Concepts & Examples
ScreenOS Reference Guide

Volume 12:
WAN, ADSL, Dial, and Wireless

Release 5.4.0, Rev. A

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-015779-01, Revision A

Copyright Notice

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Writers: ScreenOS Team

Editor: Lisa Eldridge

Table of Contents

Chapter 1 Continued

Chapter 1 Continued

Chapter 4 Wireless Local Area Network 113

Chapter 4 Continued

Appendix A

About This Volume

Volume 12: WAN, ADSL, Dial, and Wireless describes the asymmetric digital subscriber line (ADSL) and wireless local area network (WLAN) interfaces. This volume contains the following chapters:

- Chapter 1, "Wide Area Networks," describes how to configure a wide area network (WAN).
- Chapter 2, "Asymmetric Digital Subscriber Line," describes the Asymmetric Digital Subscriber Line (ADSL) interface on the security device. ADSL is a Digital Subscriber Line (DSL) technology that allows existing telephone lines to carry both voice telephone service and high-speed digital transmission.
- Chapter 3, "ISP Failover and Dial Recovery," describes how to set priority and define conditions for ISP failover and how to configure a dialup recovery solution.
- Chapter 4, "Wireless Local Area Network," describes the wireless interfaces on Juniper Networks wireless devices and provides example configurations.
- Appendix A, "Wireless Information," lists available channels, frequencies, and regulatory domains and lists the channels that are available on wireless devices for each country.

Refer to the *NetScreen-5GT Wireless User's Guide* for information about installing the device and performing basic configuration tasks.

Document Conventions

This document uses several types of conventions, which are introduced in the following sections:

- "CLI Conventions" on this page
- "Illustration Conventions" on page xi
- "Naming Conventions and Character Types" on page xii
- "WebUI Conventions" on page xii

CLI Conventions

The following conventions are used to present the syntax of CLI commands in examples and in text.

In examples:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example:

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  means "set the management options for the ethernet1, the ethernet2, *or* the ethernet3 interface."
- Variables are in *italic* type:

  set admin user *name1* password *xyz*

In text:

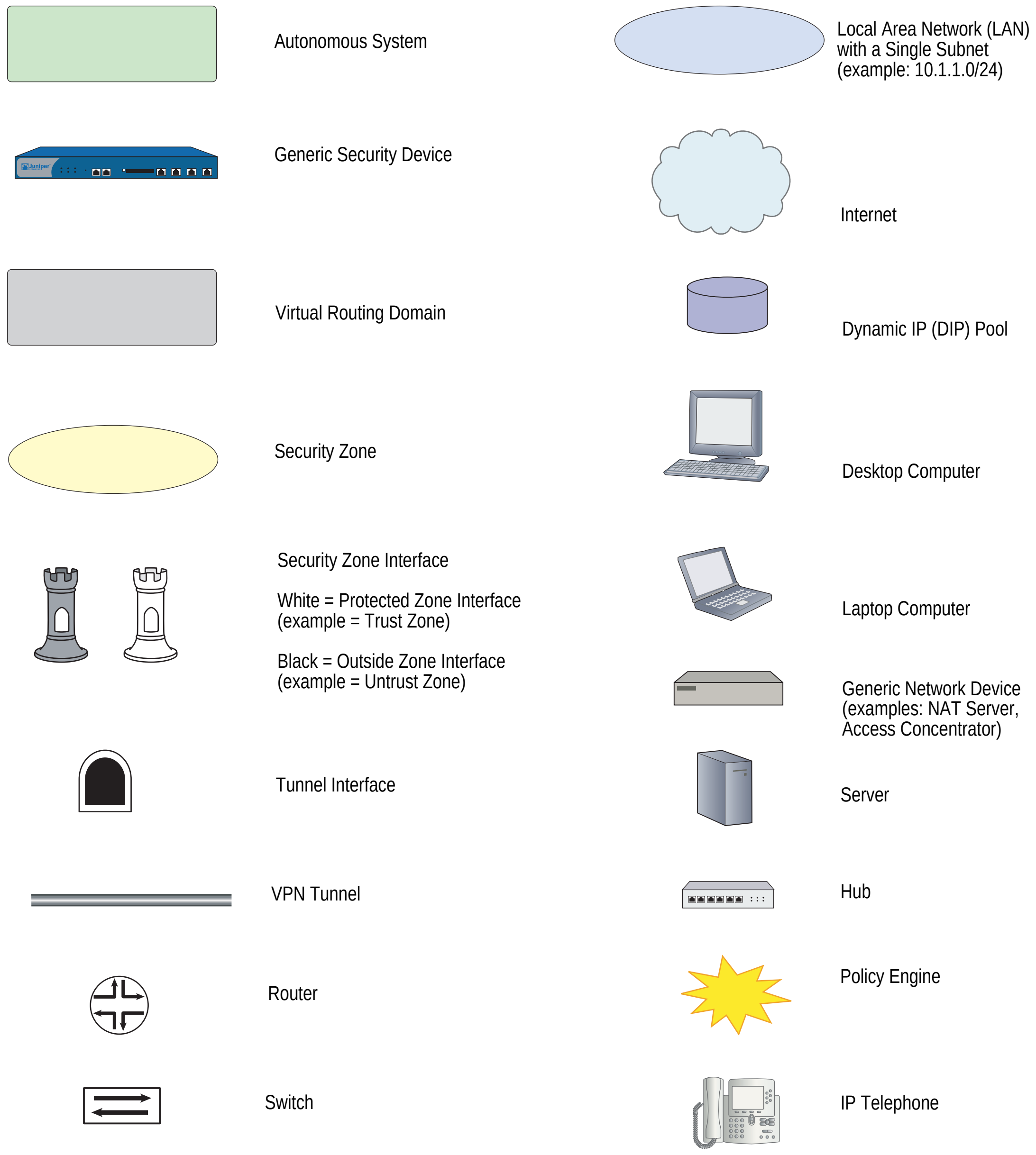
- Commands are in **boldface** type.
- Variables are in *italic* type.

NOTE: When entering a keyword, you only have to type enough letters to identify the word uniquely. For example, typing **set adm u kath j12fmt54** is enough to enter the command **set admin user kathleen j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.

Illustration Conventions

The following figure shows the basic set of images used in illustrations throughout this manual.

Figure 1: Images in Manual Illustrations



Naming Conventions and Character Types

ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations:

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes; for example:

  set address trust "local LAN" 10.1.1.0/24

- Any leading spaces or trailing text within a set of double quotes are trimmed; for example, **" local LAN "** becomes **"local LAN"**.

- Multiple consecutive spaces are treated as a single space.

- Name strings are case-sensitive, although many CLI keywords are case-insensitive. For example, **"local LAN"** is different from **"local lan"**.

ScreenOS supports the following character types:

- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.

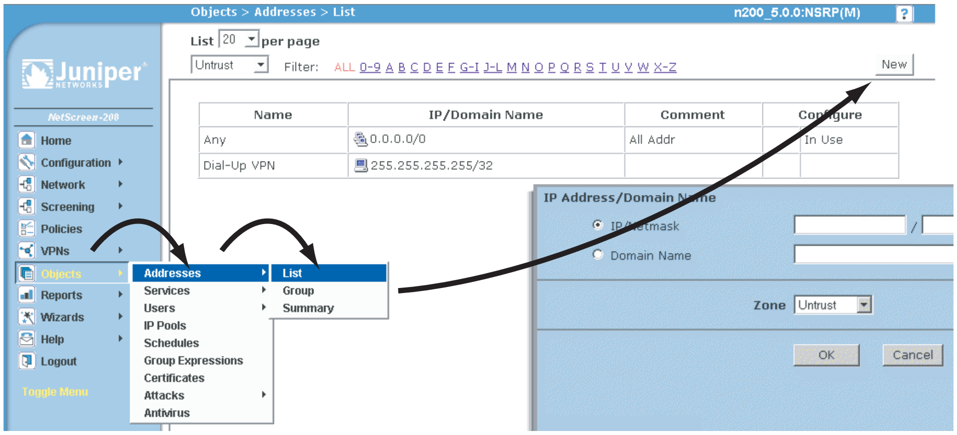
- ASCII characters from 32 (0x20 in hexadecimals) to 255 (0xff), except double quotes ("), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

NOTE: A console connection only supports SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your browser supports.

WebUI Conventions

A chevron (>) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The following figure shows the following path to the address configuration dialog box—Objects > Addresses > List > New:

Figure 2: WebUI Navigation



Objects > Addresses > List

n200_5.0.0:NSRP(M)

List 20 per page

Untrust Filter: ALL 0-9 A B C D E F G-I J-L M N O P Q R S T U V W X-Z

Name	IP/Domain Name	Comment	Configure
Any	0.0.0.0/0	All Addr	In Use
Dial-Up VPN	255.255.255.255/32		

IP Address/Domain Name

● IP/Netmask /

○ Domain Name

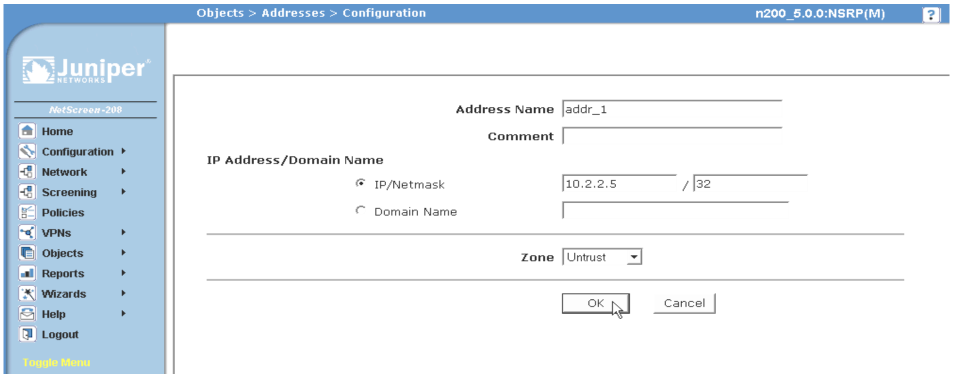
Zone Untrust

To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. The set of instructions for each task is divided into navigational path and configuration settings:

The next figure lists the path to the address configuration dialog box with the following sample configuration settings:

> Objects > Addresses > List > New: Enter the following, then click **OK**:
>
> > Address Name: addr_1
> > IP Address/Domain Name:
> >   IP/Netmask: (select), 10.2.2.5/32
> > Zone: Untrust

Figure 3: Navigational Path and Configuration Settings



Objects > Addresses > Configuration

Address Name: addr_1
Comment:
IP Address/Domain Name
● IP/Netmask: 10.2.2.5 / 32
○ Domain Name:
Zone: Untrust

Juniper Networks Documentation

To obtain technical documentation for any Juniper Networks product, visit www.juniper.net/techpubs/.

