UBIQUITI NETWORKS

EdgeOS™

Operating System for Ubiquiti EdgeRouters

Release Version: 1.8

User Guide

Table of Contents

Chapter 1: Overview 1
Introduction 1
Configuration Interface System Requirements 1
Hardware Overview and Installation 1
Typical Deployment Scenarios 1

Chapter 2: Using EdgeOS 3
Ports and Status Information 3
Navigation 3
Common Interface Options 4

Chapter 3: Dashboard 9
Hardware 9
Services 9
Interfaces 10

Chapter 4: Traffic Analysis 17
Traffic Analysis 17
Top Hosts 18
Hosts 18
Category 19

Chapter 5: Routing 21
IPv6 Routing 21
Routes 22
OSPF 24

Chapter 6: Firewall/NAT 27
Port Forwarding 27
Firewall Policies 28
NAT 33
Firewall/NAT Groups 36

Chapter 7: Services 39
DHCP Server 39
DNS 43
PPPoE 44

Chapter 8: VPN 45
PPTP Remote Access 45
IPsec Site-to-Site 46

Chapter 9: QoS 49
Smart Queue 49
Advanced Queue 51
Chapter 10: Users 59
Local 59
Remote 60
Chapter 11: Config Tree 61
User Interface 61
Discard and Preview 62
CLI Modes 62
Configuration Example 62
Chapter 12: Wizards 65
Setup Wizards 65
Feature Wizards 78
Chapter 13: Toolbox 79
Ping 79
Bandwidth 80
Trace 80
Discover 81
Packet Capture 81
Log Monitor 82
Appendix A: Command Line Interface 83
Overview 83
Access the CLI 83
CLI Modes 85
Appendix B: Contact Information 93
Ubiquiti Networks Support 93

Chapter 1:Overview

Introduction

EdgeOS™ is a powerful, sophisticated operating system from Ubiquiti Networks. It allows you to manage your EdgeRouter and networks. This User Guide is designed for use with version 1.8 or above of the EdgeOS Configuration Interface and all of the EdgePoint and EdgeRouter models, which this User Guide will collectively refer to as EdgeRouter. Additional information is available on our website at:

http://community.ubnt.com/edgemax

http://documentation.ubnt.com/edgemax

Configuration

The intuitive EdgeOS Configuration Interface allows you to conveniently manage your EdgeRouter using your web browser. (See **"Using EdgeOS" on page 3** for more information.) If you need to configure advanced features or prefer configuration by command line, you can use the config tree or the Command Line Interface (CLI). (See **"Config Tree" on page 61** or **"Command Line Interface" on page 83** for more information.)

Configuration Interface System Requirements

- Microsoft Windows 7, Windows 8, Windows 10, Linux, or Mac OS X
- Web Browser: Google Chrome, Mozilla Firefox, Microsoft Edge, or Microsoft Internet Explorer 8 (or above)

Hardware Overview and Installation

The Quick Start Guide that accompanied your EdgeRouter includes a hardware description and instructions for hardware installation.

Typical Deployment Scenarios

While there are numerous scenarios that are possible, this section highlights three typical deployments:

- Small Office/Home Office (SOHO) Deployment
- Service Provider Deployment
- Corporate Deployment

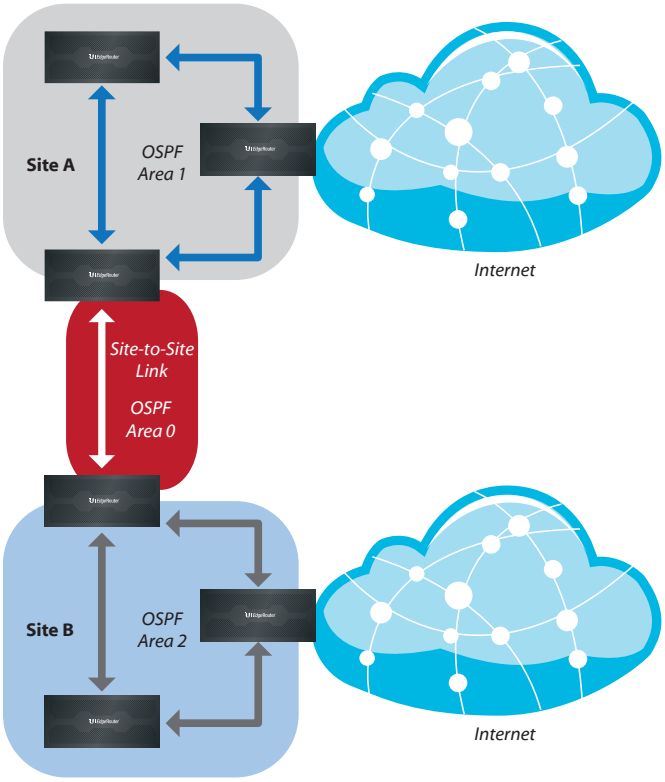
SOHO Deployment

Click the **Wizards** tab and follow the on-screen instructions. See **"SOHO Deployment Wizards" on page 71** for more information.

Service Provider Deployment

This scenario uses six EdgeRouter devices:

1. OSPF Area 0 to OSPF Area 1
2. OSPF Area 0 to OSPF Area 2
3. OSPF Area 1
4. OSPF Area 1 to Internet
5. OSPF Area 2
6. OSPF Area 2 to Internet



Here are the typical steps to follow:

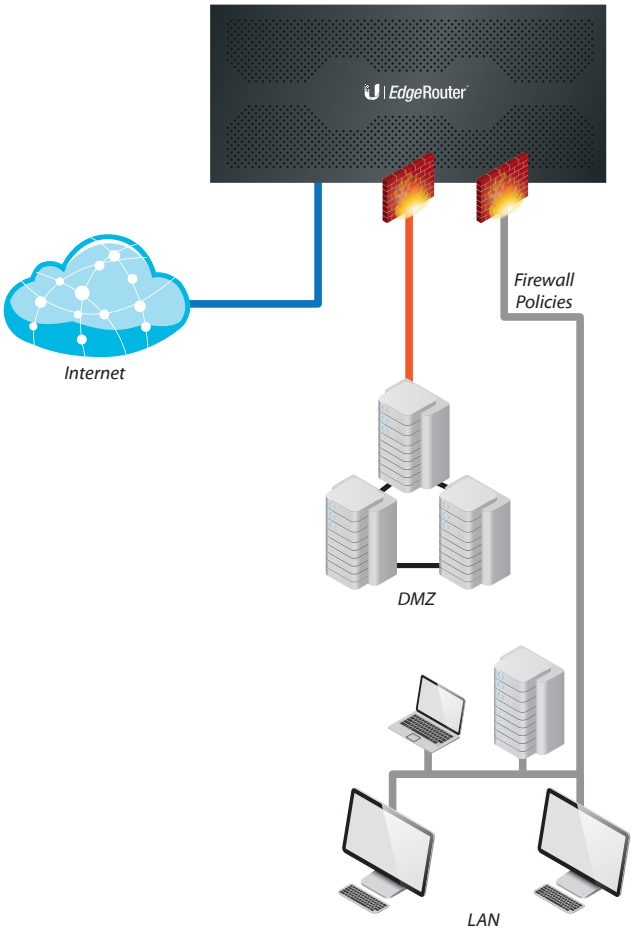
1. Configure the appropriate settings on the *System* tab (see **"System" on page 4** for more information):
   - *Host Name*
   - *Time Zone*
   - *Gateway*
   - *Name Server*
   - *Domain Name*
   - *NTP*
2. Configure the interfaces on the *Dashboard* tab; see **"Interfaces" on page 10** for more information.
3. Configure OSPF settings on the *Routing* > *OSPF* tab; see **"OSPF" on page 24** for more information.
4. Configure DHCP server(s) on the *Services* tab; see **"DHCP Server" on page 39** for more information.
5. Configure NAT rules on the *Firewall/NAT* > *NAT* tab; see **"NAT" on page 33** for more information.

6. Configure firewall rules on the *Firewall/NAT* > *Firewall Policies* tab; see **"Firewall Policies" on page 28** for more information.
7. Configure additional settings as needed for your network.

Corporate Deployment

This scenario uses a single EdgeRouter device. The three independent interfaces connect to the following:

- Internet
- DMZ
- LAN



Here are the typical steps to follow:

1. Configure the appropriate settings on the *System* tab (see **"System" on page 4** for more information):
   - *Host Name*
   - *Time Zone*
   - *Gateway*
   - *Name Server*
   - *Domain Name*
   - *NTP*
2. Configure the interfaces on the *Dashboard* tab; see **"Interfaces" on page 10** for more information.
3. Configure DHCP server(s) on the *Services* tab; see **"DHCP Server" on page 39** for more information.
4. Configure NAT rules on the *Firewall/NAT* > *NAT* tab; see **"NAT" on page 33** for more information.
5. Configure firewall rules on the *Firewall/NAT* > *Firewall Policies* tab; see **"Firewall Policies" on page 28** for more information.
6. Configure additional settings as needed for your network.

Chapter 2: Using EdgeOS

EdgeOS is a powerful, sophisticated operating system that manages your EdgeRouter. It offers both a browser-based interface (EdgeOS Configuration Interface) for easy configuration and a Command Line Interface (CLI) for advanced configuration.

To access the EdgeOS Configuration Interface:

1. Connect an Ethernet cable from the Ethernet port of your computer to the port labeled *eth0* on the EdgeRouter.

2. Configure the Ethernet adapter on your computer with a static IP address on the 192.168.1.x subnet (e.g., 192.168.1.100).

   Note: As an alternative, you can connect a serial cable to the *Console* port of the EdgeRouter. See **"Command Line Interface" on page 83** for more information.

3. Launch your web browser. Type **https://192.168.1.1** in the address field. Press **enter** (PC) or **return** (Mac).

4. The login screen will appear. Enter **ubnt** in the *Username* and *Password* fields. Read the Ubiquiti License Agreement, and check the box next to *I agree to the terms of this License Agreement* to accept it. Click **Login**.

The EdgeOS Configuration Interface will appear, allowing you to customize your settings as needed.

Note: To enhance security, we recommend that you change the default login using one of the following:

- Set up a new user account on the *Users* > *Local* tab (preferred option). For details, go to **"Local" on page 59**.
- Change the default password of the *ubnt* login on the *Users* > *Local* tab. For details, go to **"Configure the User" on page 60**.

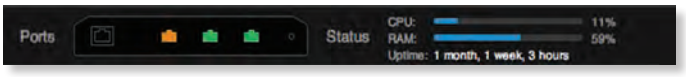
Ports and Status Information

The *Ports* image displays the active connections. A purple port indicates 10 Mbps, an amber port indicates 100 Mbps, and a green port indicates 1000 Mbps. The *Status* bar graphs display the following:

CPU The percentage of processing power used by the EdgeRouter.

RAM The percentage of RAM used by the EdgeRouter.

Uptime The duration of the EdgeRouter's activity.



Place your mouse over a port to view the following:

Enabled/Disabled The administrative status is displayed.

Link The connection status is displayed.

Speed The speed (in Mbps) and duplex mode are displayed.

Navigation

The EdgeOS software consists of 10 primary tabs, and some of these tabs have sub-tabs. This User Guide covers each tab with a chapter. For details on a specific tab, refer to the appropriate chapter.

- **Dashboard** **"Dashboard" on page 9** displays status information about services and interfaces. You can also configure interfaces and Virtual Local Area Networks (VLANs).
- **Traffic Analysis** **"Traffic Analysis" on page 17** displays Deep Packet Inspection (DPI) information about the applications and IP addresses using the most bandwidth.
- **Routing** **"Routing" on page 21** configures static routes and Open Shortest Path First (OSPF) settings, including metrics, areas, and interfaces.
- **Firewall/NAT** **"Firewall/NAT" on page 27** configures port forwarding, firewall policies, Network Address Translation (NAT) rules, and firewall/NAT groups.
- **Services** **"Services" on page 39** configures DHCP servers, DNS forwarding, and the PPPoE server.
- **VPN** **"VPN" on page 45** configures PPTP remote access and IPSec site-to-site VPN options.

- **QoS** **"QoS" on page 49** configures Smart Queue and Advanced Queue management.
- **Users** **"Users" on page 59** configures user accounts with administrator or operator access.
- **Config Tree** **"Config Tree" on page 61** is a graphical representation of the CLI config settings.
- **Wizards** **"Wizards" on page 65** offers a variety of wizards: setup wizards that configure the EdgeRouter for typical SOHO deployments, load balancing wizards, and feature wizards that configure TCP MSS clamping and UPnP.

Depending on the tab you click, some of the screens display information and options in multiple sections. You can click the **open/close** tab to hide or display a section.

Common Interface Options

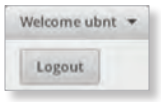
The common interface options are accessible from all tabs on the EdgeOS interface:

- Welcome
- CLI
- Toolbox
- Alerts
- System

Required fields are marked by a blue asterisk *. When the information ⓘ icon is displayed, you can click the icon for more information about an option.

Welcome

At the top left of the screen, click **Welcome** to view the *Logout* option:



Logout To manually log out of the EdgeRouter Configuration Interface, click this option.

CLI

Advanced users can make configuration changes using Linux commands. At the top right of the screen, click CLI. See **"Command Line Interface" on page 83** for more information.

Toolbox

At the top right of the screen, click Toolbox. The following network administration and monitoring tools are available:

- **"Ping" on page 79**
- **"Bandwidth" on page 80**
- **"Trace" on page 80**
- **"Discover" on page 81**
- **"Packet Capture" on page 81**
- **"Log Monitor" on page 82**

Alerts

The number of new alerts is displayed in a red popup.

At the bottom of the screen, click the **Alerts** tab.

A table displays the following information about each important event.

Message A description of the event is displayed.

Field The settings that are affected by the event are displayed.

Actions The following options are available:

- **Remove** Click this button to clear an alert.
- **Clear All** Click this button to clear all alerts.

Click the top right corner of the *Alerts* tab to close it.

System

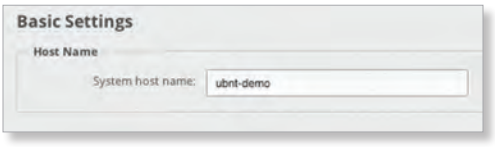
At the bottom of the screen, click the **System** tab to access the device settings.

The device settings are organized into these sections:

- **"Basic Settings" on page 5**
- **"Management Settings" on page 6**
- **"Configuration Management & Device Maintenance" on page 7**
- **"Restart & Shut Down Router" on page 7**

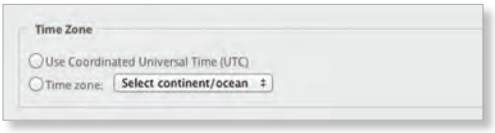
Basic Settings

Host Name



System host name Enter a name for the EdgeRouter. The host name identifies the EdgeRouter as a specific device. For example, a .com URL typically uses this format: <*host_name*>.domain_name.com

Time Zone



Use Coordinated Universal Time (UTC) UTC is the international time standard used by Network Time Protocol (NTP) servers. If your routers are located in multiple time zones, then you may want to use UTC.

Time zone To set your network to a specific time zone, select **Time zone** and configure the following:

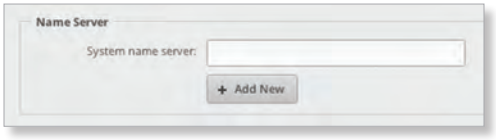
- **Select continent/ocean** Select your location.
- **Select country/region** Select your location.
- **Select time zone** Select your time zone.

Gateway

System gateway address Enter the IP address of your gateway. This will set up your default route. If you want to set up additional default routes, configure them as static routes on the *Routing* tab. See **"Routing" on page 21** for more information.

Name Server

Domain Name System (DNS) translates domain names to IP addresses; each DNS server on the Internet holds these mappings in its respective DNS database.



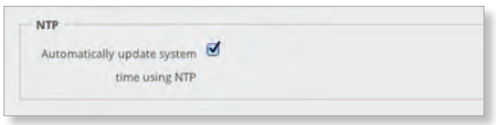
System name server Enter the IP address of your DNS server (example: *192.0.2.1* for IPv4 or *2001:db8::1* for IPv6). Click **Add New** to add additional servers.

Domain Name

System domain name Enter the domain name of your EdgeRouter. The domain name identifies the EdgeRouter's network on the Internet. For example, a .com URL typically uses this format: host_name.<*domain_name*>.com

NTP

NTP is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. You can use it to set the system time on the EdgeRouter. If the *System Log* option is enabled, then the system time is reported next to every log entry that registers a system event.

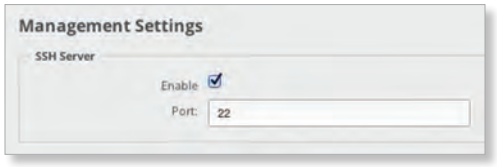


Automatically update system time using NTP By default, the EdgeRouter obtains the system time from a time server on the Internet.

Click **Save** to apply your changes.

Management Settings

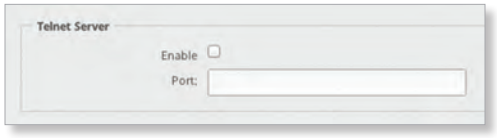
SSH Server



Enable Enabled by default. This option allows SSH (Secure Shell) access to the EdgeRouter for remote configuration by command line. SSH uses encryption and authentication, so it is a secure form of communication. See **"Command Line Interface" on page 83** for more information.

Port Specify the TCP/IP port of the SSH server. The default is *22*.

Telnet Server

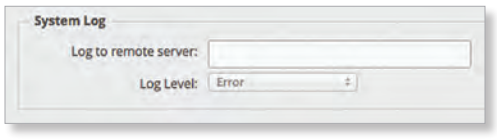


Enable Disabled by default. This option allows Telnet access to the EdgeRouter for remote configuration by command line. Telnet is not a secure form of communication, so we recommend SSH. See **"Command Line Interface" on page 83** for more information.

Port Specify the TCP/IP port of the Telnet server. The default is *23*.

System Log

Every logged message contains at least a system time and host name. Usually a specific service name that generates the system event is also specified within the message. Messages from different services have different contexts and different levels of detail. Usually error, warning, or informational system service messages are reported; however, more detailed debug level messages can also be reported. The more detailed the system messages reported, the greater the volume of log messages generated.



Log to remote server This option allows the EdgeRouter to send system log messages to a remote server. Enter the remote host IP address and TCP/IP port that should receive the system log (syslog) messages. *514* is the default port for the commonly used, system message logging utilities.

Log Level Select the appropriate level of log messages for reporting: **Emergency**, **Urgent**, **Critical**, **Error**, **Warning**, **Further Investigation**, **Informational**, or **Debug**. The default is *Error*.

Note: Properly configure the remote host to receive syslog protocol messages.

UBNT Discovery

The *UBNT Discovery* feature enables the EdgeRouter to be discovered by other Ubiquiti devices through the *Discovery* tool, which is available in the *Toolbox* (refer to **"Discover" on page 81**) or as a separate download at: **www.ubnt.com/download/utilities**

Enable Enabled by default. This option activates the *UBNT Discovery* feature.

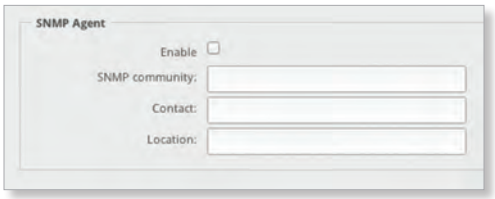
SNMP Agent

Simple Network Monitor Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. Network administrators use SNMP to monitor network-attached devices for issues that warrant attention.

The EdgeRouter contains an SNMP agent, which does the following:

- Provides an interface for device monitoring using SNMP
- Communicates with SNMP management applications for network provisioning
- Allows network administrators to monitor network performance and troubleshoot network problems

For the purpose of equipment identification, configure the SNMP agent with contact and location information:



Enable Disabled by default. This option activates the SNMP agent.

SNMP community Specify the SNMP community string. It is required to authenticate access to MIB (Management Information Base) objects and functions as an embedded password. The device supports a read-only community string; authorized management stations have read access to all the objects in the MIB except the community strings, but do not have write access. The device supports SNMP v1. The default is *public*.

Contact Specify the contact who should be notified in case of emergency.

Location Specify the physical location of the EdgeRouter.

Click **Save** to apply your changes.

Configuration Management & Device Maintenance

The controls in this section manage the device configuration routines, firmware maintenance, and reset to factory default settings.

Back Up Config

We recommend that you back up your current system configuration before updating the firmware or uploading a new configuration.

Download backup config file Click **Download** to download the current system configuration file.

Note: We strongly recommend that you save the configuration file in a secure location because it includes confidential information. The user login passwords are encrypted; however, other passwords and keys (such as those used for VPN, BGP, authentication, and RADIUS) are stored in plain text.

Restore Config

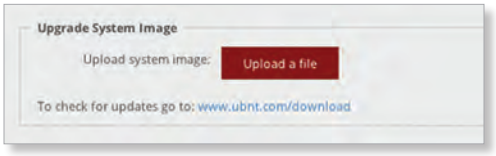
Upload config file Click **Upload a file** to locate the configuration file previously created by the *Back Up Config* option. Select the file and click **Choose**. We recommend that you back up your current system configuration before uploading the new configuration.

Note for advanced users: You can also upload a raw configuration file, */config/config.boot*, using this option.

Upgrade System Image

Download the firmware file from **downloads.ubnt.com** and save it on your computer.

The firmware update is compatible with all configuration settings. The system configuration is preserved while the EdgeRouter is updated with a new firmware version. However, we recommend that you back up your current system configuration before updating the firmware.



Upload system image To update the EdgeRouter with new firmware, click **Upload a file** and locate the new firmware file. Then click **Choose**.

Please be patient, as the firmware update routine can take three to seven minutes. You cannot access the EdgeRouter until the firmware update routine is completed.

WARNING: Do not power off, do not reboot, and do not disconnect the EdgeRouter from the power supply during the firmware update process as these actions will damage the EdgeRouter!

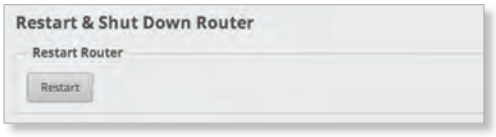
Reset Config to Default

This option resets the EdgeRouter to the default configuration. This option will reboot the EdgeRouter, and the default configuration will be restored. We recommend that you back up your current system configuration before resetting the EdgeRouter to its default configuration.

Reset to Default To reset the EdgeRouter to its default configuration, click this option.

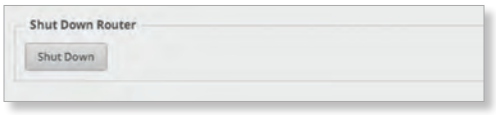
Restart & Shut Down Router

Restart Router



Restart To turn the EdgeRouter off and back on again, click this option.

Shut Down Router



Shut Down To turn off the EdgeRouter, click this option.

WARNING: Click **Shut Down** to properly shut down the EdgeRouter. An improper shutdown, such as disconnecting the EdgeRouter from its power supply, runs the risk of data corruption!

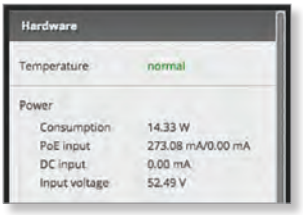
Click the top right corner of the *System* tab to close it.

Chapter 3: Dashboard

The *Dashboard* tab displays status information about services and interfaces. You can also configure interfaces and Virtual Local Area Networks (VLANs). Any setting marked with a blue asterisk * is required. When the information ⓘ icon is displayed, you can click the icon for more information about an option.

Hardware

Hardware status information is displayed for the EdgePoint EP-R8.



Temperature The status is displayed.

Power

Consumption The number of watts used by the EdgePoint is displayed.

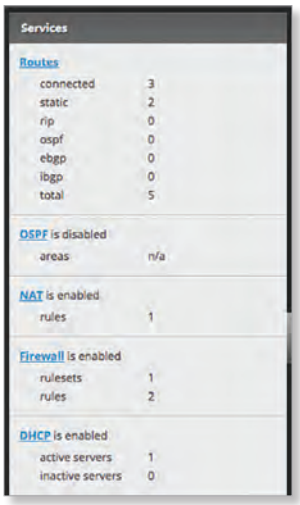
PoE input The PoE amperage is displayed.

DC input The DC amperage is displayed.

Input voltage The input voltage is displayed.

Services

Services status information is displayed. Each heading is a convenient link to the appropriate tab.



Routes

The following route types are listed:

- Connected
- Static
- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- EBGP (Exterior Border Gateway Protocol)
- IBGP (Interior Border Gateway Protocol)

The number of each route type and the total number of routes are displayed. Click **Routes** to display the *Routing* > *Routes* tab. Go to **"Routes" on page 22** for more information.

OSPF

The OSPF status, settings, and number of areas are displayed. Click **OSPF** to display the *Routing* > *OSPF* tab. Go to **"OSPF" on page 24** for more information.

NAT

The NAT (Network Address Translation) status and number of NAT rules are displayed. Click **NAT** to display the *Firewall/NAT* > *NAT* tab. Go to **"NAT" on page 33** for more information.

Firewall

The firewall status and numbers of sets and rules are displayed. Click **Firewall** to display the *Firewall/NAT* > *Firewall Policies* tab. Go to **"Firewall Policies" on page 28** for more information.

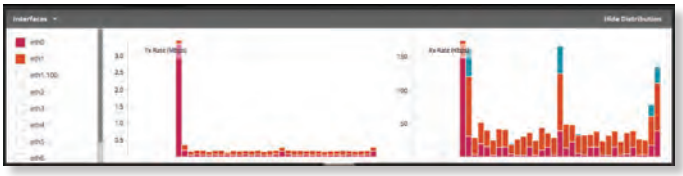
DHCP

The DHCP server status and numbers of active and inactive servers are displayed. Click **DHCP** to display the *Services* tab. Go to **"DHCP Server" on page 39** for more information.

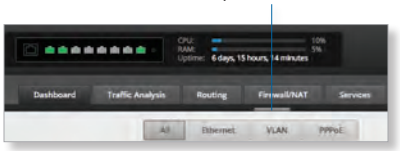
Interfaces

Distribution

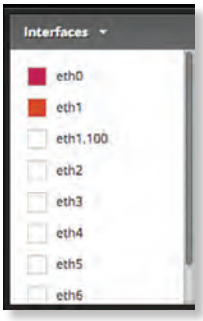
Click **Hide Distribution** to hide the *Interfaces* > *Distribution* section. Click the remaining **open/close** tab to display the *Interfaces* > *Distribution* section again.



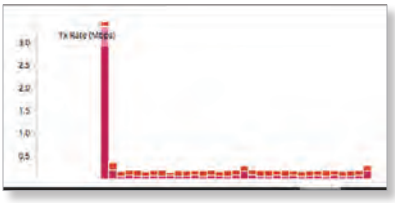
Open/Close Tab

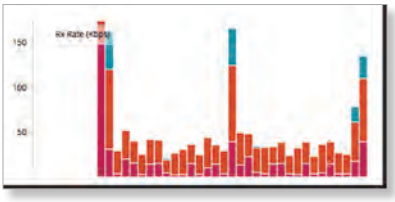


Select the physical or virtual interfaces you want to display from the *Interfaces* column. Click the ▼ to hide or display this column.

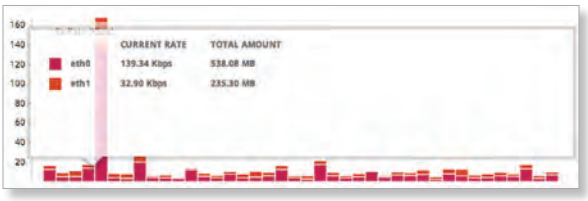


The *TX Rate* and *RX Rate* bar graphs display the current data traffic, which is color-coded to match the corresponding interface. The graph scale and throughput dimension (Mbps, for example) change dynamically depending on the mean throughput value. The statistics are updated automatically.





Place your mouse over a bar to view the *Current Rate* and *Total Amount* of traffic for the selected interfaces.

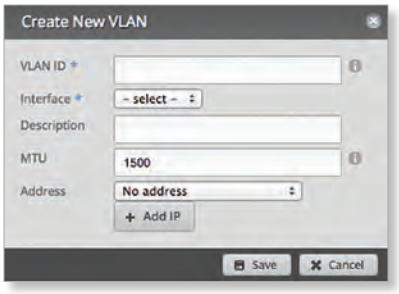


All/Ethernet/VLAN/PPPoE

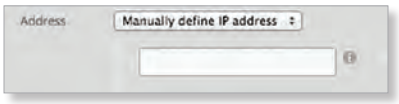
Add Interface To create a new VLAN or PPPoE interface, click **Add Interface**. Then follow the appropriate instructions for your interface type.

Add VLAN

The *Create a New VLAN* screen appears.



- **VLAN ID** The VLAN ID is a unique value assigned to each VLAN at a single device; every VLAN ID represents a different VLAN. The valid VLAN ID range is *0* to *4094*.
- **Interface** Select the appropriate interface.
- **Description** Enter keywords to describe this VLAN.
- **MTU** Enter the MTU (Maximum Transmission Unit) value, which is the maximum packet size (in bytes) that a network interface can transmit. For the ER-X, ER-X-SFP, and EP-R6, the valid MTU range is *68* to *2018*. For all other models, the valid MTU range is *68* to *9000*. The default is *1500*.
- **Address** Select one of the following:
  - **No address** The VLAN uses no address settings. (In most cases, an address is needed.)
  - **Use DHCP** The VLAN acquires network settings from a DHCPv4 server.
  - **Use DHCP for IPv6** The VLAN acquires network settings from a DHCPv6 server.
  - **Manually define IP address(es)** Enter the static IP address (example: *192.0.2.1/24* for IPv4 or *2001:db8::1/32* for IPv6).



  - **Add IP** Click **Add IP** to enter additional IP addresses.

Click **Save** to apply your changes, or click *Cancel*.

Add PPPoE

The *Create a New PPPoE* screen appears.

- **PPPoE ID** The PPPoE ID is a unique value assigned to each PPPoE connection at a single device; every PPPoE ID represents a different PPPoE connection. The valid PPPoE ID range is *0* to *15*.
- **Interface** Select the appropriate interface.
- **Account Name** Enter the username to connect to the PPPoE server; this must match the username configured on the PPPoE server.
- **Password** Enter the password to connect to the PPPoE server; this must match the password configured on the PPPoE server. Check the box to display the password.
- **MTU** Enter the MTU (Maximum Transmission Unit) value, which is the maximum packet size (in bytes) that a network interface can transmit. The valid MTU range is *68* to *1500*. The default is *1492*.

Note: Setting the MTU higher than 1492 will require ISP support and also require increasing the MTU value of the parent interface (ethX) accordingly.

Click **Save** to apply your changes, or click *Cancel*.

Search Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

All/Ethernet/VLAN/PPPoE Click the appropriate tab to filter the interfaces as needed.

- **All** All interfaces are displayed by default.
- **Ethernet** All of the Ethernet interfaces are displayed.
- **VLAN** All VLANs are displayed.

A table displays the following information about each interface. Click a column heading to sort by that heading.

Description The keywords you entered to describe the interface are displayed.

Interface The name of the interface is displayed.

Note: A switch interface is created by default (EdgeRouter PoE only); however, there are no switched ports by default. To configure ports for the switch interface, click **Actions** > **Config** and go to **"Configure the Switch" on page 14**.

Type The type of interface is displayed.

PoE (Available for the EdgePoint EP-R6, EdgePoint EP-R8, or EdgeRouter PoE only.) The status (*off*) or voltage of the *PoE* feature is displayed.

IP Addr The IP address of the interface is displayed.

MTU The MTU (Maximum Transmission Unit) value of the interface is displayed. This is the maximum packet size (in bytes) that the interface can transmit.

TX The transmit speed of the interface is displayed.

RX The receive speed of the interface is displayed.

Status The connection status of the interface is displayed.

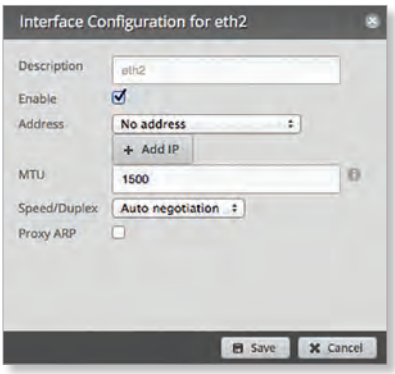
Actions Click the **Actions** button to access the following options:

- **Config** To configure the interface, click **Config**. Proceed to the appropriate interface type:
  - **ethernet** If the interface is a physical port, go to the *Configure the Interface* section in the next column.
  - **VLAN** If the interface is a VLAN, go to **"Configure the VLAN" on page 13**.
  - **PPPoE** If the interface is a PPPoE connection, go to **"Configure PPPoE" on page 13**.
  - **switch** If the interface is a switch (available for the EdgeRouter PoE only), go to **"Configure the Switch" on page 14**.
- **PoE** (Available for the EdgePoint EP-R6, EdgePoint EP-R8, or EdgeRouter PoE only.) To configure the PoE settings, click **PoE**. Go to **"Configure the PoE Settings" on page 14**.
- **Disable** Disable the interface while keeping its configuration. (The switch interface cannot be disabled.)

  Note: If you disable a port, its *PoE* functionality remains. (This applies only to the EdgeRouter PoE.)
- **Delete** (Available for VLANs only.) Delete the VLAN from the EdgeRouter configuration.

Configure the Interface

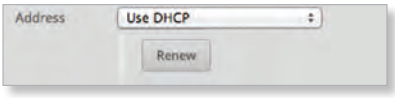
After you click *Config*, the *Interface Configuration* screen appears.



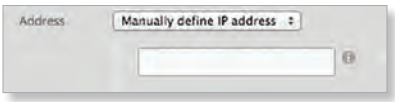
Make changes as needed.

- **Description** Enter keywords to describe this interface.
- **Enable** Check the box to enable the interface. All of the interfaces are saved in the system configuration file; however, only the enabled interfaces are active on the device.

  Note: If you disable a port, its *PoE* functionality remains. (This applies only to the EdgeRouter PoE.)
- **Address** Select one of the following:
  - **No address** The interface uses no address settings. (In most cases, an address is needed.)
  - **Use DHCP** The interface acquires network settings from a DHCPv4 server. Click the **Renew** button to acquire fresh network settings.

  - **Use DHCP for IPv6** The interface acquires network settings from a DHCPv6 server.
  - **Manually define IP address(es)** Enter the static IP address (example: *192.0.2.1/24* for IPv4 or *2001:db8::1/32* for IPv6).

  - **Add IP** Click **Add IP** to enter additional IP addresses.
- **MTU** Enter the MTU (Maximum Transmission Unit) value, which is the maximum packet size (in bytes) that a network interface can transmit. For the ER-X, ER-X-SFP, and EP-R6, the valid MTU range is *68* to *2018*. For all other models, the valid MTU range is *68* to *9000*. The default is *1500*.

- **Speed/Duplex** The default is *Auto negotiation*. The EdgeRouter automatically negotiates transmission parameters, such as speed and duplex, with its counterpart. In this process, the networked devices first share their capabilities and then choose the fastest transmission mode they both support.

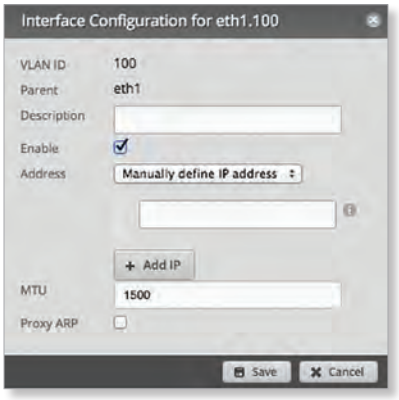
  To manually specify the transmission link speed and duplex mode, select one of the following options: **100/full**, **100/half**, **10/full**, or **10/half**.

  Full-duplex mode allows communication in both directions simultaneously. Half-duplex mode allows communication in both directions, but not simultaneously and only in one direction at a time.
- **Proxy ARP** Enable the EdgeRouter to answer a source host's ARP (Address Resolution Protocol) requests for the IP address of a destination host that is not located on the source host's network. ARP allows hosts on the same network to discover each other's IP address via a layer 2 broadcast to all MAC addresses. If they are not on the same network, the layer 2 broadcast will not reach its destination; however, the EdgeRouter can serve as the go-between if *Proxy ARP* is enabled.

  Click **Save** to apply your changes, or click *Cancel*.

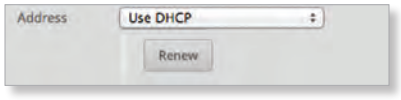
Configure the VLAN

After you click *Config*, the *Interface Configuration* screen appears.

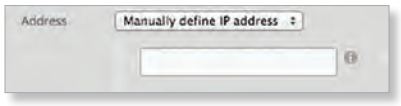


Make changes as needed.

- **VLAN ID** The VLAN ID is displayed.
- **Parent** The interface belonging to this VLAN is displayed.
- **Description** Enter keywords to describe this interface.
- **Enable** Check the box to enable the VLAN. All of the VLANs are saved in the system configuration file; however, only the enabled VLANs are active on the device.
- **Address** Select one of the following:
  - **No address** The interface uses no address settings. (In most cases, an address is needed.)
  - **Use DHCP** The interface acquires network settings from a DHCPv4 server. Click the **Renew** button to acquire fresh network settings.



  - **Use DHCP for IPv6** The interface acquires network settings from a DHCPv6 server.
  - **Manually define IP address(es)** Enter the static IP address (example: *192.0.2.1/24* for IPv4 or *2001:db8::1/32* for IPv6).

