

HP R100-Series Wireless VPN Routers Configuration and Administration Guide

HP Part Number: 5998-5394
Published: September 2014
Edition: 1



© Copyright 2014 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

Microsoft® and Windows® are U.S. trademarks of the Microsoft group of companies. Google Chrome™ browser is a trademark of Google Inc.

Warranty

WARRANTY STATEMENT: See the warranty information sheet provided in the product box and available online.

Contents

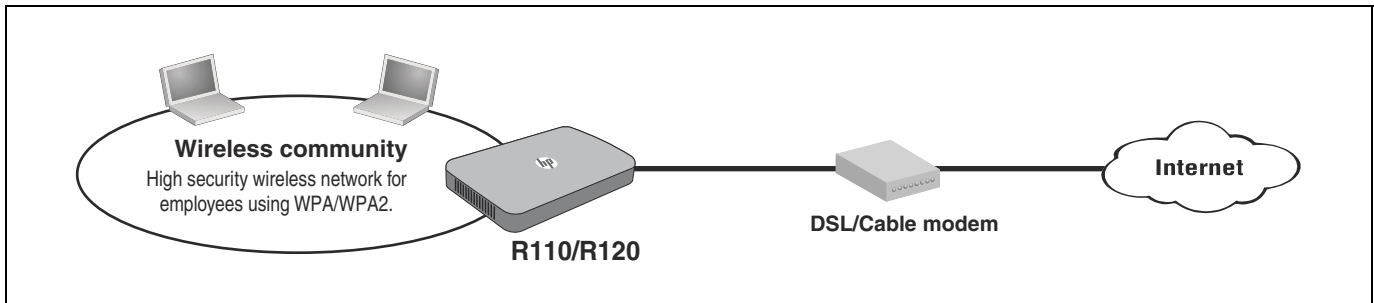
1 Deploying the HP R110/R120	7
2 Using the Wizard Setup	11
Overview	11
Automatically running the Wizard Setup the first time you log in	11
Accessing the Wizard Setup after your first login	11
Wizard Setup	11
Step 1: Specify system time settings	11
Step 2: Specify WAN settings	12
Step 3: Specify wireless settings.....	15
Step 4: Summary.....	20
3 Managing the HP R110/R120 system.....	23
Viewing the router status	23
Setting the HP R110/R120 mode	24
General administration settings.....	25
System information (General) settings	25
Administrator login credentials	25
Setting the Country Code.....	25
Configuring web server settings	25
Configuring trusted users.....	26
System time settings.....	26
Set system time	27
Daylight saving	28
Configuring SNMP.....	28
Managing system logs.....	29
Events	30
Proxy ARP settings.....	31
Rebooting the router.....	33
Viewing traffic statistics	33
4 WAN configuration	35
Viewing the WAN interface status	35
Settings	36
DHCP IP address	36
Static IP address	36
PPPoE.....	37
PPTP.....	39
L2TP	40
DDNS	41
MAC clone	42
5 LAN configuration	43
Viewing the LAN interface status.....	43
LAN Settings	44
Default VLAN settings.....	44
DHCP relay.....	46
Spanning Tree.....	46

DHCP client list.....	47
VLAN settings.....	47
IGMP settings.....	49
6 Wireless configuration	51
Viewing wireless interface status	51
Basic wireless settings.....	52
Configuring virtual access point interfaces.....	55
Configuring wireless security	56
Advanced wireless settings.....	64
WDS settings	66
WPS settings	67
WMM settings	68
MAC authentication settings.....	70
Viewing the client list.....	71
7 VPN configuration	73
Viewing VPN status.....	73
VPN settings	74
IPSec settings	74
L2TP over IPSec settings	77
PPTP settings	78
VPN passthrough settings.....	79
8 Routing configuration	81
Viewing routing status.....	81
Viewing the IPv4 routing table	82
IPv4 Dynamic route settings.....	83
IPv4 Static route settings	84
Viewing the IPv6 routing table	85
IPv6 Dynamic route settings.....	86
IPv6 Static route settings	86
9 Firewall configuration	89
Viewing the firewall status	89
Security settings.....	90
Client filtering.....	92
MAC filtering	93
URL filtering.....	94
Content filtering	95
SPI settings.....	95
10 NAT configuration	99
Viewing NAT status	99
NAT settings.....	100
Virtual server settings.....	100
DMZ settings.....	102
ALG settings.....	103
Port trigger settings.....	103
11 IPv6 configuration	105
Viewing IPv6 status	105
IPv6 settings.....	106
Static IPv6	106
SLAAC	108
DHCPv6	109
PPPoE.....	110

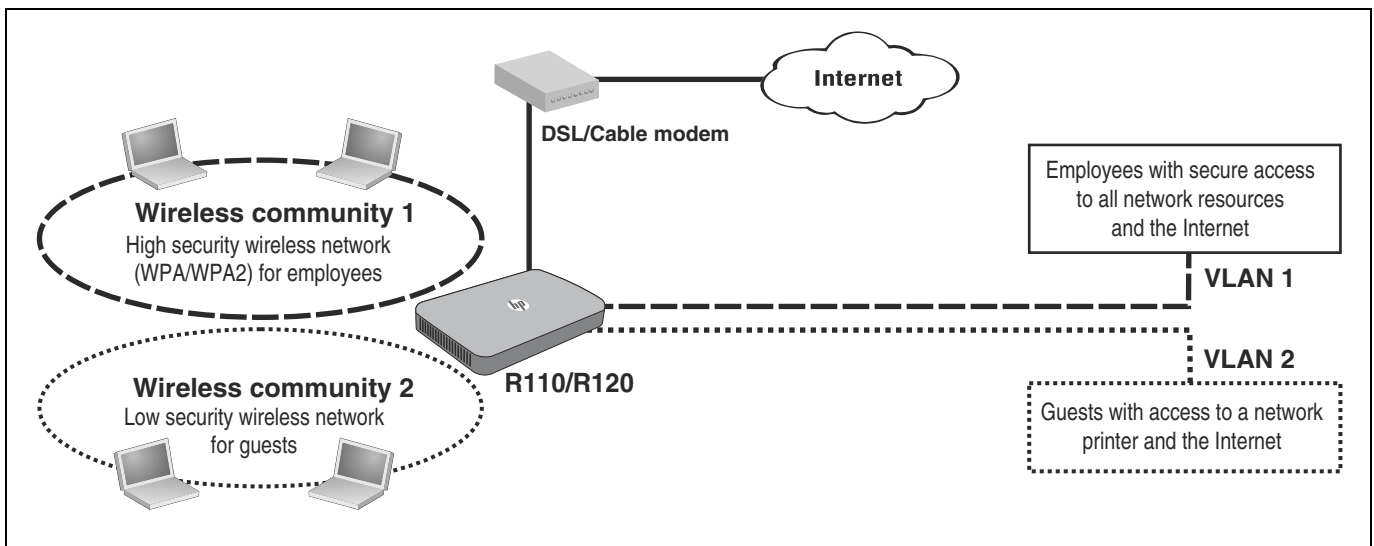
DHCPv6 client list	111
MLD settings	112
12 QoS configuration	113
Viewing QoS status	113
Traffic shaping	114
Traffic mapping	115
13 USB configuration	117
User Account	117
File Sharing settings	118
FTP settings	119
Safe removal	120
14 Tools	121
Viewing tools status	121
Updating software	121
Saving configuration settings	122
Ping	124
Nslookup	125
Traceroute	125
Email alert	126
Scheduling	128
Support file	129
Viewing the EULA	129
15 Support and other resources	131
Online documentation	131
Contacting HP	131
HP websites	131
Conventions	132
A Resetting to factory defaults	133
Factory reset procedures	133
Using the reset button	133
Using the management interface	133
B Factory default settings	135

1 Deploying the HP R110/R120

In a small office, the HP R110/R120 can be directly connected to a broadband modem (DSL or cable) to provide secure wireless networking for all employees. In the following scenario, employees can share data and resources with each other and access the Internet at the same time:



With its wireless community feature, the R110 can be configured to provide up to four separate wireless networks (all on the same wireless channel), and the R120 up to eight wireless networks (split between two radios), each with its own configuration settings for security, VLAN support, and more.

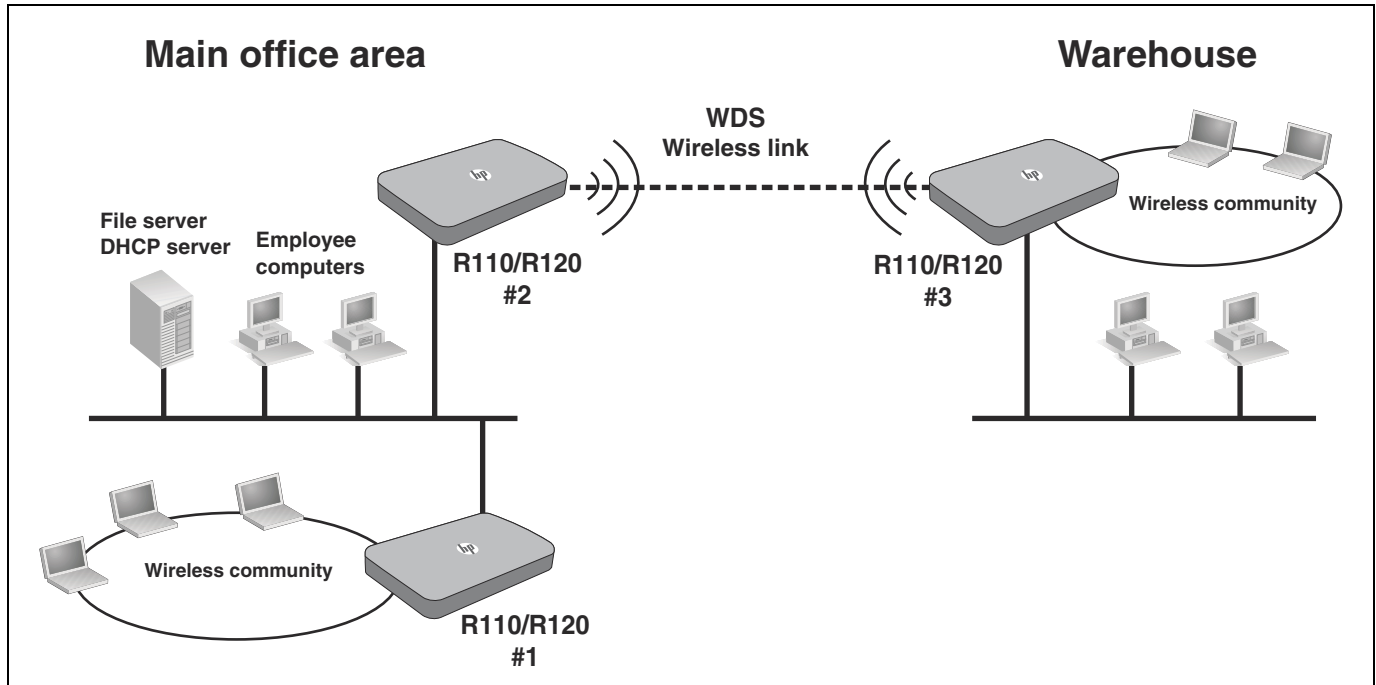


In this scenario, employees connect to wireless community 1, which is protected with WPA/WPA2. All employee traffic exits the HP R110/R120 on VLAN 1, providing access to private resources on the company network and on the Internet.

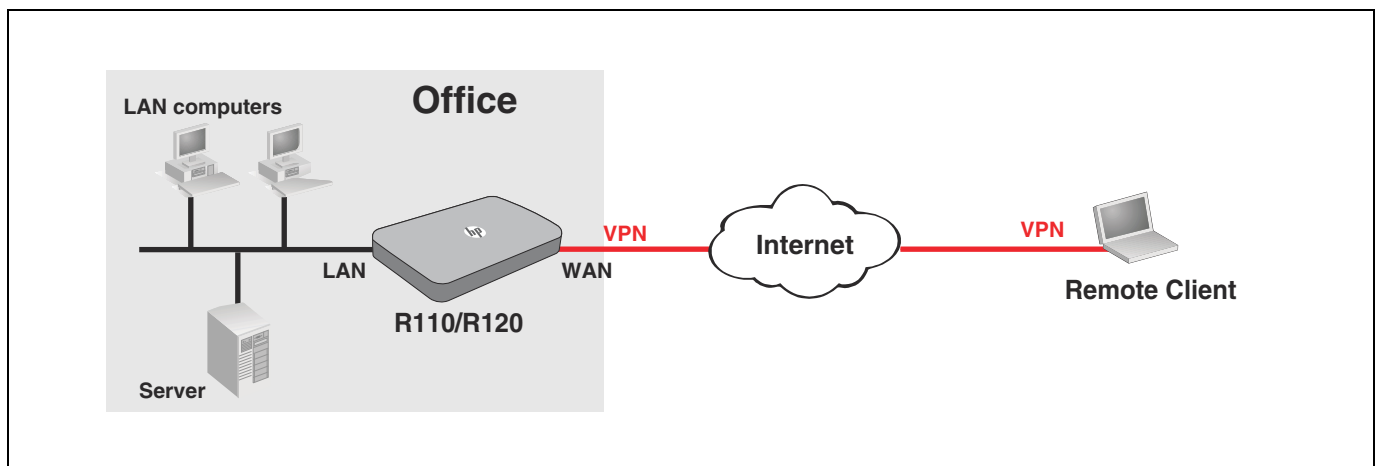
Guests connect to wireless community 2, which is protected with WEP. All guest traffic exits the HP R110/R120 on VLAN 2, providing access only to the Internet.

For offices that need Ethernet ports for wired connectivity, the R110/R120 has a built-in 4-port Gigabit switch. It can also be used to extend the reach of the network to areas that are difficult or impossible to reach with traditional cabling.

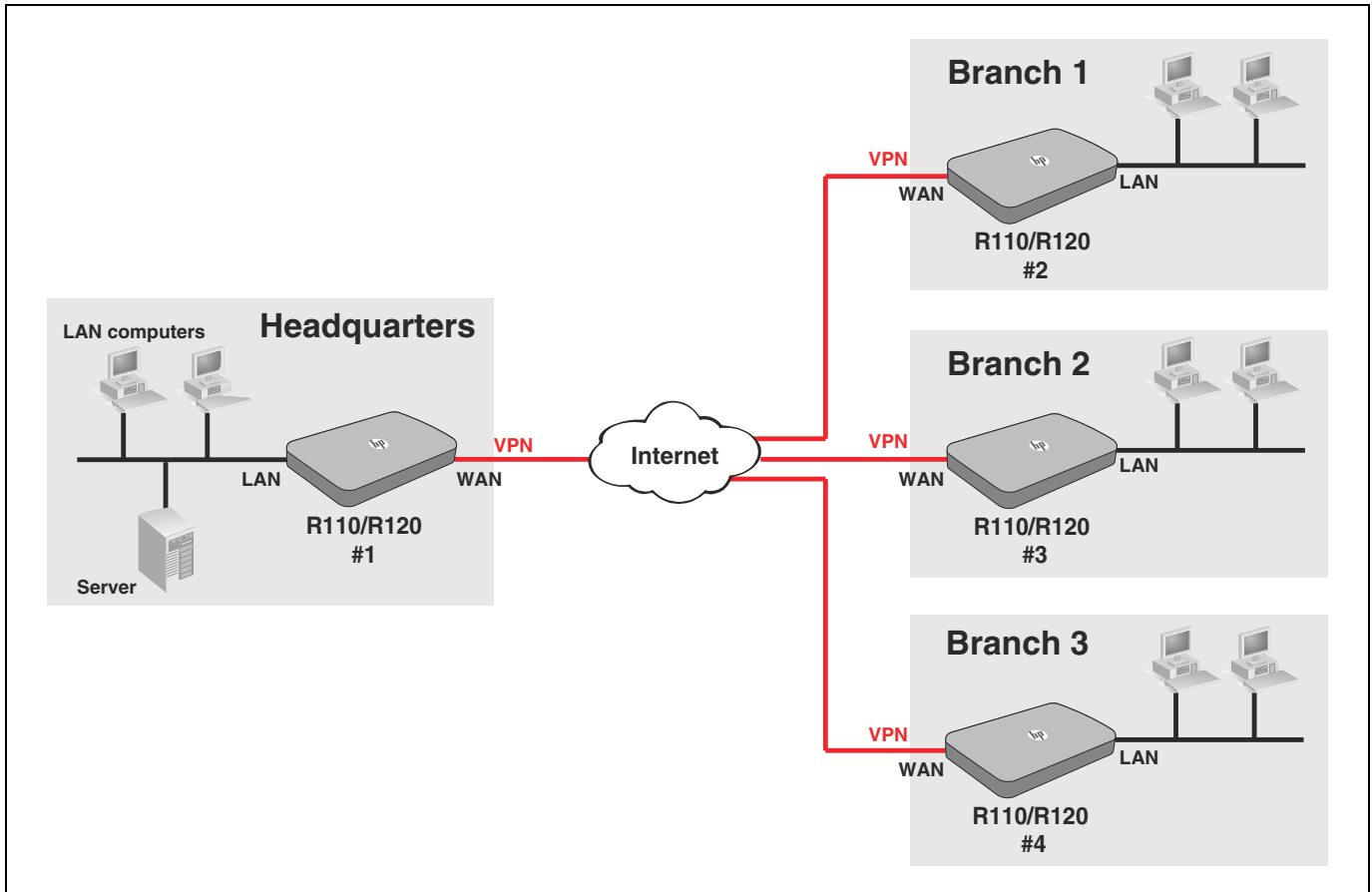
In the following scenario, HP R110/R120 #1 provides wireless network services to the employees in the main office, while HP R110/R120 #2 and HP R110/R120 #3 use the Wireless Distribution System (WDS) to create a wireless link between the main office network and a small network in a warehouse. WDS eliminates the need to run cabling, allowing for fast and easy deployment.



In the following scenario, an HP R110/R120 located in an office provides a virtual private network (VPN) connection across the Internet to a remote client (typically a mobile worker). The R110/R120 forms secure VPN (IPSec, PPTP, L2TP/IPSec) tunnel connection to the client, which can then access the computers and servers in the office network. The remote client can be a Windows or Mac computer, or any Apple iOS or Android mobile device.



In the following scenario, four HP R110/R120s provide a virtual private network (VPN) across the Internet between a headquarters and three branch offices. The R110/R120 #1 forms secure VPN tunnel connections to R110/R120 #2, R110/R120 #3, and R110/R120 #4 at three branch locations. The computers on each branch network can access the computers and servers on the headquarters network.



2 Using the Wizard Setup

Overview

The Wizard Setup provides an easy way to quickly configure basic settings on the R110/R120 and make the router operational.

Automatically running the Wizard Setup the first time you log in

The first time you log in to the management interface (see the *HP R100-Series Wireless VPN Routers Quickstart* for first time login procedure), the HP end user license agreement displays. When you accept the agreement, a page displays to enable you to select your country so that wireless radio settings are configured appropriately. Select the country in which the router is operating, and then click **Save**. The first page in the Wizard Setup appears.

Accessing the Wizard Setup after your first login

When you log in subsequent to completing or cancelling out of the Wizard Setup, the *System Status* page displays by default.

See also the *HP R100-Series Wireless VPN Routers Quickstart*, which describes the configuration procedure for a basic wireless network.

Wizard Setup

To start the Wizard Setup, select **Home > Wizard Setup**, and then click **Start**:

Step 1: Specify system time settings

The router keeps time by connecting to a Network Time Protocol (NTP) server. This enables the router to synchronize the system clock to the global Internet. The synchronized clock in the router is used to record the system log and control client filtering. Select the time zone that you reside in. The system clock may not update immediately. The router updates the current time after it has made contact with time servers on the Internet and received a response. Alternatively, the system clock can be entered manually or imported from the host computer (copies the system time from the management computer).

Select to configure the system time manually or have it automatically configured by an NTP server. You can also enable support for daylight savings time, if required for your location

This page includes the following settings:

Set system time

- **NTP:** Enables the router to use NTP to synchronize the system clock to global Internet time, or allows the time to be set manually.
- **Current System Time:** Displays the current time setting of the router.
- **Time Server Address:** The IP address or name of an NTP server.
- **Set Time Zone:** The local time zone where the router is installed.

Daylight saving

- **Enable:** Enables daylight saving for the system time. The router automatically sets daylight saving start and end dates based on the time zone selected.
- **Manually Set Time For Daylight Savings:** Sets the dates for starting and ending the daylight saving.

Step 2: Specify WAN settings

The Internet Connection page allows you to set up the router for the type of Internet connection you have. Before setting up your connection type, have your account information from your ISP ready.

DHCP IP Address

A dynamic connection type is the most common method used with cable modems. In many cases, setting the connection type to dynamic is enough to complete the connection to your ISP. Some dynamic connection types may require a Host Name. Enter the Host Name in the space provided if you were assigned one by your ISP (do not use characters ` ` " & ' # \). Some dynamic connections may require that you clone the MAC address of the PC that was originally connected to the modem. To do so, click **WAN** on the main menu and then **MAC Clone** to set the WAN MAC address.

Static IP Address

The Static IP addresses mode sets the router to operate with a fixed IP address to connect to the Internet. If your ISP uses static IP addressing, you need an IP address, subnet mask, and ISP gateway address. This information is available from your ISP or on the paperwork that your ISP left with you. Enter your information in the provided spaces, and then click **Next**.

PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) is a common WAN protocol that provides a secure “tunnel” connection between the service provider and the local network.

Enter the PPPoE information in the provided spaces, and then click **Next** to activate your settings.

- **Username:** Enter your ISP-assigned user name. (Do not use characters ` ` & ' # \)
- **Password:** Enter your password (usually assigned by your ISP). (Do not use characters ` ` & ' # \)
- **Confirm Password:** Confirm the password.

PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a common WAN protocol used for Virtual Private Networks (VPNs) that provides a secure “tunnel” connection between the service provider and the local network.

L2TP

The Layer 2 Tunneling Protocol (L2TP) is a common WAN protocol used for Virtual Private Networks (VPNs) that provides a secure “tunnel” connection between the service provider and the local network.

Step 3: Specify wireless settings

The R110 router supports a dual-band single radio for 2.4 GHz or 5 GHz operation. The R120 router supports two radios, one for 2.4 GHz and one for 5 GHz. This means that the R110 can operate at 2.4 GHz or 5 GHz, but not both at the same time. The R120 can operate concurrently at 2.4 GHz and 5 GHz.

Therefore, the wireless settings differ for the R110 and R120 routers. The R110 router has a single configuration page for 2.4 GHz or 5 GHz operation. The R120 router includes separate configuration pages for 2.4 GHz and 5 GHz operation.

Enable Radio

Enables the 2.4 GHz or 5 GHz wireless section of your LAN. When disabled, no wireless computers can gain access to either the Internet or other computers on your wired or wireless LAN.

Configure the radio band and mode

Radio Band

(Applies to HP R110 only) Allows you to select the band of your wireless network. The R110 router can operate in the 2.4 GHz band (for 802.11b/g/n) or the 5 GHz band (for 802.11a/n). The R110 router does not support concurrent operation at 2.4 GHz and 5 GHz.

Mode

For 2.4 GHz, the R110 and R120 routers support 802.11b, 802.11g, and 802.11n wireless standards. This option allows the user to select whether the router will operate in 802.11b/g mode, 802.11b/g/n mode, or 802.11n mode only.

For 5 GHz, the R110 router supports 802.11a and 802.11n wireless standards. This option allows the user to select whether the router will operate in 802.11a only mode, 802.11n only mode, or 802.11a/n mode. The R120 router also supports the 802.11ac wireless standard and allows the selection of an 802.11ac operating mode.

Select a 2.4 GHz radio mode for the R110 and R120 routers.

- **11b/g Mixed:** (Compatibility mode.) Up to 11 Mbps for 802.11b and 54 Mbps for 802.11g.
- **11b/g/n Mixed:** (Compatibility mode.) Up to 11 Mbps for 802.11b, 54 Mbps for 802.11g, and 450 Mbps for 802.11n. If support for 802.11b/g is not required, HP recommends that you choose the 802.11n-only mode.
- **11n only:** (Pure 802.11n) Up to 450 Mbps.

Select a 5 GHz radio mode for the R110 router.

- **11a only:** (Pure 802.11a) Up to 54 Mbps.
- **11n only:** (Pure 802.11n) Up to 450 Mbps.
- **11a/n Mixed:** (Compatibility mode.) Up to 450 Mbps for 802.11n and 54 Mbps for 802.11a.

Select a 5 GHz radio mode for the R120 router.

- **11a only:** (Pure 802.11a) Up to 54 Mbps.
- **11n only:** (Pure 802.11n) Up to 450 Mbps.
- **11a/n Mixed:** (Compatibility mode.) Up to 450 Mbps for 802.11n and 54 Mbps for 802.11a.
- **11ac/n/a:** (Compatibility mode.) Up to 1.3 Gbps.

Configure the primary SSID

The R110 allows you to create up to four wireless communities, and the R120 allows you to create up to eight wireless communities. Each wireless community defines the settings for a distinct wireless network, with its own network name (SSID), settings for wireless protection, user authentication, VLANs, and more. Radio settings are shared by all wireless communities.

A default wireless community is defined on the R110/R120. Its name (or SSID) is **HP1** on the R110, **HP1_2G** and **HP1_5G** on the R120, and it is assigned to VLAN 1. The settings that initially display in the wireless community settings pertain to the default community.