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

If you find any errors or omissions in this document, please contact us at the email address below:

techpubs-comments@juniper.net

Chapter 1

Wide Area Networks

Some security devices allow you to use wide area network (WAN) data links to transmit and receive traffic across geographically dispersed networks. These networks can be privately owned but more typically include public or shared networks. Certain properties must be configured before WAN links can operate correctly, such as the clocking and signal-handling options (for the physical line) and the encapsulation method (for transferring data across the WAN).

This chapter contains the following sections:

- "WAN Overview" on this page
- "WAN Interface Options" on page 7
- "WAN Interface Encapsulation" on page 30
- "Multi-Link Encapsulation" on page 42
- "WAN Interface Configuration Examples" on page 49
- "Encapsulation Configuration Examples" on page 60

WAN Overview

This section defines the following WAN interfaces:

- "Serial" on page 2
- "T1" on page 3
- "E1" on page 3
- "T3" on page 4
- "ISDN" on page 5

Serial

Serial links provide bidirectional links that require very few control signals. In a basic serial setup, the data communications equipment (DCE) is responsible for establishing, maintaining, and terminating a connection. A modem is a typical DCE device. A serial cable connects the DCE to a telephony network where, ultimately, a link is established with data terminal equipment (DTE). DTE is typically where a link terminates.

Some security devices support the following types of serial interfaces:

- TIA/EIA 530—The Telecommunications Industry Association/Electronics Industries Alliance (TIA/EIA) Standard 530, *High-Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment*, describes the interconnection of DTE and DCE using serial binary data interchange with control information exchanged on separate control circuits.

- V.35—The Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T) Recommendation V.35, *Data Transmission at 48 kbit/s Using 60-108 kHz Group Band Circuits***,** describes a synchronous, Physical Layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and Europe.

- X.21—The ITU-T Recommendation X.21, *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment for Synchronous Operation on Public Data Networks*, describes serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.

- RS-232—TIA/EIA-232-F (the current revision), *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, describes the physical interface and protocol for communication with modems and other serial devices.

- RS-449—The EIA standard *EIA-449 General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, specifies the interface between DTE and DCE.

When a serial connection is made, a serial line protocol—such as EIA-530, X.21, RS-422/449, RS-232, or V.35—begins controlling the transmission of signals across the line as follows:

1. The DCE transmits a DSR signal to the DTE, which responds with a DTR signal. After this transmission, the link is established and traffic can pass.

2. When the DTE device is ready to receive data, it sets its RTS signal to a marked state (all 1s) to indicate to the DCE that it can transmit data.

3. When the DCE device is ready to receive data, it sets its clear-to-send (CTS) signal to a marked state to indicate to the DTE that it can transmit data.

4. When the negotiation to send information has taken place, data is transmitted across the transmitted data (TD) and received data (RD) lines:

- TD line—Line through which data from a DTE device is transmitted to a DCE device.

- RD line—Line through which data from a DCE device is transmitted to a DTE device.

T1

T1, also known as data signal 1 (DS1), is a digital data transmission medium capable of handling 24 simultaneous connections running at a combined 1.544 Mbps. T1 combines these 24 separate connections, called *channels* or *time slots*, onto a single link.

The T1 data stream is broken into frames. Each frame consists of a single framing bit and 24 8-bit channels, totalling 193 bits per T1 frame. Frames are transmitted 8,000 times per second, at a data transmission rate of 1.544 Mbps (8,000 x 193 = 1.544 Mbps). As each frame is received and processed, the data in each 8-bit channel is maintained with the channel data from previous frames, enabling T1 traffic to be separated into 24 separate flows across a single medium.

Supported T1 standards include:

- American National Standards Institute (ANSI) T1.107, *Digital Hierarchy - Formats Specifications,* describes digital-hierarchy formats and is used in conjunction with T1.102, *Digital Hierarchy - Electrical Interfaces*.

- Telcordia GR 499-CORE, *Transport Systems Generic Requirements (TSGR): Common Requirements,* describes basic generic requirements common to transport systems. Telcordia GR 253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria,* describes generic SONET criteria.

- AT&T Technical Reference 54014, *ACCUNET T45 and T45R Service Description and Interface Specification,* describes the service description and interface specification for AT&T ACCUNET T45 and T45R services.

- International Telecommunications Union (ITU-T) Recommendations G.751 and G.703 describe physical and electrical characteristics of hierarchical digital interfaces.

E1

E1 is the European format for DS1 digital transmission. E1 links are similar to T1 links except that they carry signals at 2.048 Mbps. Each signal has 32 channels, and each channel transmits at 64 Kbps. E1 links have higher bandwidth than T1 links because they use all 8 bits of a channel.

The following standards apply to E1 interfaces:

- ITU-T Recommendation G.703, *Physical/Electrical Characteristics of Hierarchical Digital Interfaces*, describes data rates and multiplexing schemes.

- ITU-T Recommendation G.751, *General Aspects of Digital Transmission Systems: Terminal Equipment*, describes framing methods.

- ITU-T Recommendation G.775, *Loss of Signal (LOS) and Alarm Indication Signal (AIS) Defect Detection and Clearance Criteria*, describes alarm-reporting methods.

T3

T3, also known as data signal 3 (DS3), is a high-speed data-transmission medium formed by multiplexing 28 DS1signals into seven separate DS2 signals, and combining the DS2 signals into a single DS3 signal. T3 links operate at 43.736 Mbps.

Supported T3 standards include:

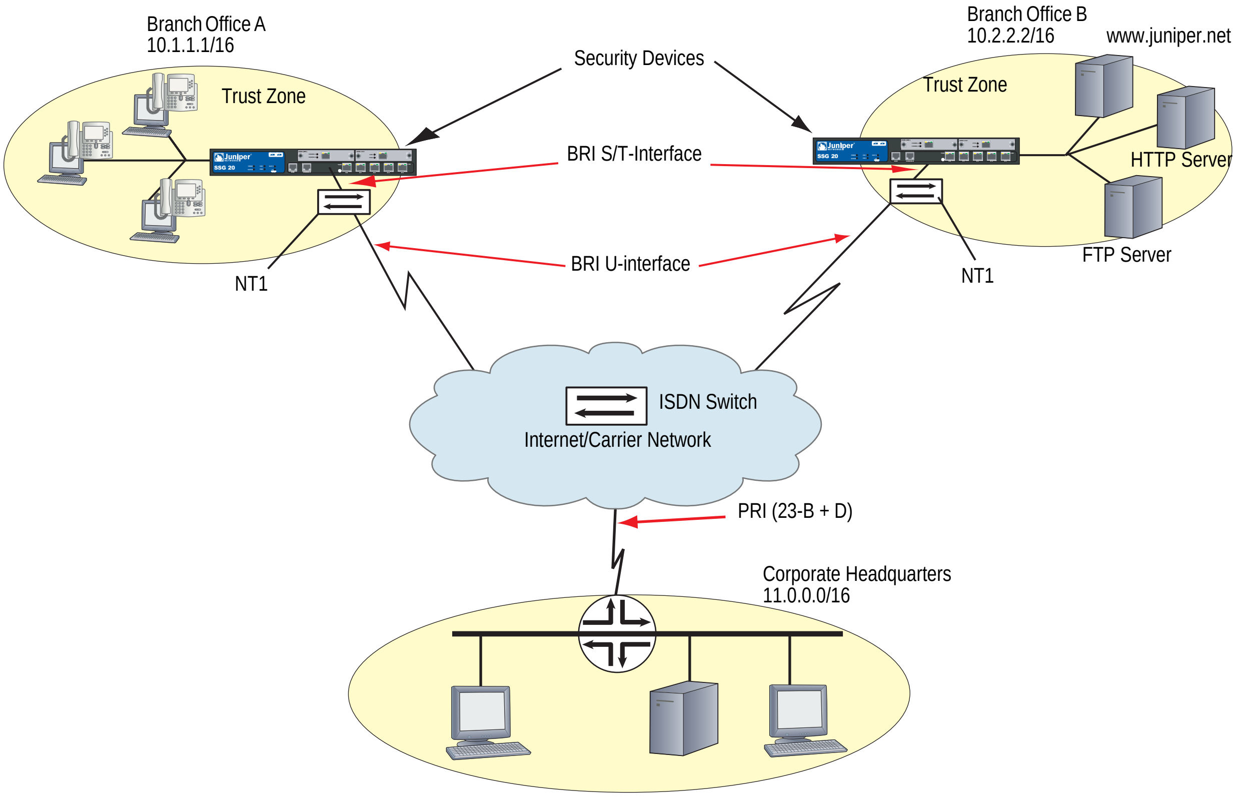
- American National Standards Institute (ANSI) T1.107, *Digital Hierarchy - Formats Specifications,* describes digital-hierarchy formats and is used in conjunction with T1.102, *Digital Hierarchy - Electrical Interfaces*.
- Telcordia GR 499-CORE, *Transport Systems Generic Requirements (TSGR): Common Requirements*, describes basic generic requirements common to transport systems. Telcordia GR 253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*, describes generic SONET criteria.
- Telcordia TR-TSY-000009, A*synchronous Digital Multiplexes, Requirements and Objectives*, describes generic technical requirements and objectives for asynchronous multiplexes that operate at DS1C (3.152 Mbps), DS2 (6.312 Mbps), and/or DS3 (44.736 Mbps) digital rates.
- AT&T Technical Reference 54014, *ACCUNET T45 and T45R Service Description and Interface Specification*, describes the service description and interface specification for AT&T ACCUNET T45 and T45R Services.
- ITU G.751, *Digital multiplex equipment operating at the third order bit rate of 34 368 kbit/s and the fourth order bit rate of 139 264 kbit/s and using positive justification*, G.703, *Physical/electrical characteristics of hierarchical digital interfaces*, and G.823, *The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy*, describe transmission systems and media, digital systems, and networks.

ISDN

Integrated Services Digital Network (ISDN) is an international communications standard for sending voice, video, and data over digital telephone lines. As a dial-on-demand service, ISDN has fast call setup and low latency as well as the ability to carry high-quality voice, data, and video transmissions. ISDN is also a circuit-switched service that can be used on both multipoint and point-to-point connections.

Figure 1 illustrates a basic setup for ISDN connectivity. The Branch office is connected to the Corporate headquarters using ISDN. The connection is automatically established for any request to send a packet to the Internet and the connection is dropped after a set number of seconds elapses with no traffic. Because ISDN connections typically takes a few milliseconds to establish (almost instantaneously) the connection can be easily made and broken as demand warrants.

