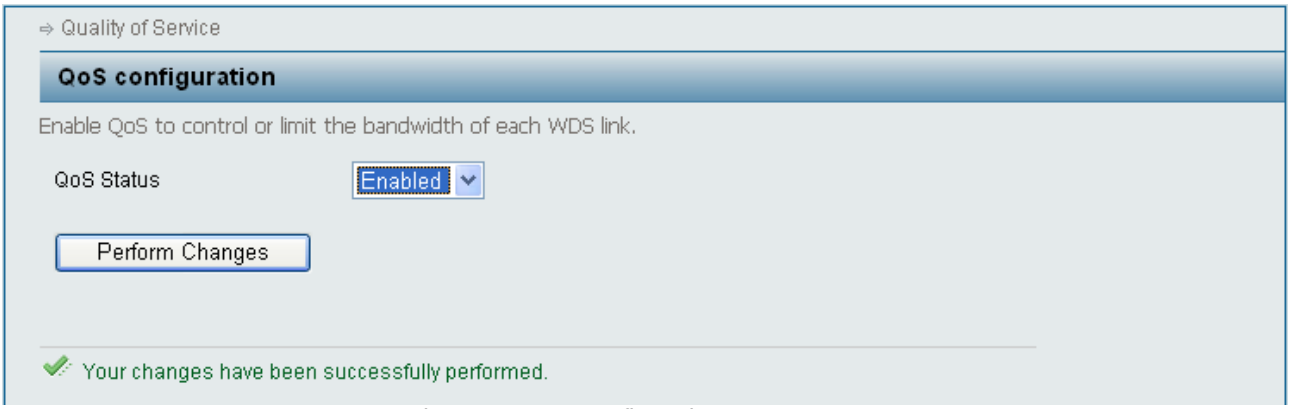


Figure 74 QoS Configuration Success Page

Configuring QoS Classes

A list of QoS Classes are also defined in the router (see Figure 75).

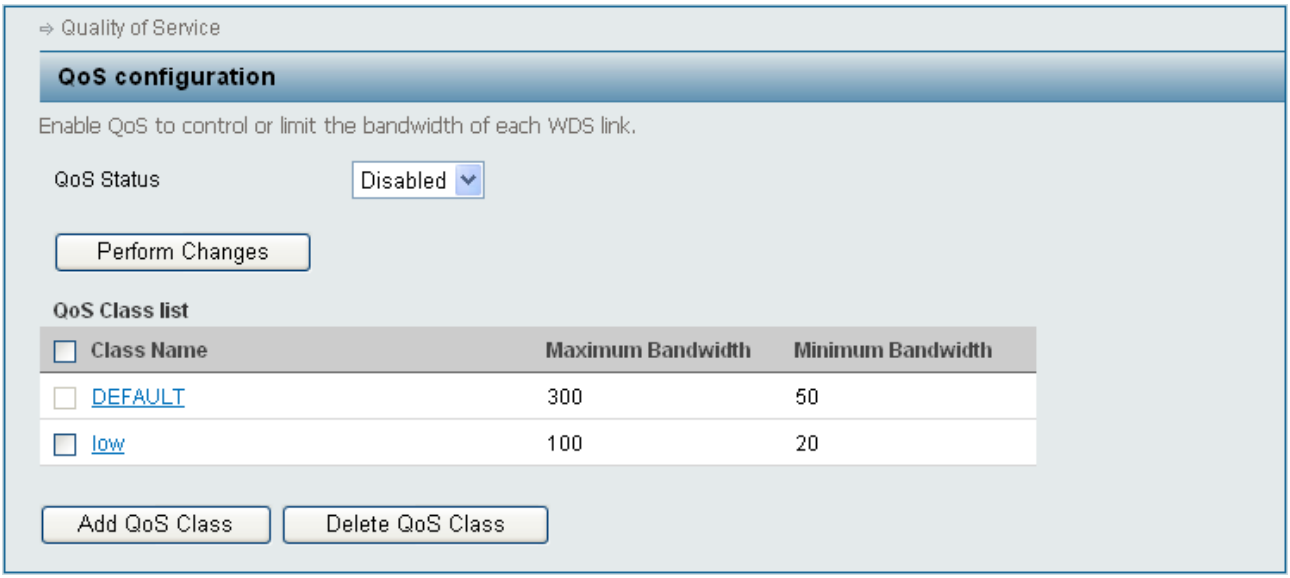


Figure 75 QoS Class List

Each QoS class describes a particular type of network traffic through the definition of the minimum and the maximum bandwidth. QoS class is the network default configuration, once it enabled, it can active automatically.

Adding a QoS Class

To add a QoS class, click the "Add QoS Class" button at the bottom of the list. The "Add new Class for QoS" page appears:

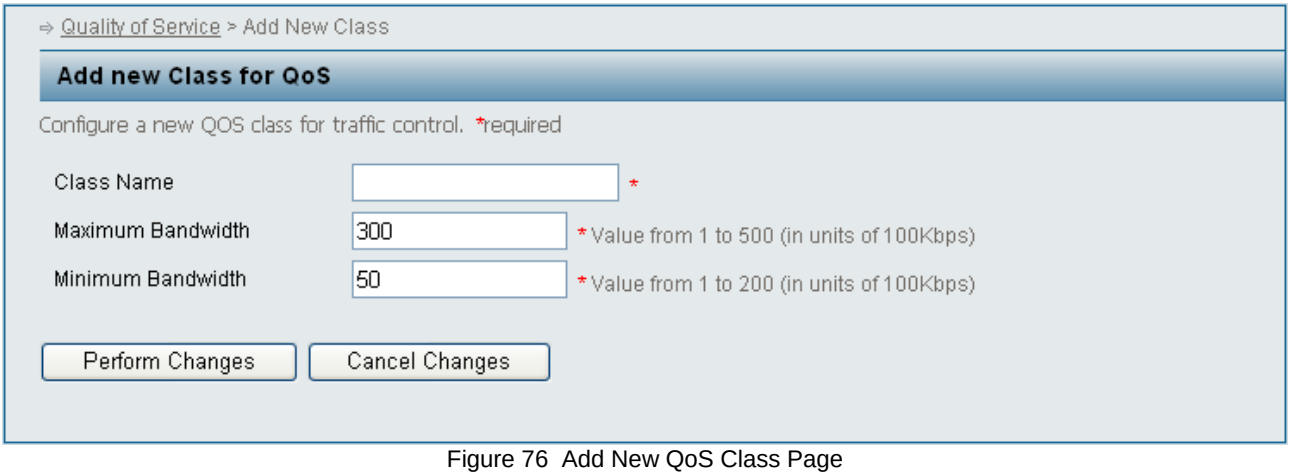


Figure 76 Add New QoS Class Page

The allowed maximum QoS class of DWR is 16.