The SSID can be changed if desired. The SSID name is case-sensitive and can contain up to 32 standard alphanumeric characters, including spaces. The following are not allowed:

- only spaces
- space as the first character
- space as the last character

If there are other wireless networks in your area, make sure that you give your wireless network a unique name. Click on the SSID box and enter a new name. Click **Next** to make the change.

Configure wireless security

A security method (or no security method) can be associated with the default wireless community and any additional communities you create. This section defines the available security methods as they display in the quick setup wizard. To modify these settings after you complete the quick setup wizard, or to access additional configuration options, use the Wireless pages.

MAC Authentication

You can control access to the wireless network based on the MAC address of a user's wireless device. You can either block access or allow access, depending on your requirements.

Select whether to disable MAC authentication, use a MAC authentication list stored locally on the router, or use a list stored on a RADIUS server. If local MAC authentication is selected, configure your MAC address list on the **Wireless > MAC Authentication** page.

Note that MAC authentication occurs after other authentication methods have been applied.

Authentication Mode and Encryption Type

The router supports several different security mechanisms that provide various levels of authentication and encryption depending on the requirements of the network. Using encryption can help keep your network secure. Encryption works on a system of keys, where the key on a computer must match the key on the router. The router supports the following authentication and encryption methods:

WEP: Wired Equivalent Privacy (WEP) is the security protocol initially specified in the IEEE 802.11 standard for wireless communications. WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and the router. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network. WEP is not as secure as the other security methods available.

WPA and WPA2: Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP, replacing WEP encryption with TKIP. WPA2 includes the complete wireless security standard (802.11i) and offers backward compatibility with WPA, but uses the stronger AES-CCMP encryption. Both WPA and WPA2 provide an “enterprise” and “personal” mode of operation. The “personal” WPA Pre-Shared Key mode uses a common password phrase for user authentication that is manually entered on the router and all wireless clients. The “enterprise” mode of WPA and WPA2 uses IEEE 802.1X for user authentication and requires a RADIUS authentication server to be configured on the wired network. WPA2 is more secure than WPA (TKIP) or WEP, therefore HP recommends that you select WPA2 for maximum possible security.

The router provides the following **Authentication Mode** and **Encryption Type** options:

- **Open:** Allows a client to associate with the router without any authentication, but provides the option of using WEP for encrypting data. If WEP encryption is used, clients must have the correct WEP key to exchange traffic with the router. Selecting WEP encryption also provides the option of using 802.1X for user authentication from a RADIUS server, which dynamically generates WEP keys and distributes them to all clients.
- **WPA2:** The Enterprise mode of WPA2 using AES encryption. If all clients in the network are WPA2 compatible, select this option for maximum security. This mode requires the use of a RADIUS server.
- **WPA2-PSK:** The Personal (pre-shared key) mode of WPA2 using AES encryption. The pre-shared key mode uses a common password phrase for user authentication that is manually entered on the router and all wireless clients. Data encryption keys are automatically generated by the router and distributed to all clients connected to the network.
- **WPA/WPA2 Enterprise:** The WPA2 Enterprise mode for mixed clients, that is, when there are some wireless clients in the network that support only WPA (TKIP encryption). This setting enables both WPA and WPA2 clients to associate and authenticate, but uses the more robust AES encryption (WPA2) for clients that support it. This option allows more interoperability at the expense of some security. This mode requires the use of a RADIUS server.
- **WPA/WPA2-PSK Mixed:** The WPA2 Personal mode for mixed clients, that is, when there are some wireless clients in the network that support only WPA (TKIP encryption). This setting enables both WPA and WPA2 clients to associate and authenticate, but uses the more robust AES encryption (WPA2) for clients that support it. This option allows more interoperability at the expense of some security.
- **WEP Keys:** To configure WEP keys on the router you must first specify the key length and type. You must configure at least one key, although up to four keys can be entered. Only four WEP keys are supported for each radio, that is, the four keys are shared by all SSIDs using a static WEP security configuration. Therefore, you must have a consistent WEP key setup for all SSIDs. Note that the number of keys, the key index (1-4), type, and length must match those configured on the clients.
 - **Key Length:**
 - 64-bit
 - 128-bit

- **Key Type:**
 - Hexadecimal (characters 0-9, a-f, and A-F)
 - ASCII (characters 0-9, a-z, and A-Z)
- **Key 1-4 String:** Enter encryption keys
 - Hexadecimal: Enter keys as 10 hexadecimal characters (0-9 and A-F) for 64 bit keys, or 26 hexadecimal characters for 128 bit keys.
 - ASCII: Enter keys as 5 alphanumeric characters for 64 bit keys, or 13 alphanumeric characters for 128 bit keys.
- **Default Key:** You can enter up to four keys (Key 1 to Key 4). Select the key number from the list that is used to transmit data.
- **Re-Key Interval:** When using 802.1X dynamic WEP keys, enter the interval at which the router refreshes the keys for each associated client. Specify a value in the range of 60 to 86400 seconds.
- **WPA/WPA2 Pre-Shared Key:** The router uses the pre-shared key (PSK) you specify to generate the WPA (TKIP) or WPA2 (AES) keys that are used for data encryption. Each client that connects to the network must use the same pre-shared key.
 - **Key Type:**
 - Hexadecimal (characters 0-9, a-f, and A-F)
 - ASCII (alphanumeric characters 0-9, a-z, and A-Z, plus spaces and symbols)
 - **Passphrase:** Enter the key according to the type selected; in ASCII passphrase style (8-63 alphanumeric characters), or in exactly 64 hexadecimal characters. For an ASCII key, it is recommended that the key be at least 20 characters long, and be a mix of letters and numbers. The passphrase key cannot begin or end with spaces.
- **RADIUS Settings:** When using WPA2, WPA/WPA2 Enterprise, or WEP with 802.1X, the RADIUS server details must be configured.
 - **Group Key Interval:** Enter the interval at which the broadcast (group) key is refreshed for clients associated with the router. Specify a value of 0 to disable refreshing of broadcast keys.
 - **Session Key Interval:** Enter the interval at which the router refreshes session (unicast) keys for each associated client. Specify a value of 0 to disable refreshing of unicast keys.
 - **Primary RADIUS Server:** Enter the IPv4 address for the primary RADIUS server that the router uses by default, for example 192.168.1.23.
 - **RADIUS Key:** The RADIUS key is the shared secret key for the RADIUS server. You can use up to 64 alphanumeric and special characters (do not use characters ` " & ' # \). Do not use blank spaces in the key. The key is case-sensitive, and you must configure the same key on the router and on the RADIUS server.

- **Secondary RADIUS Server:** Enter the IPv4 address for a backup RADIUS server. If authentication fails with the primary server, the configured backup server is tried instead. If a secondary RADIUS server is configured, be sure to enter the RADIUS key.
- **Accounting Enable:** Select this option to track and measure the resources a particular user has consumed, such as system time, amount of data transmitted and received, and so on. If you enable RADIUS accounting, it is enabled for the primary and secondary RADIUS servers.
- **Interim Interval:** The interval between transmitting accounting updates to the RADIUS server. The valid range is 30 to 3600 seconds and the default is 300 seconds.

Step 4: Summary

After you complete the Wizard Setup, the Summary page displays.

Confirm the settings, and then click **Finish**. The router reboots and the HP R110/R120 is operational.

The screenshot shows the Summary page of the Wizard Setup. The progress bar at the top indicates that the first three steps (System Time, Internet Connection, and Wireless) are completed, and the fourth step (Summary) is the current page. The left sidebar contains a navigation menu with the following items: Home, Wizard Setup, System, WAN, LAN, Wireless, VPN, Routing, Firewall, NAT, IPv6, QoS, USB, and Tools. The main content area is divided into three sections: System Time Parameters, WAN Parameters, and Wireless Parameters. Each section contains a table of configuration options.

System Time Parameters	
NTP	Using network time protocol (NTP)
Time Zone	Pacific Time (US)
Daylight Saving	Enabled

WAN Parameters	
Connection Type	DHCP

Wireless Parameters	
Enable Radio	Enabled
Radio Band	2.4GHz
Mode	11b/g/n Mixed
SSID	HP1
MAC Authentication	Disabled
Authentication Mode	WPA2PSK
Encryption Type	AES

At the bottom right of the page, there are three buttons: Back, Finish, and Cancel.

This page includes the following information:

NTP

Indicates if the router is using NTP to synchronize the system clock to global Internet time.

Time Zone

The configured local time zone where the router is installed.

Daylight Saving

Shows if the router is applying daylight saving to the time setting.

Connection Type

The connection method used for the WAN port.

Enable Radio

Shows if the router's wireless radio is enabled. The R120 includes a radio setting for 2.4 GHz and 5 GHz.

Radio Band

The operating band of the R110. The R110 includes one radio that can operate at 2.4 GHz or 5 GHz.

Mode

The wireless standard operating mode of the radio.

SSID

The primary wireless network SSID.

MAC Authentication

The configured MAC authentication setting used for the primary SSID.

Authentication Mode

The configured wireless security mode used for the primary SSID.

Encryption Type

The configured encryption type used for the primary SSID.

3 Managing the HP R110/R120 system

The HP R110/R120 is managed via its web-based management interface using Microsoft Internet Explorer 8 or later, Google Chrome v29, or Mozilla Firefox v24 or later. You can access the HP R110/R120 management tool using either **http** or **https**. Using **https** is more secure, but you will see a warning because the security certificate is issued by the router and not a known certificate authority. With **https**, it is acceptable to choose the option that allows you to proceed through the security warning.

In a web browser, specify either: **http://192.168.1.1** or **https://192.168.1.1**.

For information on launching the web-based management interface for the first time, see the *HP R100-Series Wireless VPN Routers Quickstart*.

Viewing the router status

The Status page displays a summary of the router's key settings. Click **Refresh** to update the status.

Status ?

[-] Device Information

System Name	HP-R110
Software Version	V1.0.0.0-R110-B0010
Serial Number	AD45027960
Device Description	HP R110 Wireless 11n VPN WW Router
Country Selection	Taiwan

[-] Resource Utilization

CPU	10%
Memory Total	110 Mbytes
Memory Free	95 Mbytes
System Uptime	0 days 00h:01m:27s

[+] Security

[+] Wireless

[+] WAN

[+] LAN

[+] USB

[+] SNMP

[Refresh](#)

The Status page includes these items:

Device Information

Shows the router's software version, hardware serial number, host name, device description, and country selection.

Resource Utilization

Indicates the status of the router's resources, including CPU and memory usage.

Security

Displays the current settings for Denial of Service (DoS) and Stateful Packet Inspection (SPI) features.

Wireless

Displays the current settings for the wireless interface, including radio enable, operating frequency, mode, channel, SSID, MAC address, authentication, and encryption.

WAN

Displays the WAN connection type, status, and IP address assignment.

LAN

Displays the router's local network IP address, MAC address, and DHCP server status.

USB

Displays the current status of a device attached to the router's USB port.

SNMP

Displays the status of the Simple Network Management Protocol feature.

Setting the HP R110/R120 mode

The device supports Router and Bridge modes for different applications.

- Router Mode: The normal router mode that allows connections between a wired LAN and wireless clients to the WAN Internet connection, such as a cable or DSL modem. This is the factory set default mode.
- Bridge Mode: The router operates like an access point, extending a wired LAN to wireless clients. In this mode there is no WAN configuration, including routing, VPN, NAT, firewall, and QoS settings; all Internet access features are disabled. In fact, all four LAN ports and WAN port are bridged together, so the WAN port operates like another LAN port.

Operation Mode ?

The device can be used as router or bridge. If used as a bridge, the WAN port and all associated features are disabled.

General Settings

System Mode Router Bridge

Save **Cancel**

General administration settings

The Admin page configures the following settings for the router:

System information (General) settings

Configures settings that help identify the router, including the system name, location, and the name of a person to contact for administrative purposes. The system name appears on the banner and login screen. (Do not use characters ` ` " & ' # \)

General Settings		
System Name	<input type="text" value="HP-R110"/>	(0 - 64 characters)
System Location	<input type="text"/>	(0 - 255 characters)
System Contact	<input type="text"/>	(0 - 255 characters)

Administrator login credentials

Configures the web management interface login username and password. The administrator user name and password can be from 6 to 32 alphanumeric and special characters. (Do not use characters ` ` " & ' # \)

Administrator Login Credentials		
Username	admin	
New Username	<input type="text"/>	(6 - 32 characters)
Current Password	<input type="text"/>	(6 - 32 characters)
New Password	<input type="text"/>	(6 - 32 characters)
Confirm Password	<input type="text"/>	(6 - 32 characters)

Setting the Country Code

The country of operation, also known as the regulatory domain, determines the availability of certain wireless settings on the router. When the country is set, the router automatically limits the available wireless channels and channel width, and adjusts the radio power level in accordance with the regulations of the selected country.

Caution

Incorrectly selecting the country can result in illegal operation and can cause harmful interference to other systems. You must ensure that the router is operating in accordance with channel, power, indoor/outdoor restrictions, and license requirements for the intended country. If you fail to heed this caution, you might be held liable for violating the local regulatory compliance.

Country Code	
Country Code	<input type="text" value="Taiwan"/>

Configuring web server settings

This section configures access to the web management interface.

HTTP Server HTTPS Server

The router software includes HTTP and HTTPS functionality to enable communication with your web browser. Unlike HTTP, HTTPS enables secure sessions, using a digital certificate to encrypt data exchanged between the router and your web browser. HTTP and HTTPS are both enabled by default.

Session Timeout

Configure the Session Timeout for automatic log out from the web interface. If there is no activity on the management session for the specified time, then the administrator will be automatically logged off.

Web Server Configuration

HTTP Server	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
HTTPS Server	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Session Timeout	<input type="text" value="1440"/> (1 - 1440 minutes)

Configuring trusted users

When using the trusted users feature, only computers with specified MAC or IP addresses can access the router's web management interface. All other devices, either LAN or WLAN, cannot access the web interface. A maximum of five rules can be defined.

Trusted Users

Access to the management interface is enabled for the computer specified below.

MAC IP

MAC Address : : : : :

Use Client List

MAC/IP Address	Action
00:11:22:33:44:55	<input type="button" value="🗑️"/> <input type="button" value="✎"/>

System time settings

Correct system time is important for proper operation of the HP R110/R120, especially when using the logs to troubleshoot.

Select **System** > **System time** to open the System Time page. This page enables you to configure time server and time zone information.

Set system time

This section displays the current system time. You can configure the time manually or have it automatically configured by a Network Time Protocol (NTP) server.

Manually

Select the date, time (in 24-hour notation), and timezone.

System Time ?

Configure the connection to the SNTP server. The "Import from Host computer" feature allows you to copy the date and time settings from the administrator's computer.

Set System Time

Current System Time	2013-01-01 01:16:33
Set System Time	<input type="radio"/> Using network time protocol (SNTP) <input checked="" type="radio"/> Manually
	<input type="button" value="Import From Host Computer"/>
System Date	<input type="text"/> (yyyy-mm-dd)
System Time	<input type="text"/> (hh:mm)
Set Time Zone	<input type="text" value="-08:00 Pacific Time (US)"/>

Using network time protocol (NTP)

NTP servers transmit Coordinated Universal Time (UTC, also known as Greenwich Mean Time) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock. The timestamp is used to indicate the date and time of each event in the system log or syslog messages.

When you select this option, a field displays for you to specify the NTP server. You can specify the NTP hostname or IP address, although using the IP address is not recommended, as these are more likely to change. If you specify a hostname, note the following requirements:

- The length must be from 1 to 63 characters.
- Upper and lower case characters, numbers, and hyphens are accepted.
- The first character must be a letter (a to z or A to Z), and the last character cannot be a hyphen.

A actual NTP server host name, **pool.ntp.org**, is configured by default and will provide the time when the AP is connected to the Internet.

System Time ?

Configure the connection to the SNTP server. The "Import from Host computer" feature allows you to copy the date and time settings from the administrator's computer.

Set System Time

Current System Time	2013-01-01 01:26:10
Set System Time	<input checked="" type="radio"/> Using network time protocol (SNTP) <input type="radio"/> Manually
Time Server Address	<input type="text" value="pool.ntp.org"/>
Set Time Zone	<input type="text" value="-08:00 Pacific Time (US)"/>

Daylight saving

Use this section to enable support for daylight saving time, if required for your location. When you select **Manually Set Time For Daylight Savings**, additional fields display to enable you to configure the starting and ending dates and times, and the DST offset.

The DST offset specifies how many minutes to move the clock forward or backward.

Daylight Saving

Enable

Manually Set Time For Daylight Savings

DST Start (24 HR) First Tuesday in January at 00 : 00

DST End (24 HR) First Tuesday in January at 00 : 00

Configuring SNMP

The Simple Network Management Protocol (SNMP) enables the remote management of the HP R110/R120 router by a computer that has SNMP management software installed. The HP R110/R120 provides a robust SNMP v1/v2c implementation supporting both industry-standard MIB II objects and HP-specific MIB objects. Read-only and read-write access are supported.

Select **System** > **SNMP** to open the SNMP configuration page.

SNMP ?

Simple Network Management Protocol (SNMP) enables remote monitoring and management of the device from SNMP-based management platforms.

Settings

Enable SNMP

Read Community (0 - 30 characters)

Write Community (0 - 30 characters)

Trap Receiver IP Address

Trap Receiver Port (1 - 65535)

Trap Community (0 - 30 characters)

To configure SNMP, set the following options:

- **Enable SNMP:** Use this checkbox to enable/disable the SNMP agent. By default, the SNMP agent is disabled. When the agent is disabled, the HP R110/R120 does not respond to SNMP requests.
- **Read Community:** The password that controls read-only access to SNMP information on the router. A network management program must supply this name when attempting to get SNMP information from the router. By default, the name is set to **public**. (Do not use characters ` ` & ' # \)
- **Write Community:** The password that controls read/write access to SNMP information on the router. A network management program must supply this name when attempting to

get or set SNMP information on the router. By default, the name is set to **private**. (Do not use characters ` ` " & ' # \)

The router can also be configured to send status messages to an SNMP server if a problem occurs on the network. This is done by setting the Trap Receiver option. To configure an SNMP Trap Receiver, set the following options:

- **Trap Receiver IP Address:** The IP address of the computer to which the status messages are to be sent.
- **Trap Receiver Port:** The port number of the computer to which the status messages are to be sent.
- **Trap Community:** The computer network management program must supply this name to receive the trap messages. (Do not use characters ` ` " & ' # \)

Managing system logs

The system log is a list of system messages, some of which may indicate error conditions. The router stores up to 2048 system messages in volatile memory (RAM). You can view these events using the router's management interface, and you can configure the router to relay them as syslog messages to a syslog server residing on the network. Note that the log messages in volatile memory are lost when the system reboots.

Log ?

The router supports a logging process that controls which error messages are saved to memory or sent to a Syslog server.

Settings

System Log Level	<input type="text" value="INFORMATIONAL"/>	
Max Size	<input type="text" value="256"/>	(1 - 2048 entries)
Log Prefix	<input type="text"/>	(0 - 16 characters)
Remote Syslog Configuration	<input checked="" type="checkbox"/>	
IP Address	<input type="text"/>	
Port	<input type="text" value="514"/>	(1 - 65535)
Log Level	<input type="text" value="DEBUG"/>	

To configure system logging, set the following options:

System Log Level

You can specify the minimum severity level of the log messages to write to the system log. In the following list, the severity levels are listed from most severe (top) to least severe (bottom):

- **Emergency** indicates that the system is unusable. It is the highest level of severity.
- **Alert** indicates action must be taken immediately.
- **Critical** indicates critical conditions.
- **Error** indicates error conditions.
- **Warning** indicates warning conditions.

- **Notice** indicates normal but significant conditions.
- **Informational** indicates informational messages.
- **Debug** indicates debug-level messages.

For example, if you select **Critical**, only critical, alert, and emergency messages are written to the log.

Max Size

Specifies the maximum number of log entries to store in the router's volatile memory. When the maximum number is reached, the old log messages are overwritten by new messages.

Log Prefix

A text identification string that is added to the log messages. This is useful for quickly identifying events you are interested in when using a remote syslog server.

Remote Syslog Configuration

To view a longer history of log messages, you can set up a remote syslog server that acts as a syslog log relay host on your network. Then, you can configure the router to send syslog messages to the remote server. The System Log Level setting determines which messages are stored in RAM and are available for relay to a remote syslog server.

- **IP Address:** Specify the IP address of the remote syslog server.
- **Port:** The syslog process uses logical port 514 by default. It is recommended that you keep this default. If you specify a different port number, ensure that the port number is not being used by another protocol on your network and that your syslog server is also configured to use that port.
- **Log Level:** When Remote Syslog is enabled, messages of the selected Log Level or higher are sent to the configured syslog server.

Events

The **Events** section of the System log page shows real-time system events on the router, such as wireless clients associating with the router and being authenticated. The log shows the date the event occurred, its severity level, the software program or process that caused the event message, and the message text.

You can select **Refresh** to display the most recent data from the router, or **Clear** to remove all entries from the list. Click **Download** to save all entries to a file on the management computer.

Events

```
Jan 1 04:21:35 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:22:40 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:23:45 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:24:46 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:25:21 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:25:22 HP-R110 hostapd: ath0: STA b4:52:7d:a2:f9:a7 IEEE 802.11: associated
Jan 1 04:25:22 HP-R110 kernel: ath0: STA b4:52:7d:a2:f9:a7 IEEE 802.11: associated
Jan 1 04:25:22 HP-R110 kernel: Node Added (NC = 2)
Jan 1 04:25:22 HP-R110 kernel: [ieee80211_ioctl_setmlme] non sta mode, skip to set bssid
Jan 1 04:25:22 HP-R110 udhcpd[921]: Received bootp packet [state: 3] from b4:52:7d:a2:f9:a7
Jan 1 04:25:26 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:25:26 HP-R110 udhcpd[921]: Received bootp packet [state: 3] from b4:52:7d:a2:f9:a7
Jan 1 04:25:31 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:26:06 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:27:12 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:28:17 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:29:18 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:30:13 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:30:13 HP-R110 kernel: ath0: STA b4:52:7d:a2:f9:a7 IEEE 802.11: disassociated
Jan 1 04:30:13 HP-R110 kernel: Node deleted (NC = 1)
Jan 1 04:30:18 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:30:53 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:31:58 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:32:59 HP-R110 udhcpd[814]: Sending discover...
Jan 1 04:34:24 HP-R110 udhcpd[814]: Sending discover...
```

Refresh Download Clear

Proxy ARP settings

Proxy ARP (Address Resolution Protocol) is a mechanism that enables a computer in a network connected to a router appear to be logically part of another network connected to the same router. This means that a computer on the router's LAN network can appear to be logically on the WAN network, accessible using a public IP address. Note that although the computer appears as part of the public network, it is actually protected behind the router's firewall on the LAN network. That is, traffic between the public network and the host computer on the LAN is still subject to the rules and policies configured on the router. A maximum of eight rules can be defined.

Proxy ARP ?

Proxy ARP is the technique in which one host, usually a router, answers ARP requests that are intended for another machine. The router accepts responsibility for routing packets to the intended destination.

Enable ARP Proxy

Name (1 - 31 characters)

Popular Services

Type

Port(s)

IP Address Of Public Hosts In LAN

Subnet Mask Of Public Hosts In LAN

Rules Name

Add

Name	Type	Port(s)/ Protocol(s)	IP Range Of Public Hosts	Rules Name	Action
SSH	tcp/udp	22	201.123.3.5/255.255.255.0	None	

To configure Proxy ARP, set the following options:

Enable ARP Proxy

Enables the feature on the router.

Name

A text name (1-31 alphanumeric or special characters) that describes the Proxy ARP service. (Do not use characters ` " & ' # \)

Popular Services

Selects common protocols that identify traffic that can be forwarded through the router to a host computer on the local LAN.

Type

Selects TCP or UDP as the protocol type, or other special protocols. When Special Protocol is selected, the protocol numbers can be entered in the Protocol field.

Port(s)

Specifies the TCP/UDP port numbers. More than one number can be entered separated by commas.

Protocol(s)

Specifies special protocol numbers, separated by commas.

IP Address Of Public Hosts In LAN

The IP address of a computer in the local LAN. The IP address and mask can define a range of addresses. For example, IP address 10.8.0.100 with mask 255.255.255.252 specifies addresses 10.8.0.100 to 10.8.0.103.

Subnet Mask Of Public Hosts In LAN

The local subnet mask for the IP address.

Rules Name

Applies a schedule rule to the Proxy ARP service. The schedule rules are configured on the **Tools > Scheduling** page.

Rebooting the router

For maintenance purposes or as a troubleshooting measure, you can reboot the HP R110/R120 by selecting **Reboot**.

The process may take several minutes during which time the AP is unavailable. The HP R110/R120 resumes normal operation with the same configuration settings it had before the reboot.

Reboot

This feature power cycles the device and interrupts router operations. Unsaved configuration changes are lost.

[Reboot](#)

Viewing traffic statistics

To view statistics on Ethernet packets received and transmitted on the wired and wireless ports, select **System > Traffic Statistics**. The Traffic Statistics page displays.

The statistics accumulate until the router is rebooted.

Port Statistics

Displays the WAN and LAN port status together with the number of frames/bytes that have been transmitted and received.