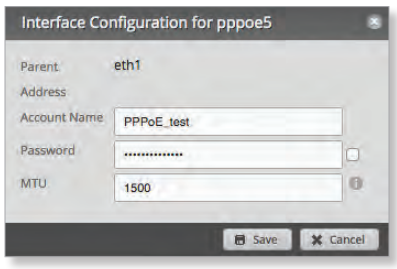


  - **Add IP** Click **Add IP** to enter additional IP addresses.
- **MTU** Enter the MTU (Maximum Transmission Unit) value, which is the maximum packet size (in bytes) that a network interface can transmit. For the ER-X, ER-X-SFP, and EP-R6, the valid MTU range is *68* to *2018*. For all other models, the valid MTU range is *68* to *9000*. The default is *1500*.
- **Proxy ARP** Enable the EdgeRouter to answer a source host's ARP (Address Resolution Protocol) requests for the IP address of a destination host that is not located on the source host's network. ARP allows hosts on the same network to discover each other's IP address via a layer 2 broadcast to all MAC addresses. If they are not on the same network, the layer 2 broadcast will not reach its destination; however, the EdgeRouter can serve as the go-between if *Proxy ARP* is enabled.

  Click **Save** to apply your changes, or click *Cancel*.

Configure PPPoE

After you click *Config*, the *Interface Configuration* screen appears.



Make changes as needed.

- **PPPoE ID** The PPPoE ID is displayed.
- **Address** The IP address is displayed.
- **Account Name** Enter the username to connect to the PPPoE server; this must match the username configured on the PPPoE server.

- **Password** Enter the password to connect to the PPPoE server; this must match the password configured on the PPPoE server. Check the box to display the password.
- **MTU** Enter the MTU (Maximum Transmission Unit) value, which is the maximum packet size (in bytes) that a network interface can transmit. The valid MTU range is *68* to *1500*. The default is *1492*.

  Note: Setting the MTU higher than 1492 will require ISP support and also require increasing the MTU value of the parent interface (ethX) accordingly.

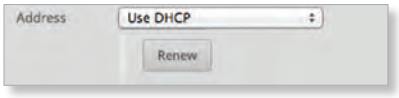
Click **Save** to apply your changes, or click *Cancel*.

Configure the Switch

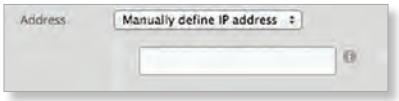
(Available for the EdgeRouter PoE only.) After you click *Config*, the *Interface Configuration* screen appears.

Make changes as needed.

- **Description** Enter keywords to describe this switch.
- **Address** Select one of the following:
  - **No address** The switch uses no address settings. (In most cases, an address is needed.)
  - **Use DHCP** The switch acquires network settings from a DHCPv4 server. Click the **Renew** button to acquire fresh network settings.



  - **Use DHCP for IPv6** The switch acquires network settings from a DHCPv6 server.
  - **Manually define IP address(es)** Enter the static IP address (example: *192.0.2.1/24* for IPv4 or *2001:db8::1/32* for IPv6). Click **Add IP** to enter additional IP addresses.



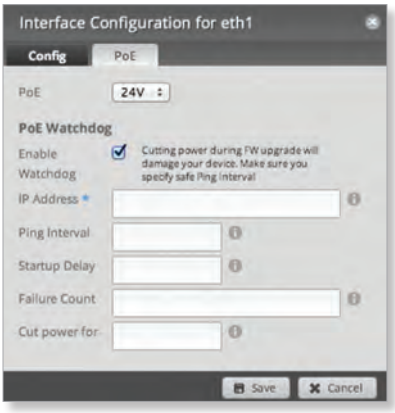
- **Switch Ports** Select the ports for the switch interface.
- **Proxy ARP** Enable the EdgeRouter to answer a source host's ARP (Address Resolution Protocol) requests for the IP address of a destination host that is not located on the source host's network. ARP allows hosts on the same network to discover each other's IP address via a layer 2 broadcast to all MAC addresses. If they are not on the same network, the layer 2 broadcast will not reach its destination; however, the EdgeRouter can serve as the go-between if *Proxy ARP* is enabled.

Click **Save** to apply your changes, or click *Cancel*.

Configure the PoE Settings

Note: Before enabling PoE, check the specifications of your airFiber, airMAX, UniFi, UniFi Video, legacy, or third-party devices to ensure they support passive PoE and require the available amount of voltage.

(Available for the EdgePoint EP-R6, EdgePoint EP-R8, or EdgeRouter PoE only.) After you click *PoE*, the *PoE* tab of the *Interface Configuration* screen appears.



PoE is disabled by default on all ports. Follow the instructions for your model:

- EdgePoint EP-R6 (below)
- EdgePoint EP-R8 (below)
- **"EdgeRouter PoE" on page 15**

EdgePoint EP-R6

- **PoE** Select one of the following:
  - **Off** To disable *PoE*, select **Off**.

    Note: To disable *PoE*, you must use this setting. If you disable a port, its *PoE* functionality remains.

  - **24V** To output 24V, 2-pair PoE to the connected device, select **24V**.

EdgePoint EP-R8

- **PoE** Select one of the following:
  - **Off** To disable *PoE*, select **Off**.

  Note: To disable *PoE*, you must use this setting. If you disable a port, its *PoE* functionality remains.
  - **24V-4pair** (Available for eth1-2 only) To output 24V, 4-pair PoE to the connected device, select **24V-4pair**.
  - **54V-4pair** (Available for eth1-2 only) To output 54V, 4-pair PoE to the connected device, select **54V-4pair**.
  - **24V** (Available for eth3-7 only) To output 24V, 2-pair PoE to the connected device, select **24V**.

EdgeRouter PoE

- **PoE** Select one of the following:
  - **Off** To disable *PoE*, select **Off**.

  Note: To disable *PoE*, you must use this setting. If you disable a port, its *PoE* functionality remains.
  - **24V** To output 24V PoE to the connected device, select **24V**.
  - **48V** To output 48V PoE to the connected device, select **48V**.

  Note: You must have a 48V power adapter (not included) powering the EdgeRouter PoE; otherwise, 48V PoE is not allowed.

PoE Watchdog

PoE Watchdog is only for PoE-enabled ports. It configures the device to continuously ping a user-defined IP address (it can be the Internet gateway, for example). If it is unable to ping under the user-defined constraints, then the device will automatically turn off PoE on the port, and then turn it back on. This option creates a kind of "fail-proof" mechanism.

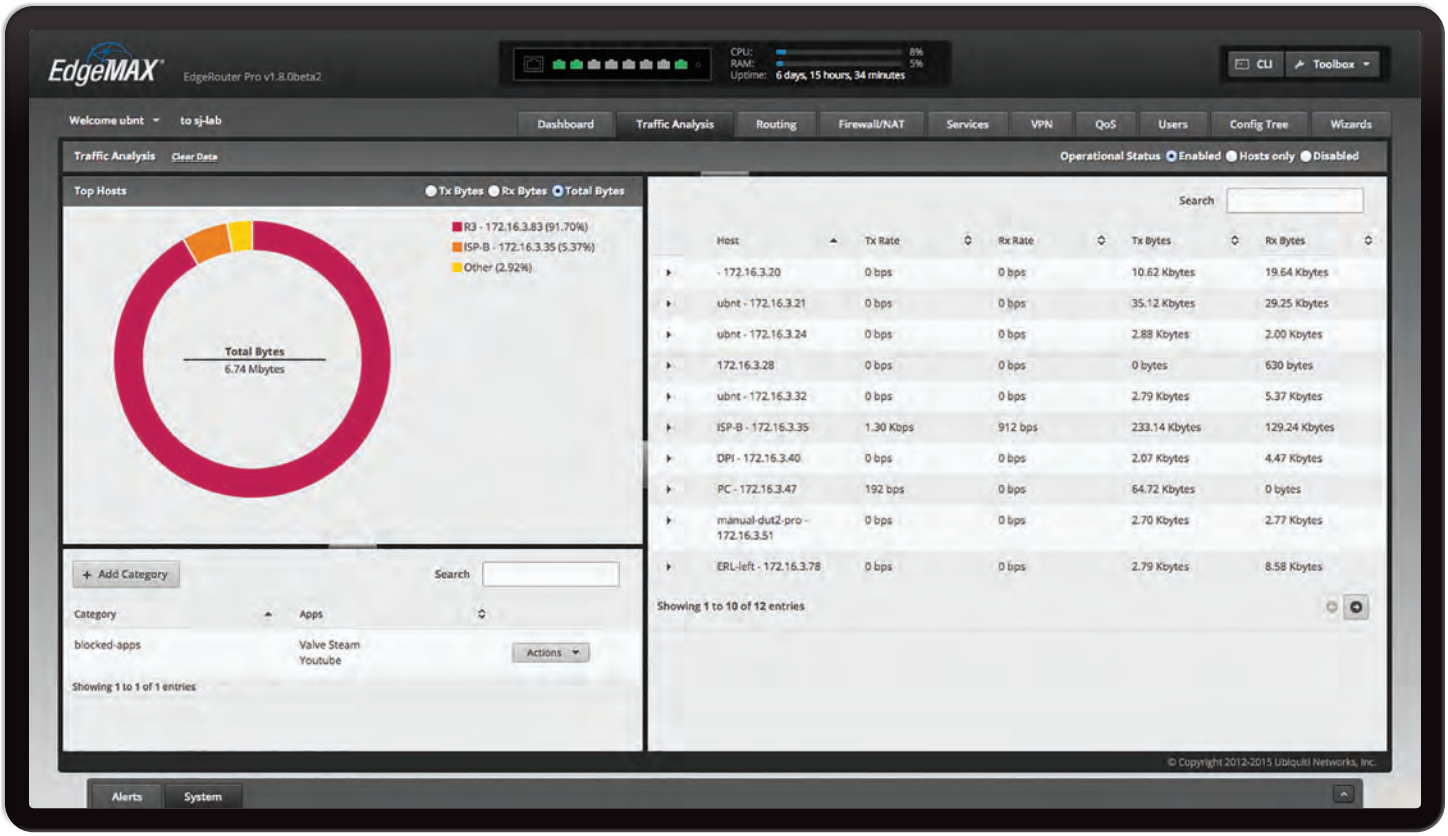
PoE Watchdog is dedicated to continuous monitoring of the specific connection to the remote host using the *Ping* tool. The *Ping* tool works by sending ICMP echo request packets to the target host and listening for ICMP echo response replies. If the specified number of replies is not received, the tool reboots the device.

- **Enable Watchdog** Enable the use of *PoE Watchdog*.
  - **IP Address To Ping** Specify the IPv4 or IPv6 address of the target host to be monitored by *PoE Watchdog*.
  - **Ping Interval** Specify the time interval (in seconds) between the ICMP echo requests that are sent by *PoE Watchdog*. The default value is *15* seconds.
  - **Startup Delay** Specify the initial time delay (in seconds) until the first ICMP echo requests are sent by *PoE Watchdog*. The default value is *300* seconds.

    The *Startup Delay* value should be at least 60 seconds as the network interface and wireless connection initialization takes a considerable amount of time if the device is rebooted.
  - **Failure Count** Specify the number of ICMP echo response replies. If the specified number of ICMP echo response packets is not received continuously, *PoE Watchdog* will reboot the device. The default value is *3*.
  - **Cut power for** Specify the number of seconds this port should pause PoE (if applicable). The default value is *5*.

  WARNING: Cutting power during a firmware upgrade can damage your device. Ensure that you specify a safe *Ping Interval*.

Click **Save** to apply your changes, or click *Cancel*.



Chapter 4: Traffic Analysis

The *Traffic Analysis* tab displays status information about the traffic traveling through the EdgeRouter, including the local hosts and types of network traffic. You can also configure the application category options. Any setting marked with a blue asterisk * is required. When the information ⓘ icon is displayed, you can click the icon for more information about an option.

Starting with EdgeOS v1.7, the traffic analysis feature with Deep Packet Inspection (DPI) is available for the EdgeRouter Lite, EdgeRouter PoE, EdgeRouter, and EdgeRouter PRO.

Note: The traffic analysis feature is not available on the EdgeRouter X and EdgeRouter X SFP due to platform differences.

DPI is more advanced than conventional Stateful Packet Inspection (SPI) filtering. Ubiquiti's advanced, proprietary DPI engine includes the latest application identification signatures to track which applications (and IP addresses) are using the most bandwidth.

The traffic analysis feature provides monitoring and reporting functionality. There are no licensing fees for DPI or signature updates, which are automatically updated on a periodic basis to maintain the accuracy of application identification.

Click the corresponding **open/close** tab to hide or display the *Traffic Analysis* section, the *Top Hosts* section, or both the *Top Hosts* and *Category* sections.

Traffic Analysis

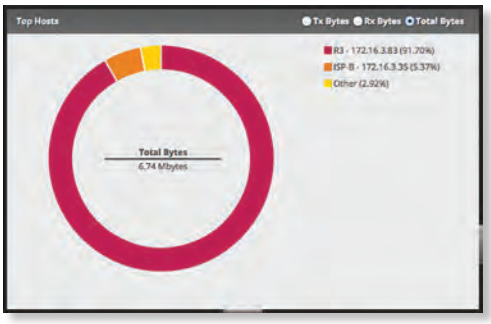
Clear Data Click to clear the current traffic statistics.

Operational Status You have three options:

- **Enabled** Select this option to allow traffic analysis with application identification using DPI. All forwarded traffic (both offloaded and non-offloaded) is displayed.
- **Hosts only** Select this option to analyze traffic at the host level only, without DPI.
- **Disabled** Disabled by default.

Top Hosts

The pie chart represents the use of bandwidth by the hosts using the most bandwidth.



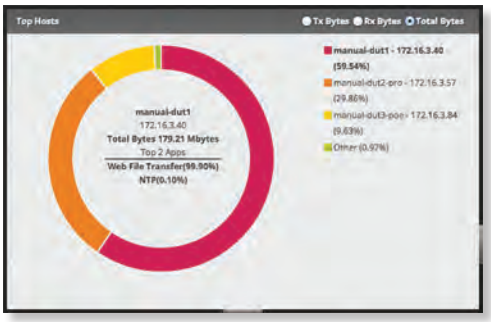
TX Bytes Displays the transmit bandwidth in bytes used by the top hosts.

RX Bytes Displays the receive bandwidth in bytes used by the top hosts.

Total Bytes Displays the total bandwidth in bytes used by the top hosts.

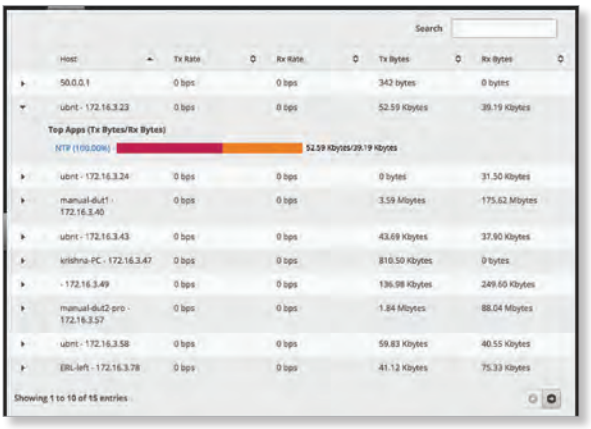
The list on the right displays the top hosts and their percentages of bandwidth use.

Place the mouse over a host's segment of the pie chart, and that host's top applications will be displayed in the middle of the pie chart. Click the host's segment to automatically select the host in the table.



Hosts

Each row corresponds to a single host. Click a row to display the applications usage of a specific host.



Search Allows you to search for specific text within the host table. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

Host Displays the host name and IP address.

TX Rate Displays the transmit rate.

RX Rate Displays the receive rate.

TX Bytes Displays the amount of data transmitted.

RX Bytes Displays the amount of data received.

Click any row to display the applications usage.

- **Top Apps (TX Bytes/RX Bytes)** Displays the following:
  - **(name)** Click the application name to add it to a custom category or create a custom category. Go to the *Application Category* section below.
  - **(_%)** Each application's usage is represented as a percentage of the host's bandwidth.
  - **(bar graph)** The TX and RX usage of an application is represented in a bar graph.
  - **(TX/RX)** The TX and RX bytes of an application are displayed.

Application Category

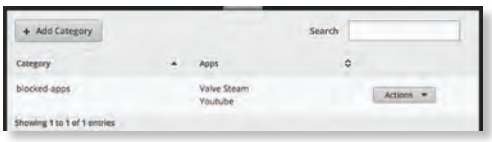
The *App Configuration* screen appears.

- **App** The name of the application is displayed.
- **Category** If the category already exists, then select it from the drop-down menu. Otherwise, select **Create New Category** and enter the name of the new category in the field below.

Click **Save** to apply your changes or click *Cancel*.

Category

You can create custom application categories for use in firewall policies. This allows a firewall to match packets that are identified by DPI as certain applications. (Refer to **"Advanced" on page 31** for more information.)



Add Category To create a new category, click **Add Category**.

The *Create Category* screen appears.

Complete the following:

- **Category** Enter a name for this category.
- **Apps** Click **Add App** to add an application. Then enter the name of the application. (An application can only appear in a single custom category.)

  Note: The name of the application must match one of the applications displayed on the *Traffic Analysis* tab.
- **Remove** Click **Remove** to delete an application.

  Click **Save** to apply your changes or click *Cancel*.

Search Allows you to search for specific text within the category table. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

Category The name of the custom category is displayed.

Apps The names of the included applications are displayed.

Actions Click the **Actions** button to access the following options:

- **Config** To configure the category, click **Config**. Go to the *Configure the Category* section in the next column.
- **Delete** Remove the category.

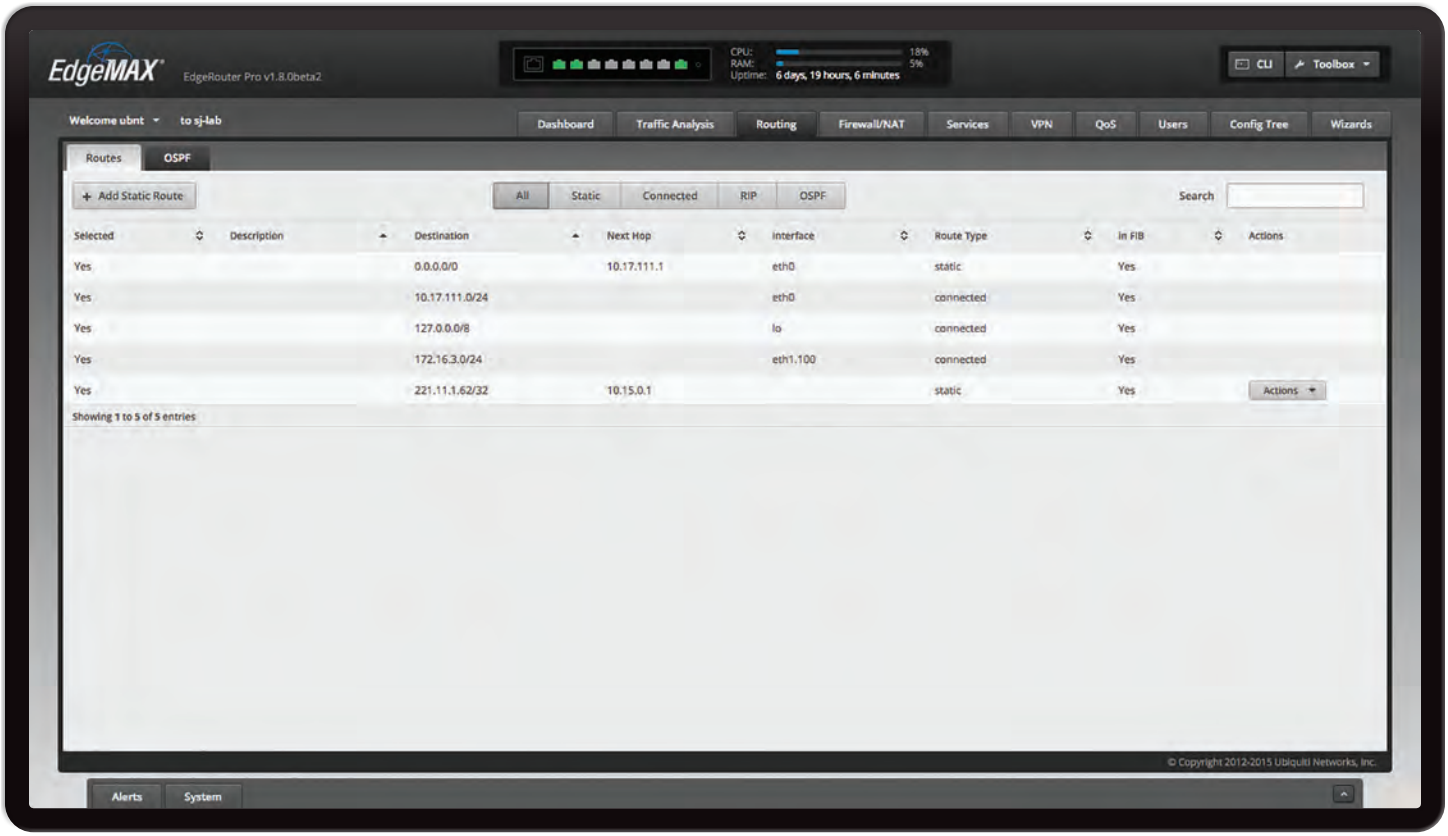
Configure the Category

After you click *Config*, the *Category Configuration* screen appears.

- **Category** You can change the name for this category.
- **Apps** Click **Add App** to add an application. Then enter the name of the application. (An application can only appear in a single custom category.)

  Note: The name of the application must match one of the applications displayed on the *Traffic Analysis* tab.
- **Remove** Click **Remove** to delete an application.

  Click **Save** to apply your changes or click *Cancel*.



Chapter 5: Routing

The *Routing* tab displays status information about a variety of connected, static, RIP, and OSPF routes. You can also configure static routes and OSPF options. Any setting marked with a blue asterisk * is required. When the information ⓘ icon is displayed, you can click the icon for more information about an option.

You have two sub-tabs:

Routes View route information and create static routes.

OSPF Configure OSPF options.

IPv6 Routing

IPv6 (Internet Protocol version 6) is gaining popularity and is bound to grow as IP addressing demands increase. The EdgeOS Configuration Interface supports IPv6 for the following options:

- *System* > *Name Server* configuration
  (Refer to **"Name Server" on page 5**.)
- *Dashboard* > *VLAN* creation
  (Refer to **"Add VLAN" on page 11**.)
- *Dashboard* > *Interface* configuration
  (Refer to **"Configure the Interface" on page 12**.)
- *Dashboard* > *VLAN* configuration
  (Refer to **"Configure the VLAN" on page 13**.)
- *VPN* > *IPsec Site-to-Site* configuration
  (Refer to **"IPsec Site-to-Site" on page 46**.)
- *Config Tree*
  (Refer to **"Config Tree" on page 61**.)

For IPv6 addresses, the EdgeOS Configuration Interface supports "::" (double-colon) notation, which substitutes "::" for a contiguous sequence of 16-bit blocks set to zero. Here is an example: *2001:db8::1*

If written out, the IPv6 address becomes: *2001:db8:0000:0000:0000:0000:0000:0001*

The EdgeOS Configuration Interface displays IPv6 addresses only in three locations:

- *System* > *Name Server* section
- *Dashboard* tab
- *VPN* > *IPsec Site-to-Site* tab

The EdgeOS Configuration Interface will increase its support of IPv6 in future releases. For other options, you can use the config tree or CLI, which has comprehensive IPv6 support.

Note: Use the config tree or CLI to view or configure IPv6 options that are not supported by the rest of the EdgeOS Configuration Interface.

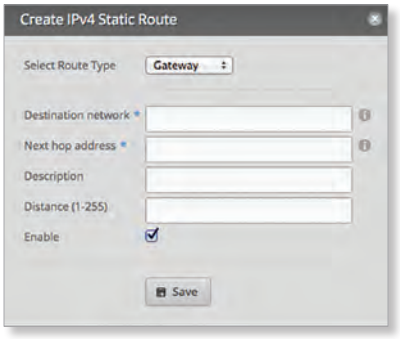
Routes

A route determines how traffic travels to its destination network. If more than one route is suitable, the EdgeRouter uses administrative distance as a metric to compare all available routes, including directly connected routes, manually configured static routes, dynamic routes, and the default route. The EdgeRouter uses the route with the lowest administrative distance.

All/Static/Connected/RIP/OSPF

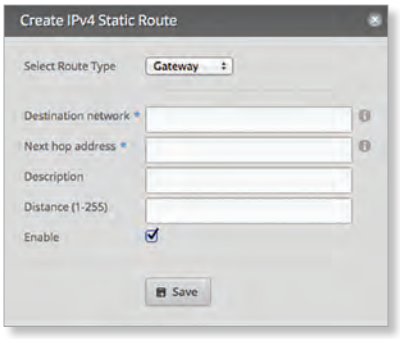
Add Static Route To create a new static route, click **Add Static Route**.

The *Create Static Route* screen appears.



Complete the following:

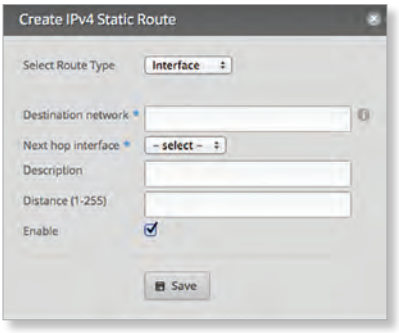
- **Select Route Type** You have three options: *Gateway*, *Interface*, or *Black Hole*.
  - **Gateway** Define a route using the IP address and subnet mask of the next hop gateway.



    - **Destination network** Enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).

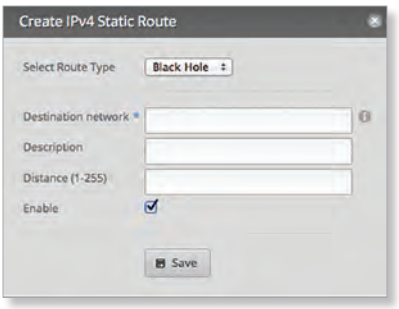
      The first default route is configured on the *System* tab; see **"System gateway address" on page 5** for more information. To create multiple default routes, set up static routes and enter **0.0.0.0/0**.
    - **Next hop address** Enter the IP address.
    - **Description** Enter keywords to identify this route.
    - **Distance (1-255)** Enter the administrative distance. If there are identical routes from different sources (such as static, RIP, or OSPF), the EdgeRouter compares the routes and uses the route with the lowest distance.
    - **Enable** Check the box to enable the route.

    Click **Save** to apply your changes.
  - **Interface** Define a route using a next hop interface.



    - **Destination network** Enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).
    - **Next hop interface** Select the appropriate interface from the drop-down list.
    - **Description** Enter keywords to identify this route.
    - **Distance (1-255)** Enter the administrative distance. If there are identical routes from different sources (such as static, RIP, and OSPF), the EdgeRouter compares the routes and uses the route with the lowest distance.
    - **Enable** Check the box to enable the route.

    Click **Save** to apply your changes.
  - **Black Hole** Define a route that drops unwanted traffic.



    - **Destination network** Enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).
    - **Description** Enter keywords to identify this route.

- **Distance (1-255)** Enter the administrative distance. If there are identical routes from different sources (such as static, RIP, and OSPF), the EdgeRouter compares the routes and uses the route with the lowest distance.
- **Enable** Check the box to enable the route.

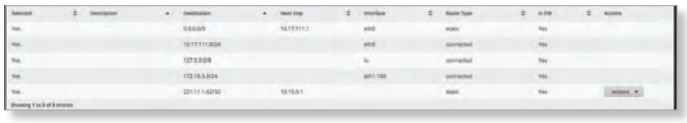
Click **Save** to apply your changes.

Search Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

All/Static/Connected/RIP/OSPF Click the appropriate tab to filter the routes as needed.

- **All** All routes are displayed by default.
- **Static** All static routes that you have configured are displayed.
- **Connected** All routes that are directly connected to the EdgeRouter are displayed.
- **RIP** All RIP (Routing Information Protocol) routes are displayed. RIP is an interior, distance vector routing protocol that uses hop count as a metric to determine the best route.
- **OSPF** All OSPF (Open Shortest Path First) routes are displayed. OSPF is an interior, link-state routing protocol that uses cost as a metric to determine the best route. The bandwidth of an interface determines the cost – the higher the bandwidth, the lower the cost.

A table displays the following information about each route. Click a column heading to sort by that heading.



Selected The status of the route, whether it has been selected for the routing table, is displayed.

Description If available, the keywords describing the route are displayed.

Destination The destination IP address is displayed.

Next Hop The IP address of the next-hop interface is displayed.

Interface The name of the interface is displayed.

Route Type The type of route is displayed.

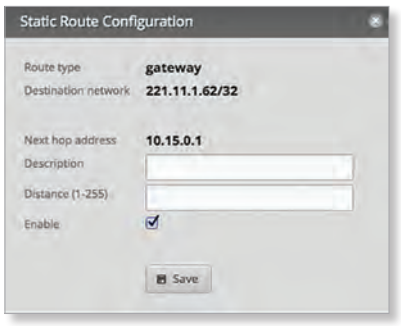
In FIB The forwarding status of the route, whether it is in the FIB (Forwarding Information Base), is displayed.

Actions Click the **Actions** button to access the following options:

- **Config** To configure the route, click **Config**. Go to the *Configure the Static Route section* in the next column.
- **Delete** Delete the route; its configuration will be removed.
- **Disable** Disable the route while keeping its configuration. (This option is not available for black hole routes.)

Configure the Static Route

After you click *Config*, the *Static Route Configuration* screen appears.



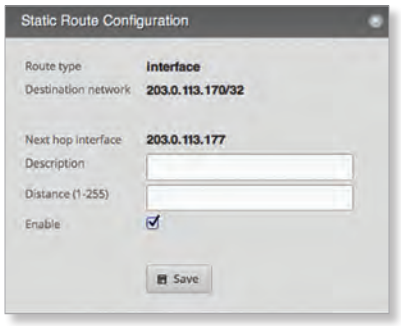
Follow the instructions for your route type:

Gateway

- **Route type** The *gateway* route uses the IP address and subnet mask of the next hop gateway.
- **Destination network** The IP address and subnet mask are displayed in slash notation.
- **Next hop address** The IP address of the next hop gateway is displayed.
- **Description** Enter keywords to identify this route.
- **Distance (1-255)** Enter the administrative distance. If there are identical routes from different sources (such as static, RIP, and OSPF), the EdgeRouter compares the routes and uses the route with the lowest distance.
- **Enable** Check the box to enable the route.

Click **Save** to apply your changes.

Interface

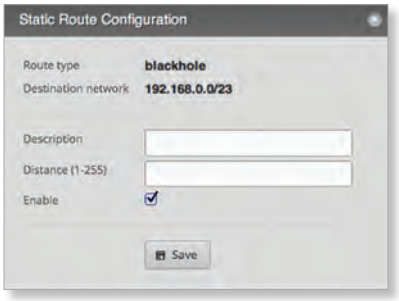


- **Route type** The *interface* route uses the next hop interface.
- **Destination network** The IP address and subnet mask are displayed in slash notation.
- **Next hop interface** The name of the next hop interface is displayed.
- **Description** Enter keywords to identify this route.

- **Distance (1-255)** Enter the administrative distance. If there are identical routes from different sources (such as static, RIP, and OSPF), the EdgeRouter compares the routes and uses the route with the lowest distance.
- **Enable** Check the box to enable the route.

Click **Save** to apply your changes.

Black Hole

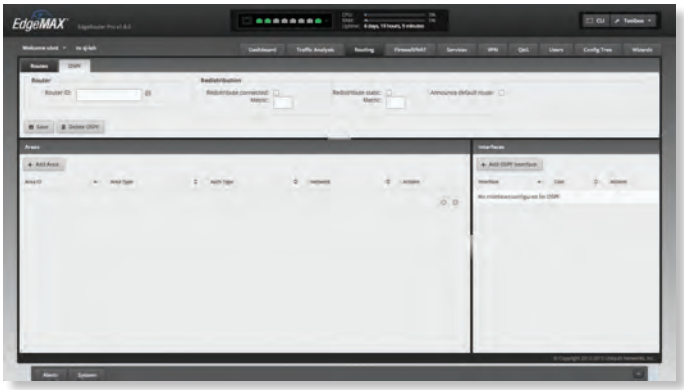


- **Route type** The *black hole* route drops unwanted traffic.
- **Destination network** The IP address and subnet mask are displayed in slash notation.
- **Description** Enter keywords to identify this route.
- **Distance (1-255)** Enter the administrative distance. If there are identical routes from different sources (such as static, RIP, and OSPF), the EdgeRouter compares the routes and uses the route with the lowest distance.
- **Enable** Check the box to enable the route.

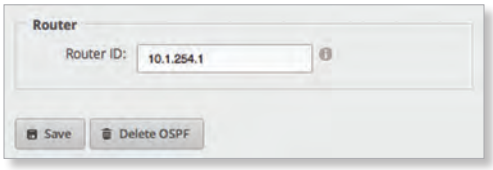
Click **Save** to apply your changes.

OSPF

Using Link State Advertisements, routers communicate with each other when there is a router or link status change. Each router maintains the information in a database, which is used to create and update a network map from the router's point of view. Each router then uses the map to build and update a routing table.



Router



Router ID Enter the IP address that identifies a specific router in an OSPF network. In OSPF, the highest *Router ID* determines which router is the Designated Router (DR), which distributes updates to the other OSPF routers.

Click **Save** to apply your changes, or click *Delete OSPF* to remove the *Router*, *Redistribution*, and *Area* settings (*Interfaces* settings are retained).

Redistribution

A single router can use multiple routing protocols, such as OSPF and RIP, which use incompatible metrics. It must reconcile information from multiple protocols to determine which route to use for a specific destination network. You can change the metrics of the distributed protocol to create protocol compatibility.

Redistribute connected If enabled, the EdgeRouter connects an OSPF area to a network using a different routing protocol and redistributes the other protocol's directly connected routes into the OSPF area. These routes become external OSPF routes.

- **Metric** If there are multiple routes to the same destination, OSPF uses the metric to select a route for the routing table. Assign a cost value to the redistributed connected routes. The EdgeRouter can then use this metric to compare these routes to other OSPF routes.

Redistribute static If enabled, the EdgeRouter connects an OSPF area to a network using a different routing protocol and redistributes the other protocol's static routes into the OSPF area. These routes become external OSPF routes.

- **Metric** If there are multiple routes to the same destination, OSPF uses the metric to select a route for the routing table. Assign a cost value to the redistributed static routes. The EdgeRouter can then use this metric to compare these routes to other OSPF routes.

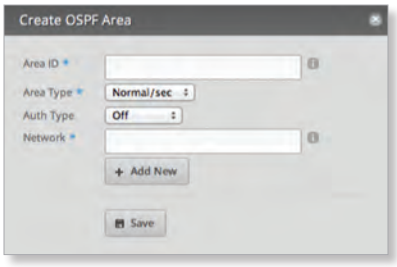
Announce default route If enabled, the EdgeRouter communicates the default route to the other routers of the OSPF network, eliminating the need to configure the default route on the other routers. The default route connects the OSPF network to an outside network.

Areas

To enhance scalability, an OSPF network is comprised of smaller sections called areas. At the minimum, there is the backbone area, called Area 0.

Add Area To create a new area, click **Add Area**.

The *Create OSPF Area* screen appears.



Complete the following:

- **Area ID** This is the number that identifies an area. It can be an integer or use a format similar to an IPv4 address.
- **Area Type** This defines the routes that are acceptable inside the area. Select the appropriate option:
  - **Normal/sec** The default type accepts all routes.
  - **NSSA** A NSSA (Not So Stubby Area) network is a variation of a stub network. It can import external routes from type 7 Link State Advertisements, which are NSSA-specific.
  - **Stub** The network has no external routes. Typically, it has a default route for outbound traffic.
- **Auth Type** Authentication helps secure communication between routers. Select the appropriate option:
  - **Off** No authentication is used.
  - **MD5/sec** Each router uses a key (password) and key ID. This is the most secure option because the key is never transmitted.
  - **Plain text** Each router uses a key. This provides minimal security because the key is transmitted in plain text format.
- **Network** Enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).

  Click **Add New** to enter more network addresses.

  Click **Save** to apply your changes.

A table displays the following information about each OSPF Area. Click a column heading to sort by that heading.

Area ID The identification number of the area is displayed.

Area Type The type of area is displayed.

Auth Type The authentication type of the area is displayed.

Network The network address of the area is displayed.

Actions Click the **Actions** button to access the following options:

- **Config** To configure the OSPF Area, click **Config**. Go to the *Configure the OSPF Area* section.
- **Delete** Delete the OSPF Area.

Configure the OSPF Area

After you click *Config*, the *OSPF Area Configuration* screen appears.

Make changes as needed.

- **Area ID** This is the number that identifies an area. It can be an integer or use a format similar to an IPv4 address.
- **Area Type** This defines the routes that are acceptable inside the area. Select the appropriate option:
  - **Normal/sec** The default type accepts all routes.
  - **NSSA** A NSSA (Not So Stubby Area) network is a variation of a stub network. It can import external routes from type 7 Link State Advertisements, which are NSSA-specific.
  - **Stub** The network has no external routes. Typically, it has a default route for outbound traffic.
- **Auth Type** Authentication helps secure communication between routers. Select the appropriate option:
  - **Off** No authentication is used.
  - **MD5/sec** Each router uses a key (password) and key ID. This is the most secure option because the key is never transmitted.
  - **Plain text** Each router uses a key. This provides minimal security because the key is transmitted in plain text format.