Figure 1: Basic ISDN Topology



In North America, most Carriers provide a U-interface for ISDN connectivity. To communicate with your security device, you must use additional equipment, Network Termination unit (NT1), to convert the U-interface to a S/T-interface. Juniper Networks security devices are provided with the S/T-interface only. The NT1 is located at the customer's site (see Branch Offices in Figure 1) and may be provided by the Carrier.

ISDN in ScreenOS supports the following features on your security device:

- Dial-on-Demand Routing (DDR)

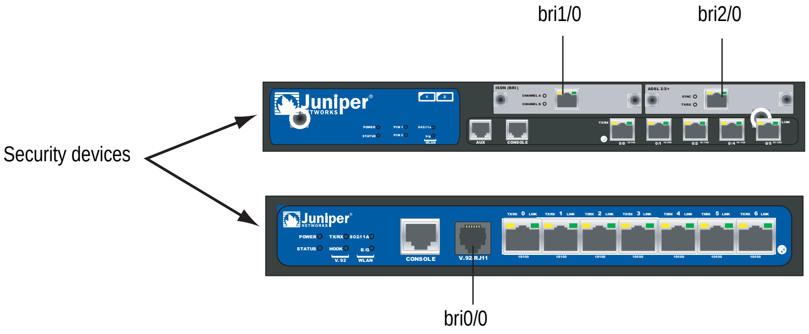
  DDR allows the security device to automatically initiate and close a session as transmitting stations demand. The device spoofs keepalives so that end stations treat the session as active. DDR lets the user bring up WAN links only when necessary and thus reduce remote-site access costs.

- Basic Rate Interface (BRI)

  BRI is also called 2B + D, because it consists of two 64 Kbps B-channels and one 16 Kbps D-channel. The B-channels are used for user data, and the D-channel is responsible for carrying signalling traffic to establish and terminate connections between sites.

  Each ISDN BRI uses the naming convention bri*x*/0, where *x* = slot-id and *x*/0 represents **slot-id/port-id** as shown in Figure 2. The two B-channels for bri0/0, for example, are identified as *bri0/0.1* and *bri0/0.2*.

Figure 2: Basic Rate Interfaces



- Bandwidth on Demand

  The two 64-Kbps B-channels can be combined to form a single 128-Kbps connection as needed. The device supports bandwidth-on-demand on the ISDN interface as follows:

  - Brings up more channel when traffic is beyond configured threshold
  - Disconnects channel when traffic is less than the configured threshold

  Bandwidth on demand is implemented on your security device using multi-link PPP (MLPPP) encapsulation.

- Dialer interface and dialer pool

  The dialer interface and dialer pool allows the ISDN interface to dial out to multiple destinations when the number of destinations exceeds the number of available physical lines. The ISDN interface can belong to more than one pool, allowing a single line to be used to dial out to more than one destination.

For more information on this feature, see "Dialing Out Using the Dialer Interface" on page 54.

- Dial backup

  You can use the ISDN interface for dial backup, to activate a secondary WAN link when a primary synchronous line fails.

- Leased Line

  The ISDN leased line is supported for 128Kbps. In leased line mode, the ISDN interface operates as Layer 3 interface that can only deliver data, so the D-channel is not required.

- Monitor ISDN and Dialer interfaces

WAN Interface Options

This section explains the WAN interfaces options that are available on some of the security devices. Table 1 displays which physical attributes are available on the WAN interfaces.

Table 1: WAN Interface Physical Attributes

Physical Attributes	Serial	T1	E1	T3	ISDN (BRI)
Hold time	X	X	X	X	X
DTE options	X				
Frame checksum		X	X	X	
Idle-cycle Flag		X	X	X	X
Start/End Flag		X	X	X	
Signal Handling	X				
Clocking					
Clocking Mode	X				
Clocking source		X	X	X	
Internal Clock rate	X				
Transmit clock Inversion	X				
Time Slots					
Fractional T1 Time Slots		X			
Fractional E1 Time Slots			X		
Line Encoding					
AMI		X			
B8ZS		X			
HDB3			X		
Byte Encoding		X			
Data Inversion		X	X		
Framing					

Physical Attributes	Serial	T1	E1	T3	ISDN (BRI)
Superframe		X			
Extended Frame		X			
G.704 Frame			X		
C-Bit Parity Frame				X	
Loopback Signal					
Loopback Mode		X			X
Bit-Error Rate Test (BERT)		X	X	X	
CSU Compatibility Mode				X	
Remote loopback response		X			
FEAC Response				X	
ISDN Options					
Switch type					X
SPID1					
SPID2					X
TEI negotiation					X
Calling number					X
T310 value					X
Send complete					X
BRI Mode (leased line/dialer)					X
Dialer Options					
Primary/alternate numbers					X
Load Threshold					X
Idle time					X
Retry times					X
Interval					X
Dialer pool					X

Hold time

Hold time specifies how much time can pass before the device considers the interface connection to be up or down. The hold time is useful in situations where an interface is connected to an add-drop multiplexer (ADM) or a wavelength-division multiplexer (WDM), or to protect against Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) framer holes because you might not want the interface to advertise that its connection status is up or down.

For example, if an interface goes from up to down, it is not advertised to the rest of the system as being down until it has remained down for the specified hold-time period. Similarly, an interface is not advertised to the rest of the system as being up until it has remained up for the specified hold-time period.

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Enter the following, then click **Apply**:

Hold time
Down: 500
Up: 500

CLI

```
set interface interface hold-time { down 500 | up 500 }
save
```

NOTE: A 0 hold-time indicates that the interface drops traffic when the device receives an message that the interface is down.

Frame Checksum

Frame checksum verifies that frames passing through a device are valid using a bit-encoding scheme. Some WAN interfaces use a 16-bit frame checksum, but can configure a 32-bit checksum to provide more reliable packet verification.

To configure the WAN interface to use a 32-bit checksum, use the WebUI or CLI (x is either t1, e1, or t3):

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: For the **Frame Checksum** option select **32-bits**, then click **Apply.**

CLI

```
set interface interface x-options fcs 32
save
```

Idle-cycle Flag

An idle cycle is the duration when the device has no data to transmit. Idle-cycle flags allow some WAN interfaces to transmit the value 0x7E in the idle cycles. To configure the WAN interface to transmit the value 0xFF (all ones), use the WebUI or CLI (x is either t1, e1, t3, or bri):

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: For the Idle-cycle Flags option select **0xFF (All ones)**, then click **Apply.**

CLI

```
set interface interface x-options idle-cycle-flag ones
save
```

Start/End Flag

Start and end flags for T1 or E1 interfaces wait two idle cycles between sending a start and an end flag. To configure the interface to share the transmission of start and end flags, use the WebUI or CLI (x is either t1 or e1):

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: For the Start/End Flags on Transmission option select **Shared**, then click **Apply.**

CLI

```
set interface interface x-options start-end-flag shared
```

To share the transmission of start and end flags on a T3 interface, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the Line encoding type, then click **Apply**.

CLI

```
set interface interface t3-options start-end-flag
save
```

Line Encoding

Following are common T1 and E1 encoding techniques:

- Alternate mark inversion (AMI)—T1 and E1
- Bipolar with 8-zero substitution (B8ZS)—T1 only
- High-density bipolar 3 code (HDB3)—E1 only

To change the encoding type, use the WebUI or CLI (x is either t1 or e1):

WebUI

Network > Interfaces > List > Edit (*X Interface*) > WAN: Select the Line encoding type, then click **Apply**.

CLI

```
set interface interface x-options line-encoding option
save
```

Alternate Mark Inversion (AMI) Encoding

AMI encoding forces the 1s signals on a T1 or E1 line to alternate between positive and negative voltages for each successive 1 transmission. When AMI encoding is used, a data transmission with a long sequence of 0s has no voltage transitions on the line. In this situation, devices have difficulty maintaining clock synchronization, because they rely on the voltage fluctuations to constantly synchronize with the transmitting clock. To counter this effect, the number of consecutive 0s in a data stream is restricted to 15. This restriction is called the 1s density requirement, because it requires a certain number of 1s for every 15 0s that are transmitted. On an AMI-encoded line, two consecutive pulses of the same polarity—either positive or negative—are called a bipolar violation (BPV), which is generally flagged as an error.

Data Inversion

When you enable data inversion, all data bits in the datastream are transmitted inverted; that is, zeroes are transmitted as ones, and ones are transmitted as zeroes. Data inversion is normally used only in AMI mode to provide the density in the transmitted stream. To enable data inversion, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Check the Invert data checkbox, then click **Apply.**

CLI

```
set interface interface t1-options invert-data
save
```

B8ZS and HDB3 Line Encoding

Both bipolar with 8-zero substitution (B8ZS) and high-density bipolar 3 code (HDB3) encoding do not restrict the number of 0s that can be transmitted on a line. Instead, these encoding methods detect sequences of 0s and substitute bit patterns in their place to provide the signal oscillations required to maintain timing on the link. The B8ZS encoding method for T1 lines detects sequences of eight consecutive 0 transmissions and substitutes a pattern of two consecutive BPVs (11110000). Because the receiving end uses the same encoding, it detects the BPVs as 0s substitutions, and no BPV error is flagged. A single BPV, which does not match the 11110000 substitution bit sequence, is likely to generate an error, depending on the configuration of the device.

The HDB3 encoding method for E1 lines detects sequences of four consecutive 0 transmissions and substitutes a single BPV (1100). Similar to B8ZS encoding, the receiving device detects the 0s substitutions and does not generate a BPV error.

Byte Encoding

A T1 interface uses byte encoding of 8 bits per byte (nx64). You can configure an alternative byte encoding of 7 bits per byte (nx56). To configure the interface byte encoding, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the byte encoding type, then click **Apply.**

CLI

```
set interface interface t1-options byte-encoding option
save
```

Line Buildout

Some WAN interfaces allow you to configure the line buildout, which is the programmable distance between the device and your main office. A T1 interface has five possible setting ranges for the line buildout:

- 0 to 132 feet (ft) (0 to 40 meters (m))
- 133 to 265 ft (40 to 81 m)
- 266 to 398 ft (81 to 121 m)
- 399 to 531 ft (121 to 162 m)
- 532 to 655 ft (162 to 200 m)

A T3 interface has two settings for the T3 line buildout: a short setting, which is less than 255 feet (about 68 meters), and a long setting, which is greater than 255 feet and less than 450 feet (about 137 meters).

To set the interface line range, use the WebUI (X is either t1 or t3) or CLI:

WebUI

Network > Interfaces > List > Edit (*X Interface*) > WAN: Select the line buildout range, then click **Apply.**

CLI

```
set interface interface t1-options buildout range
save
```

or

```
set interface interface t3-options long-buildout
save
```

Framing Mode

T1 interface uses two types of framing: superframe (SF) and extended superframe (ESF). E1 interfaces use G.704 framing or G.704 with no CRC4 framing, or can be in unframed mode.

