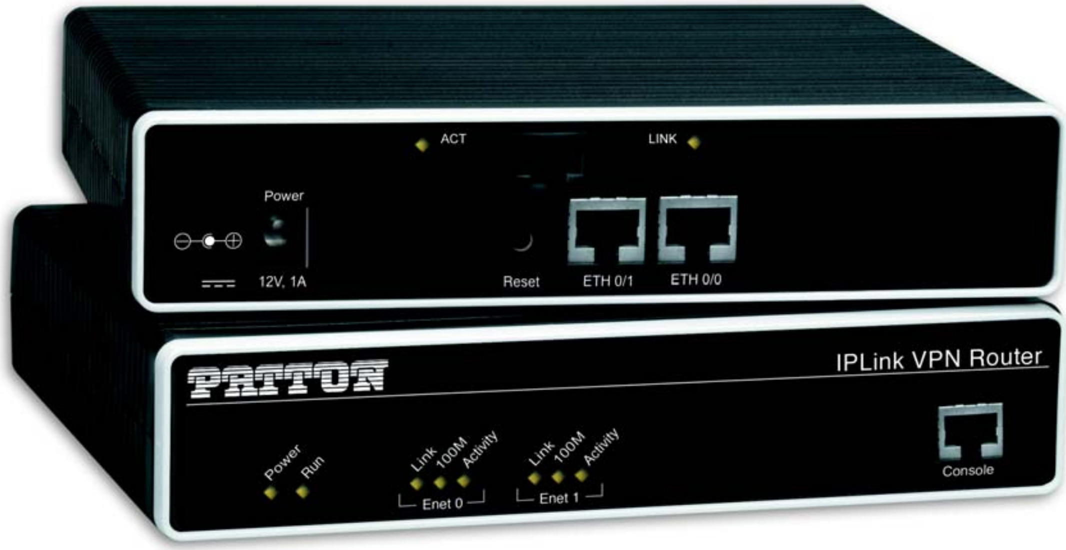
OnSite 3210 Series

G.SHDSL VPN Router

User Manual



Sales Office: **+1 (301) 975-1000**
Technical Support: **+1 (301) 975-1007**
E-mail: **support@patton.com**
WWW: **www.patton.com**

Part Number: **07M3210-GS, Rev. B**
Revised: **February 23, 2012**

Patton Electronics Company, Inc.
7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
Tel: +1 (301) 975-1000
Fax: +1 (301) 869-9293
Support: +1 (301) 975-1007
URL: www.patton.com
E-Mail: support@patton.com

Trademark Statement

The term *OnSite* is a trademark of Patton Electronics Company. All other trademarks presented in this document are the property of their respective owners.

Copyright © 2012, Patton Electronics Company. All rights reserved.

The information in this document is subject to change without notice. Patton Electronics assumes no liability for errors that may appear in this document.

Warranty Information

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

Patton Electronics warrants all OnSite router components to be free from defects, and will—at our option—repair or replace the product should it fail within one year from the first date of the shipment.

This warranty is limited to defects in workmanship or materials, and does not cover customer damage, abuse or unauthorized modification. If the product fails to perform as warranted, your sole recourse shall be repair or replacement as described above. Under no condition shall **Patton Electronics** be liable for any damages incurred by the use of this product. These damages include, but are not limited to, the following: lost profits, lost savings and incidental or consequential damages arising from the use of or inability to use this product. **Patton Electronics** specifically disclaims all other warranties, expressed or implied, and the installation or use of this product shall be deemed an acceptance of these terms by the user.

Summary Table of Contents

Table of Contents

List of Figures

List of Tables

About this guide

This guide describes OnSite VPN router hardware, installation, and configuration.

Audience

This guide is intended for the following users:

- Operators
- Installers
- Maintenance technicians

Structure

This guide contains the following chapters and appendices:

- Chapter 1 on page 16 provides information about router features, capabilities, operation, and applications
- Chapter 2 on page 23 provides hardware installation procedures
- Chapter 3 on page 31 provides quick-start procedures for configuring the OnSite VPN router
- Chapter 4 on page 37 provides information on G.SHDSL basic configuration.
- Chapter 5 on page 42 describes how to configure the VPN connections between two OnSite routers or between an OnSite and a third-party device.
- Chapter 6 on page 54 provides an overview of IP access control lists and describes the tasks involved in their configuration through the OnSite router.
- Chapter 7 on page 68 describes how to use and configure OnSite *quality of service* (QoS) features.
- Chapter 8 on page 87 provides LED definitions
- Chapter 9 on page 89 contains information on contacting Patton technical support for assistance
- Appendix A on page 92 contains compliance information
- Appendix B on page 95 contains specifications for the routers
- Appendix C on page 100 provides cable recommendations
- Appendix D on page 104 describes the router's ports and pin-outs
- Appendix E on page 107 lists the factory configuration settings for the OnSite VPN router
- Appendix F on page 109 provides license information that describes acceptable usage of the software provided with the OnSite VPN router

For best results, read the contents of this guide *before* you install the router.

Precautions

Notes, cautions, and warnings, which have the following meanings, are used throughout this guide to help you become aware of potential problems. ***Warnings*** are intended to prevent safety hazards that could result in personal injury. ***Cautions*** are intended to prevent situations that could result in property damage or impaired functioning.

Note A note presents additional information or interesting sidelights.

IMPORTANT

The alert symbol and IMPORTANT heading calls attention to important information.

CAUTION

The alert symbol and CAUTION heading indicate a potential hazard. Strictly follow the instructions to avoid property damage.

CAUTION

The shock hazard symbol and CAUTION heading indicate a potential electric shock hazard. Strictly follow the instructions to avoid property damage caused by electric shock.

WARNING

The alert symbol and WARNING heading indicate a potential safety hazard. Strictly follow the warning instructions to avoid personal injury.

WARNING

The shock hazard symbol and WARNING heading indicate a potential electric shock hazard. Strictly follow the warning instructions to avoid injury caused by electric shock.

Safety when working with electricity

WARNING

The OnSite contains no user serviceable parts. The equipment shall be returned to Patton Electronics for repairs, or repaired by qualified service personnel. Opening the OnSite case will void the warranty.

WARNING

Mains Voltage: Do not open the case the when the power cord is attached. For systems without a power switch, line voltages are present within the power supply when the power cords are connected. The mains outlet that is utilized to power the devise shall be within 10 feet (3 meters) of the device, shall be easily accessible, and protected by a circuit breaker.

WARNING

For units with an external power adapter, the adapter shall be a listed Limited Power Source.

WARNING

For AC powered units, ensure that the power cable used with this device meets all applicable standards for the country in which it is to be installed, and that it is connected to a wall outlet which has earth ground.

WARNING

Hazardous network voltages are present in WAN ports regardless of whether power to the OnSite is ON or OFF. To avoid electric shock, use caution when near WAN ports. When detaching cables, detach the end away from the OnSite first.

WARNING

Do not work on the system or connect or disconnect cables during periods of lightning activity.

WARNING

Before opening the chassis, disconnect the telephone network cables to avoid contact with telephone line voltages. When detaching the cables, detach the end away from the OnSite first.

CAUTION

The power supply automatically adjusts to accept an input voltage from 100 to 240 VAC (50/60 Hz).

Verify that the proper voltage is present before plugging the power cord into the receptacle. Failure to do so could result in equipment damage.

CAUTION

The interconnecting cables shall be acceptable for external use and shall be rated for the proper application with respect to voltage, current, anticipated temperature, flammability, and mechanical serviceability.

In accordance with the requirements of council directive 2002/96/EC on Waste of Electrical and Electronic Equipment (WEEE), ensure that at end-of-life you separate this product from other waste and scrap and deliver to the WEEE collection system in your country for recycling.

General observations

- Clean the case with a soft slightly moist anti-static cloth
- Place the unit on a flat surface and ensure free air circulation
- Avoid exposing the unit to direct sunlight and other heat sources
- Protect the unit from moisture, vapors, and corrosive liquids

Typographical conventions used in this document

This section describes the typographical conventions and terms used in this guide.

General conventions

The procedures described in this manual use the following text conventions:

Table 1. General conventions

Convention	Meaning
Garamond blue type	Indicates a cross-reference hyperlink that points to a figure, graphic, table, or section heading. Clicking on the hyperlink jumps you to the reference. When you have finished reviewing the reference, click on the **Go to Previous View** button ⬅ in the Adobe® Acrobat® Reader toolbar to return to your starting point.
Futura bold type	Commands and keywords are in **boldface** font.
Futura bold-italic type	Parts of commands, which are related to elements already named by the user, are in ***boldface italic*** font.
Italicized Futura type	Variables for which you supply values are in *italic* font
Futura type	Indicates the names of fields or windows.
Garamond bold type	Indicates the names of command buttons that execute an action.
< >	Angle brackets indicate function and keyboard keys, such as <SHIFT>, <CTRL>, <C>, and so on.
[ ]	Elements in square brackets are optional.
{a | b | c}	Alternative but required keywords are grouped in braces ({ }) and are separated by vertical bars (|)
blue screen	Information you enter is in `blue screen` font.
screen	Terminal sessions and information the system displays are in `screen font.`
node	The leading IP address or nodename of an OnSite is substituted with ***node*** in ***boldface italic*** font.
3210	The leading **3210** on a command line represents the nodename of the OnSite
#	An hash sign at the beginning of a line indicates a comment line.

Chapter 1 General information

Chapter contents

OnSite Model 3210 Series overview

The OnSite Model 3210 Series G.SHDSL VPN Router (see figure 1) is a next generation business-class G.SHDSL router that addresses both the security and the traffic prioritization needs of enterprises while providing complete broadband integration with existing DSLAM neteworks. VPN routers enable the secure communication between remote offices, home offices, and mobile users across insecure IP networks such as the Internet. The 3210 takes it one step further and integrates quality of service (QoS).

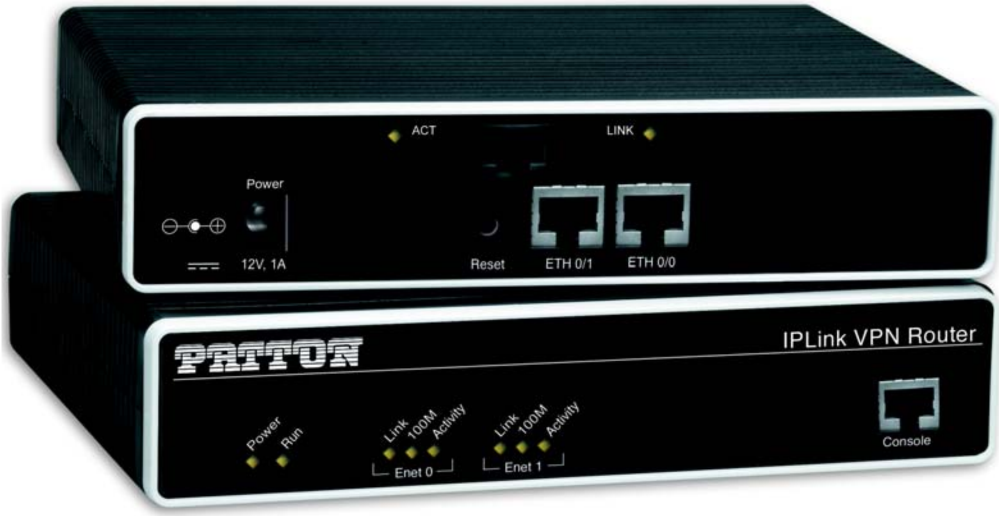


Figure 1. OnSite G.SHDSL VPN Router

The Model 3210 provides two 10/100Base-T Ethernet ports and one G.SHDSL port to deliver a managed virtual-private-network (VPN) connection over the Internet or any unsecured IP network.

The OnSite 3210 Router supports Frame-Relay and PPP networking with VPN and firewall functionality. Authentication and firewall services protect against unauthorized users while encryption, and anti-replay capabilities preserve data confidentiality. Patton's powerful CoS and QoS mechanisms provide traffic-shaping and prioritization to guarantee your mission-critical data is delivered promptly and unimpeded by traffic from other users on the same LAN. Besides assuring first priority for key information, Patton's advanced QoS technology enhances the quality and clarity of realtime application such as live voice and video communications with the main office. These compact VPN Routers support PPP/PPPoE and Frame Relay services over the serial WAN link.

The OnSite VPN Router performs the following major functions:

- Routed LAN-to-WAN connectivity between two 10/100 Ethernet LAN ports and one G.SHDSL port.
- IP Routing with class-of-service/quality-of-service (CoS/QoS) support for Internet or IP-WAN access with traffic shaping and prioritization.
- VPN tunneling for secure traversal of unsecured IP networks
- IPSec payload encryption with authentication header (AH, specified in RFC 2402) and encapsulating security payload (ESP, specified in RFC 2406) protects data integrity and confidentiality and prevents unauthorized data-replay.

- Firewall capabilities including IP-address and IP-port filtering, access control lists (ACLs), and denial-of-service (DoS) attack detection.
- Enhanced IP services include domain name service (DNS) resolver and relay, NAT/NAPT, dynamic DNS, and DHCP server.

OnSite 3210 Series detailed description

The OnSite 3210 Series G.SHDSL VPN Router provides secure managed VPN routed networking with 2-port Ethernet LAN connectivity and a G.SHDSL WAN interface (see figure 2).

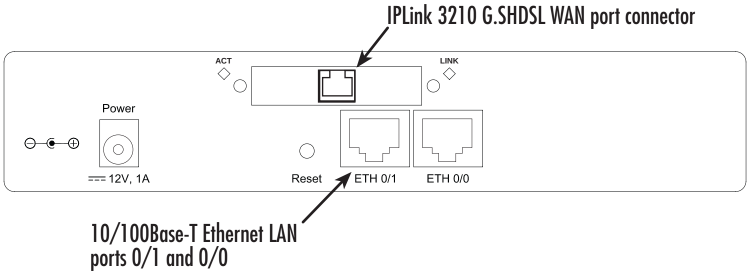

IPLink 3210 G.SHDSL WAN port connector
ACT
LINK
Power
12V, 1A
Reset
ETH 0/1
ETH 0/0
10/100Base-T Ethernet LAN ports 0/1 and 0/0

Figure 2. OnSite 3210 Series G.SHDSL connector

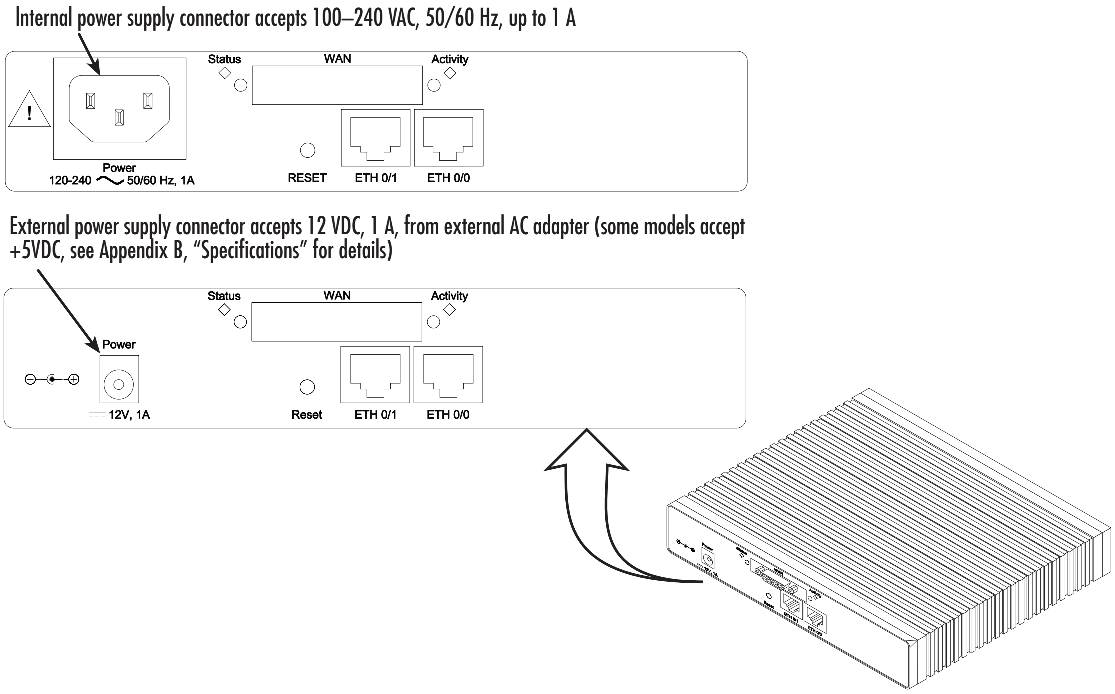

Internal power supply connector accepts 100–240 VAC, 50/60 Hz, up to 1 A
Status
WAN
Activity
!
Power
120-240 ∿ 50/60 Hz, 1A
RESET
ETH 0/1
ETH 0/0
External power supply connector accepts 12 VDC, 1 A, from external AC adapter (some models accept +5VDC, see Appendix B, “Specifications” for details)
Status
WAN
Activity
Power
12V, 1A
Reset
ETH 0/1
ETH 0/0

Figure 3. OnSite 3210 Series power input connectors

Model code extensions

A model-code extension indicates the type of power supply the Router model provides. The model-code conventions are:

- *UI* stands for internal 100–240V AC universal input power supply (see figure 3)

- *EUI* stands for external 100–240V AC universal input power supply (see figure 3)

Ports descriptions

The OnSite 3210 Series rear-panel ports are described in table 2.

Table 2. Rear panel ports

Port	Location	Description
10/100 Ethernet **ETH 0/0 (WAN) & ETH 0/1 (LAN)**	Rear panel	RJ-45 connectors (see figure 2 on page 18) that connect the router to an Ethernet device (e.g., a cable or DSL modem, LAN hub or switch).
G.SHDSL	Rear panel	Provides up to 5.7 Mbps symmetrical throughput, supporting ATM QoS. Supports multiple PVC and DSLAM interoperability. The DSL LEDs are located on either side of the DSL port. ACT (when lit or blinking) shows activity, and Link (when lit) shoes that the DSL port is connected.
Power	Rear panel	The router is available in a DC or AC power input version (see figure 3 on page 18), labeled as follows: AC version (Internal power supply): *100–240 VAC, 50/60 Hz, 1 A* DC version: +12 V, 1 A or +5 VDC 1 A
Console	Front panel	Used for service and maintenance, the *Console* port (see figure 4), an RS-232 RJ-45 connector, connects the router to a serial terminal such as a PC or ASCII terminal (also called a dumb terminal).

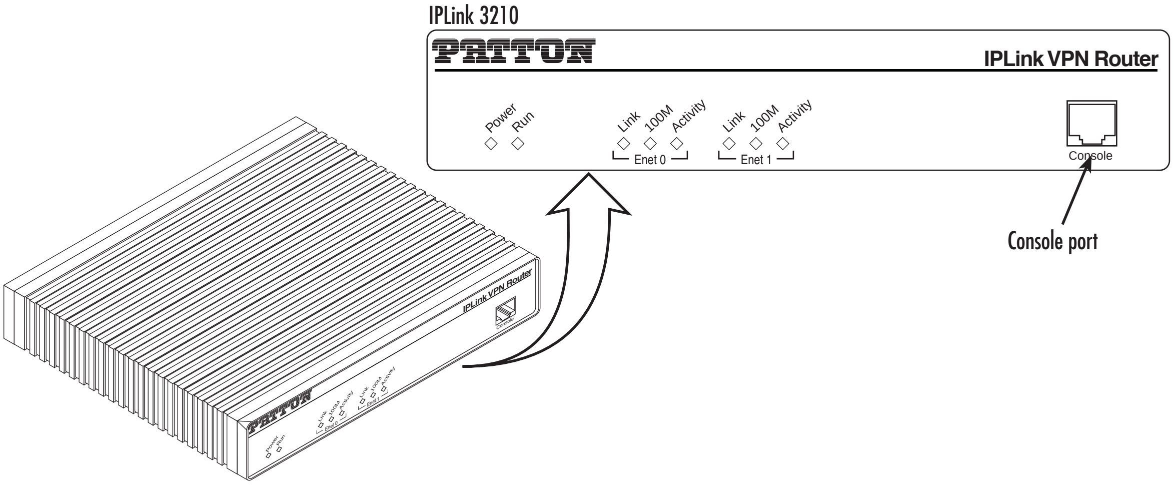


Figure 4. OnSite 3210 Series front panels

Note For LED descriptions, refer to chapter 8, "LEDs status and monitoring" on page 87.

Applications overview

Patton's OnSite managed VPN routers deliver the features you need for secure, optimized communication over non-secured IP networks. Combining VPN tunneling, standard IPSec encryption, and firewall capabilities with Patton's powerful *quality of service* technology, OnSite VPN routers deliver private, prioritized networking for business, government, and military applications.

Banking, insurance, retail, utilities, railroads, or government, any organization with more than one site can benefit from the security and traffic-shaping advantages of the OnSite family of VPN routers. As traffic traverses unsecured networks, VPN tunneling with standard IPSec encryption plus firewall capabilities preserve data security and integrity. Meanwhile, OnSite's ToS/Qos traffic-shaping and prioritization prevent critical information getting blocked or impeded by less important traffic while enhancing the quality of real-time applications such as voice and video.

OnSite 3210 Series models provide dual 10/100Base-T Ethernet ports with a G.SHDSL port. The two Ethernet ports provide full-featured IP routing plus Ethernet and IP-layer QoS services. The G.SHDSL port provides WAN access by means of a leased-line connection to the network. The following sections show some typical applications for the OnSite 3210 Series.