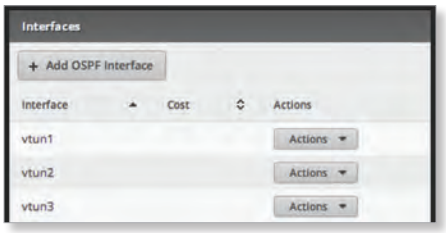
- **Network** Enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).

  Click **Add New** to enter more network addresses.

  Click **Save** to apply your changes.

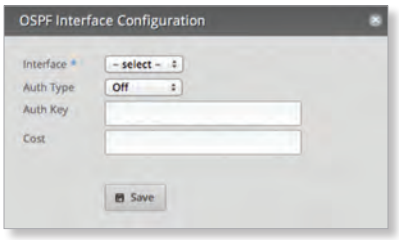
Interfaces

You can configure interfaces with specific OSPF options.



Add OSPF Interface To create a new interface, click **Add OSPF Interface**.

The *OSPF Interface Configuration* screen appears.



Complete the following:

- **Interface** Select the appropriate interface from the drop-down list.
- **Auth Type** OSPF authentication helps secure communication between routers. Select the appropriate option:
  - **Off** No authentication is used.
  - **MD5/sec** Each router uses a key (password) and key ID. This is the most secure option because the key is never transmitted.
  - **Plain text** Each router uses a key. This provides minimal security because the key is transmitted in plain text format.
- **Auth Key** Enter the key used for authentication.
- **Cost** By default, the cost of an interface is based on its bandwidth; however, you can manually assign a cost to the interface.

  Click **Save** to apply your changes.

A table displays the following information about each OSPF Interface. Click a column heading to sort by that heading.

Interface The name of the interface is displayed.

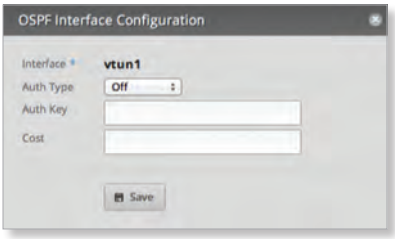
Cost The cost of the interface is displayed. OSPF uses cost as a metric to determine the best route.

Actions Click the **Actions** button to access the following options:

- **Config** To configure the OSPF Interface, click **Config**. Go to the *Configure the OSPF Interface* section.
- **Delete** Delete the OSPF Interface.

Configure the OSPF Interface

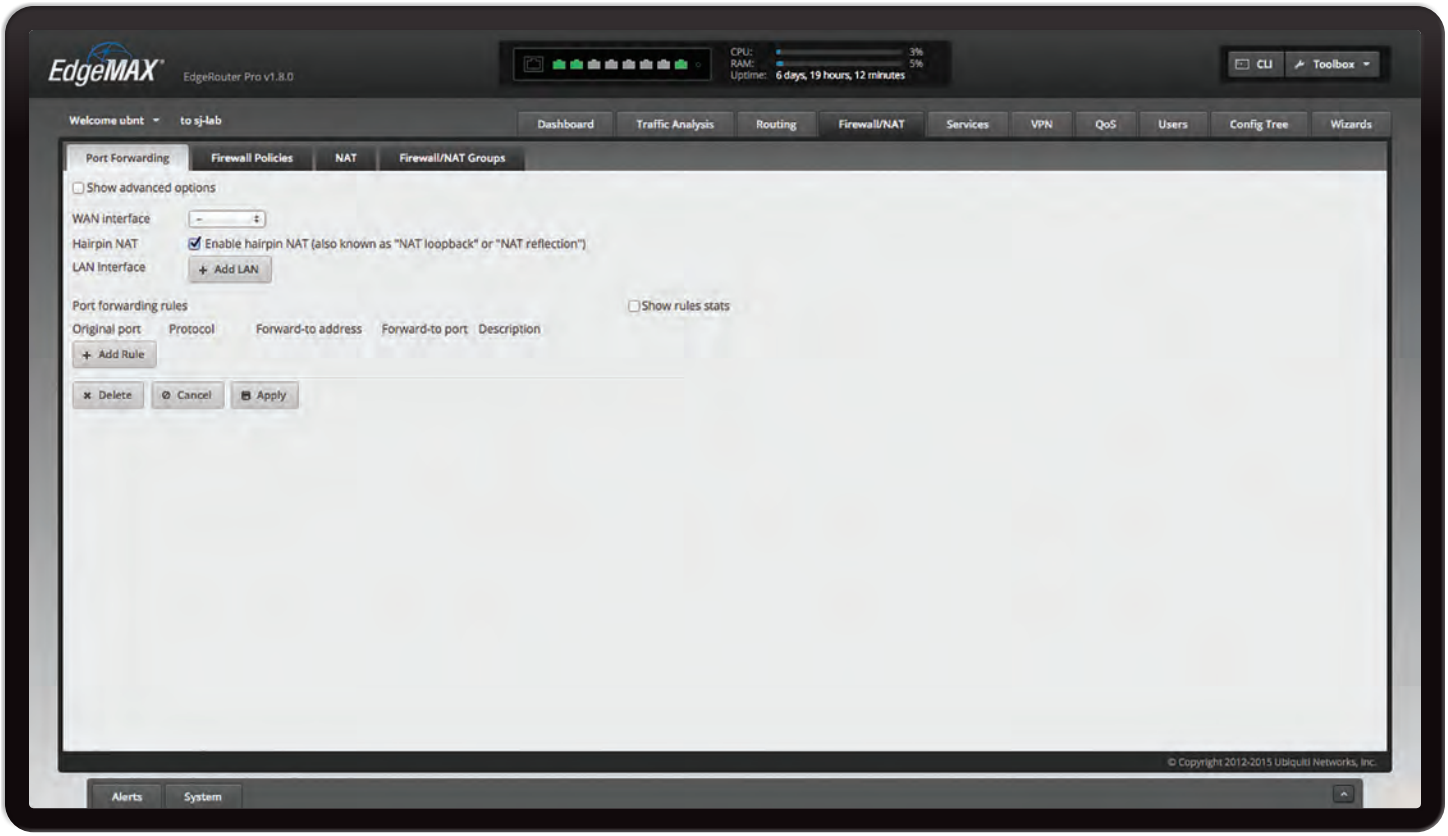
After you click *Config*, the *OSPF Interface Configuration* screen appears.



Make changes as needed.

- **Interface** The name of the interface is displayed.
- **Auth Type** Authentication helps secure communication between routers. Select the appropriate option:
  - **Off** No authentication is used.
  - **MD5/sec** Each router uses a key (password) and key ID. This is the most secure option because the key is never transmitted.
  - **Plain text** Each router uses a key. This provides minimal security because the key is transmitted in plain text format.
- **Auth Key** Enter the key used for authentication.
- **Cost** By default, the cost of an interface is based on its bandwidth; however, you can manually assign a cost to the interface.

  Click **Save** to apply your changes.



Chapter 6: Firewall/NAT

The *Firewall/NAT* tab displays status information about port forwarding, firewall policies, NAT (Network Address Translation) rules, and firewall/NAT groups. You can also configure these policies, groups, rules, and options. Any setting marked with a blue asterisk * is required. When the information ⓘ icon is displayed, you can click the icon for more information about an option.

You have four sub-tabs:

Port Forwarding View and create port forwarding rules.

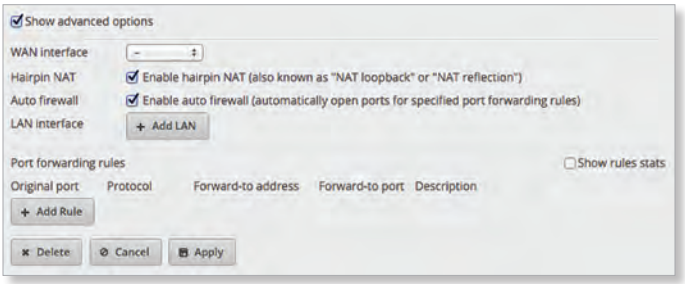
Firewall Policies Each firewall policy is a set of rules applied in the order you specify.

NAT View and create NAT rules.

Firewall/NAT Groups Create groups defined by IP address, network address, or port number.

Port Forwarding

Typically you configure a port forwarding rule so a host on the external network can access a server on the internal network by using the public IP address (or hostname) of the EdgeRouter.



Show advanced options Select this checkbox to display the *Auto firewall* option.

WAN interface Select the appropriate interface from the drop-down menu. (If you select *Other*, then enter the interface name in the field provided.)

Hairpin NAT Enabled by default. If you want to allow a host on the internal network to use the public IP address to access an internal server, then keep *Hairpin NAT* enabled. (Hairpin NAT is also known as NAT loopback or NAT reflection.)

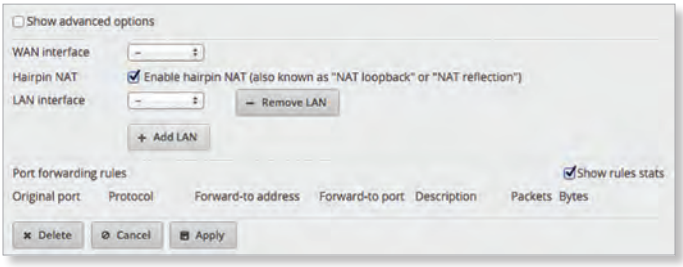
Note: If *Hairpin NAT* is enabled, then it only enables *Hairpin NAT* for the port forwarding rules defined in the wizard; it does not affect the Destination NAT Rules defined on the *Firewall/NAT* > *NAT* tab (refer to **"Destination NAT Rules" on page 35**).

Auto firewall Enabled by default. Displayed if *Show advanced options* is enabled. If you want the EdgeRouter to automatically open ports for the specified port forwarding rules, then keep *Auto firewall* enabled.

If you disable the *Auto firewall* option, then you will need to manually define firewall rules on the *Firewall/NAT* > *Firewall Policies* tab (refer to the *Firewall Policies* section in the next column).

LAN interface Click **Add LAN** to display the drop-down menu. Then select the appropriate interface. (If you select *Other*, then enter the interface name in the field provided.)

- **Remove LAN** Click **Remove LAN** to delete an interface.
- **Add LAN** Click **Add LAN** to add another new interface.

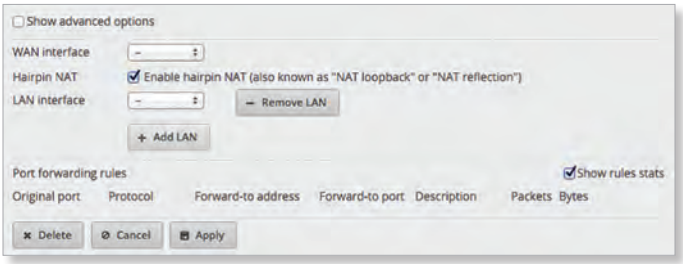


Port Forwarding Rules

This section allows you to create port forwarding rules and manage them.

Show rules stats Select this checkbox to display statistics for each rule:

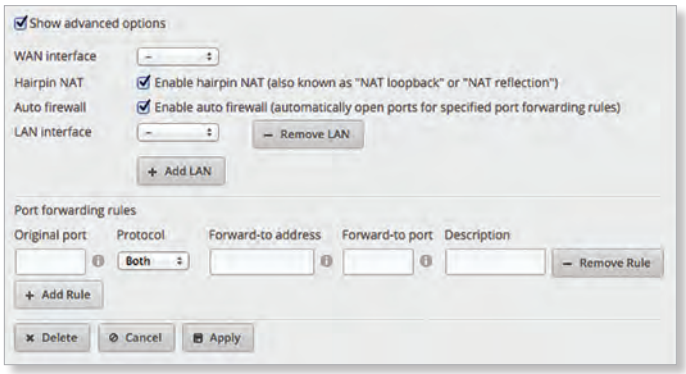
- **Packets** The number of forwarded packets is displayed.
- **Bytes** The number of forwarded bytes is displayed.



Add Rule Click **Add Rule** to create a new rule.

- **Original port** Enter the port or ports that will be forwarded to the LAN. You can identify the port or ports by name, number, and/or range. To specify multiple ports, use a comma-separated list.

  Example: *https,20-23,554*
- **Protocol** Enter the protocol that will be forwarded to the LAN: **Both**, **TCP**, or **UDP**.
- **Forward-to address** Enter the LAN IP address that will receive the forwarded port traffic.
- **Forward-to port** Enter the port or ports that will receive the forwarded port traffic. You can identify the port or ports by name, number, and/or range. If you do not specify the *Forward-to port*, then the original destination port of the traffic will be used.
- **Description** Enter keywords that will identify this rule.
- **Remove** Click **Remove** to delete a rule.
- **Add Rule** Click **Add Rule** to create a new rule.



To remove the entire port forwarding configuration, click *Delete*.

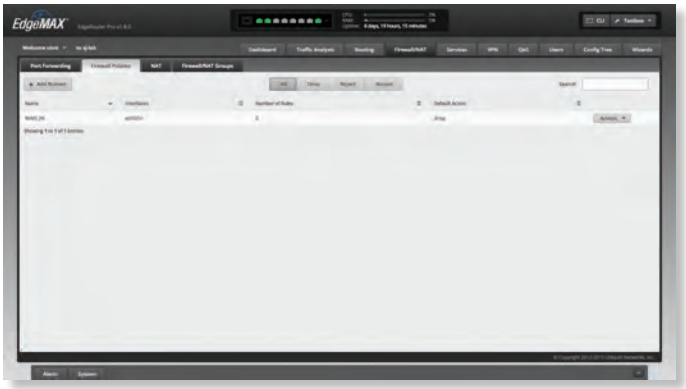
Click **Apply** to apply your changes, or click *Cancel*.

Firewall Policies

A firewall policy is a set of rules with a default action. Firewall policies are applied before SNAT (Source Network Address Translation) and after DNAT (Destination Network Address Translation).

To create a firewall policy:

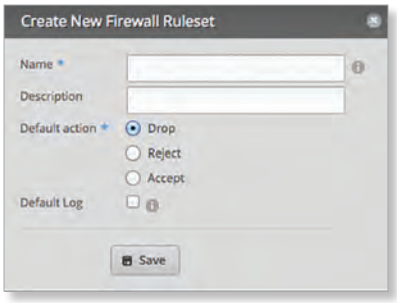
1. Click the **Firewall/NAT Groups** tab, and create the applicable firewall groups. See **"Firewall/NAT Groups" on page 36** for more information.
2. Click the **Firewall Policies** tab, and then click **Add Ruleset**. Configure the basic parameters. See the *Add Ruleset* description in the next column for more information.
3. Configure the details of the firewall policy. See **"Configure the Firewall Policy" on page 29** for more information.



All/Drop/Reject/Accept

Add Ruleset To create a new policy, click **Add Ruleset**.

The *Create New Firewall Ruleset* screen appears.



Complete the following:

- **Name** Enter a name for this policy.
- **Description** Enter keywords to describe this policy.
- **Default action** All policies have a default action if the packets do not match any rule. Select the appropriate default action:
  - **Drop** Packets are blocked with no message.
  - **Reject** Packets are blocked, and an ICMP (Internet Control Message Protocol) message is sent saying the destination is unreachable.
  - **Accept** Packets are allowed through the firewall.
- **Default Log** Check this box to log packets that trigger the default action.

  Click **Save** to apply your changes.

Search Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

All/Drop/Reject/Accept Click the appropriate tab to filter the policies by default action.

- **All** All policies are displayed by default.
- **Drop** All of the drop policies are displayed.
- **Reject** All of the reject policies are displayed.
- **Accept** All of the accept policies are displayed.

A table displays the following information about each policy. Click a column heading to sort by that heading.

Name The name of the policy is displayed.

Interfaces The specified interface and direction of traffic flow are displayed.

Number of Rules The number of rules in the policy is displayed.

Default Action The action that the policy will execute if the packets do not match any rule is displayed.

Actions Click the **Actions** button to access the following options:

- **Edit Rules** To configure the rules, click **Edit Rules**. Go to the *Rules* section in the next column.
- **Configuration** To configure the policy, click **Configuration**. Go to **"Configuration" on page 32**.
- **Interfaces** To select interfaces and direction of traffic flow for your policy, click **Interfaces**. Go to **"Interfaces" on page 32**.
- **Stats** To view statistics on firewall usage, click **Stats**. Go to **"Stats" on page 33**.
- **Copy Ruleset** To create a duplicate, click **Copy Ruleset**. The *Copy Firewall Ruleset* screen appears.

  - **Name** Enter a new name for this policy.

  Click **Copy** to confirm, or click *Cancel*.
- **Delete Ruleset** Remove the ruleset.

Configure the Firewall Policy

The *Ruleset Configuration for _* screen appears.

You have four tabs available:

- Rules (see below)
- **"Configuration" on page 32**
- **"Interfaces" on page 32**
- **"Stats" on page 33**

Add New Rule To create a new rule, click **Add New Rule**. Go to **"Add or Configure a Rule" on page 30**.

Save Rule Order To change the rule order, click and drag a rule up or down the sequence, and then release the rule. When you are finished, click **Save Rule Order**.

Rules

A rule tells the EdgeRouter what action to take with a specific packet. Define the following:

- Criteria for matching packets
- Action to take with matching packets

Rules are organized into a set and applied in the specified *Rule Order*. If the packets match a rule's criteria, then its action is triggered. If not, then the next rule is applied.

A table displays the following information about each rule. Click a column heading to sort by that heading.

Order The rules are applied in the order specified. The number of the rule in this order is displayed.

Description The keywords you entered to describe this rule are displayed.

Source The source specified by this rule is displayed.

Destination The destination specified by this rule is displayed.

Protocol The protocol that matches the rule is displayed.

Action The action specified by this rule is displayed.

Actions Click the **Actions** button to access the following options:

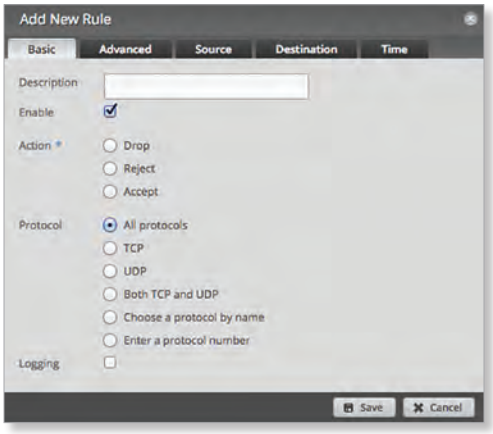
- **Basic** To configure the basic options of a rule, click **Basic**. Go to the *Basic* section in the next column.
- **Advanced** To configure the advanced options of a rule, click **Advanced**. Go to **"Advanced" on page 31**.
- **Source** To configure the source options of a rule, click **Source**. Go to **"Source" on page 31**.
- **Destination** To configure the destination options of a rule, click **Destination**. Go to **"Destination" on page 32**.
- **Time** To configure the time options of a rule, click **Time**. Go to **"Time" on page 32**.
- **Copy Rule** To create a duplicate, click **Copy Rule**. The duplicate rule appears at the bottom of the list.
- **Delete Rule** Remove the rule.

Add or Configure a Rule

The *Rule Configuration for _* screen appears. You have five tabs available:

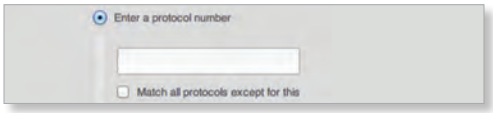
- Basic (see below)
- Advanced (see the next column)
- **"Source" on page 31**
- **"Destination" on page 32**
- **"Time" on page 32**

Basic



- **Description** Enter keywords to describe this rule.
- **Enable** Check the box to enable this rule.
- **Action** Select the action for packets that match this rule's criteria.
  - **Drop** Packets are blocked with no message.
  - **Reject** Packets are blocked, and an ICMP (Internet Control Message Protocol) message is sent saying the destination is unreachable.
  - **Accept** Packets are allowed.
- **Protocol**
  - **All protocols** Match packets of all protocols.
  - **TCP** Match TCP packets.
  - **UDP** Match UDP packets.
  - **Both TCP and UDP** Match TCP and UDP packets.
  - **Choose a protocol by name** Select the protocol from the drop-down list. Match packets of this protocol.
    - **Match all protocols except for this** Match packets of all protocols except for the selected protocol.

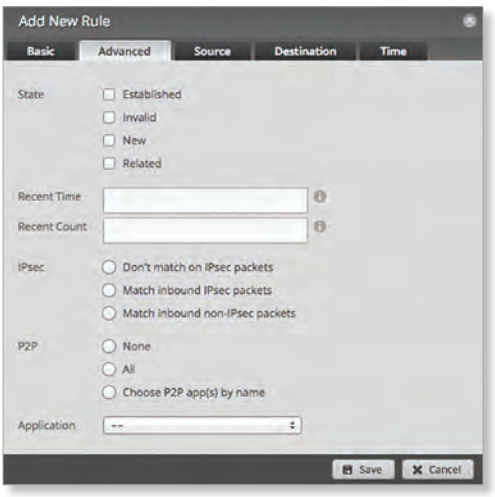
  - **Enter a protocol number** Enter the port number of the protocol. Match packets of this protocol.
    - **Match all protocols except for this** Match packets of all protocols except for the selected protocol.



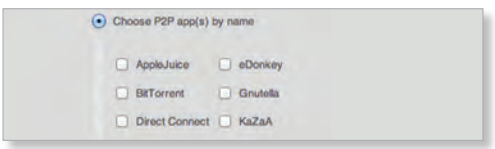
- **Logging** Check this box to log instances when the rule is matched.

Click **Save** to apply your changes, or click *Cancel*.

Advanced



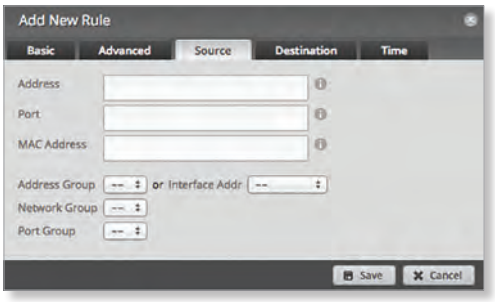
- **State** This describes the connection state of a packet.
  - **Established** Match packets that are part of a two-way connection.
  - **Invalid** Match packets that cannot be identified.
  - **New** Match packets creating a new connection.
  - **Related** Match packets related to established connections.
- **Recent Time** Enter the number of seconds to monitor for attempts to connect from the same source.
- **Recent Count** Enter the number of times the same source is detected within the *Recent Time* duration. This helps thwart attacks using continual attempts to connect.
- **IPsec** IPsec (Internet Protocol security) helps secure packet routing.
  - **Don't match on IPsec packets** Do not match any IPsec packets.
  - **Match inbound IPsec packets** Match IPsec packets that are entering the EdgeRouter.
  - **Match inbound non-IPsec packets** Match non-IPsec packets that are entering the EdgeRouter.
- **P2P** Match P2P (Peer-to-Peer) applications.
  - **None** Do not match P2P connections.
  - **All** Match all P2P connections.
  - **Choose P2P app(s) by name** Match packets of the selected P2P application(s). Check the box of any P2P application on this list to select it.



- **Application** Select the appropriate application category from the drop-down menu. (You can create custom application categories on the *Traffic Analysis* tab; go to **"Traffic Analysis" on page 17** for more information.)

Click **Save** to apply your changes, or click *Cancel*.

Source



- **Address** Enter the IP address of the source.
- **Port** Enter the port number or range of the source.
- **MAC Address** Enter the MAC address of the source.

Firewall groups are created on the *Firewall/NAT Groups* tab; see **"Firewall/NAT Groups" on page 36** for more information. Select the appropriate group(s); you can specify up to two groups maximum in these combinations:

- An address group and port group
- A network group and port group

The packets must match both groups to apply the rule.

- **Address Group or Interface Addr.** Select the appropriate address group or interface address. If you select *Other* as the interface address, then enter the interface name in the field provided. The firewall rule will match the IP address of the selected interface.
- **Network Group** Select the appropriate network group.
- **Port Group** Select the appropriate port group.

Click **Save** to apply your changes, or click *Cancel*.

Destination

- **Address** Enter the IP address of the destination.
- **Port** Enter the port number of the destination.

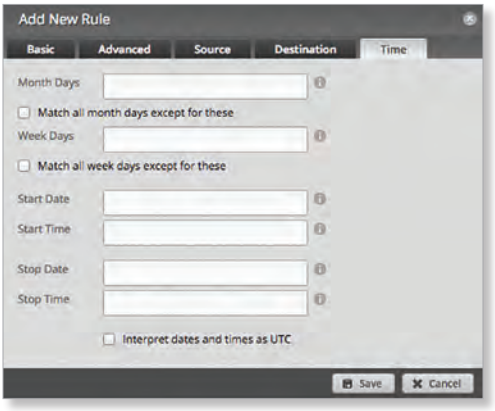
  Firewall groups are created on the *Firewall/NAT Groups* tab; see **"Firewall/NAT Groups" on page 36** for more information. Select the appropriate group(s); you can specify up to two groups maximum in these combinations:

  - An address group and port group
  - A network group and port group

  The packets must match both groups to apply the rule.
- **Address Group or Interface Addr.** Select the appropriate address group or interface address. If you select *Other* as the interface address, then enter the interface name in the field provided. The firewall rule will match the IP address of the selected interface.
- **Network Group** Select the appropriate network group.
- **Port Group** Select the appropriate port group.

  Click **Save** to apply your changes, or click *Cancel*.

Time



- **Month Days** Enter the days of the month when the rule should be applied. Enter numbers in the range 1 to 31. If you enter more than one day, use commas to separate the numbers (example: *3, 4, 5*).
  - **Match all month days except for these** Match all days of the month except for the selected days.
- **Week Days** Enter the days of the week when the rule should be applied. Enter *Sun*, *Mon*, *Tue*, *Wed*, *Thu*, *Fri*, or *Sat*. If you enter more than one day, use commas to separate the days (example: *Mon, Tue, Wed*).
  - **Match all week days except for these** Match all days of the week except for the selected days.
- **Start Date** Enter the date the rule should start being applied. Use the YYYY-MM-DD (year-month-day) format.
- **Start Time** Enter the time the rule should start being applied. Use the 24-hour format, HH:MM:SS (hours:minutes:seconds).
- **Stop Date** Enter the date the rule should stop being applied. Use the YYYY-MM-DD (year-month-day) format.
- **Stop Time** Enter the time the rule should stop being applied. Use the 24-hour format, HH:MM:SS (hours:minutes:seconds).
- **Interpret dates and times as UTC** Check the box if your network uses UTC.

  Click **Save** to apply your changes, or click *Cancel*.

Configuration

Name The name of this policy is displayed.

Description Enter keywords to describe this policy.

Default action All policies have a default action if the packets do not match any rule. Select the appropriate default action:

- **Drop** Packets are blocked with no message.
- **Reject** Packets are blocked, and an ICMP (Internet Control Message Protocol) message is sent saying the destination is unreachable.
- **Accept** Packets are allowed.

Default Log Check this box to log packets that trigger the default action.

Click **Add Ruleset** to apply your changes.

Interfaces

- **Interface** Select the appropriate interface from the drop-down list.

- **Direction** Select the direction of the traffic flow.
  - **in** Match inbound packets.
  - **out** Match outbound packets.
  - **local** Match local packets.
- **Remove** Click **Remove** to remove an interface.
- **Add Interface** Click **Add Interface** to enter more interfaces.

Click **Save Ruleset** to apply your changes.

Stats

A table displays the following statistics about each rule. Click a column heading to sort by that heading.

Rule The rules are applied in the order specified. The number of the rule in this order is displayed.

Packets The number of packets that triggered this rule is displayed.

Bytes The number of bytes that triggered this rule is displayed.

Action The action specified by this rule is displayed.

Description The keywords you entered to describe this rule are displayed.

NAT

NAT changes the addressing of packets. A NAT rule tells the EdgeRouter what action to take with a specific packet. Define the following:

- Criteria for matching packets
- Action to take with matching packets

Rules are organized into a set and applied in the specified *Rule Order*. If the packets match a rule's criteria, then its action is performed. If not, then the next rule is applied.

Source NAT Rules

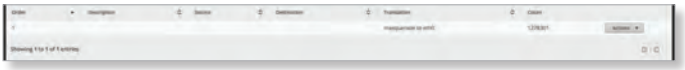
Source NAT Rules change the source address of packets; a typical scenario is that a private source needs to communicate with a public destination. A Source NAT Rule goes from the private network to the public network and is applied after routing, just before packets leave the EdgeRouter.

Add Source NAT Rule To create a new rule, click **Add Source NAT Rule**. Go to **"Add or Configure a Source NAT Rule" on page 34**.

Save Rule Order To change the rule order, click and drag a rule up or down the sequence, and then release the rule. When you are finished, click **Save Rule Order**.

Search Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

A table displays the following information about each rule. Click a column heading to sort by that heading.



Order The rules are applied in the order specified. The number of the rule in this order is displayed.

Description The keywords you entered to describe this rule are displayed.

Source The source IP address or group is displayed.

Destination The destination IP address or group is displayed.

Translation A description of the translation (such as *masquerade to eth_*) is displayed.

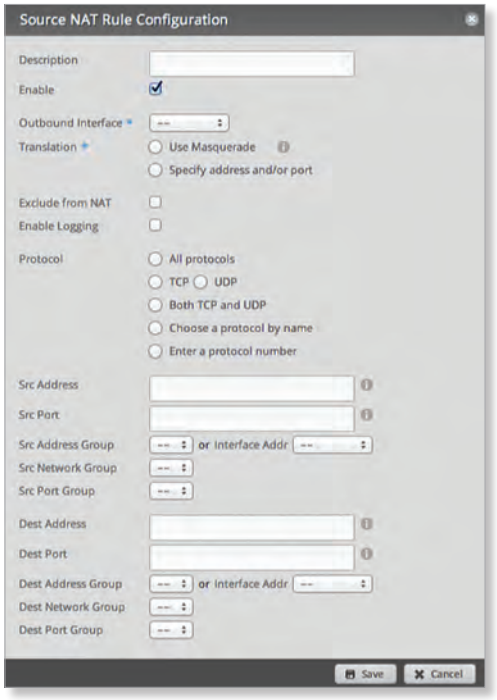
Count The number of translations is displayed.

Actions Click the **Actions** button to access the following options:

- **Config** To configure the rule, click **Config**. Go to the *Add or Configure a Source NAT Rule* section below.
- **Copy** To create a duplicate, click **Copy**. The duplicate rule appears at the bottom of the list.
- **Delete** Remove the rule.

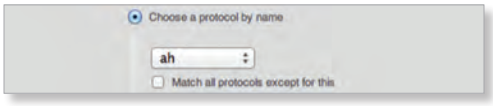
Add or Configure a Source NAT Rule

After you click *Config*, the *Source NAT Rule Configuration* screen appears.

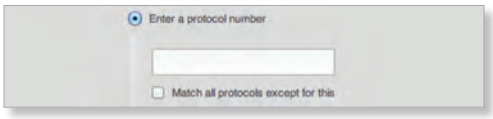


- **Description** Enter keywords to describe this rule.
- **Enable** Check the box to enable this rule.
- **Outbound Interface** Select the interface through which the outgoing packets exit the EdgeRouter. This is required only for Source NAT Rules that use Masquerade.
- **Translation** Select one of the following:
  - **Use Masquerade** Masquerade is a type of Source NAT. If enabled, the source IP address of the packets becomes the public IP address of the outbound interface.
  - **Specify address and/or port** If enabled, the source IP address of the packets becomes the specified IP address and port.
    - **Address** Enter the IP address that will replace the source IP address of the outgoing packet. You can also enter a range of IP addresses; one of them will be used.
    - **Port** Enter the port number that will replace the source port number of the outgoing packet. You can also enter a range of port numbers; one of them will be used.

- **Exclude from NAT** Check the box to exclude packets that match this rule from NAT.
- **Enable Logging** Check this box to log instances when the rule is matched.
- **Protocol** Select one of the following:
  - **All protocols** Match packets of all protocols.
  - **TCP** Match TCP packets.
  - **UDP** Match UDP packets.
  - **Both TCP and UDP** Match TCP and UDP packets.
  - **Choose a protocol by name** Select the protocol from the drop-down list. Match packets of this protocol.
    - **Match all protocols except for this** Match packets of all protocols except for the selected protocol.



  - **Enter a protocol number** Enter the port number of the protocol. Match packets of this protocol.
    - **Match all protocols except for this** Match packets of all protocols except for the selected protocol.



- **Src Address** Enter the IP address or network address of the source. You can also enter a range of IP addresses; one of them will be used.

  Note: If you enter a network address, enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).
- **Src Port** Enter the port name or number of the source. You can also enter a range of port numbers; one of them will be used.

  NAT groups are created on the *Firewall/NAT Groups* tab; see **"Firewall/NAT Groups" on page 36** for more information. Select the appropriate group(s); you can specify up to two groups maximum in these combinations:
  - An address group and port group
  - A network group and port group

  The packets must match both groups to apply the rule.
- **Src Address Group or Interface Addr.** Select the appropriate address group or interface address. If you select *Other* as the interface address, then enter the interface name in the field provided. The NAT rule will match the IP address of the selected interface.
- **Src Network Group** Select the appropriate network group.
- **Src Port Group** Select the appropriate port group.

- **Dest. Address** Enter the IP address or network address of the destination. You can also enter a range of IP addresses; one of them will be used.

  Note: If you enter a network address, enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).
- **Dest. Port** Enter the port name or number of the destination. You can also enter a range of port numbers; one of them will be used.
- **Dest Address Group or Interface Addr.** Select the appropriate address group or interface address. If you select *Other* as the interface address, then enter the interface name in the field provided. The NAT rule will match the IP address of the selected interface.
- **Dest Network Group** Select the appropriate network group.
- **Dest Port Group** Select the appropriate port group.

Click **Save** to apply your changes, or click *Cancel*.

Destination NAT Rules

Destination NAT Rules change the destination address of packets; a typical scenario is that a public source needs to communicate with a private destination. A Destination NAT Rule goes from the public network to the private network and is applied before routing.

Add Destination NAT Rule To create a new rule, click **Add Destination NAT Rule**. Go to the *Add or Configure a Destination NAT Rule* section.

Save Rule Order To change the rule order, click and drag a rule up or down the sequence, and then release the rule. When you are finished, click **Save Rule Order**.

Search Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

A table displays the following information about each rule. Click a column heading to sort by that heading.

Order The rules are applied in the order specified. The number of the rule in this order is displayed.

Description The keywords you entered to describe this rule are displayed.

Source The source IP address or group is displayed.

Destination The destination IP address or group is displayed.

Translation A description of the translation (such as *to <IP_address>*) is displayed.

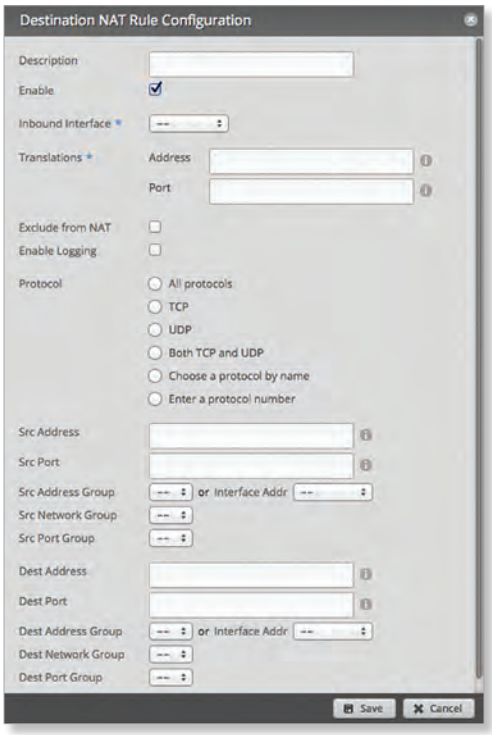
Count The number of translations is displayed.

Actions Click the **Actions** button to access the following options:

- **Config** To configure the rule, click **Config**. Go to the *Add or Configure a Destination NAT Rule* section below.
- **Copy** To create a duplicate, click **Copy**. The duplicate rule appears at the bottom of the list.
- **Delete** Remove the rule.

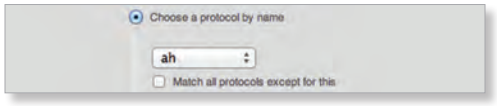
Add or Configure a Destination NAT Rule

After you click *Config*, the *Destination NAT Rule Configuration* screen appears.

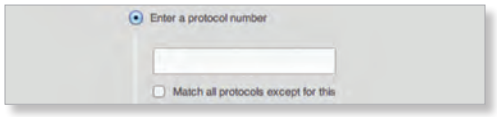


- **Description** Enter keywords to describe this rule.
- **Enable** Check the box to enable this rule.
- **Inbound Interface** Select the interface through which the incoming packets enter the EdgeRouter.
- **Translations** Complete the following:
  - **Address** Enter the IP address that will replace the destination IP address of the incoming packet.
  - **Port** Enter the port number that will replace the destination port number of the incoming packet.

- **Exclude from NAT** Check the box to exclude packets that match this rule from NAT.
- **Enable Logging** Check this box to log instances when the rule is matched.
- **Protocol**
  - **All protocols** Match packets of all protocols.
  - **TCP** Match TCP packets.
  - **UDP** Match UDP packets.
  - **Both TCP and UDP** Match TCP and UDP packets.
  - **Choose a protocol by name** Select the protocol from the drop-down list. Match packets of this protocol.
    - **Match all protocols except for this** Match packets of all protocols except for the selected protocol.