Table 16 summarizes the QoS class settings.

Table 16 QoS Class Settings

Setting	Explanation	Default
Class Name	An alphanumeric name for the class; must start with a letter and not contain any spaces. ***This parameter cannot be changed after the QoS class is created.***	N/A
Maximum Bandwidth	The maximum bandwidth a traffic flow of the current class would be allowed to consume; entered in units of 100Kbps and the value may	300 (30Mbps)

	range from 1 to 200 (100Kbps to 50Mbps)	
Minimum Bandwidth	The minimum bandwidth a traffic flow of the current class will be allocated during congestion; entered in units of 100Kbps and the value may range from 1 to 500 (100Kbps to 50Mbps)	50 (5Mbps)

Deleting a QoS Class

To delete a QoS class, check the boxes beside each entry to be deleted, and click the “Delete” button. A confirmation dialog would appear. (Figure 77) Click “Ok” to perform the deletion, and click “Cancel” to cancel.

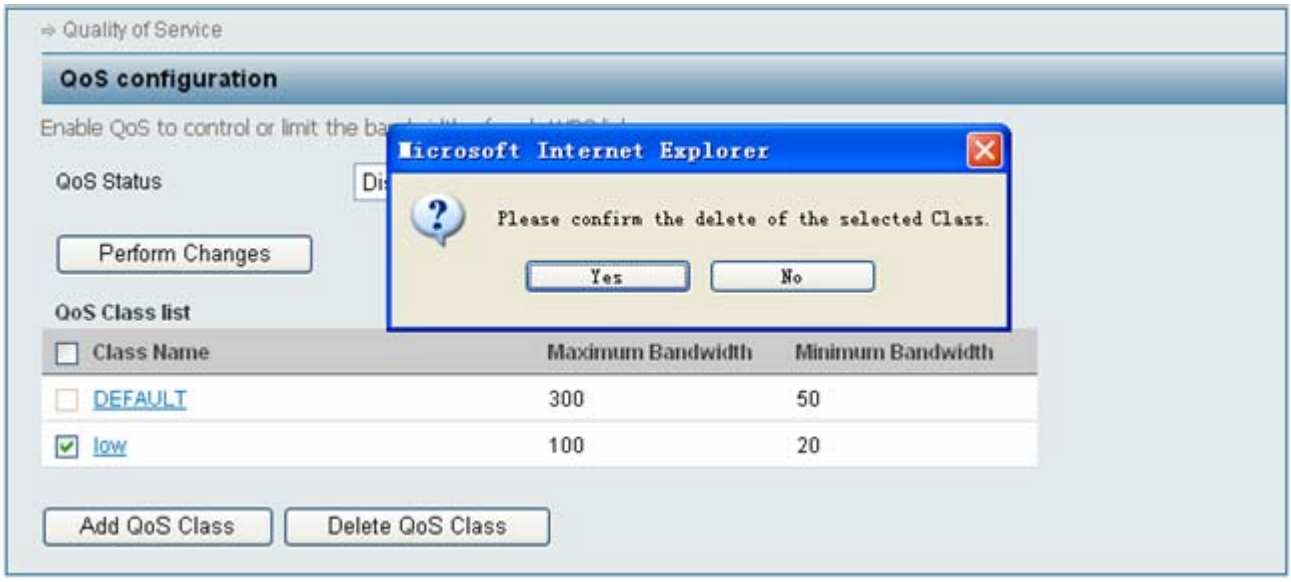


Figure 77 Deleting QoS Class

The Association of QoS Class and WDS

When QoS class configured, it takes effect after the association with WDS. One QoS class can associate with several WDS.

Chapter 11 SNMP Configuration

DWR series mesh routers all provide remote management through the popular Simple Network Management Protocol (SNMP). Using SNMP, network management products can read/write configuration and store data on the mesh routers. For more information on SNMP, please refer to the CLI Configuration Guide.

This chapter describes how SNMP service can be configured using the web-based management interface. It includes the following sections:

- Configuring SNMP Communities
- Configuring SNMP Trap Receivers
- Configuring SNMPv3 User Accounts

SNMP Communities

SNMP Communities is the basic authentication scheme used by SNMP v1 and v2. Each mesh router may have one or more community strings defined; each string can have an access-mode of read-only or read-write. When the router receives an SNMP command (which is usually a read or a write), it allows the operation if it matches a known community string with a matching access-mode.

For more information about SNMP Communities, please refer to the CLI Configuration Guide.

Configuring SNMP Communities

Select “SNMP” > “Communities” from the left-side menu tree to enter “SNMP Communities” configuration page. The result is shown in Figure 78. It displays all of the configured communities and their access-modes in a table.

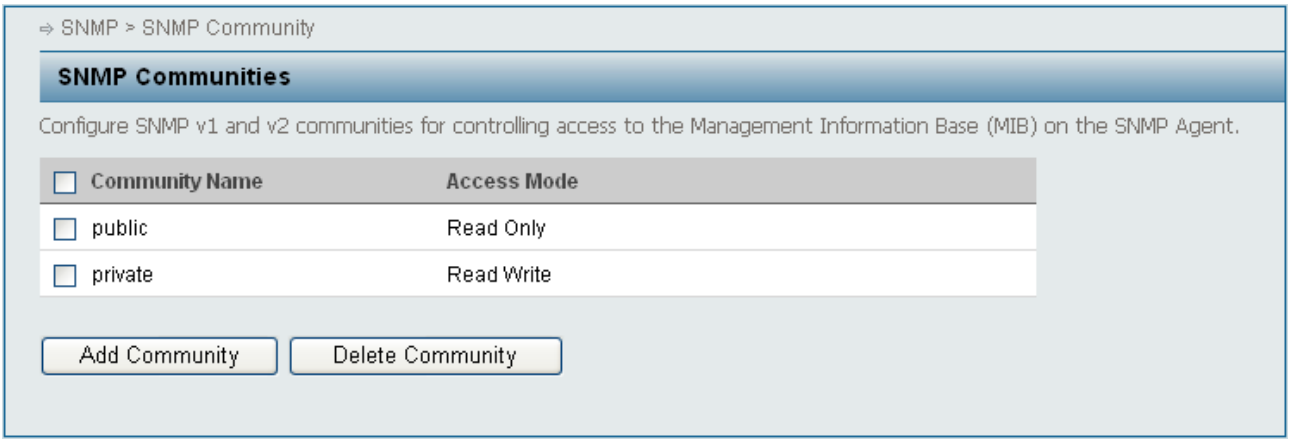


Figure 78 SNMP Communities Configuration Page

Adding a New Community

To add a community, click the “Add Community” button at the bottom of the table. The “Add New Community” page appears:

