

Configuring Tunnels with Generic Routing Encapsulation

Contents

Overview	12-2
Configuring GRE Tunnels	12-4
Creating GRE Tunnels	12-4
Mapping a WLAN to a GRE Tunnel	12-6
Enabling Proxy ARP for WLANs Mapped to Tunnels	12-9
Configuring IP Settings for Stations in a WLAN Mapped to a Tunnel	12-10
Ensuring That the Remote Endpoint Can Forward Traffic	12-11
Viewing GRE Tunnels and WLAN Mappings	12-12

Overview

The ProCurve Wireless Edge Services xl Module can forward all of a wireless LAN's (WLAN's) traffic to another device to be processed. To enable this feature, you must complete these steps:

1. Configure a Generic Routing Encapsulation (GRE) tunnel to that device.
2. Configure your Wireless Edge Services xl Module to forward all traffic received on a particular WLAN over that GRE tunnel.

A GRE tunnel is a virtual point-to-point connection between two devices. Traffic sent over the tunnel is encapsulated with a delivery header, and the inner layers are transparent to intervening devices (that is, not seen by them).

When you map a WLAN to a GRE tunnel interface, the Wireless Edge Services xl Module follows these steps:

1. It receives a frame from a station associated to the WLAN.
2. It removes the 802.11 header.
3. It encapsulates the IP packet with a GRE header.

Note

The Wireless Edge Services xl Module only encapsulates and forwards IP packets over the tunnel.

4. It encapsulates the GRE header with a delivery IP header:
 - The delivery header's source IP address is that for the tunnel source endpoint.
 - The delivery header's destination IP address is that for the tunnel destination endpoint.

When the Wireless Services xl Module receives a packet over the tunnel, it removes the delivery IP header and the GRE header. The module then looks up the destination IP address in the original header. If this address is valid, the module encapsulates the packet in an 802.11 header and forwards the resulting frame toward the appropriate RP, just as it would any packet destined to a WLAN.

The destination endpoint of a GRE tunnel on a Wireless Edge Services xl Module can be any ProCurve GRE-capable device such as:

- a ProCurve Secure Router 7000dl Series
- another Wireless Edge Services xl Module
- a Redundant Wireless Services xl Module

For example, you might establish a wireless network at a remote office. You want all the wireless traffic to return to the main office, so you create a GRE tunnel from the Wireless Edge Services xl Module to the router at the main office.

You could also tunnel traffic to a WAN router to protect your internal network from guests in a WLAN that is intended to provide access to the Internet only. The Wireless Edge Services xl Module receives guest traffic and readies it for transmission in the Ethernet network, as usual. However, the module then encapsulates the traffic and sends it over the tunnel to the Internet router—the guest traffic never interacts with your internal network.

Manually creating a GRE tunnel to another Wireless Edge Services xl Module is not typical, but it is supported. When you configure your module to forward traffic over a tunnel to another module, you are making the first module behave somewhat like an RP that is adopted by the second module: the second module handles the task of forwarding the traffic onto the Ethernet network. However, the first module still handles the security settings for the WLAN.

Note

Wireless Edge Services xl Modules in a Layer 3 mobility domain also tunnel traffic. However, the modules create the tunnels automatically; you should not create them manually. If you want to set up Layer 3 roaming, see *Chapter 9: Fast Layer 2 Roaming and Layer 3 Mobility*.

Configuring GRE Tunnels

This section explains how to:

- create GRE tunnels
- map WLANs to the GRE tunnels

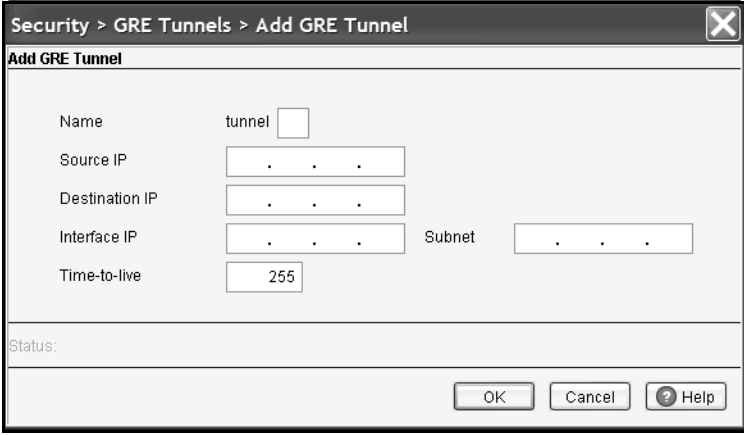
If a device such as a router will act as the remote endpoint, you should also verify that this device can receive and forward the traffic. Use the documentation included with that product to do so.