  - **Enter a protocol number** Enter the port number of the protocol. Match packets of this protocol.
    - **Match all protocols except for this** Match packets of all protocols except for the selected protocol.



- **Src Address** Enter the IP address or network address of the source. You can also enter a range of IP addresses; one of them will be used.

  Note: If you enter a network address, enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).
- **Src Port** Enter the port name or number of the source. You can also enter a range of port numbers; one of them will be used.

  NAT groups are created on the *Firewall/NAT Groups* tab; refer to the *Firewall/NAT Groups* section in the next column for more information. Select the appropriate group(s); you can specify up to two groups maximum in these combinations:
  - An address group and port group
  - A network group and port group

  The packets must match both groups to apply the rule.
- **Src Address Group or Interface Addr.** Select the appropriate address group or interface address. If you select *Other* as the interface address, then enter the interface name in the field provided. The NAT rule will match the IP address of the selected interface.
- **Src Network Group** Select the appropriate network group.
- **Src Port Group** Select the appropriate port group.
- **Dest. Address** Enter the IP address or network address of the destination. You can also enter a range of IP addresses; one of them will be used.

  Note: If you enter a network address, enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).
- **Dest. Port** Enter the port name or number of the destination. You can also enter a range of port numbers; one of them will be used.
- **Dest Address Group or Interface Addr.** Select the appropriate address group or interface address. If you select *Other* as the interface address, then enter the interface name in the field provided. The NAT rule will match the IP address of the selected interface.
- **Dest Network Group** Select the appropriate network group.
- **Dest Port Group** Select the appropriate port group.

Click **Save** to apply your changes, or click *Cancel*.

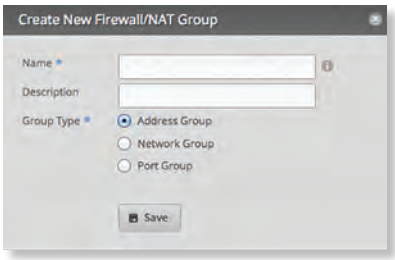
Firewall/NAT Groups

Create groups organized by IP address, network address, or port number.

All/Address/Network/Port

Add Group To create a new group, click **Add Group**.

The *Create New Firewall/NAT Group* screen appears.



Complete the following:

- **Name** Enter a name for this group.
- **Description** Enter keywords to describe this group.

- **Group Type** Select the appropriate option:
  - **Address Group** Define a group by IP address.
  - **Network Group** Define a group by network address.
  - **Port Group** Define a group by port numbers.

  Click **Save** to apply your changes.

Search Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

All/Address/Network/Port Click the appropriate tab to filter the groups as needed.

- **All** All groups are displayed by default.
- **Address** All of the address groups are displayed.
- **Network** All of the network groups are displayed.
- **Port** All of the port groups are displayed.

A table displays the following information about each group. Click a column heading to sort by that heading.

Name The name of the group is displayed.

Description The keywords you entered to describe the group are displayed.

Type The type of group is displayed.

Number of group members The number of members is displayed.

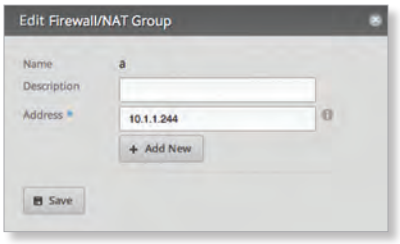
Actions Click the **Actions** button to access the following options:

- **Config** To configure the group, click **Config**. Go to the *Configure the Firewall/NAT Group* section below.
- **Delete** Remove the group.

Configure the Firewall/NAT Group

After you click *Config*, the *Edit Firewall Group* screen appears. Follow the instructions for your group type:

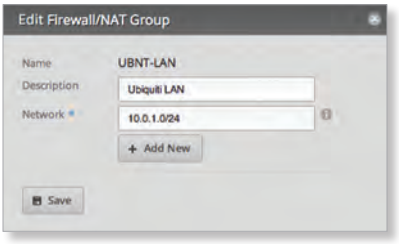
- **Address Group** Make changes as needed.



  - **Name** The name of this group is displayed.
  - **Description** Enter keywords to describe this group.
  - **Address** Enter the IP address or range of addresses (examples: *192.0.2.1* or *192.0.2.1-15*). Click **Add New** to enter more IP addresses.

  Click **Save** to apply your changes.

- **Network Group** Make changes as needed.

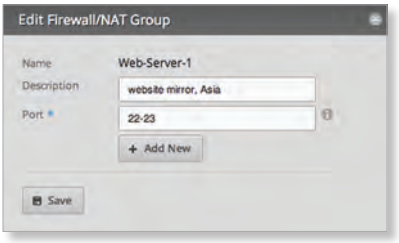


  - **Name** The name of this group is displayed.
  - **Description** Enter keywords to describe this group.
  - **Network** Enter the IP address and subnet mask using slash notation:
    <network_IP_address>/<subnet_mask_number>
    (example: *192.0.2.0/24*).

    Click **Add New** to enter more network addresses.

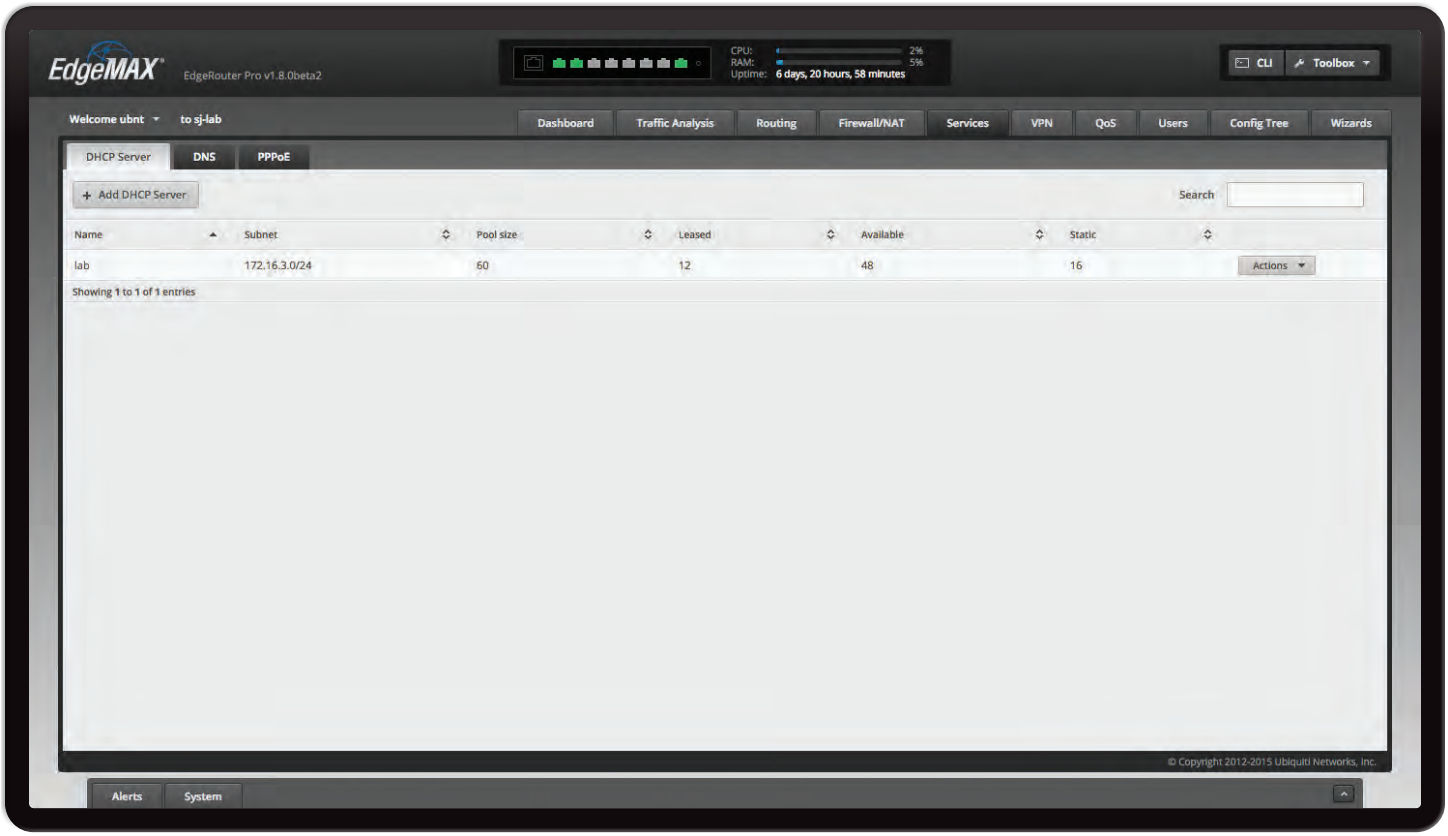
  Click **Save** to apply your changes.

- **Port Group** Make changes as needed.



  - **Name** The name of this group is displayed.
  - **Description** Enter keywords to describe this group.
  - **Port** Enter the port name, number, or range. Click **Add New** to enter more ports.

  Click **Save** to apply your changes.



Chapter 7: Services

The *Services* tab displays status information about DHCP servers, Domain Name System (DNS) forwarding, Dynamic DNS, and the PPPoE server. Any setting marked with a blue asterisk * is required. When the information ⓘ icon is displayed, you can click the icon for more information about an option.

You have three sub-tabs:

DHCP Server Configure DHCP servers to implement different subnets on the independent interfaces.

DNS Configure DNS forwarding and Dynamic DNS interfaces and services.

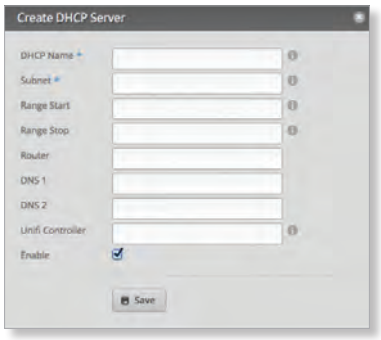
PPPoE Server Configure the PPPoE server so a remote PPPoE client can establish a tunnel to the EdgeRouter for network access.

DHCP Server

A DHCP server assigns IP addresses to DHCP clients. You can configure multiple DHCP servers to assign IP ranges in different subnets on the different interfaces.

Add DHCP Server To create a new DHCP server, click **Add DHCP Server**.

The *Create DHCP Server* screen appears.



Complete the following:

- **DHCP Name** Enter a name for this DHCP server.
- **Subnet** Enter the IP address and subnet mask using slash notation: *<network_IP_address>*/*<subnet_mask_number>* (example: *192.0.2.0/24*).
- **Range Start** Enter the starting IP address of the range.
- **Range Stop** Enter the last IP address of the range.
- **Router** Enter the default route of the DHCP clients. The DHCP clients route all packets to this IP address, which is the EdgeRouter's own IP address in most cases.
- **DNS 1** Enter the IP address of the primary DNS server. Your ISP may provide this information, or you can use Google's DNS server at *8.8.8.8*.
- **DNS 2** Enter the IP address of the secondary DNS server.

- **UniFi Controller** Enter the IP address of the UniFi® Controller. The DHCP server will return the UniFi Controller's IP address to its DHCP clients, so if a client is a UniFi AP, it will know how to contact the UniFi Controller.
- **Enable** Check the box to enable this DHCP server.

Click **Save** to apply your changes.

Search Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

A table displays the following information about each DHCP server. Click a column heading to sort by that heading.

Name The name of the DHCP server is displayed.

Subnet The IP address and subnet mask of the DHCP server are displayed.

Pool size The total number of IP addresses is displayed.

Leased The number of leased IP addresses is displayed.

Available The number of available IP addresses is displayed.

Static The number of static IP addresses is displayed.

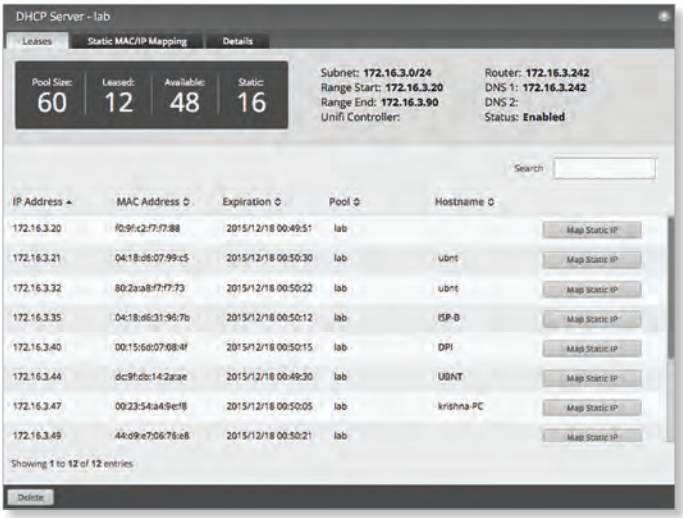
Actions Click the **Actions** button to access the following options:

- **View Leases** To view the current DHCP leases, click **View Leases**. Go to the *Configure the DHCP Server > Leases* section.
- **Configure Static Map** To map static IP addresses to MAC addresses, click **Configure Static Map**. Go to **"Static MAC/IP Mapping" on page 41**.
- **View Details** To configure the DHCP server, click **View Details**. Go to **"Details" on page 42**.
- **Delete** Delete the DHCP server; its configuration will be removed.
- **Disable** Disable the DHCP server while keeping its configuration.

Configure the DHCP Server

The *DHCP Server* - screen appears. You have three tabs available.

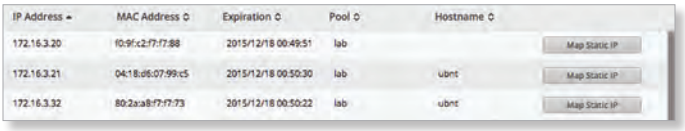
Leases



The top section displays the following status information:

- **Pool Size** The total number of IP addresses is displayed. The DHCP server assigns IP address from the pool (or group) of IP addresses.
- **Leased** The number of used IP addresses is displayed.
- **Available** The number of available IP addresses is displayed.
- **Static** The number of static IP addresses is displayed.
- **Subnet** The IP address and subnet mask of the DHCP server are displayed in slash notation.
- **Range Start** The starting IP address of the range is displayed.
- **Range End** The last IP address of the range is displayed.
- **Router** The default route of the DHCP clients is displayed. The DHCP clients route all packets to this IP address, which is the EdgeRouter's own IP address in most cases.
- **DNS** The IP address of the DNS server is displayed.
- **Status** The *Enabled*/*Disabled* status of the DHCP server is displayed.
- **Search** Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

A table displays the following information about each DHCP client. Click a column heading to sort by that heading.

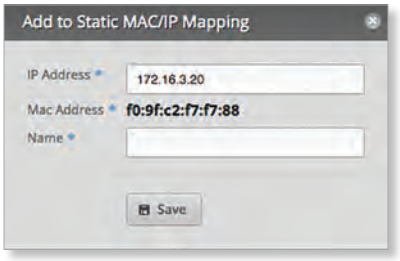


- **IP Address** The IP address assigned to the DHCP client is displayed.
- **MAC Address** The MAC address of the DHCP client is displayed.
- **Lease Expiration** The date and time when the DHCP lease will expire is displayed.
- **Pool** The name of the DHCP server is displayed.
- **Hostname** The name used to identify the DHCP client is displayed.
- **Map Static IP** To convert a dynamic DHCP lease into a static mapping, click **Map Static IP**. Go to the *Add to Static MAC/IP Mapping* section below.

  At the bottom of the screen, you can click *Delete* to delete the DHCP server and its configuration.

Add to Static MAC/IP Mapping

The *Add to Static MAC/IP Mapping* appears.

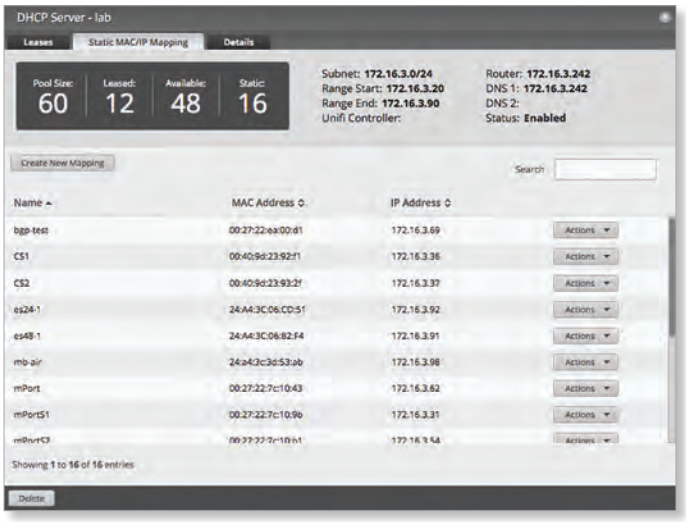


Complete the following:

- **IP Address** The IP address assigned to the DHCP client is displayed. You can change this as needed.
- **MAC Address** The MAC address of the DHCP client is displayed.
- **Name** The name used to identify the DHCP client is displayed. You can change this as needed.

Click **Save** to apply your changes.

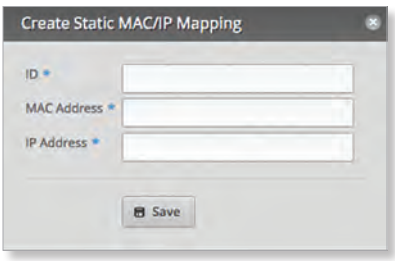
Static MAC/IP Mapping



The top section displays the following status information:

- **Pool Size** The total number of IP addresses is displayed.
- **Leased** The number of used IP addresses is displayed.
- **Available** The number of available IP addresses is displayed.
- **Static** The number of static IP addresses is displayed.
- **Subnet** The IP address and subnet mask of the DHCP server are displayed in slash notation.
- **Range Start** The starting IP address of the range is displayed.
- **Range End** The last IP address of the range is displayed.
- **Router** The default route of the DHCP clients is displayed. The DHCP clients route all packets to this IP address, which is the EdgeRouter's own IP address in most cases.
- **DNS 1/2** The IP address of the DNS server is displayed.
- **Status** The *Enabled*/*Disabled* status of the DHCP server is displayed.
- **Create New Mapping** To map a static IP address to a specific MAC address, click **Create New Mapping**.

  The *Create Static MAC/IP Mapping* appears.



Complete the following:

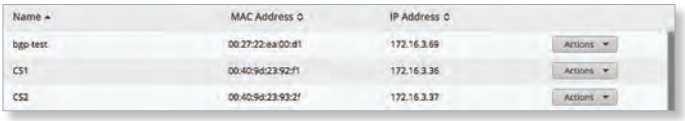
- **ID** Enter a name for this mapping.
- **MAC Address** Enter the MAC address of the DHCP client.

- **IP Address** Enter the IP address that should be assigned.

Click **Save** to apply your changes.

- **Search** Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

A table displays the following information about each static MAC/IP mapping. Click a column heading to sort by that heading.

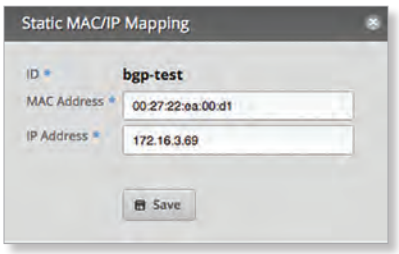


- **Name** The name of the mapping is displayed.
- **MAC Address** The MAC address of the DHCP client is displayed.
- **IP Address** The IP address assigned to the corresponding MAC address is displayed.
- **Actions** Click the **Actions** button to access the following options:
  - **Config** To configure the mapping, click **Config**. Go to the *Configure Static MAC/IP Mapping* section below.
  - **Delete** Remove the selected mapping.

  At the bottom of the screen, you can click *Delete* to delete the DHCP server and its configuration.

Configure Static MAC/IP Mapping

The *Static MAC/IP Mapping* screen appears.

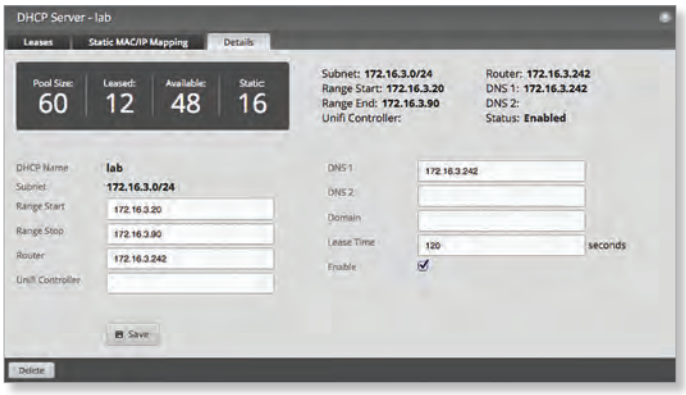


Make changes as needed.

- **ID** The name of this mapping is displayed.
- **MAC Address** Enter the MAC address of the DHCP client.
- **IP Address** Enter the IP address that should be assigned.

Click **Save** to apply your changes.

Details



The top section displays the following status information:

- **Pool Size** The total number of IP addresses is displayed.
- **Leased** The number of used IP addresses is displayed.
- **Available** The number of available IP addresses is displayed.
- **Static** The number of static IP addresses is displayed.
- **Subnet** The IP address and subnet mask of the DHCP server are displayed in slash notation.
- **Range Start** The starting IP address of the range is displayed.
- **Range End** The last IP address of the range is displayed.
- **Router** The default route of the DHCP clients is displayed. The DHCP clients route all packets to this IP address, which is the EdgeRouter's own IP address in most cases.
- **DNS 1/2** The IP address of the DNS server is displayed.
- **Status** The *Enabled*/*Disabled* status of the DHCP server is displayed.

The rest of the *Details* tab displays the following:

- **DHCP Name** The name of the DHCP server is displayed.
- **Subnet** The IP address and subnet mask of the DHCP server are displayed in slash notation.

Make changes as needed to the following options:

- **Range Start** Enter the starting IP address of the range.
- **Range Stop** Enter the last IP address of the range.
- **Router** Enter the default route of the DHCP clients. The DHCP clients route all packets to this IP address, which is the EdgeRouter's own IP address in most cases.
- **UniFi Controller** Enter the IP address of the UniFi Controller. The DHCP server will return the UniFi Controller's IP address to its DHCP clients, so if a client is a UniFi AP, it will know how to contact the UniFi Controller.
- **DNS 1** Enter the IP address of the primary DNS server. Your ISP may provide this information, or you can use Google's DNS server at *8.8.8.8*.
- **DNS 2** Enter the IP address of the secondary DNS server.

- **Domain** Enter the domain name for DHCP clients.
- **Lease Time** Enter the period of time (in seconds) that a DHCP lease should last.
- **Enable** Check the box to enable this DHCP server.

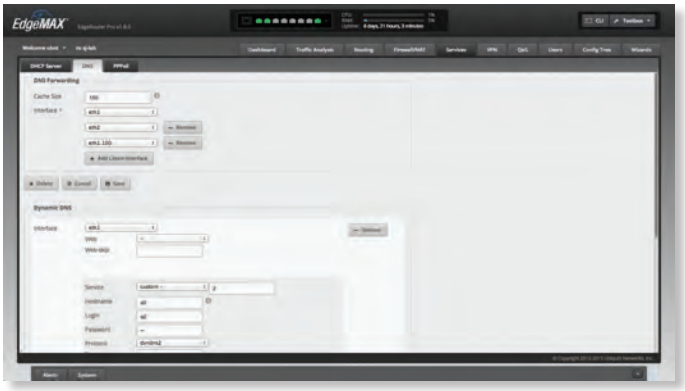
  Click **Save** to apply your changes.

  At the bottom of the screen, you can click *Delete* to delete the DHCP server and its configuration.

DNS

DNS translates domain names to IP addresses; each DNS server on the Internet holds these mappings in its respective DNS database.

On the *DNS* tab, you can configure multiple interfaces for DNS forwarding. You can also configure multiple Dynamic DNS interfaces using multiple Dynamic DNS services.



DNS Forwarding

The EdgeRouter receives all LAN DNS requests and forwards them to the service provider's DNS server. The EdgeRouter receives responses from the DNS server and forwards them to the LAN clients.

Cache Size Completed DNS requests are cached so response time is faster for cached entries, and there is less traffic traveling to the DNS server. Enter the maximum number of DNS queries to cache.

Interface Select the appropriate interface that the EdgeRouter will listen to so it can forward DNS requests.

Add Listen Interface You can select multiple interfaces. To add another interface for DNS forwarding, click **Add Listen Interface**. From the new *Interface* drop-down menu, select the appropriate interface.

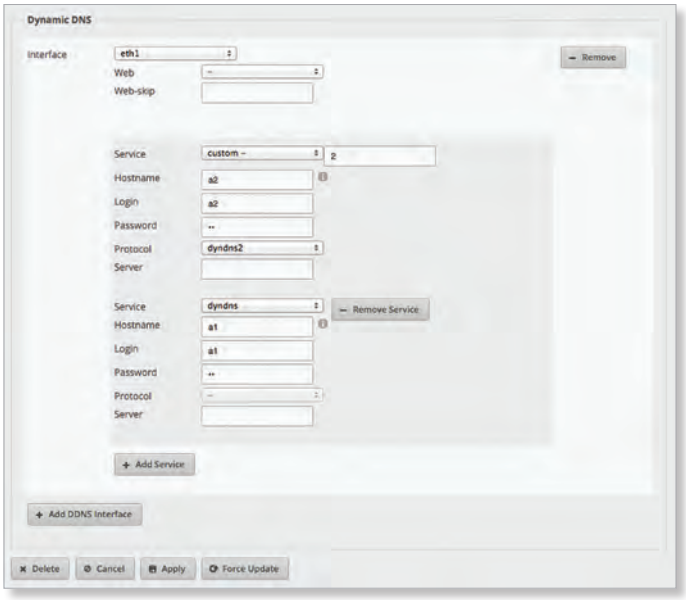
Remove Click **Remove** to delete an interface.

You can click *Delete* to delete the DNS forwarding configuration.

Click **Save** to apply your changes, or click *Cancel*.

Dynamic DNS

Dynamic DNS (DDNS) is a network service that notifies the DNS server in real time of any changes in the device's IP settings. Even if the device's IP address changes, you can still access the device through its domain name.



Add DDNS Interface To add an interface for DDNS service, click **Add DDNS Interface**. Then configure its settings.

- **Interface** Select the appropriate interface of the EdgeRouter.
- **Remove** Click **Remove** to delete an interface.
- **Web** Select the appropriate webpage used to obtain the public IP address, or select **URL** and enter the custom URL. The *Web* and *Web-skip* settings support scenarios in which the router is behind another level of NAT.
- **Web-skip** Enter the text that should be ignored and precedes the public IP address on the selected webpage. This will vary depending on the DDNS service you use. Examples: '*IP Address:* ' and '*Current IP Address:* ' (Ensure you include a space after the colon.)
  - **Service** Select the appropriate DDNS service provider from the drop-down menu, or select **custom** and enter the name of the DDNS service provider.
  - **Hostname** Enter the host name of the device, which has to be updated on the DDNS server. Example: *sample.ddns.com*
  - **Login** Enter the username of the DDNS account.
  - **Password** Enter the password of the DDNS account.
  - **Protocol** Select the appropriate protocol from the drop-down menu.
  - **Server** Enter the IP address or hostname of the DDNS server that should receive DDNS updates.

- **Add Service** You can use multiple services as long as they use the same protocol. To add another DDNS service, click **Add Service**. Then configure a new set of DDNS service settings (except for the *Protocol* setting).

Add DDNS Interface You can use multiple DDNS interfaces. To add another interface for DDNS service, click **Add DDNS Interface**. Then configure a new set of DDNS interface settings.

You can click *Delete* to delete the DDNS configuration.

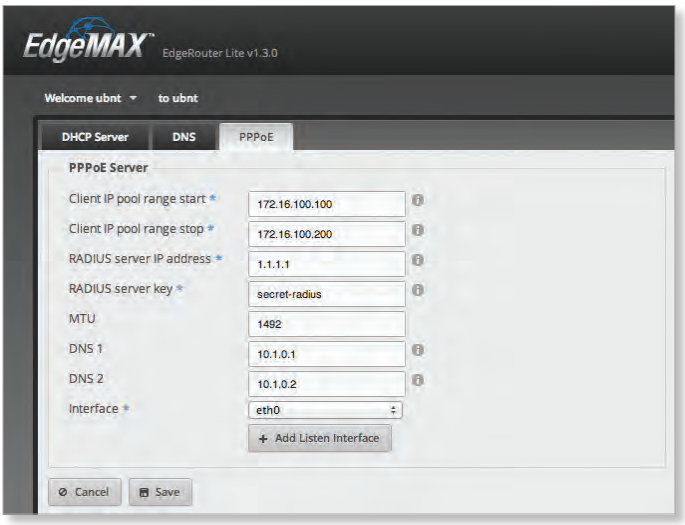
Click **Apply** to save your changes, or click *Cancel*.

You can click *Force Update* to initiate an update of the device's IP address on the DDNS server.

PPPoE

The EdgeRouter can function as a PPPoE (Point-to-Point Protocol over Ethernet) server so a remote PPPoE client can establish a tunnel to the EdgeRouter for network access.

PPPoE Server



Note: If you configured PPPoE using the CLI or the config tree, then you must disable those changes before using the *PPPoE* tab in the web UI.

Client IP pool range start The client IP pool is the pool of IP addresses that remote PPPoE clients will use. Enter the starting IP address of the range (this address must in a /24 subnet).

Client IP pool range stop Enter the last IP address of the range.

RADIUS server IP address The RADIUS (Remote Access Dial-In User Service) server provides authentication to help secure PPPoE connections. Enter the IP address of the RADIUS server.

RADIUS server key Enter the key shared with the RADIUS server.

MTU Enter the MTU (Maximum Transmission Unit) value, which is the maximum packet size (in bytes) that a network interface can transmit. The default is *1492* for the PPPoE connection.

DNS 1 Enter the IP address of the primary remote access DNS server that your PPPoE client will use.

DNS 2 Enter the IP address of the secondary remote access DNS server.

Interface Select the appropriate interface that the EdgeRouter will listen to so it can forward PPPoE requests.

Add Listen Interface You can select multiple interfaces. To add another interface for PPPoE connections, click **Add Listen Interface**. From the new *Interface* drop-down menu, select the appropriate interface.

Click **Save** to apply your changes, or click *Cancel*.

Chapter 8: VPN

The *VPN* tab displays status information about PPTP and IPsec VPN options. You can also configure these options. Any setting marked with a blue asterisk * is required. When the information ⓘ icon is displayed, you can click the icon for more information about an option.

You have two sub-tabs:

PPTP Remote Access Configure the EdgeRouter as a PPTP VPN server.

IPsec Site-to-Site Configure the EdgeRouter as a peer router for a basic IPsec site-to-site VPN tunnel.

PPTP Remote Access

A common type of VPN uses PPTP (Point-to-Point Tunneling Protocol). The EdgeRouter can function as a PPTP VPN server so a remote VPN client can access the LAN using a PPTP VPN tunnel over the Internet.

Client IP pool range start The client IP pool is the pool of IP addresses that remote VPN clients will use. Enter the starting IP address of the range (this address must in a /24 subnet).

Client IP pool range stop Enter the last IP address of the range.

Server outside address Enter the IP address that VPN clients will connect to; this is the outside or external address of the PPTP server.

RADIUS server IP address The RADIUS (Remote Access Dial-In User Service) server provides authentication to help secure VPN tunnels. Enter the IP address of the RADIUS server.

RADIUS server key Enter the key shared with the RADIUS server.

MTU Enter the MTU (Maximum Transmission Unit) value, which is the maximum packet size (in bytes) that a network interface can transmit. The default is *1492* for the PPTP VPN connection.

DNS 1 Enter the IP address of the primary remote access DNS server that your VPN client will use.

DNS 2 Enter the IP address of the secondary remote access DNS server.

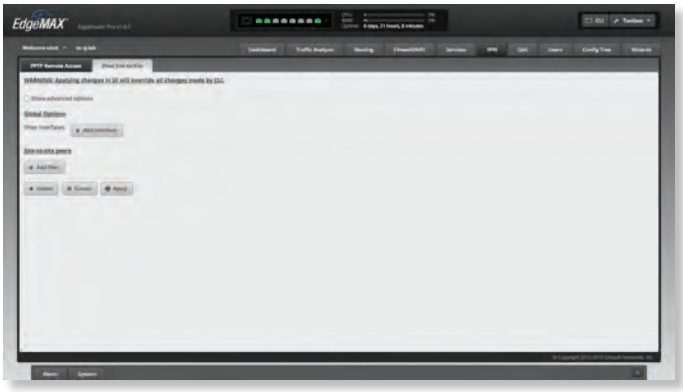
You can click *Delete* to delete the PPTP remote access configuration.

Click **Save** to apply your changes, or click *Cancel*.

IPsec Site-to-Site

A common type of VPN uses IPsec (IP security protocol). The EdgeRouter can function as a peer router so two peer routers can create an IPsec site-to-site VPN tunnel over the Internet. Configuration supports multiple peers, multiple tunnels per peer, and pre-shared secrets.

Note: Any changes you save in the graphical user interface will override any changes you made in the CLI.

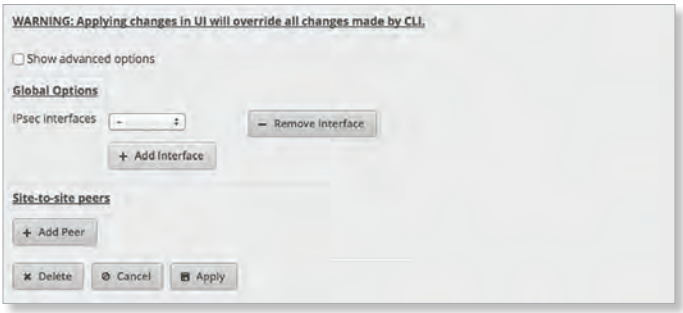


Show advanced options Select this checkbox to display the *Firewall* option.

Global Options

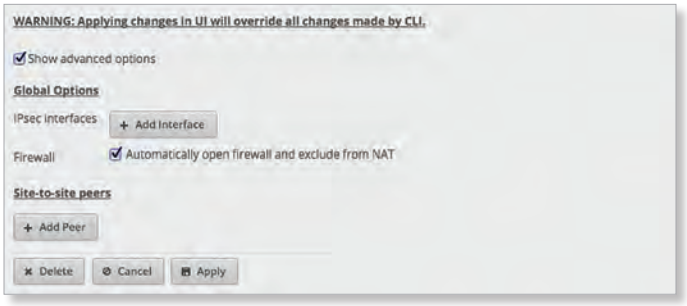
IPsec Interfaces To create a new IPsec interface, click **Add Interface**. Then select the appropriate interface from the drop-down menu.

Remove Interface To delete an IPsec interface, click **Remove Interface**.



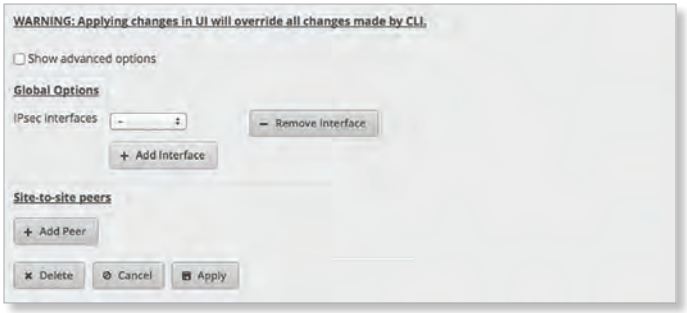
Firewall Enabled by default. Displayed if *Show advanced options* is enabled. If you want the EdgeRouter to automatically open the firewall and exclude it from the NAT, then keep *Firewall* enabled.

If you disable the *Firewall* option, then you will need to manually define firewall rules on the *Firewall/NAT* > *Firewall Policies* tab (refer to **"Firewall Policies" on page 28**).



Site-to-Site Peers

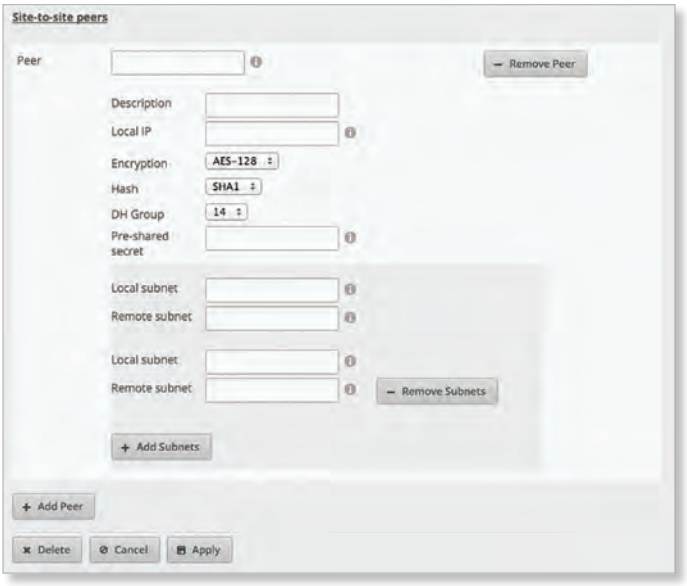
Add Peer To add a site-to-site peer, click **Add Peer**.