This chapter describes typical applications for which the OnSite 3210 Series series is uniquely suited.

Branch-Office virtual private network over Frame Relay service

Featuring VPN tunneling combined with built-in frame-relay support and a selection of standard serial interfaces on-board, the OnSite 3210 Series offers the remote-branch office a secure, private and prioritized network connection to another location over virtually any available network service and any standard WAN interface.

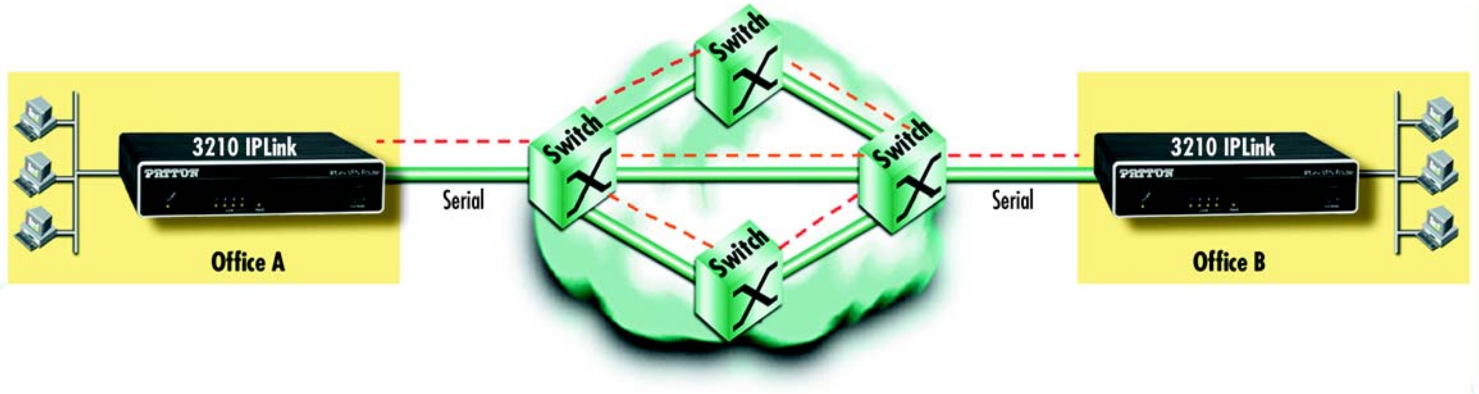


Figure 5. Branch-office virtual private network over a Frame-Relay service network

Figure 5 shows a branch-to-branch VPN connection through a frame-relay service network as delivered on serial lines. The OnSite 3210 Series can support a similar scenario with network service delivered via an Ethernet WAN interface. For remote sites where PPP service is available, the 3210 Series also supports PPP network access over all the standard WAN interface options mentioned above.

In this specific application, all traffic between the branch and corporate offices is carried in an IPSec tunnel. All of the IPSec VPN traffic is encapsulated in Frame Relay for transport over the Frame Relay service network. The serial port is configured for Frame Relay.

To configure this application, you need to configure the following features:

- The WAN port with Frame Relay as the encapsulation protocol
- An IPSec VPN between the two endpoints.

See chapter 4 on page 40 to configure the serial port and chapter 5 on page 42 to configure the VPN.

Corporate multi-function virtual private network

The OnSite 3210 Series can deliver both private corporate intranet service and public Internet access to multiple remote sites by leveraging OnSite's multiple frame-relay PVC support (see figure 6). The enterprise enjoys the benefits of secure multi-office virtual private networking with QoS for prioritized traffic flow for mission-critical information.

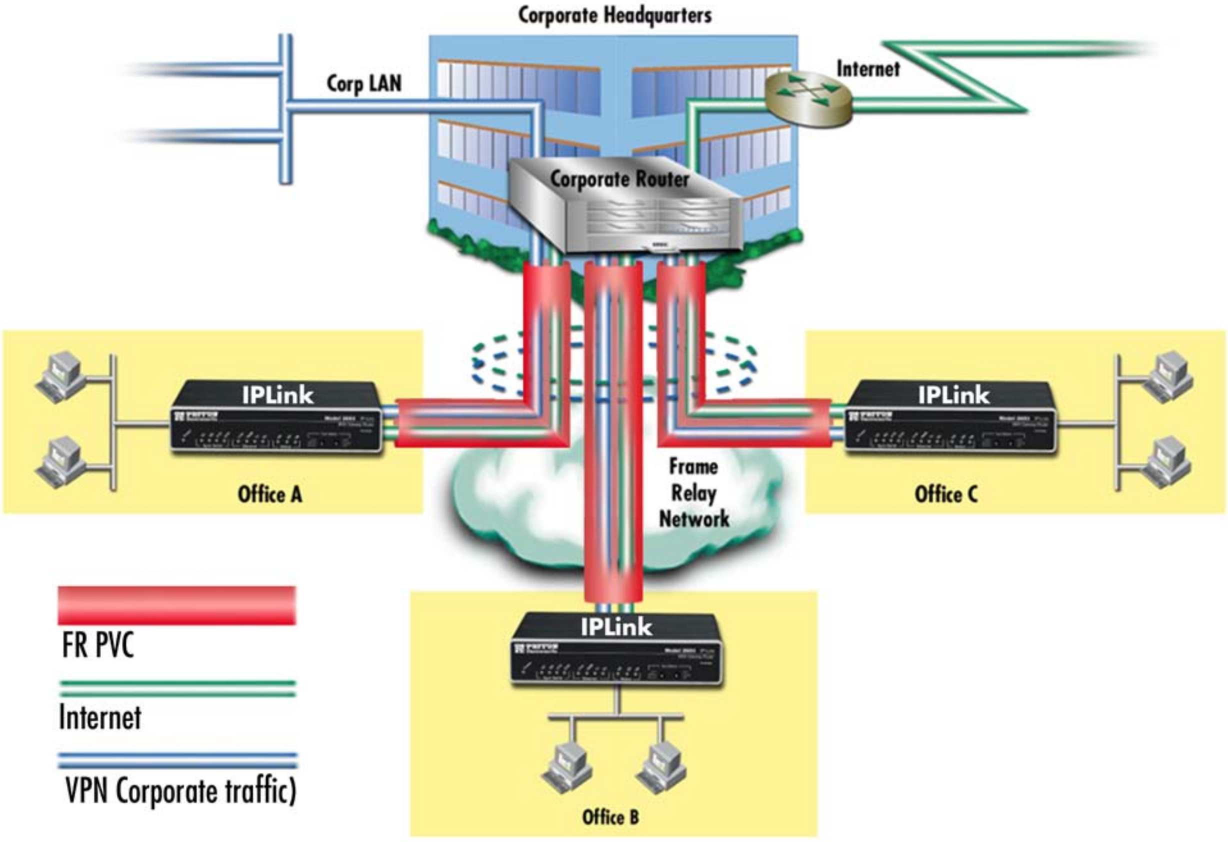


Figure 6. Corporate multi-function virtual private network

In figure 6, the blue pipes represent VPN connections for private traffic within the corporate intranet, while the green pipes represent the Internet traffic. The red pipe is a Frame Relay PVC transporting Internet traffic and private corporate traffic over the VPN. Each of the three remote sites is connected with headquarters via an OnSite VPN router. Each remote site can take advantage of the most convenient and locally available interface the WAN service can offer.

The corporate multi-function application carries two types of traffic between each remote office and corporate's central office:

- Private corporate traffic (the intranet/extranet)
- Internet traffic

The service provider offers a Frame Relay network for access, so both the private corporate traffic and the Internet traffic is transported over a Frame Relay PVC with one DLCI. The corporate traffic is transported within IPSec VPN that is in the Frame Relay PVC. The separation of corporation and Internet traffic is managed by using an ACL using IP addresses as the watershed.

To configure this application, you must configure the following features:

- A serial Frame Relay link as the WAN service which will carry both private corporate traffic and public Internet traffic
- An IPSec VPN for private corporate traffic
- An ACL to distinguish between the two types of traffic so only the private corporate traffic is carried over the VPN.

See chapter 4 on page 40 to configure the serial port, chapter 5 on page 42 to configure the VPN, and chapter 6 on page 54 to configure the ACL. Chapter 7 on page 68 provides more in-depth explanations of scheduling various types of traffic. Various techniques are also described, including QoS and TOS.

Chapter 2 Hardware installation

Chapter contents

Planning the installation

Before you start the actual installation, we strongly recommend that you gather all the information you will need to install and setup the device. See table 3 for an example of what pre-installment checks you might need to carry out. Completing the pre-installation checks enables you to install and set up your VPN router within an existing network infrastructure with confidence.

⚠ CAUTION

The mains outlet that is utilized to power the equipment must be within 1 meter (3 feet) of the device and shall be easily accessible.

Note When setting up your VPN router you must consider cable length limitations, and potential electromagnetic interference (EMI) as defined by the applicable local and international regulations. Ensure that your site is properly prepared before beginning installation.

Before installing the VPN Router device, the following tasks should be completed:

- **Create a network diagram** (see section "Network information" on page 26)
- **Gather IP related information** (see section "IP related information" on page 26 for more information)
- **Install the hardware and software needed to configure the OnSite router.** (See section "Software tools" on page 26)
- **Verify power source reliability** (see section "Power source" on page 26).

When you finish preparing for your VPN Router installation, go to section "Installing the VPN router" on page 27 to install the device.

Installation checklist

The installation checklist (see table 3) lists the tasks for installing an OnSite 3210 Series VPN Router. Make a copy of this checklist and mark the entries as you complete each task. For each OnSite 3210 Series VPN Router, include a copy of the completed checklist in your site log.

Table 3. Installation checklist

Task	Verified by	Date
Network information available & recorded in site log		
Environmental specifications verified		
Site power voltages verified		
Installation site pre-power check completed		
Required tools available		
Additional equipment available		
All printed documents available		
OnSite release & build number verified		
Rack, desktop, or wall mounting of chassis completed		
Initial electrical connections established		
ASCII terminal attached to console port		
Cable length limits verified		
Initial configuration performed		
Initial operation verified		

Site log

Patton recommends that you maintain a site log to record all actions relevant to the system, if you do not already keep such a log. Site log entries should include information such as listed in table 4.

Table 4. Sample site log entries

Entry	Description
Installation	Make a copy of the installation checklist and insert it into the site log
Upgrades and maintenance	Use the site log to record ongoing maintenance and expansion history
Configuration changes	Record all changes and the reasons for them
Maintenance	Schedules, requirements, and procedures performed
Comments	Notes, and problems
Software	Changes and updates to OnSite software

Network information

When planning your installation there are certain network-connection considerations that you should take into account. The following sections describe such considerations for several types of network interfaces.

Network Diagram

Draw a network overview diagram that displays all neighboring IP nodes, connected elements and telephony components.

IP related information

Before you can set up the basic IP connectivity for your OnSite 3210 Series you should have the following information:

- IP addresses and subnet masks used for Ethernet LAN and WAN ports
- IP addresses and subnet masks used for the V.35 or X.21 serial WAN port
- IP addresses and subnet masks used for the T1/E1 WAN port
- IP addresses of central TFTP Server used for configuration upload and download
- Login and password for PPPoE Access.

Software tools

You will need a PC (or equivalent) with a VT-100 emulation program (e.g. HyperTerminal) to configure the software on your OnSite VPN Router.

Power source

If you suspect that your AC power is not reliable, for example if room lights flicker often or there is machinery with large motors nearby, have a qualified professional test the power. Install a power conditioner if necessary.

Location and mounting requirements

The OnSite VPN Router is intended to be placed on a desktop or similar sturdy, flat surface that offers easy access to the cables. Allow sufficient space at the rear of the chassis for cable connections. Additionally, you should consider the need to access the unit for future upgrades and maintenance.

Installing the VPN router

OnSite VPN Router installation consists of the following:

- Placing the device at the desired installation location (see section "Mounting the VPN router" on page 27)
- Installing the interface and power cables (see section "Connecting cables" on page 27)

When you finish installing the OnSite router, go to chapter 3, "Getting started with the OnSite" on page 31.

Mounting the VPN router

Place the VPN Router on a desktop or similar sturdy, flat surface that offers easy access to the cables. The VPN Router should be installed in a dry environment with sufficient space to allow air circulation for cooling.

Note For proper ventilation, leave at least 2 inches (5 cm) to the left, right, front, and rear of the OnSite VPN Router.

Connecting cables

WARNING **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

CAUTION The interconnecting cables must be acceptable for external use and must be rated for the proper application with respect to voltage, current, anticipated temperature, flammability, and mechanical serviceability.

Installing VPN Router cables takes place in the following order:

1. Installing the 10/100 Ethernet port cable or cables (see section "Installing the Ethernet cable" on page 27)
2. Installing the cables (see section "Installing the DSL cable" on page 28)
3. Installing the power input (see section "Connecting to external power source" on page 29)

Installing the Ethernet cable

The OnSite 3210 Series has automatic MDX (auto-cross-over) detection and configuration on the Ethernet ports. Any of the two ports can be connected to a host or hub/switch with a straight-through wired cable (see figure 7). Ethernet devices (10Base-T or 100Base-T) are connected to the OnSite's Ethernet ports (see table 5 for port pin-out listing) via a cable terminated with RJ-45 plugs.

Table 5. Ethernet 10/100Base-T (RJ-45) port pin-outs

Pin	Signal
1	TX+
2	TX-
3	RX+
6	RX-

Note Pins not listed are not used.

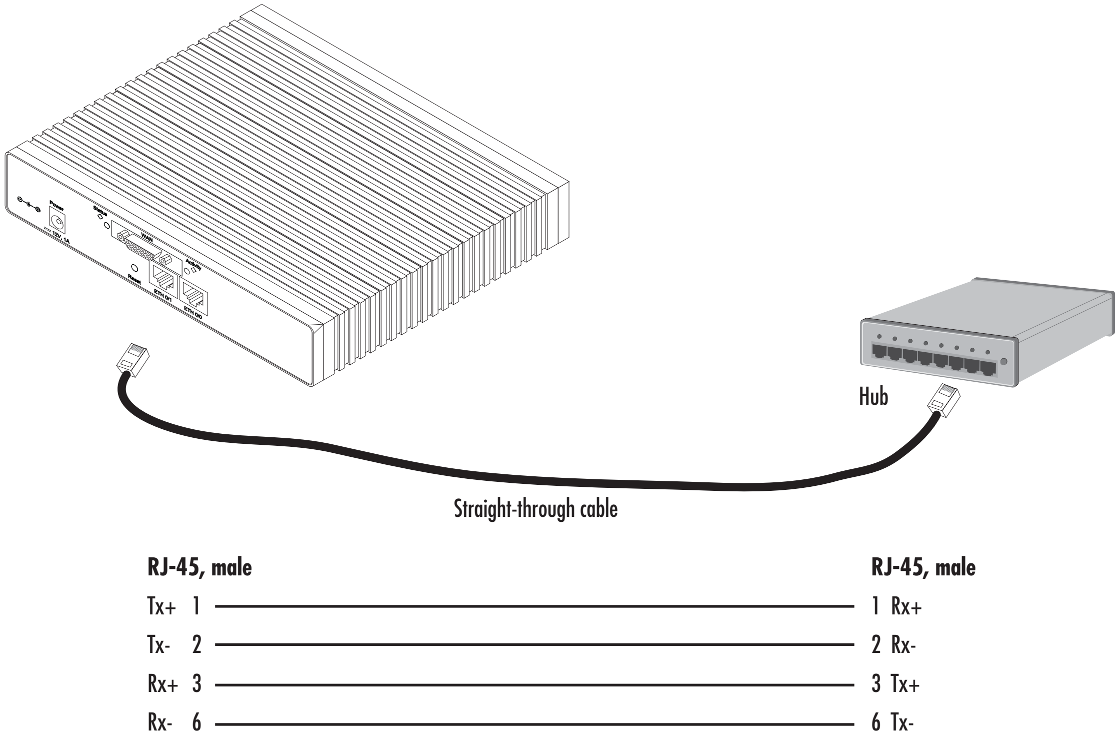


Figure 7. Connecting an OnSite 3210 Series device to a hub

Installing the DSL cable

The OnSite 3210 comes with a G.SHDSL interface. Use a straight-through RJ-11 cable to connect the DSL port.

Connecting to external power source

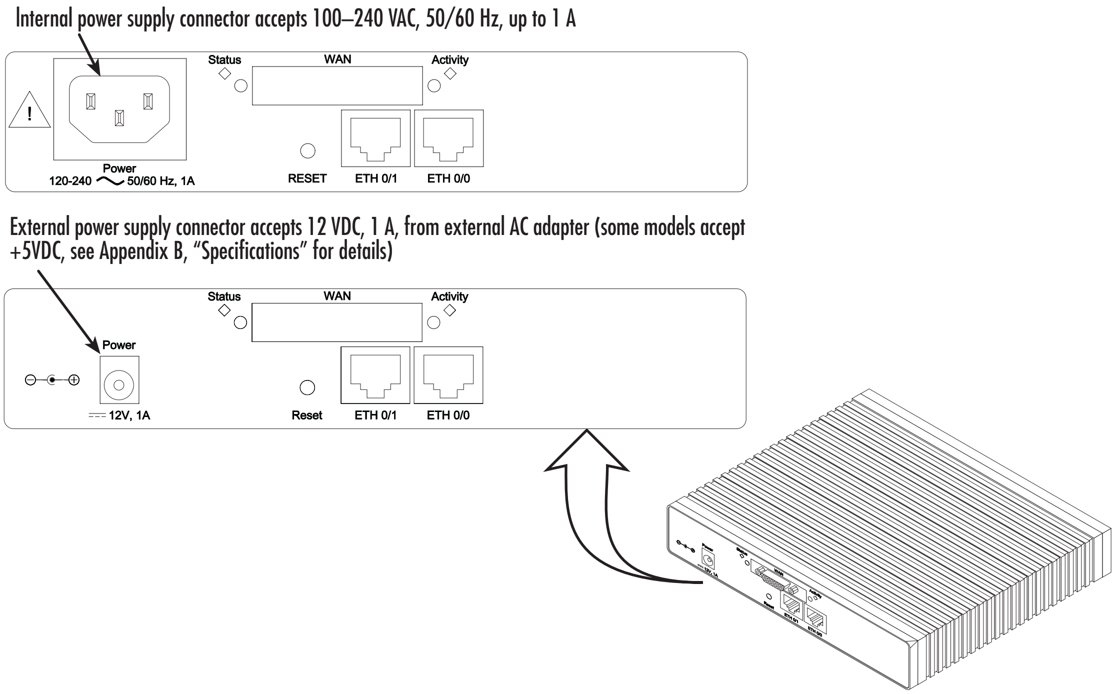
The VPN Router comes with one of the following power supply options as best-suited to the expected installation environment:

- 120/140VAC internal power supply (designated by the model code extension ***UI***)
- 120/140VAC external power supply (designated by the model code extension ***EUI***)
- 120VAC external power supply (designated by the model code extension ***E***)

This section below describes installing the power cord into the VPN Router. Do the following:

Note Do not connect the power cord to the power outlet at this time.

1. If your unit is equipped with an internal power supply, go to step 2. Otherwise, insert the barrel type connector end of the AC power cord into the external power supply connector (see figure 8).
2. Insert the female end of the power cord into the internal power supply connector (see figure 8).


Internal power supply connector accepts 100–240 VAC, 50/60 Hz, up to 1 A

External power supply connector accepts 12 VDC, 1 A, from external AC adapter (some models accept +5VDC, see Appendix B, “Specifications” for details)

Figure 8. Power connector location on rear panel

CAUTION

The UI and EUI power supplies automatically adjust to accept an input voltage from 100 to 240 VAC (50/60 Hz).

Verify that the proper voltage is present before plugging the power cord into the receptacle. Failure to do so could result in equipment damage.

3. Verify that the AC power cord included with your VPN Router is compatible with local standards. If it is not, refer to chapter 9, "Contacting Patton for assistance" on page 89 to find out how to replace it with a compatible power cord.