Traffic Statistics

This page displays traffic statistics. To refresh or reset statistics, navigate to the bottom of the page and select the appropriate option.

Port Statistics

Port	Status	Operational Mode	Bytes		Frames	
			RX	TX	RX	TX
LAN1	Disabled	N/A	N/A	N/A	N/A	N/A
LAN2	Enabled	1000 FULL	544724	9393681	5589	12490
LAN3	Disabled	N/A	N/A	N/A	N/A	N/A
LAN4	Disabled	N/A	N/A	N/A	N/A	N/A
WAN	Disabled	N/A	N/A	N/A	N/A	N/A

Wireless LAN Statistics

Displays the traffic statistics for the wireless LAN (SSID interfaces 1 to 4). Statistics include packets/bytes received and transmitted, and the number of packets with errors.

Wireless LAN Statistics

SSID	Packets		Bytes		Error	
	RX	TX	RX	TX	RX	TX
HP1	65523	21294	3723235	2543387	0	213
Total	65523	21294	3723235	2543387	0	213

Interface Statistics

Displays a summary of traffic statistics for the WAN and LAN ports.

Interface Statistics

Interface	Packets		Collisions	Bytes	
	RX	TX		RX	TX
WAN	N/A	N/A	N/A	N/A	N/A
LAN	5590	12490	0	544788	9393681

Poll Interval (10 - 100 seconds) Start Stop Reset Counters

Refresh

Set the poll interval for updating statistics on the page and click **Start**. You can also click **Refresh** anytime to immediately update values. Click **Reset Counters** to set all statistics values back to zero.

4 WAN configuration

The WAN pages are used to configure the parameters for your Internet connection. The information necessary to set up a connection can be obtained from your ISP. Check with your ISP first to find out what type of connection you should choose.

Viewing the WAN interface status

The Status page displays the setting of the WAN interface. If you are using DHCP as the connection type, you can click **Renew** to request a new IP address.

Status	
WAN	
Connection Type	DHCP
Connection Time	0 days 00h:00m:00s
IP Address	0.0.0.0 Renew
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0
MAC Address	70:72:CF:9F:C4:0D
DDNS	
Status	Disabled
MAC Clone	
MAC Address	Disabled

This page includes the following information:

Connection Type

The router's method of connection to the ISP.

Connection Time

The time elapsed since the Internet connection was established.

IP Address

The IP address assigned to the router's WAN port by the ISP.

Subnet Mask

The IP subnet mask assigned to the router's WAN port by the ISP.

Gateway

The IP address of the ISP's gateway.

Primary/Secondary DNS Address

The IP addresses of primary and secondary domain name servers.

DDNS

The status of a dynamic DNS service.

MAC Clone

Indicates if the WAN port MAC address has been copied from a LAN computer.

Settings

The WAN settings page configures the method that the router uses to connect to an ISP through the WAN port. The router supports five Internet connection methods.

DHCP IP address

A dynamic connection type is the most common method used with cable modems. In many cases, setting the connection type to dynamic is enough to complete the connection to your ISP. Some dynamic connection types may require a Host Name. Enter the Host Name in the space provided if you were assigned one by your ISP (do not use characters ` " & ' # \).

Some dynamic connections require that you clone the MAC address of the PC that was originally connected to the modem. To do so, click on **WAN > MAC Clone** to set the WAN MAC address. For more information, see ["MAC clone" on page 42](#).

Settings ?

This page is used to configure parameters for your Internet connection. The information needed for these settings can be obtained from your Internet Service Provider (ISP).

Connection Type	<input type="text" value="DHCP"/>	
Host Name	<input type="text" value="HP-R110"/>	(0 - 255 characters)
Primary DNS Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	(optional)
Secondary DNS Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	(optional)

This page includes the following information:

Connection Type

Select **DHCP** as the router's method of connecting to the ISP.

Host Name

The host name of the DHCP client. The host name is optional, but may be required by some ISPs.

Primary/Secondary DNS Address

The IP addresses of primary and secondary domain name servers.

Static IP address

The Static IP address mode sets the router to operate with a fixed IP address to connect to the Internet. If your ISP uses static IP addressing, you need an IP address, subnet mask, and ISP gateway address. This information is available from your ISP or on the paperwork that your ISP left with you. Enter your information in the provided spaces, and then click **Save**.

Settings ?

This page is used to configure parameters for your Internet connection. The information needed for these settings can be obtained from your Internet Service Provider (ISP).

Connection Type	<input style="width: 100%;" type="text" value="Static IP Address"/>
IP Address	<input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/>
Subnet Mask	<input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/>
Gateway	<input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/>
Primary DNS Address	<input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> (optional)
Secondary DNS Address	<input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> . <input style="width: 25px;" type="text"/> (optional)

This page includes the following information:

Connection Type

Select **Static IP Address** as the router's method of connecting to the ISP.

IP Address

Enter the IP address assigned to the router's WAN port by the ISP.

Subnet Mask

Enter the IP subnet mask assigned to the router's WAN port by the ISP.

Gateway

Enter the IP address of the ISP's gateway.

Primary/Secondary DNS Address

Enter the IP addresses of primary and secondary domain name servers.

PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) is a common WAN protocol that provides a secure "tunnel" connection between the service provider and the local network.

Enter the PPPoE information in the provided spaces, and then click **Save** to activate your settings.

Settings ?

This page is used to configure parameters for your Internet connection. The information needed for these settings can be obtained from your Internet Service Provider (ISP).

Connection Type	<input type="text" value="PPPoE"/>
Username	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Service Name	<input type="text"/>
Idle Time	<input type="text" value="Always On"/> (minutes)
MTU	<input type="text" value="1454"/> (1360 - 1492 bytes)
Manual	<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>
Multiple-PPPoE	<input checked="" type="checkbox"/>
Username	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Service Name	<input type="text"/>
Routing Table	<input checked="" type="checkbox"/>
Source Network	<input type="text" value="."/> . <input type="text" value="."/> . <input type="text" value="."/> . <input type="text" value="."/> / <input type="text" value="24"/>
Destination Network	<input type="text" value="."/> . <input type="text" value="."/> . <input type="text" value="."/> . <input type="text" value="."/> / <input type="text" value="24"/>
Protocol	<input type="text" value="TCP"/>
Source Port	<input type="text"/> (1 - 65535)
Destination Port	<input type="text"/> (1 - 65535)
PPP	<input type="text" value="1"/>
	<input type="button" value="Add"/>

Source Network	Destination Network	Protocol	Source Port	Destination Port	PPP	Action
Empty data						

This page includes the following information:

Connection Type

Select **PPPoE** as the router's method of connecting to the ISP.

Username

Enter your ISP-assigned user name. (Do not use characters ` " & ' # \)

Password

Enter your password (usually assigned by your ISP). (Do not use characters ` " & ' # \)

Confirm Password

Enter the password again to confirm it.

Service Name

The service name is normally optional, but may be required by some service providers. The service name defines the attributes used to set up a dynamic PPPoE subscriber interface.

Idle Time

Select the number of minutes to elapse without activity before the PPPoE connection is disconnected. Or, you can leave the default setting of **Always On** so that the connection is kept open regardless of any activity. (Options: 1, 2, 5, 10, 30, 120 minutes and Always On)

MTU

Sets the size of the Maximum Transmission Unit (MTU) for the largest packet that the network protocol can transmit.

Manual Connection:

You can click **Connect** and **Disconnect** to connect or disconnect the PPPoE connection immediately.

Multiple-PPPoE

Allows you to configure a second PPPoE session to run over the same connection. The second session connects to another PPPoE server and the configuration allows routing rules to be defined so that different traffic can be routed through either PPPoE channel.

Routing Table

The routing table contains rules that are used to route PPPoE traffic by source IP, destination IP, TCP/UDP protocol, source port, or destination port. A maximum of eight rules can be defined.

- **Source network:** The source IPv4 address and mask that identifies traffic to be routed through the specified PPP channel.
- **Destination network:** The destination IPv4 address and mask that identifies traffic to be routed through the specified PPP channel.
- **Protocol:** Identifies TCP or UDP protocol traffic.
- **Source port:** Identifies traffic by a specified TCP or UDP source port.
- **Destination port:** Identifies traffic by a specified TCP or UDP destination port.
- **PPP:** Selects the PPPoE session (1 or 2) to which the classified traffic is to be routed.

PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a common WAN protocol used for Virtual Private Networks (VPNs) that provides a secure "tunnel" connection between the service provider and the local network.

Settings

This page is used to configure parameters for your Internet connection. The information needed for these settings can be obtained from your Internet Service Provider (ISP).

Connection Type	PPTP
Server IP	0 . 0 . 0 . 0
Username	
Password	
Confirm Password	
Idle Time	Always On (minutes)
DHCP Enable	<input checked="" type="checkbox"/>

Renew **Release**

Save **Cancel**

This page includes the following information:

Connection Type

Select **PPTP** as the router's method of connecting to the ISP.

Server IP

Enter the PPTP server IPv4 address as assigned by your ISP.

Username

Enter your ISP-assigned user name. (Do not use characters ` ` " & ' # \)

Password

Enter your password (usually assigned by your ISP). (Do not use characters ` ` " & ' # \)

Confirm Password

Enter the password again to confirm it.

Idle Time

Select the number of minutes to elapse without activity before the PPTP connection is disconnected. Or, you can leave the default setting of **Always On** so that the connection is kept open regardless of any activity. (Options: 1, 2, 5, 10, 30, 120 minutes and Always On)

DHCP Enable

Enables DHCP for the dynamic assignment of the WAN IP address from the ISP. You can click **Release** and **Renew** to refresh the DHCP assignment. If you disable DHCP, enter the static IPv4 address, subnet mask, gateway address, as well as primary and secondary DNS server addresses, as provided by the ISP.

L2TP

The Layer 2 Tunneling Protocol (L2TP) is a common WAN protocol used for Virtual Private Networks (VPNs) that provides a secure "tunnel" connection between the service provider and the local network

Settings

This page is used to configure parameters for your Internet connection. The information needed for these settings can be obtained from your Internet Service Provider (ISP).

Connection Type	L2TP
Server IP	0 . 0 . 0 . 0
Username	
Password	
Confirm Password	
Idle Time	Always On (minutes)
DHCP Enable	<input checked="" type="checkbox"/>

Renew **Release**

Save **Cancel**

This page includes the following information:

Connection Type

Select **L2TP** as the router's method of connecting to the ISP.

Server IP

Enter the L2TP server IPv4 address as assigned by your ISP.

Username

Enter your ISP-assigned user name. (Do not use characters ` ` " & ' # \)

Password

Enter your password (usually assigned by your ISP). (Do not use characters ` " & ' # \)

Confirm Password

Enter the password again to confirm it.

Idle Time

Select the number of minutes to elapse without activity before the L2TP connection is disconnected. Or, you can leave the default setting of **Always On** so that the connection is kept open regardless of any activity. (Options: 1, 2, 5, 10, 30, 120 minutes and Always On)

DHCP Enable

Enables DHCP for the dynamic assignment of the WAN IP address from the ISP. You can click **Release** and **Renew** to refresh the DHCP assignment. If you disable DHCP, enter the static IPv4 address, subnet mask, gateway address, as well as primary and secondary DNS server addresses, as provided by the ISP.

DDNS

Dynamic DNS (DDNS) is a system for allowing an Internet domain name to be assigned to a varying IP address. This makes it possible for other sites on the Internet to establish connections to the server without needing to track the IP address themselves. A common use is for running server software on a computer that has a dynamic IP address (for example, a dialup connection where a new address is assigned at each connection or a DSL service where the address is changed by the ISP occasionally). To implement Dynamic DNS, you must set the maximum caching time of the domain to an unusually short period (typically a few minutes). This prevents other sites on the Internet from retaining the old address in their cache, so that they have to contact the name server of the domain for each new connection. Some "client" programs operate in the background and check the IP address of the computer every few minutes. If it has changed, then it sends an update request to the service.

The router provides pre-configured settings to commonly used DDNS services, such as www.dyndns.org, [zoneedit](http://zoneedit.com), [noip](http://noip.com), [DfDNS](http://DfDNS.com), or 3322.org. You should first register with a DDNS service and obtain an account. This is for users with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider provides a password or key to be entered here.

DDNS ?

Dynamic DNS (DDNS) is a feature that allows an Internet domain name to be assigned to a dynamic IP address for this router.

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Server	<input type="text" value="DynDNS.org"/>
Domain Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>

The DDNS related parameters are described as follows:

Enable DDNS

Select to use a Dynamic DNS service.

DDNS Server

This is the name of your Dynamic DNS service provider.

Domain Name

The name of your host domain.

Username

Enter the user name assigned by your DDNS service. (Do not use characters ` ` " & ' # \)

Password

Enter your password. (Do not use characters ` ` " & ' # \)

Confirm Password

Enter the password again to confirm it.

MAC clone

Some ISPs limit Internet connections to a specified MAC address of one computer. This setting allows you to manually change the MAC address of the router's WAN interface to match the computer's MAC address provided to your ISP for registration. If you are unsure of the computer MAC address originally registered by your ISP, call your ISP and request to register a new MAC address for your account. Register the default MAC address of the router's WAN port.

MAC Clone ?

This feature allows you to manually change the MAC address of the router's WAN interface to match the computer's MAC address that was provided to your ISP for registration.

MAC Address : : : : :

Use Client List

Set to Default MAC Address

You can enter the registered MAC address by manually entering it in the boxes provided. Otherwise, connect the computer with the registered MAC address to the router, and select the computer's name from the **Use Client List**. Click **Save**. The computer's MAC address is now copied to the router's WAN interface.

To restore the default MAC address to the WAN port, click **Reset**.

5 LAN configuration

The HP R110/R120 router is equipped with a DHCP server that automatically assigns IP addresses to each computer on your network. The factory default settings for the DHCP server work with most applications. If you need to make changes to the settings, the LAN setting pages allow you to:

- Change the default IP address of the router.
- Configure VLANs
- Enable the DHCP server function for each VLAN.
- Enable NAT features for each VLAN.
- Enable IGMP Snooping and IGMP Proxy for each VLAN.
- Enable the DHCP Relay function.
- Enable Spanning Tree support.

Viewing the LAN interface status

The Status page displays the current status of LAN related features, including IP settings and VLAN configuration.

Status ?

LAN

MAC Address	70:72:CF:9F:C4:09
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
IGMP Proxy	Enabled
IGMP Snooping	Enabled

STP

Version	RSTP
Root Port	None
Root MAC Address	70:72:CF:9F:C4:09
LAN1	Disabled
LAN2	Blocking
LAN3	Disabled
LAN4	Disabled

VLAN

No.	VLAN	VLAN ID	Grouped Interfaces	IP Address	Subnet Mask
1	Default	1	LAN Port1, LAN Port2, LAN Port3, LAN Port4, WLAN1	192.168.1.1	255.255.255.0

[Refresh](#)

This page includes the following information:

LAN

Displays current settings for the default VLAN.

- **MAC address:** The Ethernet base MAC address of the router.
- **IP address:** The IPv4 address of the router.
- **Subnet mask:** The subnet mask for the IP address.
- **DHCP Server:** The status of the DHCP server for the default VLAN.
- **IGMP Proxy:** The status of the IGMP Proxy feature for the default VLAN
- **IGMP Snooping:** The status of the IGMP Snooping feature for the default VLAN

STP

Displays Spanning Tree Protocol information.

- **Version:** Indicates if the Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) are enabled for the default VLAN.
- **Root Port:** The port on the router that is connected to the Spanning Tree root device. If there is no root port, then this router has been accepted as the root device of the Spanning Tree network.
- **Root MAC Address:** The MAC address of the root device in the Spanning Tree network.
- **LAN1-LAN4:** Displays the state of the router's port interfaces in the Spanning Tree network; Disabled, Learning, Forwarding, or Blocking.

VLAN

The table includes all VLANs currently configured on the router.

LAN Settings

The router must have a valid IP address for management using a web browser and to support other features. The router has a default IP address of 192.168.1.1. You can use this IP address or assign another address that is compatible with an existing local network.

Default VLAN settings

The **IP Address** on the Settings page is the IP address of the default VLAN. To access the web interface, enter this IP address into the address bar of your web browser. This address can be changed if needed. To change the IP address, enter the new IP address and click **Save**. The IP address you choose should be a private IP.

Examples of a private IP are:

192.168.x.x (where x is anything between 0 and 255)

10.x.x.x (where x is anything between 0 and 255)

Settings ?

This page configures parameters for your local area network.

IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>	
Subnet Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>	
Enable DHCP Server	<input checked="" type="checkbox"/>	
IP Pool Starting Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="2"/>	Auto IP Range
IP Pool Ending Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="254"/>	
Lease Time	<input type="text" value="1 day"/>	
VLAN ID	<input type="text" value="1"/> (1 - 4094)	

DHCP Relay

DHCP Relay Enable

Spanning Tree

STP Version

This page includes the following settings:

IP Address

The IPv4 address of the router for the default VLAN.

Subnet Mask

There should be no need to change the subnet mask; however, it is possible to change the subnet mask if necessary. Only make changes to the subnet mask if you have a specific reason to do so.

Enable DHCP Server

The Dynamic Host Configuration Protocol (DHCP) server function automatically assigns IP addresses to each computer in a VLAN. The DHCP server can be turned off if necessary. Turning off the DHCP server requires you to manually set static IP addresses for each computer in the VLAN.

IP Pool Starting/Ending Address

The IP pool is the range of IP addresses set aside for dynamic assignment to the computers in the VLAN. The default is 2-254 (253 computers). You can enter new starting and ending IP addresses for the VLAN IP pool, or click **Auto IP Range** to automatically set a valid range of addresses.

Lease Time

The length of time the DHCP server reserves an IP address for each computer in the VLAN.

VLAN ID

The ID number for the default VLAN. The default VLAN ID is 1. For more information on configuring VLANs, see ["VLAN settings" on page 47](#).

DHCP relay

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate IP addresses and other configuration information to network clients that broadcast a request. To receive broadcast requests, a DHCP server would normally have to be in the same broadcast domain (VLAN) as the clients. However, when the router's DHCP relay feature is enabled, the received client requests can be forwarded directly by the router to a specified DHCP server on another broadcast domain (VLAN). Responses from the DHCP server are returned to the router, which then broadcasts them back to clients.

Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches and routers. Enabling STP allows the router to interact with other STP-compliant switches and routers in the network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The STP versions supported by this router include STP (IEEE 802.1D) and Rapid STP (IEEE 802.1w).

- Spanning Tree Protocol: STP uses a distributed algorithm to select a switch or router that serves as the root of the spanning tree network. It selects a root port on each device (except for the root device) that incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated device from each LAN that incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all devices listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root device (Root Bridge). If a device does not get a Hello BPDU after a predefined interval (Maximum Age), the device assumes that the link to the Root Bridge is down. This device will then initiate negotiations with other devices to reconfigure the network to reestablish a valid network topology.

- Rapid Spanning Tree Protocol: RSTP is designed as a general replacement for the slower, legacy STP. RSTP achieves much faster reconfiguration (around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

Note

The router includes some fixed (not configurable) STP parameters, including the Hello Time (set to 2 seconds) and Forward Delay (set to 4 seconds).

DHCP client list

The DHCP Clients List displays the IP address, host name, MAC address, and client type of each client that has requested an IP address since the last reboot of the router.

Only clients that have requested an IP address since the router's last reboot and fixed associations are displayed in this list. Click **Manual Assignment** to reserve the dynamically assigned IP address for a specific computer. A maximum of 32 static-lease rules can be defined.

DHCP Client List ?

This page provides details about devices that have received IP addresses from the router. You may also convert a dynamically assigned IP address to a static IP address.

MAC Address	IP Address	Host Name	Client Type	Customize
00:22:2D:28:8C:86	192.168.1.9	*	Wired	Manual Assignment

Static Leases

MAC Address : : : : :

IP Address . . .

MAC Address	IP Address	Action
Empty data		

VLAN settings

VLANs on the router are organized and controlled by VLAN profiles. Up to four VLAN profiles can be created. After a new VLAN profile is created, LAN or WLAN interfaces must be added to the VLAN by changing the VLAN settings of the interfaces. An interface can be a member of only one VLAN, either tagged or untagged. Add an interface as a VLAN tagged port if any connected network devices support VLANs, otherwise add the port as untagged. To prevent the forwarding of traffic between VLANs for security, select **Block routing between VLANs**.

Note that the default VLAN profile is read only and cannot be deleted. To create a new VLAN profile, click **Add**. To modify or delete a VLAN profile, click the edit or delete icons in the **Action** column of each VLAN profile entry. Note that there is no delete icon for the default VLAN profile because the default VLAN cannot be deleted.

VLAN ?

The virtual LAN feature provides a convenient way to organize hosts into groups. This page allows you to set up VLAN configuration parameters including NAT and the DHCP server.

VLAN Table

No.	VLAN	VLAN ID	Grouped Interfaces	Action
1	Default	1	LAN Port1, LAN Port2, LAN Port3, LAN Port4, WLAN1, WLAN5	

Add

VLAN Port Membership

LAN Port1

LAN Port2

LAN Port3

LAN Port4

WLAN1

WLAN5

Block routing between VLANs

Port tag/un-tag

Save **Cancel**

On the Add VLAN page, you can set the parameters to configure the behavior of VLANs.

Add VLAN ?

Name (1 - 32 characters)

IP Address . . .

Subnet Mask . . .

Enable NAT

Enable IGMP Snooping

Enable DHCP Server

IP Pool Starting Address . . . **Auto IP Range**

IP Pool Ending Address . . .

Lease Time

VLAN ID (1 - 4094)

Save **Cancel**

This page includes the following settings:

Name

A text description of the VLAN. (Do not use characters ` ` & ' # \)

IP Address

The IP address of the VLAN interface.

Subnet Mask

The subnet mask of the VLAN interface.

Enable NAT

Enables the NAT function for the VLAN interface.

Enable IGMP Snooping

Enables the feature that blocks unnecessary IP multicast traffic from flooding VLAN ports without a specific multicast membership. This feature is based on snooping IGMP join/leave messages from VLAN ports to update the bridging forwarding database. IGMP Snooping is extremely useful in saving bandwidth of low-speed interfaces to improve the network utilization.

Enable DHCP Server

Enables the automatic assignment of IP addresses to clients in the VLAN.

IP Pool Starting/Ending Address

Sets the IP addresses to use for automatic assignment. You can click **Auto IP Range** to automatically set a valid range of pool addresses.

Lease Time

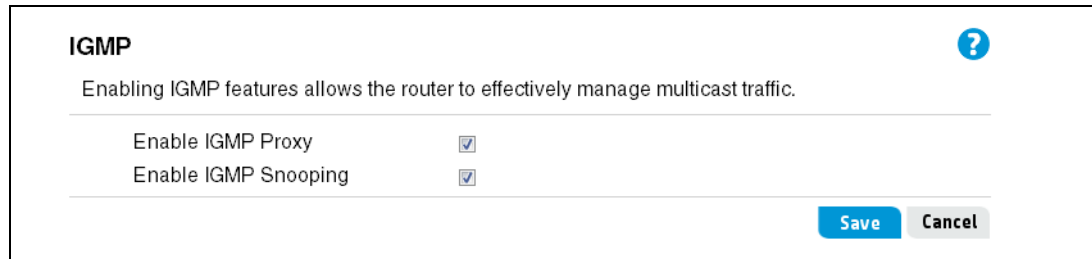
The time interval that clients can use assigned IP addresses.

VLAN ID

The ID number of the VLAN.

IGMP settings

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP can be used for one-to-many networking applications, such as on line streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.



IGMP ?

Enabling IGMP features allows the router to effectively manage multicast traffic.

Enable IGMP Proxy

Enable IGMP Snooping

Save **Cancel**

This page includes the following settings:

Enable IGMP Proxy

IGMP proxy actively filters IGMP packets in order to reduce the load on the multicast router. Join and leave messages heading upstream to the router are filtered so that only the minimal quantity of information is sent.

Enable IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast streams. Multicast traffic can be filtered from the links that do not need them, and thus control the ports that receive specific multicast traffic.

6 Wireless configuration

The wireless settings section displays configuration settings for the access point functionality of the router. The sections include configuration options for radio signal characteristics, wireless security features, Wireless Distribution System (WDS), Wi-Fi Protected Setup (WPS), Wi-Fi Multimedia (WMM), and MAC authentication.

The R110 router supports a dual-band single radio for 2.4 GHz and 5 GHz operation. The R120 router supports two radios, one for 2.4 GHz and one for 5 GHz. This means that the R110 can operate at 2.4 GHz or 5 GHz, but not both at the same time. The R120 can operate concurrently at 2.4 GHz and 5 GHz.

Therefore, the wireless settings differ for the R110 and R120 routers. The R110 router has a single configuration page for 2.4 GHz or 5 GHz operation. The R120 router includes separate configuration pages for 2.4 GHz and 5 GHz operation.

Note

The router supports a maximum of 64 wireless clients per radio.

Viewing wireless interface status

The Status page displays the current status of radio settings, including operating frequency, mode, and channel, as well as specific SSID settings.

Note

The web interface examples in this chapter show the R110, the web pages for the R120 are slightly different.