Complete the following:

- **Peer** Enter the host name or IPv4/IPv6 address of the peer router.
- **Description** Enter keywords to describe the peer router.
- **Local IP** Enter the IPv4/IPv6 address of the EdgeRouter, or enter **any**.
- **Encryption** Displayed if *Show advanced options* is enabled. Both peer routers must use the same encryption method. Select the appropriate encryption method: **AES-128**, **AES-256**, or **3DES**. The default is *AES-128*.
- **Hash** Displayed if *Show advanced options* is enabled. Both peer routers must use the same hash algorithm. Select the appropriate hash algorithm: **SHA1** or **MD5**. The default is *SHA1*.
- **DH Group** Displayed if *Show advanced options* is enabled. The DH (Diffie-Hellman) group specifies the strength of the DH encryption key for the key exchange. Both peer routers must use the same DH group. Select the appropriate DH group: **2**, **5**, **14**, **15**, **16**, **19**, **20**, **21**, **25**, or **26**. The default is *14*.
- **Pre-shared secret** Enter the pre-shared secret key. Both peer routers must use the same pre-shared secret key for authentication.
- **Local subnet** Enter the local IPv4/IPv6 network address.
- **Remote subnet** Enter the remote IPv4/IPv6 network address.
- **Add Subnets** To create a new set of subnets, click **Add Subnets**. Then complete the new *Local subnet* and *Remote subnet* fields.

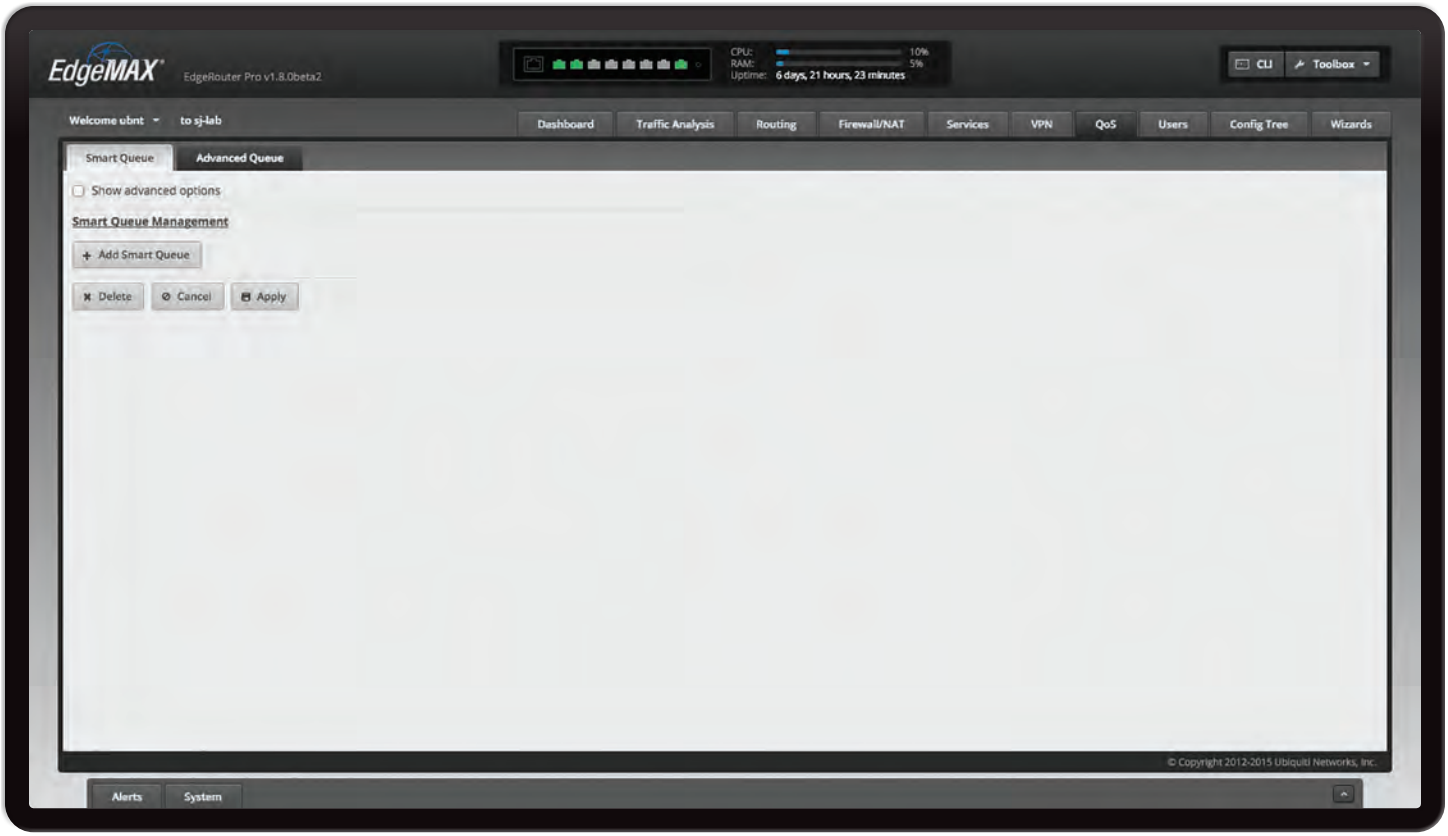
- **Remove Subnets** To delete a set of subnets, click **Remove Subnets**.



Remove Peer To delete a peer, click **Remove Peer**.

You can click *Delete* to delete the IPsec site-to-site configuration.

Click **Apply** to save your changes, or click *Cancel*.



Chapter 9: QoS

The *QoS* tab displays status information about Smart Queue QoS and Advanced Queue QoS options. You can also configure these options. Any setting marked with a blue asterisk * is required. When the information ⓘ icon is displayed, you can click the icon for more information about an option.

You have two sub-tabs:

Smart Queue Optimize the usage of overall WAN bandwidth.

Advanced Queue Configure a hierarchical tree of queues to implement a sophisticated bandwidth-sharing scheme.

Smart Queue

The Smart Queue feature provides FQ-CODEL (Fair Queuing with Controlled Delay) + HTB (Hierarchical Token Bucket) function and supports dynamic interfaces, even if the dynamic interfaces do not exist yet (the policy will be applied later when the interface comes up).

The HTB rate limiting is computation-intensive, so the rate limiting will not work well (cannot achieve the specified rate) above a certain threshold rate. The actual threshold (applied to the sum of the upload and download rates) depends on the specific model and conditions of the actual environment.

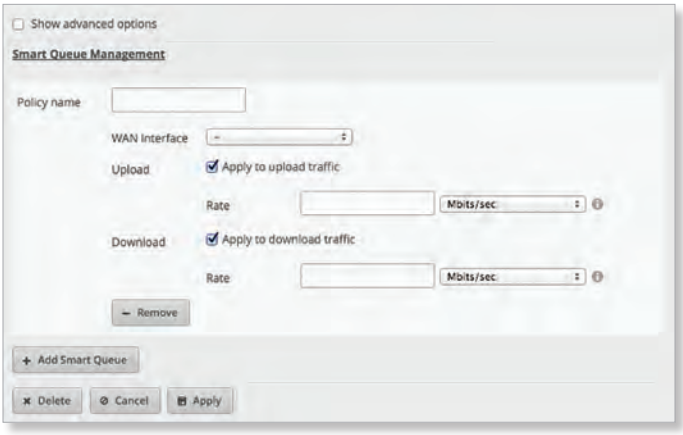
Here are general guidelines on the expected Smart Queue shaping performance:

Model	Most Likely Will Work Below This Speed	Most Likely Will Not Work Above This Speed
EP-R6	100 Mbps	250 Mbps
EP-R8	120 Mbps	330 Mbps
ER-X	100 Mbps	250 Mbps
ER-X-SFP	100 Mbps	250 Mbps
ERLite-3	60 Mbps	200 Mbps
ERPoe-5	60 Mbps	200 Mbps
ER-8	160 Mbps	450 Mbps
ERPro-8	200 Mbps	550 Mbps

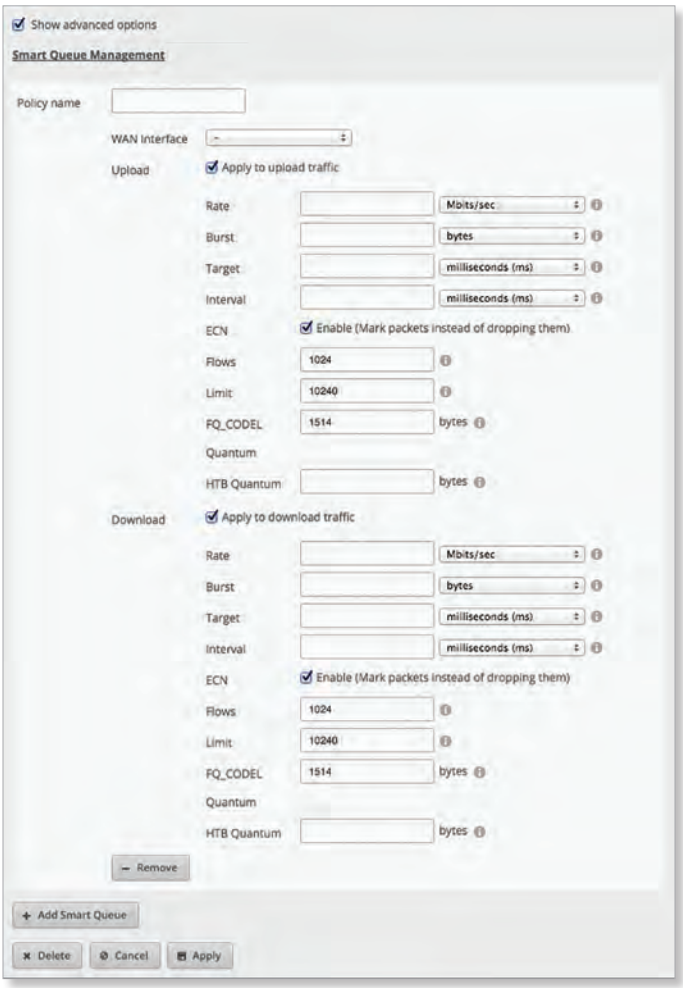
It may require some testing to find the actual threshold in a specific environment, depending on the actual setup, traffic patterns, and other conditions. The actual rate limits will be set to 95% of the specified value, so you can experiment with different values if necessary.

Each smart queue policy applies to one interface. You can configure multiple policies for different interfaces.

Note: The Smart Queue feature conflicts with the existing traffic policy configuration, so the two should not be applied to the same interface at the same time.



Show advanced options Select this checkbox to display the *Burst*, *Target*, *Interval*, *ECN*, *Flows*, *Limit*, *FQ_CODEL*, *Quantum*, and *HTB Quantum* options.



Smart Queue Management To create a new smart queue, click **Add Smart Queue**. Then complete the following options:

- **Policy name** Enter a descriptive name.
- **WAN Interface** Select the appropriate interface.
- **Upload** Select **Apply to upload traffic** to manage QoS for upload traffic.
  - **Rate** Enter the bandwidth limit, and select the unit of measurement: **bits/sec**, **Kbits/sec**, or **Mbits/sec**.
  - **Burst** Displayed if *Show advanced options* is enabled. Enter the amount of data that can burst at best-effort, and select the unit of measurement: **bytes**, **Kbytes**, or **Mbytes**. The valid range is *1500 bytes* to *10 Mbytes*.
  - **Target** Displayed if *Show advanced options* is enabled. Enter the minimum queue delay, and select the unit of measurement: **microseconds (µs)**, **milliseconds (ms)**, or **seconds**. The valid range is *10 µs* to *10 s*.

  Note: The *Target* and *Interval* are automatically calculated for low-bandwidth links if the values are not specified.
  - **Interval** Displayed if *Show advanced options* is enabled. When the minimum queue delay has exceeded the *Target* for longer than the configured *Interval*, the EdgeRouter will enter drop mode. Enter the time interval, and select the unit of measurement: **microseconds (µs)**, **milliseconds (ms)**, or **seconds**. The valid range is *1 ms* to *20 s*.

  Note: The *Target* and *Interval* are automatically calculated for low-bandwidth links if the values are not specified.
  - **ECN** Displayed if *Show advanced options* is enabled. Select the ECN (Explicit Congestion Notification) option if you want to mark packets instead of dropping them. Enabled by default.
  - **Flows** Displayed if *Show advanced options* is enabled. Enter the number of flows into which the incoming packets are classified. The valid range is *1* to *65535*. The default is *1024*.
  - **Limit** Displayed if *Show advanced options* is enabled. Enter the hard limit on the real queue size. The valid range in number of packets is *1* to *1000000*. The default is *10240*.
  - **FQ_CODEL Quantum** Displayed if *Show advanced options* is enabled. Enter the packet scheduling quantum for FQ_CODEL. The valid range in bytes is *256* to *65535*. The default is *1514*.
  - **HTB Quantum** Displayed if *Show advanced options* is enabled. Enter the packet scheduling quantum for HTB. The valid range in bytes is *1* to *65535*.
- **Download** Select **Apply to download traffic** to manage QoS for download traffic.
  - **Rate** Enter the bandwidth limit, and select the unit of measurement: **bits/sec**, **Kbits/sec**, or **Mbits/sec**.
  - **Burst** Displayed if *Show advanced options* is enabled. Enter the amount of data that can burst at best-effort, and select the unit of measurement: **bytes**, **Kbytes**, or **Mbytes**. The valid range is *1500 bytes* to *10 Mbytes*.

- **Target** Displayed if *Show advanced options* is enabled. Enter the minimum queue delay, and select the unit of measurement: **microseconds (µs)**, **milliseconds (ms)**, or **seconds**. The valid range is *10 µs* to *10 s*.

Note: The *Target* and *Interval* are automatically calculated for low-bandwidth links if the values are not specified.

- **Interval** Displayed if *Show advanced options* is enabled. When the minimum queue delay has exceeded the *Target* for longer than the configured *Interval*, the EdgeRouter will enter drop mode. Enter the time interval, and select the unit of measurement: **microseconds (µs)**, **milliseconds (ms)**, or **seconds**. The valid range is *1 ms* to *20 s*.

Note: The *Target* and *Interval* are automatically calculated for low-bandwidth links if the values are not specified.

- **ECN** Displayed if *Show advanced options* is enabled. Select this option if you want to mark packets instead of dropping them. Enabled by default.
- **Flows** Displayed if *Show advanced options* is enabled. Enter the number of flows into which the incoming packets are classified. The valid range is *1* to *65535*. The default is *1024*.
- **Limit** Displayed if *Show advanced options* is enabled. Enter the hard limit on the real queue size. The valid range in number of packets is *1* to *1000000*. The default is *10240*.
- **FQ_CODEL Quantum** Displayed if *Show advanced options* is enabled. Enter the packet scheduling quantum for FQ_CODEL. The valid range in bytes is *256* to *65535*. The default is *1514*.
- **HTB Quantum** Displayed if *Show advanced options* is enabled. Enter the packet scheduling quantum for HTB. The valid range in bytes is *1* to *65535*.

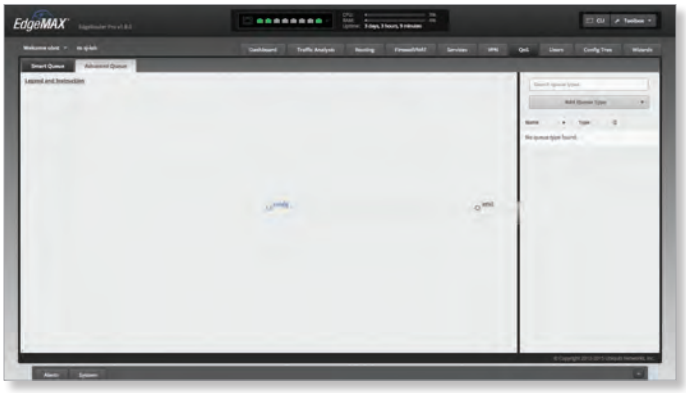
Remove To delete a smart queue, click **Remove**.

You can click *Delete* to delete the smart queue configuration.

Click **Apply** to save your changes, or click *Cancel*.

Advanced Queue

The Advanced Queue feature provides more functionality and flexibility than the existing traffic policy features. With the Advanced Queue feature, you can configure a hierarchical tree of queues to implement a more complex bandwidth-sharing scheme, as opposed to the existing traffic-policy shaper, which only supports flat queues.



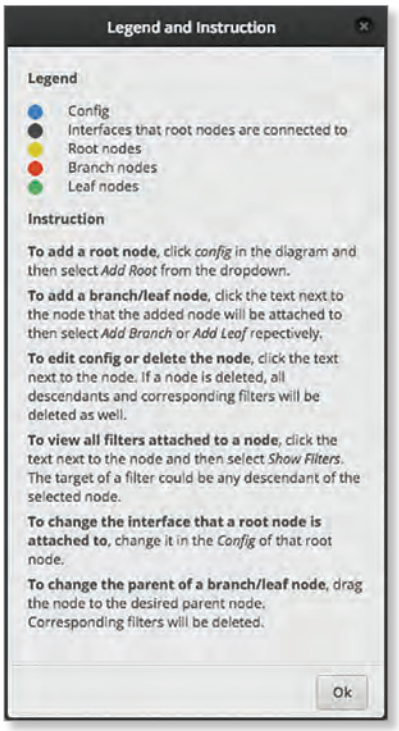
You can attach a QoS policy globally instead of attaching it to only a specific interface. A global attachment designates all traffic – not traffic specific to one interface and direction. A global attachment can make it easier to design the policy and can also provide greater flexibility, as the QoS policy is applied after destination NAT and before source NAT (for example, private IP addresses can be used for QoS policy matching).

A tree of queues consists of root, branch, and leaf nodes. For example, there is a root node R1, which is attached globally. Branch node B11 represents download policies, and leaf node L12 represents upload policies. For download, the traffic is further divided to use different policies according to the subnet.

At each root or branch node, you can attach filters to classify the different traffic that belongs to different child nodes. At each leaf node, a separately defined queue type is attached. For example, the upload direction uses FQ-CODEL. For download, one subnet uses SFQ (Stochastic Fairness Queueing) while the other uses HFQ (Host Fairness Queueing).

Legend and Instructions

Legend and Instructions Click **Legend and Instructions** to display UI (User Interface) information on-screen.



Click **OK** to close the popup.

Icons

The icons indicate the type of node or interface in the diagram depicting the tree of queues:

Icon	Description
	Config
	Interfaces that root nodes are connected to
	Root nodes
	Branch nodes
	Leaf nodes

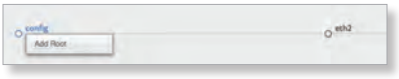
User Interface

The *Advanced Queue* tab allows you to set up the root/branch/leaf nodes, filters, and queue types using an intuitive graphical user interface. The diagram allows for the following interactions:

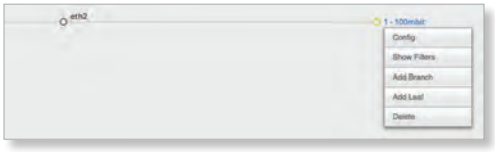
- **Drag and Drop** Drag and drop a node so you can move a branch node from one root node to another.
- **Pan** Pan the tree of queues by dragging it with your mouse.
- **Center** Click a node to center the diagram around that node.
- **Zoom** Use your mouse wheel to zoom in or out.

Configuration Options

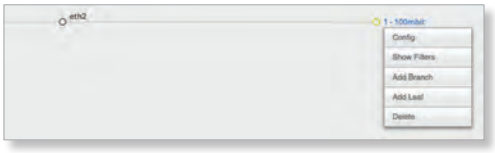
config (to add root node) This option creates a root node. Click **config** in the diagram and then select **Add Root** from the drop-down menu. Proceed to **"Add Root" on page 53**.



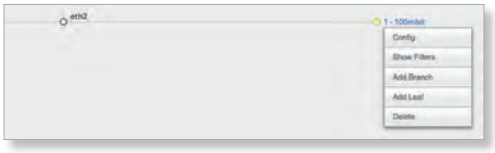
config (to edit a configuration) This option allows you to make changes, including changing the interface that the node is attached to. Click the text next to the node icon. Proceed to **"Config" on page 53**.



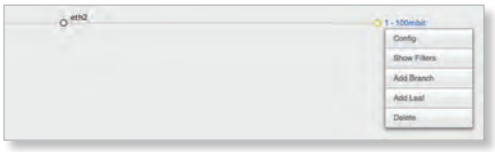
Show Filters (Not available for leaf nodes.) This option displays any filter you have created. The target of a filter can be any descendant of the selected node. Click the text next to the node icon and select **Show Filters**. Proceed to **"Show Filters" on page 53**.



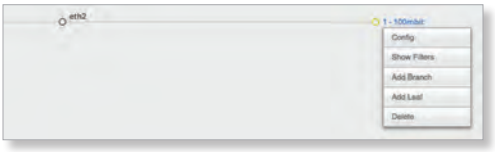
Add Branch This option creates a branch node associated with a root node. Click the text next to the node icon that the added node will be attached to. Then select **Add Branch**. Proceed to the appropriate section: **"Add Branch" on page 55**.



Add Leaf This option creates a leaf node associated with a root node. Click the text next to the node that the added node will be attached to. Then select **Add Leaf**. Proceed to the appropriate section: **"Add Leaf" on page 55**.



Delete This option deletes a node, as well as all of its descendants and corresponding filters. Click the text next to the node icon. Proceed to the appropriate section: **"Delete" on page 56**.



Add Root

- **Queue ID** Enter an identifier. The valid range is *1* to *1023*.
- **Attach to** Select **global** or the appropriate interface that the queue will attach to.
- **Description** Enter keywords to describe the traffic class.
- **Bandwidth** Enter the bandwidth limit, and select the appropriate unit of measurement: **bits/sec**, **Kbits/sec**, or **Mbits/sec**.

  Click **Save** to apply your changes, or click *Cancel*.

Config

- **Queue ID** The identifier is displayed.
- **Attach to** Select **global** or the appropriate interface that the queue will attach to.
- **Description** Enter keywords to describe the traffic class.
- **Bandwidth** Enter the bandwidth limit, and select the appropriate unit of measurement: **bits/sec**, **Kbits/sec**, or **Mbits/sec**.

  Click **Save** to apply your changes, or click *Cancel*.

Show Filters

Note: The *Show Filters* option does not apply to leaf nodes.

- **Search** Allows you to search for specific text. Begin typing; there is no need to press enter. The results are filtered in real time as soon as you type two or more characters.

  A table displays the following information about each filter. Click a column heading to sort by that heading.
- **Description** The keywords describing the filter are displayed.
- **Filter ID** The identifier is displayed.
- **Target** The target is displayed.
- **Source** The source IP address is displayed.
- **Destination** The destination IP address is displayed.
- **Add New Filter** Click to create a new filter. The *Create Filter* screen appears.

You have two tabs available:

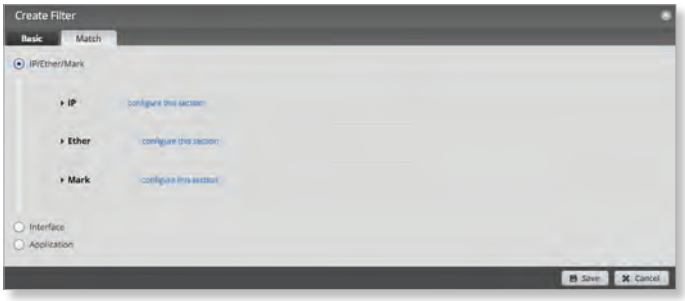
- Basic (below)
- Match (next column)

Basic

- **Filter ID** Enter the identifier.
- **Attach to** The queue ID that the filter will attach to is displayed.
- **Target** Select the appropriate target from the drop-down menu.
- **Description** Enter keywords to describe the filter.

Click **Save** to apply your changes, or click *Cancel*.

Match



You have three options available:

- IP/Ether/Mark (below)
- **"Interface" on page 55**
- **"Application" on page 55**

Select the option you want to match and go to the appropriate instructions.

IP/Ether/Mark

You can configure one or more of the following options:

- IP (below)
- **"Ethernet" on page 54**
- **"Mark" on page 55**

Go to the appropriate instructions.

IP

Click **configure this section** to configure the *IP* settings.

- **DSCP** Enter the IP DSCP (Differentiated Services Code Point) value. The valid range is *0* to *63*.

802.1p Class of Service	TOS Range	DSCP Range	WME Category
0 – Best Effort	0x00-0x1f	0-7	Best Effort
1 – Background	0x20-0x3f	8-15	Background
2 – Spare	0x40-0x5f	16-23	Background
3 – Excellent Effort	0x60-0x7f	24-25, 28-31	Best Effort
4 – Controlled Load	0x80-0x9f	32-39	Video
5 – Video (<100 ms latency)	0xa0-0xbf	40-45	Video
6 – Voice (<10 ms latency)	0x68, 0xb8, 0xc0-0xdf	26-27, 46-47, 48-55	Voice
7 – Network Control	0xe0-0xff	56-63	Voice

- **Protocol** Enter the port number of the protocol. The valid range is *0* to *255*.
- **Source Address** Enter the IP address or network address of the source. You can also enter a range of IP addresses; one of them will be used.

Note: If you enter a network address, enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).

- **Source Port** Enter the port name or number of the source. You can also enter a range of port numbers; one of them will be used.
- **Destination Address** Enter the IP address or network address of the destination. You can also enter a range of IP addresses; one of them will be used.

Note: If you enter a network address, enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).

- **Destination Port** Enter the port name or number of the destination. You can also enter a range of port numbers; one of them will be used.

Click **Save** to apply your changes, or click *Cancel*.

Ethernet

Click **configure this section** to configure the *Ether* settings.

- **Protocol**
  - **No restrictions on protocols** Match packets of all protocols.
  - **Choose a protocol by name** Select the protocol from the drop-down list. Match packets of this protocol.

  - **Enter a protocol number** Enter the port number of the protocol. Match packets of this protocol. The valid range is *0* to *65535*.

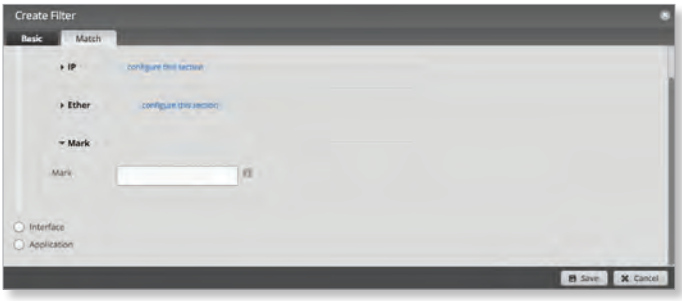
- **Enter a protocol name** Enter the name of the protocol. Match packets of this protocol.

- **Source** Enter the Ethernet source address.
- **Destination** Enter the Ethernet destination address.

Click **Save** to apply your changes, or click *Cancel*.

Mark

Click **configure this section** to configure the *Mark* settings.



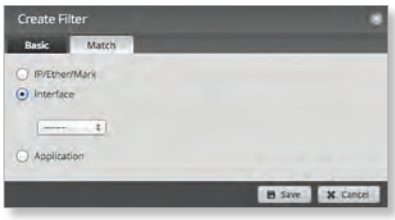
- **Mark** Configure the filter to match packets with the specified marking. For example, you can configure a firewall policy to add different markings to packets according to certain criteria (refer to **"Firewall Policies" on page 28** for more information). These markings can then be matched in the QoS filters.

  Enter the appropriate decimal or hexadecimal value. The valid decimal range is *0* to *255*. The valid hexadecimal range is *0x0* to *0xff*.

Note: Advanced users can use a higher value than 255 or *0xff*; however, proceed with caution.

Click **Save** to apply your changes, or click *Cancel*.

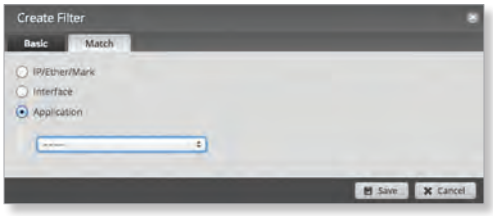
Interface



- **Interface** Select the appropriate interface from the drop-down menu.

Click **Save** to apply your changes, or click *Cancel*.

Application



- **Application** Select the appropriate application category from the drop-down menu. Refer to **"Category" on page 19** for more information.

Click **Save** to apply your changes, or click *Cancel*.

Add Branch

- **Queue ID** Enter an identifier. The valid range is *1* to *1023*.
- **Parent** The queue ID that the branch node will attach to is displayed.
- **Priority** Select the appropriate priority for usage of excess bandwidth.
- **Description** Enter keywords to describe the traffic class.
- **Bandwidth** Enter the bandwidth limit, and select the appropriate unit of measurement: **bits/sec**, **Kbits/sec**, or **Mbits/sec**.

Click **Save** to apply your changes, or click *Cancel*.

Note: To change the parent of a branch node, drag the branch node to the desired parent node. The corresponding filters will also be deleted.

Add Leaf

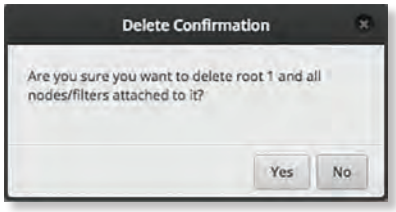
- **Queue ID** Enter an identifier. The valid range is *1* to *1023*.
- **Parent** The queue ID that the leaf node will attach to is displayed.
- **Priority** Select the appropriate priority for usage of excess bandwidth.
- **Queue Type** Select the queue type for this class. Go to **"Queue Types" on page 56** for more information.

- **Description** Enter keywords to describe the traffic class.
- **Bandwidth** Enter the guaranteed bandwidth, and select the appropriate unit of measurement: **bits/sec**, **Kbits/sec**, or **Mbits/sec**.
- **Ceiling** Enter the bandwidth ceiling (maximum allowed bandwidth), and select the appropriate unit of measurement: **bits/sec**, **Kbits/sec**, or **Mbits/sec**.

Click **Save** to apply your changes, or click *Cancel*.

Note: To change the parent of a leaf node, drag the leaf node to the desired parent node.

Delete



Click **Yes** to delete the node and all nodes and filters attached to it, or click *No* to cancel.

Queue Types

Queueing determines how the EdgeRouter prioritizes traffic. You can create multiple queue types that use different algorithms to manage traffic.

Note: The *Queue Types* option does not apply to root or branch nodes.

Search Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

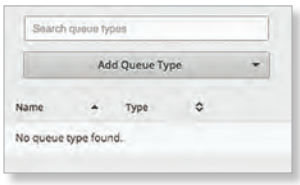
Add Queue Type To add a queue type, click **Add Queue Type** and select one of the following options:

- **"FQ_CODEL" on page 56**
- **"HFQ" on page 57**
- **"SFQ" on page 57**
- **"PFIFO" on page 57**

Proceed to the appropriate instructions for your queue type.

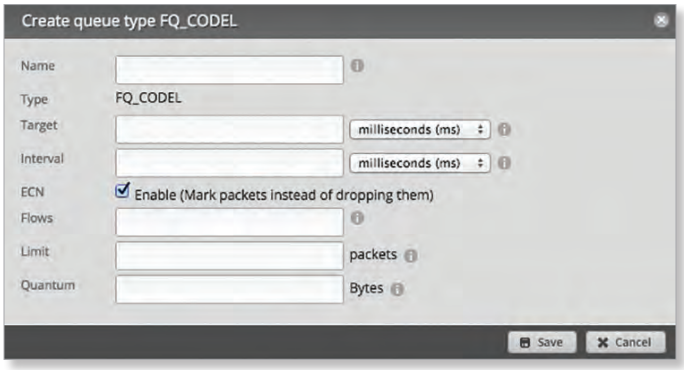
A table displays the following information about each queue type. Click a column heading to sort by that heading.

- **Name** The identifier of the queue type is displayed.
- **Type** The queue type is displayed.



FQ_CODEL

FQ-CODEL (Fair Queuing with Controlled Delay) is designed to provide equal service for all traffic flows while minimizing delays.

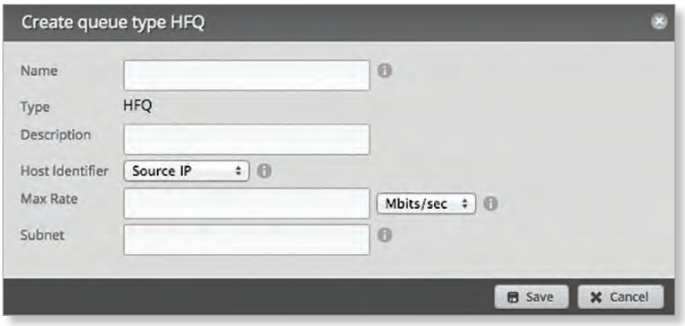


- **Name** Enter a unique identifier for this queue type.
- **Type** *FQ_CODEL* is displayed.
- **Target** Enter the minimum queue delay, and select the unit of measurement: **microseconds (µs)**, **milliseconds (ms)**, or **seconds**. The valid range is *10 µs* to *10 s*.
- **Interval** When the minimum queue delay has exceeded the *Target* for longer than the configured *Interval*, the EdgeRouter will enter drop mode. Enter the time interval, and select the unit of measurement: **microseconds (µs)**, **milliseconds (ms)**, or **seconds**. The valid range is *1 ms* to *20 s*.
- **ECN** Select this option if you want to mark packets instead of dropping them. Enabled by default.
- **Flows** Enter the number of flows into which the incoming packets are classified. The valid range is *1* to *65535*.
- **Limit** Enter the hard limit on the real queue size. The valid range in number of packets is *1* to *1000000*.
- **Quantum** Enter the packet scheduling quantum for FQ_CODEL. The valid range in bytes is *256* to *65535*.

Click **Save** to apply your changes, or click *Cancel*.

HFQ

Host Fairness Queueing (HFQ) provides simplified policy setup for scenarios in which all hosts of a specific subnet share the same policy. The EdgeRouter automatically applies the specified policy to every host in the specified subnet.



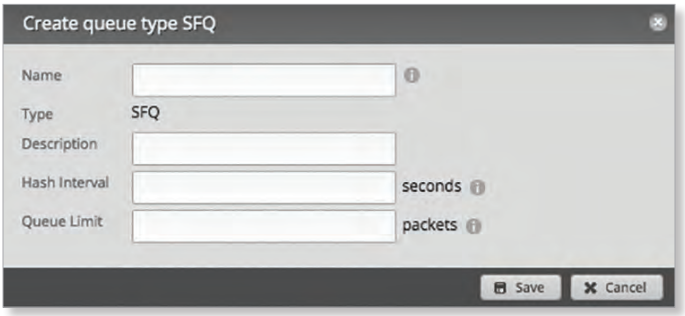
- **Name** Enter a unique identifier for this queue type.
- **Type** *HFQ* is displayed.
- **Description** Enter keywords to describe the queue type.
- **Host Identifier** Select the appropriate host identifier for the host fairness queue, **Source IP** or **Destination IP**. The default is *Source IP*.
- **Max Rate** Enter the maximum bandwidth limit per host, and select the appropriate unit of measurement: **bits/sec**, **Kbits/sec**, or **Mbits/sec**.
- **Subnet** Enter the IPv4 subnet (up to /22 in size) for the host fairness queue.

  Note: If you enter a network address, enter the IP address and subnet mask using slash notation: *<network_IP_address>/<subnet_mask_number>* (example: *192.0.2.0/24*).

Click **Save** to apply your changes, or click *Cancel*.

SFQ

With SFQ (Stochastic Fairness Queueing), traffic is separated into multiple FIFO (First In, First Out) queues, which are then serviced using a round-robin algorithm.



- **Name** Enter a unique identifier for this queue type.
- **Type** *SFQ* is displayed.
- **Description** Enter keywords to describe the queue type.
- **Hash Interval** Enter the hash interval in seconds. The valid range is *0* to *4294967295*.
- **Queue Limit** Enter the maximum queue size in packets. The valid range is *1* to *127*.