4. Connect the male end of the power cord to an appropriate power outlet.

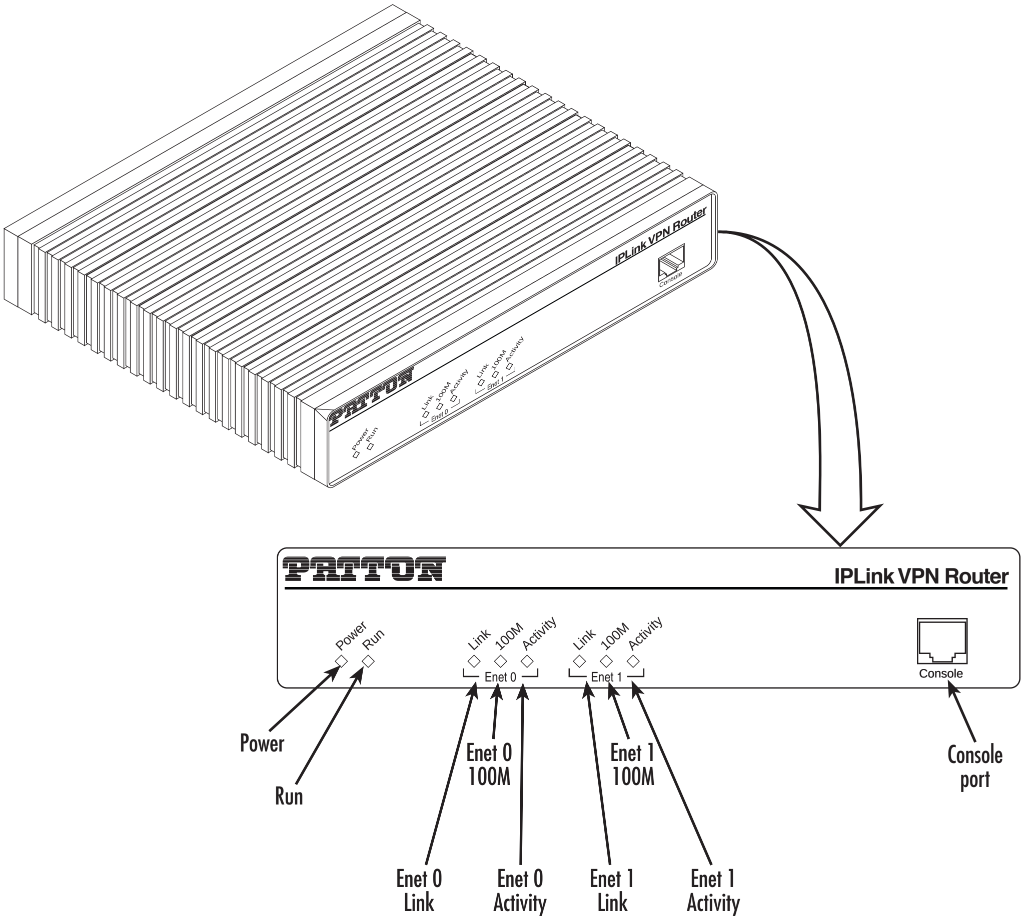


Figure 9. VPN Router front panel LEDs and Console port locations

5. Verify that the green *Power* LED is lit (see figure 9).

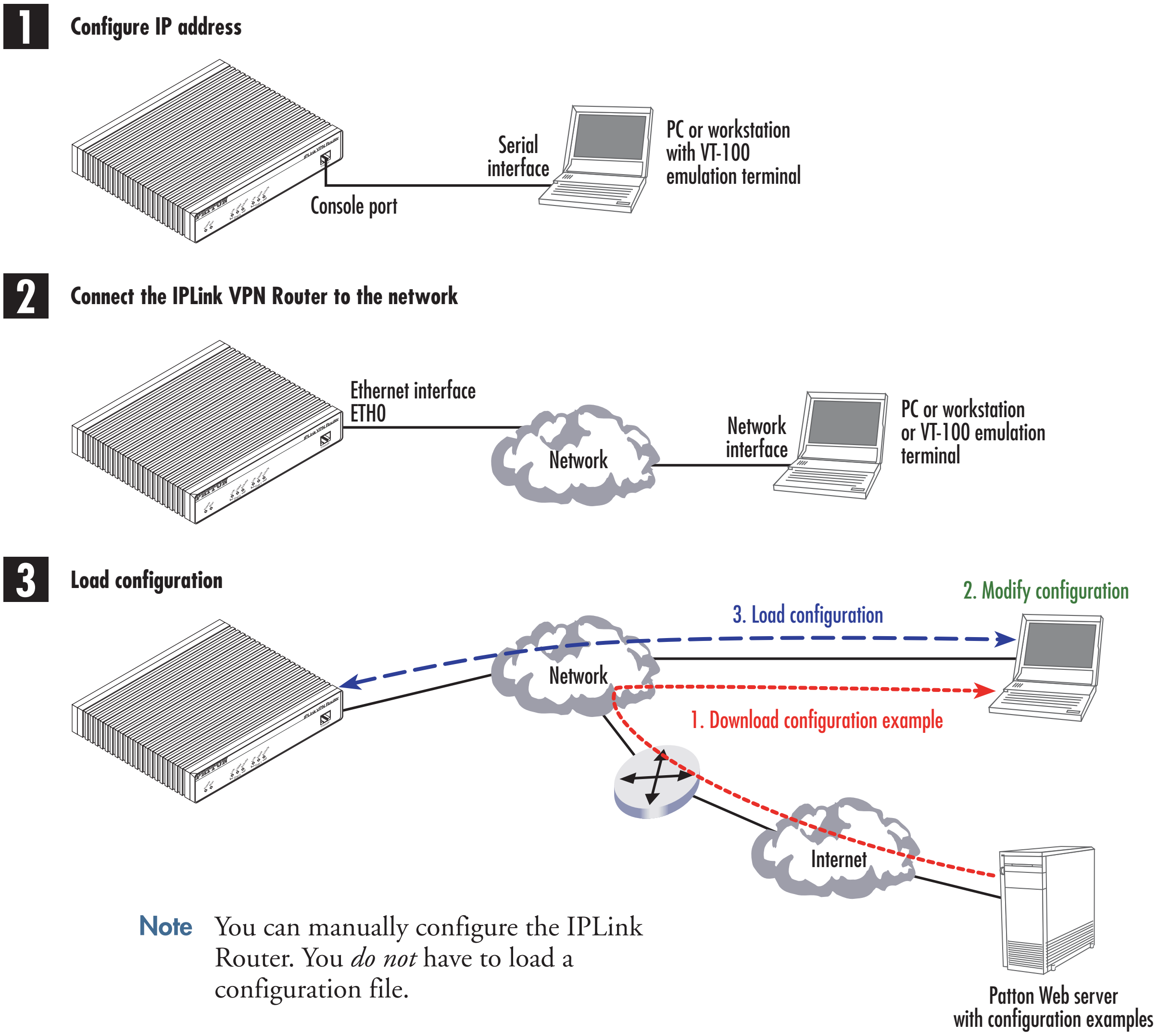
Congratulations, you have finished installing the OnSite VPN Router! Now go to chapter 3, "Getting started with the OnSite" on page 31.

Chapter 3 Getting started with the OnSite

Chapter contents

Introduction

This chapter leads you through the basic steps to set up a new OnSite VPN Router. Figure 10 show the main steps for setting up a new OnSite VPN Router.


1
Configure IP address
Serial interface
PC or workstation with VT-100 emulation terminal
Console port
2
Connect the IPLink VPN Router to the network
Ethernet interface ETH0
Network
Network interface
PC or workstation or VT-100 emulation terminal
3
Load configuration
2. Modify configuration
3. Load configuration
Network
1. Download configuration example
Internet
Patton Web server with configuration examples

Note You can manually configure the IPLink Router. You *do not* have to load a configuration file.

Figure 10. Steps for setting up a new OnSite VPN Router

1. Configure IP address

Power connection and default configuration

First the OnSite VPN Router must be connected to the mains power supply with the power cable. Wait until the Run LED stops blinking and lights constantly. Now the OnSite VPN Router is ready.

The factory default configuration for the Ethernet interface IP addresses and network masks are listed in table 6.

Table 6. Factory default IP address and network mask configuration

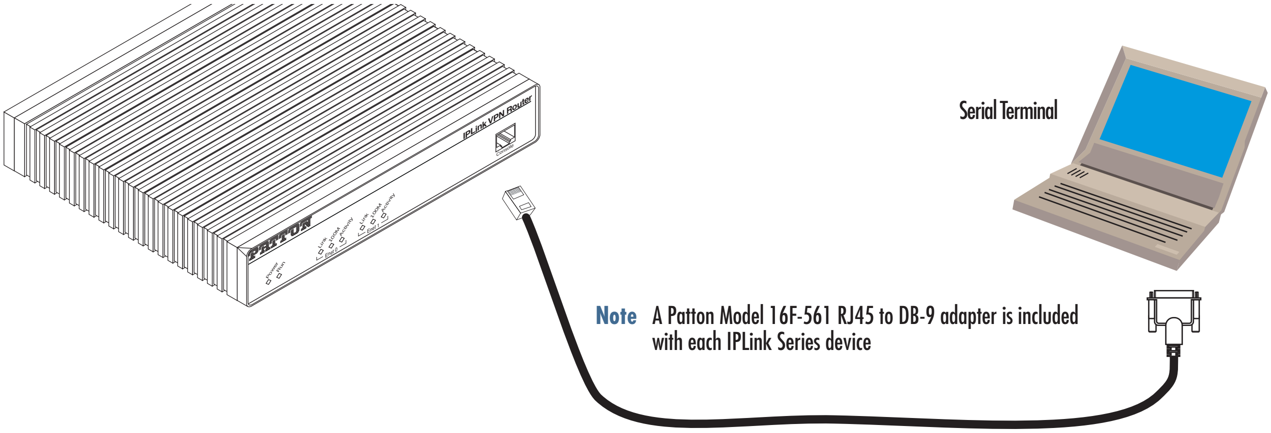
	IP Address	Network Mask
Interface Ethernet 0/0 (ETH0)	172.16.40.1	255.255.0.0
Interface Ethernet 0/1 (ETH1)	192.168.1.1	255.255.255.0
Interface Ethernet 0/2 (ETH2)	x.x.x.x	x.x.x.x
Interface Ethernet 0/3 (ETH3)	x.x.x.x	x.x.x.x
Interface Ethernet 0/4 (ETH4)	x.x.x.x	x.x.x.x

All Ethernet interfaces are activated upon power-up.

If these addresses match with those of your network, go to section "2. Connect the OnSite VPN Router to the network" on page 35. Otherwise, refer to the following sections to change the addresses and network masks.

Connect with the serial interface

The *Console* port is wired as an EIA-561, RS-232 port. Use the included Model 16F-561 adapter and cable (see figure 11) between the OnSite VPN Router's *Console* port and a PC or workstation's RS-232 serial interface. Activate the terminal emulation program on the PC or workstation that supports the serial interface (e.g. HyperTerm).



Note A Patton Model 16F-561 RJ45 to DB-9 adapter is included with each IPLink Series device

Figure 11. Connecting to the terminal

Terminal emulation program settings:

- 9600 bps
- no parity
- 8 bit

- 1 stop bit
- No flow control

Login

Accessing your OnSite VPN Router via the local console port (or via a Telnet session) causes the login screen to display. Type the factory default login: *administrator* and leave the password empty. Press the *Enter* key after the password prompt.

```
login:administrator
password: <Enter>
172.16.40.1>
```

After you have successfully logged in you are in the operator execution mode, indicated by > as command line prompt. With the commands *enable* and *configure* you enter the configuration mode.

```
172.16.40.1>enable
172.16.40.1#configure
172.16.40.1(cfg)#
```

Changing the IP address

Select the context IP mode to configure an IP interface.

```
172.16.40.1(cfg)#context ip router
172.16.40.1(ctx-ip)[router]#
```

Now you can set your IP address and network mask for the interface *eth0*. Within this example a class C network (172.16.1.0/24) is assumed. The IP address in this example is set to *172.16.1.99* (you should set this to an unused IP address on your network).

```
172.16.40.1(ctx-ip)[router]#interface eth0
172.16.40.1(if-ip)[eth0]#ipaddress 172.16.1.99 255.255.255.0
2002-10-29T00:09:40 : LOGINFO    : Link down on interface eth0.
2002-10-29T00:09:40 : LOGINFO    : Link up on interface eth0.
172.16.1.99(if-ip)[eth0]#
```

Copy this modified configuration to your new start-up configuration. Upon the next start-up the system will initialize itself using the modified configuration.

```
172.16.1.99(if-ip)[eth0]#copy running-config startup-config
172.16.1.99(if-ip)[eth0]#
```

The OnSite VPN Router can now be connected with your network.

2. Connect the OnSite VPN Router to the network

Depending whether you connect the OnSite VPN Router to a host directly or via a hub or switch either straight-through wired or cross-over cables must be used (see figure 12).

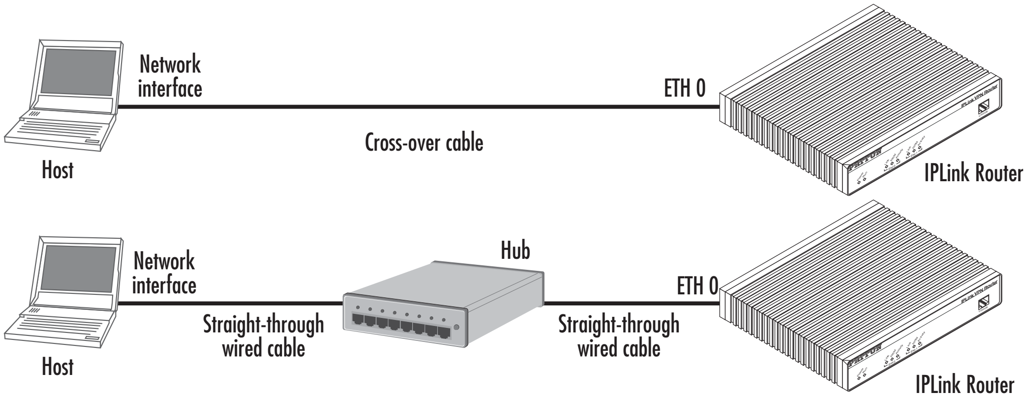


Figure 12. Connecting the OnSite VPN Router to the network

You can check the connection with the ping command to another host on the local LAN.

```
172.16.1.99(if-ip)[eth0]#ping <IP Address of the host>
```

Respectively from the host: *ping 172.16.1.99*

Note To ping outside your local LAN, you will need to configure the default gateway.

3. Load configuration

Patton provides a collection of configuration templates online at **www.patton.com/support/upgrades**—one of which may be similar enough to your application that you can use it to speed up configuring the OnSite router. Simply download the configuration note that matches your application to your PC. Adapt the configuration as described in the configuration note to your network (remember to modify the IP address) and copy the modified configuration to a TFTP server. The OnSite VPN Router can now load its configuration from this server.

In this example we assume the TFTP server on the host with the IP address 172.16.1.11 and the configuration named *IPL.cfg* in the root directory of the TFTP server.

```
172.16.1.99(if-ip)[eth0]#copy tftp://172.16.1.11/IPL.cfg startup-config
Download...100%
172.16.1.99(if-ip)[eth0]#
```

After the OnSite VPN Router has been rebooted the new start up configuration will be activated.

```
172.16.1.99(if-ip)[eth0]#reload
Running configuration has been changed.
Do you want to copy the 'running-config' to the 'startup-config'?
Press 'yes' to store, 'no' to drop changes : no
Press 'yes' to restart, 'no' to cancel : yes
The system is going down
```

Chapter 4 G.SHDSL Basic Configuration

Chapter contents

Introduction

The OnSite 3210 model has an option for a built-in G.SHDSL modem. The modem appears in the configuration as "port dsl 0 0" mode.

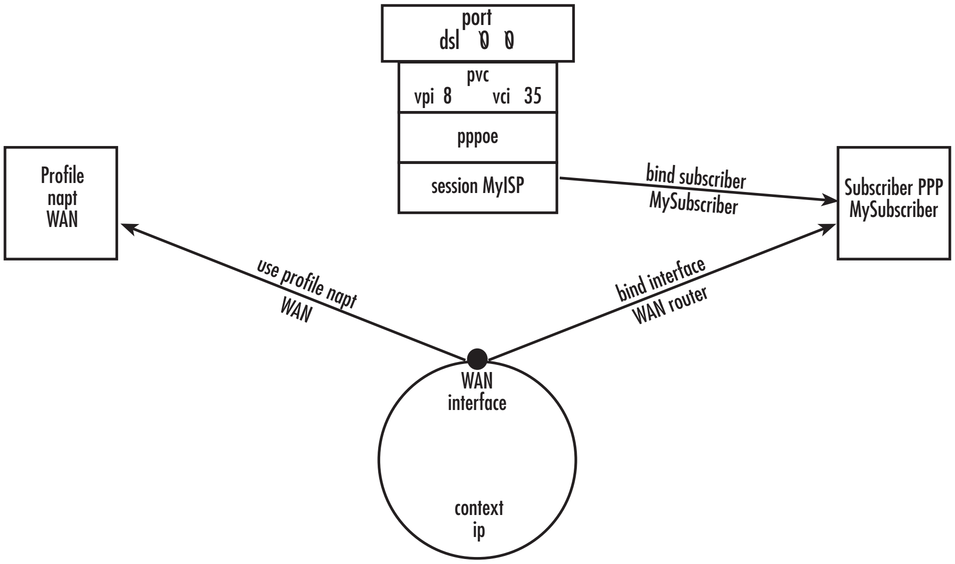


Figure 13. Configuring the G.SHDSL card for PPPoE

CAUTION

The Modem setup uses IP messages within its own subnet: 192.0.2.0/24.

Note For information about the specifications of the G.SHDSL daughter card, see Appendix B, "Specifications" on page 95.

Line Setup

There is no line modulation setting. The modems automatically adapt to the bit rate and modulation used. The status LED on the back of the device is blinking while the modem attempts to connect and lit when the link is established. If the modem keeps blinking, check the cabling,

Configuring PPPoE

Figure 13 explains how to configure PPPoE on the SmartNode's built-in G.SHDSL card. To configure the DSL port for PPPoE, first you need to log in to the SmartNode via the CLI and enter configuration mode.

```
login: administrator
password: <enter>
SN4xxx>enable
SN4xxx>#configure
```

Next, you will need to create a WAN profile, create a WAN interface, and create a subscriber. Then, you can configure the DSL port (port dsl 0 0) for PPPoE.
Follow this example:

```
profile napt WAN

context ip router
  interface WAN
     ipaddress unnumbered
     point-to-point
     use profile napt WAN
     tcp adjust-mss rx mtu
     tcp adjust-mss tx mtu

subscriber ppp MySubscriber
  dial out
  authentication chap
  identification outbound <username> password <password>
  bind interface WAN router

port dsl 0 0
  pvc vpi 8 vci 35
     pppoe
        session MyISP
           bind subscriber MySubscriber
           no shutdown
```

The line - `use profile napt WAN -` defines that the NAPT profile <*profile*> will be used on the ip interface <*name*>. For PPPoE, you will only use outbound for identification. You will want to use authentication, which is why you bind to a subscriber. You can use authentication chap or authentication pap. The line - `bind subscriber MySubscriber` - binds the PPPoE session to the PPP subscriber, in case authentication is required. If you do not use authentication, then you will not have a subscriber and you will bind directly to the interface.

Configuration Summary

The modems offer multiple bridged Ethernet connections through logical channels within the DSL link. A logical connection is called a Permanent Virtual Circuit (PVC) and is identified by a VPI/VCI number pair. Consult your provider's configuration instructions for connections used on your DSL link. You define those PVCs inside "port dsl 0 0":

```
port dsl 0 0
  pvc vpi 8 vci 35
```

Iin the mode "pvc", you define what to do with the bridged Ethernet connection it offers:

- Bind one or more IP interfaces when your providers uses fixed ip addresses or DHCP in the network
- Enter PPPoE mode and define a PPP session if the provider is using PPPoE.

Note PPPoA is not supported.

Setting up permanent virtual circuits (PVC)

The modems currently available are using ATM to multiplex traffic over the DSL framing connection. ATM allows you to have separate logical connections running in parallel. Those connections are called permanent virtual circuits (PVC). All permanent virtual circuits use AAL5 framing.

Table 7. PVC Commands

	Command	Purpose
Step 1	**node(prt-dsl)[0/0]# [no] pvc vpi 8 vci 35**	Creates PVC 8/35 and enters configuration mode for this PVC. The "no"-variant deletes the PVC configuration.
Step 2	**node(pvc)[8/35]# encapsulation {llc|vc}**	Sets the encapsulation to be used. Optionally select either LLC encapsulation or VC multiplexing for this PVC. Default: llc

Using PVC channels in bridged Ethernet mode

The PVC offers a bridged Ethernet connection as specified in RFC1483, which can be used as an IP link e.g. with DHCP to assign the address, DNS server, and default gateway. To do this, you bind an IP interface to the PVC like it would be done to a normal Ethernet port.

Table 8. PVC channels in bridged Ethernet mode

	Command	Purpose
Step 1	**node(pvc)[vpi/vci]# [no] bind interface <if-name>**	Associates an IP interface configuration with this PVC.

Using PVC channels with PPPoE

The RFC1483 bridged Ethernet connection can also be used for PPPoE. To do this, you enter PPPoE mode within the PVC mode. All PPPoE commands apply as if the PVC was a regular Ethernet port.

Table 9. PVC channels in PPPoE mode

	Command	Purpose
Step 1	**node(pvc)[vpi/vci]# pppoe**	Enters PPPoE configuration mode for this PVC.
Step 2	**node(pppoe)# session <name>**	Defines a PPPoE session.
Step 3	**node(session)[<name>]# bind subscriber <subscriber-name>**	Links the session to a subscriber definition.
Step 4	**node(session)[<name>]# no shutdown**	Enables the PPPoE session

Note The bridged PVC connections are internally mapped to VLANs on a virtual Ethernet port 0/2. You will therefore see references to this third Ethernet port when displaying PPPoE status information or debug logs.

Diagnostics

Table 10. Diagnostics commans

	Command	Purpose
Step 1	**node> show dsl type**	Displays the type of modem installed.
Step 2	**node> show dsl line-state**	Displays information about the state of the DSL link.
Step 3	**node> show dsl version**	Display firmware version information for the modem.
Step 4	**node# debug dsl-setup**	Lists the configuration interactions between the gateway and the modem module.