Status ?	
Wireless	
Radio	Enabled
Operating Frequency	2.4GHz
Mode	11b/g/n Mixed
Channel	6
WMM	Enabled
WMM Power Save	Enabled
Radio ON/OFF Schedule	Disabled
VAP1	
SSID	HP1
MAC Address	70:72:CF:9F:C4:0C
Authentication Mode	OPEN
Encryption Type	NONE
WPS	Enabled
WDS	Disabled

[Refresh](#)

This page includes the following information:

Wireless

Displays the basic radio settings and the status of other features.

- **Radio:** Displays the status of the router's radio.
- **Operating Frequency:** (Applies to the R110 only) Shows if the radio is operating at 2.4 GHz or 5 GHz.
- **Mode:** The current radio mode.
- **Channel:** The current operating channel.
- **WMM:** Displays the status of the WMM feature.
- **WMM Power Save:** Displays the status of the WMM power save feature
- **Radio ON/OFF Schedule:** Shows if a defined time schedule is set for the radio.

VAP1

Displays the settings and feature status for the primary Virtual Access Point (VAP) interface. If other VAP interfaces are enabled (VAP2 to VAP4), they are also listed.

- **SSID:** The service set identifier, or network name, of the VAP interface.
- **MAC Address:** The physical layer address of the VAP interface.
- **Authentication Mode:** The wireless security method configured for the VAP.
- **Encryption Type:** The data encryption configured for the VAP.
- **WPS:** Indicates if WPS is enabled for the VAP.
- **WDS:** Indicates if WDS is enabled for the VAP.

Basic wireless settings

The basic wireless settings allow you to turn the router's wireless function on or off, and set up basic wireless settings for radio signal characteristics and wireless security features.

Basic ?

This page allows you to configure basic wireless settings, such as the SSID, security settings and radio mode operation.

Enable Radio

Radio Band 2.4GHz

Radio Mode 11b/g/n Mixed

Channel Auto

Current Channel 6

Bandwidth 20 MHz

Enable Schedule Rules

Rules Name None

Comment (0 - 31 characters)

Add

Rules Name	Action	Comment	Action
Empty data			

Enable	SSID	Station Isolation	Broadcast	Encryption	
<input checked="" type="checkbox"/>	HP1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE	
<input type="checkbox"/>	HP2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE	
<input type="checkbox"/>	HP3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE	
<input type="checkbox"/>	HP4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE	

Save
Cancel

This page includes the following settings:

Enable Radio

Enables the wireless section of your LAN. When disabled, no wireless clients can have access to either the Internet or other clients on your wired or wireless LAN.

Radio Band

(Applies to the R110 only) Allows you to select the band of your wireless network. The R110 can operate in the 2.4 GHz band (for 802.11b/g/n) or the 5 GHz band (for 802.11a/n). The R110 does not support concurrent operation at 2.4 GHz and 5 GHz.

Radio Mode

For 2.4 GHz, the R110 and R120 support 802.11b, 802.11g, and 802.11n wireless standards. This option allows the user to select whether the router will operate in 802.11b/g mode, 802.11b/g/n mode, or 802.11n mode only.

For 5 GHz, the R110 supports 802.11a and 802.11n wireless standards. This option allows the user to select whether the router will operate in 802.11a only mode, 802.11n only mode, or 802.11a/n mode. The R120 also supports the 802.11ac wireless standard and allows the selection of an 802.11ac/n/a operating mode.

Select a 2.4 GHz radio mode for the R110 and R120.

- **11b/g Mixed:** (Compatibility mode.) Up to 11 Mbps for 802.11b and 54 Mbps for 802.11g.

- **11b/g/n Mixed:** (Compatibility mode.) Up to 11 Mbps for 802.11b, 54 Mbps for 802.11g, and 450 Mbps for 802.11n. If support for 802.11b/g is not required, it is recommended that you choose the 802.11n-only mode.
- **11n only:** (Pure 802.11n) Up to 450 Mbps.

Select a 5 GHz radio mode for the R110.

- **11a only:** (Pure 802.11a) Up to 54 Mbps.
- **11n only:** (Pure 802.11n) Up to 450 Mbps.
- **11a/n Mixed:** (Compatibility mode.) Up to 450 Mbps for 802.11n and 54 Mbps for 802.11a.

Select a 5 GHz radio mode for the R120.

- **11a only:** (Pure 802.11a) Up to 54 Mbps.
- **11n only:** (Pure 802.11n) Up to 450 Mbps.
- **11a/n Mixed:** (Compatibility mode.) Up to 450 Mbps for 802.11n and 54 Mbps for 802.11a.
- **11ac/n/a:** (Compatibility mode.) Up to 1.3 Gbps.

Channel

To change the wireless channel that the router uses, select the required channel from the Channel list. When you select **Auto**, the router searches and selects a channel with the least amount of interference. Click **Save** to save the setting.

Current Channel

When the channel setting is **Auto**, this displays the automatically selected channel number.

Bandwidth

A single channel bandwidth is 20 MHz. When two channels are bonded the bandwidth is a total of 40 MHz. It is possible to use either 20MHz or 40MHz channels with 802.11n.

- **20 MHz:** A single channel bandwidth is 20 MHz.
- **20/40 MHz:** When two channels are bonded the bandwidth is a total of 40 MHz.
- **20/40/80 MHz:** (Applies to 802.11ac setting for the R120) When two 40 MHz channels are bonded the bandwidth is a total of 80 MHz.









Enable Schedule Rules

Implements a defined time schedule to start and stop the wireless network. Click **Add** to add the schedule to the rules table. A maximum of 10 rules can be defined.

- **Rules Name:** Select the name of a configured schedule from the list. The schedule rules are configured on the **Tools > Scheduling** page.
- **Comment:** Enter a text comment to describe the schedule rule.

Configuring virtual access point interfaces

The router supports up to four virtual access point (VAP) interfaces per radio; a total of four for the R110 and eight for the R120. One VAP is the primary (with default SSID “HP1” for R110), and the others can be enabled if required. Each VAP essentially functions as a separate access point, and can be configured with its own Service Set Identifier (SSID) and security settings. Wireless clients associate with these VAPs the same as they would with separate physical access points. This allows access to specific VAPs to be based on certain user groups or application traffic.

Enable	SSID	Station Isolation	Broadcast	Encryption
<input checked="" type="checkbox"/>	HP1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE  
<input type="checkbox"/>	HP2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE  
<input type="checkbox"/>	HP3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE  
<input type="checkbox"/>	HP4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE  

[Save](#) [Cancel](#)

The VAP table includes the following settings:

Enable

Enables secondary VAP interfaces. By default, only the primary VAP interface is enabled (under the basic radio settings), but up to four VAP interfaces can be enabled and configured on the R110. The R120 supports four VAPs per radio, or a total of eight VAPs.

SSID

The SSID is equivalent to the wireless network name and it can be changed if needed. The SSID can contain any standard letters and should be a maximum of 32 characters in length. If there are other wireless networks in your area, you need to give your wireless network a unique name. Enter a new name in the **SSID** box and click **Save** to make the change.

Station Isolation

This function prevents wireless clients connected to the router from communicating with one another. When enabled, this creates a separate virtual network for your wireless network. Your wireless clients are in their own virtual network and are not able to communicate with each other.

Broadcast

By default, the router always broadcasts SSIDs in its beacon signal. When disabled, the router does not include SSIDs in beacon messages, nor does it respond to probe requests from clients that do not include a valid SSID. Disabling the SSID broadcast increases security of the network because wireless clients need to know the SSID before attempting to connect to the network. If you decide to disable the SSID broadcast, ensure that your clients know the name of the network first.

Encryption

Click the edit icon for a VAP interface to configure security settings. The settings are displayed below the table. See the following section for more information on wireless security settings.

Configuring wireless security

The router's wireless interface is configured by default as an open system, which broadcasts a beacon signal including the configured SSID. Wireless clients can read the SSID from the beacon and automatically connect to the wireless network. To implement wireless security, you need to employ authentication, which verifies users connecting to the network, and traffic encryption, to protect transmitted data from interception and eavesdropping.

The router supports a number of security mechanisms that provide various levels of authentication and encryption, depending on the requirements of the network.

MAC Authentication









You can control access to the wireless network based on the MAC address of a user's wireless device. You can either block access or allow access, depending on your requirements.

Select whether to disable MAC authentication, use a MAC authentication list stored locally on the router, or use a list stored on a RADIUS server. If local MAC authentication is selected, configure your MAC address list on the **Wireless > MAC Authentication** page. See [“MAC authentication settings” on page 70](#).

Note that MAC authentication occurs after other authentication methods have been applied.

Authentication Mode and Encryption Type

Using authentication and encryption can help keep your network secure. Encryption works on a system of keys, where the key on a computer must match the key on the router. The router supports a number authentication and encryption methods. When an authentication mode is selected from the list, only the valid encryption types can be selected and all other available configuration options, if any, are displayed.

Enable	SSID	Station Isolation	Broadcast	Encryption
<input checked="" type="checkbox"/>	HP1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE  
<input type="checkbox"/>	HP2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE  
<input type="checkbox"/>	HP3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE  
<input type="checkbox"/>	HP4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	OPEN-NONE  

MAC Authentication

Authentication Mode

Encryption Type

The router provides the following Authentication Mode options:

- **Open:** Allows a client to associate with the router without any authentication, but provides the option of using WEP for encrypting data. If WEP encryption is used, clients must have the correct WEP key to exchange traffic with the router. Selecting WEP encryption also provides the option of using 802.1X for user authentication from a RADIUS server, which dynamically generates WEP keys and distributes them to all clients.

For WEP settings, see [“WEP security” on page 57](#).

For RADIUS settings, see [“Configuring RADIUS settings” on page 62](#).

- **WPA2:** The Enterprise mode of WPA2 using AES encryption. If all clients in the network are WPA2 compatible, select this option for maximum security. This mode requires the use of a RADIUS server. See [“WPA2” on page 59](#).
- **WPA2-PSK:** The Personal (pre-shared key) mode of WPA2 using AES encryption. The pre-shared key mode uses a common password phrase for user authentication that is manually entered on the router and all wireless clients. Data encryption keys are automatically generated by the router and distributed to all clients connected to the network. See [“WPA2-PSK” on page 60](#).
- **WPA/WPA2 Enterprise:** The WPA2 Enterprise mode for mixed clients, that is, when there are some wireless clients in the network that support only WPA (TKIP encryption). This setting enables both WPA and WPA2 clients to associate and authenticate, but uses the more robust AES encryption (WPA2) for clients that support it. This option allows more interoperability at the expense of some security. This mode requires the use of a RADIUS server. See [“WPA/WPA2 enterprise” on page 61](#).
- **WPA/WPA2-PSK Mixed:** The WPA2 Personal mode for mixed clients, that is, when there are some wireless clients in the network that support only WPA (TKIP encryption). This setting enables both WPA and WPA2 clients to associate and authenticate, but uses the more robust AES encryption (WPA2) for clients that support it. This option allows more interoperability at the expense of some security. See [“WPA/WPA2-PSK mixed” on page 61](#).

WEP security

Wired Equivalent Privacy (WEP) is the security protocol initially specified in the IEEE 802.11 standard for wireless communications. WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and the router. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network. The static WEP security on the router enables wireless data encryption, but does not provide for user authentication. WEP is not as secure as the other security methods available.

To configure WEP keys on the router you must first specify the key length and type. You must configure at least one key, although up to four keys can be entered. Only four WEP keys are supported for each radio, that is, the four keys are shared by all SSIDs using a static WEP security configuration. Therefore, you must have a consistent WEP key setup for all SSIDs. Note that the number of keys, the key index (1-4), type, and length must match those configured on the clients.

MAC Authentication	<input type="text" value="Disable"/>
Authentication Mode	<input type="text" value="OPEN"/>
Encryption Type	<input type="text" value="WEP"/>
802.1X	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Key Length	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits
Key Type	<input checked="" type="radio"/> Hexadecimal <input type="radio"/> ASCII
Key1 String	<input type="text"/> (10 characters)
Key2 String	<input type="text"/> (10 characters)
Key3 String	<input type="text"/> (10 characters)
Key4 String	<input type="text"/> (10 characters)
Default Key	<input type="text" value="1"/>

WEP security includes the following settings:

Authentication Mode

Leave as **OPEN** to configure WEP security. The static WEP security does not support user authentication.

Encryption Type

Select **WEP** to display the security options and to configure the keys.

802.1X

Enables dynamic WEP security on the router. IEEE 802.1X enables you to authenticate wireless clients via user accounts stored on a third-party RADIUS server. The RADIUS server is also able to dynamically generate WEP keys and distribute them to all authenticated clients. If you enable dynamic WEP security, be sure to also configure the RADIUS server settings. See [“Configuring RADIUS settings” on page 62](#).

Key Length

The number of characters you specify for the key determines the level of encryption.

- 64-bit
- 128-bit

Key Type

Select the format used to specify the encryption keys. The definition for the encryption keys must be the same on the router and all wireless clients.

- Hexadecimal (characters 0-9, a-f, and A-F)
- ASCII (characters 0-9, a-z, and A-Z)

Key 1 - 4 String

Enter the encryption keys.

- Hexadecimal: Enter keys as 10 hexadecimal characters (0-9 and A-F) for 64 bit keys, or 26 hexadecimal characters for 128 bit keys.
- ASCII: Enter keys as 5 alphanumeric characters for 64 bit keys, or 13 alphanumeric characters for 128 bit keys.

Default Key

You can enter up to four keys (Key 1 to Key 4). Select the key number from the list that is used to transmit data.

Re-Key Interval

When using 802.1X dynamic WEP keys, enter the interval at which the router refreshes the keys for each associated client. Specify a value in the range of 60 to 86400 seconds.

Configuring WPA and WPA2 security

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP, replacing WEP encryption with TKIP. WPA2 includes the complete wireless security standard (802.11i) and offers backward compatibility with WPA, but uses the stronger AES-CCMP encryption. Both WPA and WPA2 provide an “enterprise” and “personal” mode of operation. The “personal” WPA Pre-Shared Key mode uses a common password phrase for user authentication that is manually entered on the router and all wireless clients. The “enterprise” mode of WPA and WPA2 uses IEEE 802.1X for user authentication and requires a RADIUS authentication server to be configured on the wired network. WPA2 is more secure than WPA (TKIP) or WEP, therefore HP recommends to select WPA2 for maximum possible security.

WPA2

The enterprise mode of WPA2 that provides the maximum security. You must set up at least one configured RADIUS server in your network before enabling WPA2 security.

For RADIUS server settings, see “Configuring RADIUS settings” on page 62.

MAC Authentication	<input type="text" value="Disable"/>	
Authentication Mode	<input type="text" value="WPA2"/>	
Encryption Type	<input type="text" value="AES"/>	
Group Key Interval	<input type="text" value="3600"/>	(60 - 86400 seconds) (0: Disabled)
Session Key Interval	<input type="text" value="0"/>	(60 - 86400 seconds) (0: Disabled)
Primary Radius Server	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>	
Radius Key	<input type="text"/>	(1 - 64 characters)
Secondary Radius Server	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>	
Radius Key	<input type="text"/>	(1 - 64 characters)
Accounting Enable	<input type="checkbox"/>	

WPA2 security includes the following settings:

Authentication Mode

Select **WPA2** to display all settings for WPA2 security.

Encryption Type

AES is the specified encryption for WPA2. All wireless clients must be capable of supporting AES encryption to be able to associate with the router.

Group Key Interval

Enter the interval at which the broadcast (group) key is refreshed for clients associated with this VAP interface (the default is 3600 seconds). The valid range is 60 to 86400 seconds. Specify a value of 0 to disable the refreshing of broadcast keys.

Session Key Interval

Enter the interval at which the router refreshes session (unicast) keys for each client associated with the VAP interface. To enable session key refreshing, specify a value in the range of 60 to 86400 seconds. Specify a value of 0 to disable session key refresh.

WPA2-PSK

If your network does not have a RADIUS server, select the WPA2 preshared key (PSK) option. The WPA2-PSK security option is typically used for home or small business networks.

MAC Authentication	<input type="text" value="Disable"/>
Authentication Mode	<input type="text" value="WPA2-PSK"/>
Encryption Type	<input type="text" value="AES"/>
Key Type	<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal
Passphrase	<input type="text"/> (8 - 63 characters)
Group Key Interval	<input type="text" value="3600"/> (60 - 86400 seconds) (0: Disabled)
Session Key Interval	<input type="text" value="0"/> (60 - 86400 seconds) (0: Disabled)

WPA2-PSK security includes the following settings:

Authentication Mode

Select **WPA2-PSK** to display all settings for WPA2-PSK security.

Encryption Type

AES is the specified encryption for WPA2-PSK. All wireless clients must be capable of supporting AES encryption to be able to associate with the router.

Key Type

The WPA preshared key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format.

- **Hexadecimal:** Enter exactly 64 Hexadecimal characters (characters 0-9, a-f, and A-F).
- **ASCII:** Enter 8-63 characters (alphanumeric characters 0-9, a-z, and A-Z, plus spaces and symbols).

Passphrase

Enter the key according to the type selected; in ASCII passphrase style (8-63 alphanumeric characters), or in exactly 64 Hexadecimal characters. For an ASCII key, HP recommends that the key be at least 20 characters long, and be a mix of letters and numbers. The passphrase key cannot begin or end with spaces.

Group Key Interval

Enter the interval at which the broadcast (group) key is refreshed for clients associated with this VAP interface (the default is 3600 seconds). The valid range is 60 to 86400 seconds. Specify a value of 0 to disable the refreshing of broadcast keys.

Session Key Interval

Enter the interval at which the router will refresh session (unicast) keys for each client associated with the VAP interface. To enable session key refreshing, specify a value in the range of 60 to 86400 seconds. Specify a value of 0 to disable session key refresh.

WPA/WPA2 enterprise

If you have a mix of wireless clients, some of which support WPA2 (AES) and others which support only the original WPA (TKIP), select the **WPA/WPA2 Enterprise** security mode. This setting enables both WPA and WPA2 wireless clients to associate to the router, but uses the more robust WPA2 for clients that support it. This security option allows more interoperability, at the expense of some security.

You must set up at least one configured RADIUS server in your network before enabling WPA/WPA2 security. For RADIUS server settings, see “[Configuring RADIUS settings](#)” on page 62.

MAC Authentication	<input type="text" value="Disable"/>
Authentication Mode	<input type="text" value="WPA/WPA2 Enterprise"/>
Encryption Type	<input type="text" value="TKIP/AES"/>
Group Key Interval	<input type="text" value="3600"/> (60 - 86400 seconds) (0: Disabled)
Session Key Interval	<input type="text" value="0"/> (60 - 86400 seconds) (0: Disabled)
Primary Radius Server	<input type="text" value="."/> . <input type="text" value="."/> . <input type="text" value="."/> . <input type="text" value="."/>
Radius Key	<input type="text"/> (1 - 64 characters)
Secondary Radius Server	<input type="text" value="."/> . <input type="text" value="."/> . <input type="text" value="."/> . <input type="text" value="."/>
Radius Key	<input type="text"/> (1 - 64 characters)
Accounting Enable	<input type="checkbox"/>

WPA/WPA2 security includes the following settings:

Authentication Mode

Select **WPA/WPA2 Enterprise** to display all settings for mixed WPA/WPA2 security.

Encryption Type

The TKIP/AES type is the only encryption available for mixed WPA/WPA2 security. In mixed mode, the unicast encryption (TKIP or AES) is negotiated for each client as they associate with the network.

Group Key Interval

Enter the interval at which the broadcast (group) key is refreshed for clients associated with this VAP interface (the default is 3600 seconds). The valid range is 60 to 86400 seconds. Specify a value of 0 to disable the refreshing of broadcast keys.

Session Key Interval

Enter the interval at which the router refreshes session (unicast) keys for each client associated with the VAP interface. To enable session key refreshing, specify a value in the range of 60 to 86400 seconds. Specify a value of 0 to disable session key refresh.

WPA/WPA2-PSK mixed

If your network does not have a RADIUS server, and you need to support a mix of wireless clients, some of which support WPA2 (AES) and others which support only the original WPA (TKIP), select the **WPA/WPA2-PSK** security option. The WPA/WPA2-PSK option is typically used for home or small business networks.

This setting enables both WPA and WPA2 wireless clients to associate to the router, but uses the more robust WPA2 for clients that support it. This security option allows more interoperability, at the expense of some security.

MAC Authentication	<input type="text" value="Disable"/>	
Authentication Mode	<input type="text" value="WPA/WPA2-PSK Mixed"/>	
Encryption Type	<input type="text" value="TKIP/AES"/>	
Key Type	<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal	
Passphrase	<input type="text"/>	(8 - 63 characters)
Group Key Interval	<input type="text" value="3600"/>	(60 - 86400 seconds) (0: Disabled)
Session Key Interval	<input type="text" value="0"/>	(60 - 86400 seconds) (0: Disabled)

WPA/WPA2-PSK security includes the following settings:

Authentication Mode

Select **WPA/WPA2-PSK Mixed** to display all settings for WPA/WPA2-PSK security.

Encryption Type

The TKIP/AES type is the only encryption available for mixed WPA/WPA2 security. In mixed mode, the unicast encryption (TKIP or AES) is negotiated for each client as they associate with the network.

Key Type

The WPA/WPA2 preshared key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format.

- **Hexadecimal:** Enter exactly 64 Hexadecimal characters (characters 0-9, a-f, and A-F).
- **ASCII:** Enter 8-63 characters (alphanumeric characters 0-9, a-z, and A-Z, plus spaces and symbols).

Passphrase

Enter the key according to the type selected; in ASCII passphrase style (8-63 alphanumeric characters), or in exactly 64 Hexadecimal characters. For an ASCII key, HP recommends that the key be at least 20 characters long, and be a mix of letters and numbers. The passphrase key cannot begin or end with spaces.

Group Key Interval

Enter the interval at which the broadcast (group) key is refreshed for clients associated with this VAP interface (the default is 3600 seconds). The valid range is 60 to 86400 seconds. Specify a value of 0 to disable the refreshing of broadcast keys.

Session Key Interval

Enter the interval at which the router refreshes session (unicast) keys for each client associated with the VAP interface. To enable session key refreshing, specify a value in the range of 60 to 86400 seconds. Specify a value of 0 to disable session key refresh.

Configuring RADIUS settings

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires network access.

When using WPA2 or WPA/WPA2 enterprise security, both of which use 802.1X as the method of user authentication, or WEP with 802.1X, a RADIUS server must be configured and available on the connected wired network.

Primary Radius Server	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Radius Key	<input type="text"/>	(1 - 64 characters)
Secondary Radius Server	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Radius Key	<input type="text"/>	(1 - 64 characters)
Accounting Enable	<input checked="" type="checkbox"/>	
Interim Interval	<input type="text" value="300"/>	(30 - 3600 seconds)

The RADIUS server configuration includes the following settings:

Primary RADIUS Server

Enter the IPv4 address for the primary RADIUS server that the router uses by default, for example 192.168.1.23.

RADIUS Key

The RADIUS key is the shared secret key for the RADIUS server. You can use up to 64 alphanumeric and special characters (do not use characters ` ` " & ' # \). Do not use blank spaces in the key. The key is case-sensitive, and you must configure the same key on the router and on the RADIUS server.

Secondary RADIUS Server

Enter the IPv4 address for a backup RADIUS server. If authentication fails with the primary server, the configured backup server is tried instead. If a secondary RADIUS server is configured, be sure to enter the RADIUS key.

Accounting Enable

Select this option to track and measure the resources a particular user has consumed, such as system time, amount of data transmitted and received, and so on. If you enable RADIUS accounting, it is enabled for the primary and secondary RADIUS servers.

Interim Interval

The interval between transmitting accounting updates to the RADIUS server. The valid range is 30 to 3600 seconds and the default is 300 seconds.

Advanced wireless settings

The Advanced wireless settings page includes additional parameters concerning the wireless network.

Advanced ?

Advanced radio settings allow administrators to adjust radio settings in order to improve performance. Caution: Incorrect settings can result in network connection issues.

Beacon Interval	<input type="text" value="100"/>	(20 - 1000 ms)
DTIM Interval	<input type="text" value="1"/>	(1 - 255 beacons)
RTS Threshold	<input type="text" value="2347"/>	(256 - 2347 bytes)
Short Guard Interval	<input type="text" value="Enable"/>	
802.11g Protection Mode	<input type="text" value="CTS to Self"/>	
Extension Channel Protection Mode	<input type="text" value="No Protection"/>	
Preamble Mode	<input type="text" value="Auto"/>	
Max TX Power	<input type="text" value="100%"/>	

This page includes the following settings:

Beacon Interval

The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router to synchronize the wireless network.

DTIM Interval

The DTIM Interval indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The DTIM value is decremented every time a beacon is sent at the beacon interval.

RTS Threshold

Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The router sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

If the RTS threshold is set to 256, the router always sends RTS signals. If set to 2347, the router never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism will be enabled. The stations contending for the wireless medium may not be aware of each other. The RTS/CTS mechanism can solve this "Hidden Node Problem."

Short Guard Interval

This setting is available only if the selected radio mode includes 802.11n.

The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns interval is optional for transmit and receive. The guard interval is the dead time, in nanoseconds, between symbols (or characters) transmitted by the AP. The guard interval helps distinguish where one symbol transmission stops and another starts, thereby reducing inter-symbol interference. Enabling the Short Guard Interval improves throughput and is recommended.