To configure framing for the WAN interface, use the WebUI or CLI (x is either t1 or e1):

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the framing mode, then click **Apply.**

CLI

```
set interface interface x-options framing options
```

Superframe (SF) Framing for T1

A SF, also known as D4, frame consists of 192 data bits: 24 8-bit channels and a single framing bit. The single framing bit is part of a 12-bit framing sequence. The 193rd bit in each T1 frame is set to a value, and every 12 consecutive frames are examined to determine the framing bit pattern for the 12-bit superframe. The receiving device detects these bits to synchronize with the incoming data stream and determine when the framing pattern begins and ends.

Extended Superframe (ESF) Framing for T1

ESF extends the D4 superframe from 12 frames to 24 frames, which also increase the bits from 12 to 24. The extra bits are used for frame synchronization, error detection, and maintenance communications through the facilities data link (FDL). Only the framing bits from frames 4, 8, 12, 16, 20, and 24 in the superframe sequence are used to create the synchronization pattern.

C-Bit Parity Framing for T3

C-bit parity mode controls the type of framing that is present on the transmitted T3 signal. When C-bit parity mode is enabled, the C-bit positions are used for the Far End Block Error (FEBE), Far-End Alarm and Control (FEAC), terminal data link, path parity, and mode indicator bits, as defined in ANSI T1.107a-1989. When C-bit parity mode is disabled, the basic T3 framing mode (M13) is used.

To disable C-bit parity mode and use M13 framing for your T3 interface, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the framing mode, then click **Apply.**

CLI

```
unset interface interface t3-options cbit-parity
save
```

Clocking

Clocking determines how networks sample transmitted data. As streams of information are received by a router in a network, a clock source specifies when to sample the data. Some WAN interfaces allow you to configure the following clocking information:

- Clocking Mode
- Clocking Source
- Internal Clock Rate
- Transmit Clock Inversion

Clocking Mode

There are three clocking modes:

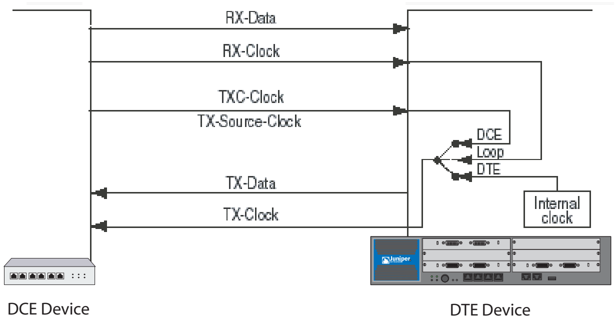
- **Loop clocking mode** uses the DCE Receive (RX) clock to clock data from the DCE to the DTE.
- **DCE clocking mode** uses the DTE Transmit (TX) clock, which the DCE generates for the DTE to use as the transmit clock for DTE.
- **Internal clocking mode**, also known as *line timing*, uses an internally generated clock.

NOTE: For TIA/EIA 530, V.35, RS0232, and RS-449 interfaces, you can configure each interface independently to use loop, DCE, or internal clocking mode. For X.21 interfaces, only loop clocking mode is supported.

DCE clocking mode and loop clocking mode use external clocks generated by the DCE.

Figure 3 shows the clock sources for loop, DCE, and internal clocking modes.

Figure 3: Serial Interface Clocking Mode



To configure the clocking mode of a serial interface, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN:

Hold Time
Clock Mode
Select the clocking mode, then click **Apply**.

CLI

```
set interface interface serial-options clocking-mode { dce | internal | loop }
```

Clocking Source

The clock source can be the internal stratum 3 clock, which resides on the control board, or an external clock that is received from the interface you are configuring.

By default, the interface clocking source is internal, which means that each interface uses the internal stratum 3 clock. For interfaces that can use different clock sources, the source can be internal (also called *line timing* or *normal timing*) or external (also called *loop timing*).

To set the clock source of an interface to use an external clock, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN:

Hold Time
Clocking
Select the clocking mode, then click **Apply**.

CLI

```
set interface interface clocking external
```

Internal Clock Rate

The internal clock rate is the speed of the internal clock which is typically used with the internal clocking mode.

NOTE: For RS-232 interfaces with internal clocking mode configured, the clock rate must be less than 20 KHz.

To configure the clock rate, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the following, then click **Apply**:

Hold Time
Clock Rate: Select the rate

CLI

```
set interface interface serial-options clock-rate number
save
```

You can configure the following interface rates:

1.2 KHz
2.4 KHz
9.6 KHz
19.2 KHz
38.4 KHz
56.0 KHz
64.0 KHz
72.0 KHz
125.0 KHz
148.0 KHz
250.0 KHz
500.0 KHz
800.0 KHz
1.0 Mhz
1.3 Mhz
2.0 Mhz
4.0 Mhz
8.0 Mhz

Although the WAN interface is intended for use at the default rate of 8.0 MHz, you might need to use a slower rate under any of the following conditions:

- The interconnecting cable is too long for effective operation.
- The interconnecting cable is exposed to an extraneous noise source that might cause an unwanted voltage in excess of + 1 volt measured differentially between the signal conductor and circuit common at the load end of the cable, with a 50-ohm resistor substituted for the generator.
- You need to minimize interference with other signals.
- You need to invert one or more signals.

NOTE: For TIA/EIA 530, V.35, RS-232, and RS-449 interfaces with internal clocking mode enabled, you can configure the clock rate. For more information about internal clocking mode, see “Clocking Mode” on page 13.

For detailed information about the relationship between signaling rate and interface-cable distance, see the following standards:

- EIA 422-A, *Electrical Characteristics of Balanced Voltage Digital Interface Circuits*
- EIA 423-A, *Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits*

Transmit Clock Inversion

The transmit clock aligns each outgoing packet transmitted over the WAN interfaces. When the device uses externally timed clocking mode (DCE or loop), long cables might introduce a phase shift of the DTE-transmitted clock and data. At high speeds, this phase shift could cause errors. Inverting the transmit clock corrects the phase shift, thereby reducing error rates.

To set the transmit to be inverted, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the following, then click **Apply**:

CLI

```
set interface interface serial-options transmit-clock invert
save
```

Signal Handling

Normal signal handling is defined by the following standards:

- TIA/EIA Standard 530
- ITU-T Recommendation V.35
- ITU-T Recommendation X.21

Table 2 shows the serial-interface modes that support each signal type.

Table 2: Signal Handling by Serial-Interface Type

Signal	Serial Interfaces
From-DCE signals:	
Clear-to-Send (CTS)	TIA/EIA 530, V.35, RS-232, RS-449
Data-Carrier-Detect (DCD)	TIA/EIA 530, V.35, RS-232, RS-449
Data-Set-Ready (DSR)	TIA/EIA 530, V.35, RS-232, RS-449
Test-Mode (TM)	TIA/EIA 530 only
To-DCE signals:	
Data-Transfer-Ready (DTR)	TIA/EIA 530, V.35, RS-232, RS-449
Request-to-Send (RTS)	TIA/EIA 530, V.35, RS-232, RS-449

To configure serial interface characteristics, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the following, then click **Apply**:

DTE Options
    Select your options

CLI

```
set interface interface serial-options dte-options { ... }
save
```

NOTE: If **ignore-all** is specified, other signal-handling options cannot be configured.

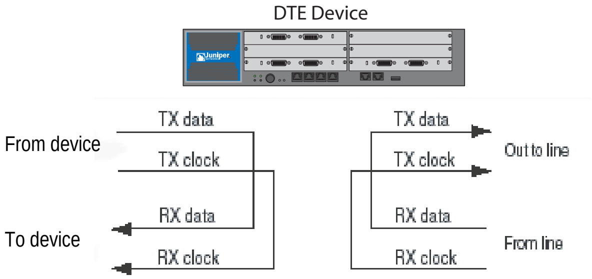
Loopback Signal

The control signal on a T1 or E1 link is the loopback signal. Using the loopback signal, the operators at the network control center can force the device at the remote end of a link to retransmit its received signals back onto the transmit path. The transmitting device can then verify that the received signals match the transmitted signals, to perform end-to-end checking on the link.

Remote and Local Loopback

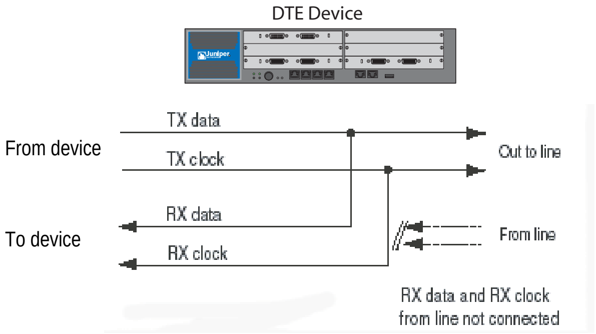
Remote line interface unit (LIU) loopback loops the transmit (TX) data and TX clock back to the device as receive (RX) data and RX clock. From the line, LIU loopback loops the RX data and RX clock back out the line as TX data and TX clock, as shown in Figure 4.

Figure 4: WAN Interface LIU Loopback



DCE local and DCE remote control the TIA/EIA 530 interface-specific signals for enabling local and remote loopback on the link-partner DCE. Figure 5 shows local loopback.

Figure 5: WAN Interface Local Loopback



Loopback Mode

You can configure loopback mode between the local T1, T3, or ISDN (bri) interface and the remote channel service unit (CSU), as shown in Figure 6. You can configure the loopback mode to be local or remote. With local loopback, the interface can transmit packets to the CSU but receives its own transmission back again and ignores data from the CSU. With remote loopback, packets sent from the CSU are received by the interface, forwarded if there is a valid route, and immediately retransmitted to the CSU. Local and remote loopback transmissions loop back both data and clocking information. Packets can be looped on either the local routing platform or the remote CSU.

To configure loopback mode on a serial interface, use the WebUI or CLI:

WebUI

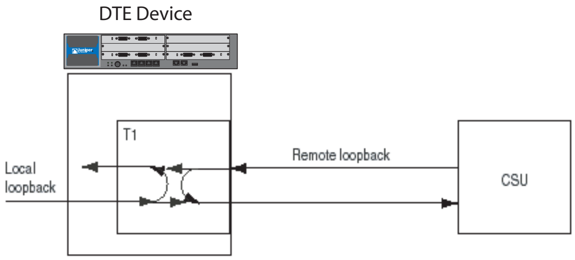
Network > Interfaces > List > Edit (*serial interface*) > WAN: Select the following, then click **Apply**:

Diagnosis Options
Loopback Mode:

CLI

```
set interface interface serial-options loopback { dce-local | local | remote }
save
```

Figure 6: Remote and Local WAN Interface Loopback Traffic



To configure the loopback mode on E1 or ISDN (bri) interface, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the following, then click **Apply**:

Diagnosis Options
Loopback Mode: local or remote

CLI

```
set interface interface e1-options loopback { local | remote }
set interface interface bri-options loopback { local | remote }
save
```

Some WAN interfaces allow you to specify the loopback payload option to loop back data without clocking information on the remote router.