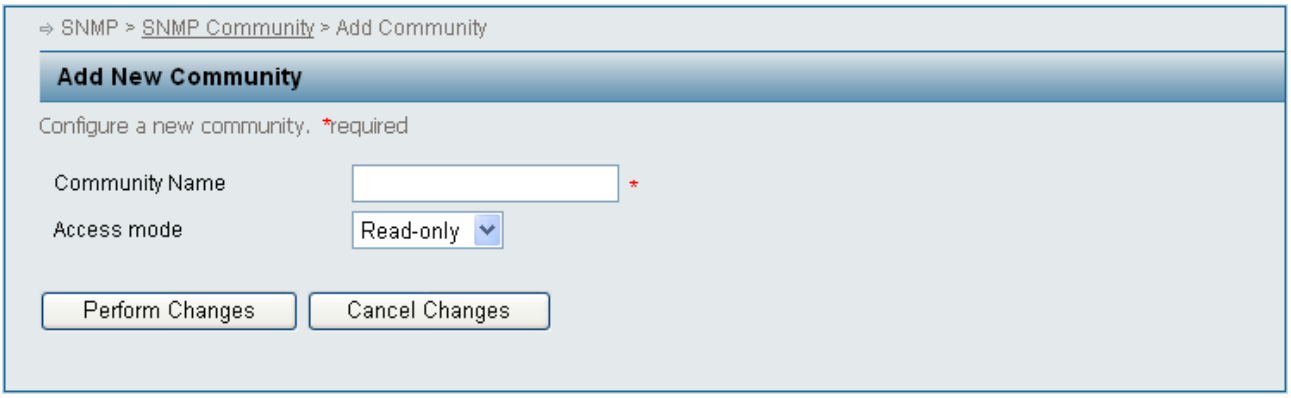


Figure 79 Add New Community Page

After specifying the community name (which must be an alphanumeric string that starts with a letter and has no spaces) and access mode in this page, add the community by clicking “Perform Changes” or cancel by clicking “Cancel Changes.” In either case, the user will be brought back to the community list page.

Deleting a Community

To delete a Community, check the boxes to be deleted beside each entry, and click the “Delete” button. A confirmation dialog would appear. Click “Ok” to perform the deletion or click “Cancel” to cancel.

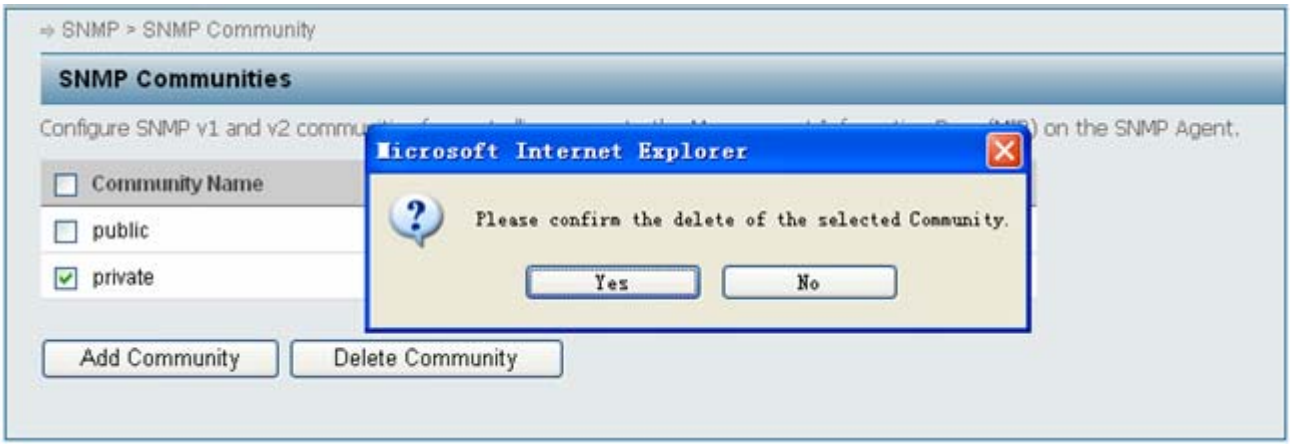


Figure 80 Deleting a Community

SNMP Trap Receivers

SNMP Trap Receivers are external hosts that receive the SNMP trap message sent by the DWR series mesh router. These receivers are generally Network Management Systems. Currently, only SNMPv1 trap messages are supported. Each mesh router may configure several receivers, each using a different trap community.

For more information about SNMP Trap Receivers, please refer to the CLI Configuration Guide.

Configuring SNMP Trap Receivers

Select “SNMP” > “Trap Receivers” from the left-side menu tree to open the “SNMP Trap Receivers”

configuration page. The result is shown in Figure 81. It displays all of the configured receivers with their ports and communities in a table.