Troubleshooting DSL Connections

Link State:

- Verify that the DSL link is established (status LED is continuously on)

PPPoE access:

- Check if "show pppoe detail 3" shows "State: .... opened". This indicates that the PVC is valid and a that you reached a PPPoE server through it.
- Check if "show ppp networks detail 3" shows "State: .... opened" for both the "LCP" and the "CHAP" section. If LCP is not working, there is probably no compatible authentication protocol configured. Make sure "authentication chap" and "authentication pap" are included in the subscriber setup. If only CHAP failed there may be an error with the username or password.
- Run the "debug" command: **node# debug dsl-setup** (See table 10 above).

Chapter 5 **VPN configuration**

Chapter contents

Introduction

This chapter describes how to configure the VPN connections between two OnSite routers or between an OnSite and a third-party device.

A *virtual private network* (VPN) is a private data network that uses the public telecommunications infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

There are different technologies to implement a VPN. OnSite applies the *internet protocol security* (IPsec) Architecture (see RFC 2401). The following sections describe the main building blocks of the IPsec architecture as implemented in OnSite router.

Authentication

Authentication verifies the integrity of data stream and ensures that it is not tampered with while in transit. It also provides confirmation about data stream origin.

Two authentication protocols are available:

- Authentication header (AH): protects the IP payload, the IP header, and the authentication header itself
- Encapsulating security payload (ESP): protects the IP payload and the ESP header and trailer, but not the IP header

Two algorithms perform the authentication:

- HMAC-MD5-96: is a combination of the *keyed-hashing for message authentication* (HMAC) and the *message digest version 5* (MD5) hash algorithm. It requires an authenticator of 128-bit length and calculates a hash of 96 bits over the packet to be protected (see RFC 2403).
- HMAC-SHA1-96: is a combination of the (HMAC) and the *secure hash algorithm version 1* (SHA1). It requires an authenticator of 160 bit length and calculates a hash of 96 bits over the packet to be protected (see RFC 2404).

Encryption

Encryption protects the data in transit from unauthorized access. Encapsulating security payload (ESP) is the protocol to transport encrypted IP packets over IP (see RFC 2406).

The following encryption algorithms are available:

	Key Length [Bit]	RFC
DES-CBC (Data Encryption Standard - Cipher Block Chaining)	56	2405
3DES-CBC (Triple Data Encryption Standard - Cipher Block Chaining)	128 or 192[a]	1851
AES-CBC (Advanced Encryption Standard - Cipher Block Chaining)	128, 192, or 256	3268

[a] The 3DES algorithm uses only 112 out of the 128 Bit or 168 out of the 192 Bit as key information. Cisco only supports 192 Bit keys with 3DES.

The single DES algorithm no longer offers adequate security because of its short key length (a minimum key length 100 bits is recommended). The AES algorithm is very efficient and allows the fastest encryption. AES with a key length of 128 bits is therefore the recommended algorithm.

Transport and tunnel modes

The mode determines the payload of the ESP packet and hence the application:

- Transport mode: Encapsulates only the payload of the original IP packet, but not its header, so the IPsec peers must be at the endpoints of the communications link.
- A secure connection between two hosts is the application of the transport mode.
- Tunnel mode: Encapsulates the payload and the header of the original IP packet. The IPsec peers can be (edge) routers that are not at the endpoints of the communications link.

  A secure connection of the two (private) LANs, a ‘tunnel’, is the application of the tunnel mode.

VPN configuration task list

To configure a VPN connection, perform the following tasks:

- Creating an IPsec transformation profile
- Creating an IPsec policy profile
- Creating/modifying an outgoing ACL profile for IPsec
- Configuration of an IP Interface and the IP router for IPsec
- Displaying IPsec configuration information
- Debugging IPsec

Creating an IPsec transformation profile

The IPsec transformation profile defines which authentication and/or encryption protocols, which authentication and/or encryption algorithms shall be applied.

Procedure: To create an IPsec transformation profile

Mode: Configure

mac-sha1-96 }Enables authentication and defines the authentication protocol and the hash algorithm

Step	Command	Purpose
1	***node*(cfg)#profile ipsec-transform** *name*	Creates the IPsec transformation profile *name*
2 optional	***node*(pf-ipstr)[*name*]#esp-encryption { aes-cbc | des-cbc | 3des-cbc }** [*key-length*]	Enables encryption and defines the encryption algorithm and the key length
3 optional	***node*(pf-ipstr)[*name*]#{ ah-authentication | esp-authentication } {hmac-md5-96 | hmac-sha1-96 }**	Enables authentication and defines the authentication protocol and the hash algorithm

Use **no** in front of the above commands to delete a profile or a configuration entry.

Example: Create an IPsec transformation profile

The following example defines a profile for AES-encryption at a key length of 128.

```
3210(cfg)#profile ipsec-transform AES_128
3210(pf-ipstr)[AES_128]#esp-encryption aes-cbc 128
```

Creating an IPsec policy profile

The IPsec policy profile supplies the keys for the encryption and/or the authenticators for the authentication, the *security parameters indexes* (SPIs), and IP address of the peer of the secured communication. Furthermore, the profile defines which IPsec transformation profile to apply and whether transport or tunnel mode shall be most effective.

The SPI identifies a secured communication channel. The IPsec component needs the SPI to select the suitable key or authenticator. Inbound and outbound channels can have the same SPI, but the channels in the same direction—inbound or outbound—must have unique SPIs. The SPI is not encrypted and can be monitored.

Procedure: To create an IPsec policy profile

Mode: Configure

Step	Command	Purpose
1	***node*(cfg)#profile ipsec-policy-manual** *name*	Creates the IPsec policy profile name
2	***node*(pf-ipstr)[name]#use profile ipsec-transform** *name*	Selects the IPsec transformation profile to be applied
3 optional	***node*(pf-ipstr)[***name***]#session-key** **{ inbound | outbound }** **{ ah-aauthentication | esp-authentication | esp-encryption }** *key*	Sets a key for encryption or an authenticator for authentication, either for inbound or outbound direction. The key shall consist of hexadecimal digits (0..9, A..F); one digit holds 4 Bit of key information. The key setting must match definitions in the respective IPsec transformation profile. In particular, the length of the key or authenticator must match the implicit (see section "Authentication" on page 43 and "Encryption" on page 43) or explicit specification. Keys must be available for inbound and outbound directions. They can be different for the two directions. Make sure that the inbound key of one peer matches the outbound key of the other peer.
4	***node*(pf-ipstr)[***name***]#spi** **{ inbound | outbound } { ah | esp }** *spi*	Sets the SPI for encryption (esp) or authentication (ah), either for inbound or outbound direction. The SPI shall be a decimal figure in the range 1..2^{32}–1. SPIs must be available for encryption and/or authentication as specified in the respective IPsec transformation profile. SPIs must be available for inbound and outbound directions. They can be identical for the two directions but must be unique in one direction. Make sure that the inbound SPI of one peer matches the outbound SPI of the other peer.
5	***node*(pf-ipstr)[***name***]#peer** *ip-address*	Sets the IP address of the peer **Note** The peers of the secured communication must have static IP address. DNS resolution is not available yet.
6	***node*(pf-ipstr)[***name***]#mode** **{ tunnel | transport }**	Selects tunnel or transport mode

Use **no** in front of the above commands to delete a profile or a configuration entry.

Example: Create an IPsec policy profile

The following example defines a profile for AES-encryption at a key length of 128.

```
3210(cfg)#profile ipsec-policy-manual ToBurg
3210(pf-ipsma)[ToBurg]#use profile ipsec-transform AES_128
3210(pf-ipsma)[ToBurg]#session-key inbound esp-encryption
1234567890ABCDEF1234567890ABCDEF
3210(pf-ipsma)[ToBurg]#session-key outbound esp-encryption
FEDCBA0987654321FEDCBA0987654321
3210(pf-ipsma)[ToBurg]#spi inbound esp 1111
3210(pf-ipsma)[ToBurg]#spi outbound esp 2222
3210(pf-ipsma)[ToBurg]#peer 200.200.200.1
3210(pf-ipsma)[ToBurg]#mode tunnel
```

Creating/modifying an outgoing ACL profile for IPsec

An access control list (ACL) profile in the outgoing direction selects which outgoing traffic to encrypt and/or authenticate, and which IPsec policy profile to use. IPsec does not require an incoming ACL.

Note Outgoing and incoming IPsec traffic passes an ACL (if available) twice, once before and once after encryption/authentication. So the respective ACLs must permit the encrypted/authenticated and the plain traffic.

For detailed information on how to set-up ACL rules, see chapter 6, "Access control list configuration" on page 54.

Procedure: To create/modify an outgoing ACL profile for IPsec

Mode: Configure

Step	Command	Purpose
1	***node*(cfg)#profile acl** *name*	Creates or enters the ACL profile name
2	***node*(pf-ipstr)[*name*]#permit …** **[ipsec-policy** *name* **]**	The expression 'ipsec-policy name' appended to a permit ACL rule activates the IPsec policy profile *name* to encrypt/authenticate the traffic identified by this rule.

Note New entries are appended at the end of an ACL. Since the position in the list is relevant, you might need to delete the ACL and rewrite it completely.

Example: Create/modify an ACL profile for IPsec

The following example configures an outgoing ACL profile that interconnects the two private networks 192.168.1/24 and 172.16/16.

```
3210(cfg)#profile acl VPN_Out
3210(pf-acl)[VPN_Out]#permit ip 192.168.1.0 0.0.0.255 172.16.0.0 0.0.255.255 ipsec-
policy ToBurg
3210(pf-acl)[VPN_Out]#permit ip any any
```

Configuration of an IP interface and the IP router for IPsec

The IP interface that provides connectivity to the IPsec peer, must now activate the outgoing ACL profile configured in the previous section. Furthermore, the IP router must have a route for the remote network that points to the respective IP interface.

Procedure: To activate the outgoing ACL profile and to establish the necessary route

Mode: Configure

Step	Command	Purpose
1	***node*(cfg)#context ip router**	Enter IP context
2	***node*(ctx-ip)[**router**]#interface** *if-name*	Create/enter the IP interface *if-name*
3	***node*(if-ip)[***if-name***]# use profile acl** *name* **out**	Activate the outgoing ACL profile *name*
4	***node*(if-ip)[***if-name***]#context ip router**	Enter IP context
5 **optional**	***node*(ctx-ip)[**router**]#route** *remote-network-address remote-network-mask if-name* **0**	Creates a route for the remote network that points the above IP interface *if-name* You can omit this setting if the default route already points to this IP interface or to a next hub reachable via this IP interface, and if there is no other route. Make also sure that the IP router knows how to reach the peer of the secured communication. Usually, a default route does this job.

Example: Activate outgoing ACL and establish route

The following example configures an outgoing ACL profile that interconnects the two private networks 192.168.1/24 and 172.16/16.

```
3210(cfg)#context ip router
3210(ctx-ip)[router]#interface WAN
3210(if-ip)[WAN]#use profile acl VPN_Out out
3210(if-ip)[WAN]#context ip router
3210(ctx-ip)[router]#route 172.16.0.0 255.255.0.0 WAN 0
```

Displaying IPsec configuration information

This section shows how to display and verify the IPsec configuration information.

Procedure: To display IPsec configuration information

Mode: Configure

Step	Command	Purpose
1 **optional**	***node*(cfg)#show profile ipsec-transform**	Displays all IPsec transformation profiles
2 **optional**	**node(cfg)#show profile ipsec-policy-manual**	Displays all IPsec policy profiles

Example: Display IPsec transformation profiles

```
3210(cfg)#show profile ipsec-transform

IPSEC transform profiles:

Name: AES_128
 ESP Encryption: AES-CBC, Key length: 128
```

Example: Display IPsec policy profiles

```
3210(cfg)#show profile ipsec-policy-manual

Manually keyed IPsec policy profiles:

Name: ToBurg, Peer: 200.200.200.1, Mode: tunnel, transform-profile: AES_128
 ESP SPI Inbound: 1111, Outbound: 2222
 ESP Encryption Key Inbound: 1234567890ABCDEF1234567890ABCDEF
 ESP Encryption Key Outbound: FEDCBA0987654321FEDCBA0987654321
```

Debugging IPsec

A debug monitor and an additional **show** command are at your disposal to debug IPsec problems.

Procedure: To debug IPsec connections

Mode: Configure

Step	Command	Purpose
1	***node***(cfg)#debug ipsec	Enables IPsec debug monitor
2 optional	***node***(cfg)#show ipsec security-associations	Summarizes the configuration information of all IPsec connections. If an IPsec connection does not show up, then one or more parameters are missing in the respective Policy Profile. The information 'Bytes (processed)' supports debugging because it indicates whether IPsec packets depart from ('OUT') or arrive at ('IN') the OnSite router.

Example: IPsec Debug Output

```
3210(cfg)#debug ipsec
IPSEC monitor on
23:11:04  ipsec > Could not find security association for inbound ESP packet.
SPI:1201
```

Example: Display IPsec Security Associations

```
3210(cfg)#show ipsec security-associations

Active security associations:

Dir Type        Policy     Mode       Udp-Encapsulation
Peer            SPI AH     SPI ESP    AH            ESP-Auth    ESP-Enc
Bytes (processed/lifetime) Seconds (age/lifetime)
```

```
IN  MANUAL      ToBurg    Tunnel     no
200.200.200.1   -          1111       -             -          AES-CBC 128
3622/unlimited                19047/unlimited

OUT MANUAL      ToBurg    Tunnel     no
200.200.200.1   -          2222       -             -          AES-CBC 128
2857/unlimited                19047/unlimited
```

Sample configurations

The following sample configurations establish IPsec connections between an OnSite and a Cisco router. To interconnect two OnSite routers instead, derive the configuration for the second OnSite by doing the following modifications:

- Swap ‘inbound’ and ‘outbound’ settings
- Adjust the ‘peer’ setting
- Swap the private networks in the ACL profiles
- Adjust the IP addresses of the LAN and WAN interfaces
- Adjust the route for the remote network

IPsec tunnel, DES encryption

OnSite configuration

```
profile ipsec-transform DES
  esp-encryption des-cbc 64

profile ipsec-policy-manual VPN_DES
  use profile ipsec-transform DES
  session-key inbound esp-encryption 1234567890ABCDEF
  session-key outbound esp-encryption FEDCBA0987654321
  spi inbound esp 1111
  spi outbound esp 2222
  peer 200.200.200.1
  mode tunnel

profile acl VPN_Out
  permit ip 192.168.1.0 0.0.0.255 172.16.0.0 0.0.255.255 ipsec-policy VPN_DES
  permit ip any any

profile acl VPN_In
  permit esp any any
  permit ah any any
  permit ip 172.16.0.0 0.0.255.255 192.168.1.0 0.0.0.255
  deny ip any any

context ip router

interface LAN
  ipaddress 192.168.1.1 255.255.255.0

interface WAN
```

```
    ipaddress 200.200.200.2 255.255.255.252
    use profile acl VPN_In in
    use profile acl VPN_Out out

  context ip router
    route 0.0.0.0 0.0.0.0 200.200.200.1 0
    route 172.16.0.0 255.255.0.0 WAN 0
```

Cisco router configuration

```
crypto ipsec transform-set DES esp-des
!
crypto map VPN_DES local-address FastEthernet0/1
crypto map VPN_DES 10 ipsec-manual
 set peer 200.200.200.2
 set session-key inbound esp 2222 cipher FEDCBA0987654321
 set session-key outbound esp 1111 cipher 1234567890ABCDEF
 set transform-set DES
 match address 110
!
access-list 110 permit ip 172.16.0.0 0.0.255.255 192.168.1.0 0.0.0.255
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.0.0
!
interface FastEthernet0/1
 ip address 200.200.200.1 255.255.255.252
 crypto map VPN_DES
!
ip route 192.168.1.0 255.255.255.0 FastEthernet0/1
```

IPsec tunnel, AES encryption at 256 bit key length, AH authentication with HMAC-SHA1-96

OnSite configuration

```
profile ipsec-transform AES_SHA1
  esp-encryption aes-cbc 256
  ah-authentication hmac-sha1-96

profile ipsec-policy-manual VPN_AES_SHA1
  use profile ipsec-transform AES_SHA1
  session-key inbound ah-authentication 1234567890ABCDEF1234567890ABCDEF12345678
  session-key outbound ah-authentication FEDCBA0987654321FEDCBA0987654321FEDCBA09
  session-key inbound esp-encryption
1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF
  session-key outbound esp-encryption
FEDCBA0987654321FEDCBA0987654321FEDCBA0987654321FEDCBA0987654321
  spi inbound ah 3333
  spi outbound ah 4444
  spi inbound esp 5555
  spi outbound esp 6666
  peer 200.200.200.1
  mode tunnel
...
```

```
Rest of the configuration, see above, just change the name of the IPsec policy pro-
file in the ACL profile ‘VPN_Out’
```

Cisco router configuration

```
crypto ipsec transform-set AES_SHA1 ah-sha-hmac esp-aes 256
!
crypto map VPN_AES_SHA1 local-address FastEthernet0/1
crypto map VPN_AES_SHA1 10 ipsec-manual
 set peer 200.200.200.2
 set session-key inbound esp 6666 cipher
FEDCBA0987654321FEDCBA0987654321FEDCBA0987654321FEDCBA0987654321
 set session-key outbound esp 5555 cipher
1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF
 set session-key inbound ah 4444 FEDCBA0987654321FEDCBA0987654321FEDCBA09
 set session-key outbound ah 3333 1234567890ABCDEF1234567890ABCDEF12345678
 set transform-set AES_SHA1
 match address 110
!
...
```

For the remainder of the configuration (see above), just change the name of the IPsec policy profile in the ACL profile *VPN_Out*

IPsec tunnel, 3DES encryption at 192 bit key length, ESP authentication with HMAC-MD5-96

OnSite configuration

```
profile ipsec-transform TDES_MD5
  esp-encryption 3des-cbc 192
  esp-authentication hmac-md5-96

profile ipsec-policy-manual VPN_TDES_MD5
  use profile ipsec-transform TDES_MD5
  session-key inbound esp-authentication 1234567890ABCDEF1234567890ABCDEF
  session-key outbound esp-authentication FEDCBA0987654321FEDCBA0987654321
  session-key inbound esp-encryption
1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF
  session-key outbound esp-encryption
FEDCBA0987654321FEDCBA0987654321FEDCBA0987654321
  spi inbound esp 7777
  spi outbound esp 8888
  peer 200.200.200.1
  mode tunnel
...
```

For the remainder of the configuration (see above), just change the name of the IPsec policy profile in the ACL profile *VPN_Out*

Cisco router configuration

```
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
crypto map VPN_3DES_MD5 local-address FastEthernet0/1
crypto map VPN_3DES_MD5 10 ipsec-manual
 set peer 200.200.200.2
 set session-key inbound esp 8888 cipher
FEDCBA0987654321FEDCBA0987654321FEDCBA0987654321 authenticator
FEDCBA0987654321FEDCBA0987654321
 set session-key outbound esp 7777 cipher
1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF authenticator
1234567890ABCDEF1234567890ABCDEF
 set transform-set 3DES_MD5
 match address 110
!
...
```

For the remainder of the configuration (see above), just change the name of the IPsec policy profile in the ACL profile *VPN_Out*.

Chapter 6 Access control list configuration

Chapter contents

Introduction

This chapter provides an overview of IP Access Control Lists and describes the tasks involved in configuring them through the OnSite router.

This chapter includes the following sections:

- About access control lists
- Access control list configuration task list (see page 57)
- Examples (see page 67)

About access control lists

This section briefly describes what access lists do, why and when you should configure access lists, and basic versus advanced access lists.

What access lists do

Access lists filter network traffic by controlling whether routed packets are forwarded, dropped or blocked at the router's interfaces. Your router examines each packet to determine whether to forward or drop the packet, based on the criteria you specified within the access lists.

Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

Note Sophisticated users can sometimes successfully evade or fool basic access lists because no authentication is required.

Why you should configure access lists

There are many reasons to configure access lists. For example, you can use access lists to restrict contents of routing updates, or to provide traffic flow control. But one of the most important reasons to configure access lists is to provide security for your network, and this is the reason explored in this chapter.

You should use access lists to provide a basic level of security for accessing your network. If you do not configure access lists on your router, all packets passing through the router could be allowed onto all parts of your network.

For example, access lists can allow one host to access a part of your network, and prevent another host from accessing the same area. In figure 14 host A is allowed to access the Human Resources network and host B is prevented from accessing the Human Resources network.