To configure loopback payload on a T1 and T3 interfaces, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the following, then click **Apply**:

Diagnosis Options
Loopback Mode: payload

CLI

```
set interface interface t1-options loopback payload
save
```

T3 HDLC payload scrambling provides better link stability. Both sides of a connection must either use or not use scrambling.

To configure scrambling on the T3 channels on the interface, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN:

T3 Options
Check the Payload scrambling checkbox

CLI

```
set interface interface t3-options payload-scrambler
save
```

CSU Compatibility Mode

Subrating a T3 interface reduces the maximum allowable peak rate by limiting the HDLC-encapsulated payload. Subrate modes configure the interface to connect with CSUs that use proprietary methods of multiplexing.

You can configure a T3 interface to be compatible with a Digital Link, Kentrox, Adtran, Verilink, or Larscom CSU.

To configure a T3 interface to be compatible with the CSU at the remote end of the line, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN:

T3 Options
Select the CSU Compatibility Mode

CLI

```
set interface interface t3-options compatibility-mode { adtran | digital-link | kentrox |
    larscom | verilink } number
save
```

The subrate of a T3 interface must exactly match that of the remote CSU.

Each CSU compatibility mode has different configuration parameters:

- Adtran: You must specify the subrate as a value from 1 through 588 that exactly matches the value configured on the CSU. A subrate value of 588 corresponds to 44.2 Mbps, or 100 percent of the HDLC-encapsulated payload. A subrate value of 1 corresponds to 44.2/588, which is 75.17 Kbps, or 0.17 percent of the HDLC-encapsulated payload.

- Digital Link: You must specify the subrate as the data rate you configured on the CSU in the format **xKb** or **x.xMb**. For Digital Link CSUs, you can specify the subrate value to match the data rate configured on the CSU in the format **xkb** or **x.xMb**. For a list of supported values, enter **?** after the **compatibility-mode digital-link subrate** option.

- Kentrox: You must specify the subrate as a value from 1 through 69 that exactly matches the value configured on the CSU. A subrate value of 69 corresponds to 34.995097 Mbps, or 79.17 percent of the HDLC-encapsulated payload (44.2 Mbps). A subrate value of 1 corresponds to 999.958 Kbps, which is 2.26 percent of the HDLC-encapsulated payload. Each increment of the subrate value corresponds to a rate increment of about 0.5 Mbps.

- Larscom: You must specify the subrate as a value from 1 through 14 that exactly matches the value configured on the CSU. A subrate value of 14 corresponds to 44.2 Mbps, or 100 percent of the HDLC-encapsulated payload. A subrate value of 1 corresponds to 44.2/14, which is 3.16 Mbps, 7.15 percent of the HDLC-encapsulated payload.
- Verilink: You must specify the subrate as a value from 1 through 28 that exactly matches the value configured on the CSU. To calculate the maximum allowable peak rate, multiply the configured subrate by 1.578 Mbps. For example, a subrate value of 28 corresponds to 28 multiplied by 1.578 Mbps, which is 44.2 Mbps, 100 percent of the HDLC-encapsulated payload. A subrate value of 1 corresponds to 1.578 Mbps, 3.57 percent of the HDLC-encapsulated payload. A subrate value of 20 corresponds to 20 multiplied by 1.578 Mbps, which is 31.56 Mbps, 71.42 percent of the HDLC-encapsulated payload.

Remote Loopback Response

The T1 facilities data-link loop-request signal is used to communicate various network information in the form of in-service monitoring and diagnostics. Extended superframe (ESF), through the facilities data link (FDL), supports non intrusive signaling and control, thereby offering clear-channel communication. Remote loopback requests can be over the FDL or inband. To configure the interface to respond to remote-loopback requests, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the following, then click **Apply**:

T1 Options
Remote Loopback Respond: (select)

CLI

```
set interface interface t1-options remote-loopback-respond
save
```

FEAC Response

The T3 far-end alarm and control (FEAC) signal is used to send alarm or status information from the far-end terminal back to the near-end terminal and to initiate T3 loopbacks at the far-end terminal from the near-end terminal.

To allow the remote Channel Service Unit (CSU) to place the local routing platform into loopback, you must configure the routing platform to respond to the CSU's FEAC request with the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Select the following, then click **Apply**:

T3 Options
Remote Loopback Respond: (select)

CLI

```
set interface interface t3-options feac-loop-respond
save
```

NOTE: If you configure remote or local loopback with the T3 loopback option, the routing platform does not respond to FEAC requests from the CSU even if you include the feac-loop-respond option in the configuration. In order for the routing platform to respond, you must delete the **loopback** option from the configuration.

Time Slots

Time slots, also known as channels or connectors, are used with T1 and E1 links and allow users to fraction pin usage or use all of them a create a single link.

Fractional T1

You can designate any combination of time slots. For a T1 interface, the time-slot range is from 1 through 24.

NOTE: Use hyphens to configure ranges of time slots. Use commas to configure discontinuous time slots. Do not include spaces.

To allocate a specific set of time slots to a fractional T1 interface, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Enter the following, then click **Apply**:

T1 Options
Timeslots: **1-5,10,24**

CLI

```
set interface interface t1-options timeslots 1-5,10,24
save
```

Fractional E1

You can designate any combination of time slots. ScreenOS reserves shot 1 for framing and cannot be used to configure a fractional E1 interface. For an E1 interface, the time-slot range is from 2 through 32.

NOTE: Use hyphens to configure ranges of time slots. Use commas to configure discontinuous time slots. Do not include spaces.

To allocate a specific set of time slots to a fractional E1 interface, use the WebUI or CLI:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Enter the following, then click **Apply**:

E1 Options
Timeslots: **4-6,11,25**

CLI

```
set interface interface e1-options timeslots 4-6,11,25
save
```

Bit-Error Rate Testing

Bit-error rate testing (BERT) checks the quality of links and allows you to troubleshoot interface errors. You can configure some of the WAN interfaces to execute a BERT when the interface receives a request to run this test.

A BERT requires a line loop to be in place on either the transmission device or the far-end router. The local router generates a known bit pattern then sends it out the transmit path. The received pattern is then verified against the sent pattern. The higher the bit-error rate (BER) of the received pattern, the worse the noise is on the physical circuit. As you move the position of the line loop increasingly downstream toward the far-end router, you can isolate the troubled portion of the link.

Before you can start BERT, disable the interface with the **set interface** *interface* **disable** CLI command.

To configure the BERT parameters, perform the following steps:

1. Set the bit pattern or algorithm to send on the transmit path
2. Set the error rate to monitor when receiving the inbound pattern. You specify this rate in the form of an integer from 0 (the default) through 7, which corresponds to a BER from 10^{-0} (1 error per bit) to 10^{-7} (1 error per 10 million bits)
3. Set the test duration
4. Save your configuration
5. Start the BERT test

In this example you set the T3 interface BERT parameters to run the test for 60 seconds, with the algorithm of pseudo-2t35-o151, and error rate of 10^{-4}:

WebUI

Network > Interfaces > List > Edit (*WAN Interface*) > WAN: Enter the following, then click **Apply**:

BERT Algorithm: pseudo-2e9-o153 (select)
BERT Error Rate: 4
BERT Test Length: 60
Loopback mode: None (select)

CLI

```
set interface serial1/0 t3-options bert-algorithm pseudo-2t35-o151
set interface serial1/0 t3-options bert-error-rate 4
set interface serial1/0 t3-options bert-period 60
```

```
save
exec interface serial1/0 bert-test start
```

NOTE: If you want to terminate the test sooner, use the **exec interface** *interface* **bert-test stop** CLI command.

To view the results of the BERT, use the **get counter statistics interface** *interface* **extensive** CLI command.

NOTE: To exchange BERT patterns between a local and a remote routing platform, include the loopback remote option in the interface configuration at the remote end of the link. From the local routing platform, issue the **exec interface** *interface* **bert-test start** CLI command.

You can determine whether there is an internal or an external problem by checking the error counters in the output with the **show interface** *interface* **extensive** CLI command.

ISDN Options

The minimum ISDN options you must configure is the ISDN switch type. The other options are determined by your Carrier.

Switch Type

The supported ISDN switch types are ATT5E, NT DMS-100, INS-NET, ETSI, and NI1.

WebUI

Network > Interfaces > List > Edit (*bri*) > **WAN**: Enter the following, then click **Apply**:

Switch Type After Reboot:

CLI

```
set interface bri0/0 isdn switch-type att5e
```

SPID

If you are using an ISP that requires a Service Profile Identifier (SPID), your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the ISP when it accesses the switch to initialize the connection.

A SPID is usually a seven-digit telephone number with some optional numbers. However, different ISPs may use different numbering schemes. For the DMS-100 switch type, two SPIDs are assigned, one for each B-channel. Your Carrier defines the SPID numbers.

Currently, only the DMS-100 and NI1 switch types require a SPID. The AT&T 5ESS switch type may support a SPID, but we recommend that you set up that ISDN service without one. In addition, SPIDs have significance at the local access ISDN interface only. Remote routers never receive the SPID.

WebUI

Network > Interfaces > List > Edit (*bri*) > **ISDN**: Enter the following, then click **Apply**:

SPID1:123456789
SPID2:987654321

CLI

```
set interface bri0/0 isdn spid1 123456789
```

TEI Negotiation

Terminal Endpoint Identifier (TEI) negotiation is useful for switches that may deactivate Layer 1 or 2 when there are no active calls. Typically, this setting is used for ISDN service offerings in Europe and connections to DMS-100 switches that are designed to initiate TEI negotiation.

WebUI

Network > Interfaces > List > Edit (*bri*) > **ISDN**: Enter the following, then click **Apply**:

TEI negotiation:First Call

CLI

```
set interface bri0/0 isdn tei-negotiation first-call
```

You can have TEI negotiation occur when the first call is made (default) or at device power up.

Calling Number

A router with an ISDN BRI might need to supply the ISDN with a billing number for outgoing calls. Some networks offer better pricing on calls where the number is presented. When configured, this information is included in the outgoing call-setup message.

WebUI

Network > Interfaces > List > Edit (*bri*) > **ISDN**: Enter the following, then click **Apply**:

Calling Number:1234567890

CLI

```
set interface bri0/0 isdn calling-number 1234567890
```

The calling number must be a string with fewer than 32 characters.