Creating GRE Tunnels

Create a GRE tunnel between your Wireless Edge Services xl Module and the device that should forward the WLAN's traffic to its destination. For example, a WLAN might provide guests with Internet access, and you might tunnel this WLAN's traffic to the WAN router that connects to the Internet.

To create a GRE tunnel, complete these steps:

1. Select **Security > GRE Tunnels**.
2. Click the **Add** button. The **Add GRE Tunnel** screen is displayed.



The screenshot shows a configuration window titled "Security > GRE Tunnels > Add GRE Tunnel". The window has a close button (X) in the top right corner. Below the title bar, the text "Add GRE Tunnel" is displayed. The main area contains several input fields: "Name" with the value "tunnel", "Source IP", "Destination IP", "Interface IP", "Subnet", and "Time-to-live" with the value "255". At the bottom left, there is a "Status:" label. At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

Figure 12-1. Add GRE Tunnel Screen

3. In the **Name** field, enter a number for the tunnel. You can enter a number from 1 through 32.

The number you enter will be appended to the word *tunnel* to form the name of the tunnel interface (such as tunnel1, tunnel2, and so on).

4. In the **Source IP** field, enter a valid IP address on this Wireless Edge Services xl Module for a virtual LAN (VLAN) tagged on the uplink port. Often, you will enter the IP address for the management VLAN.

This IP address is the source address in the delivery IP header; the remote endpoint device must be able to reach this address.

5. In the **Destination IP** field, enter the IP address of the remote end of the GRE tunnel.

This IP address is the destination address in the delivery IP header. Enter an accessible address on the remote endpoint—for example, a remote Wireless Edge Services xl Module's management IP address. If the remote endpoint is your company's router, you might enter the IP address for the router's Ethernet interface.

6. In the **Interface IP** field, assign the tunnel interface an IP address in a tunnel subnetwork.

The local Wireless Edge Services xl Module should use the same tunnel subnetwork as the remote endpoint. For example, you could set the local tunnel interface to 10.200.1.2/24 and the remote tunnel interface to 10.200.1.1/24.

7. In the **Subnet** field, enter the subnet mask for the tunnel subnetwork.
8. In the **Time-to-live** field, specify a value from 1 through 255.

This value represents the maximum number of transmissions (or hops) for a packet traversing the tunnel. You should set the time-to-live value at least one higher than the maximum number of hops between this Wireless Edge Services xl Module and the remote endpoint. Valid time-to-live values are from 1 through 255.

9. Click the **OK** button. The GRE tunnel is now listed on the **Security > GRE Tunnels** screen.

Security > GRE Tunnels

Show Filtering Options

Name	Source IP	Destination IP	Interface IP	Admin Status	Operation Status
tunnel1	10 . 4 . 1 . 30	10 . 1 . 2 . 30	10 . 200 . 1 . 2	Up	Up

Filtering is disabled

WLAN Mappings

No WLANs mapped

EditDeleteAdd

Help

Figure 12-2. Security > GRE Tunnels Screen

- Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

Mapping a WLAN to a GRE Tunnel

In a typical WLAN configuration, the Wireless Edge Services xl Module takes the following action when it receives traffic from a WLAN: it removes the 802.11 header, adds an Ethernet header, and forwards the traffic on the specified VLAN interface. When you map a WLAN to a tunnel, the module still removes the 802.11 header from traffic. Instead of simply adding an Ethernet header, however, the module adds a GRE header, a delivery IP header, and *then* the Ethernet header. Finally, the module forwards the traffic on the specified tunnel interface.

The remote endpoint then decapsulates the traffic, examines its inner IP header, and forwards the traffic toward its destination.

To allow the Wireless Edge Services xl Module to send traffic from a WLAN over a tunnel, you must map the tunnel interface that you created to the appropriate WLAN. Complete these steps:

1. Select **Network Setup > WLAN Setup > Configuration**.
2. Select the WLAN and click the **Edit** button. The **Edit** screen for that WLAN is displayed.

Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID: ☐ VLAN ID: ☐ Dynamic Assignment

Description: ☒ Tunn...: Gateway: Mask:

Authentication

☐ 802.1X EAP

☐ Web-Auth

☐ MAC Authentication

☒ No Authentication

Encryption

☐ WEP 64

☐ WEP 128

☒ WPA/WPA2-TKIP

☐ WPA2-AES

Advanced

Accounting Mode: Inter-station Traffic:

☒ Answer Broadcast ESS

☐ Use Voice Prioritization

☐ Enable SVP

☐ Closed System

Inactivity Timeout: seconds

Access Category:

MCast Addr 1:

MCast Addr 2:

Status:

Figure 12-3. WLAN Edit Screen

3. Configure the WLAN as described in *Chapter 4: Wireless Local Area Networks (WLANs)*. However, instead of mapping the WLAN to a VLAN, map the WLAN to a tunnel interface, as follows:
 - a. In the **Configuration** section, select **Tunnel**. In the accompanying field, enter the number that you previously configured for the tunnel.