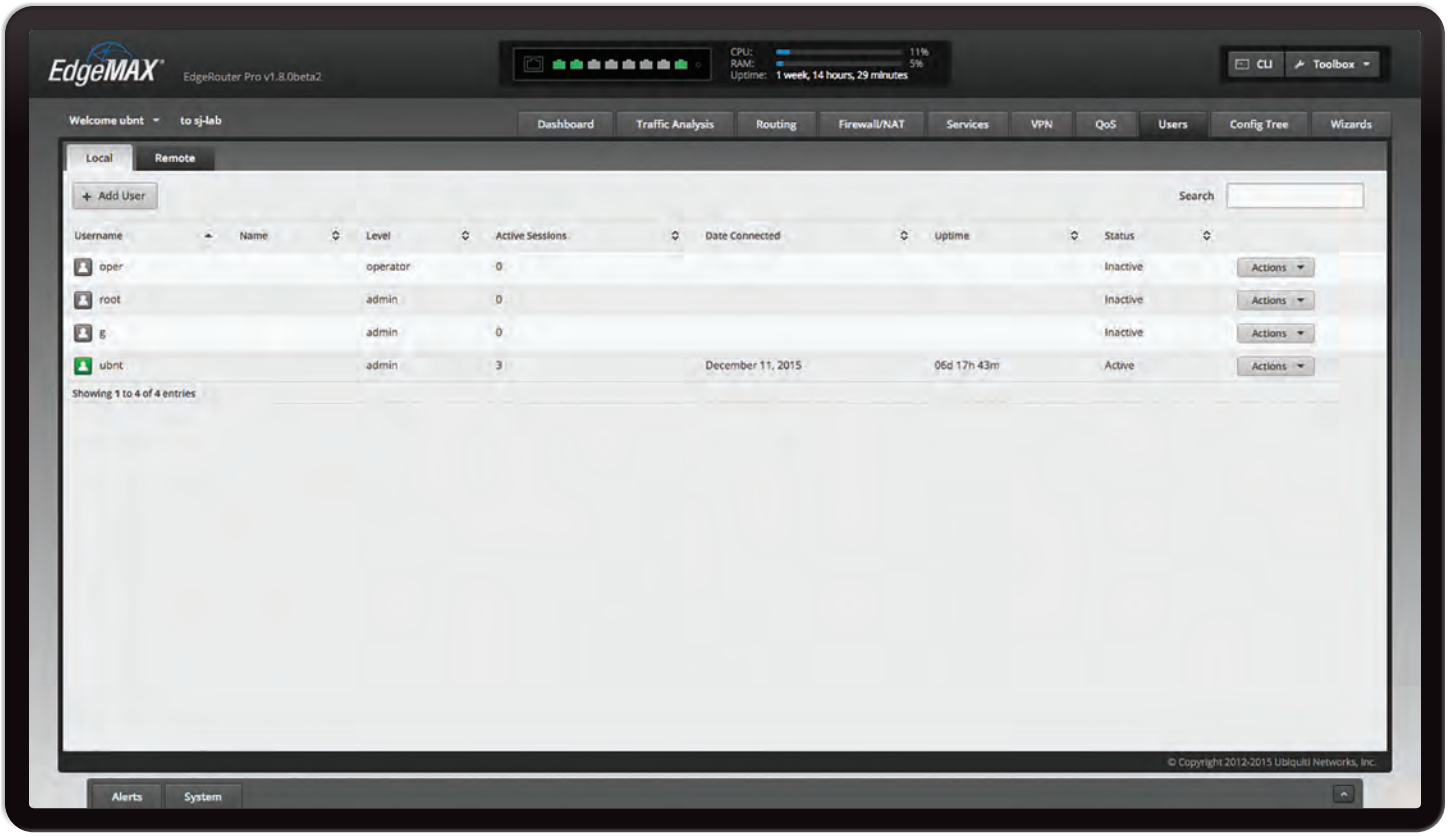
Click **Save** to apply your changes, or click *Cancel*.

PFIFO

With PFIFO (Priority First In, First Out) queueing, packets are serviced in order of priority, so highest-priority packets are serviced first. Medium-priority packets are serviced next. Low-priority packets are serviced last.

- **Name** Enter a unique identifier for this queue type.
- **Type** *PFIFO* is displayed.
- **Limit** Enter the hard limit on the real queue size. The valid range in number of packets is *1* to *1000000*.

Click **Save** to apply your changes, or click *Cancel*.



Chapter 10: Users

The *Users* tab displays account information about users. You can also configure these user accounts. Any setting marked with a blue asterisk * is required. When the information ⓘ icon is displayed, you can click the icon for more information about an option.

You have two sub-tabs:

Local Displays configurable user accounts.

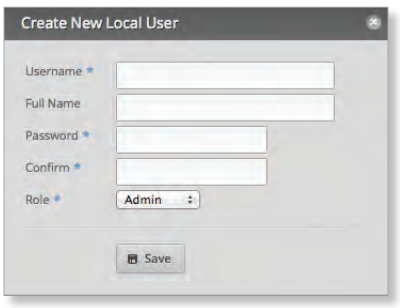
Remote Displays statistics about the users who remotely access the EdgeRouter.

Local

Configure user accounts with unique logins.

Add User To create a new user, click **Add User**.

The *Create New Local User* screen appears.



Complete the following:

- **Username** Enter a unique account name for the user.
- **Full Name** Enter the actual name of the user.
- **Password** Enter the password.
- **Confirm** Enter the password again.
- **Role** Select the appropriate permission level:
  - **Admin** The user can make changes to the EdgeRouter configuration.
  - **Operator** The user can view the EdgeRouter configuration but cannot make changes.

Click **Save** to apply your changes.

Search Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

A table displays the following information about each user. Click a column heading to sort by that heading.

Username The account name of the user is displayed.

Name The actual name of the user is displayed.

Level The permission level of the user is displayed.

Active Sessions The number of times the user has accessed the EdgeRouter is displayed.

Date Connected The date of the user's most recent access is displayed.

Uptime The duration of the user's access is displayed.

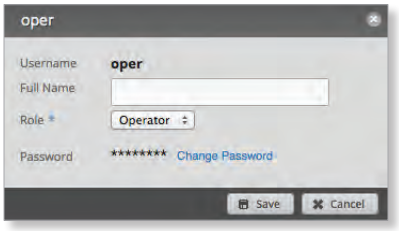
Status The status of the user is displayed.

Actions Click the **Actions** button to access the following options:

- **Config** To configure the user, click **Config**. Go to the *Configure the User* section below.
- **Delete** Delete the user account; its configuration will be removed.

Configure the User

After you click *Config*, the *Username* screen appears. Make changes as needed.



- **Username** The unique account name is displayed.
- **Full Name** Enter the actual name of the user.
- **Role** Select the appropriate permission level:
  - **Admin** The user can make changes to the EdgeRouter configuration.
  - **Operator** The user can view the EdgeRouter configuration but cannot make changes.
- **Password** Click **Change Password** to make a change.
  - **Password** Enter the new password.
  - **Confirm** Enter the new password again.
  - **Cancel Change Password** Click this option to cancel.

Click **Save** to apply your changes, or click *Cancel*.

Remote

Remote access of the EdgeRouter is logged on this tab.

Search Allows you to search for specific text. Begin typing; there is no need to press *enter*. The results are filtered in real time as soon as you type two or more characters.

PPTP/L2TP/PPPOE/All Click the appropriate tab to filter the remote users as needed.

- **PPTP** All users who use PPTP (Point-to-Point Tunneling Protocol) connections are displayed.
- **L2TP** All users who use L2TP (Layer 2 Tunneling Protocol) connections are displayed.
- **PPPOE** All users who use PPPOE (Point-to-Point over Ethernet) connections are displayed.
- **All** All remote users are displayed by default.

A table displays the following information about each remote user. Click a column heading to sort by that heading.

Name The actual name of the user is displayed.

Type The type of connection used by the user is displayed.

Time The duration of the user's access is displayed.

Interface The specific interface used by the user is displayed.

Remote IP The remote IP address of the user is displayed.

TX packets The number of packets transmitted is displayed.

TX bytes The number of bytes transmitted is displayed.

RX packets The number of packets received is displayed.

RX bytes The number of bytes received is displayed.

Chapter 11: Config Tree

The *Config Tree* tab allows you to view and modify the configuration using the config tree in the graphical user interface instead of typing commands in the Command Line Interface (CLI). (Refer to **"Command Line Interface" on page 83** for more information about the CLI.)
This chapter describes the basic functionality and user interface of the Config Tree.

When the information ⓘ icon is displayed, you can click the icon for more information about an option.

Click the corresponding **open/close** tab to hide or display the *Configuration* tree section or the *Discard* and *Preview* section.

User Interface

The following are used throughout the config tree:

node The term node describes any feature or field.

+ (plus sign) Equivalent to the *set* command in the CLI. Completing a field also means *set*. Click to add a node to the config. The node is displayed in regular font.

When you click **+** (plus sign), the node + becomes node -.

- (minus sign) Equivalent to the *delete* command in the CLI. Click to remove a node from the config. The node is displayed in boldface.

When you click - (minus sign), the **node -** becomes ~~node +~~.

node (red text) If you click + (plus sign) and the node is new, then the node is displayed in red.

For an existing node, the value of the node or child nodes will be changed after changes are applied. For example, if the value of *host-name* under *system* changes on the user interface, then system and host-name are displayed in red.

For a new node, the color red indicates that the node will be added to the EdgeRouter after changes are applied.

~~node~~ (red text with red strikethrough) If you click - (minus sign) for an existing node, then the node is displayed in red with red strikethrough. It will be removed after changes are applied.

. (period) Enter . (period) as an empty value.

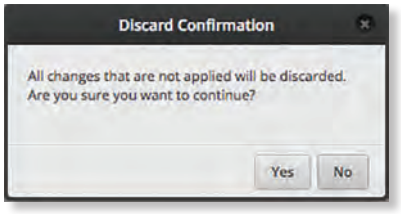
(blank field) A blank field deletes the value.

Update List If displayed, click **Update List** when you have added a node. This adds the node to the *Configuration* section on the left.

Discard and Preview

Discard Click *Discard* to cancel your changes. The *Discard Confirmation* screen appears.

- **Yes** Click **Yes** to remove your changes.
- **No** Click **No** to keep your changes, which are not applied yet.



Preview Click **Preview** to preview your new configuration changes. The *Commands to commit* screen appears and displays a summary of changes. You have two options:

- **Apply** Click **Apply** to save your changes immediately.
- **Not Now** Click **Not Now** to wait.

CLI Modes

Operational Mode

The root level of the config tree includes the following:

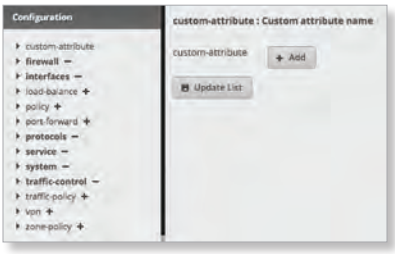
- custom-attribute
- firewall
- interfaces
- load-balance
- policy
- port-forward
- protocols
- service
- system
- traffic-control
- traffic-policy
- vpn
- zone-policy

Place your mouse over any node to display a brief description.

Configuration Example

Here is an example:

1. In the *Configuration* section, click **custom-attribute**.
2. Click **Add** to add a custom attribute.



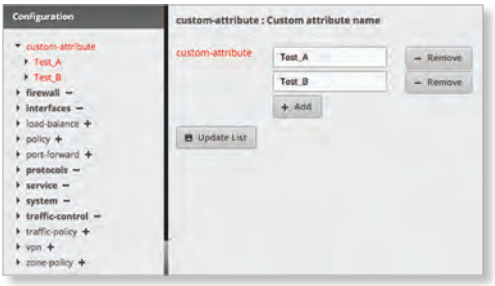
3. In the *custom-attribute* field, enter the name you want to use. You have two options:

   To add another custom attribute, click **Add**.

   To remove a custom attribute, click **Remove**.

Note: Type validation for generic types (such as text, numbers, and IP addresses) is used for fields.

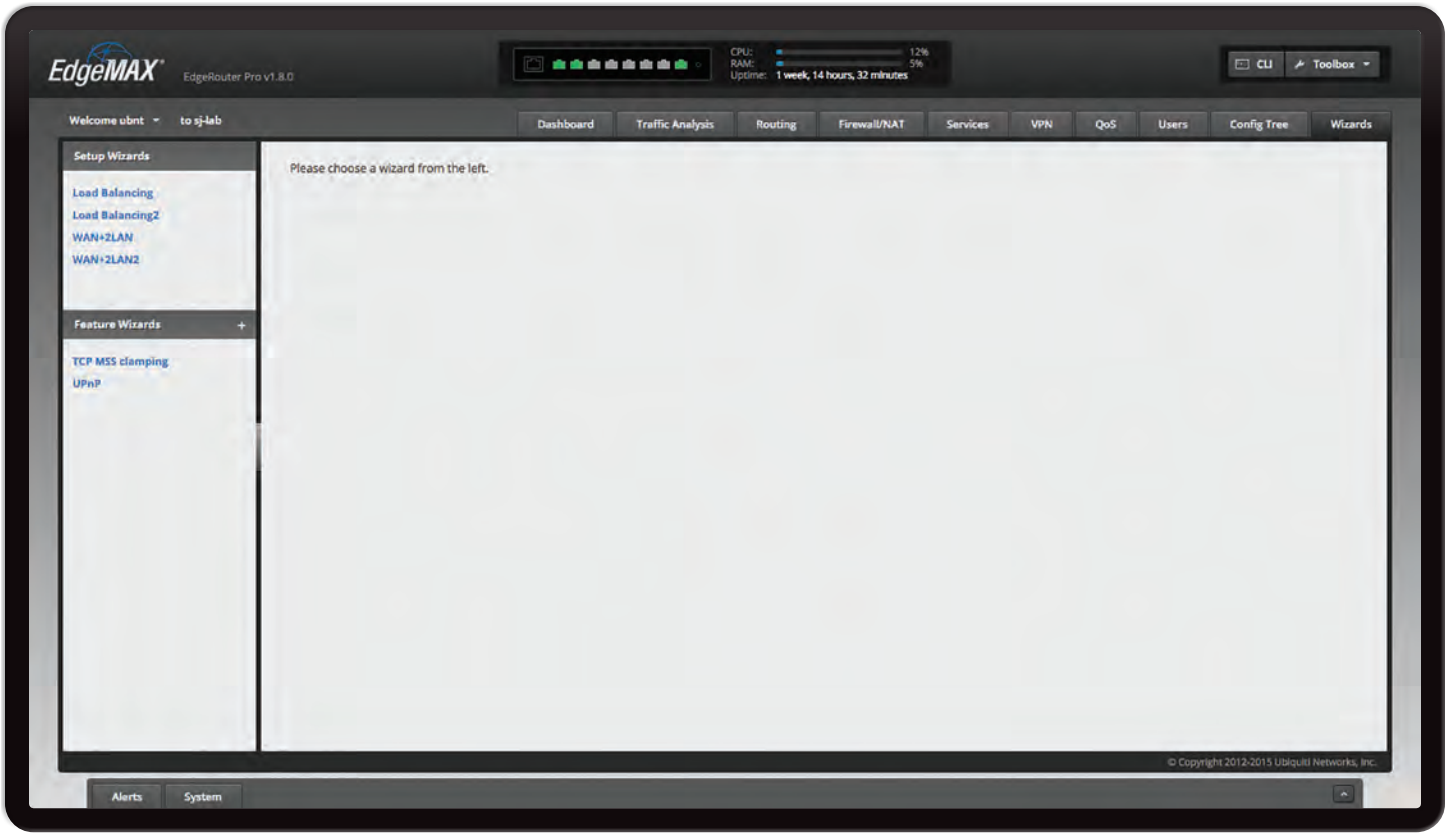
4. Click **Update List** to update your list of custom attributes.



5. Click **Preview**.

6. Click **Apply** to save your changes.

The configuration has been saved.



Chapter 12: Wizards

The *Wizards* tab allows you to access any available wizards:

- Setup Wizards
  - Load Balancing Wizard (in the next column)
  - **"Load Balancing2 Wizard" on page 70**
  - **"WAN+2LAN Wizard" on page 71**
  - **"WAN+2LAN2 Wizard" on page 74**
- Feature Wizards
  - **"TCP MSS Clamping" on page 78**
  - **"UPnP" on page 78**

Required fields are marked by a blue asterisk *. When the information ⓘ icon is displayed, you can click the icon for more information about an option.

Setup Wizards

There are two types of setup wizards:

- Load Balancing Wizards (in the next column)
- **"SOHO Deployment Wizards" on page 71**

Load Balancing Wizards

There are two load balancing setup wizards available:

- **Load Balancing** The *Load Balancing* setup wizard sets up basic load balancing and failover using two different Internet connections. You can also configure user accounts during setup. Go to the *Load Balancing* section below.
- **Load Balancing2** The *Load Balancing2* setup wizard sets up basic load balancing and failover using two different wireless links. You can also configure user accounts during setup. Go to **"Load Balancing2 Wizard" on page 70**.

Load Balancing Wizard

Before You Begin

Use the *Load Balancing* setup wizard to set up basic load balancing with two Internet connections from different Internet Service Providers (ISPs).

The *Load Balancing* setup wizard will replace the entire configuration and require a reboot when the new configuration is applied.

Overview

Click the **Load Balancing** setup wizard to begin.

Go to **"Load Balancing" on page 66** unless you have the ERPoe-5, then go to **"Load Balancing > ERPoe-5" on page 68**.

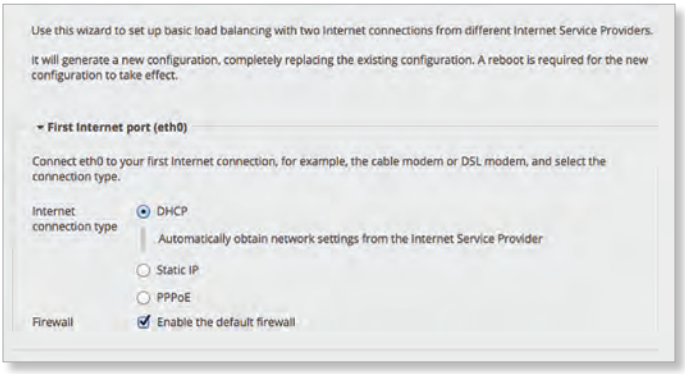
Load Balancing

First Internet Port (eth0)

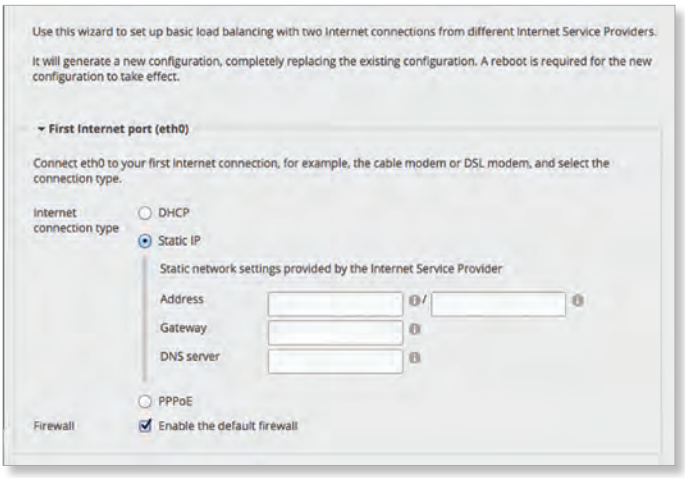
Connect *eth0* to your Internet connection.

Internet connection type Select the first Internet connection type your network is using.

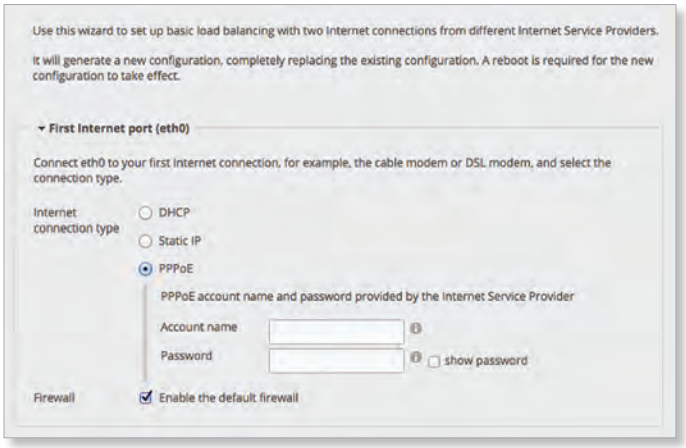
- **DHCP** Select this option if your ISP automatically assigns network settings to your network.



- **Static IP** Select this option if your ISP has assigned static network settings to your network.
  - **Address** Enter the IP address in the first field and the subnet mask or prefix length in the second field.
  - **Gateway** Enter the IP address of the ISP's gateway server, which provides the point of connection to the Internet.
  - **DNS server** Enter the IP address of the ISP's DNS server.



- **PPPoE** Select this option if your ISP uses PPPoE.
  - **Account Name** Enter the name of your PPPoE account.
  - **Password** Enter the password of your PPPoE account.
    - **show password** Select to display the password in plaintext.



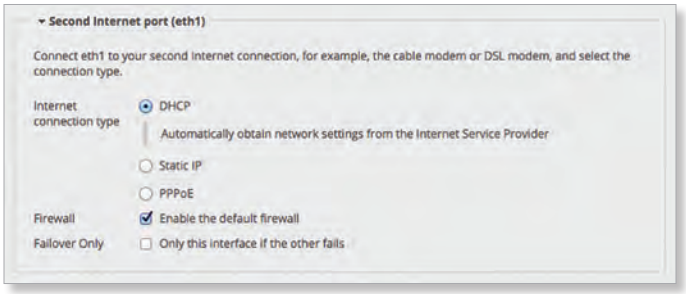
Firewall Enabled by default. This option applies the default firewall settings to the EdgeRouter; only established and related traffic types are allowed for local and inbound traffic.

Second Internet Port (eth1)

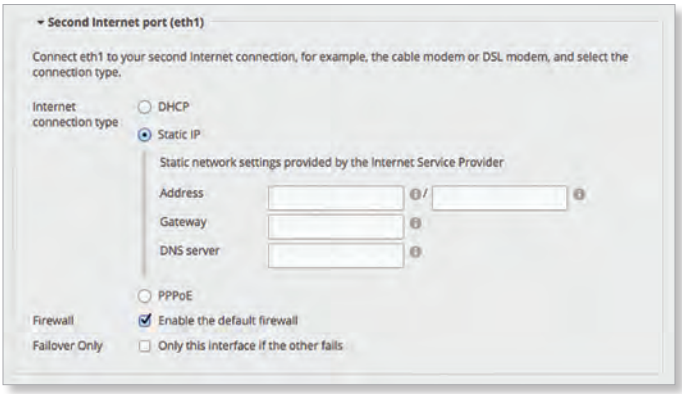
Connect *eth1* to your Internet connection.

Internet connection type Select the second Internet connection type your network is using.

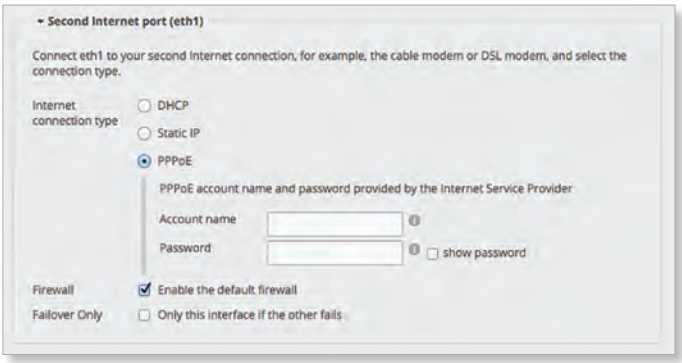
- **DHCP** Select this option if your ISP automatically assigns network settings to your network.



- **Static IP** Select this option if your ISP has assigned static network settings to your network.
  - **Address** Enter the IP address in the first field and the subnet mask or prefix length in the second field.
  - **Gateway** Enter the IP address of the ISP's gateway server, which provides the point of connection to the Internet.
  - **DNS server** Enter the IP address of the ISP's DNS server.

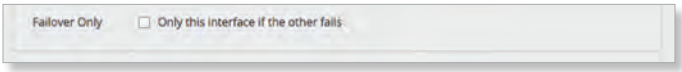


- **PPPoE** Select this option if your ISP uses PPPoE.
  - **Account Name** Enter the name of your PPPoE account.
  - **Password** Enter the password of your PPPoE account.
    - **show password** Select to display the password in plaintext.



Firewall Enabled by default. This option applies the default firewall settings to the EdgeRouter; only established and related traffic types are allowed for local and inbound traffic.

Failover Only Disabled by default. Select this option if you want to use *eth1* only if *eth0* fails.

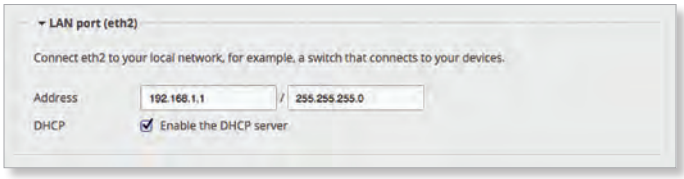


LAN Port (eth2)

Click **configure this section** if you connect *eth2* to your local network, such as a switch.

Address The IP address is displayed in the first field, and the subnet mask or prefix length is displayed in the second field.

DHCP Select this checkbox to have the EdgeRouter assign IP addresses.

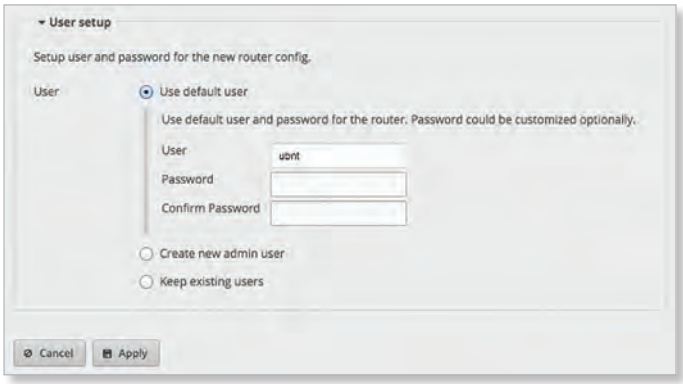


User Setup

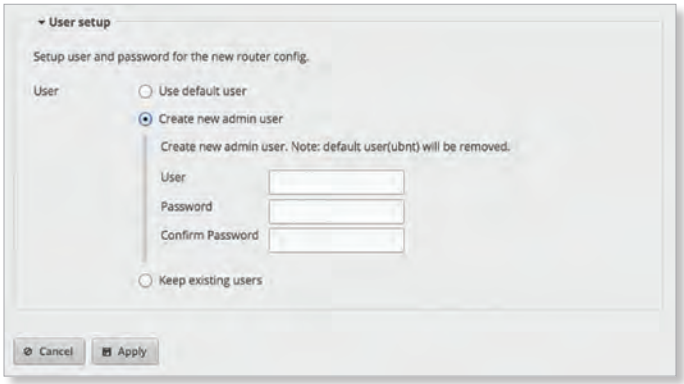
You can set up the username and password for the new EdgeRouter configuration.

User Select one of the following options:

- **Use default user** Replace the default user, *ubnt*.
  - **User** Enter a new admin username.
  - **Password** Enter a new password.
  - **Confirm Password** Enter the new password again.



- **Create new admin user** Create a new admin user and remove the default user, *ubnt*. Complete the following:
  - **User** Enter a new admin username.
  - **Password** Enter a new password.
  - **Confirm Password** Enter the new password again.



- **Keep existing users** Keep the existing usernames and passwords on the EdgeRouter.

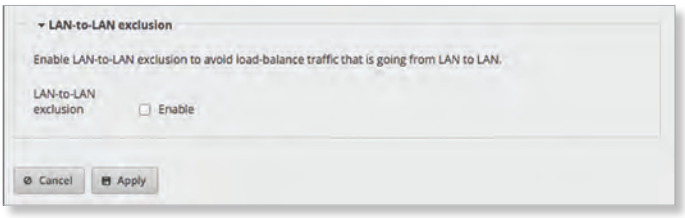
LAN-to-LAN Exclusion

The LAN-to-LAN exclusion feature excludes LAN-to-LAN traffic from load-balancing. Click **configure this section** to manage this feature.

The load balancing feature creates new routing tables for the WAN interfaces to use. This works well for LAN-to-WAN traffic; however, you do not want to load-balance traffic that is going from LAN to LAN. We recommend that you create a firewall/NAT group for the LAN networks and add a rule to the appropriate firewall policy, so this group uses the main routing table for LAN-to-LAN destinations. Refer to **"Firewall/NAT" on page 27** for more information.

Note: The LAN networks rule must precede the load-balance rule.

LAN-to-LAN exclusion This option excludes LAN-to-LAN traffic from load-balancing. Enabled by default.



Click **Apply** to save your changes, or click *Cancel*.

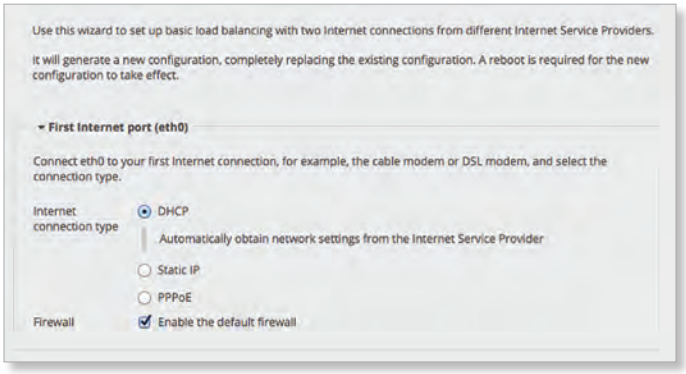
Load Balancing > ERPoe-5

First Internet Port (eth0)

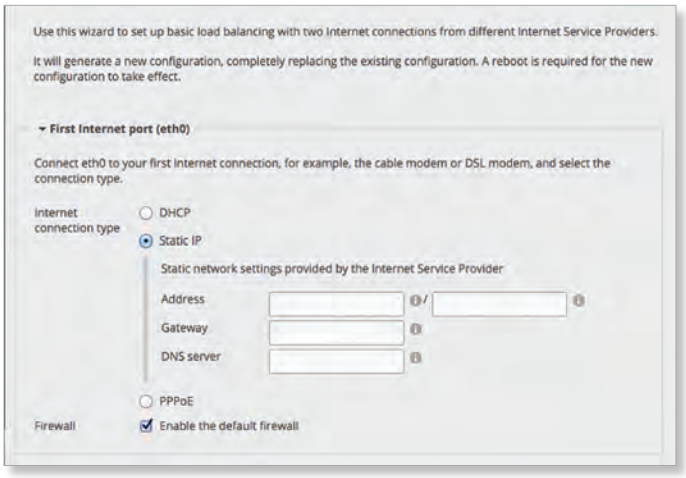
Connect *eth0* to your Internet connection.

Internet connection type Select the first Internet connection type your network is using.

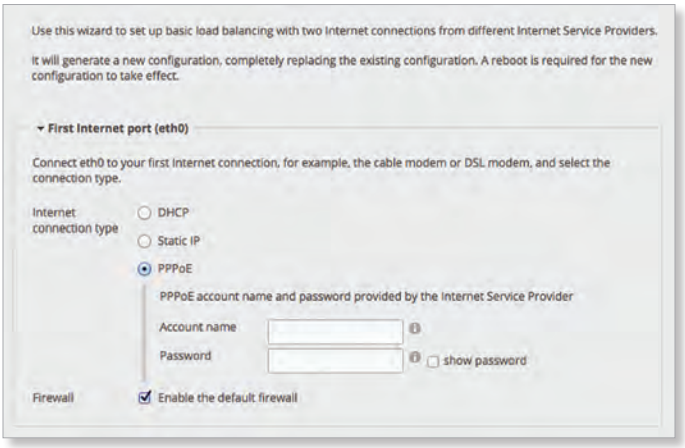
- **DHCP** Select this option if your ISP automatically assigns network settings to your network.



- **Static IP** Select this option if your ISP has assigned static network settings to your network.
  - **Address** Enter the IP address in the first field and the subnet mask or prefix length in the second field.
  - **Gateway** Enter the IP address of the ISP's gateway server, which provides the point of connection to the Internet.
  - **DNS server** Enter the IP address of the ISP's DNS server.



- **PPPoE** Select this option if your ISP uses PPPoE.
  - **Account Name** Enter the name of your PPPoE account.
  - **Password** Enter the password of your PPPoE account.
    - **show password** Select to display the password in plaintext.



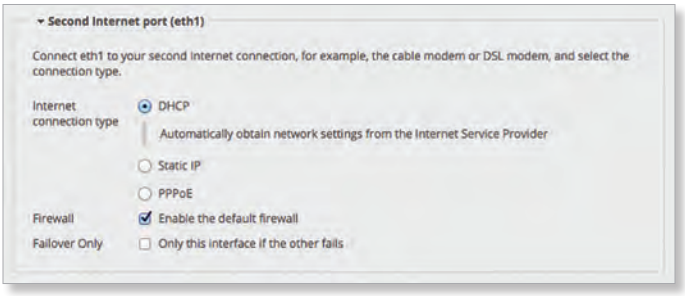
Firewall Enabled by default. This option applies the default firewall settings to the EdgeRouter; only established and related traffic types are allowed for local and inbound traffic.

Second Internet Port (eth1)

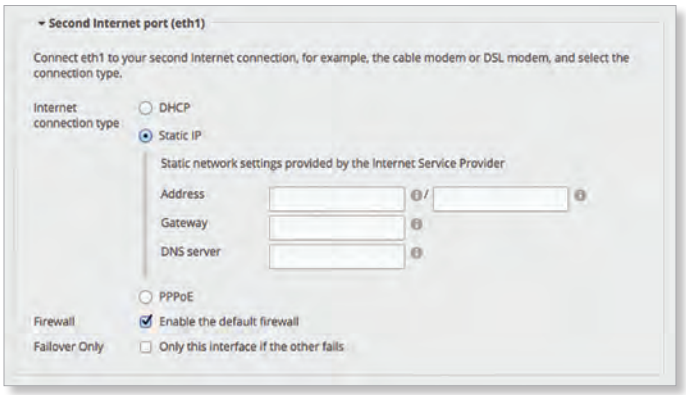
Connect *eth1* to your Internet connection.

Internet connection type Select the second Internet connection type your network is using.

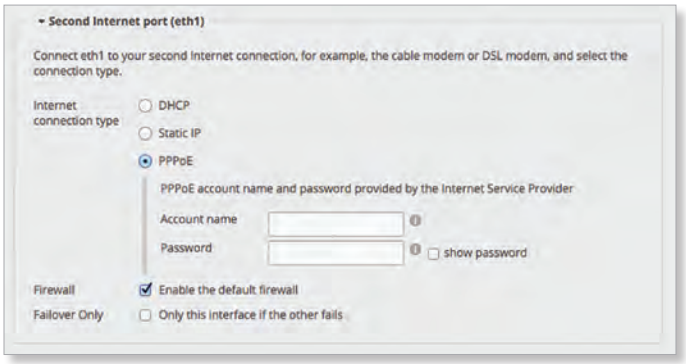
- **DHCP** Select this option if your ISP automatically assigns network settings to your network.



- **Static IP** Select this option if your ISP has assigned static network settings to your network.
  - **Address** Enter the IP address in the first field and the subnet mask or prefix length in the second field.
  - **Gateway** Enter the IP address of the ISP's gateway server, which provides the point of connection to the Internet.
  - **DNS server** Enter the IP address of the ISP's DNS server.

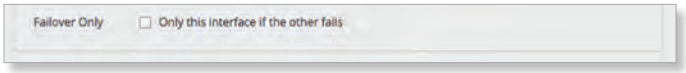


- **PPPoE** Select this option if your ISP uses PPPoE.
  - **Account Name** Enter the name of your PPPoE account.
  - **Password** Enter the password of your PPPoE account.
    - **show password** Select to display the password in plaintext.



Firewall Enabled by default. This option applies the default firewall settings to the EdgeRouter; only established and related traffic types are allowed for local and inbound traffic.

Failover Only Disabled by default. Select this option if you want to use *eth1* only if *eth0* fails.

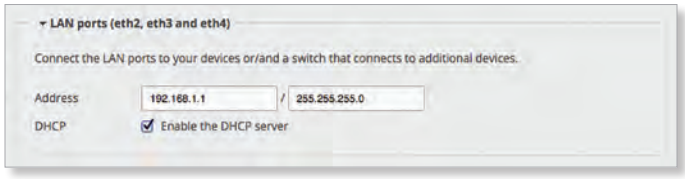


LAN Ports (eth2, eth3, and eth4)

Click **configure this section** if you connect *eth2*, *eth3*, and/or *eth4* to your devices and/or a switch. (The *eth2*, *eth3*, and/or *eth4* become switch ports for a local network.)

Address The IP address is displayed in the first field, and the subnet mask or prefix length is displayed in the second field.

DHCP Select this checkbox to have the EdgeRouter assign IP addresses.

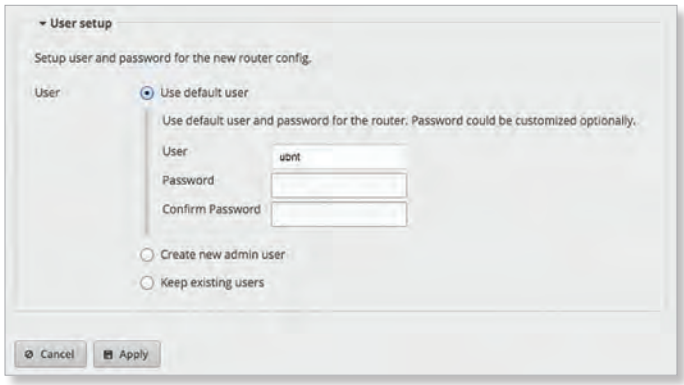


User Setup

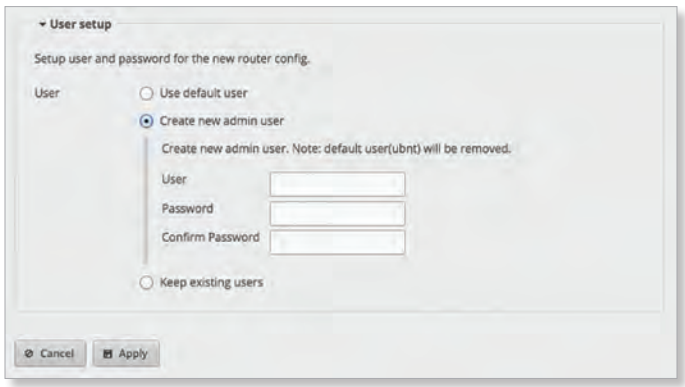
You can set up the username and password for the new EdgeRouter configuration.