T310 Value

If the security device does not receive an ALERT, a CONNECT, a DISC, or a PROGRESS message after receiving a CALL PROC message, it sends a DISC message out to the network after the T310 timeout value expires.

WebUI

Network > Interfaces > List > Edit (*bri*) > **ISDN**: Enter the following, then click **Apply**:

T310 Value:20

CLI

```
set interface bri0/0 isdn t310-value 20
```

You can enter a value between 5 and 100 seconds. The default T310 timeout value is 10 seconds.

Send Complete

In some geographic locations, such as Hong Kong and Taiwan, ISDN switches require that the Sending Complete Information Element be added in the outgoing call-setup message to indicate that the entire number is included. This IE is generally not required in other locations.

WebUI

Network > Interfaces > List > Edit (*bri*) > **ISDN**: Enter the following, then click **Apply**:

Send Complete: check

CLI

```
set interface bri0/0 isdn sending-complete
```

The default setting does not include the send complete information element.

BRI Mode

The ISDN interface (bri) can be configured for leased line mode or as a dialer.

Leased-Line Mode

The BRI can be configured to support leased-line mode, which eliminates signaling on the D-channel. If the BRI is configured for leased-line mode, it becomes a Layer 3 interface that can only deliver data. If you have the BRI in leased-line mode, you must also provide the IP address of the security device and include PPP encapsulation in your BRI configuration.

The Q931 dialing is not required to setup a channel. For more information on the Q931 and Q921 protocols, refer to the *ScreenOS Command Line Reference Guide*. All other ISDN options do not function in the leased-line mofe.

WebUI

Network > Interfaces > List > Edit (*bri*) > Enter the following, then click **Apply**:

BRI Mode
Leased Line (128kps): check

CLI

```
set interface bri0/0 isdn leased-line 128kbps
```

Dialer Enable

If an ISDN BRI is set to enable dialing, the BRI can act as a dialer interface. The BRI must be configured as a dialer interface before it can provide Dial-on-Demand Routing (DDR). By default, an ISDN BRI is not dialer-enabled.

WebUI

Network > Interfaces > List > Edit (*bri*) > Enter the following, then click **Apply**:

BRI Mode
Dial using BRI: check

CLI

```
set interface bri0/0 isdn dialer-enable
```

When you click apply, the Dialer Options appear. For more information on configuring the dialer options, see the following section, “Dialer Options”.

Dialer Options

The dialer interface name is formatted as **dialer*x***, where *x* is a number from 0 to 9. If a dialer interface has not yet been created, the dialer interface with the number you specify is automatically created.

The following dialer options can be set using **set interface dialer*x*** command:

- Primary/alternate number(s)

The primary number provides a remote destination for the security device to call. If the primary number is not connected, the alternate number is used. The primary and alternate numbers can be any string length less than 32 characters.

- Load threshold

  This option provides additional bandwidth on demand. If you set this option and the traffic exceeds the load threshold you specified for one B-channel, then the second B-channel is utilized. The range for the B-channel load threshold is 1 to 100 (in percent). The default is 80 percent.

- Idle time

  Use this option to set the amount of time (in seconds) you want the device to wait for traffic before it drops the connection. The idle time can be set for 0 to 60000 seconds, where a setting of zero (0) means the connection cannot be idle. The default is 180 seconds.

- Retry times

  Use this option to set the number of attempts you want the security device to dial the phone number specified. If the call does not connect, the number is redialed (one to six times) the number of attempts specified. The default is three attempts.

- Interval

  Use this option to set the dial interval (in seconds) between redial attempts caused by no connection. You can specify 1 to 60 seconds; the default is 30 seconds.

- Dialer pool

  Use this option to identify the dialer pool that you want the dialer interface to use. The dialer pool identification can be any string length less than 32 characters.

Use the following command to create a dialer interface:

WebUI

Network > Interfaces > List > New > **Dialer IF**: Enter the following, then click **Apply**:

Interface Name: dialerx
Primary Number: 16900
Alternate Number: 44440
Load Threshold: 80
Idle Time:100
Retry times:3
Interval:30
Dailer Pool:

CLI

```
set interface dialerx primary-number 16900
set interface dialerx alternative-number 44440
set interface dialerx load-threshold 80
set interface dialerx idle-time 100
set interface dialerx retry 30
```

Disabling a WAN Interface

You can disable a WAN interface using either the WebUI or the CLI.

WebUI

Network > Interfaces > Edit (*interface*) > WAN: Deselect the Enable checkbox, then click **Apply**.

CLI

```
set interface interface disable
save
```

WAN Interface Encapsulation

After the WAN interface is configured, interface encapsulation can be set. This section describes the following WAN interface encapsulation types:

- "Point-to-Point Protocol (PPP)" on this page
- "Frame Relay" on page 31
- "Cisco-High-Level Data Link Control (Cisco-HDLC)" on page 32

Single Interface Encapsulation Option	Encapsulation Type Supported
Unnumbered Interfaces	PPP, FR, and Cisco-HDLC
Protocol MTU	PPP and FR
Static IP	PPP and Cisco-HDLC
Keepalives	PPP, FR, and Cisco-HDLC
Keepalive LMI	FR

Point-to-Point Protocol (PPP)

Point-to-Point Protocol (PPP) links provide full-duplex, simultaneous, bidirectional operation and are a common solution for easy connection of a wide variety of hosts, bridges, and routers.

PPP encapsulation allows different Network Layer protocols to be multiplexed simultaneously over commonly used physical links. PPP uses High-Level Data Link Control (HDLC) for packet encapsulation. HDLC is a bit-oriented, synchronous, Data Link Layer protocol that specifies a data-encapsulation method on synchronous serial links using frame characters and checksums. PPP encapsulation is defined in RFC 1661, *The Point-to-Point Protocol (PPP)*.

To establish a PPP connection, each end of a PPP link configures the link by exchanging Link Control Protocol (LCP) packets. LCP is used to establish, configure, and test data-link options. These options include encapsulation format options; authentication of the peer on the link; handling of varying limits on sizes of packets, detecting a looped-back link, and other common misconfiguration errors; determining when a link is functioning properly or failing; and terminating the link.

PPP allows for authentication during link-establishment to permit or deny connection to a device. This authentication can be performed using either Password Authentication Protocol (PAP) or Challenge-Handshake Authentication Protocol (CHAP), as documented in RFC 1334, *PPP Authentication Protocols*. These authentication protocols are intended for use primarily by hosts and routers that connect to a network server over switched circuits or dial-up lines, but they can also be used with dedicated lines.

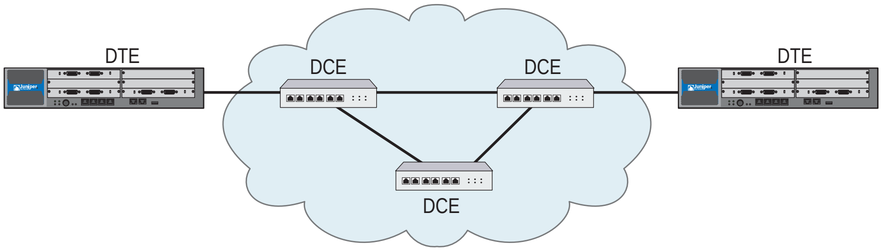
Frame Relay

Frame Relay is a WAN protocol that operates at the Data Link Layer of the Open Systems Interconnection (OSI) Reference Model. Frame Relay encapsulation is defined in RFC 1490, *Multiprotocol Interconnect over Frame Relay*, and in the Frame Relay Forum Implementation Agreement FRF3.1/3.2.

The Frame Relay protocol allows you to reduce costs by using shared data-transmission facilities that are managed by a Frame Relay service provider. You pay fixed charges for the local connections from each site in the Frame Relay network to the first point of presence (POP) in which the provider maintains a Frame Relay switch. The portion of the network between Frame Relay switches is shared by all customers of the service provider.

Figure 7 depicts the devices in a Frame Relay network.

Figure 7: Devices in the Frame Relay Network



Two categories of device can be attached to a Frame Relay network:

- **Data terminal equipment (DTE)** devices are generally the terminating equipment for a specific network and are typically located on the customer premises.

- **Data circuit-terminating equipment (DCE)** devices are generally carrier-owned internet-working devices that provide switching services in a network. DCEs are typically packet switches.

A Frame Relay permanent virtual circuit (PVC) provides a logical connection between two DTE devices across a Frame Relay network. A number of PVCs can be multiplexed into a single physical circuit for transmission across the network. Each PVC is assigned a unique data-link connection identifier (DLCI) to ensure that each customer receives only their own traffic.

Cisco-High-Level Data Link Control (Cisco-HDLC)

The default protocol for serial interfaces on Cisco routers and bridges is Cisco High-Level Data Link control (Cisco-HDLC). Cisco-HDLC is used to encapsulate local area network (LAN) protocol packets for transfer over WAN links.

Cisco-HDLC is an extension to the standard HDLC protocol developed by the International Organization for Standardization (ISO). HDLC is a bit-oriented, synchronous, Data Link Layer protocol that specifies a data-encapsulation method on synchronous serial links using frame characters and checksums.

Cisco-HDLC monitors line status on a serial interface by exchanging keepalive messages with peer network devices. A keepalive message is a signal from one endpoint to the other that the first endpoint is still active. Keepalives are used to identify inactive or failed connections. Keepalives can also allow routers to discover IP addresses of neighbors by exchanging Serial Line Address Resolution Protocol (SLARP) address-request and address-response messages with peer network devices.

Basic Encapsulation Options

To configure encapsulation on a WAN interface, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (WAN *interface*): Select the *WAN Encapsulation type* and the *Security zone*, then click **Apply**.

(Optional) Configure encapsulation options for the physical link. This step is required only if you need to change the default HDLC options for a link.

CLI

set interface *interface* encapsulation *type*
set interface *interface* zone *zone*

NOTE: You configure the physical link by configuring the interface that represents the link.

Unnumbered Interfaces

An unnumbered interface is not assigned its own IP address but instead borrows an IP address from other interfaces. In this way, address space is conserved. If an unnumbered interface is pointing to an interface that is not functioning (Interface status UP or Protocol UP is not displayed), then the unnumbered interface also does not function. We recommend that unnumbered interfaces point to a loopback interface since loopback interfaces do not fail.

To configure an IP unnumbered interface, use the WebUI or the CLI:

WebUI

Network > Interface > Edit (*WAN interface*): Select the **Unnumbered option**, select the source interface, then click **Apply**.

CLI

set interface *interface* ip unnumbered interface *src interface*

```
save
```

Protocol Maximum Transmission Unit Configuration

You can configure the protocol Maximum Transmission Unit (MTU) on each physical interface with PPP or Frame Relay encapsulation. The default protocol MTU is 1500 bytes for serial, T1, E1, and multilink interfaces, and 4470 bytes for T3 interfaces. You can specify a value from 800 to 8192 bytes.