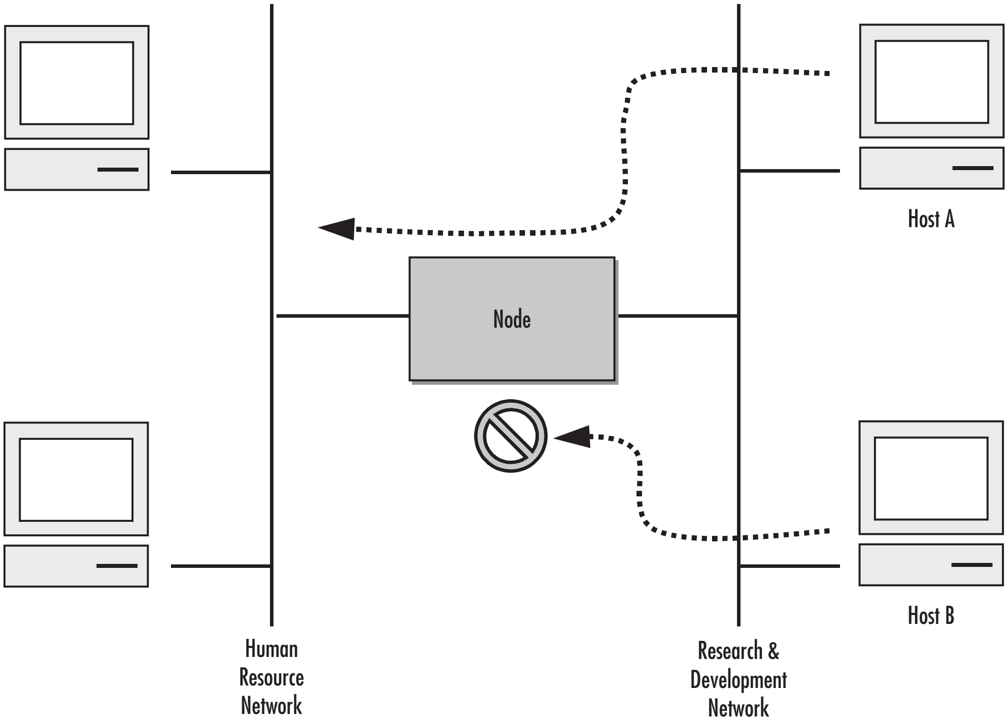


Figure 14. Using traffic filters to prevent traffic from being routed to a network

You can also use access lists to decide which types of traffic are forwarded or blocked at the router interfaces. For example, you can permit e-mail traffic to be routed but at the same time block all Telnet traffic.

When to configure access lists

Access lists should be used in firewall routers, which are often positioned between your internal network and an external network such as the Internet. You can also use access lists on a router positioned between two parts of your network, to control traffic entering or exiting a specific part of your internal network.

To provide the security benefits of access lists, you should configure access lists at least on border routers, i.e. those routers situated at the edges of your networks. This provides a basic buffer from the outside network or from a less controlled area of your own network into a more sensitive area of your network.

On these routers, you should configure access lists for each network protocol configured on the router interfaces. You can configure access lists so that inbound traffic or outbound traffic or both are filtered on an interface.

Features of access control lists

The following features apply to all IP access control lists:

- A list may contain multiple entries. The order access of control list entries is significant. Each entry is processed in the order it appears in the configuration file. As soon as an entry matches, the corresponding action is taken and no further processing takes place.

- All access control lists have an implicit *deny ip any any* at the end. A packet that does not match the criteria of the first statement is subjected to the criteria of the second statement and so on until the end of the access control list is reached, at which point the packet is dropped.
- Filter types include IP, Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP).
- An empty access control list is treated as an implicit *deny ip any any* list.

Note Two or more administrators should not simultaneously edit the configuration file. This is especially the case with access lists. Doing this can have unpredictable results.

Once in access control list configuration mode, each command creates a statement in the access control list. When the access control list is applied, the action performed by each statement is one of the following:

- **permit** statement causes any packet matching the criteria to be accepted.
- **deny** statement causes any packet matching the criteria to be dropped.

To delete an entire access control list, enter configuration mode and use the **no** form of the **profile acl** command, naming the access list to be deleted, e.g. no profile acl *name*. To unbind an access list from the interface to which it was applied, enter the IP interface mode and use the **no** form of the access control list command.

Access control list configuration task list

To configure an IP access control list, perform the tasks in the following sections.

- Mapping out the goals of the access control list
- Creating an access control list profile and enter configuration mode (see page 58)
- Adding a filter rule to the current access control list profile (see page 58)
- Adding an ICMP filter rule to the current access control list profile (see page 60)
- Adding a TCP, UDP or SCTP filter rule to the current access control list profile (see page 62)
- Binding and unbinding an access control list profile to an IP interface (see page 64)
- Displaying an access control list profile (see page 65)
- Debugging an access control list profile (see page 65)

Mapping out the goals of the access control list

To create an access control list you must:

- Specify the protocol to be filtered
- Assign a unique name to the access list
- Define packet-filtering criteria

A single access control list can have multiple filtering criteria statements.

Before you begin to enter the commands that create and configure the IP access control list, be sure that you are clear about what you want to achieve with the list. Consider whether it is better to deny specific accesses and permit all others or to permit specific accesses and deny all others.

Note Since a single access control list can have multiple filtering criteria statements, but editing those entries online can be tedious. Therefore, we recommend editing complex access control lists offline within a configuration file and downloading the configuration file later via TFTP to your OnSite device.

Creating an access control list profile and enter configuration mode

This procedure describes how to create an IP access control list and enter access control list configuration mode

Mode: Administrator execution

Step	Command	Purpose
1	***node***(**cfg)#profile acl** *name*	Creates the access control list profile *name* and enters the configuration mode for this list

name is the name by which the access list will be known. Entering this command puts you into *access control list configuration mode* where you can enter the individual statements that will make up the access control list.

Use the **no** form of this command to delete an access control list profile. You cannot delete an access control list profile if it is currently linked to an interface. When you leave the access control list configuration mode, the new settings immediately become active.

Example: Create an access control list profile

In the following example the access control list profile named *WanRx* is created and the shell of the access control list configuration mode is activated.

```
3210>enable
3210#configure
3210(cfg)#profile acl WanRx
3210(pf-acl)[WanRx]#
```

Adding a filter rule to the current access control list profile

The commands **permit** or deny are used to define an IP filter rule. This procedure describes how to create an IP access control list entry that permits access

Mode: Profile access control list

Step	Command	Purpose
1	***node***(**pf-acl)**[*name*]**#permit ip** {*src src-wildcard* **| any | host** *src*} {*dest dest-wildcard* **| any | host** *dest*} **[cos** *group*]	Creates an IP access of control list entry that permits access defined according to the command options

This procedure describes how to create an IP access control list entry that denies access

Mode: Profile access control list

Step	Command	Purpose
1	***node*****(pf-acl)[***name***]#deny ip {***src src-wildcard* **| any | host** *src***} {***dest dest-wildcard* **| any | host** *dest***} [cos** *group***]**	Creates an IP access of control list entry that denies access defined according to the command options

Where the syntax is:

Keyword	Meaning
src	The source address to be included in the rule. An IP address in dotted-decimal-format, e.g. 64.231.1.10.
src-wildcard	A wildcard for the source address. Expressed in dotted-decimal format this value specifies which bits are significant for matching. One-bits in the wildcard indicate that the corresponding bits are ignored. An example for a valid wildcard is 0.0.0.255, which specifies a class C network.
any	Indicates that IP traffic to or from all IP addresses is to be included in the rule.
host *src*	The address of a single source host.
dest	The destination address to be included in the rule. An IP address in dotted-decimal-format, e.g. 64.231.1.10.
dest-wildcard	A wildcard for the destination address. See *src-wildcard*
host dest	The address of a single destination host.
cos	Optional. Specifies that packets matched by this rule belong to a certain Class of Service (CoS). For detailed description of CoS configuration refer to chapter 7, "Link scheduler configuration" on page 68.
group	CoS group name.

If you place a *deny ip any any* rule at the top of an access control list profile, no packets will pass regardless of the other rules you defined.

Example: Create IP access control list entries

Select the access-list profile named WanRx and create some filter rules for it.

```
3210(cfg)#profile acl WanRx
3210(pf-acl)[WanRx]#permit ip host 62.1.2.3 host 193.14.2.11 cos Urgent
3210(pf-acl)[WanRx]#permit ip 62.1.2.3 0.0.255.255 host 193.14.2.11
3210(pf-acl)[WanRx]#permit ip 97.123.111.0 0.0.0.255 host 193.14.2.11
3210(pf-acl)[WanRx]#deny ip any any
3210(pf-acl)[WanRx]#exit
3210(cfg)#
```

Adding an ICMP filter rule to the current access control list profile

The command **permit** or **deny** are used to define an ICMP filter rule. Each ICMP filter rule represents an ICMP access of control list entry.

This procedure describes how to create an ICMP access control list entry that permits access

Mode: Profile access control list

Step	Command	Purpose
1	***node*****(pf-acl)[***name***]#permit icmp {***src src-wildcard* **| any | host** *src***} {***dest dest-wildcard* **| any | host** *dest***} [msg** *name* **| type** *type* **| type** *type* **code** *code***] [cos** *group***]**	Creates an ICMP access of control list entry that permits access defined according to the command options

This procedure describes how to create an ICMP access control list entry that denies access

Mode: Profile access control list

Step	Command	Purpose
1	***node*****(pf-acl)[***name***]#deny icmp {***src src-wildcard* **| any | host** *src***} {***dest dest-wildcard* **| any | host** *dest***} [msg** *name* **| type** *type* **| type** *type* **code** *code***] [cos** *group***]**	Creates an ICMP access of control list entry that denies access defined according to the command options

Where the syntax is as following:

Keyword	Meaning
src	The source address to be included in the rule. An IP address in dotted-decimal-format, e.g. 64.231.1.10.
src-wildcard	A wildcard for the source address. Expressed in dotted-decimal format this value specifies which bits are significant for matching. One-bits in the wildcard indicate that the corresponding bits are ignored. An example for a valid wildcard is 0.0.0.255, which specifies a class C network.
any	Indicates that IP traffic to or from all IP addresses is to be included in the rule.
host *src*	The address of a single source host.
dest	The destination address to be included in the rule. An IP address in dotted-decimal-format, e.g. 64.231.1.10
dest-wildcard	A wildcard for the destination address. See *src-wildcard*.
host *dest*	The address of a single destination host.
msg *name*	The ICMP message name. The following are valid message names: administratively-prohibited, alternate-address, conversion-error, dod-host-prohibited, dod-net-prohibited, echo, echo-reply, general-parameter-problem, host-isolated, host-precedence-unreachable, host-redirect, host-tos-redirect, host-tos-unreachable, host-unknown, host-unreachable, information-reply, information-request, mask-reply, mask-request, mobile-redirect, net-redirect, net-tos-redirect, net-tos-unreachable, net-unreachable, network-unknown, no-room-for-option, option-missing, packet-too-big, parameter-problem, port-unreachable, precedence-unreachable, protocol-unreachable, reassembly-timeout, redirect, router-advertisement, router-solicitation, source-quench, source-route-failed, time-exceeded, timestamp-reply, timestamp-request, traceroute, ttl-exceeded, unreachable
type *type*	The ICMP message type. A number from 0 to 255 (inclusive)
code *code*	The ICMP message code. A number from 0 to 255 (inclusive)
cos	Optional. Specifies that packets matched by this rule belong to a certain Class of Service (CoS). For detailed description of CoS configuration refer to chapter 7, "Link scheduler configuration" on page 68.
group	CoS group name.

If you place a *deny ip any any* rule at the top of an access-list profile, no packets will pass regardless of the other rules you defined.

Example: Create ICMP access control list entries

Select the access-list profile named WanRx and create the rules to filter all ICMP echo requests (as used by the ping command).

```
3210(cfg)#profile acl WanRx
3210(pf-acl)[WanRx]#deny icmp any any type 8 code 0
3210(pf-acl)[WanRx]#exit
3210(cfg)#
```

The same effect can also be obtained by using the simpler message name option. See the following example.

```
3210(cfg)#profile acl WanRx
3210(pf-acl)[WanRX]#deny icmp any any msg echo
3210(pf-acl)[WanRX]#exit
3210(cfg)#
```

Adding a TCP, UDP or SCTP filter rule to the current access control list profile

The commands **permit** or **deny** are used to define a TCP, UDP or SCTP filter rule. Each TCP, UDP or SCTP filter rule represents a respective access of control list entry.

This procedure describes how to create a TCP, UDP or SCTP access control list entry that permits access

Mode: Profile access control list

Step	Command	Purpose
1	***node***(**pf-acl**)[*name*]**#permit {tcp | udp | sctp}** {*src src-wildcard* **| any | host** *src*} **[{eq** *port* **| gt** *port* **| lt** *port* **| range** *from to*}] {*dest dest-wildcard* **| any | host** *dest*} **[{eq** *port* **| gt** *port* **| lt** *port* **| range** *from to*}] **[{cos** *group* **| cos-rtp** *group-data group-ctrl*}]	Creates a TCP, UDP or SCTP access of control list entry that permits access defined according to the command options

This procedure describes how to create a TCP, UDP or SCTP access control list entry that denies access

Mode: Profile access control list

Step	Command	Purpose
1	***node***(**pf-acl**)[*name*]**#deny {tcp | udp | sctp}** {*src src-wildcard* **| any | host** *src*} **[{eq** *port* **| gt** *port* **| lt** *port* **| range** *from to*}] {*dest dest-wildcard* **| any | host** *dest*} **[{eq** *port* **| gt** *port* **| lt** *port* **| range** *from to*}] **[{cos** *group* **| cos-rtp** *group-data group-ctrl*}]	Creates a TCP, UDP or SCTP access of control list entry that denies access defined according to the command options

Where the syntax is:

Keyword	Meaning
src	The source address to be included in the rule. An IP address in dotted-decimal-format, e.g. 64.231.1.10.
src-wildcard	A wildcard for the source address. Expressed in dotted-decimal format this value specifies which bits are significant for matching. One-bits in the wildcard indicate that the corresponding bits are ignored. An example for a valid wildcard is 0.0.0.255, which specifies a class C network.
any	Indicates that IP traffic to or from all IP addresses is to be included in the rule.
host src	The address of a single source host.
eq port	Optional. Indicates that a packets port must be equal to the specified port in order to match the rule.
lt port	Optional. Indicates that a packets port must be less than the specified port in order to match the rule.
gt port	Optional. Indicates that a packets port must be greater than the specified port in order to match the rule
range from to	Optional. Indicates that a packets port must be equal or greater than the specified from port and less than the specified to port to match the rule.
dest	The destination address to be included in the rule. An IP address in dotted-decimal-format, e.g. 64.231.1.10.
dest-wildcard	A wildcard for the destination address. See *src-wildcard*.
host dest	The address of a single destination host.
cos	Optional. Specifies that packets matched by this rule belong to a certain Class of Service (CoS). For detailed description of CoS configuration refer to chapter 7, "Link scheduler configuration" on page 68.
cos-rtp	Optional. Specifies that the rule is intended to filter RTP/RTCP packets. In this mode you can specify different CoS groups for data packets (even port numbers) and control packets (odd port numbers). Note: this option is only valid when protocol UDP is selected.
group	CoS group name.
group-data	CoS group name for RTP data packets. Only valid when the rtp option has been specified
group-ctrl	CoS group name for RTCP control packets. Only valid when the rtp option has been specified.

Example: Create TCP or UDP access control list entries

Select the access-list profile named WanRx and create the rules for:

Permitting any TCP traffic to host 193.14.2.10 via port 80, and permitting UDP traffic from host 62.1.2.3 to host 193.14.2.11 via any port in the range from 1024 to 2048.

```
3210(cfg)#profile acl WanRx
3210(pf-acl)[WanRx]#permit tcp any host 193.14.2.10 eq 80
3210(pf-acl)[WanRx]#permit udp host 62.1.2.3 host 193.14.2.11 range 1024 2048
3210(pf-acl)[WanRx]#exit
3210(cfg)#
```

Binding and unbinding an access control list profile to an IP interface

The command **use** is used to bind an access control list profile to an IP interface. This procedure describes how to bind an access control list profile to incoming packets on an IP interface

Mode: Profile access control list

Step	Command	Purpose
1	***node*(if-ip)[*if-name*]#use profile acl** *name* **in**	Binds access control list profile name to incoming packets on IP interface *if-name*

Where the syntax is:

Keyword	Meaning
if-name	The name of the IP interface to which an access control list profile gets bound
name	The name of an access control list profile that has already been created using the profile acl command. This argument must be omitted in the **no** form
in	Specifies that the access control list profile applies to incoming packets on this interface.
out	Specifies that the access control list applies to outgoing packets on this interface.

The **no** form of the **use** command is used to unbind an access control list profile from an interface. When using this form the name of an access control list profile, represented by the *name* argument above, is not required. This procedure describes how to unbind an access control list profile to incoming packets on an IP interface

Mode: Interface

Step	Command	Purpose
1	***node*(if-ip)[*if-name*]#no use profile acl in**	Unbinds access control list profile for incoming packets on IP interface *if-name*

Where the syntax is:

Keyword	Meaning
if-name	The name of the IP interface to which an access control list profile gets bound
in	Specifies that the access control list profile applies to incoming packets on this interface.
out	Specifies that the access control list applies to outgoing packets on this interface.

Thus for each IP interface only one incoming and outgoing access control list can be active at the same time.

Example: Bind and unbind an access control list entries to an IP interface

Bind an access control list profile to incoming packets on the interface *wan* in the IP router context.

```
3210(cfg)#context ip router
3210(cfg-ip)[router]#interface wan
3210(cfg-if)[wan]#use profile acl WanRx in
```

Unbind an access control list profile from an interface.

```
3210(cfg)#context ip router
3210(cfg-ip)[router]#interface wan
3210(cfg-if)[wan]#no use profile acl in
```

Note When unbinding an access control list profile the *name* argument is not required, since only one incoming and outgoing access control list can be active at the same time on a certain IP interface.

Displaying an access control list profile

The **show profile acl** command displays the indicated access control list profile. If no specific profile is selected all installed access control list profiles are shown. If an access control list is linked to an IP interface the number of matches for each rule is displayed. If the access control list profile is linked to more than one IP interface, it will be shown for each interface.

This procedure describes how to display a certain access control list profile

Mode: Administrator execution or any other mode, except the operator execution mode

Step	Command	Purpose
1	***node*#show profile acl** *name*	Displays the access control list profile *name*

Example: Displaying an access control list entries

The following example shows how to display the access control list profile named WanRx.

```
3210#show profile acl WanRx
IP access-list WanRx. Linked to router/wan/in.
    deny icmp any any msg echo
    permit ip 62.1.2.3 0.0.255.255 host 193.14.2.11
    permit ip 97.123.111.0 0.0.0.255 host 193.14.2.11
    permit tcp any host 193.14.2.10 eq 80
    permit udp host 62.1.2.3 host 193.14.2.11 range 1024 2048
    deny ip any any
```

Debugging an access control list profile

The **debug acl** command is used to debug the access control list profiles during system operation. Use the **no** form of this command to disable any debug output.

This procedure describes how to debug the access control list profiles

Mode: Administrator execution or any other mode, except the operator execution

Step	Command	Purpose
1	**node#debug acl**	Enables access control list debug monitor

This procedure describes how to activate the debug level of an access control list profiles for a specific interface.

Mode: Interface

Step	Command	Purpose
1	***node*(cfg)#context ip router**	Selects the IP router context
2	***node*(ctx-ip)[router]#interface** *if-name*	Selects IP interface *if-name* for which access control list profile shall be debugged
3	***node*(if-ip)[*if-name*]#debug acl {in | out} [level]**	Enables access control list debug monitor with a certain debug level for the selected interface *if-name*

Where the syntax is:

Keyword	Meaning
if-name	The name of the IP interface to which an access control list profile gets bound
level	The detail level. Level 0 disables all debug output, level 7 shows all debug output.
in	Specifies that the settings for incoming packets are to be changed.
out	Specifies that the settings for outgoing packets are to be changed.

Example: Debugging access control list profiles

The following example shows how to enable debugging for incoming traffic of access control lists on interface *wan*. On level 7 all debug output is shown.

```
3210(cfg)#context ip router
3210(cfg-ip)[router]#interface wan
3210(cfg-if)[wan]#debug acl in 7
```

The following example enables the debug monitor for access control lists globally.

```
3210#debug acl
```

The following example disables the debug monitor for access control lists globally.

```
3210#no debug acl
```

Examples

Denying a specific subnet

Figure 15 shows an example in which a server attached to network 172.16.1.0 shall not be accessible from outside networks connected to IP interface *lan* of the OnSite device. To prevent access, an incoming filter rule named *Jamming* is defined, which blocks any IP traffic from network 172.16.2.0 and has to be bound to IP interface *lan*.

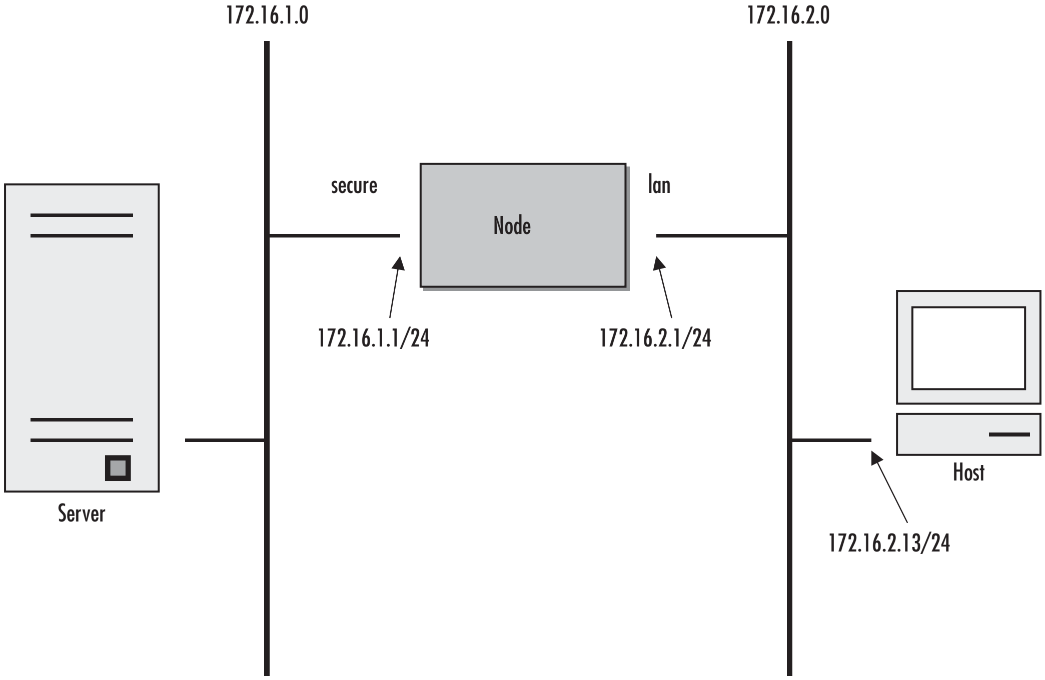


Figure 15. Deny a specific subnet on an interface

The commands that have to be entered are listed below. The commands access the OnSite device via a Telnet session running on a host with IP address 172.16.2.13, which accesses the OnSite via IP interface *lan*.

```
172.16.2.1>enable
172.16.2.1#configure
172.16.2.1(cfg)#profile acl Jamming
172.16.2.1(pf-acl)[Jamming]#deny ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
172.16.2.1(pf-acl)[Jamming]#permit ip any any
172.16.2.1(pf-acl)[Jamming]#exit
172.16.2.1(cfg)#context ip router
172.16.2.1(cfg-ip)[router]#interface lan
172.16.2.1(if-ip)[lan]#use profile acl Jamming in
172.16.2.1(if-ip)[lan]#exit
172.16.2.1(cfg-ip)#copy running-config startup-config
```

Chapter 7 Link scheduler configuration

Chapter contents

Introduction

This chapter describes how to use and configure the OnSite Quality of Service (QoS) features. Refer to 6, "Access control list configuration" on page 54 for more information on the use of access control lists.