802.11g Protection Mode

Enables a backward compatible protection mechanism for 802.11g and 802.11b clients. The 802.11 standard provides a way to protect transmission against other device transmission by using the RTS/CTS protocol. There are two types of protection:

- **CTS to Self:** The AP that wants to send a frame sends a CTS frame “to itself.”
- **RTS/CTS:** The AP that wants to send frame first sends a Request-To-Send frame and waits for a Clear-To-Send frame from the intended destination. By “seeing” the RTS or CTS frames, 802.11-compliant devices know that somebody is about to transmit and therefore do not initiate transmission themselves.

Extension Channel Protection Mode

With 802.11n, there is the option to use a 40 (2x20) MHz bandwidth to double the data rate. One is the primary channel, and the other is the extension channel. The primary channel is used for communications with clients incapable of the 40 MHz mode. If the extension channel is used, the 802.11 standard provides a way to protect transmission against other device transmission by using the RTS/CTS protocol. There are two types of protection:

- **CTS to Self:** The AP that wants to send a frame sends a CTS frame “to itself.”
- **RTS/CTS:** The AP that wants to send frame first sends a Request-To-Send frame and waits for a Clear-To-Send frame from the intended destination. By “seeing” the RTS or CTS frames, 802.11-compliant devices know that somebody is about to transmit and therefore do not initiate transmission themselves.

Preamble Mode

Sets the length of the signal preamble that is used at the start of a data transmission. Using a short preamble increases data throughput when it is supported by all connected clients. Using a long preamble ensures that 802.11b clients can connect to the network. (Default: Auto)

Max TX Power

Adjusts the power of the radio signals transmitted from the router. The higher the transmission power, the farther the transmission range. Power selection is not just a tradeoff between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the area. (Range - Percentage mode: min, 12.5%, 25%, 50%, 100%; Default: 100%)

WDS settings

The router supports WDS (wireless Distribution System). WDS enables one or more access points to rebroadcast received signals to extend the range and reach of the wireless network, although this can affect the overall throughput of data.

Note that WDS implementations can vary from product to product. Hence, there is no guarantee that different products will interoperate. In addition, the security settings for WDS links are the same as those set up for your wireless clients.

WDS ?

Wireless distribution system can be used to extend wireless network coverage.

VAP	<input type="text" value="1"/>
WDS Mode	<input type="text" value="WDS-STA"/>
Parent SSID	<input type="text" value="HP1"/>
Parent MAC	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> (optional)
Authentication Mode	<input type="text" value="OPEN"/>
Encryption Type	<input type="text" value="NONE"/>

This page includes the following settings:

VAP

The VAP interface number on the router.

WDS Mode

Enables and sets the operating mode for the VAP interface.

- **Disable:** Wireless clients can access the VAP interface as a normal access point service.
- **WDS-AP:** The VAP interface uses WDS to connect to another AP or router. Wireless clients can associate to this VAP interface.
- **WDS-STA:** The VAP interface uses WDS to connect to another AP or router. Only wired clients can connect to the router.

Parent SSID

The SSID of the WDS network. The VAP interface associates with other APs using this SSID.

Parent MAC

For WDS-STA mode, optionally enter a specific MAC address of a parent AP with which the VAP interface should associate.

Authentication Mode and Encryption Type

For information on setting wireless security for WDS links, see “Authentication Mode and Encryption Type” on page 56.

WPS settings

Wi-Fi Protected Setup (WPS) is designed to be a convenient method to securely add new clients to a wireless network. WPS has two basic modes of operation, Push-button Configuration (PBC) and Personal Identification Number (PIN). The WPS PIN setup is optional to the PBC setup and provides more security. You can use this mode by entering a PIN number on the web page. Alternatively, the WPS button on the back of the router can be pressed to allow a single WPS-compliant device to join the network.

WPS ?

Wi-Fi Protected Setup (WPS) is a convenient way to establish secure connections between the router and WPS-compatible wireless clients. You can enable this function using the web interface, or by pressing the WPS button on the rear of the router.

WPS Enable

Configuration State Configured Unconfigured

Lock Enable Disable

Settings

WPS Method PIN PBC

PIN Code

Start

Status

WPS Status	Unconfigured
Lock Status	False
Self PinCode	63454284
SSID	HP1
Authentication Mode	OPEN
Pre-Shared Key	

Save **Refresh** **Cancel**

This page includes the following settings:

WPS enable

Enables the WPS function on the router.

Configuration state

Allows the wireless security to be set manually for the router, or selected automatically by WPS.

- **Configured:** Wireless security is manually set by the user.
- **Unconfigured:** Wireless security is set automatically by WPS.

Lock

This function enables you to lock the WPS PIN setting, which prevents it being changed by any external WPS registrar. Wireless clients can still be added to the network using the WPS push-button configuration. It is still possible to manually change the router's wireless settings.

WPS Method

Selects the WPS method for clients wanting to join the network:

- **PIN:** Uses the PIN setting method. Make sure the WPS function has been enabled on the device. On the client side, start the WPS utility that is provided by your Wi-Fi card's vendor and select the PIN method. You should have an 8-digit PIN number with the WPS utility.

Enter the 8-digit PIN number and click **Start** to activate the PIN method. If the WPS function is working correctly, you should see the WPS LED light up.

- **PBC**: Uses the push-button method. Make sure the WPS function has been enabled on the device. On the client side, start the WPS utility that is provided by your Wi-Fi card's vendor and select the PBC method. Follow the instruction of your WPS utility. Push the WPS button on the router; the WPS LED begins blinking. While the LED is blinking, do not push the button again. If the WPS function is working correctly, the WPS LED lights up.

Status

Displays the following WPS status information:

- **WPS Status**: Displays the WPS configured state.
- **Lock Status**: Displays the PIN lock function state.
- **Self PinCode**: The PIN code of the router.
- **SSID**: The SSID of the router's primary VAP interface.
- **Authentication Mode**: The wireless security mode being used by WPS.
- **Pre-shared Key**: The security key being used by WPS.

WMM settings

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e draft standard. WMM provides basic Quality of service (QoS) features for IEEE 802.11 networks. WMM prioritizes traffic according to four Access Categories (AC), however it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phones.

WMM ?

Wireless Multimedia (WMM) settings allow you to assign different priorities to wireless traffic. The WMM Power Save setting can be used to lower power consumption on compatible wireless clients.

Enable WMM

Enable Power Saving

WMM Parameters

	CWmin (0 - 15)	CWmax (0 - 15)	AIFSN (0 - 15)	TXOP (0 - 8192)	ACM	AckPolicy
AC_BK	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="7"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AC_BE	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="3"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AC_VI	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="2"/>	<input type="text" value="3008"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="2"/>	<input type="text" value="1504"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

This page includes the following settings.

Enable WMM

Select the checkbox to enable the WMM QoS features on the router.

Enable Power Saving

The WMM-Power Save feature enables mobile client devices to save a significant amount of battery life by going into a sleep mode between sending and receiving data.

WMM Parameters

The WMM table includes these parameters:

- **AC_BK**: Access Category - Background. Lowest priority. Data with no delay or throughput requirement, such as bulk data transfers.
- **AC_BE**: Access Category - Best Effort. Normal priority, medium delay and throughput. Data only affected by long delays. Data from applications or devices that lack QoS capabilities.
- **AC_VI**: Access Category - Video. High priority, minimum delay. Time-sensitive data such as streaming video.
- **AC_VO**: Access Category - Voice. Highest priority, minimum delay. Time-sensitive data such as VoIP (Voice over IP) calls.
- **CWmin**: Minimum Contention Window. The initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the CWMin value. Specify the CWMin value in the range 0-15 microseconds. Note that the CWMin value must be equal or less than CWMax value.
- **CWmax**: Maximum Contention Window. The maximum upper limit of the random backoff wait time before wireless medium can be attempted. The contention window is doubled after each detected collision up to the CWMax value. Specify the CWMax value in the range 0-15 microseconds. Note that the CWMax must be greater or equal to the CWMin value.
- **AIFSN**: Arbitration Inter-Frame Space Number. The minimum amount of wait time before the next transmission attempt. Specify the AIFSN value in the range 0-15 microseconds.
- **TXOP**: Transmit Opportunity. The maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TXOP. This data bursting greatly improves the efficiency for high data-rate traffic. Specify a value in the range 0-8192 microseconds.
- **ACM**: The admission control mode for the access category. When enabled, clients are blocked from using the access category.
- **AckPolicy**: Acknowledge Policy. By default, all wireless data transmission requires the sender to wait for an acknowledge message from the receiver. WMM allows the acknowledgement wait time to be turned off for each Access Category (AC). Although this increases data throughput, it can also result in a high number of errors when traffic levels are heavy.

MAC authentication settings

For a more secure wireless network, you can specify that only certain wireless computers can connect to the router. Up to 20 MAC addresses can be added to the MAC Filtering Table. When enabled, all registered MAC addresses are controlled by the access rule.

MAC Authentication is a powerful security feature that allows you to specify which wireless computers are allowed on the network. By setting the access rule to **Allow only stations in list**, any wireless computer attempting to access the network that is not specified in the filter list is denied access. When you enable this feature, you must enter the MAC address of each client in your network to allow network access, or copy the MAC address by selecting the name of the computer from **Choose a PC**. By setting the access rule to **Block all stations in list**, you can block specific wireless computers from accessing the network by adding them to the filter list. A maximum of 20 rules can be defined.

MAC Authentication ?

This feature is used to filter clients based on their MAC address. You can use this function to limit the access of wireless clients to each SSID.

Filter Allow only stations in list
 Block all stations in list

SSID

MAC Address

Use Client List

MAC Address	Action
00:11:22:33:44:55	<input type="button" value="🗑️"/> <input type="button" value="✎"/>

This page includes the following settings.

Filter

Select **Allow only stations in list** to configure only known device MAC addresses that are permitted access to the network. Select **Block all stations in list** to configure known MAC addresses that are denied access to the network.

SSID

Select the VAP interface from the **SSID** list for which you want to configure MAC authentication.

MAC Address

Specify a wireless client MAC address to add to the filter table.

Use Client List

Select a wireless client MAC address to add to the filter table from those already associated with the VAP interface.

Viewing the client list

The Client List page allows you to view all the wireless clients currently associated with the router. Select the SSID interface from the **SSID** list to display associated clients.

The table of associated clients lists the MAC address, Receive Signal Strength Indicator (RSSI) value, wireless mode, and traffic statistics.

Client List ?

This page lists all wireless clients that are connected to each SSID and associated traffic statistics.

SSID HP1 ▾

Total Number Of Associated Clients 1

MAC Address	RSSI	MODE	Packets		Bytes	
			RX	TX	RX	TX
D0:22:BE:87:B4:9E	54	11NG	88	17	5086	1534

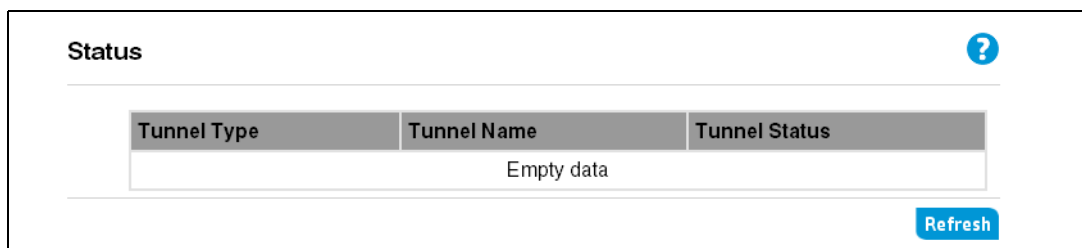
[Refresh](#)

7 VPN configuration

The router includes a Virtual Private Network feature to provide a secure link between remote users and the corporate network by establishing an authenticated and encrypted tunnel for passing secure data over the Internet. The router supports IPSec, L2TP over IPSec client and server, and PPTP client and server for security protection. A maximum of five VPN connections can be enabled.

Viewing VPN status

The Status page displays the current status of VPN tunnel connections to the router.



Tunnel Type	Tunnel Name	Tunnel Status
Empty data		

This page includes the following information:

Tunnel type

The tunnel type configured; either IPSec, L2TP over IPSec, or PPTP.

Tunnel name

The descriptive name that identifies the configured tunnel.

Tunnel status

Indicates the status of the tunnel.

VPN settings

The VPN Settings page allows you to add and edit IPSec, L2TP over IPSec, and PPTP connections for the router. When creating VPN connections, remember that both ends of the connection must be configured in the same way.

Settings ?

This page is used to configure VPN parameters to establish an authenticated and encrypted tunnel for passing secure data over the Internet.

VPN

Enable IPSec

Enable L2TP over IPSec

Enable PPTP

L2TP over IPSec

Pre-shared Key

IP Address Pool for L2TP/PPTP

Start Address . . .

End Address . . .

VPN Connections	Type	Enable
Empty data		

When you click **Add** on this page, the VPN connection page opens where the connection details can be configured. The VPN connection details depend on the protocol selected.

IPSec settings

The router supports the IPSec tunneling protocol. It allows users to create multiple secure IPSec tunnels to remote end points. To establish an IPSec tunnel, the user needs to enable the feature, and enter inbound and outbound addresses for the IPsec tunnel. This router supports MD5 and SHA1 hash algorithm, and DES, 3DES, AES 128, AES 192, and AES 256 encryption algorithms.

-
- Note** Enabling IPSec VPN disables pass-through to IPSec and L2TP over IPSec Virtual Servers on the LAN. Pass-through outbound from clients on the LAN to servers on the Internet is unaffected.
-
- The VPN connection page displays when you click the “Add” button on the VPN Settings page. From the VPN connection page you can configure detailed parameters for your IPSec VPN connection. A maximum of five IPSec connections can be defined.

VPN Tunnel Parameters

?

Tunnel Type:

Tunnel Name: (1 - 19 characters)

Remote VPN Gateway: IP Address / Host Name ANY

IP Address / Host Name:

Remote Secure Group

Remote Party ID:

Remote Network Address: . . .

Remote Subnet Mask: . . .

Local Secure Group

Local Party ID:

Network Address: . . .

Subnet Mask: . . .

Phase I IKE parameters

Key Management:

Hash Algorithm:

Encrypt Algorithm:

Key lifetime: (300 - 99999 seconds)

Diffie-Hellman Group: Group 1 Group 2 Group 5

Pre-shared Key: (1 - 30 characters)

Phase II IPSec Parameters

Authentication Algorithm:

Encrypt Algorithm:

Key lifetime: (300 - 99999 seconds)

PFS:

Diffie-Hellman Group: Group 1 Group 2 Group 5

IKE Keep Alive:

This page includes the following settings:

VPN Tunnel Parameters

- **Tunnel Type:** Select **IPSec** as the tunnel type.
- **Tunnel Name:** Enter a descriptive text name for the tunnel. (Do not use characters ` " & ' # \)
- **Remote VPN Gateway:** Enter the IP address or host name of the remote VPN server, or select **ANY** if there is no specific server.
- **IP Address / Host Name:** The IP address or host name of the remote VPN server.

Remote Secure Group

- **Remote Party ID:** Select either **ID_IPV4_ADDR**, **ID_FQDN**, or **ID_USER_FQDN**. This information must be entered identically on the IPSec software installed on the client's machine.

If **ID_IPV4_ADDR** is selected, enter the IPv4 address and subnet mask in the **Remote Network Address**, and **Remote Subnet Mask** fields. The remote network address is usually the network address of the LAN connected to the remote server.

If **ID_FQDN** or **ID_USER_FQDN** (fully qualified domain name) is selected, enter the name for the **Remote Party ID** in the text box next to the list. For example, an FQDN name could be "mycompany.com", and a user FQDN could be a mail address, such as "my_name@mycompany.com." This name must be unique for each connection rule that you create.

- **Remote Network Address:** Enter the IPv4 address of the remote network.
- **Remote Subnet Mask:** Enter the subnet mask for the remote network.

Local Secure Group

- **Local Party ID:** Enter the identifier of the local secure group.
- **Network Address:** The network address of the local secure group is usually the network address of the local network.
- **Subnet Mask:** Enter the subnet mask for the local network.

Phase I IKE Parameters

- **Key Management:** Select either **IKE Main Mode** or **IKE Aggressive Mode** as the Internet Key Exchange (IKE) method. Note that the Main Mode is more secure but slower, and Aggressive Mode is less secure but faster.
- **Hash Algorithm:** Select either **MD5** or **SHA1** as the algorithm to use for IPSec authentication.
- **Encrypt Algorithm:** Select an encryption algorithm from the list. Both authentication and encryption algorithms must be the same on the router and remote host.
- **Key lifetime:** Sets a time for the keys to be valid, after which they are renewed.
- **Diffie-Hellman Group:** Select one of the groups to use for the Diffie-Hellman key exchange.
- **Pre-shared Key:** Enter the same key on the router and the remote VPN gateway or client. (Do not use characters ` " & ' # \)

Phase II IPSec Parameters

- **Authentication Algorithm:** Select either **MD5** or **SHA1** as the algorithm to use for IPSec authentication.
- **Encrypt Algorithm:** Select an encryption algorithm from the list. Both authentication and encryption algorithms must be the same on the router and remote host.
- **Key lifetime:** Sets a time for the keys to be valid, after which they are renewed.
- **PFS:** Select for Perfect Forward Secrecy (PFS). The Diffie-Hellman Group options then become available. The use of PFS is optional, enabling PFS adds another layer of encryption security.
- **Diffie-Hellman Group:** Select one of the groups to use for the Diffie-Hellman key exchange.
- **IKE Keep Alive:** Enables the router to send IKE keep-alive packets so that the VPN connection remains open even when there is no activity.

L2TP over IPSec settings

The Layer 2 Tunneling Protocol is a common connection method used for VPN connections. You can specify the detailed L2TP tunnel settings on the VPN connections page by clicking **Add**. You can specify the Keep Alive time, which defines the time period without traffic after which the PPP session is terminated. For a client tunnel, both host mode and router mode (LAN-to-LAN) are supported. The tunnel can also be configured to automatically reconnect to the server when Internet traffic is generated.

The VPN connections page displays when you click **Add** on the VPN Settings page. From the VPN connection page you can configure detailed parameters for your L2TP over IPSec VPN connection. A maximum of five L2TP connections can be defined.

VPN Tunnel Parameters

Tunnel Type: L2TP over IPSec

Tunnel Name: (1 - 19 characters)

Username: (1 - 60 characters)

Password: (1 - 60 characters)

Confirm Password: (1 - 60 characters)

Idle Timeout: 10 (0 - 32767 minute)

L2TP Type Setting

L2TP Type: L2TP Server L2TP Client

Enable Auto reconnect:

Remote Server:

IPSec Setting

Pre-shared Key: (1 - 30 characters)

Remote Party ID: ID_IPV4_ADDR

Remote Networking setting

Enable:

Remote Network Address: 0 . 0 . 0 . 0

Remote Subnet Mask: 0 . 0 . 0 . 0

Save **Cancel**

This page includes the following settings:

VPN Tunnel Parameters

- **Tunnel Type:** Select **L2TP over IPSec** as the tunnel type.
- **Tunnel Name:** Enter a descriptive text name for the tunnel. (Do not use characters ` ` " & ' # \)
- **Username:** Enter the user name for L2TP tunnel. (Do not use characters ` ` " & ' # \)
- **Password:** Enter the password for the L2TP tunnel. (Do not use characters ` ` " & ' # \)
- **Confirm Password:** Confirm the L2TP tunnel password.
- **Idle Timeout:** Set the time after which the tunnel is closed when there is no activity.

L2TP Type Setting

- **L2TP Type:** Sets the router to act as the L2TP server or client. When you set the type as **L2TP Client**, you can then enter the **Remote Server** IP address.

- **Enable Auto Reconnect:** For L2TP client connections, you can automatically reconnect when there is activity after a disconnection.
- **Remote Server:** Enter the remote server IP address.

IPSec Setting

- **Pre-shared Key:** When set to client mode, enter the key for the client connection. (Do not use characters ` ` & ' # \)
- **Remote Party ID:** When set to server mode, select either **ID_IPV4_ADDR** or **ID_USER_FQDN**.

If **ID_IPV4_ADDR** is selected, enter the IPv4 address in the text box next to the list.

If **ID_USER_FQDN** (fully qualified domain name) is selected, enter the name in the text box next to the list. For example, a user FQDN could be a mail address, such as "my_name@mycompany.com."


Remote Networking Setting

Enable the remote network setting, and then set the IP address and subnet mask.

PPTP settings

The Point-to-Point Tunneling Protocol is used by some providers in Europe. This router allows computers to use the Internet to remotely log into the LAN using the PPTP tunneling protocol. You can configure the detailed PPTP tunnel settings on the VPN connection page by clicking **Add**. You can specify the Idle Timeout, which defines the time period without traffic after which the PPTP session is terminated. You can also configure the tunnel to behave as either a client or server. For a client tunnel, both the host mode and network mode (LAN-to-LAN) are supported. The tunnel can also be configured to automatically reconnect to the server when Internet traffic is generated.

The VPN connection page displays when you click **Add** on the VPN Settings page. From the VPN connection page you can configure detailed parameters for your PPTP VPN connection. A maximum of five PPTP connections can be defined.

VPN Tunnel Parameters


Tunnel Type	<input type="text" value="PPTP"/>	
Tunnel Name	<input type="text"/>	(1 - 19 characters)
Username	<input type="text"/>	(1 - 60 characters)
Password	<input type="text"/>	(1 - 60 characters)
Confirm Password	<input type="text"/>	(1 - 60 characters)
Idle Timeout	<input type="text" value="10"/>	(0 - 32767 minute)

PPTP Type Setting

PPTP Type PPTP Server PPTP Client

Enable Auto reconnect

Remote Server

Remote Networking setting

Enable

This page includes the following settings:

VPN Tunnel Parameters

- **Tunnel Type:** Select **PPTP** as the tunnel type.
- **Tunnel Name:** Enter a descriptive text name for the tunnel. (Do not use characters ` ` " & ' # \)
- **Username:** Enter the user name for PPTP tunnel. (Do not use characters ` ` " & ' # \)
- **Password:** Enter the password for the PPTP tunnel. (Do not use characters ` ` " & ' # \)
- **Confirm Password:** Confirm the PPTP tunnel password.
- **Idle Timeout:** Set the time after which the tunnel is closed when there is no activity.

PPTP Type Setting

- **PPTP Type:** Sets the router to act as the PPTP server or client. When you set the type as a **PPTP Client**, you can then enter the **Remote Server** IP address.
- **Enable Auto Reconnect:** For PPTP client connections, you can automatically reconnect when there is activity after a disconnection.
- **Remote Server:** Enter the remote server IP address.

Remote Networking Setting

Enable the remote network setting, and then set the IP address and subnet mask.

VPN passthrough settings

VPN Passthrough allows VPN traffic that originates from a VPN client to pass through the router. For example, if you are not using a VPN that is configured on the router, but are using a laptop to access a VPN at another site, configuring VPN passthrough allows that connection.

Passthrough ?

VPN passthrough allows VPN traffic that originates from VPN clients to pass through the router..

PPTP Passthrough	<input checked="" type="checkbox"/>
L2TP Passthrough	<input checked="" type="checkbox"/>
L2TP/IPSec Passthrough	<input checked="" type="checkbox"/>

Save Cancel

8 Routing configuration

Routing configuration allows a static and dynamic methods to set up routing between networks. The network administrator configures static routes by entering routes directly into the routing table. Static routing has the advantage of being predictable and easy to configure.

Alternatively, you can enable dynamic routing using RIP for IPv4 or RIPng for IPv6. The Routing Information Protocol (RIP) is the most common used method for dynamically maintaining routing tables in small networks. RIP uses a distance vector-based approach to routing. Routes are chosen to minimize the distance vector, or hop count, which serves as a rough estimate of transmission cost.

Viewing routing status

The Status page shows whether RIP or RIPng are enabled, and displays the current IPv4 and IPv6 routing tables.

The routing tables include the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network.

Status ?

RIP	Disabled
RIPng	Disabled

IPv4 Routing Table

Flags	Route	Gateway	Subnet Mask	Interface	Metric
C	192.168.1.0	0.0.0.0	255.255.255.0	VLAN(Default)	0
C	239.0.0.0	0.0.0.0	255.0.0.0	VLAN(Default)	0

C: Directly Connected
S: Static
R: RIP

IPv6 Routing Table

Flags	Destination	Gateway	Interface	Metric
Empty data				

C: Directly Connected
S: Static
R: RIPng

[Refresh](#)

This page includes the following information:

Status

- **RIP**: The current status of RIP on the router.
- **RIPng**: The current status of RIPng on the router.

IPv4 routing table

Displays the IPv4 routes statically configured or dynamically learned by the router. For a detailed description, see “Viewing the IPv4 routing table” on page 82.

IPv6 routing table

Displays the IPv6 routes statically configured or dynamically learned by the router. For a detailed description, see “Viewing the IPv6 routing table” on page 85.

Viewing the IPv4 routing table

The routing table shows all the current IPv4 routes used by the router, including any routes created using static routing or RIP.

Routing Table ?

This page displays IPv4 routes created using static routing or RIP.