The media MTU is derived from the protocol MTU. If you increase the size of the protocol MTU, you must ensure that the size of the media MTU is equal to or greater than the sum of the protocol MTU and the encapsulation overhead.

To configure the protocol MTU on a physical interface, use the WebUI or the CLI:

WebUI

Network > Interfaces > Edit (WAN *interface*): Enter a value between 800 and 8192 in the **Maximum Transfer Unit (MTU)** field, then click **OK**.

CLI

```
set interface interface mtu number
save
```

Static IP Address Configuration

A WAN interface uses an IP address dynamically assigned by a server at the other end of the WAN data link. Alternatively, you can explicitly assign a static IP address to the interface.

To assign an IP address to the WAN interface, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (WAN *interface*): Enter an IP address and netmask in the **IP Address/Netmask** fields, then click **Apply**.

CLI

```
set interface interface ip ip_addr/mask
save
```

Keepalives

A keepalive message is a signal from one endpoint to the other that the first endpoint is still active. Keepalives are used to identify inactive or failed connections. Physical interfaces configured with WAN encapsulation send keepalive packets at 10-second intervals.

To configure the interface to send keepalive packets at a different interval, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (WAN *interface*) > *WAN Encapsulation type*: Enter the number of seconds in **Keepalive Interval**, then click **Apply**

CLI

```
set interface interface keepalives seconds
save
```

To disable the sending of keepalives on a physical interface, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*WAN interface*) > *WAN Encapsulation type*: Deselect the **Keepalive** checkbox, then click **Apply**.

CLI

```
unset interface interface keepalives
save
```

The receipt of keepalive packets by a destination determines whether the link is down or up. By default, if a destination fails to receive three successive keepalive packets, ScreenOS determines that the link is down. A down link returns to up when the destination receives a single keepalive packet.

To change the counts by which the destination determines a link to be down or up, use the WebUI or the CLI:

WebUI

Network > Interfaces > Edit (*interface*) > *WAN Encapsulation type*: Enter the number of counts for **Down Counter** or **Up Counter**, then click **Apply**.

CLI

```
set interface interface keepalives down-count number
set interface interface keepalives up-count number
save
```

PPP Encapsulation Options

This section explains the Point-to-Point Protocol (PPP) encapsulation options that are available on some WAN interfaces. To configure MLPPP, see “Multi-Link PPP Configuration Options” on page 45.

To configure PPP on a single physical link on an device that supports WAN interfaces:

1. Configure PPP encapsulation on the physical link, and assign the link to a security zone. Configure the IP address on the physical link.

2. (Optional) Configure PPP options for the physical link. This step is required only if you need to change the default PPP options for the link.

3. Configure a PPP access profile, and bind it to the interface. This step is required even if no authentication is used on the PPP data link.

4. (Optional) If CHAP or PAP authentication is used, configure the peer’s username and password in the local database of the device.

PPP Access Profile

A PPP access profile includes the following information:

- Whether authentication is used to permit or deny connection to devices during Link Control Protocol (LCP) link setup. If authentication is specified, you can configure options for the selected authentication method.

NOTE: Even if no authentication is used on the PPP connection, you must configure an access profile that specifies no authentication method and bind it to the interface.

- Whether the interface uses a static IP address that you have already configured. If the interface uses an IP address dynamically assigned by a server, you can specify the netmask for the IP address.

During LCP link setup, authentication can be used to permit or deny connection to devices; if authentication fails, the PPP link is terminated. By default, authentication is disabled on interfaces that are configured for PPP encryption. If you do not explicitly enable authentication on the interface, the interface makes no authentication requests and denies all incoming authentication challenges.

You can configure interfaces to support one or both of the following authentication protocols:

- Password Authentication Protocol (PAP), as defined in RFC 1334, *PPP Authentication Protocols*
- Challenge Handshake Authentication Protocol (CHAP), as defined in RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*

To configure a WAN interface with PPP encapsulation, do the following with the WebUI or CLI:

WebUI

Network > PPP > PPP Profile > New: Enter *profile_name* in the **PPP Profile** field and enter other options, then click **OK**.

Network > Interfaces > Edit (*WAN interface*): Select the *profile_name* in the **Binding a PPP Profile** dropdown list, then click **Apply**.

CLI

```
set ppp profile profile_name ...
set interface interface ppp profile profile_name
save
```

PPP Authentication Method

During LCP link setup, authentication can be used to permit or deny connection to devices; if authentication fails, the PPP link is terminated. To se the PPP authentication method, use the WebUI or CLI:

WebUI

Network > PPP > PPP Profile > Edit (*profile_name*): Select **Any**, **CHAP**, **PAP**, or **none**, then click **OK**.

CLI

```
set ppp profile profile_name { chap | pap | any | none }
save
```

If you use a static IP address in an access profile, you can only bind the profile to an interface that has an explicitly configured IP address. Conversely, if an interface has a static IP address, the access profile you bind to the interface must specify the static IP option.

If the IP address for the interface is dynamically assigned by a server, the netmask for the interface is /32 (255.255.255.255). To specify a different netmask value for the interface, use the WebUI or CLI:

WebUI

Network > PPP > PPP Profile > Edit (*profile_name*): Enter a new *mask* value in the **Netmask** field, then click **OK**.

CLI

```
set ppp profile profile_name netmask mask
save
```

Password

The password is used to authenticate the PPP client on the interface with its peer. To set the password, use the WebUI or CLI:

WebUI

Network > PPP > PPP Profile > Edit (*profile_name*): Enter a string in **Password**, then click **OK**.

CLI

```
set ppp profile profile_name auth secret password
save
```

PPP Authentication Protocols

This section explains the PPP authentication protocols that are available on some of the WAN interfaces.

Challenge Handshake Authentication Protocol (CHAP)

When Challenge Handshake Authentication Protocol (CHAP) authentication is enabled on an interface, the interface uses the system hostname as the name sent in challenge and response packets. You can configure a different name for the interface to use in challenge and response packets. To change the CHAP local name, use the WebUI or CLI:

WebUI

Network > PPP > PPP Profile > Edit (*profile_name*): Enter a name in the **Local Name** field, then click **OK**.

CLI

```
set ppp profile profile_name auth local-name name
save
```

By default, when PPP authentication is enabled on the interface, the interface always challenges its peer and responds to challenges from its peer. You can configure the interface not to challenge its peer and to respond only when challenged (this behavior is called *passive mode*).

NOTE: Passive mode only works for Challenge Handshake Authentication Protocol (CHAP).

To enable passive mode, use the WebUI or CLI:

WebUI

Network > PPP > PPP Profile > Edit (*profile_name*): Select **Passive**, then click **OK**.

CLI

```
set ppp profile profile_name passive
save
```

Password Authentication Protocol (PAP)

The Password Authentication Protocol (PAP) uses a two-way handshake and transmits account names and passwords over the link in clear text. Systems generally use PAP only when they have no other authentication protocols in common.

To set the authentication protocol to PAP, use the WebUI or CLI:

WebUI

Network > PPP > Edit (profile_name): Select the Authentication type, then click **Apply**.

CLI

```
set ppp profile profile_name auth type pap
save
```

Local Database User

If CHAP or PAP is used on the PPP link, the peer device sends its username and password to the device for authentication. The device compares the received username and password with WAN user-type entries configured in its local database. Only a peer whose username and password match an entry in the local database is allowed to connect to the device to send or receive data.

To configure a WAN user, use the WebUI or CLI:

WebUI

Objects > Users > Local > New: Enter the following, then click **OK**:

WAN User: (select)
User Name: *name_str*
User Password: *pswd_str*
Confirm Password: *pswd_str*

CLI

```
set user name_str password pswd_str
set user name_str type wan
save
```

NOTE: WAN users can only be configured in a local database.

Frame Relay Encapsulation Options

This section describes how to configure Frame Relay encapsulation options that are available on some WAN interfaces. To configure MLFR, see “Multi-Link Frame Relay Configuration Options” on page 46.

NOTE: Make sure that the Main Link option is selected in the Basic Properties page for the WAN interface.

Keep Alive Messages

Frame Relay keepalive messages are implemented by the sending of Local Management Interface (LMI) packets. ScreenOS sends LMI keepalive messages by default on a Frame Relay interface.

For back-to-back Frame Relay connections, either disable the sending of keepalives on both sides of the connection, or configure one side of the connection as DTE (the default ScreenOS configuration) and the other as DCE.

If keepalives are enabled, the number of possible DLCI configurations on a multipoint or multicast connection is limited by the MTU size selected for the interface. To calculate the available DLCIs, use the following formula:

(MTU – 12) / 5

To increase the number of possible DLCIs, disable keepalives. To disable the sending of keepalives on a physical interface, you use the WebUI or the CLI.

WebUI

Network > Interfaces > Edit (*interface*) > FR: Select **No-Keepalive**, then click **Apply**.

CLI

```
set interface interface frame-relay lmi no-keepalive
save
```

Frame Relay LMI Type

By default, ScreenOS sends LMIs specified by ANSI T1.617 Annex D. To change the LMI type to ITU Q933 Annex A, use the WebUI or the CLI:

WebUI

Network > Interfaces > Edit (WAN *interface*) > FR: Select **ITU**, then click **Apply**.

CLI

```
set interface interface frame-relay lmi type itu
save
```

You can configure the following Frame Relay LMI keepalive options:

- **DTE full status polling interval** (denoted by the n391-dte keyword in the CLI). The DTE sends a status inquiry to the DCE at the interval specified by the DTE polling timer. The polling interval specifies the frequency at which these inquiries receive a full status report; for example, a value of 10 would specify a full status report in response to every tenth inquiry. The intermediate inquiries request a keepalive exchange only.

- **DTE error threshold** (denoted by the n392-dte keyword in the CLI). The number of errors required to bring down the link, within the event-count specified by the DTE monitored event-count.

- **DTE monitored event-count** (denoted by the n393-dte keyword in the CLI). The range is from 1 through 10, with a default value of 4.

- **DTE keepalive timer** (denoted by the t391-dte keyword in the CLI). The period at which the DTE sends out a keepalive response request to the DCE and updates status depending on the DTE error-threshold value.

To configure Frame Relay LMI options, use the WebUI or the CLI:

WebUI

Network > Interfaces > Edit (WAN *interface*) > FR: Enter appropriate values for the LMI options, then click **Apply**.

CLI

```
set interface interface frame-relay lmi option
save
```

Creating and Configuring PVCs

Within a single Frame Relay physical interface you can create multiple point-to-point virtual interfaces, which are identified as subinterfaces. Each subinterface maps to a permanent virtual circuit (PVC), which is identified by a data-link connection identifier (DLCI). You can specify only one DLCI for each subinterface. The DLCI is a value from 16 through 1022. (Numbers 1 through 15 are reserved.) You can choose to multiplex a number of PVCs onto a single physical link for transmission across a Frame Relay packet-switched network.