This chapter includes the following sections:

- Quick references (see page 73)
- Packet Classification (see page 75)
- Assigning bandwidth to traffic classes (see page 73)
- Link scheduler configuration task list (see page 74)

QoS in networking refers to the capability of the network to provide a better service to selected network traffic. This chapter shows you how to configure the OnSite router to best use the access link.

In many applications you can gain a lot by applying the minimal configuration found in the quick reference section, but read sections "Applying scheduling at the bottleneck" and "Using traffic classes" first to understand the paradox of why we apply a rate-limit to reduce delay and what a "traffic-class" means.

Configuring access control lists

Packet filtering helps to control packet movement through the network. Such control can help to limit network traffic and to restrict network use by certain users or devices. To permit or deny packets from crossing specified interfaces, the OnSite 3210 provides access control lists.

An access control list is a sequential collection of permit and deny conditions that apply to packets on a certain interface. Access control lists can be configured for all routed network protocols (IP, ICMP, TCP, UDP, and SCTP) to filter the packets of those protocols as the packets pass through an OnSite 3210. The 3210 tests packets against the conditions in an access list one by one. The first match determines whether the OnSite 3210 accepts or rejects the packet. Because the OnSite 3210 stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the software rejects the address.

For information and examples on how configure access control lists, refer to chapter 6, "Access control list configuration" on page 54.

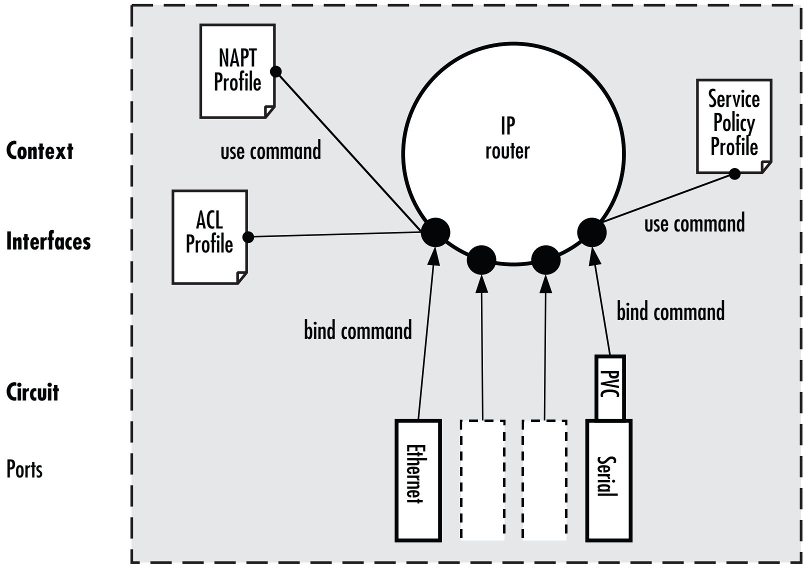


Figure 16. IP context and related elements

Configuring quality of service (QoS)

In the OnSite 3210, the link scheduler enables the definition of QoS profiles for network traffic on a certain interface, as shown in figure 16. QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Frame Relay, Ethernet and 802.x type networks, and IP-routed networks. In particular, QoS features provide improved and more predictable network service by providing the following services:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

Applying scheduling at the bottleneck

When an OnSite acts as an access router, the access link is the point where intelligent use of scarce resources really makes a difference. Frequently, the access link modem is outside of the OnSite and the queueing would happen in the modem, which does not distinguish between packet types. To improve QoS, you can configure the OnSite to send no more data to the Internet than the modem can carry. This keeps the modem's queue empty and gives the OnSite control over which packet is sent over the access link at what time.

Using traffic classes

The link scheduler needs to distinguish between different types of packets. We refer to those types as "traffic-classes". You can think of the traffic-class as if every packet in the OnSite has a tag attached to it on which the classification can be noted. The access control list "stage" (ACL) can be used to apply such a traffic-class name to some type of packet based on its IP-header filtering capabilities. The traffic-class tags exist only inside the OnSite router, but layer 2 priority bits (802.1pq class-of-service) and IP header type-of-service bits (TOS field) can be used to mark a specific packet type for the other network nodes. By default the traffic-class tag is empty. Refer to figure 17 on page 71 when using the ACL to classify traffic. It illustrates the sequence of processing stages every routed packet passes. Only stages that have been installed in the data path with a “use profile...” statement in the corresponding interface configuration are present. Both an input direction ACL on the receiving interface as well as an output ACL on the transmitting interface can be used to classify a packet for special handling by the output link scheduler on the transmit interface. But as visible from the figure no ACL can be used for an input link scheduler.

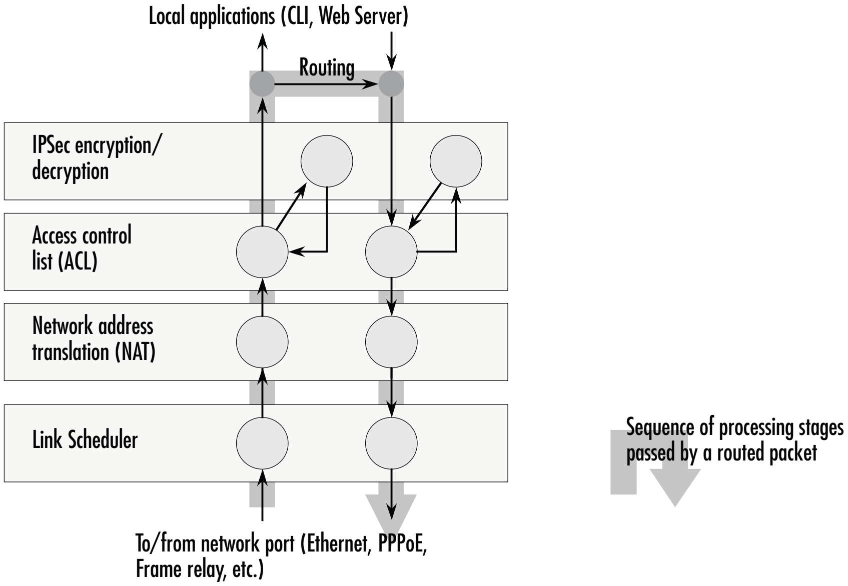

Local applications (CLI, Web Server)
Routing
IPSec encryption/ decryption
Access control list (ACL)
Network address translation (NAT)
Link Scheduler
To/from network port (Ethernet, PPPoE, Frame relay, etc.)
Sequence of processing stages passed by a routed packet

Figure 17. Packet routing in OnSite

The QoS features in OnSite are a combination of an access control list (used for packet classification) and a service-policy profile (used by the link arbiter to define the arbitration mode and the order in which packets of different classes are served).

Introduction to Scheduling

Scheduling essentially means to determine the order in which packets of the different traffic-classes are served. The following sections describe the ways this arbitration can be done.

Priority

One way of ordering packets is to give priority to one traffic-class and to serve the other traffic-classes when the first has nothing to send. OnSite uses the priority scheme to make sure that voice packets generated by the OnSite will experience as little delay as possible.

Weighted fair queuing (WFQ)

This arbitration method assures a given minimal bandwidth for each source. An example: you specify that traffic-class A gets three times the bandwidth of traffic-class B. So A will get a minimum of 75% and B will get a minimum of 25% of the bandwidth. But if no class A packets are waiting B will get 100% of the bandwidth.

Each traffic-class is in fact assigned a *relative* weight, which is used to share the bandwidth among the currently active classes. Patton recommends that you specify the weight as percent which is best readable.

Shaping

There is another commonly used way to assign bandwidth. It is called *shaping* and it makes sure that each traffic-class will get just as much bandwidth as configured and not more. This is useful if you have subscribed to a service that is only available for a limited bandwidth e.g. low delay. When connecting the OnSite to a *DiffServ* network shaping might be a required operation.

Burst tolerant shaping or wfq

For weighted fair queuing and shaping there is a variation of the scheduler that allows to specify if a traffic class may temporarily receive a higher rate as long as the average stays below the limit. This burstiness measure allows the network to explicitly assign buffers to bursty sources.

When you use shaping on the access link the shaper sometimes has the problem that multiple sources are scheduled for the same time - and therefore some of them will be served too late. If the rate of every source had to strictly obey its limit, all following packets would also have to be delayed by the same amount, and further collisions would reduce the achieved rate even further. To avoid this effect, the OnSite shaper assumes that the burstiness needed for sources to catch up after *collisions* is implicitly allowed. Future versions of OnSite might allow setting the burst rate and bursting size if more control over its behavior is considered necessary.

Burst tolerance has a different effect when used with *weighted fair queuing*. Think of it as a higher initial rate when a source device starts transmitting data packets. This allows giving a higher *weight* to short data transfers. This feature is sometimes referred to as a *service curve*.

Hierarchy

An arbiter can either use wfq *or* shaping to determine which source to serve next. If you want the scheduler to follow a combination of decision criteria you can combine different schedulers in hierarchy to do a multi-level arbitration.Hierarchical scheduling is supported in OnSite with service-policy profiles used inside service-policy profiles.In figure 18 an example of hierarchical scheduling is illustrated. The 1st level arbiter *Level_1* uses weighted fair queuing to share the bandwidth among source classes VPN, Web and incorporates the traffic from the 2nd level arbiter *Low_Priority*, which itself uses shaping to share the bandwidth among source classes Mail and Default.

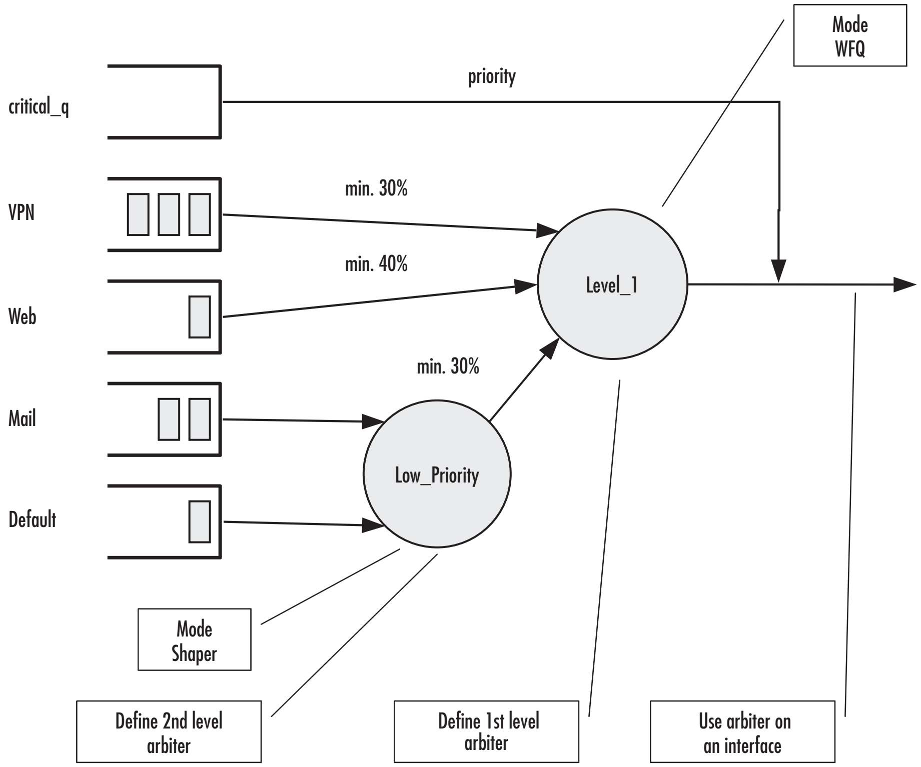


Figure 18. Example of Hierarchical Scheduling

Quick references

The following sections provide a minimal "standard" link scheduler configuration for the case where a (DSL/cable) modem link is shared for all traffic. You will also find a command cross reference list for administrators familiar with Cisco's IOS QoS features and having to become acquainted with OnSite QoS configuration.

Setting the modem rate

To match the data multiplexing of different traffic types to the capacity of the access link is the most common application of the OnSite link scheduler.

1. Create a minimal profile.

```
profile service-policy modem-512
  rate-limit 512 header-length 20 atm-modem
  source traffic-class critical_q
    priority
```

2. Apply the profile just created to the interface connected to the modem.

```
context ip
interface wan
  use profile service-policy modem-512 out
```

Some explanations:

- “modem-512” is the title of the profile which is referred to when installing the scheduler
- “rate-limit 512” allows no more than 512 kbit/sec to pass which avoids queueing in the modem.
- “header-length 20” specifies how many framing bytes are added by the modem to “pack” the IP packet on the link. The framing is taken into account by the rate limiter.
- “atm-modem” tells the rate limiter that the access link is ATM based. This option includes the ATM overhead into the rate limit calculation. Please add 8 bytes to the header-length for AAL5 in this case.
- “source traffic-class” enters a sub-mode where the specific handling for a traffic-class is described. The list of sources in the service-policy profile tells the arbiter which “traffic sources” to serve.
- “critical_q” is the traffic-class for the higheest priority packet streams that you have selected.
- “priority” means that packet of the source being described are always passed on immediately, packets of other classes follow later if the rate limit permits.

Command cross reference

Comparing OnSite with the Cisco IOS QoS software command syntax often helps administrators to straightforwardly configure OnSite devices. In table 11 the Cisco IOS Release 12.2 QoS commands are in contrast with the respective OnSite commands.

Table 11. Command cross reference

Action	IOS command	OnSite command
Specifies the name of the policy map or profile to be created or modified.	**policy-map** policy-map-name	**profile service-policy** *profile-name*
Specifies the name of the class map or class to be created.	**class-map** *class-map-name*	**source traffic-class** *class-name*
For IOS specifies average or peak bit rate shaping. for the OnSite assigns the average bit rate to a source.	**shape** {average | peak} *cir* [bc] [be]	**rate** *bit-rate*
For IOS specifies or modifies the bandwidth allocated for a class belonging to a policy map. Percent defines the percentage of available bandwidth to be assigned to the class. for the OnSite assigns the weight of the selected source (only used with wfq).	**bandwidth** {*bandwidth-kbps* | **percent** *percent*}	**share** *percent-of-bandwidth*

Link scheduler configuration task list

To configure QoS features, perform the tasks described in the following sections. Depending on your requirements some of the tasks are required while other tasks are optional.

- Defining the access control list profile
- Creating a service-policy profile (see page 77)
- Specifying the handling of traffic-classes (see page 79)
- Devoting the service policy profile to an interface (see page 84)
- Displaying link arbitration status (see page 85)

- Displaying link scheduling profile information (see page 85)
- Enable statistics gathering (see page 85)

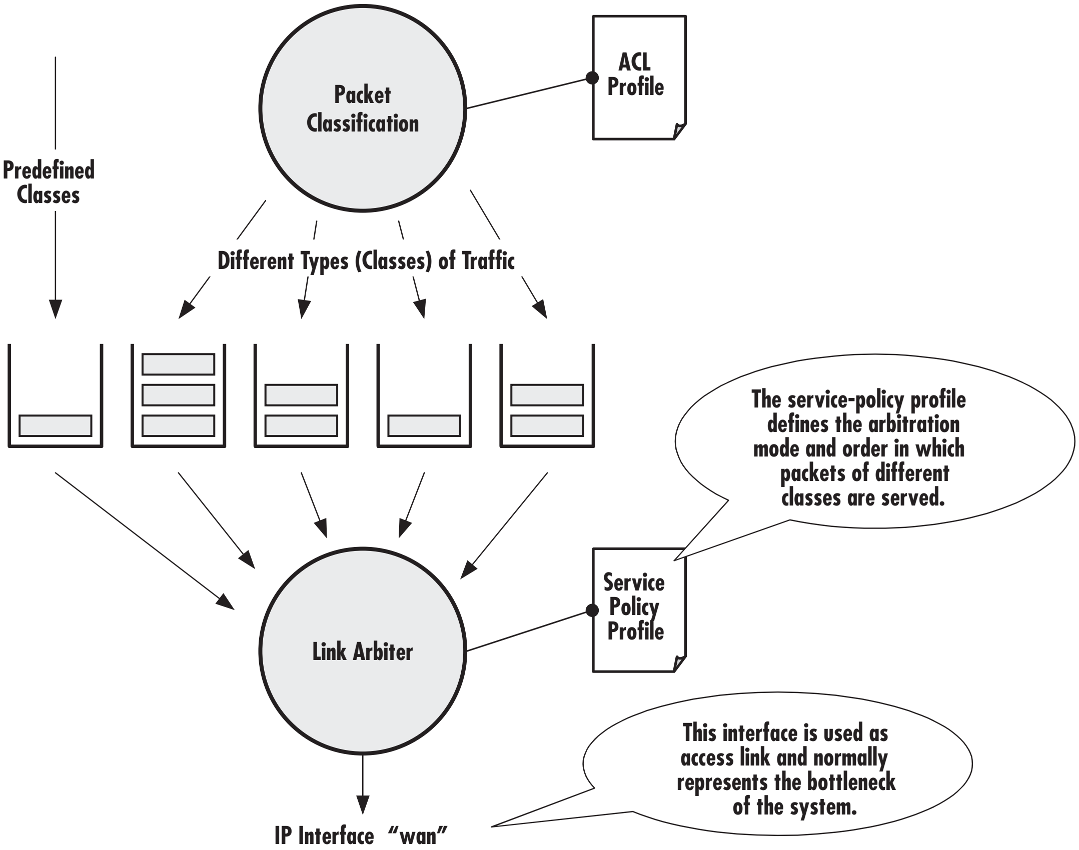

Packet Classification
ACL Profile
Predefined Classes
Different Types (Classes) of Traffic
The service-policy profile defines the arbitration mode and order in which packets of different classes are served.
Service Policy Profile
Link Arbiter
This interface is used as access link and normally represents the bottleneck of the system.
IP Interface "wan"

Figure 19. Elements of link scheduler configuration

Defining the access control list profile

Packet classification

The basis for providing any QoS lies in the ability of a network device to identify and group specific packets. This identification process is called *packet classification*. In OnSite access control lists are used for packet classification.

An access control list in OnSite consists of a series of packet descriptions like "addressed to xyz". Those descriptions are called rules. For each packet the list of descriptions is sequentially checked and the first rule that matches decides what happens to the packet. As far as filtering is concerned the rule decides if the packet is discarded ("deny") or passed on ("permit"). You can also add a traffic-class to the rule and if this rule is the first matching rule for a packet it is tagged with the traffic-class name.

Some types of packets you do not have to tag with ACL. Voice and data packets from of for the OnSite itself are automatically tagged with predefined traffic-class names: Predefined internal classes for data are:

- **local-default**—All other packets that originate from the OnSite itself.
- **default**—All traffic that has not otherwise been labeled.

Creating an access control list

The procedure to create an access control list is described in detail in chapter 6, "Access control list configuration" on page 54.

At this point a simple example is given, that shows the necessary steps to tag any outbound traffic from a Web server. The scenario is depicted in figure 20. The IP address of the Web server is used as source address in the permit statement of the IP filter rule for the access control list.