- b. In the **Gateway** and **Mask** fields, specify the default gateway and subnet mask for the tunnel subnetwork.

This IP address should be the IP address of the remote endpoint *on the tunnel subnetwork*.

In Figure 12-4, for example, the tunnel interface on the local module has the IP address of 10.200.1.2/24, and the tunnel destination is 10.1.2.30. The IP address you enter for the gateway is *not* the tunnel destination, but the remote endpoint's address on the 10.200.1.0/24 network—in this case, 10.200.1.1.

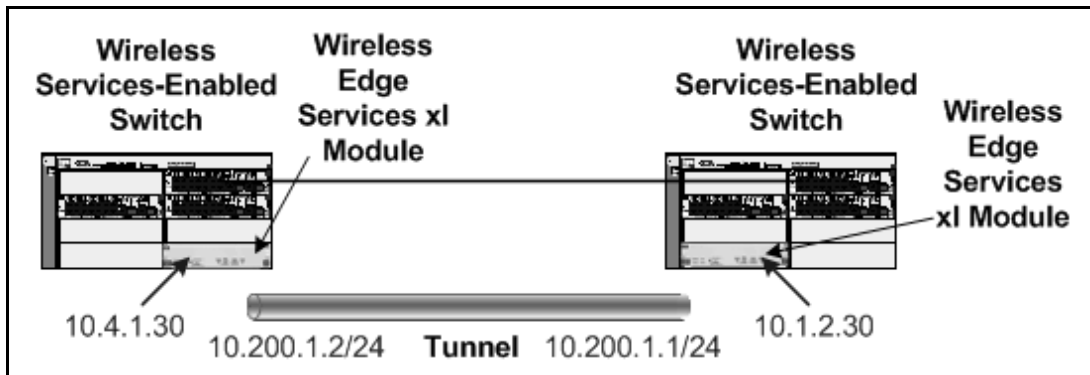


Figure 12-4. Example of a GRE Tunnel

4. Click the **OK** button. The **Network Setup > WLAN Setup > Configuration** screen shows that the WLAN is mapped to the tunnel interface.

Network Setup > WLAN Setup

Configuration
Statistics
VLAN/Tunnel Assignment
WMM

Show Filtering Options

Index	Enabled	SSID	Description	VLAN / Tunnel	Authentication	Encryption
1	✓	MyWLAN		Tunnel 1	None	TKIP
2	✓	802.1X		VLAN 1	802.1X EAP	TKIP
3	✗	SSID 3		VLAN 1	None	None
4	✗	SSID 4		VLAN 1	None	None
5	✗	SSID 5		VLAN 1	None	None
6	✗	SSID 6		VLAN 1	None	None
7	✗	SSID 7		VLAN 1	None	None
8	✗	SSID 8		VLAN 1	None	None
9	✗	SSID 9		VLAN 1	None	None
10	✗	SSID 10		VLAN 1	None	None
11	✗	SSID 11		VLAN 1	None	None
12	✗	SSID 12		VLAN 1	None	None
13	✗	SSID 13		VLAN 1	None	None
14	✗	SSID 14		VLAN 1	None	None
15	✗	SSID 15		VLAN 1	None	None
16	✗	SSID 16		VLAN 1	None	None
17	✗	SSID 17		VLAN 1	None	None
18	✗	SSID 18		VLAN 1	None	None
19	✗	SSID 19		VLAN 1	None	None
20	✗	SSID 20		VLAN 1	None	None
21	✗	SSID 21		VLAN 1	None	None
22	✗	SSID 22		VLAN 1	None	None

Filtering is disabled

Edit
Enable
Disable
Global Settings
Help

Figure 12-5. Network Setup > WLAN Setup Screen

Enabling Proxy ARP for WLANs Mapped to Tunnels

A GRE tunnel does not carry non-IP traffic such as Address Resolution Protocol (ARP). Therefore, a Wireless Edge Services xl Module that maps a WLAN to a tunnel must be able to respond to ARP requests on behalf of wireless stations.

Proxy ARP is enabled by default. If it has been disabled, complete these steps to re-enable it:

1. Select **Network Setup > WLAN Setup > Configuration**.
2. Click the **Global Settings** button. The **Global WLAN Settings** screen is displayed.