User Select one of the following options:

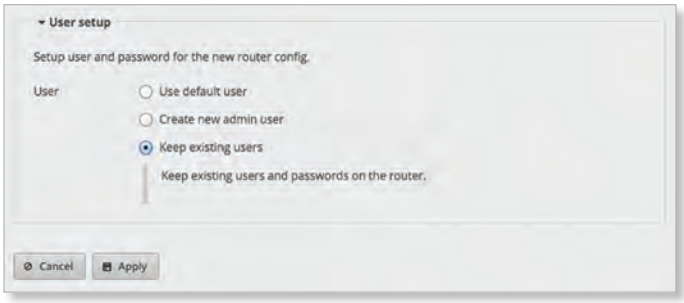
- **Use default user** Replace the default user, *ubnt*.
  - **User** Enter a new admin username.
  - **Password** Enter a new password.
  - **Confirm Password** Enter the new password again.



- **Create new admin user** Create a new admin user and remove the default user, *ubnt*. Complete the following:
  - **User** Enter a new admin username.
  - **Password** Enter a new password.
  - **Confirm Password** Enter the new password again.



- **Keep existing users** Keep the existing usernames and passwords on the EdgeRouter.



LAN-to-LAN Exclusion

The LAN-to-LAN exclusion feature excludes LAN-to-LAN traffic from load-balancing. Click **configure this section** to manage this feature.

The load balancing feature creates new routing tables for the WAN interfaces to use. This works well for LAN-to-WAN traffic; however, you do not want to load-balance traffic that is going from LAN to LAN. We recommend that you create a firewall/NAT group for the LAN networks and add a rule to the appropriate firewall policy, so this group uses the main routing table for LAN-to-LAN destinations. Refer to **"Firewall/NAT" on page 27** for more information.

Note: The LAN networks rule must precede the load-balance rule.

LAN-to-LAN exclusion This option excludes LAN-to-LAN traffic from load-balancing. Enabled by default.

Click **Apply** to save your changes, or click *Cancel*.

Load Balancing2 Wizard

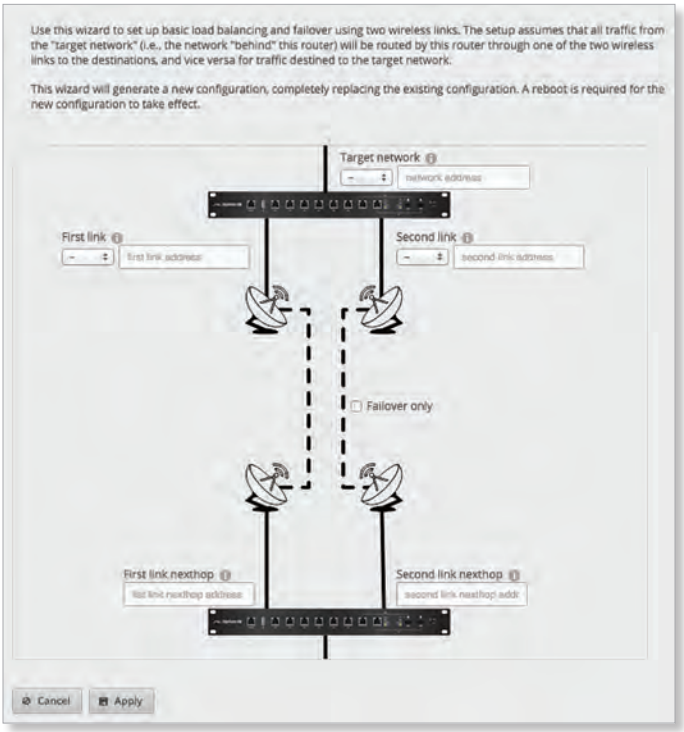
Before You Begin

Use the *Load Balancing2* setup wizard to set up basic load balancing and failover using two wireless links. The setup assumes that all traffic from the target network (the network behind the EdgeRouter) will be routed by the EdgeRouter through one of the two wireless links to the destinations, and vice versa for traffic destined for the target network.

The *Load Balancing2* setup wizard will replace the entire configuration and require a reboot when the new configuration is applied.

Overview

Click the **Load Balancing2** setup wizard to begin.



Target Network

(interface) Select the appropriate interface.

(network address) Enter the IPv4 address with subnet mask or prefix for the target network. Example: *192.0.3.1/24*

First Link

(interface) Select the appropriate interface.

(network address) Enter the IPv4 address with subnet mask or prefix for the first wireless link. Example: *192.0.1.1/24*

Second Link

(interface) Select the appropriate interface.

(network address) Enter the IPv4 address with subnet mask or prefix for the second wireless link. Example: *192.0.2.1/24*

Failover Only

(checkbox) Disabled by default. Select this option if you want to use the second link only if the first link fails.

First Link Nexthop

(next hop address) Enter the next hop IPv4 address for the first wireless link (the address on the corresponding interface of the other router). Example: *192.0.1.2*

Second Link Nexthop

(next hop address) Enter the next hop IPv4 address for the second wireless link (the address on the corresponding interface of the other router). Example: *192.0.2.2*

Click **Apply** to save your changes, or click *Cancel*.

SOHO Deployment Wizards

The setup wizard will guide you through a typical Small Office Home Office (SOHO) deployment:

- Configures the Internet connection and NAT masquerade for the Internet port
- Enables default firewall settings for the Internet port
- Enables DHCP server functionality for local networks
- Automatically enables DNS (Domain Name System) forwarding for local networks
- Automatically enables TCP MSS (Maximum Segment Size) clamping for a PPPoE (Point-to-Point over Ethernet) connection

There are two SOHO deployment setup wizards available:

- **WAN+2LAN** The *WAN+2LAN* setup wizard is the most basic version available. The WAN port is eth1. Go to the *WAN+2LAN* section below.
- **WAN+2LAN2** The *WAN+2LAN2* setup wizard allows you to bridge the LAN interfaces and/or change the subnets configured on the LAN interfaces. The WAN port is eth0. You can also configure user accounts during setup. Go to **"WAN+2LAN2 Wizard" on page 74**.

WAN+2LAN Wizard

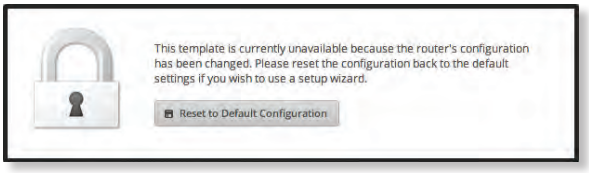
Before You Begin

If the EdgeRouter is already configured, then the *WAN+2LAN* setup wizard is not available. It is available only if the EdgeRouter uses its default configuration.

You can reset the EdgeRouter to its factory defaults using the EdgeOS Configuration Interface:

System Tab Refer to **"Reset Config to Default" on page 7** for instructions.

Wizards Tab Click the **WAN+2LAN** setup wizard in the column on the left. The following window will appear.



Click Reset to Default Configuration and then follow the on-screen instructions.

Overview

Click the **WAN+2LAN** setup wizard to begin the SOHO configuration.

Go to the *WAN+2LAN* section below unless you have the ERPoe-5, then go to **"WAN+2LAN > ERPoe-5" on page 73**.

Note: The *WAN+2LAN* setup wizard is designed to set up a basic SOHO network. For full configuration functionality, use the other tabs of the EdgeOS Configuration Interface or the Command Line Interface (CLI).

WAN+2LAN

LAN Port (eth0)

Connect *eth0* to your local network, such as a switch.

Address The IP address is displayed in the first field, and the subnet mask or prefix length is displayed in the second field.

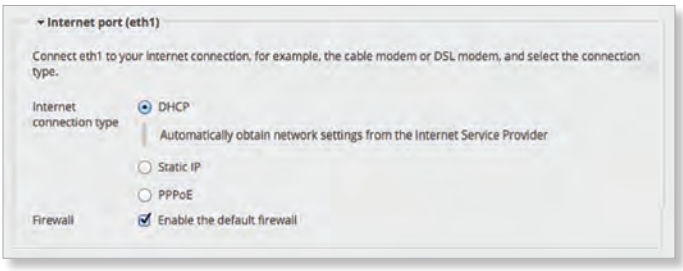
DHCP Select this checkbox to have the EdgeRouter assign IP addresses.

Internet Port (eth1)

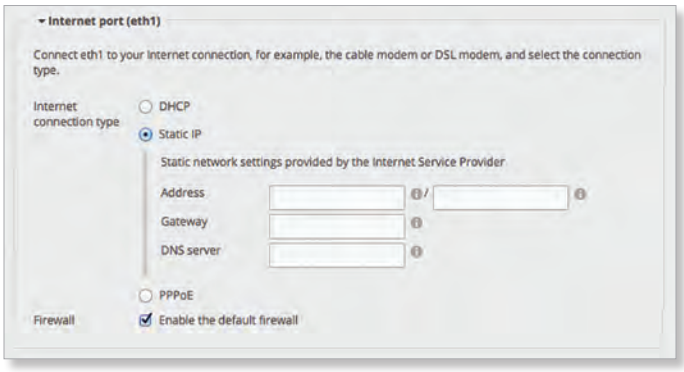
Connect *eth1* to your Internet connection.

Internet connection type Select the Internet connection type your network is using.

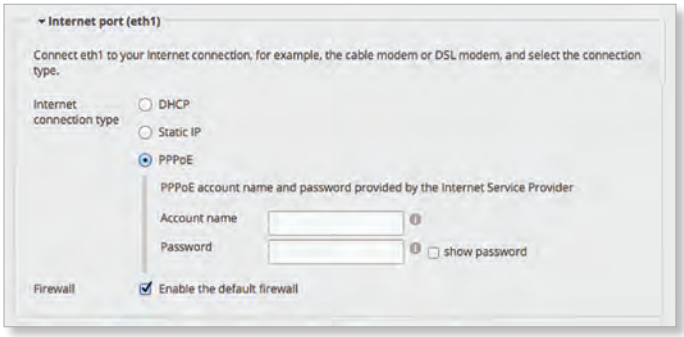
- **DHCP** Select this option if your ISP automatically assigns network settings to your network.



- **Static IP** Select this option if your ISP has assigned static network settings to your network.
  - **Address** Enter the IP address in the first field and the subnet mask or prefix length in the second field.
  - **Gateway** Enter the IP address of the ISP's gateway server, which provides the point of connection to the Internet.
  - **DNS server** Enter the IP address of the ISP's DNS server.



- **PPPoE** Select this option if your ISP uses PPPoE.
  - **Account Name** Enter the name of your PPPoE account.
  - **Password** Enter the password of your PPPoE account.
    - **show password** Select to display the password in plaintext.



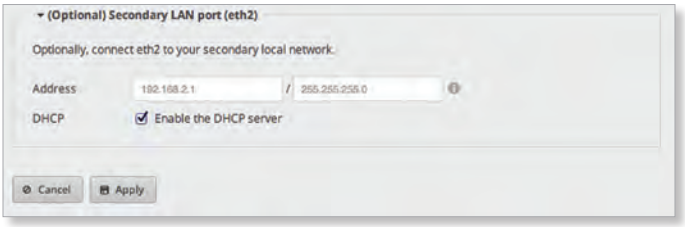
Firewall Enabled by default. This option applies the default firewall settings to the EdgeRouter; only established and related traffic types are allowed for local and inbound traffic.

(Optional) Secondary LAN Port (eth2)

Click **configure this section** if you connect *eth2* to your local network, such as a switch.

Address The IP address is displayed in the first field, and the subnet mask or prefix length is displayed in the second field.

DHCP Select this checkbox to have the EdgeRouter assign IP addresses.

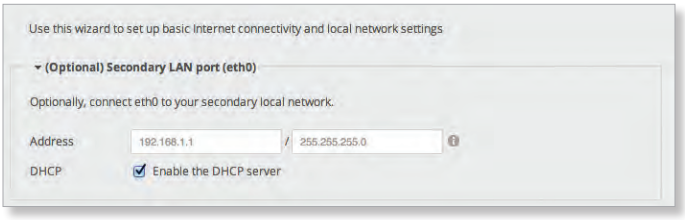


Click **Apply** to save your changes, or click *Cancel*.

WAN+2LAN > ERPoe-5

Optional Secondary LAN Port (eth0)

Click **configure this section** if you connect *eth0* to your secondary local network.



Address The IP address is displayed in the first field, and the subnet mask or prefix length is displayed in the second field.

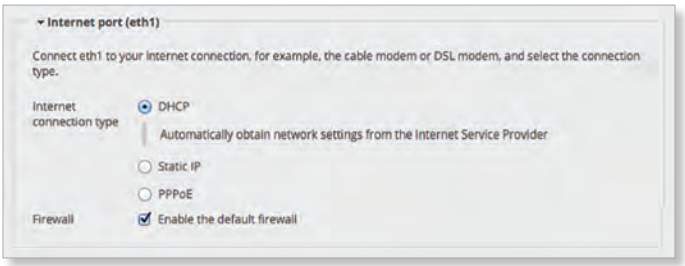
DHCP Select this checkbox to have the EdgeRouter assign IP addresses.

Internet port (eth1)

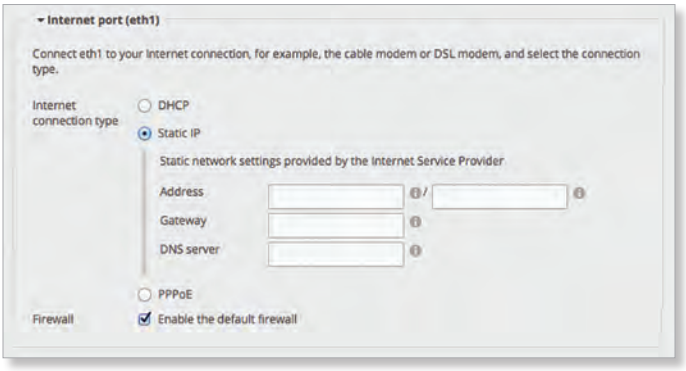
Connect *eth1* to your Internet connection.

Internet connection type Select the Internet connection type your network is using.

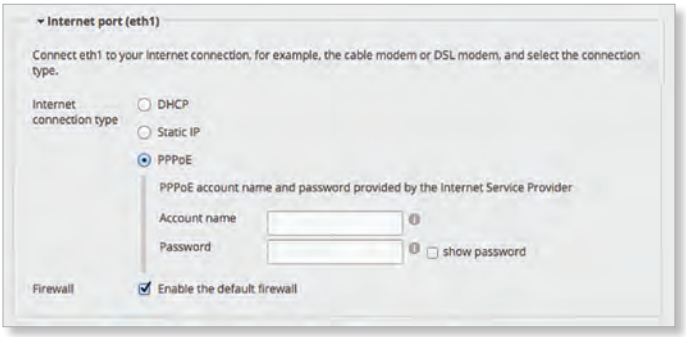
- **DHCP** Select this option if your ISP automatically assigns network settings to your network.



- **Static IP** Select this option if your ISP has assigned static network settings to your network.
  - **Address** Enter the IP address in the first field and the subnet mask or prefix length in the second field.
  - **Gateway** Enter the IP address of the ISP's gateway server, which provides the point of connection to the Internet.
  - **DNS server** Enter the IP address of the ISP's DNS server.



- **PPPoE** Select this option if your ISP uses PPPoE.
  - **Account Name** Enter the name of your PPPoE account.
  - **Password** Enter the password of your PPPoE account.
    - **show password** Select to display the password in plaintext.



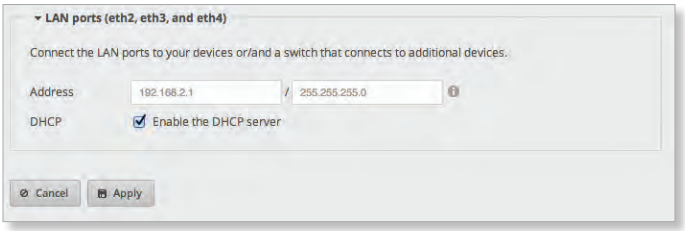
Firewall Enabled by default. This option applies the default firewall settings to the EdgeRouter; only established and related traffic types are allowed for local and inbound traffic.

LAN Ports (eth2, eth3, and eth4)

Click **configure this section** if you connect *eth2*, *eth3*, and/or *eth4* to your devices and/or a switch. (The *eth2*, *eth3*, and/or *eth4* become switch ports for a local network.)

Address The IP address is displayed in the first field, and the subnet mask or prefix length is displayed in the second field.

DHCP Select this checkbox to have the EdgeRouter assign IP addresses.



Click **Apply** to save your changes, or click *Cancel*.

WAN+2LAN2 Wizard

Before You Begin

You can still use the *WAN+2LAN* setup wizard even if the EdgeRouter is already configured. The *WAN+2LAN* setup wizard will replace the entire configuration and require a reboot when the new configuration is applied.

Overview

Click the **WAN+2LAN2** setup wizard to begin the SOHO configuration.

Go to the *WAN+2LAN2* section in the next column unless you have the ERPoe-5, then go to **"WAN+2LAN2 > ERPoe-5" on page 76**.

Note: The *WAN+2LAN2* setup wizard is designed to set up a basic SOHO network. For full configuration functionality, use the other tabs of the EdgeOS Configuration Interface or the Command Line Interface (CLI).

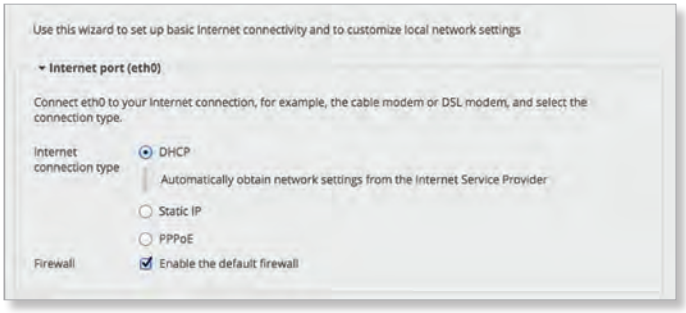
WAN+2LAN2

Internet Port (eth0)

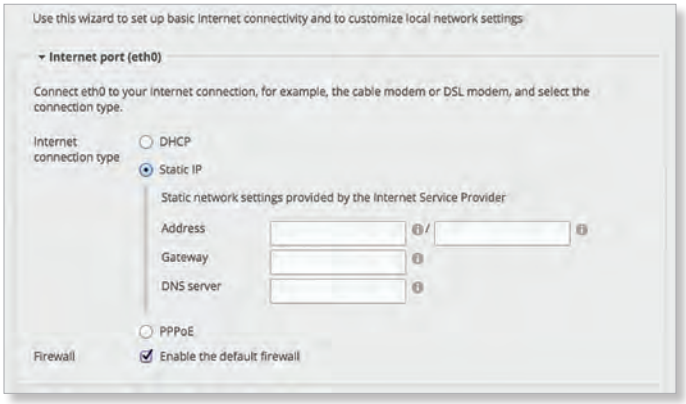
Connect *eth0* to your Internet connection.

Internet connection type Select the Internet connection type your network is using.

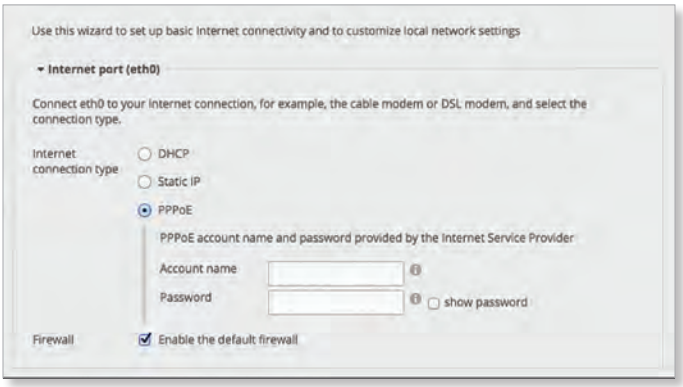
- **DHCP** Select this option if your ISP automatically assigns network settings to your network.



- **Static IP** Select this option if your ISP has assigned static network settings to your network.
  - **Address** Enter the IP address in the first field and the subnet mask or prefix length in the second field.
  - **Gateway** Enter the IP address of the ISP's gateway server, which provides the point of connection to the Internet.
  - **DNS server** Enter the IP address of the ISP's DNS server.



- **PPPoE** Select this option if your ISP uses PPPoE.
  - **Account Name** Enter the name of your PPPoE account.
  - **Password** Enter the password of your PPPoE account.

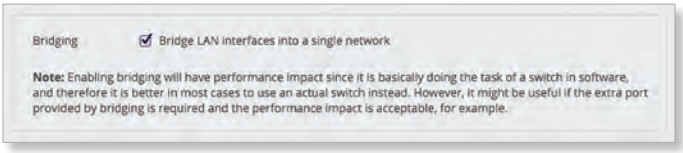


Firewall Enabled by default. This option applies the default firewall settings to the EdgeRouter; only established and related traffic types are allowed for local and inbound traffic.

Bridging

Bridging Select this option to bridge the LAN interfaces into a single network.

Bridging will decrease performance because it performs the task of a switch in software; in most cases, it is better to use a hardware switch instead. However, bridging may be useful if the extra port provided by bridging is required and the performance impact is acceptable.



You have two options:

If *Bridging* is disabled, then configure the following:

- **"LAN Port (eth1)" on page 75** section below
- **"(Optional) Secondary LAN port (eth2)" on page 75**section in the next column

If *Bridging* is enabled, then go to the **"LAN Ports (eth1 and eth2)" on page 75** section in the next column.

LAN Port (eth1)

If *Bridging* is disabled, connect *eth1* to your local network, such as a switch. Then click **configure this section**.

Address Enter the IP address in the first field, and enter the subnet mask or prefix length in the second field.

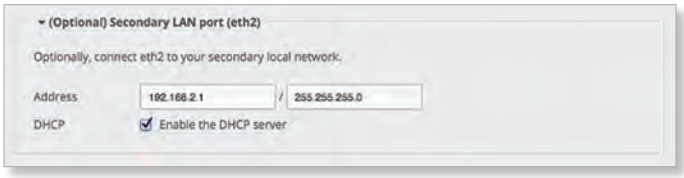
DHCP Select this checkbox to have the EdgeRouter assign IP addresses.

(Optional) Secondary LAN port (eth2)

If *Bridging* is disabled, you can connect *eth2* to your secondary local network. Then click **configure this section**.

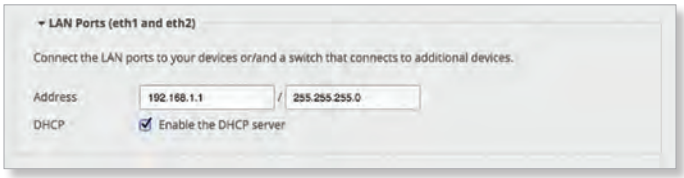
Address Enter the IP address in the first field, and enter the subnet mask or prefix length in the second field.

DHCP Select this checkbox to have the EdgeRouter assign IP addresses.



LAN Ports (eth1 and eth2)

If *Bridging* is enabled, connect the local ports to your devices and/or a switch that connects to additional devices. Then click **configure this section**.



Address Enter the IP address in the first field, and enter the subnet mask or prefix length in the second field.

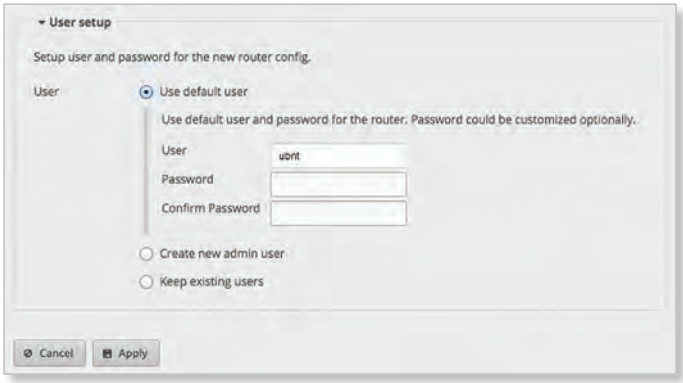
DHCP Select this checkbox to have the EdgeRouter assign IP addresses.

User Setup

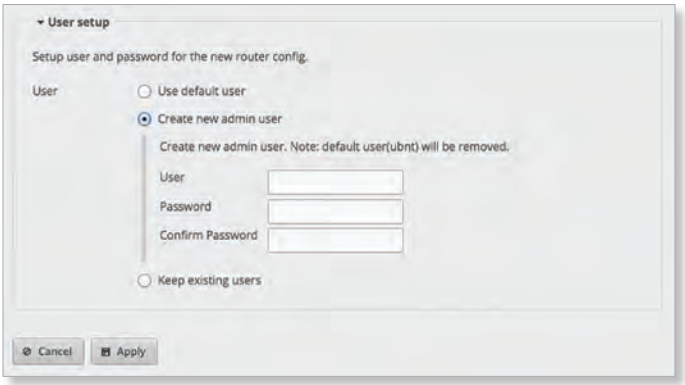
You can set up the username and password for the new EdgeRouter configuration.

User Select one of the following options:

- **Use default user** Replace the default user, *ubnt*.
  - **User** Enter a new admin username.
  - **Password** Enter a new password.
  - **Confirm Password** Enter the new password again.



- **Create new admin user** Create a new admin user and remove the default user, *ubnt*. Complete the following:
  - **User** Enter a new admin username.
  - **Password** Enter a new password.
  - **Confirm Password** Enter the new password again.



- **Keep existing users** Keep the existing usernames and passwords on the EdgeRouter.

Click **Apply** to save your changes, or click *Cancel*.

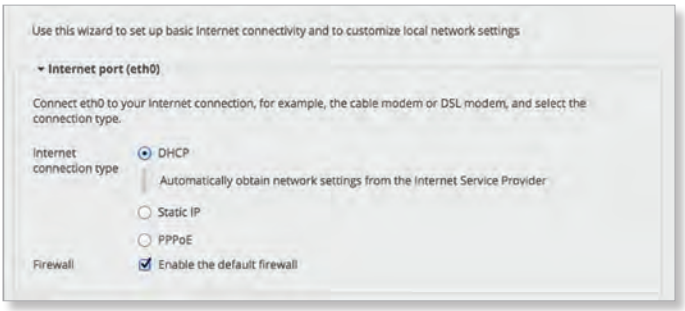
WAN+2LAN2 > ERPoe-5

Internet port (eth0)

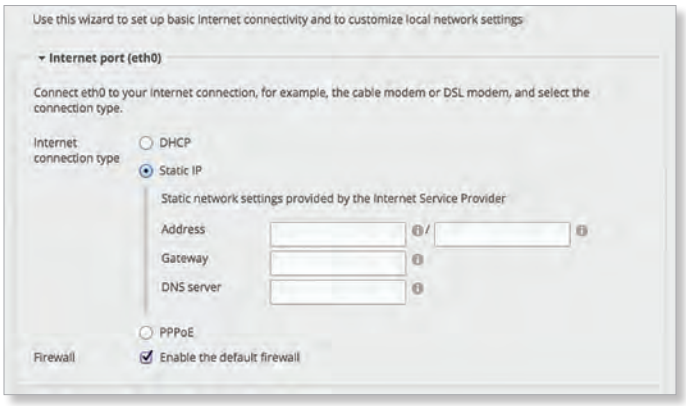
Connect *eth0* to your Internet connection.

Internet connection type Select the Internet connection type your network is using.

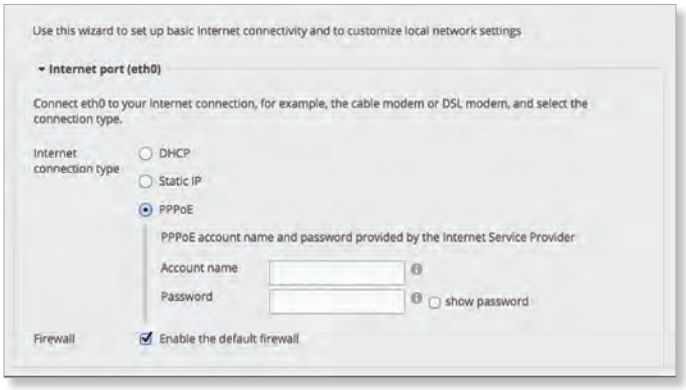
- **DHCP** Select this option if your ISP automatically assigns network settings to your network.



- **Static IP** Select this option if your ISP has assigned static network settings to your network.
  - **Address** Enter the IP address in the first field and the subnet mask or prefix length in the second field.
  - **Gateway** Enter the IP address of the ISP's gateway server, which provides the point of connection to the Internet.
  - **DNS server** Enter the IP address of the ISP's DNS server.



- **PPPoE** Select this option if your ISP uses PPPoE.
  - **Account Name** Enter the name of your PPPoE account.
  - **Password** Enter the password of your PPPoE account.

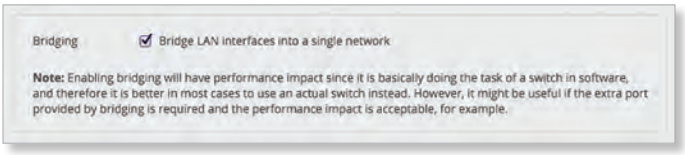


Firewall Enabled by default. This option applies the default firewall settings to the EdgeRouter; only established and related traffic types are allowed for local and inbound traffic.

Bridging

Bridging Select this option to bridge the LAN interfaces into a single network.

Bridging will decrease performance because it performs the task of a switch in software; in most cases, it is better to use a hardware switch instead. However, bridging may be useful if the extra port provided by bridging is required and the performance impact is acceptable.



You have two options:

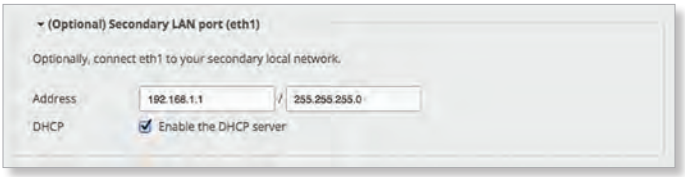
If *Bridging* is disabled, then configure the following

- **"(Optional) Secondary LAN Port (eth1)" on page 77**section below
- **"LAN Ports (eth2, eth3, and eth4)" on page 77** section below

If *Bridging* is enabled, then go to the **"LAN ports (eth1, eth2, eth3, and eth4)" on page 77** in the next column.

(Optional) Secondary LAN Port (eth1)

If *Bridging* is disabled, connect *eth1* to your local network, such as a switch. Then click **configure this section**.



Address Enter the IP address in the first field, and enter the subnet mask or prefix length in the second field.

DHCP Select this checkbox to have the EdgeRouter assign IP addresses.

LAN Ports (eth2, eth3, and eth4)

If *Bridging* is disabled, connect *eth2*, *eth3*, and/or *eth4* to your devices and/or a switch. (The *eth2*, *eth3*, and/or *eth4* become switch ports for a local network.) Then click **configure this section**.

Address Enter the IP address in the first field, and enter the subnet mask or prefix length in the second field.

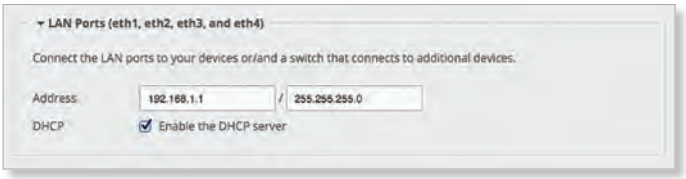
DHCP Select this checkbox to have the EdgeRouter assign IP addresses.

LAN ports (eth1, eth2, eth3, and eth4)

If *Bridging* is enabled, connect *eth1*, *eth2*, *eth3*, and/or *eth4* to your devices and/or a switch. (The *eth1*, *eth2*, *eth3*, and/or *eth4* become switch ports for a local network.) Then click **configure this section**.

Address Enter the IP address in the first field, and enter the subnet mask or prefix length in the second field.

DHCP Select this checkbox to have the EdgeRouter assign IP addresses.

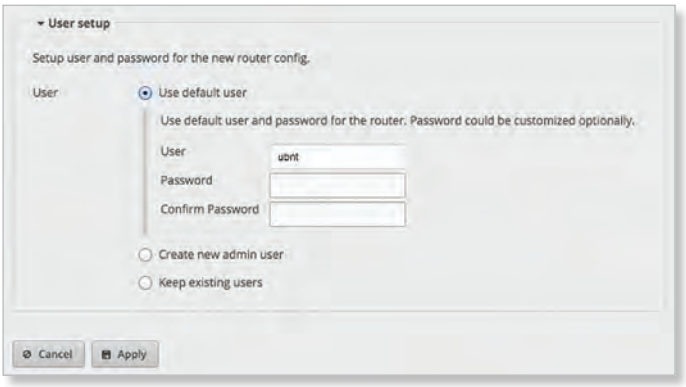


User Setup

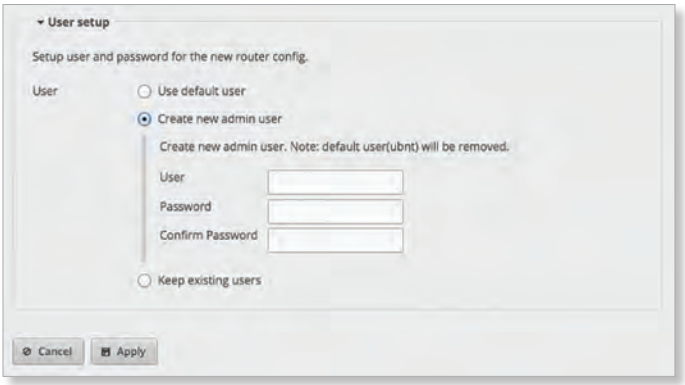
You can set up the username and password for the new EdgeRouter configuration.

User Select one of the following options:

- **Use default user** Replace the default user, *ubnt*.
  - **User** Enter a new admin username.
  - **Password** Enter a new password.
  - **Confirm Password** Enter the new password again.



- **Create new admin user** Create a new admin user and remove the default user, *ubnt*. Complete the following:
  - **User** Enter a new admin username.
  - **Password** Enter a new password.
  - **Confirm Password** Enter the new password again.



- **Keep existing users** Keep the existing usernames and passwords on the EdgeRouter.

Click **Apply** to save your changes, or click *Cancel*.

Feature Wizards

Each wizard will guide you through configuration of the corresponding feature: TCP MSS clamping or UPnP.

TCP MSS Clamping

TCP MSS (Maximum Segment Size) clamping is typically used when Path MTU Discovery is not working properly.

Using ICMP messages, Path MTU Discovery determines the highest allowable MTU (Maximum Transmission Unit) of traffic traveling between two hosts to avoid fragmentation.

TCP uses MSS, which is the MTU minus the IP and TCP headers. The sender should limit its data so it does not exceed the MSS reported by the receiver.

Sometimes security firewalls or other issues interfere with the Path MTU Discovery process (for example, ICMP messages are blocked), so you can use a workaround, TCP MSS clamping, which sets the MSS value for all TCP connections.

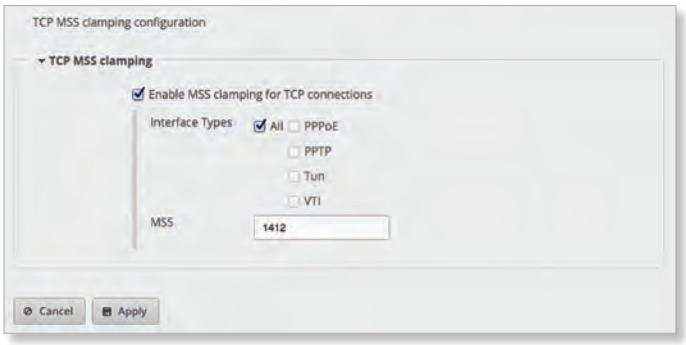
Click the **TCP MSS Clamping** feature wizard to begin configuration.

TCP MSS Clamping

Enable MSS clamping for TCP connections Select this option to specify the MSS value for TCP connections.

Interface Types Select which interface types use MSS clamping: **PPPoE**, **PPTP**, **Tun**, or **VTI**. *All* are enabled by default.

MSS Enter the MSS value to use; *1412* is the default.



Click **Apply** to save your changes, or click *Cancel*.

UPnP

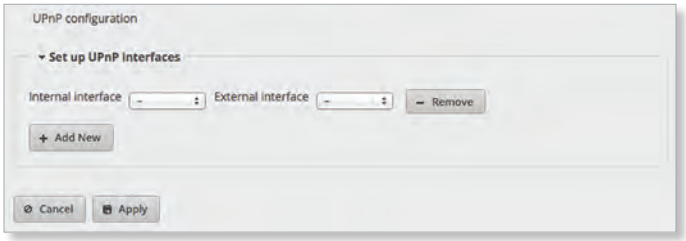
Instead of manually configuring port forwarding rules, you can use UPnP for automatic port forwarding when you have hardware that supports UPnP.

Click the **UPnP** feature wizard to begin configuration.

Set Up UPnP Interfaces

Add New Click **Add New** to create a new UPnP interface.

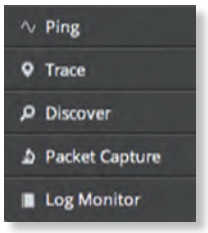
- **Internal interface** Select the appropriate LAN interface from the drop-down menu. (If you select *Other*, then enter the interface name in the field provided.)
- **External interface** Select the appropriate WAN interface from the drop-down menu. (If you select *Other*, then enter the interface name in the field provided.)
- **Remove** Click **Remove** to delete a UPnP interface.
- **Add New** Click **Add New** to create another new UPnP interface.



Click **Apply** to save your changes, or click *Cancel*.

Chapter 13: Toolbox

Each tab of the EdgeOS interface contains network administration and monitoring tools. At the top right of the screen, click the **Toolbox** Toolbox button. The *Toolbox* drop-down menu appears.