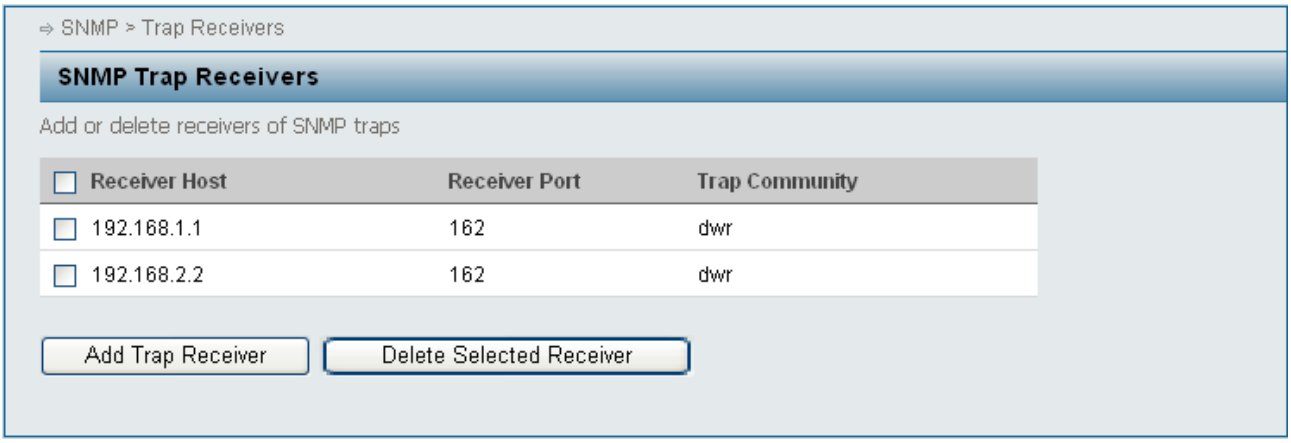


Figure 81 SNMP Trap Receivers Configuration Page

Adding a New Receiver

To add a receiver, click the "Add Trap Receiver" button at the bottom of the table. The "Add New Trap Receiver" page appears:

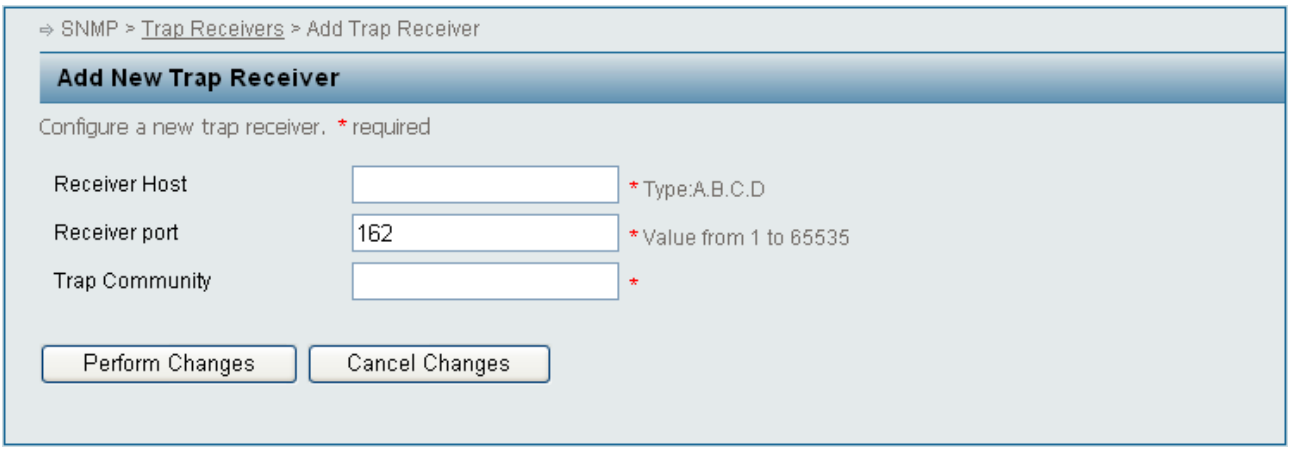


Figure 82 Add New Trap Receiver Page

Table 17 summarizes the settings for an SNMP Trap Receiver.

Table 17 SNMP Trap Receiver Settings

Setting	Explanation	Default
Receiver Host	The IP Address for the trap receiver. Example: 192.168.1.1	N/A
Receiver Port	The port number at which the trap receiver would receive the trap messages.	162
Trap Community	The community string for the trap messages sent to this receiver. The community must be alphanumeric, starting with a letter, and contain no spaces. Example: routertrap	N/A

After specifying the trap receiver settings in this page, add the receiver by clicking “Perform Changes” or cancel by clicking “Cancel Changes.” In either case, the user will be brought back to the trap receiver list page.

Deleting a Trap Receiver

To delete a trap receiver, check the boxes beside each receiver to be deleted, and click the “Delete” button. A confirmation dialog would appear. Click “Ok” to perform the deletion or click “Cancel” to cancel.

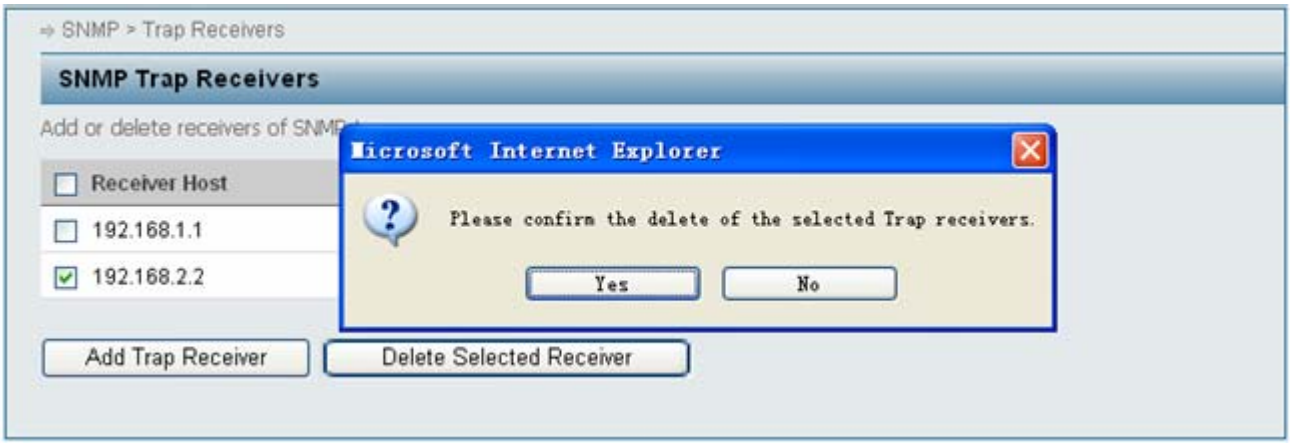


Figure 83 Deleting a Trap Receiver

SNMP v3 Users

SNMPv3 introduced the concept of user accounts along with strong encryption and authentication methods. DWR series mesh routers support SNMPv3 and allows the configuration of multiple SNMPv3 users, each with different access rights as well as authentication and encryption methods.