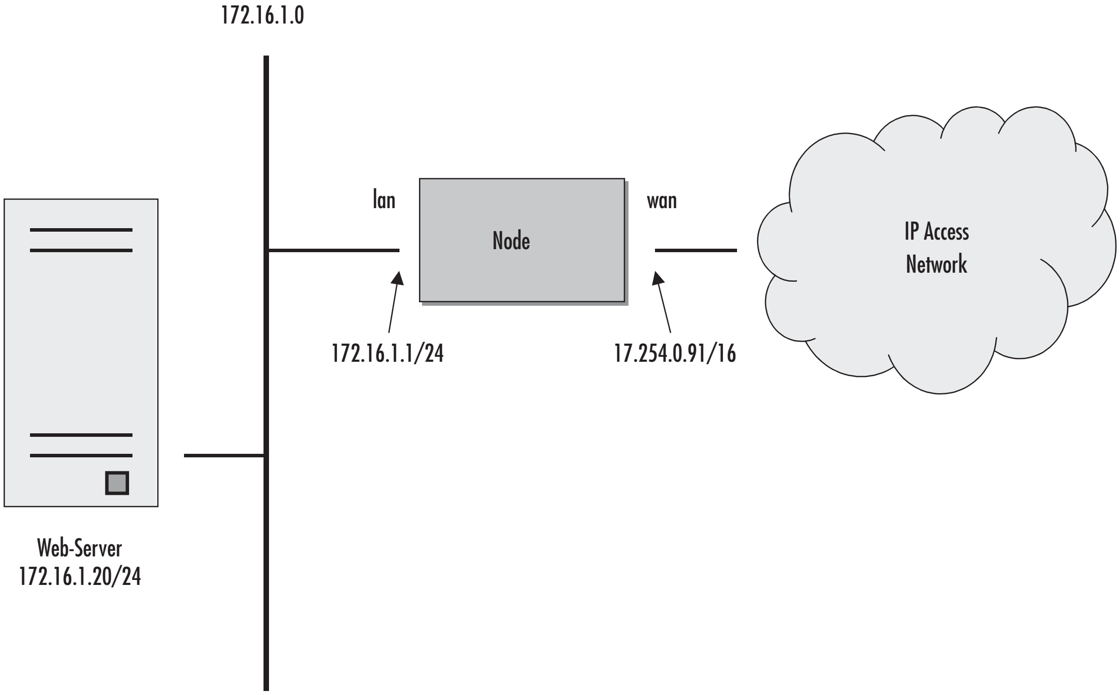


Figure 20. Scenario with Web server regarded as a single source host

A new access control list has to be created. In the example above, the traffic-class that represents outbound Web related traffic is named *Web*.

Access control list have an implicit "deny all" entry at the very end, so packets that do not match the first criteria of outbound Web related traffic will be dropped. That is why a second access control list entry—one that allows all other traffic—is necessary.

This procedure describes creating an access control list for tagging web traffic from the single source host at a certain IP address.

Mode: Configure

Step	Command	Purpose
1	***node*(cfg)#profile acl** *name*	Creates a new access control list profile named *name*
2	***node*(pf-acl)[*name*]#permit ip host ip-address any traffic-class** *class-name*	Creates an IP access control list entry that permits access for host at IP address *ip-address*, and specifies that packets matched by this rule belong to the traffic-class *class-name*.
3	***node*(pf-acl)[*name*]#permit ip any** *any*	Creates an IP access control list entry that permits IP traffic to or from all IP addresses.

Example: Defining the access control list profile

In the example below a new access control list profile named *Webserver* is created. In addition an IP access control list entry that permits access for host at IP address *172.16.1.20*, and specifies that packets matched by this rule belong to the traffic-class *Web* is added. Finally an IP access control list entry that permits IP traffic to or from all IP addresses is added to the access control list.

```
3210(cfg)#profile acl Webserver
3210(pf-acl)[Webserv~]#permit ip host 172.16.1.20 any traffic-class Web
3210(pf-acl)[Webserv~]#permit ip any any
```

After packet classification is done using access control lists, the link arbiter needs rules defining how to handle the different traffic-classes. For that purpose you create a service-policy profile. The service policy profile defines how the link arbiter has to share the available bandwidth among several traffic classes on a certain interface.

Creating a service policy profile

The service-policy profile defines how the link scheduler should handle different traffic-classes. The overall structure of the profile is as follows:

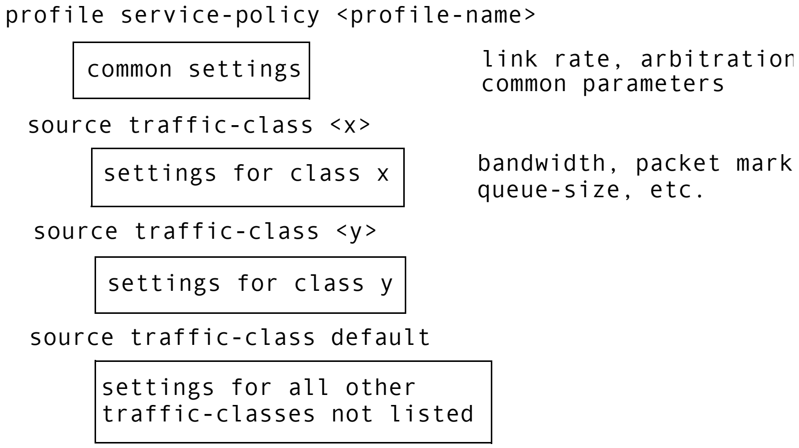


Figure 21. Structure of a Service-Policy Profile

The template shown above specifies an arbiter with three inputs which we call “sources”: x, y and “default”. The traffic-class “default” stands for all other packets that belong neither to traffic-class x nor y. There is no limit on the number of sources an arbiter can have.

Example: Creating a service policy profile

The following example shows how to create a top service-policy profile named *sample*. This profile does not include any hierarchical sub-profiles. The bandwidth of the outbound link is limited to 512 kbps therefore the interface rate-limit is set to 512. In addition weighted fair queuing (wfq) is used as arbitration scheme among the source classes.

```
profile service-policy sample
rate-limit 512
mode wfq
source traffic-class Web
share 30
source traffic-class local-default
share 20
source traffic-class default
queue-limit 40
share 50
```

The first line specifies the name of the link arbiter profile to configure. On the second line the global bandwidth limit is set. The value defining the bandwidth is given in kilobits per second. Each service-policy profile must have a “rate-limit” except if no scheduling is used i.e. the link scheduler is used for packet marking only (like setting the TOS byte).

How the bandwidth on an IP interface is shared among the source classes is defined on the third line. The mode command allows selecting between the weighted fair queuing and shaping arbitration mode. The default mode is wfq - the command shown above can therefore be omitted.

The following lines configure the source traffic-classes. When using weighted fair queuing (wfq) each user-specified source traffic-class needs a value specifying its share of the overall bandwidth. For this purpose the share command is used, which defines the relative weights of the source traffic-classes and policies.

At a some point the source traffic-class *default* must be listed. This class must be present, because it defines how packets, which do not belong to any of the traffic-classes listed in the profile are to be handled. When all listed "traffic-classes" have "priority" the handling of the remaining traffic is implicitly defined and the "default" section can be omitted. Similarly if no scheduling is used i.e. the link scheduler is used for packet marking only (e.g. setting the TOS byte) the "default" section can also be omitted.

The table below shows the basic syntax of the service-policy profile structure:

Mode: Configure

Step	Command	Purpose
1	***node***(**cfg**)**# profile service-policy** *name*	Creates a new service policy profile named name
2	***node***(**pf-srvpl)**[*name*]**#rate-limit** *value*	Limits global interface rate to value in kbps. Be aware, that the actual rate-limit on a given interface has to be defined for reliable operation.
3	***node***(**pf-srvpl)**[*name*]**#mode {shaper | wfq}**	Sets the arbitration scheme to mode shaper or weighted fair queuing (wfq). If not specified wfq is default.
4	***node***(**pf-srvpl)**[*name*]**#source {traffic-class | policy}** *src-name*	Enters source configuration mode for a traffic-class or a hierarchical lower level service-policy profile named *src-name*.
5	***node (src)[src-name]...***	At this point the necessary commands used to specify the handling of the traffic-class(es) have to be entered.
6	***node (src)[src-name]exit***	Leaves the source configuration mode (optional)
7	***node***(**pf-srvpl)*****[name]*****#...**	Repeat steps 4 to 6 for all necessary source classes or lower level service policy profiles.
8	***node(pf-srvpl)[name]#exit***	Leaves the service-policy profile mode

Specifying the handling of traffic-classes

Several commands are available to specify what happens to a packet of a specific traffic-class.

Defining fair queuing weight

The command **share** is used with wfq link arbitration to assign the weight to the selected traffic-class. When defining a number of source classes, the values are relative to each other. It is recommended to split 100—which can be read as 100%—among all available source classes, e.g. with 20, 30 and 50 as value for the respective share commands, which represent 20%, 30% and 50%.

Mode: Source

Command	Purpose
***node*(src)[*name*]#share** *percentage*	Defines fair queuing weight (relative to other sources) to *percentage* for the selected class or policy *name*

Defining the bit-rate

The command **rate** is used with shaper link arbitration to assign the (average) bit-rate to the selected source. When enough bandwidth is available each source will exactly receive this bandwidth (but no more), when overloaded the shaper will behave like a wfq arbiter. Bit-rate specification for shaper (kilobits).

Mode: Source

Command	Purpose
***node*(src)[name]#rate** [*kilobits* | **remaining]**	Defines the (average) bit-rate to the selected in kbps *kilobits* or as *remaining* if a second priority source is getting the unused bandwidth for the selected class or policy *name*

Defining absolute priority

This command **priority** can only be applied to classes, but not to lower level polices. The class is given absolute priority effectively bypassing the link arbiter. Care should be taken, as traffic of this class may block all other traffic. The packets given “priority” are taken into account by the “rate-limit”. Use the command **police** to control the amount of “priority” traffic.

Mode: Source

Command	Purpose
node(src)[*name*]#priority	Defines absolute priority effectively bypassing the link arbiter for the selected class or policy *name*

Defining the maximum queue length

The command **queue-limit** specifies the maximum number of packets queued for the class *name*. Excess packets are dropped. Used in “class” mode—queuing only happens at the leaf of the arbitration hierarchy tree. The **no** form of this command reverts the queue-limit to the internal default value, which depends on your configuration.

Mode: Source

Command	Purpose
***node*(src)[*name*]#queue-limit** *number-of-packets*	Defines the maximum number of packets queued for the selected class or policy *name*

Specifying the type-of-service (TOS) field

The **set ip tos** command specifies the type-of-service (TOS) field value applied to packets of the class *name*. TOS and DSCP markings cannot be used at the same time. The **no** form of this command disables TOS marking.

The type-of-service (TOS) byte in an IP header specifies precedence (priority) and type of service (RFC791, RFC1349). The precedence field is defined by the first three bits and supports eight levels of priority. The next four bits—which are set by the **set ip tos** command—determine the type-of-service (TOS).

Table 12. TOS values and their meaning

TOS Value	OnSite Value	Meaning
1000	8	Minimize delay.
0100	4	Maximize throughput.
0010	2	Maximizes reliability.
0001	1	Minimize monetary costs.
0000	0	All bits are cleared, normal service, "default TOS".

Historically those bits had distinct meanings but since they were never consistently applied routers will ignore them by default. Nevertheless you can configure your routers to handle specific TOS values and OnSite allows you to inspect the TOS value in the ACL rules and to modify the TOS value with the link scheduler **set ip tos** command.

Mode: Source

Command	Purpose
***node*(src)[*name*]#set ip tos** *value*	Defines the type-of-service (TOS) value applied to packets of for the selected class or policy *name*. Standard ToT values are 0, 1, 2, 4, and 8, as given in table 12 on page 81, but any number from 0 to 15 can be configured.

Specifying the precedence field

The **set ip precedence** command specifies the precedence marking applied to packets of the class name. Precedence and DSCP markings cannot be used at the same time.

The type-of-service (TOS) byte in an IP header specifies precedence (priority) and type of service (RFC791, RFC1349). The precedence field is defined by the first three bits and supports eight levels of priority. The lowest priority is assigned to 0 and the highest priority is 7.

The **no** form of this command disables precedence marking.

Mode: Source

Command	Purpose
***node*(src)[*name*]#set ip precedence** *value*	Defines the precedence marking value applied to packets of for the selected class or policy *name*. The range for *value* is from 0 to 7, but only values from 0 to 5 should be used.

Specifying differentiated services codepoint (DSCP) marking

Differentiated services enhancements to the Internet protocol are intended to enable the handling of "traffic-classes" throughout the Internet. In this context the IP header TOS field is interpreted as something like a “traffic-class” number called. With OnSite you can inspect the DSCP value in the ACL rules and modify the DSCP value with the link scheduler **set ip dscp** command.

Note When configuring service differentiation on the OnSite router, ensure that codepoint settings are arranged with the service provider.

The command **set ip dscp** sets the DS field applied to packets of the class *name*. Additionally shaping may be needed to make the class conformant. The **no** form of this command disables packet marking.

Mode: Source

Command	Purpose
***node*(src)[*name*]#set ip dscp** *value*	Defines the Differentiated Services Codepoint value applied to packets of for the selected class or policy *name*. The range for *value* is from 0 to 63.

Specifying layer 2 marking

The IEEE ratified the 802.1p standard for traffic prioritization in response to the realization that different traffic classes have different priority needs. This standard defines how network frames are tagged with user priority levels ranging from 7 (highest priority) to 0 (lowest priority). 802.1p-compliant network infrastructure devices, such as switches and routers, prioritize traffic delivery according to the user priority tag, giving higher priority frames precedence over lower priority or non-tagged frames. This means that time-critical data can receive preferential treatment over non-time-critical data.

Under 802.1p, a 4-byte Tag Control Info (TCI) field is inserted in the Layer 2 header between the Source Address and the MAC Client Type/Length field of an Ethernet Frame. Table 13 lists the tag components.

Table 13. Traffic control info (TCI) field

Tag Control Field	Description
Tagged Frame Type Interpretation	Always set to 8100h for Ethernet frames (802.3ac tag format)
3-Bit Priority Field (802.1p)	Value from 0 to 7 representing user priority levels (7 is the highest)
Canonical	Always set to 0
12-Bit 802.1Q VLAN Identifier	VLAN identification number

802.1p-compliant infrastructure devices read the 3-bit user priority field and route the frame through an internal buffer/queue mapped to the corresponding user priority level.

The command **set layer2 cos** specifies the layer 2 marking applied to packets of this class by setting the 3-bit priority field (802.1p). The **no** form of this command disables packet marking.

Please note that the Ethernet port must be configured for 802.1Q framing. Standard framing has no class-of-service field.

Mode: Source

Command	Purpose
***node*(src)[*name*]#set layer2 cos** *value*	Defines the Class-Of-Service value applied to packets of for the selected class or policy *name*. The range for *value* is from 0 to 7.

Defining random early detection

The command **random-detect** is used to request random early detection (RED). When a queue carries lots of TCP transfers that last longer than simple web requests, there is a risk that TCP flow-control might be inefficient. A burst-tolerance index between 1 and 10 may optionally be specified (exponential filter weight). The **no** form of this command reverts the queue to default "tail-drop" behavior.

Mode: Source

Command	Purpose
node(**src)**[*name*]**#random-detect** {*burst-tolerance*}	Defines random early detection (RED) for queues of for the selected traffic-class or policy *name*. The range for the optional value *burst-tolerance* is from 1 to 10.

Discarding Excess Load

The command **police** controls traffic arriving in a queue for class *name*. The value of the first argument *average-kilobits* defines the average permitted rate in kbps, the value of the second argument *kilobits-ahead* defines the tolerated burst size in kbps ahead of schedule. Excess packets are dropped.

This procedure describes defining discard excess load

Mode: Source

Command	Purpose
node(**src)**[*name*]**#police** *average-kilobits* **burst-size** *kilobits-ahead*	Defines how traffic arriving in a queue for the selected class or policy *name* has to be controlled. The value *average-kilobits* for average rate permitted is in the range from 0 to 10000 kbps. The value *kilobits-ahead* for burst size tolerated ahead of schedule is in the range from 0 to 10000.

Devoting the service policy profile to an interface

Any service policy profile needs to be bound to a certain IP interface to get activated. According the terminology of OnSite a service policy profile is used on a certain IP interface, as shown in figure 22.

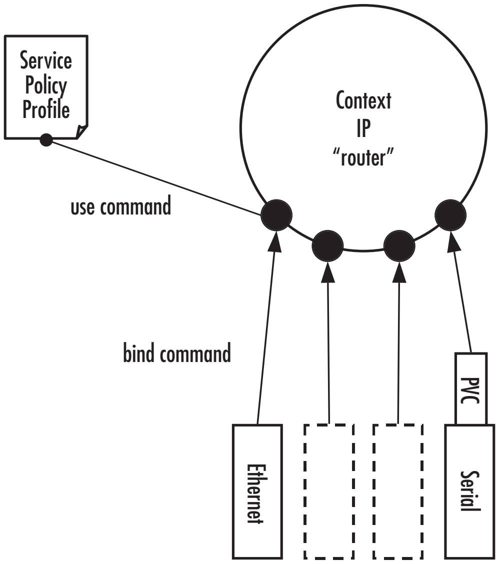


Figure 22. Using a Service Policy Profile on an IP Interface

Therefore the **use profile service-policy** command allows attaching a certain service policy profile to an IP interface that is defined within the IP context. This command has an optional argument that defines whether the service policy profile is activated in receive or transmit direction.

Providers may use input shaping to improve downlink voice jitter in the absence of voice support. The default setting **no service-policy** sets the interface to FIFO queuing.

Mode: Interface

Step	Command	Purpose
1	***node*(if-ip)[*if-name*]#use profile service-policy** *name* **{in | out}**	Applies the service policy profile *name* to the selected interface *if-name*. Depending on selecting the optional **in** or **out** argument the service policy profile is active on the receive or transmit direction. Be aware that service policy profiles can only be activated on the transmit direction at the moment.

Example: Devoting the service policy profile to an interface

The following example shows how to attach the service policy profile *Voice_Prio* to the IP interface wan that is defined within the IP context for outgoing traffic.

```
3210>enable
3210#configure
3210(cfg)#context ip router
3210(ctx-ip)[router]#interface wan
3210(if-ip)[wan]#use profile service-policy Voice_Prio out
```

Displaying link arbitration status

The **show service-policy** command displays link arbitration status. This command supports the optional argument **interface** that select a certain IP interface. This command is available in the operator mode.

Mode: Operator execution

Step	Command	Purpose
1	***node*>show service-policy {interface** *name***}**	Displays the link arbitration status

Example: Displaying link arbitration status

The following example shows how to display link arbitration status information.

```
3210>show service-policy
available queue statistics
--------------------------
default
   - packets in queue: 10
```

Displaying link scheduling profile information

The **show profile service-policy** command displays link scheduling profile information of an existing service-policy profile. This command is only available in the administrator mode.

Mode: Administrator execution

Step	Command	Purpose
1	***node*#show profile service-policy** *name*	Displays link scheduling profile information of the service-policy profile *name*

Example: Displaying link scheduling profile information

The following example shows how to display link scheduling profile information of an existing service-policy profile *VoIP_Layer2_CoS*.

```
3210#show profile service-policy VoIP_Layer2_CoS
VoIP_Layer2_CoS
  default (mark layer 2 cos -1)
```

Enable statistics gathering

Using the **debug queue statistics** commands enables statistic gathering of link scheduler operations.

The command has optional values (in the range of 1 to 4) that define the level of detail (see table 14).

Table 14. Values defining detail of the queuing statistics

Optional Value	Implication on Command Output
0	Statistic gathering is switched off
1	Display amount of packets *passed* (did not have to wait), *queued* (arrived earlier than rate permitted) and *discarded* (due to overflowing queue)
2	Also collects byte counts for the categories listed above
3	Also keeps track of the peek queue lengths ever reached since the last configuration change or reload
4	Adds delay time monitoring

Note The debug features offered by OnSite require the CPU resources of your OnSite router. Therefore do not enable statistic gathering or other debug features if it is not necessary. Disable any debug feature after use with the **no** form of the command.

You can enable queue statistics for all queues of a link scheduler by placing the **debug queue statistics** command in the profile header. Queue statistics are reset whenever the configuration is changed or OnSite is reloaded.

Mode: Source

Step	Command	Purpose
1	***node***(**src**)[*name*]#**debug queue statistics** *level*	Enables statistic gathering for the selected class or policy *name*. The optional argument *level*, which is in the range from 1 to 4, defines the verbosity of the command output.

Example: Enable statistics gathering for all queues of a profile

The following example shows how to enable statistic gathering for all traffic-classes

```
3210>enable
3210#configure
3210(cfg)#profile service-policy sample
3210(pf-srvpl)[sample]#debug queue statistics 4
```

Chapter 8 LEDs status and monitoring

Chapter contents

Status LEDs

This chapter describes OnSite gateway router front panel LEDs. Figure 23 shows OnSite 3210 Series LEDs. LED definitions are listed in table 15 on page 88.