Figure 12-6. Global WLAN Settings Screen

3. Check the **Proxy ARP handling for Stations** box.
4. Click the **OK** button.
5. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

Configuring IP Settings for Stations in a WLAN Mapped to a Tunnel

Follow these guidelines to ensure that wireless stations' traffic reaches its destination:

- The stations require an IP address in the tunnel subnetwork.
- The stations' default gateway IP address should be the IP address on the destination device's tunnel interface.

Typically, wireless stations receive these settings as part of their DHCP configuration.

Ensuring That the Remote Endpoint Can Forward Traffic

A Wireless Edge Services xl Module GRE tunnel has two endpoints:

- one that receives traffic from a WLAN and forwards it over the tunnel, or (for return traffic) receives traffic over the tunnel and forwards it to the WLAN

The Wireless Edge Services xl Module plays this role.

- one that receives traffic over the tunnel and forwards it onto the destination network (a LAN or the Internet), or (for return traffic) receives traffic from the destination network and forwards it over the tunnel

Make sure that the remote endpoint knows the proper routes. Remember: it is the wireless station's default router. The remote endpoint should also implement DHCP services or DHCP relay on the tunnel interface.

Viewing GRE Tunnels and WLAN Mappings

To view GRE tunnels, select **Security > GRE Tunnels**.

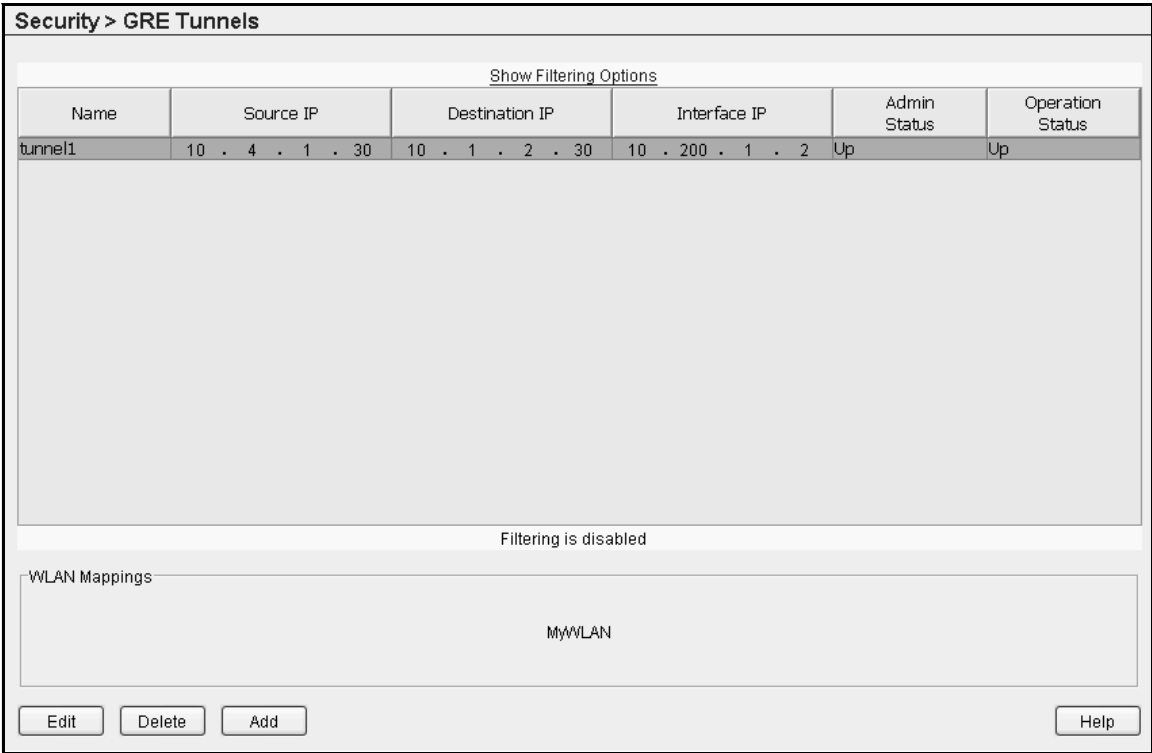


Figure 12-7. Viewing a GRE Tunnel's WLAN Mappings

When you select one of the GRE tunnels listed on the **Security > GRE Tunnels** screen, all WLANs mapped to the GRE tunnel are listed in the **WLAN Mappings** section of the screen, as shown in Figure 12-7.

You can also view tunnels' status on the **Security > GRE Tunnels** screen. The **Admin Status** column indicates whether the interface has been successfully configured on the module (**Up**). The **Operation Status** column reports whether the tunnel has been successfully established with the remote endpoint (**Up**).