For more information about SNMPv3 users, please refer to the CLI Configuration Guide.

Configuring SNMPv3 Users

Choose “SNMP” > “V3 Users” from the left-side menu tree to open the “SNMPv3 Users” configuration page. The page is shown in Figure 84. It displays all of the configured v3 users and their information.

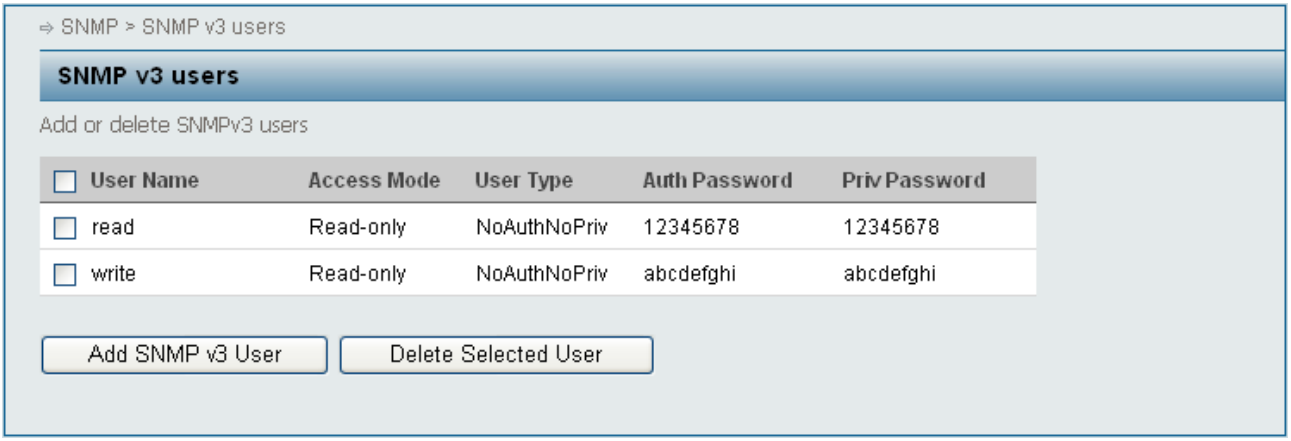


Figure 84 SNMPv3 Users Configuration Page

Adding a New v3 User

To add a receiver, click the “Add SNMPv3 User” button at the bottom of the table. The “Add New SNMPv3 User” page appears (Figure 85)

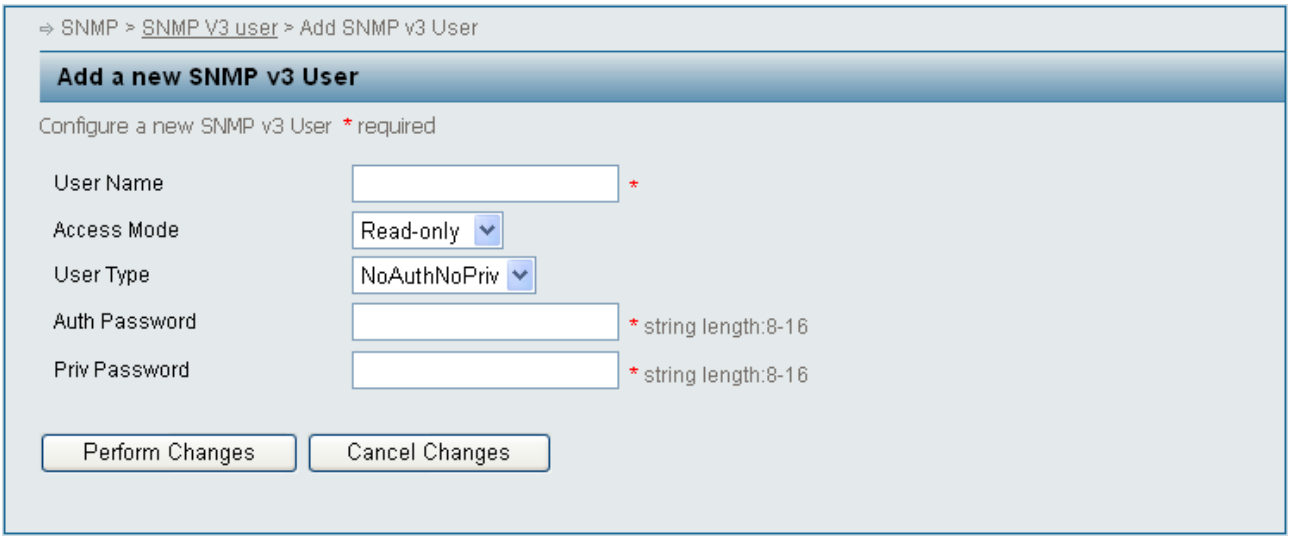


Figure 85 Add New Trap Receiver Page

Table 18 summarizes the settings for a SNMPv3 user

Table 18 SNMPv3 User Settings

Setting	Explanation	Default
User Name	The SNMPv3 User Name; must be an alphanumeric string, start with a letter, and contain no spaces. Example: read123	N/A
Access Mode	Can be Read-only or Read-write Read-only: the user may retrieve information from the router MIB, but not change it Read-write: the user may both retrieve and change information in the router MIB.	Read-only
User Type	The authentication and encryption methods used by this v3 user; can be NoAuthNoPriv, AuthNoPriv, or AuthPriv. NoAuthNoPriv: No secure authentication or encryption AuthNoPriv: Use secure authentication, but do not use encryption. AuthPriv: Use both secure authentication and encryption	NoAuthNoPriv
Auth Password	The authentication password used for AuthNoPriv and AuthPriv users. Must be an alphanumeric string between 8 and 16 characters long. Example: a1a2a3a4a5	N/A
Priv Password	The encryption password used for AuthPriv users. Must be an alphanumeric string between 8 and 16 characters long. Example: a1a2a3a4a5	N/A

After specifying the v3 user settings in this page, add the user by clicking “Perform Changes” or cancel by clicking “Cancel Changes.” In either case, the SNMPv3 user configuration page will be displayed.