Flags	Route	Gateway	Subnet Mask	Interface	Metric
S	192.168.3.0	0.0.0.0	255.255.255.0	VLAN(Default)	3
C	192.168.1.0	0.0.0.0	255.255.255.0	VLAN(Default)	0
C	239.0.0.0	0.0.0.0	255.0.0.0	VLAN(Default)	0

C: Directly Connected
S: Static
R: RIP

[Refresh](#)

This page includes the following information:

Flags

Indicates the type of route:

- C: A network directly connected to the router.
- S: A route manually entered on the router.
- R: A route dynamically learned through the RIP protocol.

Route

The destination network to which packets can be routed.

Gateway

Displays the IP address of the router at the next hop to which matching frames are forwarded.

Subnet Mask

Displays the subnetwork associated with the destination.

Interface

The VLAN interface used to route data to the network specified by the destination network address.

Metric

A number used to indicate the cost of a route so that the best route, among potentially multiple routes to the same destination, can be selected.

IPv4 Dynamic route settings

The router supports the Routing Information Protocol (RIP). RIP allows an administrator to set up routing information on one RIP-enabled device, and have that routing information replicated to all RIP-enabled devices on the network. The router supports RIP version 1 and RIP version 2 protocols. RIP is the most widely used method for dynamically maintaining routing tables. RIP uses a distance vector-based approach to routing. Routes are chosen to minimize the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to build consistent tables of next hop links which lead to relevant subnets. The default setting is Disabled.

Dynamic Route

This page allows you configure the parameters for RIP IPv4 dynamic routing.

General RIP Parameter

Enable RIP

Enable Auto Summary

Interface	Operation mode	Version	Poison Reverse	Authentication Required	Password
VLAN (Default)	Enable	2	Enable	None	
WAN	Enable	2	Enable	None	

Save **Cancel**

This page includes the following settings:

Enable RIP

Enables RIP on the router.

Enable Auto Summary

Enables Auto-Summarization on the router. Auto-Summarization sends simplified routing data to other RIP devices rather than the full routing data. Note that this only applies to RIP version 2 as RIP version 1 always uses automatic summarization.

Interface

The VLAN or WAN interface on the router for which RIP can be enabled.

Operation Mode

The router offers two modes of RIP operation.

- **Disable:** RIP is not enabled for the interface.

- **Enable:** RIP is enabled for the interface. The router will transmit and receive RIP update information to and from other RIP-enabled devices.
- **Silent:** RIP is enabled, however the router only receives RIP update messages, it will not transmit any of its own.

Version

Use this field to select **RIPv1** or **RIPv2**.

Poison Reverse

This enables RIP Poison Reverse on the router interface. Poison Reverse is a method that propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. This prevents data loops.

Authentication Required

The router offers two modes of authentication for RIPv2.

- **None:** Deactivates authentication on the specific interface.
- **Password:** An unencrypted text password that needs to be set on all RIP-enabled devices connected to the router. Otherwise, RIP information is not shared between devices with mismatched passwords.

Password

This field is used to enter the password required when password authentication is selected. (Do not use characters ` " & ' # \)

IPv4 Static route settings

The router supports a static route function. You can set up static routes to ensure that all traffic for a specific destination network is forwarded to a certain interface, for example, through a VPN tunnel. A maximum of 15 rules can be defined.

Static Route ?

This page allows you to configure the settings for IPv4 static routes.

Enable

Destination

Subnet Mask

Gateway

Metric (2 - 15)

Interface

Route	Subnet Mask	Gateway	Metric	Interface	Action
192.168.3.0	255.255.255.0	0.0.0.0	3	VLAN(Default)	<input type="button" value="x"/> <input type="button" value="p"/>

This page includes the following settings:

Enable

Enables static routes on the router.

Destination

Enter the IP address of the destination host or network to which the route leads.

Subnet Mask

Enter the IPv4 subnet mask for the destination host or network. For example, for Class C IP domains, the subnet mask is 255.255.255.0.

Gateway

Enter the IP address of the gateway through which the destination host or network can be reached. If this router is used to connect your network to the Internet, your gateway IP is the router's IP address. If you have another router handing your network's Internet connection, enter the IP address of that router instead. The gateway IP address must also be routable, otherwise the static route does not appear in the routing table.

Metric

A number used to indicate the cost of a route so that the best route, among potentially multiple routes to the same destination, can be selected.

Interface

The interface used to route data to the network specified by the network address.

Viewing the IPv6 routing table

The routing table shows all the current IPv6 routes used by the router, including any routes created using static routing or RIPng.

IPv6 Routing Table ?

This page displays IPv6 routes created using static routing or RIPng.

Flags	Destination	Gateway	Interface	Metric
Empty data				

C: Directly Connected
S: Static
R: RIPng

[Refresh](#)

This page includes the following information:

Flags

Indicates the type of route:

- C: A network directly connected to the router.
- S: A route manually entered on the router.
- R: A route dynamically learned through the RIPng protocol.

Destination

The destination network to which packets can be routed.

Gateway

Displays the IP address of the router at the next hop to which matching frames are forwarded.

Interface

The VLAN interface used to route data to the network specified by the destination network address.

Metric

A number used to indicate the cost of a route so that the best route, among potentially multiple routes to the same destination, can be selected.

IPv6 Dynamic route settings

The router supports RIP next generation (RIPng) over IPv6. Like IPv4 RIP version2, RIPng uses the same distance-vector algorithm and hop-count metric, as well as the 30 second update timer. However, RIPng uses a different message format, a different UDP port number, and has no limit on the message size. Also, RIPng does not include an authentication mechanism, it relies on the security built into IPv6 (IPsec). The default setting is Disabled.

IPv6 Dynamic Route ?

This page allows you configure the parameters for RIP IPv6 dynamic routing.

RIPng Enable

Save **Cancel**

IPv6 Static route settings

The router supports an IPv6 static route function. A maximum of 15 rules can be defined.

IPv6 Static Route ?

This page displays IPv6 routes created using static routing or RIPng.

Enable

Destination

Prefix Length (1 - 128)

Gateway

Interface

Metric (1 - 1024)

Add

Destination	Prefix Length	Gateway	Interface	Metric	Action
2001:db8:1:4::1	64	2001:db8:1:2::1	WAN	1024	

Save **Cancel**

This page includes the following settings:

Enable

Enables IPv6 static routes on the router.

Destination

Enter the IPv6 address of the destination host or network to which the route leads.

Prefix Length

Enter the IPv6 prefix length for the destination host or network.

Gateway

Enter the IP address of the gateway through which the destination host or network can be reached. If this router is used to connect your network to the Internet, your gateway IP is the router's IP address. If you have another router handling your network's Internet connection, enter the IP address of that router instead. The gateway IP address must also be routable, otherwise the static route does not appear in the routing table.

Interface

The interface used to route data to the network specified by the network address.

Metric

A number used to indicate the cost of a route so that the best route, among potentially multiple routes to the same destination, can be selected.

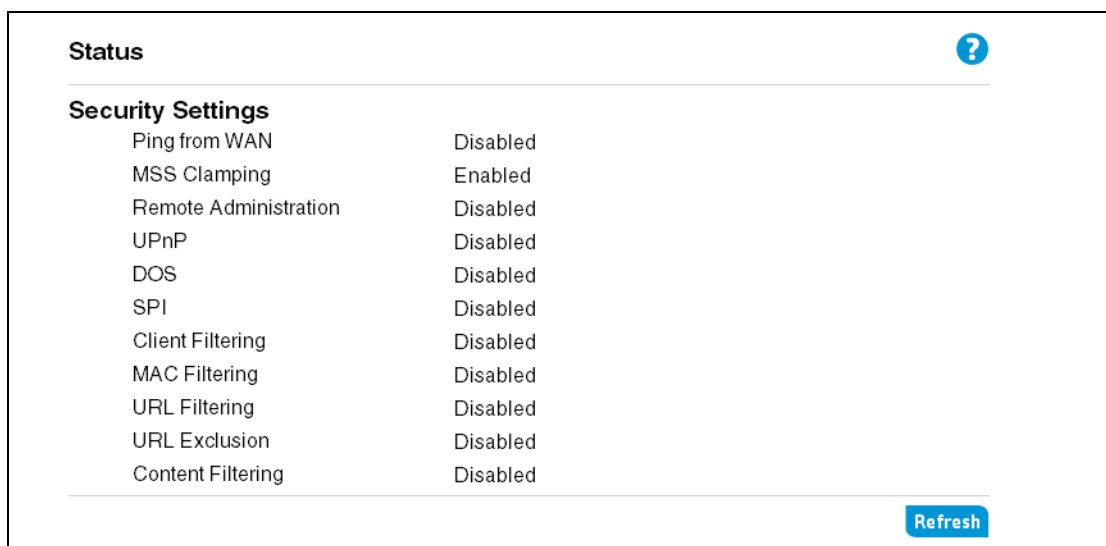
9 Firewall configuration

Your router is equipped with a firewall that will protect your network from a wide array of common hacker attacks, including Denial of Service (DoS) attacks. You can turn the firewall function off, if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but HP recommends that you leave the firewall enabled whenever possible.

In addition to the extensive firewall protection, the router can block access to the Internet from clients on the local network based on IP addresses, MAC addresses, or network service. The router can also block access to specific websites or web page content.

Viewing the firewall status

The Status page displays the current status of the firewall settings.



The screenshot shows a web interface for viewing firewall status. At the top left is the word "Status" with a question mark icon to its right. Below this is a section titled "Security Settings" which contains a list of settings and their status. At the bottom right of the section is a "Refresh" button.

Security Settings	
Ping from WAN	Disabled
MSS Clamping	Enabled
Remote Administration	Disabled
UPnP	Disabled
DOS	Disabled
SPI	Disabled
Client Filtering	Disabled
MAC Filtering	Disabled
URL Filtering	Disabled
URL Exclusion	Disabled
Content Filtering	Disabled

Security settings

The Security page allows you to configure global security parameters for the router.

Security ?

This page allows you to configure global security parameters for the device. Note: Remote Administration is disabled on the WAN port by default.

Enable PING from WAN

Enable MSS Clamping

UPnP

Enable UPnP

Remote Administration

- Disable Remote Administration
- Enable administration from a **single** Internet Host
- Enable administration from a **whole Subnet** Internet Host
- Enable administration from **any** Internet Host

DoS

Enable DDoS Attack Filter

IP Spoofing

Ping of Death

IP with zero length

Smurf Attack

UDP port loopback

Snork Attack

Syn flooding

[Save](#) [Refresh](#) [Cancel](#)

This page includes the following settings:

Enable PING from WAN

Computer hackers use what is known as “pinging” to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there. The router can be set up so it does not respond to an ICMP Ping from the outside. This heightens the level of security of your router.

Enable MSS Clamping

A technique, which works with TCP under specific scenarios only, is so-called “MSS clamping.” With this technique or rather “hack,” the TCP packet’s Maximum Segment Size (MSS) is reduced by tunnel endpoints so that the TCP connection automatically restricts itself to the maximum available packet size. Obviously, this does not work for UDP or other protocols that have no MSS. This approach is most applicable and used with PPPoE, but could be applied otherwise as well; the approach also assumes that all the traffic goes through tunnel endpoints that do MSS clamping — this is simple for single-homed access links, but could be a challenge otherwise.

Enable UPnP (Universal Plug and Play)

Universal Plug and Play (UPnP) is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP compliant. Some applications require the router’s firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports, and in some instances, setting trigger ports. An application that is UPnP compliant has the ability to communicate with the router, basically

“telling” the router which way it needs the firewall configured. The router ships with the UPnP feature disabled. If you are using any applications that are UPnP compliant and want to take advantage of UPnP, you can enable the feature. Select **Enable UPnP** in the UPnP section, and then click **Save** to save the change.

Remote Administration

Remote administration allows you to make changes to your router’s settings from anywhere on the Internet. To remotely manage the router, the remote user must type the following into their browser: `http://<router WAN IP address>:8000` or `8001` if using HTTPS (unless the default port has been changed).

Note

Before you enable this function, make sure you have set the administrator password.

DoS

The router is equipped with a firewall that protects your network from a wide array of common Denial of Service (DoS) attacks. A DoS attack is an attempt by a hacker to disrupt the normal functioning of a target server, making it unavailable to users. A Distributed DoS (DDoS) attack is a coordinated DoS attack from multiple source machines that flood a target server with disruptive traffic until it fails. Turning off the DDoS Attack Filter does not leave your network completely vulnerable to hacker attacks. HP recommends that you enable the DoS detecting function whenever possible.

- **IP Spoofing:** Prevents a hacker from creating an alias (spoof) of the unit’s IP address to which all traffic is redirected.
- **Ping of Death:** Prevents the receipt of an oversized ping packet that the unit cannot handle. Normal ping packets are 56 bytes, or 84 bytes with the IP header attached. The Ping of Death will exceed the maximum IP packet size of 65,535 bytes.
- **IP with zero length:** Prevents received IP packets with zero data length from causing the router system to crash.
- **Smurf Attack:** Prevents a hacker from forging the IP address of the unit and sending repeated ping requests to it flooding the network.
- **UDP port loopback:** Prevents UDP ports 7 (echo) and 19 (chargen) being used to send data to each other causing an infinite loop that leads to a loss of performance and high consumption of network bandwidth.
- **Snork Attack:** Prevents attacks on Windows computers that send UDP packets with a source port of 7 (echo) or 19 (chargen) to destination port 135, causing unnecessary system activity that can significantly slow performance or crash the system.
- **Syn flooding:** Prevents a synchronized (SYN) attack in which the process of the common three way TCP handshake is interrupted and the acknowledge response gets sent to a malicious IP address, or the system is flooded with false SYN requests.

Client filtering

The router can be configured to restrict access to the Internet, email, or other network services on specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers. Enter the filter details in the fields provided, and then click **Add** to add the entry to the filter table. A maximum of 10 rules can be defined.

Client Filtering ?

The router can be configured to restrict access to the Internet, email, or other network services. Restrictions can be set for a single computer or range of computers.

Client PC IP . . . -

Use Client List

Popular Services



Protocol

Port

Enable Schedule Rule

Comment (0 - 31 characters)

Add

Target IP	Protocol	Port	Rules Name	Comment	Action
192.168.1.33	TCP	80,3128,8000,8080,8001	None	WWW(HTTP)	 

Save **Cancel**

This page includes the following settings:

Client PC IP

The IPv4 address of a computer on the local network.

Use Client List

Selects a computer name or IP address from the list of clients already assigned an IP address by the router.

Popular Services

Selects a common network service from the list instead of entering the protocol and ports numbers manually.

Protocol

Selects the TCP or UDP protocol of a service to filter.

Port

The TCP or UDP port number of the service to filter.

Enable Schedule Rule

The name of a scheduling rule to apply to the filter, as configured on the **Tools > Scheduling** page.

Comment

A text comment that describes the filter. (Do not use characters ` " & ' # \)

MAC filtering

You can deny traffic from certain known machines or devices. Use its MAC address to identify a computer or device on the network and deny access. Traffic from a specified MAC address is filtered depending upon the policy. Enter the filter details in the fields provided, and then click **Add** to add the entry to the filter table. A maximum of 20 rules can be defined.

MAC Filtering ?



This page allows you to block client devices from accessing the network-based MAC address. Apply a scheduling rule to restrict access to specific days and times.

MAC Address : : : : :

Use Client List ▾

Enable Schedule Rule ▾

Add

Order	MAC Address	Rules Name	Action
1	00:11:22:33:44:55	None	 

Save **Cancel**

This page includes the following settings:

MAC Address

The MAC address of a computer on the local network.

Use Client List

Selects a computer name or MAC address from the list of clients already assigned an IP address by the router.

Enable Schedule Rule

The name of a scheduling rule to apply to the filter, as configured on the **Tools > Scheduling** page.

URL Filtering Deny List

The list of URL text and keywords that match blocked websites for computers on the LAN.

Exclusion List

The list of computers on the local LAN that are excluded from the URL filtering.

Content filtering



Based on keywords contained on web pages, you can use this screen to restrict access to certain websites that you do not want users in your network to open. Note that web page content that is compressed is not filtered. A maximum of 10 rules can be defined.

Content Filtering ?

This page allows you to block access to HTTP websites based on keywords present in website pages. Devices in the exclusion list will bypass the filters. Apply a scheduling rule to restrict access to specific days and times.

Content String

Enable Schedule Rule None ▾

Order	Content String	Rules Name	Action
1	kardashian	None	 

This page includes the following settings:

Content String

The text or keywords that match web page content to block. (Do not use characters ` " & ' # \)

Enable Schedule Rule

The name of a scheduling rule to apply to the filter, as configured on the **Tools > Scheduling** page.

SPI settings

Stateful Packet Inspection (SPI) is the intrusion detection feature of the router that limits access for incoming traffic. This feature is called “stateful” because it examines the contents of packets to determine the state of the communications; that is, it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions.

When an SPI violation occurs, the offending client is disconnected from the router for 30 minutes. When DoS attacks occur, the router’s Alert LED flashes until the attack ends.

SPI
?

Stateful Packet Inspection (SPI) is an intrusion detection feature of the router that detects and prevents common hacker attacks from incoming traffic at the WAN port.

Enable

Connection Policy

Fragmentation half-open wait	<input style="width: 50px;" type="text" value="30"/>	(30 - 120 seconds)
TCP SYN wait	<input style="width: 50px;" type="text" value="60"/>	(30 - 86400 seconds)
TCP FIN wait	<input style="width: 50px;" type="text" value="120"/>	(30 - 86400 seconds)
TCP connection idle timeout	<input style="width: 50px;" type="text" value="3600"/>	(30 - 86400 seconds)
UDP connection idle timeout	<input style="width: 50px;" type="text" value="180"/>	(30 - 86400 seconds)
H.323 data channel timeout	<input style="width: 50px;" type="text" value="180"/>	(30 - 86400 seconds)

DoS Detect Criteria

Total incomplete TCP/UDP sessions HIGH	<input style="width: 50px;" type="text" value="300"/>	(11 - 1001 sessions)
Total incomplete TCP/UDP sessions LOW	<input style="width: 50px;" type="text" value="250"/>	(10 - 1000 sessions)
Incomplete TCP/UDP sessions (per min) HIGH	<input style="width: 50px;" type="text" value="250"/>	(11 - 1001 sessions)
Incomplete TCP/UDP sessions (per min) LOW	<input style="width: 50px;" type="text" value="200"/>	(10 - 1000 sessions)
Maximum incomplete TCP/UDP sessions number from same host	<input style="width: 50px;" type="text" value="200"/>	(10 - 1000 sessions)
Incomplete TCP/UDP sessions detect sensitive time period	<input style="width: 50px;" type="text" value="1000"/>	(100 - 10000 ms)
Maximum half-open fragmentation packet number from same host	<input style="width: 50px;" type="text" value="64"/>	(64 - 6400)
Flooding cracker block time	<input style="width: 50px;" type="text" value="300"/>	(0 - 600 seconds)

This page includes the following settings:

Enable

Enables the SPI features on the router.

Connection Policy

- **Fragmentation half-open wait:** Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the un-assembled packet, freeing that structure for use by another packet.
- **TCP SYN wait:** Defines how long the software waits for a TCP session to synchronize before dropping the session.
- **TCP FIN wait:** Specifies how long a TCP session is maintained after the firewall detects a FIN packet.
- **TCP connection idle timeout:** The length of time for which a TCP session is managed if there is no activity.
- **UDP session idle timeout:** The length of time for which a UDP session is managed if there is no activity.
- **H.323 data channel timeout:** The length of time for which an H.323 session is managed if there is no activity.

DoS Detect Criteria

- **Total incomplete TCP/UDP sessions HIGH:** Defines the rate of new unestablished sessions that cause the software to start deleting half-open sessions.
- **Total incomplete TCP/UDP sessions LOW:** Defines the rate of new unestablished sessions that cause the software to stop deleting half-open sessions.
- **Incomplete TCP/UDP sessions (per min) HIGH:** Maximum number of allowed incomplete TCP/UDP sessions per minute.
- **Incomplete TCP/UDP sessions (per min) LOW:** Minimum number of allowed incomplete TCP/UDP sessions per minute.
- **Maximum incomplete TCP/UDP sessions number from same host:** Maximum number of incomplete TCP/UDP sessions from the same host. When the maximum value is exceeded, the host is placed on the “cracker list” and packets from the host are then blocked for the duration specified by the **Flooding cracker block time**. During the blocking duration, packets are just dropped and no live session exists, so there may be an incomplete session alert.
- **Incomplete TCP/UDP sessions detect sensitive time period:** The length of time before an incomplete TCP/UDP session is detected as incomplete.
- **Maximum half-open fragmentation packet number from same host:** The maximum number of half-open fragmentation packets from the same host.
- **Flooding cracker block time:** Length of time from detecting a flood attack to blocking the attack.

10 NAT configuration

Network Address Translation (NAT) is a commonly used IP translation and mapping technology. It is a technology that allows your network to share Internet access. Using a device or software that implements NAT allows an entire home network to share a single Internet connection using a single IP address. A single cable modem, DSL modem, or even 56k modem could connect all the computers in your home to the Internet simultaneously. Additionally, NAT keeps your network fairly secure from hackers. NAT acts as an interpreter between two networks. In this case, NAT sits between the Internet and your network. The Internet is considered the public side, and your network is considered the private side. When a computer on the private side requests data from the public side (the Internet), the NAT device opens a conduit between your computer and the destination computer. When the public computer returns results from the request, it is passed back through the NAT device to the requesting computer.

Viewing NAT status

The Status page displays the current status of NAT, Virtual Server, DMZ, Port Trigger, and ALG settings.

Status ?	
NAT	Enabled
Virtual Server	Disabled
DMZ	Disabled
Port Trigger	Enabled
ALG	
SIP	Enabled
H323	Enabled
Refresh	

NAT settings

The Settings page includes the global NAT enable for all VLANs on the router. If NAT is disabled on this page, the NAT features for all VLANs are also disabled.

Turning off NAT does not affect the firewall functions.

Settings ?

Network Address Translation (NAT) is the method by which the router translates a single IP address assigned by your ISP with devices in your local area network.

Enable

Save **Cancel**

Virtual server settings

This function allows you to route external (Internet) calls for services, such as a web server (port 80), FTP server (port 21), or other applications, through your router to your internal network. Because your internal computers are protected by a firewall, machines from the Internet cannot reach them because they cannot be “seen.” If you need to configure the Virtual Server function for a specific application, you need to contact the application vendor to find out which port settings you need. To manually enter settings, enter the IP address in the space provided for the internal machine, the port type (TCP or UDP), and the private and public port(s) required to pass traffic. Then click **Add** and **Save**. You can only pass one port per private IP address. Opening ports in your firewall can pose a security risk. HP recommends that you disable the settings when you are not using a specific application. A maximum of 20 rules can be defined.

Virtual Server ?

For some applications, you must assign a set or a range of ports to a specified local machine. This page allows you to configure the required ports to suit such applications.

Private IP . . .

Use Client List

Popular Services

Protocol

Private Port (1 - 65535)

Public Port (1 - 65535)

Comment (0 - 31 characters)

Add

Private IP	Protocol	Private Port	Public Port	Comment	Action
192.168.1.35	TCP	21	2021	FTP	

Save **Cancel**

This page includes the following settings:

Private IP

The IPv4 address of the computer on the local network.

Use Client List

Selects a computer name or IP address from the list of clients already discovered by the router.

Popular Services

Select one of the services to automatically configure the correct protocol and port numbers. The ports for well known services are listed below:

- FTP port 21
- SSH port 22
- Telnet port 23
- SMTP (email) port 25
- HTTP (web) port 80
- HTTPS (web) port 443
- Auth port 113
- ISAKMP port 500
- POP3 (email) port 110
- IMAP4 (email) port 143
- NetMeeting port 1720
- DNS port 53
- NBX Telephony ports 2093-2096
- L2TP port 1701
- PPTP port 1723

Protocol

The protocol used by the service. Either TCP, UDP, TCP+UDP, ICMP, GRE, ESP, AH, or IPv6-ICMP.

Private Port

The port number of the service used by the host computer on the local network.

Public Port

The port number of the service used by a client on the Internet.

Comment

A text string that describes the virtual server setting. (Do not use characters ` " & ' # \)

DMZ settings

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application, such as a game or video conferencing application. The DMZ feature allows all traffic from the public WAN that is destined for a specified computer (wired or wireless) on the private LAN, to pass through the router's firewall. Note that the router's virtual server feature allows the forwarding of a specific port, whereas the DMZ function forwards all ports/protocols to the specified IP addresses.

Caution

Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks.

To put a computer in the DMZ, enter the last digits of its LAN IP address in the Client PC IP Address field. Enter the IP address (if known) on the Internet that will be used to access the DMZ computer into the Public IP Address field. This allows the computer on the Internet to access the DMZ computer through this address without firewall protection.

For the first line setting (line 1), the Public IP address is set to 0.0.0.0, which means it uses the router's default WAN IP address. The router only allows one DMZ server to be accessed by all public IPs (many to one NAT). For all other line settings, if you have more than one DMZ server, you have to set the public IP address and specify the IP address of the DMZ server on the local network (one to one NAT).

DMZ ?

This page allows you to move a local device outside the firewall, as required for specialized applications such as a Web Server.

Enable

	Public IP	Client PC IP Address
1	0.0.0.0	192.168.1. <input type="text"/>
2	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	192.168.1. <input type="text"/>
3	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	192.168.1. <input type="text"/>
4	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	192.168.1. <input type="text"/>
5	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	192.168.1. <input type="text"/>
6	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	192.168.1. <input type="text"/>
7	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	192.168.1. <input type="text"/>
8	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	192.168.1. <input type="text"/>

This page includes the following settings:

Enable

Enables the DMZ feature for the router.