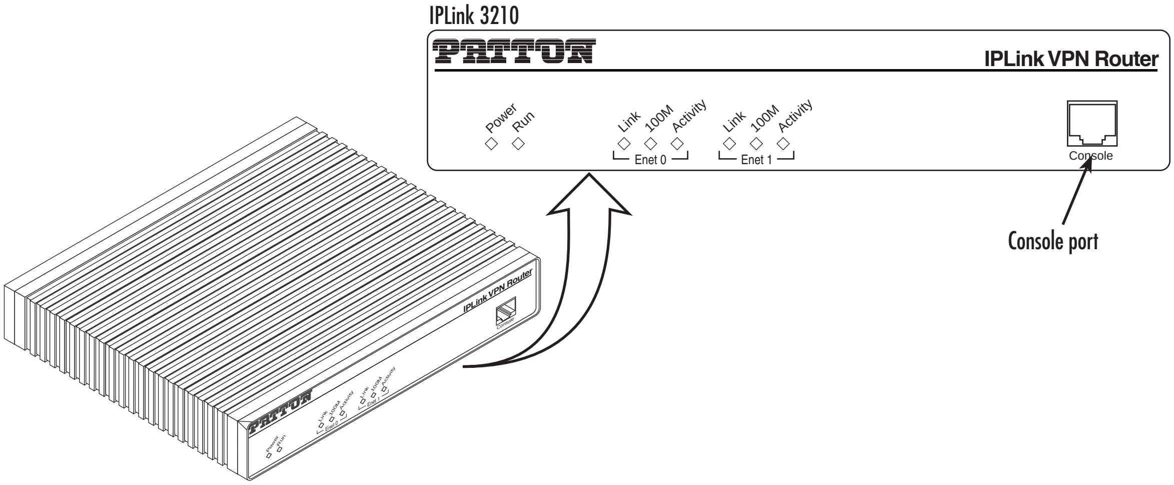


Figure 23. Examples of OnSite 3210 Series front panels

Table 15. OnSite LED Indications

LED	Description
Note	If an error occurs, all LEDs will flash once per second.
Power	When lit, indicates power is applied. Off indicates no power applied.
Run	When lit, indicates normal operation. Flashes once per second during boot (startup).
Ethernet (each port)	• Link: Lit when Ethernet link is up. • 100M: On when 100-Mbps Ethernet is selected. • Activity: Flashes when data is received or transmitted from the unit to the LAN.
WAN (Rear panel)	• STATUS: Lit when serial link is up. • ACTIVITY: Flashes when serial data is transmitted or received from the unit.

Chapter 9 Contacting Patton for assistance

Chapter contents

Introduction

This chapter contains the following information:

- "Contact information"—describes how to contact Patton technical support for assistance.
- "Warranty Service and Returned Merchandise Authorizations (RMAs)"—contains information about the RAS warranty and obtaining a return merchandise authorization (RMA).

Contact information

Patton Electronics offers a wide array of free technical services. If you have questions about any of our other products we recommend you begin your search for answers by using our technical knowledge base. Here, we have gathered together many of the more commonly asked questions and compiled them into a searchable database to help you quickly solve your problems.

Patton Support Headquarters in the USA

- Online support—available at **http://www.patton.com**
- E-mail support—e-mail sent to **support@patton.com** will be answered within 1 business day
- Telephone support—standard telephone support is available five days a week—from **8:00 am** to **5:00 pm EST** (**1300** to **2200 UTC**)—by calling **+1 (301) 975-1007**
- Fax—+1 (253) 663-5693

Alternate Patton support for Europe, Middle Ease, and Africa (EMEA)

- Online support—available at **http://www.patton-inalp.com**
- E-mail support—email sent to **support@patton-inalp.com** will be answered within 1 day
- Telephone support—standard telephone support is available five days a week—from 8:00 am to 5:00 pm CET (0900 to 1800 UTC/GMT)—by calling +41 (0) 31 985 25 55
- Fax—+41 (0) 31 985 25 26

Warranty Service and Returned Merchandise Authorizations (RMAs)

Patton Electronics is an ISO-9001 certified manufacturer and our products are carefully tested before shipment. All of our products are backed by a comprehensive warranty program.

Note If you purchased your equipment from a Patton Electronics reseller, ask your reseller how you should proceed with warranty service. It is often more convenient for you to work with your local reseller to obtain a replacement. Patton services our products no matter how you acquired them.

Warranty coverage

Our products are under warranty to be free from defects, and we will, at our option, repair or replace the product should it fail within one year from the first date of shipment. Our warranty is limited to defects in workmanship or materials, and does not cover customer damage, lightning or power surge damage, abuse, or unauthorized modification.

Out-of-warranty service

Patton services what we sell, no matter how you acquired it, including malfunctioning products that are no longer under warranty. Our products have a flat fee for repairs. Units damaged by lightning or other catastrophes may require replacement.

Returns for credit

Customer satisfaction is important to us, therefore any product may be returned with authorization within 30 days from the shipment date for a full credit of the purchase price. If you have ordered the wrong equipment or you are dissatisfied in any way, please contact us to request an RMA number to accept your return. Patton is not responsible for equipment returned without a Return Authorization.

Return for credit policy

- Less than 30 days: No Charge. Your credit will be issued upon receipt and inspection of the equipment.
- 30 to 60 days: We will add a 20% restocking charge (crediting your account with 80% of the purchase price).
- Over 60 days: Products will be accepted for repairs only.

RMA numbers

RMA numbers are required for all product returns. You can obtain an RMA by doing one of the following:

- Completing a request on the RMA Request page in the *Support* section at **http://www.patton.com**
- By calling **+1 (301) 975-1007** and speaking to a Technical Support Engineer
- By sending an e-mail to **returns@patton.com**

All returned units must have the RMA number clearly visible on the outside of the shipping container. Please use the original packing material that the device came in or pack the unit securely to avoid damage during shipping.

Shipping instructions

The RMA number should be clearly visible on the address label. Our shipping address is as follows:

Patton Electronics Company
RMA#: xxxx
7622 Rickenbacker Dr.
Gaithersburg, MD 20879-4773 USA

Patton will ship the equipment back to you in the same manner you ship it to us. Patton will pay the return shipping costs.

Appendix A **Compliance information**

Chapter contents

Compliance

EMC

- FCC Part 15, Class A
- EN55022, Class A
- EN55024

Safety

- UL 60950-1/CSA C22.2 N0.60950-1
- IEC/EN60950-1
- AS/NZS 60950-1

PSTN Regulatory

- ACTA Part 68
- CS03
- AS/ACIF S043

Radio and TV Interference (FCC Part 15)

The OnSite router generates and uses radio frequency energy, and if not installed and used properly-that is, in strict accordance with the manufacturer's instructions-may cause interference to radio and television reception. The OnSite router have been tested and found to comply with the limits for a Class A computing device in accordance with specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection from such interference in a commercial installation. However, there is no guarantee that interference will not occur in a particular installation. If the OnSite router does cause interference to radio or television reception, which can be determined by disconnecting the unit, the user is encouraged to try to correct the interference by one or more of the following measures: moving the computing equipment away from the receiver, re-orienting the receiving antenna and/or plugging the receiving equipment into a different AC outlet (such that the computing equipment and receiver are on different branches).

CE Declaration of Conformity

This equipment conforms to the requirements of Council Directive 1999/5/EC on the approximation of the laws of the member states relating to Radio and Telecommunication Terminal Equipment and the mutual recognition of their conformity.

The safety advice in the documentation accompanying this product shall be obeyed. The conformity to the above directive is indicated by the **CE** sign on the device. The signed Declaration of Conformity can be downloaded from the Patton website at www.patton.com/certifications.

Authorized European Representative

D R M Green

European Compliance Services Limited.

Oakdene House, Oak Road

Watchfield,

Swindon, Wilts SN6 8TD, UK

FCC Part 68 (ACTA) Statement

This equipment complies with Part 68 of FCC rules and the requirements adopted by ACTA. On the bottom side of this equipment is a label that contains—among other information—a product identifier in the format ***US: AAAEQ##TXXXX***. If requested, this number must be provided to the telephone company.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA.

This equipment uses a Universal Service Order Code (USOC) jack: RJ-11C.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn’t practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact our company. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Industry Canada Notice

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, *IC*, before the registration number signifies that registration was performed based on a Declaration of conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Appendix B Specifications

Chapter contents

Ethernet interfaces

10/100Base-TX Ethernet WAN port

10/100Base-TX Ethernet LAN port

All ports full duplex, autosensing, auto-MDIX 10/100 Full Duplex/Autosensing Ethernet RJ-45

PPP support

Frame-Relay (8 PVCs)

RFC1490, FRF.12 fragmentation

LMI, Q.933D, ANSI 617D, Gang of Four

PPP, PAP, CHAP, LCP, IPCP

IP services

IPv4 router; RIPv1, v2 (RFC 1058 and 2453)

Programmable static routes

ICMP redirect (RFC 792); Packet fragmentation

DiffServe/ToS set or queue per header bits

Packet Policing discards excess traffic

802.1p VLAN tagging

IPSEC AH & ESP Modes

Manual Key; IKE optional

AES/DES/3DES Encryption

Management

Industry standard CLI with local console (RJ-45, RS-232) and remote Telnet access

TFTP configuration & firmware loading

SNMP v1 agent (MIB II and private MIB)

Built-in diagnostic tools (trace, debug)

Java™ Applet; HPOV Integration with NNM

Operating environment

Operating temperature

32–104°F (0–40°C)

Operating humidity

5–80% (non condensing)

System

CPU Motorola MPC875 operating at 66 MHz

Memory:

- 32 Mbytes SDRAM
- 8 Mbytes Flash

Dimensions

7.3W x 1.6H x 6.1D in. (18.5H x 4.1W x 15.5D cm)

G.SHDSL Daughter Card

Note For information on configuring the G.SHDSL daughter card, see Chapter 4, "G.SHDSL Basic Configuration" on page 37.

Table 16. G.SHDSL Daughter Card Specifications

Factor	Specs
DSL	• ITU-T G.991.2 (and Amendment 2) • ITU-T G.991.2, Annex A, B, F, G • Upgradable to ITU-T G.shdsl.bis—Annex F and G • G.991.2 2/4 (1/2 pair) operation • G.994.1 (G.hs) (per G.991.2) • ITU-T G.991.2 Section E.9 (TPS-TC for ATM transport) • ITU-T G.991.2 Section E.11 (TPS-TC for PTM transport)
DSL Connection	RJ-11/12 (2-wire)
Management	• I.610 OAM F4/F5 • Management interfaces: GUI and Telnet • Software upgrade: GUI and TFTP
ATM Support	• Classical IPoA (RFC 1577/2225) • PPPoE Client (over ATM) (RFC 2516) • IPoA (RFC 2684/1483) • ATM AAL5 encapsulation • Max. 8 PVCs • User selectable VC MUX and LLC MUX (default) • Configurable auto-connection • ATM QoS: UBR (default), CBR, and VBR-rt, VBR-nrt, UBR: per VC queuing • Auto-configuration: TR-037 & ILMI 4.0
Interworking/Interoperability	• G.SHDSL Interoperability: - Alcatel - NEC - Lucent Anymedia - Lucent Stinger • BRAS Interoperability: - Cisco - Redback

Power supply

Internal AC version

Internal power supply 100–240 VAC, 50/60 Hz, 200 mA

12VDC version with External AC Power Adapter

Uses external AC Adaptor which provides 12VDC via barrel type connector

AC Adapter Input: 90-264VAC, 47-63Hz

AC Adapter Output: 12 VDC, 1.25A max

Note Power must be provided by an agency-approved external SELV source which provides reinforced insulation from the AC mains power and where the DC connector is the disconnect device. The source must have a rating of 12 VDC, 1.25 A.

5VDC Version with External Power Adapter

Uses external AC Adaptor which provides 5VDC via barrel type connector

AC Adapter Input: 100-240VAC, 50-60Hz

AC Adapter Output: 5 VDC, 2A max.

Note Power must be provided by an agency-approved external SELV source which provides reinforced insulation from the AC mains power and where the DC connector is the disconnect device. The source must have a rating of 5 VDC, 2 A

Appendix C **Cabling**

Chapter contents

Introduction

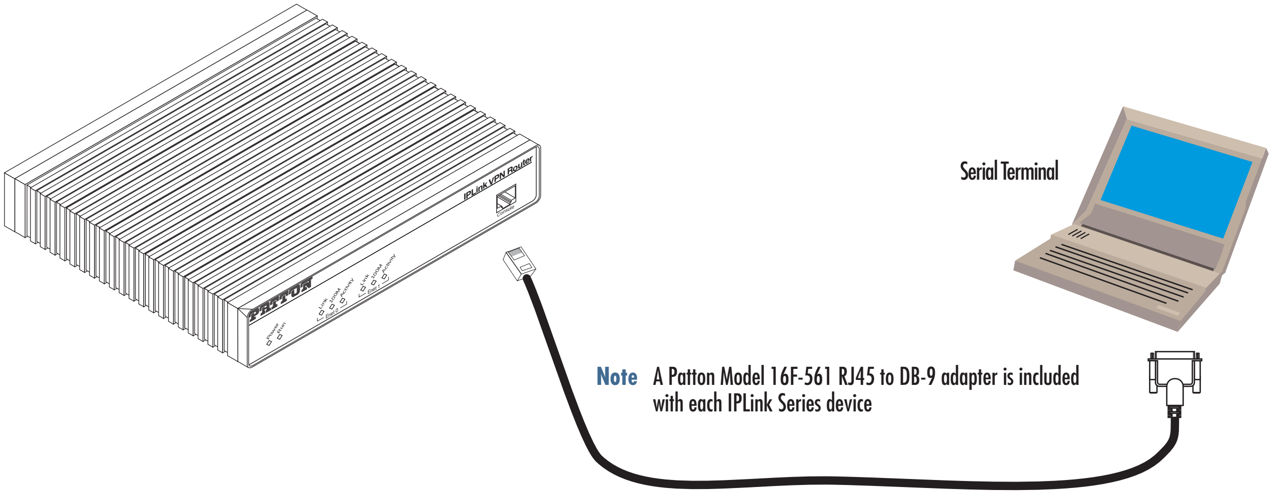
This section provides information on the cables used to connect the OnSite to the existing network infrastructure and to third party products.

CAUTION

The interconnecting cables must be acceptable for external use and must be rated for the proper application with respect to voltage, current, anticipated temperature, flammability, and mechanical serviceability.

Serial console

The OnSite can be connected to a serial terminal over its serial console port, as depicted in figure 24.



Note A Patton Model 16F-561 RJ45 to DB-9 adapter is included with each IPLink Series device

Figure 24. Connecting a serial terminal

Note See section “Console port, RJ-45, EIA-561 (RS-232)” on page 105 for console port pin-outs.

Ethernet 10Base-T and 100Base-T

Ethernet devices (10Base-T/100Base-T) are connected to the OnSite over a cable with RJ-45 plugs. Use a cross-over cable to a host, or a straight cable to a hub. See figure 25 (host) and figure 26 on page 103 (hub) for the different connections.

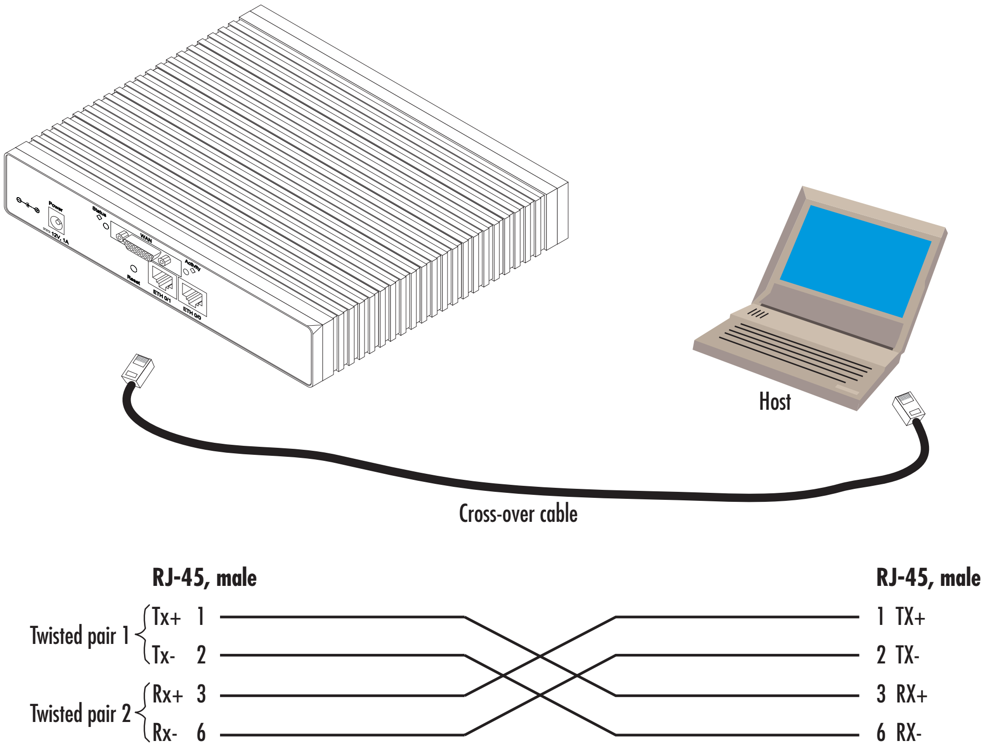
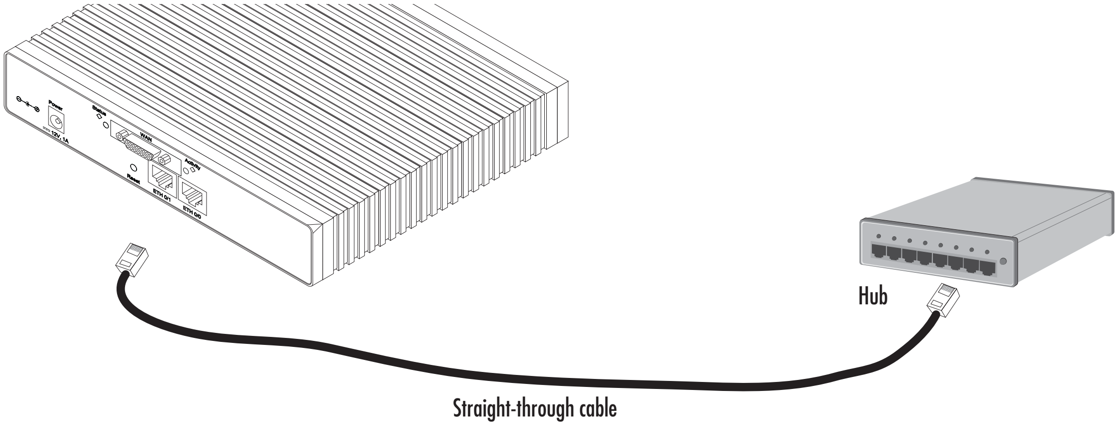


Figure 25. Ethernet cross-over



RJ-45, male			RJ-45, male
Tx+	1	1	Rx+
Tx-	2	2	Rx-
Rx+	3	3	Tx+
Rx-	6	6	Tx-

Figure 26. Ethernet straight-through

Appendix D **Port pin-outs**

Chapter contents

Introduction

This section provides pin-out information for the ports of the OnSite router.

Console port, RJ-45, EIA-561 (RS-232)

The RS-232 serial console port of the OnSite is configured to operate as a DCE. View the image in figure 27 showing the RJ-45 receptacle with the numerical identification of the pin numbers and functions.

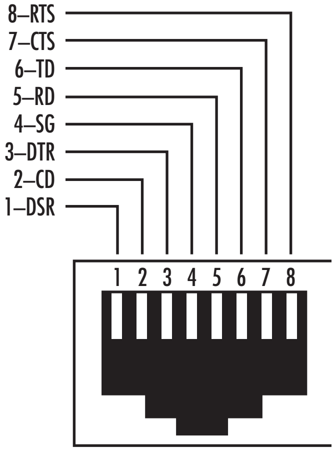


Figure 27. EIA-561 (RJ-45 8-pin) port

Table 17. RS-232 Console Port

Pin No.	Signal Name	Signal Direction
1	DSR	from OnSite
2	CD	from OnSite
3	DTR	to OnSite
4	Signal Ground	-
5	RD	from OnSite
6	TD	to OnSite
7	CTS	from OnSite
8	RTS	to OnSite

Refer to table 17 which tabulates the pin number, signal name and the direction of the signal.

Ethernet 10Base-T and 100Base-T port

Table 18. RJ-45 socket

Pin	Signal	Direction
1	TX+	from OnSite
2	TX-	from OnSite
3	RX+	to OnSite
6	RX-	to OnSite

The Ethernet ports are auto-detect MDI-X.

Note Pins not listed are not used.

DSL

Table 19. RJ-11 connector

Pin	Signal
1	No connection
2	Tip
3	Ring
6	No connection

Note Pins not listed are not used.

Appendix E OnSite 3210 Series factory configuration

Chapter contents

Introduction

The factory configuration settings for the OnSite 3210 Series devices are as follows:

```
#----------------------------------------------------------------#
# 3210 Series
# R3.xx BUILDxxxxx
# 2005-01-18T00:00:00
# Factory configuration file
#----------------------------------------------------------------#
profile napt NAPT
profile dhcp-server DHCP
  network 192.168.1.0 255.255.255.0
  include 192.168.1.10 192.168.1.19
  lease 2 hours
  default-router 192.168.1.1

context ip router

  interface eth0
    ipaddress 172.16.40.1 255.255.0.0
    use profile napt NAPT

  interface eth1
    ipaddress 192.168.1.1 255.255.255.0

context ip router
  dhcp-server use DHCP

port ethernet 0 0
  medium auto
  encapsulation ip
  bind interface eth0 router
  no shutdown

port ethernet 0 1
  medium auto
  encapsulation ip
  bind interface eth1 router
  no shutdown
```

Appendix F Installation checklist

Chapter contents

Introduction

This appendix lists the tasks for installing an OnSite 3210 Series G.SHDSL VPN Router (see table 20). Make a copy of this checklist and mark the entries as you complete each task. For each OnSite 3210 Series Router, include a copy of the completed checklist in your site log.

Table 20. Installation checklist

Task	Verified by	Date
Network information available & recorded in site log		
Environmental specifications verified		
Site power voltages verified		
Installation site pre-power check completed		
Required tools available		
Additional equipment available		
All printed documents available		
OnSite release & build number verified		
Rack, desktop, or wall mounting of chassis completed		
Initial electrical connections established		
ASCII terminal attached to console port		
Cable length limits verified		
Initial configuration performed		
Initial operation verified		