Deleting an SNMPv3 User

To delete a SNMPv3 User, check the boxes to be deleted beside each user, and click the “Delete” button. A confirmation dialog would appear. Click “Ok” to perform the deletion or click “Cancel” to cancel.

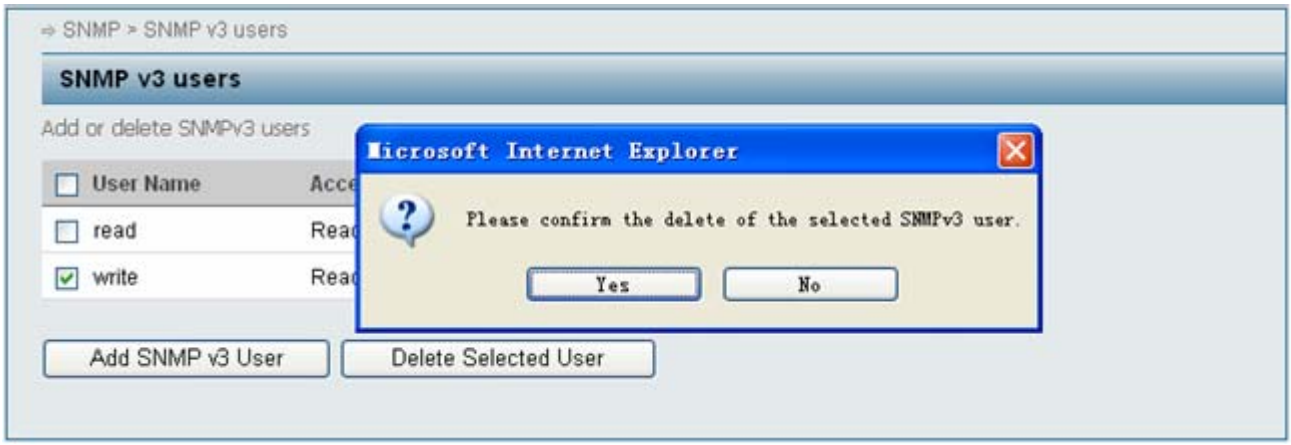


Figure 86 Deleting a SNMPv3 User

Chapter 12 Other Maintenance

This chapter describes other maintenance tasks that do not involve changing configuration on the router, such as saving configuration, rebooting the router, and upgrading the router. It includes the following sections:

- Saving Configuration
- Rebooting
- Upgrading Router Images

Saving Configuration

Configuration changes such as the ones described in the earlier chapters only affect the "running configuration;" i.e., they only take effect while the router is running, and will be lost once the router is powered off or rebooted. To make configuration changes persistent (i.e. store them in the "startup configuration3"), one can use the "Save" button located beneath the menu tree of the Web-based Management Interface.

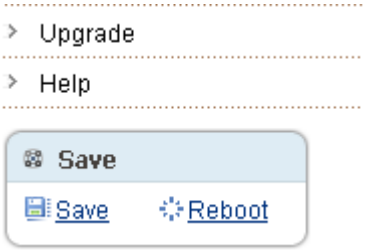


Figure 87 The Save Function

To save the current running configuration, click on "Save." A dialog box appears to ask for confirmation. Select "OK" to save, or select "Cancel" to cancel.

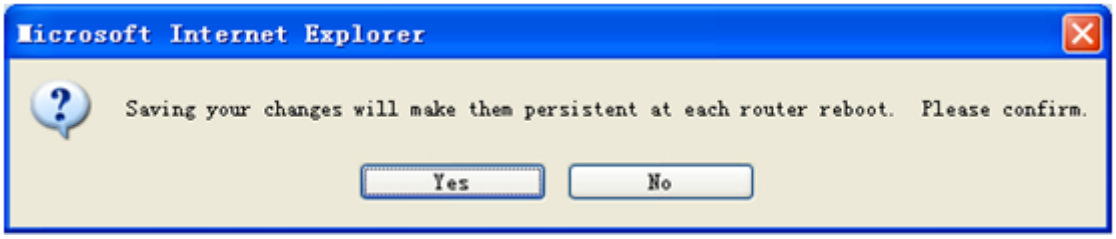
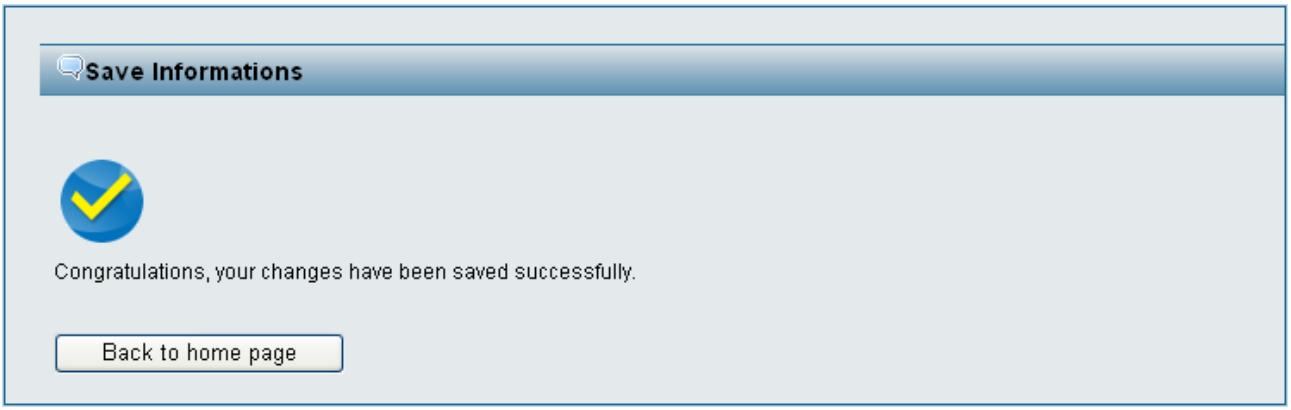


Figure 88 Saving Configuration

[3] For more information about running configuration and startup configuration, see the Configuration Guide.

If confirmed and the save is successful, the following page is displayed:



Rebooting the Router

Some configuration changes (such as the Node ID) do not take effect until it is saved to the startup configuration and the router is rebooted. To reboot the router, click on “Reboot” next to the “Save” located beneath the menu tree of the Web-based Management Interface (Figure 89) A dialog box appears to ask for confirmation. Select “OK” to reboot the router immediately, or select “Cancel” to cancel.