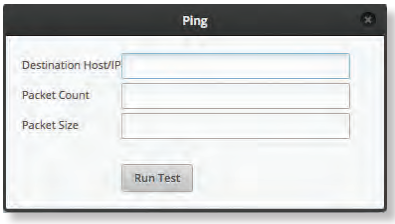
The following tools are available:

- Ping
- Bandwidth
- Trace
- Discover
- Packet Capture
- Log Monitor

Ping

You can ping other devices on the network directly from the EdgeRouter. The *Ping* tool uses ICMP packets to check the preliminary link quality and packet latency estimation between two network devices.

Click **Ping**, and the *Ping* screen appears:



Destination Host/IP Enter the IP address.

Packet Count Enter the number of packets to send for the ping test.

Packet Size Specify the size of the packet.

Run Test Click this button to start the test.

Packet loss statistics and latency time evaluation are displayed after the test is completed.

Bandwidth

You can run a speed test as the sender or receiver. To run the test between two routers, run it as a receiver on one end and sender on the other end. On the sender, enter the receiver's IP address and click **Run Test**.

Click **Bandwidth**, and the *Bandwidth* screen appears:

Sender

Receiver IP Enter the IP address.

Show advanced settings Click to display settings for advanced users.

- **Duration (s)** Enter the length of time in seconds.
- **Protocol** Select the appropriate protocol, **TCP** or **UDP**.
  - **UDP Bandwidth** If you use UDP, then this option is available. Enter the bandwidth to use.
- **Parallel flows (1-20)** If you want to increase the stress or saturate the link, enter the number of connections or streams that will run simultaneously.
- **Reverse direction** Select this option to reverse the direction of the data flow.
- **TCP window size (KBytes)** Enter the TCP window size, which is the maximum amount of data that can be sent without an acknowledgement.
- **Hide advanced settings** Click to hide settings for advanced users.

Run Test Click this button to start the test as the sender.

Bandwidth statistics are displayed after the test is completed.

Receiver

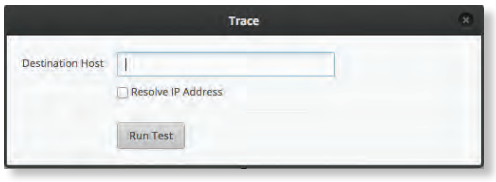
Run Test Click this button to start the test as the receiver.

The bandwidth results are displayed in Mbps after the test is completed.

Trace

The *Trace* tool traces the hops from the EdgeRouter to a specified outgoing IP address. Use this tool to find the route taken by ICMP packets across the network to the destination host.

Click **Trace**, and the *Trace* screen appears:



Destination Host Enter the IP address of the destination host.

Resolve IP Address Select this option to resolve the IP addresses symbolically (as names) instead of numerically.

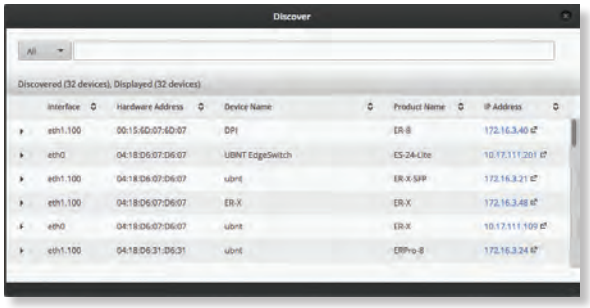
Run Test Click this button to start the test.

Responses are displayed after the test is completed.

Discover

The *Discover* tool searches for all Ubiquiti devices on your network. The *Search* field automatically filters devices containing specified names or numbers as you enter them.

Click **Discover**, and the *Discover* screen appears:



All/eth_ Select which interface to search, or select **All**.

The tool reports the number of *Discovered* and *Displayed* Ubiquiti devices. A table displays the following information about each Ubiquiti device. Click a column heading to sort by that heading.

Interface The EdgeRouter interface used by the device is displayed.

Hardware Address The MAC address of the device is displayed.

Device Name The name assigned to the device is displayed.

Product Name The Ubiquiti name of the device is displayed.

IP Address The IP address of the device is displayed. You can click it to access the device's configuration through its web management interface.

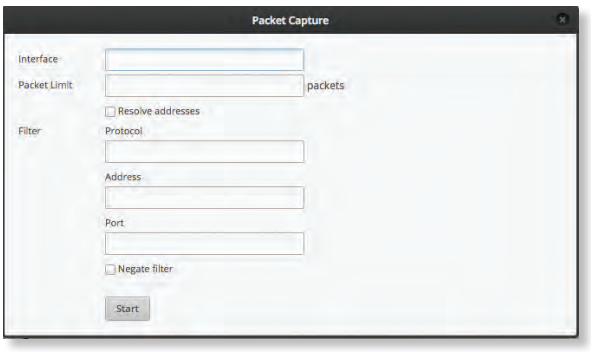
For more information, click the ▸ arrow to view the following:

- **Firmware Version** The version number of the device's firmware is displayed.
- **Uptime** The duration of the device's activity is displayed.
- **Addresses** The addresses of the device's interface are displayed. If the device has more than one interface, addresses for each interface are displayed.
  - **hwaddr** The MAC address of the device's interface is displayed.
  - **ipv4** The IP address of the device's interface is displayed.

Packet Capture

Capture packets traveling through the specified interface for analysis. You can set up filters to capture the specific types of packets you are seeking.

Click **Packet Capture**, and the *Packet Capture* screen appears:



Interface Enter the name of the interface.

Packet Limit Enter the number of packets to capture. The maximum number is 150.

Resolve addresses Select this option to resolve the IP addresses symbolically (as names) instead of numerically.

Filter

- **Protocol** Enter the protocol to filter.
- **Address** Enter the address to filter.
- **Port** Enter the port number to filter.
- **Negate filter** Check this box to capture all packets except for the ones matching the selected filter(s).

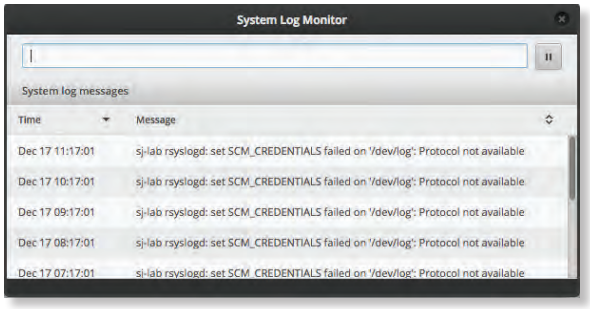
Start Click this button to start the capture. (If a *Packet Limit* is not specified, then this button becomes a *Stop* button during the capture.)

Capture results are displayed with *Time* and *Packet* descriptions.

Log Monitor

The *Log Monitor* is a log displaying live updates.

Click **Log Monitor**, and the *System Log Monitor* screen appears:



Click the *pause* button to stop the live updates. Click the *play* button to resume the live updates.

The *System log messages* table displays the following information about each log. Click a column heading to sort by that heading.

Time The system time is displayed next to every log entry that registers a system event.

Message A description of the system event is displayed.

Appendix A: Command Line Interface

Overview

The Command Line Interface (CLI) is available if you need to configure and monitor advanced features on the EdgeRouter or prefer configuration by command line. The CLI provides direct access to standard Linux tools and shell commands. This chapter explains how to access the CLI and describes a basic set of frequently used commands. Additional information is available on our website at: **community.ubnt.com/edgemax**

Access the CLI

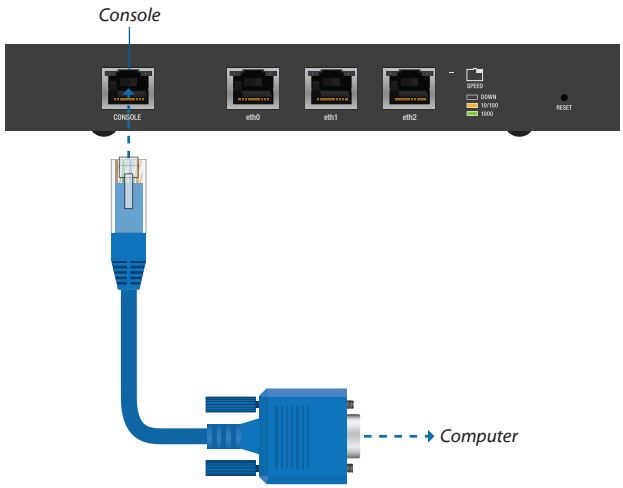
There are four methods you can use to access the CLI:

- **terminal emulator** Go to the following section, *Connect to the Console Port*.
- **SSH** If you are using the console port, go to the following section, *Connect to the Console Port*; otherwise, go to **"Access Using SSH" on page 84**.
- **Telnet** If you are using the console port, go to the following section, *Connect to the Console Port*; otherwise, go to **"Access Using Telnet" on page 84**.
- **EdgeOS Configuration Interface** Go to the *Access Using a Terminal Emulator* section in the next column.

Connect to the Console Port

Instructions may vary slightly, depending on your specific terminal emulator.

1. Use a RJ45-to-DB9, serial console cable, also known as a rollover cable, to connect the *Console* port of the EdgeRouter to your computer. (If your computer does not have a DB9 port, then you will also need a DB9 adapter.)

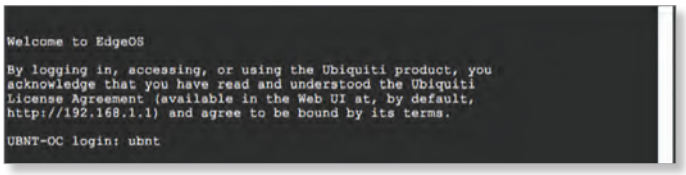


2. Follow the appropriate set of instructions:
   - **terminal emulator** Go to the following section, *Access Using a Terminal Emulator*.
   - **SSH** Go to **"Access Using SSH" on page 84**.
   - **Telnet** Go to **"Access Using Telnet" on page 84**.

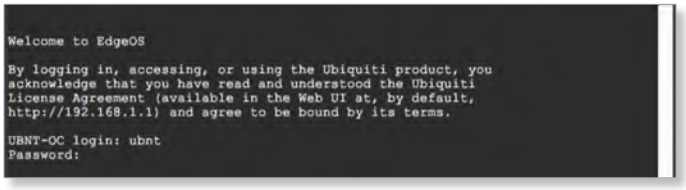
Access Using a Terminal Emulator

Instructions may vary slightly, depending on your specific terminal emulator.

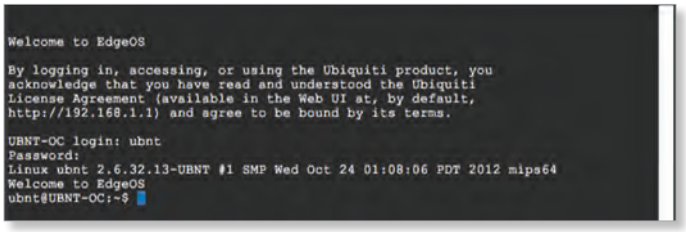
1. Open the terminal emulator on your computer, and configure it with the following serial port settings:
   - **Baud rate** 115200
   - **Data bits** 8
   - **Parity** NONE
   - **Stop bits** 1
   - **Flow control** NONE
2. Select **Serial** as the connection type.
3. Click **Open** to connect to the EdgeRouter.
4. At the *ubnt login* prompt, enter the username (the default is *ubnt*).



5. At the *Password* prompt, enter the password (the default is *ubnt*).



6. For help with commands, you can either press the **?** key or enter **show** and press the **?** key.



Note: To enhance security, we recommend that you change the default login using one of the following:

- Set up a new user account (preferred option). For details, go to **"Remove the Default User Account" on page 86**.
- Change the default password of the *ubnt* login. Use the *set* command as detailed in **"Remove the Default User Account" on page 86**.

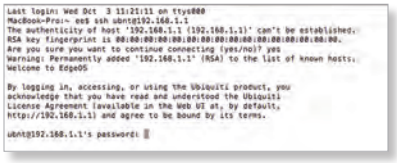
Access Using SSH

SSH is enabled by default.

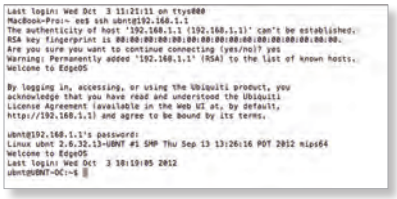
1. Open the SSH client on your computer.
2. At the *login* prompt, enter:
   ssh <*username*>**@**<*hostname*>
   The defaults are *ubnt* for the username and *192.168.1.1* for the hostname. You can also enter a domain name instead of an IP address for the hostname.

Note: Upon initial login, a host key will be displayed. You will be asked to confirm that you want to save the host key to the local database. Click **Yes** to bypass this message in the future.

At the *Password* prompt, enter the password (the default is *ubnt*).



3. For help with commands, you can either press the **?** key or enter **show** and press the **?** key.



Note: To enhance security, we recommend that you change the default login using at least one of the following options:

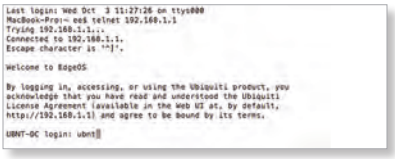
- Set up a new user account (preferred option). For details, go to **"Remove the Default User Account" on page 86**.
- Change the default password of the *ubnt* login. Use the *set* command as detailed in **"Remove the Default User Account" on page 86**.

Access Using Telnet

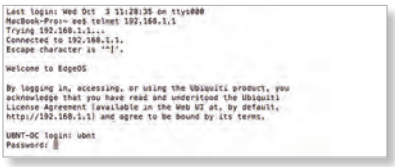
Telnet is disabled by default. To use Telnet, enable it on the *System* tab (see **"Telnet Server" on page 6**).

1. Open the telnet client on your computer.
2. At the prompt, enter:
   telnet <*hostname*>
   The default is *192.168.1.1* for the hostname. You can also enter a domain name instead of an IP address for the hostname.

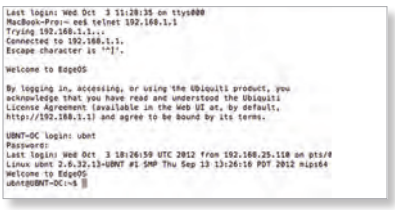
3. At the *login* prompt, enter the username (the default is *ubnt*).



4. At the *Password* prompt, enter the password (the default is *ubnt*).



5. For help with commands, you can either press the **?** key or enter **show** and press the **?** key.



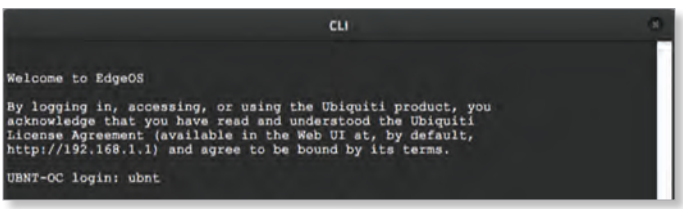
Note: To enhance security, we recommend that you change the default login using at least one of the following options:

- Set up a new user account (preferred option). For details, go to **"Remove the Default User Account" on page 86**.
- Change the default password of the *ubnt* login. Use the *set* command as detailed in **"Remove the Default User Account" on page 86**.

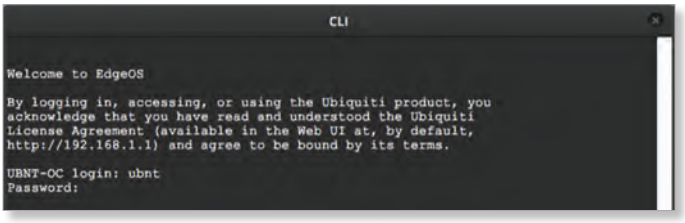
Access Using the EdgeOS Configuration Interface

Each tab of the EdgeOS interface contains CLI access.

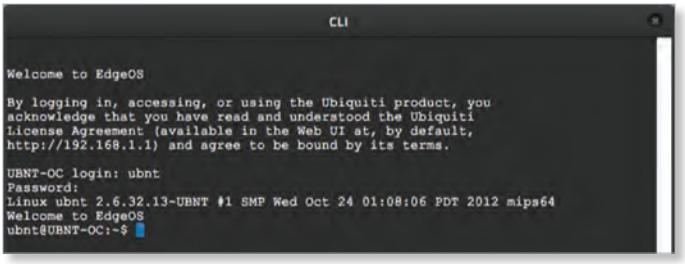
1. At the top right of the screen, click the CLI.
2. The *CLI* window appears. At the *login* prompt, enter the username (the default is *ubnt*).



3. At the *Password* prompt, enter the password (the default is *ubnt*).



4. For help with commands, you can either press the **?** key or enter **show** and press the **?** key.



Note: To enhance security, we recommend that you change the default login using at least one of the following options:

- Set up a new user account (preferred option). For details, go to **"Remove the Default User Account" on page 86**.
- Change the default password of the *ubnt* login. Use the *set* command as detailed in **"Remove the Default User Account" on page 86**.

CLI Modes

Operational Mode

When you first log in, the CLI is in operational mode. Press the **?** key to view the available commands.

```
ubnt@ubnt:~$
```

Note: The question mark does not display on-screen.

```
add          delete          ping6     reset      terminal
clear        disconnect      reboot    restart    traceroute
configure    generate        release   set        traceroute6
connect      initial-setup   remove    show       undebug
copy         no              rename    shutdown
debug        ping            renew     telnet
```

Enter **show** and press the **?** key to view the settings that you have configured.

```
ubnt@ubnt:~$ show
```

```
arp             flow-accounting  nat           tech-support
bridge          hardware         ntp           ubnt
configuration   history          openvpn       users
date            host             pppoe-server  version
debugging       incoming         queueing      vpn
dhcp            interfaces       reboot        vrrp
dhcpv6          ip               route-map     webproxy
disk            ipv6             shutdown      zebra
dns             lldp             snmp
file            log              system
firewall        login            table
```

For example, type **show interfaces** to display the interfaces and their status information.

```
ubnt@ubnt:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down,
A - Admin Down
```

```
Interface      IP Address          S/L      Description
---------      ----------          ---      -----------
eth0           -                   u/u
eth1           -                   u/D
eth2           -                   u/D
lo             127.0.0.1/8         u/u
```

To properly shut down the EdgeRouter, use the **shutdown** command.

```
ubnt@ubnt:~$ shutdown
```

WARNING: Use the **shutdown** command to properly shut down the EdgeRouter. An improper shutdown, such as disconnecting the EdgeRouter from its power supply, runs the risk of data corruption!

Configuration Mode

To switch to configuration mode, use the **configure** command.

```
ubnt@ubnt:~$ configure
[edit]
ubnt@ubnt#
```

For the *show*, *set*, and *delete* commands, you can press the **?** key for help.

- **set ?** View the available commands.
- **show ?** View the settings that you have configured. (Because configurations vary, the list you see will differ from the sample list displayed below.)
- **delete ?** View the settings that you can delete.

Enter **show** and press the **?** key.

```
ubnt@ubnt# show
```

```
firewall    interfaces    protocol    service    system
[edit]
```

To display the available command completions, press the **tab** key.

Note: The tab does not display on-screen.

```
ubnt@ubnt# show
Possible completions:
```

```
firewall                Firewall
interfaces              Network interfaces
protocols               Routing protocol parameters
service                 Services
system                  System parameters
```

The EdgeRouter uses three configurations:

- **Working** When you make changes to the working configuration, they are not applied until you commit the changes to the active configuration.
- **Active** When you commit changes to the active configuration, they are applied; however, the changes do not become part of the boot configuration until you save the changes to the boot configuration.
- **Boot** When the EdgeRouter reboots, it loads the boot configuration for use.

The following scenarios cover some of the most commonly used commands:

- *Configure an Interface* (below)
- *Remove the Default User Account* (in the next column
- **"Create a Firewall Rule" on page 87**
- **"Manage the Configuration File" on page 89**

Configure an Interface

To configure an interface, do the following:

- Assign an IP address and subnet mask
- Enter a description

Use the **set**, **compare**, **commit**, and **save** commands.

To configure an interface, use the **set** command.

```
ubnt@ubnt:~$ configure
[edit]
```

To view the possible completions for the eth0 address, enter **set interfaces ethernet eth0 address** and press the **?** key.

```
ubnt@ubnt# set interfaces ethernet eth0 address
Possible completions:

<x.x.x.x/x>          IP address and prefix length
<h:h:h:h:h:h:h:h/x>  IPv6 address and prefix length
dhcp                 Dynamic Host Configuration Protocol
dhcpv6               Dynamic Host Configuration Protocol
                     for IPv6
[edit]
ubnt@ubnt# set interfaces ethernet eth0 address
10.1.1.80/23
[edit]
ubnt@ubnt# set interfaces ethernet eth0 description
"production LAN"
```

These changes affect the working configuration, not the active configuration. To see what changes have been made to the working configuration, use the **compare** command:

```
ubnt@ubnt# compare
[edit interfaces ethernet eth0]
+address 10.1.1.2/24
+description "production LAN"
[edit]
```

To make the changes active, use the **commit** command:

```
ubnt@ubnt# commit
[edit]
```

If you reboot the EdgeRouter, the changes will be lost. To save these changes, use the **save** command to save the active configuration to the boot configuration.

```
ubnt@ubnt# save
Saving configuration to '/config/config.boot'...
Done
[edit]
ubnt@ubnt# exit
exit
ubnt@ubnt:~$
ubnt@ubnt:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down,
A - Admin Down

Interface     IP Address           S/L    Description
---------     ----------           ---    -----------
eth0          10.1.1.80/23         u/u    production LAN
eth1          -                    u/D
eth2          -                    u/D
lo            127.0.0.1/8          u/u
              ::1/128
ubnt@ubnt:$ ping 10.1.0.1
PING 10.1.0.1 (10.1.0.1) 56(84) bytes of data.
64 bytes from 10.1.0.1: icmp_req=1 ttl=64 time=0.460 ms
64 bytes from 10.1.0.1: icmp_req=2 ttl=64 time=0.407 ms
^C
--- 10.1.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time
999 ms
rtt min/avg/max/mdev = 0.407/0.433/0.460/0.033 ms
```

Remove the Default User Account

To remove the default user account, do the following:

- Create a new user
- Log out of the default user account
- Log in with the new user account
- Delete the default user account

Use the **set**, **commit**, **save**, **exit**, and **delete** commands.

```
ubnt@ubnt:~$ configure
[edit]
ubnt@ubnt:# set system login user admin1 authentication
plaintext-password admin1pass
[edit]
ubnt@ubnt:# commit
[edit]
ubnt@ubnt:# save
Saving configuration to '/config/config.boot'...
Done
[edit]
ubnt@ubnt:# exit
exit
ubnt@ubnt:~$ exit
logout
```

```
Welcome to Edge OS ubnt ttyS0

ubnt login: admin1
Password:
Linux ubnt 2.6.32.13-UBNT #1 SMP Fri Jun 8 09:48:31 PDT
2012 mips64
Welcome to EdgeOS
admin1@ubnt:~$ configure
[edit]
admin1@ubnt# delete system login user ubnt
[edit]
admin1@ubnt# commit
[edit]
admin1@ubnt# save
Saving configuration to '/config/config.boot'...
Done
[edit]
admin@ubnt# exit
exit
admin1@ubnt:~$
```

The plaintext password that you entered is converted to an encrypted password.

```
admin1@ubnt:~$ configure
[edit]
admin1@ubnt# show system login
user admin1 {
        authentication {
                encrypted-password
                $1$mv8ERQ1T$7xq/eUDwy/5And7nV.9r6.
                plaintext-password
                ""
        }
}
[edit]
admin1@ubnt# exit
exit
admin1@ubnt:~$
```

Create a Firewall Rule

To create a firewall rule, use the **set** or **edit** commands (both methods are described below). In addition, use the **compare**, **discard**, **up**, **top**, **copy**, and **rename** commands.

Create a firewall rule using the full syntax:

```
ubnt@ubnt:~$ configure
[edit]
ubnt@ubnt# set firewall name TEST default-action drop
[edit]
ubnt@ubnt# set firewall name TEST enable-default-log
[edit]
ubnt@ubnt# set firewall name TEST rule 10 description
"allow icmp"
[edit]
ubnt@ubnt# set firewall name TEST rule 10 action accept
[edit]
ubnt@ubnt# set firewall name TEST rule 10 protocol icmp
[edit]
```

To display uncommitted changes, use the **compare** command:

```
ubnt@ubnt# compare
[edit firewall]
+name TEST {
+       default-action drop
+       enable-default-log
+       rule 10 {
+               action accept
+               description "allow icmp"
+               protocol icmp
+       }
+}
[edit]
```

To undo uncommitted changes, use the **discard** command:

```
ubnt@ubnt# discard
Changes have been discarded
[edit]
ubnt@ubnt# compare
No changes between working and active configurations
[edit]
```

To create the same firewall rule while reducing the amount of repetition in the full syntax, use the **edit** command:

```
ubnt@ubnt# edit firewall name TEST
[edit firewall name TEST]
ubnt@ubnt#set default-action drop
[edit firewall name TEST]
ubnt@ubnt# set enable-default-log
[edit firewall name TEST]
ubnt@ubnt#edit rule 10
[edit firewall name TEST rule 10]
```

Press the **?** or **tab** key to display options for the specified edit level.

```
ubnt@ubnt# set

action        disable    ipsec   p2p        source   time
description   fragment   limit   protocol   state
destination   icmp       log     recent     tcp
[edit firewall name TEST rule 10]
ubnt@ubnt# set description "allow icmp"
[edit firewall name TEST rule 10]
ubnt@ubnt# set action accept
[edit firewall name TEST rule 10]
ubnt@ubnt# set protocol icmp
[edit firewall name TEST rule 10]
```

To show changes within the edit level, use the **compare** command:

```
ubnt@ubnt# compare
[edit firewall name TEST rule 10]
+action accept
+description "allow icmp"
+protocol icmp
[edit firewall name TEST rule 10]
```

To move up an edit level, use the **up** command:

```
ubnt@ubnt#up
[edit firewall name TEST]
ubnt@ubnt# compare
[edit firewall name TEST]
+default-action drop
+enable-default-log
+rule 10 {
+       action accept
+       description “allow icmp”
+       protocol icmp
+}
[edit firewall name TEST]
ubnt@ubnt# up
[edit firewall]
ubnt@ubnt# compare
[edit firewall]
+name TEST {
+       default-action drop
+       enable-default-log
+       rule 10 {
+               action accept
+               description “allow icmp”
+               protocol icmp
+       }
+}
[edit firewall]
```

To return to the top edit level, use the **top** command:

```
ubnt@ubnt# top
[edit]
ubnt@ubnt# compare
[edit firewall]
+name TEST{
+       default-action drop
+       enable-default-log
+       rule 10 {
+               action accept
+               description “allow icmp”
+               protocol icmp
+       }
+}
[edit]
```

To display the existing firewall rule, use the **show firewall** command:

```
ubnt@ubnt# show firewall
name WAN1_LOCAL {
        default-action drop
        rule 10 {
                action accept
                state {
                        established enable
                        related enable
                }
        }
        rule 20 {
                action drop
                state {
                        invalid enable
                }
        }
        rule 30 {
                action accept
                destination {
                        port 22
                }
                protocol tcp
        }
}
[edit]
```

To create a new firewall rule from an existing firewall rule, use the **copy** command.

```
ubnt@ubnt# edit firewall
[edit firewall]
ubnt@ubnt# copy name WAN1_LOCAL to name WAN2_LOCAL
[edit firewall]
ubnt@ubnt# commit
[edit firewall]
ubnt@ubnt#top
[edit]
ubnt@ubnt#show firewall
name WAN1_LOCAL {
        default-action drop
        rule 10 {
                action accept
                state {
                        established enable
                        related enable
                }
        }
        rule 20 {
                action drop
                state {
                        invalid enable
                }
        }
        rule 30 {
                action accept
                destination {
                        port 22
                }
                protocol tcp
        }
}
name WAN2_LOCAL {
        default-action drop
        rule 10 {
                action accept
                state {
                        established enable
                        related enable
                }
        }
        rule 20 {
                action drop
                state {
                        invalid enable
                }
        }
```

```
        rule 30 {
                action accept
                destination {
                        port 22
                }
                protocol tcp
        }
}
[edit]
```

To change the name of the new firewall rule, use the **rename** command.

```
ubnt@ubnt# edit firewall
[edit firewall]
ubnt@ubnt# rename name W[TAB]
WAN1_LOCAL      WAN2_LOCAL
[edit firewall]
ubnt@ubnt# rename name WAN2_LOCAL to name WAN2_IN
[edit firewall]
ubnt@ubnt# commit
[edit firewall]
ubnt@ubnt#top
[edit]
ubnt@ubnt# show firewall name
name WAN1_LOCAL {
        default-action drop
        rule 10 {
                action accept
                state {
                        established enable
                        related enable
                }
        }
        rule 20 {
                action drop
                state {
                        invalid enable
                }
        }
        rule 30 {
                action accept
                destination {
                        port 22
                }
                protocol tcp
        }
}
name WAN2_IN {
        default-action drop
        rule 10 {
                action accept
                state {
                        established enable
                        related enable
                }
        }
        rule 20 {
                action drop
                state {
                        invalid enable
                }
        }
        rule 30 {
                action accept
                destination {
                        port 22
                }
                protocol tcp
        }
}
[edit]
ubnt@ubnt#
```

Manage the Configuration File

Typically, you use the *save* command to save the active configuration to disk (*'config/config.boot'*); however, you can also save the active configuration to a different file or remote server.

Enter **save** and press the **?** key.

```
ubnt@RTR# save
Possible completions:
  <Enter>                                  Save to system
                                           config file
  <file>                                   Save to file on
                                           local machine
  scp://<user>:<passwd>@<host>/<file>      Save to file on
                                           remote machine
  ftp://<user>:<passwd>@<host>/<file>      Save to file on
                                           remote machine
  tftp://<host>/<file>                     Save to file on
                                           remote machine
[edit]
ubnt@RTR# save tftp://10.1.0.15/rtr-config.boot
Saving configuration to
'tftp://10.1.0.15rtr-config.boot'...
############################################### 100.0%
Done
[edit]
```

Scenario: In the midst of the administrator changing an IPsec tunnel into an OpenVPN tunnel, the administrator had to revert the EdgeRouter to its previous configuration with the IPsec tunnel.

1. Before making changes, the administrator saved a backup configuration file with a working IPsec tunnel configuration:

```
ubnt@RTR# save config.boot-ipsec
Saving configuration to '/config/config.boot-ipsec'...
Done
[edit]
```

Note: This is a backup; if the EdgeRouter were rebooted, it would still boot from the default file: *'/config/config.boot'*

2. After the administrator deleted the IPsec configuration and was configuring of the OpenVPN tunnel, circumstances changed so that the IPsec tunnel was required again. Consequently, the administrator reverted the EdgeRouter to its previous configuration with the IPsec tunnel.

```
ubnt@RTR# load config.boot-ipsec
Loading configuration from
'/config/config.boot-ipsec'...

Load complete. Use 'commit' to make changes active.
[edit]
ubnt@RTR# commit
[edit]
ubnt@RTR# save; exit
Saving configuration to '/config/config.boot'...
Done
exit
ubnt@RTR:~$
```

To automatically make a remote backup after every commit, use the **commit-archive** configuration option, enter **location**, and press the **?** key.

```
ubnt@RTR# set system config-management commit-archive
location
Possible completions:
<url>    Uniform Resource Identifier
Detailed information:
        "scp://<user>:<passwd>@<host>/<dir>"
        "ftp://<user>:<passwd>@<host>/<dir>"
        "tftp://<host>/<dir>"
ubnt@RTR# set system config-management commit-archive
location tftp://10.1.0.15/RTR
[edit]
ubnt@RTR# commit
Archiving config...
        tftp://10.1.0.15/RTR    OK
[edit]
```

On the remote tftp server, a copy with the hostname and date is saved for each commit.

```
admin2@server://tftpboot/RTR$ ls -l
total   8
-rw------- 1 nobody nogroup 908 Aug 17 17:19
        config.boot-RTR.20120817_171932
-rw------- 1 nobody nogroup 874 Aug 17 17:20
        config.boot-RTR.20120818_002046
```

You can also keep a specified number of revisions of the configuration file on the local disk. Use the **commit-revisions** configuration option.

```
ubnt@RTR# set system config-management commit-revisions
50
[edit]
ubnt@RTR# commit
[edit]
```

Here is an example that uses the *commit-revisions* command:

```
ubnt@RTR# set system login user joe authentication
plaintext-password secret
[edit]
ubnt@RTR# commit
[edit]
ubnt@RTR# save; exit
Saving configuration to '/config/config.boot'...
Done
exit

ubnt@RTR:~$ show system commit

0        2012-08-17 18:32:13 by ubnt via cli commit
1        2012-08-17 18:31:52 by ubnt via cli commit
2        2012-08-17 18:31:51 by root via init commit
```

Note: The following commands require that the configuration option, *commit-revisions*, be set first.

```
show system commit diff      commit-confirm
show system commit file      confirm
show system commit           rollback
commit comment
```

For details on the *commit-revisions* option, go to **"Manage the Configuration File" on page 89**.

To display the changes in revision 0, use the **show system commit diff** command.

```
ubnt@RTR:~$ show system commit diff 0
[edit system login]
+user joe       {
+       authentication {
+               encrypted-password
                $1$CWVzYggs$NyJXxC3S572rfm6pY8ZMO.
+               plaintext-password ""
+       }
+       level admin
+}
```

To display the entire configuration file for revision 0, use the **show system commit file** command.

```
ubnt@RTR:~$ show system commit file 0
```

To add a comment to the commit, use the **comment** command.

```
ubnt@RTR# set system login user joe level operator
[edit]
ubnt@RTR# commit comment "change joe from admin to op"
[edit]
ubnt@RTR# save; exit
Saving configuration to '/config/config.boot'...
Done
exit
```

Now you will see the comment when you use the **show system commit** command.

```
ubnt@RTR:~$ show system commit

0        2012-08-17 18:44:41 by ubnt via cli change joe
         from admin to op
1        2012-08-17 18:34:01 by ubnt via cli commit
2        2012-08-17 18:32:13 by ubnt via cli commit
3        2012-08-17 18:31:52 by ubnt via cli commit
4        2012-08-17 18:31:51 by root via init commit
```

When you work on a remote router, certain changes, such as a firewall or NAT rule, can cut off access to the remote router, so you then have to visit the remote router and reboot it. To avoid such issues when you make risky changes, use the **commit-confirm** command first. Then use the **confirm** command to save your changes.

```
ubnt@RTR:~$ configure
[edit]
ubnt@RTR# set firewall name WAN_IN rule 50 action drop
[edit]
ubnt@RTR# set firewall name WAN_IN rule 50 destination
address 172.16.0.0/16
[edit]
ubnt@RTR# commit-confirm
commit confirm will be automatically reboot in
10 minutes unless confirmed
Proceed? [confirm][y]
[edit]
```

After you verify that the changes should be saved, use the **confirm** command.

```
ubnt@RTR# confirm
[edit]
```

You can also specify the number of minutes to wait, but you must remember to also use the **confirm** command. Otherwise, if you forget, then you can be surprised by the EdgeRouter's reboot to its previous configuration.

```
ubnt@RTR# commit-confirm 1
commit confirm will be automatically reboot in 1 minutes
unless confirmed
Proceed? [confirm][y]
[edit]
ubnt@RTR#
Broadcast message from root@RTR (Mon Aug 20 14:00:06
2012):

The system is going down for reboot NOW!
INIT: Switching to runlevel: 6
INIT: Stopping routing services...zebra...done.
Removing all Quagga Routes.
[SNIP]
```

To roll back to an earlier commit, use the **show system commit** and **rollback** commands.

```
ubnt@RTR:~$ show system commit

0       2012-08-21 14:46:41 by admin_5 via cli
        fix bgp policy maps
1       2012-08-21 14:45:59 by admin_5 via cli
        commit
2       2012-08-21 14:45:33 by admin_5 via cli
        fix port forwarding
3       2012-08-21 14:45:15 by admin_5 via cli
        fix firewall
4       2012-08-21 14:44:29 by ubnt via cli
        commit
5       2012-08-21 14:21:15 by ubnt via cli
        add port forward for port 2222 to build-server
6       2012-08-21 14:20:24 by ubnt via cli
        add dmz interface to eth2
7       2012-08-21 14:19:53 by ubnt via cli
        add ipsec tunnel to office_exchange
8       2012-08-21 14:07:18 by ubnt via cli
        add firewall for WAN_IN
9       2012-08-21 14:06:37 by ubnt via cli
        add user first_last
10      2012-08-21 14:04:47 by ubnt via cli
        commit
11      2012-08-21 14:04:46 by root via init
        commit
```

After viewing the history of system commits, you decide to discard the last four commits by *admin_5*. Roll back the system configuration file to commit 4:

```
ubnt@RTR# rollback 4
Proceed with reboot? [confirm] [y]

Broadcast message from root@RTR (ttyS0) (Mon Aug 21
15:09:12 2012):

The system is going down for reboot NOW!
```

Appendix B: Contact Information

Ubiquiti Networks Support

Ubiquiti Support Engineers are located around the world and are dedicated to helping customers resolve software, hardware compatibility, or field issues as quickly as possible. We strive to respond to support inquiries within a 24-hour period.

Ubiquiti Networks, Inc.
2580 Orchard Parkway
San Jose, CA 95131
www.ubnt.com

Online Resources

Support: **ubnt.link/EdgeMAX-Support**

Community: **community.ubnt.com/edgemax**

Downloads: **downloads.ubnt.com/edgemax**

www.ubnt.com