Public IP

The IP address for the DMZ computer that is used to access it from the Internet. When using the "0.0.0.0" setting, the router's default WAN IP address is used.

Client PC IP Address

The IP address of the DMZ computer on the local LAN.

ALG settings

The Application-Layer Gateway (ALG) feature enables Session Initiation Protocol (SIP) and H323 VoIP traffic to pass through the router without being blocked by its firewall features.

The ALG feature works with the router's NAT feature to control and monitor SIP and H323 sessions, dynamically opening ports as required between SIP/H323 servers on the Internet and clients on the local network. Note that only SIP server ports can be configured on the router. A maximum of eight SIP server ports can be defined.

ALG ?

This page allows users to enable SIP/H323 ALGs. SIP/H323 voice protocols require ALGs to be in the network to prioritize voice traffic through the firewall.

Enable H323 ALG

Enable SIP ALG

SIP Server Ports

5060

5061

Add

Remove

Port Number (1 - 65535)

Save Cancel

This page includes the following settings:

Enable H323 ALG

Enables H323 traffic priority passthrough on the router.

Enable SIP ALG

Enables SIP traffic priority passthrough on the router for the listed ports.

SIP server ports

The SIP ports on which to provide ALG support. Up to eight ports can be configured. The default SIP server ports are 5060 and 5061.

Port number

Specifies a SIP port number to add to the server port list.

Port trigger settings

Some applications such as games, video conferencing, remote access applications, and others require that specific ports in the router's firewall be opened for access by the applications. You can configure the port settings from this screen.

Caution

Opening ports in your firewall can pose a security risk. You can enable and disable settings easily. HP recommends that you disable the settings when you are not using a specific application.

Port Trigger lets you specify ports to be opened for specific applications to work properly with the Network Address Translation (NAT) feature of the router. A maximum of 10 rules can be defined.

A list of popular applications has been included to choose from. Select your application from the **Popular Applications** list, and then click **Add**. The settings are transferred to a row in the Port Trigger table. Click **Save** to save the settings for that application. If your application is not listed, you can consult the application vendor to determine which ports need to be configured. You can then manually enter the port information into the router. Multiple ports can be entered by separating the port numbers by commas (for example; 10, 20, 30), or ranges of ports can be specified by using dashes (for example; 20-30).

Port Trigger ?

This page allows you select which ports are to be open for specific applications to work properly with the Network Address Translation (NAT) .

Enable

Rule Enable

Popular Applications - -Select one-

Trigger Port (1 - 65535)

Trigger Protocol TCP

Public Port (1 - 65535)

Public Protocol TCP

Add

Enable	Trigger Port	Trigger Protocol	Public Port	Public Protocol	Action
Yes	7175	tcp	51200-51201,51210	tcp	🗑️ ✎

Save
Cancel

This page includes the following settings:

Enable

Enables the port trigger feature on the router.

Rule Enable

Enables the configured port trigger rule.

Popular Applications

Lists a number of popular applications to automatically configure the settings.

Trigger Port

Specifies application port numbers to open on the LAN. Multiple ports can be entered by separating the port numbers by commas (for example; 10, 20, 30), or ranges of ports can be specified by using dashes (for example; 20-30).

Trigger Protocol

Selects the TCP or UDP protocol.

Public Port

Specifies port numbers to open for the WAN.

Public Protocol

Selects the TCP or UDP protocol.

11 IPv6 configuration

If the attached network uses the IPv6 protocol, you can enable IPv6 support on the router. IPv6 functionality is disabled by default.

IPv6 includes two distinct address types, link-local unicast and global unicast. A link-local address makes the router accessible over IPv6 for all devices attached to the local LAN. Traffic using this kind of address cannot be passed by any router outside of the LAN. A link-local address is easy to set up and is useful in small networks. However, to connect to a network outside of the LAN, the router's WAN port must be configured with a global unicast address.

Viewing IPv6 status

The Status page displays the current status of the IPv6 connection to the ISP.

Status ?	
Information	
Connection Type	SLAAC
WAN IP Address	fe80::7272:cff:fe9f:c40d/64
Default Gateway	
DNS	
MLD Proxy	Disabled
VLAN (Default) IPv6 Address	fe80::7272:cff:fe9f:c409/64
DHCP-PD	Enabled

[Refresh](#)

This page includes the following information:

Connection Type

Displays the method used for IPv6 configuration.

WAN IP Address

The configured IPv6 addresses for the router's WAN port.

Default Gateway

The IPv6 address of the default next-hop router to use when no routing information is known about an IPv6 address.

DNS

The IPv6 address of a known Domain Name Server.

MLD Proxy

The status of the Multicast Listener Discovery (MLD) proxy feature.

VLAN (Default) IPv6 Address

The IPv6 addresses of the default VLAN on the LAN.

DHCP-PD

The status of the DHCPv6 Prefix Delegation feature.

IPv6 settings

The router supports static, stateless address autoconfiguration (SLAAC), DHCPv6, and PPPoE modes for IPv6 settings for the WAN port. Select the method to use as instructed by your ISP, and then enter the required information and click **Save**.

Static IPv6

The Static IP addresses mode sets the router to operate with a fixed IP address to connect to the Internet. If your ISP uses static IP addressing, you need an IP address, subnet mask, and ISP gateway address. This information is available from your ISP or on the paperwork that your ISP left with you.

Settings

This page is used to configure IPv6 parameters Internet connection. The information that you need to configure IPv6 can be obtained from your ISP.

Connection Settings

IPv6 Connection	<input type="text" value="Static"/>
IPv6 Address	<input type="text"/>
Subnet Prefix Length	<input type="text"/> (1 - 128)
IPv6 Gateway	<input type="text"/>

DNS Settings

Obtain IPv6 DNS servers automatically

Use the following IPv6 DNS servers

IPv6 Primary DNS Address	<input type="text"/>
IPv6 Secondary DNS Address	<input type="text"/>

VLAN (Default) Settings

IPv6 Address	<input type="text" value="2001:db8:1:2::1"/>
Subnet Prefix Length	<input type="text" value="64"/> (1 - 128)
Auto Configuration	<input type="text" value="Stateless(RADVD)"/>
Lifetime	<input type="text" value="30"/> (1 - 43200 minutes)

This page includes the following settings:

Connection Settings

Sets basic IPv6 address configuration settings.

- **IPv6 Connection:** Select **Static** for the IPv6 address connection mode.
- **IPv6 Address:** The IPv6 address of the router. IPv6 addresses are 16 bytes long (128 bits), written as eight groups of hexadecimal quartets separated by colons. The initial bits in an IPv6 address represent the network prefix and are the same for all devices in the network. For example, an IPv6 address could be written as 2001:adca:0000:0000:0000:0000:123a:4567. Note that one double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined

fields. Therefore, the same IPv6 address could be written instead as 2001:adca::123a:4567.

- **Subnet Prefix Length:** The length of the IPv6 address prefix. For unicast addresses, the prefix is typically the first 64 bits, with the following 64 bits being the host identifier.
- **IPv6 Gateway:** The IPv6 address of the default next hop router to use when no routing information is known about an IPv6 address.

DNS Settings

Configures IPv6 DNS settings:

- **Obtain IPv6 DNS servers automatically:** Sets the IPv6 addresses for primary and secondary DNS servers automatically. (Not selectable for a static IPv6 address.)
- **Use the following IPv6 DNS servers:** Enter the primary and secondary DNS server IPv6 addresses.

VLAN (Default) Settings

Sets the IPv6 settings for the local VLAN.

- **IPv6 Address:** The IPv6 address of the router for the local LAN.
- **Subnet Prefix Length:** The prefix length of the IPv6 address.
- **Auto Configuration:** Select **Stateless (RADVD)** or **Stateful (DHCPv6)**.
 - **Disable:** Disables the automatic assignment of IPv6 addresses to local hosts.
 - **Stateless (RADVD):** Enables the automatic assignment of IPv6 addresses by hosts on the local network. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the client identifier (that is, the client MAC address).
 - **Stateful (DHCPv6):** Enables DHCPv6 automatic assignment of IPv6 addresses to local hosts based on a defined address pool. Enter the start and end of the address range to define the pool.
- **Lifetime:** The time that the IPv6 address assignment is valid.

SLAAC

Stateless Address Auto Configuration (SLAAC) enables IPv6 hosts to automatically configure themselves when connected to an IPv6 network using the Neighbor Discovery Protocol through the Internet Control Message Protocol version 6 (ICMPv6) route discovery message. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.

Settings ?

This page is used to configure IPv6 parameters Internet connection. The information that you need to configure IPv6 can be obtained from your ISP.

Connection Settings

IPv6 Connection

DNS Settings

Obtain IPv6 DNS servers automatically

Use the following IPv6 DNS servers

IPv6 Primary DNS Address

IPv6 Secondary DNS Address

VLAN (Default) Settings

Enable DHCP-PD

Auto Configuration

Lifetime (1 - 43200 minutes)

This page includes the following settings:

Connection Settings

Sets basic IPv6 address configuration settings.

- **IPv6 Connection:** Select **SLAAC** for the IPv6 address connection mode.

DNS Settings

Configures IPv6 DNS settings:

- **Obtain IPv6 DNS servers automatically:** Sets the IPv6 addresses for primary and secondary DNS servers automatically.
- **Use the following IPv6 DNS servers:** Enter the primary and secondary DNS server IPv6 addresses.

VLAN (Default) Settings

Sets the IPv6 settings for the local VLAN.

- **Enable DHCP-PD:** Enables the Prefix Delegation feature that automatically uses an IPv6 prefix for the local LAN defined by the ISP. When disabled, the IPv6 address and prefix length need to be manually defined.
 - **IPv6 Address:** The IPv6 address of the router for the local LAN.
 - **Subnet Prefix Length:** The prefix length of the IPv6 address.

- **Auto Configuration:** Select **Stateless (RADVD)** or **Stateful (DHCPv6)**.
 - **Disable:** Disables the automatic assignment of IPv6 addresses to local hosts.
 - **Stateless (RADVD):** Enables the automatic assignment of IPv6 addresses by hosts on the local network. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the client identifier (that is, the client MAC address).
 - **Stateful (DHCPv6):** Enables DHCPv6 automatic assignment of IPv6 addresses to local hosts based on a defined address pool. Enter the start and end of the address range to define the pool.
- **Lifetime:** The time that the IPv6 address assignment is valid.

DHCPv6

Dynamic Host Configuration Protocol version 6 (DHCPv6) automatically assigns IPv6 settings to hosts in an IPv6 network. A dynamic connection type is the most common connection method used by ISPs with cable/DSL modems. If your ISP supports a DHCPv6 server and recommends using this option, select **DHCPv6** from the **Connections Settings** list.

Settings ?

This page is used to configure IPv6 parameters Internet connection. The information that you need to configure IPv6 can be obtained from your ISP.

Connection Settings

IPv6 Connection DHCPv6 ▾

DNS Settings

Obtain IPv6 DNS servers automatically
 Use the following IPv6 DNS servers

IPv6 Primary DNS Address

IPv6 Secondary DNS Address

VLAN (Default) Settings

Enable DHCP-PD

Auto Configuration Stateless(RADVD) ▾

Lifetime (1 - 43200 minutes)

Save Cancel

This page includes the following settings:

Connection Settings

Sets basic IPv6 address configuration settings.

- **IPv6 Connection:** Select **DHCPv6** for the IPv6 address connection mode.

DNS Settings

Configures IPv6 DNS settings:

- **Obtain IPv6 DNS servers automatically:** Sets the IPv6 addresses for primary and secondary DNS servers automatically.
- **Use the following IPv6 DNS servers:** Enter the primary and secondary DNS server IPv6 addresses.

VLAN (Default) Settings

Sets the IPv6 settings for the local VLAN.

- **Enable DHCP-PD:** Enables the Prefix Delegation feature that automatically uses an IPv6 prefix for the local LAN defined by the ISP. When disabled, the IPv6 address and prefix length need to be manually defined.
 - **IPv6 Address:** The IPv6 address of the router for the local LAN.
 - **Subnet Prefix Length:** The prefix length of the IPv6 address.
- **Auto Configuration:** Select **Stateless (RADVD)** or **Stateful (DHCPv6)**.
 - **Disable:** Disables the automatic assignment of IPv6 addresses to local hosts.
 - **Stateless (RADVD):** Enables the automatic assignment of IPv6 addresses by hosts on the local network. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the client identifier (that is, the client MAC address).
 - **Stateful (DHCPv6):** Enables DHCPv6 automatic assignment of IPv6 addresses to local hosts based on a defined address pool. Enter the start and end of the address range to define the pool.
- **Lifetime:** The time that the IPv6 address assignment is valid.

PPPoE

If your ISP uses Point-to-Point Protocol over Ethernet (PPPoE) as the IPv6 connection type, enter the PPPoE information in the provided spaces, and then click **Save** to activate your setting.

Settings

This page is used to configure IPv6 parameters Internet connection. The information that you need to configure IPv6 can be obtained from your ISP.

Connection Settings

IPv6 Connection

Username (1 - 32 characters)

Password (1 - 255 characters)

Confirm Password (1 - 255 characters)

DNS Settings

Obtain IPv6 DNS servers automatically

Use the following IPv6 DNS servers

VLAN (Default) Settings

Enable DHCP-PD

Auto Configuration

Lifetime (1 - 43200 minutes)

This page includes the following settings:

Connection Settings

Sets basic IPv6 address configuration settings.

- **IPv6 Connection:** Select **PPPoE** for the IPv6 address connection mode.

- **Username:** Enter the name assigned by the ISP. (Do not use characters ` ` " & ' # \)
- **Password:** Enter the password provided by the ISP. (Do not use characters ` ` " & ' # \)
- **Confirm Password:** Enter the password again for confirmation.

DNS Settings

Configures IPv6 DNS settings:

- **Obtain IPv6 DNS servers automatically:** Sets the IPv6 addresses for primary and secondary DNS servers automatically.
- **Use the following IPv6 DNS servers:** Enter the primary and secondary DNS server IPv6 addresses. (Not selectable for a PPPoE IPv6 connection setting.)

VLAN (Default) Settings

Sets the IPv6 settings for the local VLAN.

- **Enable DHCP-PD:** Enables the Prefix Delegation feature that automatically uses an IPv6 prefix for the local LAN defined by the ISP. When disabled, the IPv6 address and prefix length need to be manually defined.
 - **IPv6 Address:** The IPv6 address of the router for the local LAN.
 - **Subnet Prefix Length:** The prefix length of the IPv6 address.
- **Auto Configuration:** Select **Stateless (RADVD)** or **Stateful (DHCPv6)**.
 - **Disable:** Disables the automatic assignment of IPv6 addresses to local hosts.
 - **Stateless (RADVD):** Enables the automatic assignment of IPv6 addresses by hosts on the local network. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the client identifier (that is, the client MAC address).
 - **Stateful (DHCPv6):** Enables DHCPv6 automatic assignment of IPv6 addresses to local hosts based on a defined address pool. Enter the start and end of the address range to define the pool.
- **Lifetime:** The time that the IPv6 address assignment is valid.

DHCPv6 client list

This page displays the DHCPv6 client information, such as DHCP Unique Identifier (DUID), IPv6 address, and duration time of the IPv6 address assignment for each client that has requested an IP address since the last reboot of the router.

DHCPv6 Client List ?

This page provides details on devices that have received IPv6 addresses from the router.

DUID	Address	Duration
Empty data		

[Refresh](#)

MLD settings

Multicast Listener Discovery (MLD) proxy enables the router to issue MLD host messages on behalf of hosts that the router has discovered through standard MLD interfaces.

MLD ?

Multicast Listener Discovery (MLD) proxy enables the router to issue MLD host messages on behalf of hosts that the router has discovered through standard MLD interfaces.

MLD Proxy Enable

Save **Cancel**


12 QoS configuration

The bandwidth gap between the LAN and WAN may significantly degrade performance of critical network applications, such as VoIP, gaming, and VPN. The router's Quality of Service (QoS) function allows users to classify application traffic and provide them with differentiated services (DiffServ).

The QoS feature allows you to specify which data packets have greater priority when traffic is transmitted from the WAN port. This router supports QoS with four priority queues on the WAN port. Data packets in the WAN port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the maximum bandwidth for each priority queue (traffic shaping), as well as classify traffic types, and then map them to the WAN port priority queues (traffic mapping).

Viewing QoS status

This page displays the current status of the quality-of-service (QoS) and traffic mapping features.

Status		
QoS	Enabled	
Traffic Mapping	Disabled	
		Refresh

Traffic shaping

The Traffic Shaping page enables the bandwidth of the WAN port output queues to be configured. For higher priority traffic, such as voice and video, the bandwidth allocation of queues 3 and 4 can be increased, and those for queues 1 and 2 decreased.

Traffic Shaping ?

Traffic Shaping allows you to configure the bandwidth for traffic from LAN clients to Internet hosts.

General

Enable

Diffserv

Name	Priority	Bandwidth Allocation
		Maximum
Queue 1	Low ↑ ↓ High	<input type="text" value="1024000"/> Kbps
Queue 2		<input type="text" value="1024000"/> Kbps
Queue 3		<input type="text" value="1024000"/> Kbps
Queue 4		<input type="text" value="1024000"/> Kbps

This page includes the following settings:

General

Enables the traffic shaping settings on the router.

Diffserv

Displays the table of bandwidth settings for the WAN port's four output queues.

Name

Identifies the port queue (numbered 1 to 4).

Priority

Indicates that queue 1 is the lowest-priority queue and queue 4 the highest-priority queue.

Bandwidth Allocation

Sets the bandwidth for each output queue in Kbps. By default, the maximum of 1024000 Kbps is the full bandwidth of the WAN port. You can specify any value for a queue's maximum bandwidth in the range 0 to 1024000 Kbps.

Traffic mapping

Up to 16 rules can be defined to classify traffic into DiffServ forwarding groups and outgoing connections. These rules can be mapped to the WAN port forwarding queues, for which the bandwidth can be configured on the Traffic Shaping page.

Traffic Mapping ?

The router supports up to 16 rules to classify your network traffic into DiffServ forwarding groups and outgoing connections.

Rules

Rule Name (1 - 255 characters)

Source Address

Destination Address

Popular Services

Traffic Type

802.1p Priority



DSCP/TOS

Map to Forwarding Queue

Remark 802.1p priority as

Remark DSCP as

Add

Name	Traffic Description	Map to Diffserv	Remark 802.1p priority	Remark DSCP	Action
Test1	L: 00:11:22:33:44:55 Service: Web (http) Type: tcp, dst port: 80 802.1p priority: 6	4 (Highest)	6	EF	 

Save **Cancel**

This page includes the following settings:

Rule Name

A name to identify the traffic mapping rule. (Do not use characters ` ` " & ' # \)

Source Address

Select **Any**, or a specific LAN host MAC address or IP subnet.

Destination Address

Select **Any** or a specific IP subnet as the traffic destination.

Popular Services

Select a popular service from the list to automatically configure the traffic type and IP protocol.

Traffic Type

Specifies UDP, TCP, or other IP protocol.

- **IP Protocol:** Specifies the protocol type number when an application is not included in the popular services list.

802.1p Priority

Identifies traffic by the 802.1p priority tag value.

DSCP/TOS

Identifies traffic by the IP DSCP or TOS value.

Map to Forwarding Queue

Maps the traffic to one of the WAN port forwarding queues. Queue 1 is the lowest priority queue and queue 4 the highest priority.

Remark 802.1p priority as

Before the identified traffic is sent to the forwarding queue, the 802.1p priority tag can be set to the specified value.

Remark DSCP as

Before the identified traffic is sent to the forwarding queue, the IP DSCP can be set to the specified value.

13 USB configuration

The router provides a USB 2.0-compliant port for network-connected users to share files through FTP or File Sharing. The files can be on an attached storage device that supports any number of partitions in VFAT, NTFS, EXT2, EXT3, or EXT4 format.

User Account

A File Sharing user can use Windows Network Neighborhood to access files on a USB drive. An FTP user can log into the FTP server using an FTP client. A maximum of eight File Sharing accounts and eight FTP accounts can be defined (total 16 accounts maximum).

User Account ?

This page allows you to configure user accounts to manage access to your USB storage device.

USB Type File Sharing FTP

Username (6 - 32 characters)

Password (6 - 32 characters)

Confirm Password (6 - 32 characters)

Authority

Enable

Add

Username	Password	USB Type	Access	Authority	Action
User123	1234567	samba	yes		
User456	7654321	ftp	yes	Read and Write	

Save **Cancel**

This page includes the following settings:

USB Type

Selects a user account for access to USB files through File Sharing or FTP.

Username

Enter a name containing 6 to 32 characters (do not use characters ! # \$ % ^ & * () + ~ ` " ' { } [] | \ / : ; ? > < , = or space).

Password

Enter a password containing 6 to 32 characters (do not use two or more successive spaces, or characters ` " & ' # \).

Confirm Password

Enter the same password for confirmation.

Authority

Sets the file sharing access rights for an FTP user; either **Read and Write** or **Read**. An FTP user with Read access can only download shared files. An FTP user with Read and Write access can download and upload files to the USB storage, however they cannot delete or modify any existing shared folders or files (existing files can be overwritten).

Enable

Select **Yes** to enable the user account for USB access.

File Sharing settings

The router supports a file sharing function based on Windows Network Neighborhood (depending on a user's access rights to the shared folders). That is, the shared folders and files on the USB drive appear to Microsoft Windows users as normal Windows folders accessible on the network. Users can use Windows Network Neighborhood to access files on the USB drive. A maximum of 32 shared folders can be defined.

File Sharing

This page allows you to configure access to the USB file sharing system.

Enable

Global Setting

Work Group (1 - 255 characters)
Host Name (1 - 15 characters)

Folder Sharing

Folder
Allowable Users
Folder Access

Folder Name	Allowable Users	Folder Access	Action
sda1/Chris-Data	User123	Read and Write	<input type="button" value="🗑️"/> <input type="button" value="✎"/>

This page includes the following settings:

Global Setting

- **Work Group:** The Windows networking group name. Enter 1-255 characters (do not use characters ` ` " & ' # \.)
- **Host Name:** A name that identifies the router in the Windows network. Enter 1-15 characters (do not use characters ` ` " & ' # \.)

Folder Sharing

- **Folder:** A name of a folder on the USB drive that you want to share. Click in the field to browse and select the folder on the USB drive from the pop-up "tree-browser" window.
- **Allowable Users:** Selects a user account that is permitted to access the shared folder.
- **Folder Access:** Select **Read and Write** or **Read** access to the folder. A File Sharing user with Read access can only download files from the shared folder. A File Sharing user

with Read and Write access can download and upload files to the shared folder, however they cannot delete or modify any existing shared folders (existing files can be overwritten). Note that a shared folder allows only four File Sharing client connections at one time.

FTP settings

The router can be presented as an FTP server to provide a file transfer service (depending on a user's access rights to the shared folders). Users can set up the FTP server to share or download files to local or remote users through the router. A maximum of 32 shared folders can be defined.

FTP ?

This page allows you to configure the FTP parameters for access to files stored on the USB storage device.

Enable

Global Setting

Max Client (1 - 5)

Network Sharing

Folder

Allowable Users

Folder Name	Allowable Users	Authority	Action
sda1/Chris-Data	User456	Read and Write	<input type="button" value="🗑️"/> <input type="button" value="✎"/>

This page includes the following settings:

Global Setting

- **Max Client:** Set the maximum number of FTP connections (different IP addresses) permitted at one time (range: 1 to 5). Only one connection from the same user (same IP address) is allowed at one time.

Network Sharing

- **Folder:** A name of a folder on the USB drive that you want to share. Click in the field to browse and select the folder on the USB drive from the pop-up "tree-browser" window.
- **Allowable Users:** Selects a user account that is permitted to access the shared folder.

Safe removal

To ensure USB data correctness, this router supports a USB safe removal function. Click **Remove** before unplugging a USB drive.

Safe Removal 

The router supports a USB safe removal function. Click the "Remove" button before unplugging a USB drive.

Safe Removal **Remove**

14 Tools

The router includes a number of system tools for managing software and configuration files, troubleshooting network problems, and sending email alert messages. All tools and utilities are described in this chapter.

Viewing tools status

This page displays the current versions of firmware installed on the router, the status of the email alert feature, and lists any configured time schedules.

Status		?
Active Firmware Version	V1.0.0.0-R110-B0002	
Backup Firmware Version	V0.1.2.10-R110-B0001	
Email Alert	Disabled	
Schedule	"Test1"	

[Refresh](#)

Updating software

The Software page displays the current software versions installed on the router. You can upgrade the software installed on the router to a new version downloaded from the HP support website.

The router supports a dual-image function, which means that if the router fails to boot the active image, it automatically boots from the backup image. Upgrading the software replaces the backup image and reboots the router.

Software		?
This page allows you to upgrade the router software. The upgrade process automatically updates the backup image and reboots the device.		
Firmware Version		
Active Image	V1.0.0.0-R110-B0010	
Backup Image	V1.0.0.0-R110-B0009	
Switch to Backup	<input type="checkbox"/>	
Update		
Reset Configuration	<input type="checkbox"/>	
Transfer Method	<input checked="" type="radio"/> HTTP <input type="radio"/> TFTP	
Firmware File	<input type="text"/> Browse...	