Figure 89 Reboot the Router

If confirmed, the router will reboot.

Upgrading the Router Image

DWR series mesh routers can be easily upgraded by downloading an updated software image file and upgrading a router’s on-board software with it. To upgrade the router, click on the menu tree item “Software Upgrade” to open the “Software Image Upgrade” page.

In this page, the user may select the method of downloading the software image file, the location of the image file, and initiate the upgrade. The WMI supports two methods of downloading the software image file, URL and FTP. Figure 90 shows the software image upgrade page with the “Download from URL” method selected, while Figure 91 shows it with the “Download from FTP Server” method.

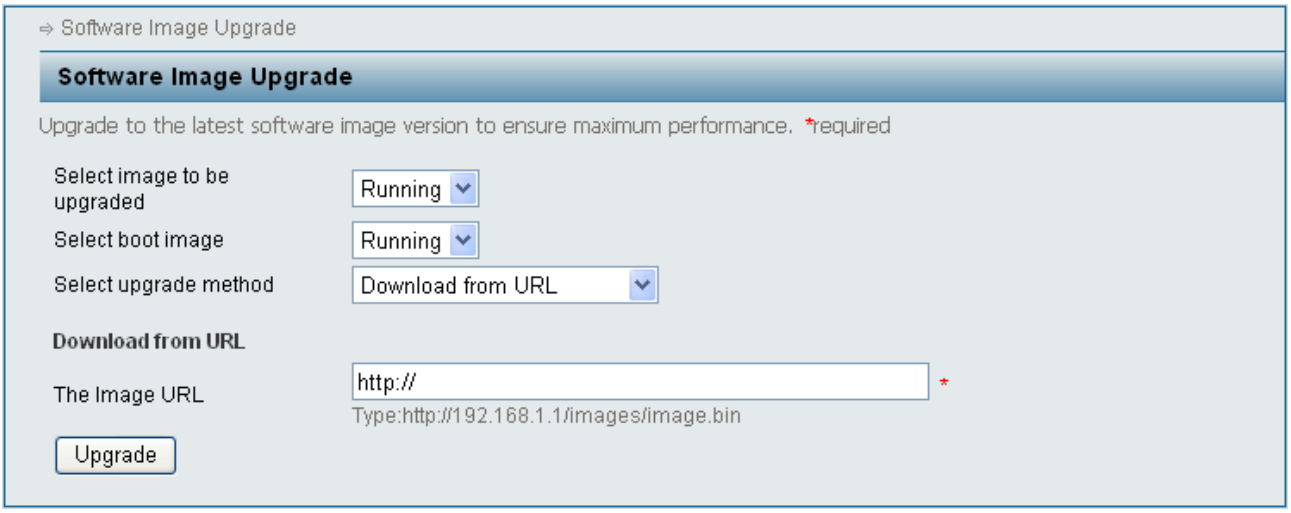


Figure 90 Software Image Upgrade using URL

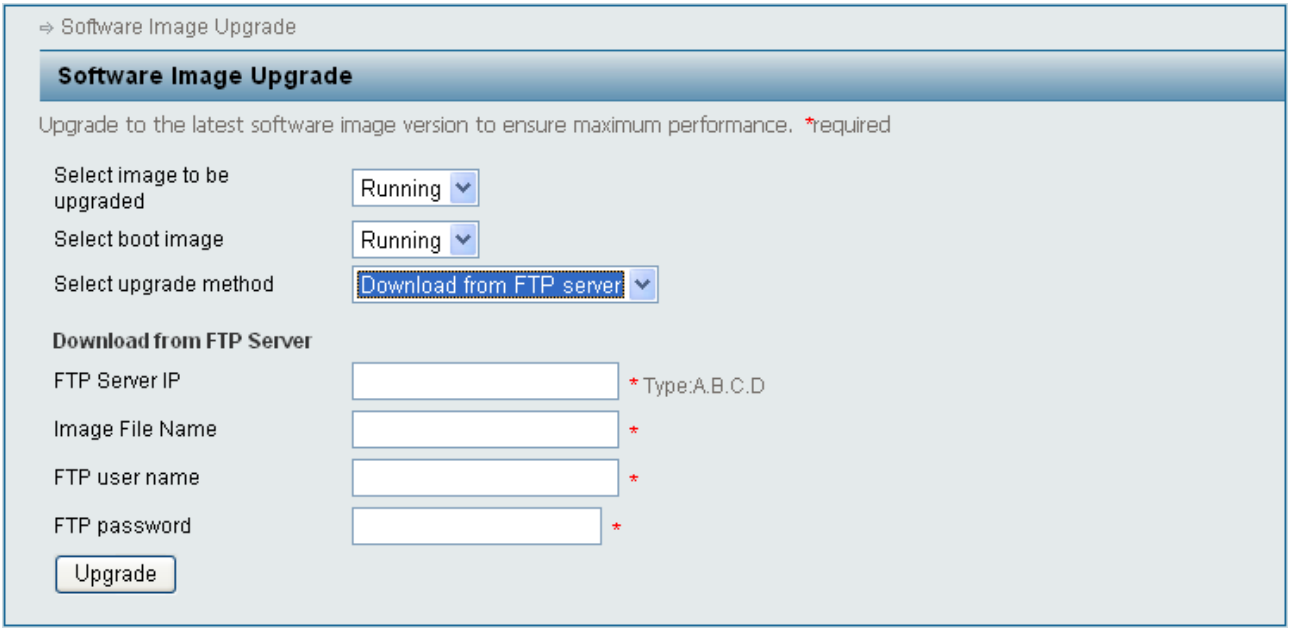


Figure 91 Software Image Upgrade using an FTP server

Table 19 summarizes the settings in the software image upgrade page.