[Start](#) [Cancel](#)

This page includes the following settings:

Firmware Version

Displays the software versions installed on the router.

- **Active Image:** The version number of the software currently running on the router.
- **Backup image:** The version number of the software installed as a backup on the router.
- **Switch to Backup:** Selecting this option and clicking **Start** reboots the router using the backup software image.

Update

To upgrade the software on the router, browse to the location of the software upgrade file on your computer by clicking **Browse**, and then click **Start**.

- **Reset Configuration:** Select this option if you want to reset all settings to factory defaults after updating the software.
- **Transfer Method:** Select either HTTP (web browser) or TFTP (requires server). If you select HTTP, you can download the software file from your computer. The TFTP option requires the software file to be placed on a computer running a TFTP server utility. The TFTP server IPv4 address and software file name must be entered.
- **Firmware File:** Locates the software file on the local computer when using the HTTP transfer method.

Saving configuration settings

You can save your current router configuration or restore a previously saved configuration by using this feature. Saving your configuration allows you to restore it later if your settings are lost or changed. HP recommends that you backup your current configuration before performing a firmware update.

Configuration ?

This page allows you to save the configuration of the router to a binary file. The file can later be uploaded to restore the routers configuration settings.

Restore All Settings to Factory Default
 Backup Settings
 Restore Settings

Save **Cancel**

Restore all settings to factory default

Using this option restores all of the router's settings to factory default values. HP recommends that you backup your settings before you restore all of the defaults.

Configuration ?

This page allows you to save the configuration of the router to a binary file. The file can later be uploaded to restore the routers configuration settings.

Restore All Settings to Factory Default
 Backup Settings
 Restore Settings

Configuration Backup

Transfer Method HTTP TFTP

TFTP Server IPv4 Address . . .

Save **Cancel**

Backup settings

Select to backup the router's settings. Select HTTP or TFTP as the transfer method (TFTP requires the server IPv4 address), and then click **Save**.

Configuration ?

This page allows you to save the configuration of the router to a binary file. The file can later be uploaded to restore the routers configuration settings.

Restore All Settings to Factory Default
 Backup Settings
 Restore Settings

Configuration Restore

Transfer Method HTTP TFTP

File Upload **Browse...**

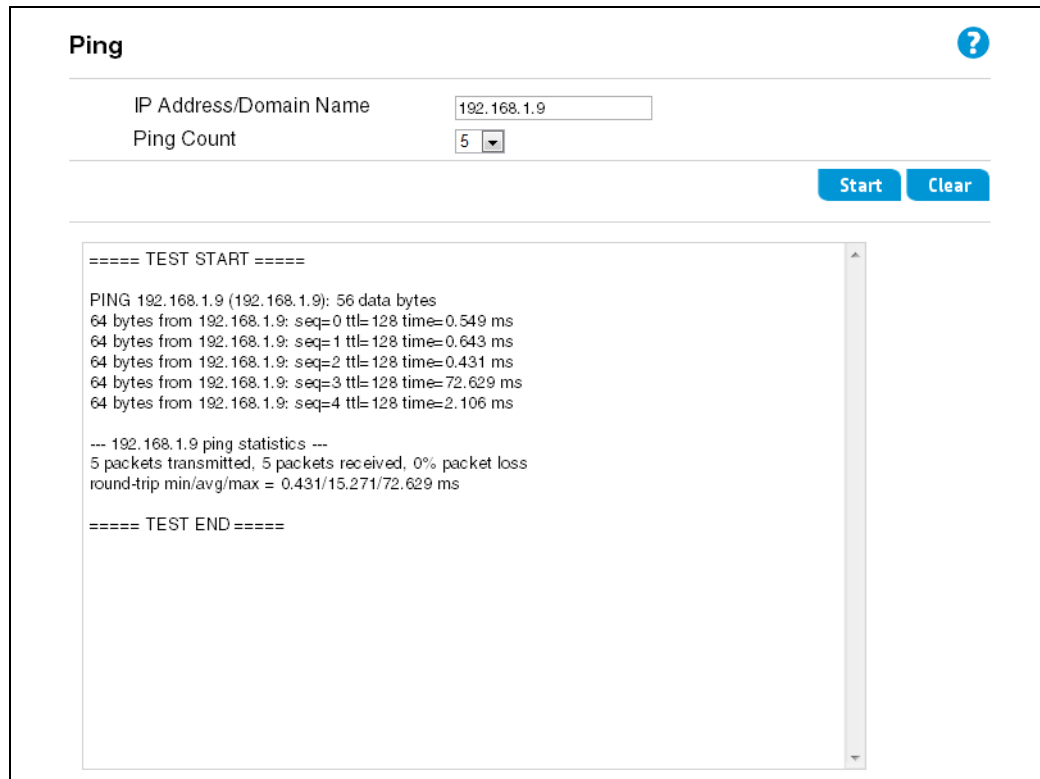
Save **Cancel**

Restore settings

Select to restore the router's settings and choose HTTP or TFTP as the transfer method. For HTTP, browse button to the location of the saved configuration file on the management computer. For TFTP, specify the file path and name on the TFTP server and enter the IPv4 server address. Click **Save** to restore the saved settings.

Ping

Ping is a network tool that sends ICMP ECHO_REQUEST datagrams to a remote host and elicits an ICMP ECHO_RESPONSE datagrams from the remote host. Enter the IPv4 or IPv6 address, or enter the domain name of the host, select the number of pings to send, and then click **Start**.



The screenshot shows a web-based Ping tool interface. At the top, the title "Ping" is displayed next to a help icon. Below the title, there are two input fields: "IP Address/Domain Name" with the value "192.168.1.9" and "Ping Count" with a dropdown menu set to "5". To the right of these fields are two buttons: "Start" and "Clear". Below the input fields is a large text area containing the following output:

```
==== TEST START =====  
  
PING 192.168.1.9 (192.168.1.9): 56 data bytes  
64 bytes from 192.168.1.9: seq=0 ttl=128 time=0.549 ms  
64 bytes from 192.168.1.9: seq=1 ttl=128 time=0.643 ms  
64 bytes from 192.168.1.9: seq=2 ttl=128 time=0.431 ms  
64 bytes from 192.168.1.9: seq=3 ttl=128 time=72.629 ms  
64 bytes from 192.168.1.9: seq=4 ttl=128 time=2.106 ms  
  
--- 192.168.1.9 ping statistics ---  
5 packets transmitted, 5 packets received, 0% packet loss  
round-trip min/avg/max = 0.431/15.271/72.629 ms  
  
==== TEST END =====
```

This page includes the following settings:

IP Address/Domain Name

You can specify an IPv4 address, an IPv6 address, or a hostname.

Ping Count

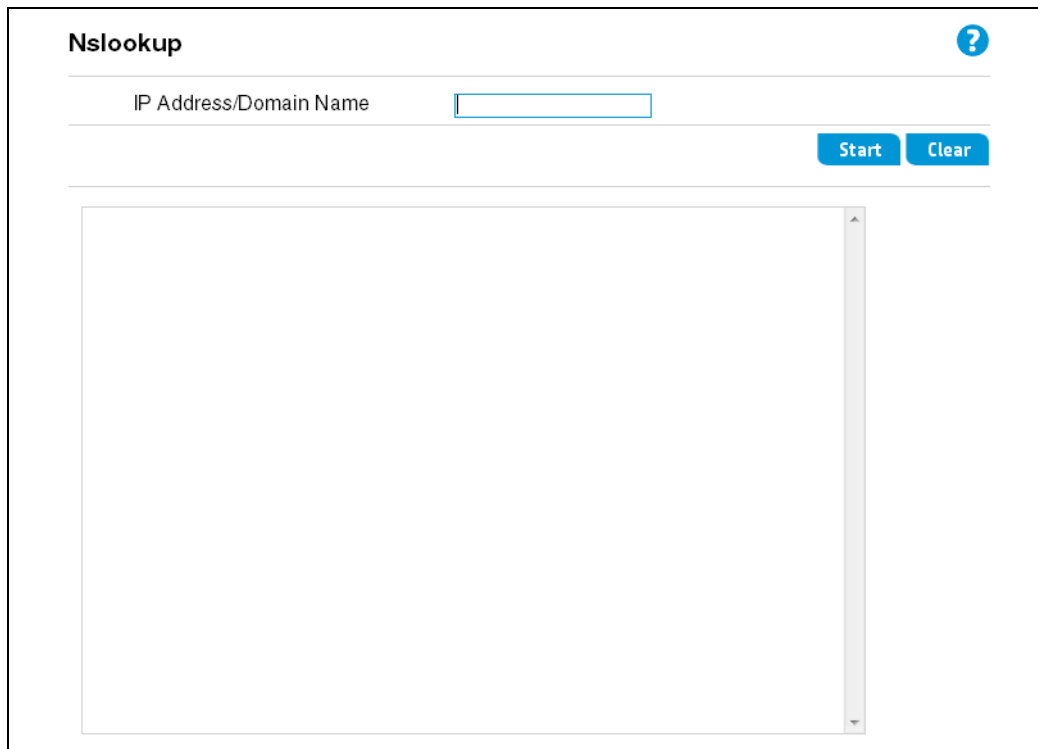
Specify the number of pings to send (1, 3, 5, 10, or 20).

Results

The results window shows the size and number of each packet sent and, if the host is reached, the size and number of each packet received in response and its round-trip time. It also displays statistics about packet loss and, if the host is reached, the average round-trip time for all packets.

Nslookup

Nslookup is a DNS client that sends DNS requests to a DNS server to find the corresponding IP address of a target host name, or the host name of a target IP address.



The screenshot shows the Nslookup web interface. At the top left, the title "Nslookup" is displayed in a bold, dark blue font. To the right of the title is a small blue circular icon containing a white question mark. Below the title is a horizontal line. Underneath this line is a text input field with the placeholder text "IP Address/Domain Name". To the right of the input field are two blue buttons: "Start" and "Clear". Below the input field and buttons is another horizontal line. Underneath this line is a large, empty rectangular area with a vertical scrollbar on the right side, intended for displaying the results of the DNS lookup.

Traceroute

Traceroute is a network tool that sends packets to a destination and produces a list of hosts that the packets have traversed to the destination. Traceroute works by increasing the "time-to-live" value of each successive batch of packets sent. The first three packets have a time-to-live (TTL) value of one (implying that they make a single hop). The next three packets have a TTL value of 2, and so on. When a packet passes through a host, typically the host decrements the TTL value by one, and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded (type 11) packet to the sender. The Traceroute utility uses these returning packets to produce a list of hosts that the packets have traversed to the destination. Traceroute does not list the real hosts, it indicates that the first host is at one hop, the second host at two hops. The IP protocol does not guarantee that all the packets take the same route.

Traceroute ?

IP Address/Domain Name

Start
Clear

Email alert

The Email alert feature allows the router to automatically send email messages when an event at or above a configured severity level occurs.

Email Alert ?

This page allows you to configure email alerts based on syslog message severity levels.

Enable	<input checked="" type="checkbox"/>	
From E-mail Address	<input type="text"/>	
To E-mail Address	<input type="text"/>	
SMTP Server Address	<input type="text"/>	
SMTP Server Port	<input type="text" value="25"/> (1 - 1023)	
Encryption	<input type="text" value="NONE"/> ▼	
Username	<input type="text"/>	(1 - 60 characters) (optional)
Password	<input type="text"/>	(1 - 60 characters) (optional)
Confirm Password	<input type="text"/>	(1 - 60 characters) (optional)
Alert Level	<input type="text" value="ALERT"/> ▼	

Save
Cancel

This page includes the following settings:

From E-mail Address

Sets the email address that is used in the "From" field of alert messages. You can use a symbolic email address that identifies the router, or the address of an administrator responsible for the router.

To E-mail Address

The recipient email address of the alert messages.

SMTP Server Address

The IPv4 or IPv6 address of the mail server.

SMTP Server Port

The TCP port number used by the SMTP server. The SMTP protocol typically uses port 25.

Encryption

If you choose to use secure connection to the mail server, select **TLS/SSL** and then enter the required user name and password.

Username

The user name to connect with the mail server. (Do not use characters ` " & ' # \)

Password

The password to use for the mail server. (Do not use characters ` " & ' # \)

Confirm Password

Enter the password again to confirm it.

Alert Level

Sets the syslog severity threshold level used to trigger alert messages. The alert levels from the lowest to the highest are Debug, Informational, Notice, Warning, Error, Critical, Alert, and Emergency. All events at the set level and higher will be sent to the configured email recipient. For example, setting the Warning level will report all events from Warning to Emergency.

Caution

Setting the Alert Level too low can result in a very high number of emails being sent to the recipient. HP recommends to only set the highest two or three levels.

Scheduling

The Scheduling feature enables the scheduling of access control and LAN server rules. Each access control or LAN server rule can be selectively activated at a predefined scheduled time. The user must first define a schedule rule on the Scheduling page, and then associate the schedule rule with a control rule on the Firewall and Wireless pages. A maximum of 10 schedule rules can be defined.

Scheduling ?

Scheduling rules can be applied to certain features of the router. This page allows you to configure scheduling rules that can be activated on specific days and times.

Rules Name



Comment (0 - 31 characters)

Date	Start Time (hh:mm)	End Time (hh:mm)
Monday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Tuesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Wednesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Thursday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Friday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Saturday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Sunday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Daily	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>

*Only accept 24 hours

Add

Rules List

Rules Name	Rules Comment	Date	Action
Test1	test schedule	Everyday 18:00-23:00	 

Save **Cancel**

This page includes the following settings:

Rules Name

A name for the scheduling rule. (Do not use the characters ` " & ' # \.)

Comment

A comment of up to 31 characters that describes the scheduling rule. (Do not use the characters ` " & ' # \.)

Date

Selects a day of the week, or daily.

Start/End Time


Specify the start and end times for the schedule in the standard 24 hour format.

Rules List

This table includes all the configured schedules on the router.

Support file

This function allows you download the router's information for support assistance. The file is saved on your local computer with the name "showtech.rtf". This is a text readable file that includes the model, software version, wireless and other basic settings, as well as the ARP table, memory usage information, and the current system log.


Support File 

This page allows you to download system information to a file for technical support assistance.

[Download](#)

Viewing the EULA

This page displays the HP End User License Agreement content.

EULA 

This page displays the HP End User License Agreement content.

HP end user license agreement

End User License Agreement
=====

PLEASE READ CAREFULLY BEFORE USING THIS EQUIPMENT: This End-User license Agreement ("EULA") is a legal agreement between (a) you (either an individual or a single entity) and (b) Hewlett-Packard Company or in-country legal entity ("HP") that governs your use of any Software Product, which is either (i) installed on or made available by HP for use with your HP product ("HP Product") or (ii) made available as part of the HP product portfolio for use on a standalone basis ("HP Software Product"), that is not otherwise subject to a separate license agreement between you and HP or its suppliers. Other software may contain a EULA in its online documentation. The term "Software Product" means computer software and may include associated media, printed materials and "online" or electronic documentation. An amendment or addendum to this EULA may accompany the HP Product or HP Software Product.

RIGHTS IN THE SOFTWARE PRODUCT ARE OFFERED ONLY ON THE CONDITION THAT YOU AGREE TO ALL TERMS AND CONDITIONS OF THIS EULA. BY INSTALLING, COPYING, DOWNLOADING OR OTHERWISE USING THE SOFTWARE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT ACCEPT THESE LICENSE TERMS, YOUR SOLE REMEDY IS TO

15 Support and other resources

Online documentation

You can download documentation from the HP Support Center website at: www.hp.com/support/manuals. Search by product number or name.

Contacting HP

For worldwide technical support information, see the HP Networking Support website: www.hp.com/networking/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Problem description and any detailed questions

HP websites

For additional information, see the following HP websites:

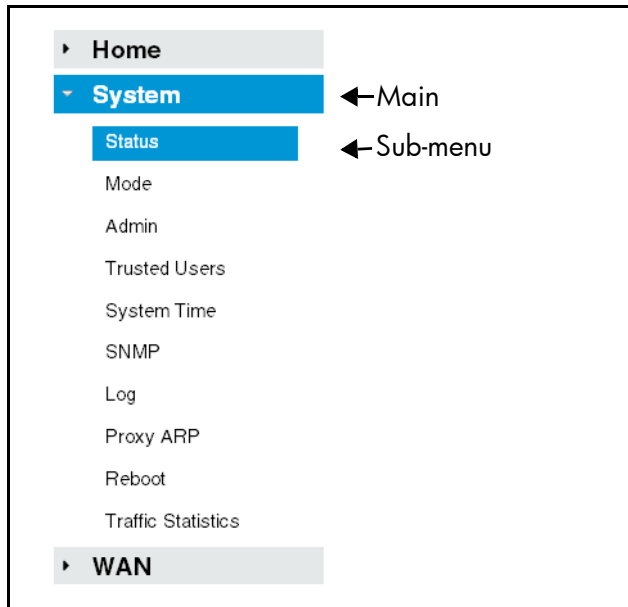
- www.hp.com/networking
- www.hp.com

Conventions

The following conventions are used in this guide.

Management tool

This guide uses specific syntax when directing you to interact with the web management user interface. Refer to the following image for identification of key user-interface elements and then the table below for example directions:



Example directions in this guide	What to do in the user interface
Select System > Admin .	Select System on the main menu, and then select Admin on the sub-menu.
Set Radio Mode to 11 n only .	For the Radio Mode setting, select 11 n only from the list.

A Resetting to factory defaults

Factory reset procedures

To force the router into its factory default state, follow the procedures in this section.

Caution

Resetting the router to factory defaults deletes all configuration settings, resets the manager user name and password to **admin**, and sets the IPv4 address to 192.168.1.1.

Using the reset button

Using a tool such as a paper clip, press and hold the reset button for more than three seconds, then release.

Using the management interface

1. Launch the web-based management interface (default <https://192.168.1.1>).
2. Select **Tools > Configuration**.
3. Select **Restore All Settings to Factory Default**, and then click **Save**.

Configuration ?

This page allows you to save the configuration of the router to a binary file. The file can later be uploaded to restore the routers configuration settings.

- Restore All Settings to Factory Default
- Backup Settings
- Restore Settings

Save **Cancel**

B Factory default settings

Feature	Parameter	Default
Mode	System Mode	Router
Admin General Settings	System Name	HP-R110 / HP-R120
	System Location	<i>Null</i>
	System Contact	<i>Null</i>
Administrator Login	Username	admin
	Password	admin
Country Code	Country Code	AM Models: US WW Models: <i>Null</i>
Web Server	HTTP Server	Enabled
	HTTPs Server	Enabled
	Session Timeout	5 minutes
Trusted Users	MAC/IP Address	<i>None configured</i>
System Time	Set System Time	SNTP
	System Date	2013-01-01
	System Time	00:00
	Time Server Address	pool.ntp.org
	Time Zone	-08:00 Pacific Time (US)
	Daylight Saving	Enabled
SNMP	Enable SNMP	Enabled
	Read Community	public
	Write Community	private
	Trap Receiver IP Address	<i>Null</i>
	Trap Receiver Port	162
	Trap Community	<i>Null</i>

Feature	Parameter	Default
System logs	System Log Level	INFORMATIONAL
	Max Size	256
	Log Prefix	<i>Null</i>
	Remote Syslog Configuration	Disabled
	Remote IP Address	<i>Null</i>
	Remote Port	514
	Remote Log Level	DEBUG
Proxy ARP	Enable Proxy ARP	Disabled
WAN settings	Connection Type	DHCP
	Host Name	HP-R110 / HP-R120
	Static IP Address	0.0.0.0
	Static Subnet Mask	0.0.0.0
	Static Gateway	0.0.0.0
	Primary DNS Address	0.0.0.0
	Secondary DNS Address	0.0.0.0
	PPPoE Username	<i>Null</i>
	PPPoE Password	<i>Null</i>
	PPPoE Service Name	<i>Null</i>
	PPPoE Idle Time	Always On
	PPPoE MTU	1454 bytes
	Multiple-PPPoE	Disabled
	PPPoE Routing Table	Disabled
	PPTP Server IP	0.0.0.0
	PPTP Username	<i>Null</i>
	PPTP Password	<i>Null</i>
	PPTP Idle Time	Always On
	PPTP DHCP Enable	Disabled
	L2TP Server IP	0.0.0.0
	L2TP Username	<i>Null</i>
L2TP Password	<i>Null</i>	
L2TP Idle Time	Always On	
L2TP DHCP Enable	Disabled	

Feature	Parameter	Default
DDNS	Enable DDNS	Disabled
	DDNS Server	DynDNS.org
	Domain Name	<i>Null</i>
	Username	<i>Null</i>
	Password	<i>Null</i>
MAC Clone	MAC Address	<i>Use router MAC</i>
LAN Settings	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Enable DHCP Server	Enabled
	IP Pool Starting Address	192.168.1.2
	IP Pool Ending Address	192.168.1.254
	Lease Time	1 day
	VLAN ID	1
	DHCP Relay	Disabled
VLAN	Spanning Tree	Disabled
	Default VLAN ID	1
	VLAN Port Membership	LAN 1, 2, 3, 4, WLAN 1 default VLAN, untagged
IGMP	Block routing between VLANs	Enabled
	Enable IGMP Proxy	Enabled
	Enable IGMP Snooping	Enabled

Feature	Parameter	Default
R110 Wireless, Basic	Enabled Radio	Enabled
	Radio Band	2.4GHz
	Radio Mode	11b/g/n Mixed
	Channel	Auto
	Bandwidth	20 MHz
	Enable Schedule Rules	Disabled
	VAP 1 SSID	Enabled, HP1
	VAP 2 SSID	Disabled, HP2
	VAP 3 SSID	Disabled, HP3
	VAP 4 SSID	Disabled, HP4
	Station Isolation	Disabled
	Broadcast	Enabled
	MAC Authentication	Disabled
	Authentication Mode	OPEN
Encryption Type	NONE	
R120 Wireless 2.4GHz, Basic	Enabled Radio	Enabled
	Radio Mode	11b/g/n Mixed
	Channel	Auto
	Bandwidth	20 MHz
	Enable Schedule Rules	Disabled
	VAP 1 SSID	Enabled, HP1_2G
	VAP 2 SSID	Disabled, HP2_2G
	VAP 3 SSID	Disabled, HP3_2G
	VAP 4 SSID	Disabled, HP4_2G
	Station Isolation	Disabled
	Broadcast	Enabled
	MAC Authentication	Disabled
	Authentication Mode	OPEN
	Encryption Type	NONE

Feature	Parameter	Default
R120 Wireless 5GHz, Basic	Enabled Radio	Enabled
	Radio Mode	11ac/n/a
	Channel	Auto
	Bandwidth	20/40/80 MHz
	Enable Schedule Rules	Disabled
	VAP 1 SSID	Enabled, HP1_5G
	VAP 2 SSID	Disabled, HP2_5G
	VAP 3 SSID	Disabled, HP3_5G
	VAP 4 SSID	Disabled, HP4_5G
	Station Isolation	Disabled
	Broadcast	Enabled
	MAC Authentication	Disabled
	Authentication Mode	OPEN
	Encryption Type	NONE
Wireless, Advanced	Beacon Interval	100 ms
	DTIM Interval	1 beacon
	RTS Threshold	2347 bytes
	Short Guard Interval	Enabled
	(2.4GHz) 802.11g Protection Mode	CTS to Self
	Extension Channel Protection Mode	No Protection
	(2.4GHz) Preamble Mode	Auto
	Max TX Power	100%
WDS	VAP	1
	WDS Mode	Disabled
	Authentication Mode	OPEN
	Encryption Type	NONE
WPS	WPS Enable	Enabled
	Configuration State	Unconfigured
	Lock	Disabled
	WPS Method	PIN
WMM	Enable WMM	Enabled
	Enable Power Saving	Enabled

Feature	Parameter	Default
MAC Authentication	Filter	Block all stations in list
	SSID	HP1
	MAC Address	<i>None configured</i>
VPN	Enable IPSec	Disabled
	Enable L2TP over IPSec	Disabled
	Enable PPTP	Disabled
	PPTP Passthrough	Enabled
	L2TP Passthrough	Enabled
	L2TP/IPSec Passthrough	Enabled
Dynamic Route	RIP	Disabled
	RIP Auto Summary	Disabled
	Static Route	Disabled
	RIPng	Disabled
	IPv6 Static Route	Disabled
Firewall	PING from WAN	Disabled
	MSS Clamping	Enabled
	UPnP	Disabled
	Remote Administration	Disabled
	Enable DDoS Attack Filter	Disabled
	Client Filtering	Disabled
	MAC Filtering	Disabled
	URL Filtering	Disabled
	URL Exclusion	Disabled
	Content Filtering	Disabled
SPI Settings	Disabled	
NAT	NAT	Enabled
	Virtual Server	Disabled
	DMZ	Disabled
	Port Trigger	Disabled
	ALG SIP	Enabled
	ALG H323	Enabled

Feature	Parameter	Default
IPv6	IPv6 Connection	Disabled
	MLD Proxy	Disabled
	DHCP-PD	Enabled
QoS	QoS	Enabled
	Traffic Mapping	Disabled
USB	User Account	Disabled
	File Sharing	Disabled
	FTP	Disabled
Tools	Email Alert	Disabled
	Scheduling Rules	<i>None configured</i>