Table 19 Software Image Upgrade Settings

Setting	Explanation	Default
Select image to be upgrade	Choose which image to be upgraded. Running: the image that is currently loaded and running Inactive: the image that is not currently loaded and running	Running
Select boot image	Choose which image to be run after rebooting	Running
Required Setting for the "Download from URL" method		
Image URL	The URL of the image file. Example: http://192.168.1.1/imagefile/image.bin ***This option is only applicable to, and only appears for, the "Download from URL" upgrade method. It is highly recommended that an IP address to be used in the URL.***	N/A

Required Settings for the “Download from FTP Server” method		
FTP Server IP	The IP address of the FTP server holding the image file Example: 192.168.1.1	N/A
Image File Name	The full FTP server path to the image file. Example: /imagefile/image.bin	N/A
FTP User Name	The user name for logging into the FTP server. Example: anonymous	N/A
FTP Password	The password for logging into the FTP server. Example: admin@dwrnet.com	N/A

After specifying the upgrade method and the download settings, click “Upgrade” to download the image file and upgrade the router. During the upgrade, the message “upgrading, please wait!” appears and the WMI is temporarily disabled (Figure 92).

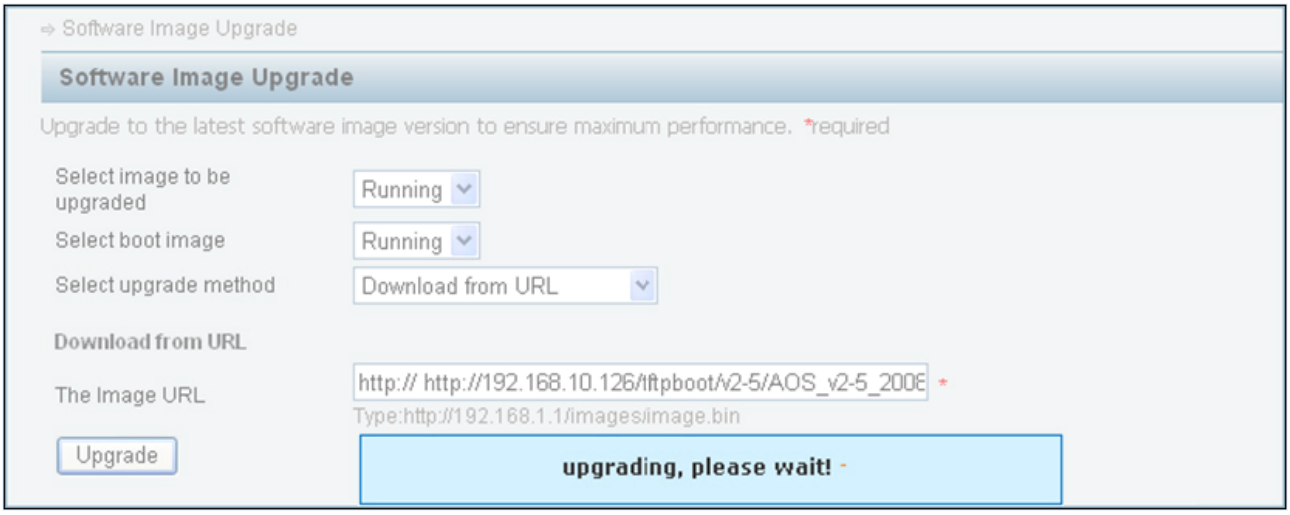


Figure 92 Software Image Upgrade In Progress

The upgrade process can last several minutes. After the upgrading is successfully completed, the page in Figure 93 is displayed. The router must then be rebooted to run the new image.

NOTE: It is highly recommended that the running configuration be saved before rebooting the router, otherwise any unsaved configuration changes made since the last boot would be lost.

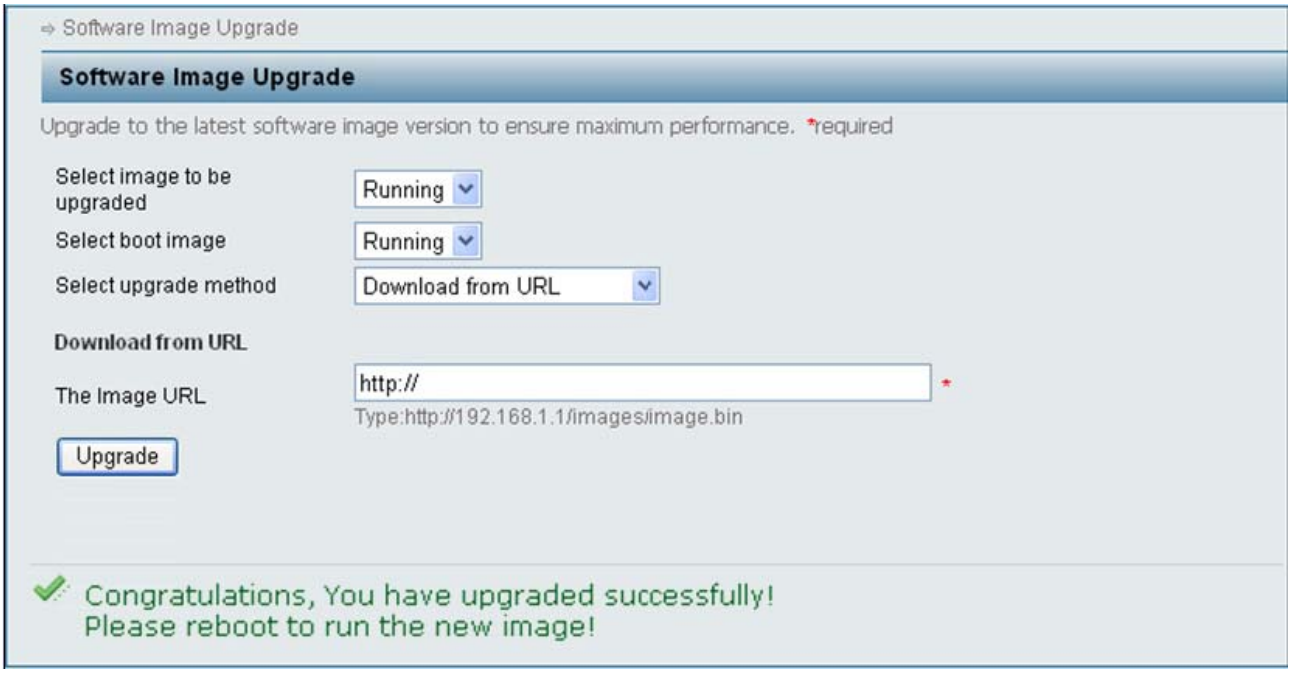


Figure 93 Software Image Upgrade Successful