NOTE: The DLCI value you specify is the DLCI that your local provider has assigned to your PVC.

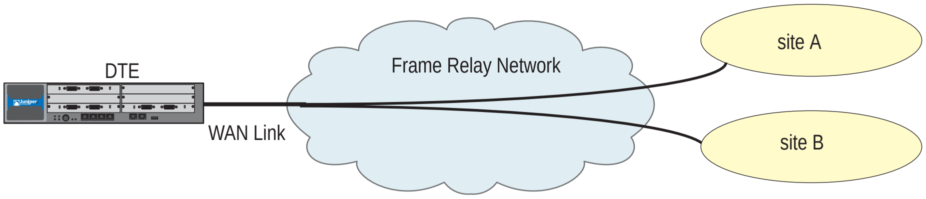
The subinterface name consists of the physical interface name and a subinterface number. For example, if the physical interface name is **serial1/1**, its subinterfaces can be **serial1/1.1** and **serial1/1.2**.

NOTE: In the WebUI, the subinterface number is automatically added when you select the interface name. In the CLI, you must enter both the interface name and the subinterface number.

You can also configure the subinterface for management functions such as a manage IP address, service options, and other features. (For more information about configuring manage IP and service options on an interface, see *Volume 2: Fundamentals*.)

Figure 8 illustrates two point-to-point PVCs configured for the physical interface serial1. You can associate each PVC with a different security zone; the security zone for each PVC can be different from the security zone assigned to the physical interface.

Figure 8: Point-to-Point Frame Relay Subinterfaces



To configure a point-to-point Frame Relay subinterface, create the subinterface and assign it to a security zone, then assign a Frame Relay DLCI and an IP address to the subinterface, use the WebUI or CLI:

NOTE: You can assign a subinterface to a different security zone from that assigned to the physical interface.

WebUI

Network > Interface > New > WAN Sub-IF: Enter the following, then click **OK**:

Interface Name: *interface* (select)
Zone Name: (select)
Frame Relay DLCI: (enter *id_num*)
IP Address/Netmask: (enter *ip_addr*)

CLI

```
set interface subinterface zone zone
set interface subinterface frame-relay dlci id_num
set interface subinterface ip ip_addr
save
```

Inverse Address Resolution Protocol

Frame Relay subinterfaces can support inverse Address Resolution Protocol (ARP), as described in RFC 2390, *Inverse Address Resolution Protocol*. When inverse ARP is enabled, the device responds to received inverse Frame Relay ARP requests by providing IP address information to the requesting device on the other end of the Frame Relay PVC. The device does not initiate inverse Frame Relay ARP requests.

By default, inverse Frame Relay ARP is disabled. To configure a device to respond to inverse Frame Relay ARP requests, use the WebUI or the CLI:

WebUI

Network > Interface > Edit (*subinterface*): Select **Frame Relay Inverse ARP**, then click **Apply**.

CLI

```
set interface subinterface frame-relay inverse-arp
save
```

Multi-Link Encapsulation

This section provides the following information about Multi-link encapsulation on WAN interfaces:

- "Multi-Link Encapsulation Overview"
- "Basic Multi-Link Bundle Configuration" on page 42
- "Multi-Link PPP Configuration Options" on page 45
- "Multi-Link Frame Relay Configuration Options" on page 46

Multi-Link Encapsulation Overview

WAN interfaces support Multilink Frame Relay (MLFR) and Multilink Point-to-Point Protocol (MLPPP) for User-to-Network Interface (UNI), based on the Frame Relay Forum FRF.16, *Multilink Frame Relay UNI/Network-to-Network Interface (NNI) Implementation Agreement*. Both multilink encapsulation types provide a cost-effective way to increase bandwidth for applications by enabling multiple physical links to be aggregated into a *bundle*. Each physical link in the bundle is referred to as a *bundle link*. For example, if an application requires more bandwidth than is available on a single T1 line, you have two choices to increase bandwidth for the application's use:

- Lease a T3 line
- Bundle multiple T1 links

MLFR and MLPPP also provides fault-tolerance. For example, when a single bundle link in the bundle fails, the bundle continues to support Frame Relay or PPP services by transmitting across the remaining bundle links. MLFR and MLPPP also provide load balancing across the links within a bundle. If a bundle link chosen for transmission is busy transmitting a long packet, another link transmits the data.

Multi-link Encapsulation Options	Encapsulation Type Supported
Minimum Links	MLPPP and MLFR
Fragment Threshold	MLPPP and MLFR
MRRU	MLPPP
Drop Timeout	MLPPP and MLFR
Acknowledge Retries	MLFR
Acknowledge Time	MLFR
Hello Timer	MLFR

Basic Multi-Link Bundle Configuration

A bundle is accessed by a multilink interface that you create. The name of the multilink interface must be ml*id_num*. For example, multilink interface names can be **ml1**, **ml2**, and so on.

NOTE: In the WebUI, *id_num* is automatically added when you create a new multilink interface. In the CLI, you must specify an *id_num* value.

NOTE: By default, the encapsulation type for new multilink interfaces is MLPPP. You must explicitly configure MLFR encapsulation on multilink interfaces that support Frame Relay.

To create a multilink interface and configure it for MLFR encapsulation, use the WebUI or the CLI:

WebUI

Network > Interfaces > New > Multilink IF: Select **Multi-Link Frame Relay** for the WAN Encapsulation, then click **Apply**.

CLI

```
set interface interface encapsulation mlfr-uni-nni
save
```

Bundle Identifier

The bundle ID, as specified by FRF.16, associates a local and a remote endpoint with a specific bundle. All bundle links in the ML bundle must use the same bundle ID, which can be up to 80 bytes. If you are configuring more than one bundle between two devices, each bundle ID should be unique. For example, you can use network node identifiers, system serial numbers, or network addresses for bundle IDs.

If you do not configure a specific bundle ID for the multilink interface, the multilink interface name (for example, **ml1** or **ml2**) is used. To configure a bundle ID, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*interface*) > Basic: Enter the *ML Type* for the WAN Encapsulation, then click **Apply**.

CLI

```
set interface interface bundle-id name_str
save
```

Drop Timeout

You can configure a drop-timeout value to provide a recovery mechanism if individual links in the multilink bundle drop one or more packets. Drop timeout is not a differential delay-tolerance setting and does not limit the overall latency. We recommend setting a drop-timeout value significantly larger than the expected differential delay across the links; this way, the timeout period elapses when there is actual packet loss and not under normal jitter conditions.

To configure the drop-timeout value, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*interface*) > *ML Encapsulation Type*: Enter the number of milliseconds in **Drop Timeout**, then click **Apply**.

CLI

```
set interface interface drop-timeout milliseconds
save
```

We do not recommend settings of less than 5 milliseconds; zero (0) disables the timeout.

NOTE: For multilink interfaces, a packet or fragment that encounters an error condition in the network while bound for a disabled bundle or link does not contribute to the dropped packet and framecount in the per-bundle statistics. ScreenOS counts the packet under the global error statistics but not in the global output bytes or output packet counts. This unusual accounting situation happens only if the error conditions are generated inside the multilink interface and not if the packet encounters errors elsewhere in the network.

The minimum-links value can be from 1 to 8. If you specify 8, all configured links of a bundle must be up in order for the bundle to be up.

Fragment Threshold

You can configure a fragmentation threshold to set a maximum size for packet payloads transmitted across the individual links within the multilink circuit. ScreenOS splits any incoming packet that exceeds the fragmentation threshold into smaller units suitable for the circuit size; it reassembles the fragments at the other end but does not affect the output traffic stream.

To configure the fragment threshold, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*interface*) > *ML Encapsulation Type*: Enter a value for **Bundle-link Fragmentation Threshold**, then click **Apply**.

CLI

```
set interface interface mlfr-uni-nni fragment-threshold number
save
```

By default, the fragment threshold is the MTU of the physical interface. (For serial, T1, and E1 bundle links, the default MTU size is 1500 bytes; for T3 bundle links, the default MTU size is 4470 bytes.) The maximum fragment size can be from 128 through 16,320 bytes. Any value you set must be a multiple of 64 bytes (*N*x64).

NOTE: To ensure proper load-balancing for MLPPP WAN interfaces, do not set both fragment-threshold and short-sequence options in the configuration.

For MLPPP interfaces, if the MTU of links in a bundle is less than the bundle MTU plus encapsulation overhead, then fragmentation is automatically enabled. You should avoid this situation for MLPPP WAN interfaces on which short-sequencing is enabled.

To configure a fragmentation threshold value, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*interface*) > *ML Encapsulation Type*: Enter a value for **Fragment Threshold**, then click **Apply**.

CLI

```
set interface interface fragment-threshold bytes
save
```

Minimum Links

You can set the minimum number of links that must be up in order for the entire bundle to be up. By default, only one link must be up for the bundle to be considered up.

To set the minimum number of links in a bundle, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*interface*) > *ML Encapsulation Type*: Enter a new number in **Minimum Links**, then click **Apply**.

CLI

```
set interface interface minimum-links number
save
```

Multi-Link PPP Configuration Options

This section explains the additional MLPPP configuration options available on some WAN interfaces.

Basic Configuration Steps

To configure MLPPP on an interface that supports MLPPP encapsulation:

1. Create a bundle, and configure it for MLPPP encapsulation. Assign the bundle to a security zone. You can also set other options such as a bundle identification or the MTU for the bundle.

2. (Optional) Configure MLPPP options for the bundle. This step is required only if you need to change the default MLPPP options for the bundle.

3. Configure a PPP access profile, and bind it to the interface. This step is required even if no authentication is used on the PPP data link.

4. (Optional) If CHAP or PAP authentication is used, configure the user name and password of the peer in the local database of the security device.

5. Assign bundle links to the bundle.

6. (Optional) Configure PPP options for each bundle link in the bundle. this step is required only if you need to change the default PPP options for the link.

Maximum Received Reconstructed Unit

The maximum received reconstructed unit (MRRU) is similar to a maximum transmission unit (MTU) but applies only to multilink bundles; it is the maximum packet size that the multilink interface can process. By default, the MRRU is set to 1500 bytes; you can configure a different MRRU value if the peer equipment allows it. The MRRU includes the original payload plus the 2-byte PPP header, but it does not include the additional MLPPP header applied while the individual multilink packets are traversing separate links in the bundle.

To configure a different MRRU, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*interface*) > MLPPP: Enter the number of bytes in Maximum Received Reconstructed Unit, then click **Apply**.

CLI

```
set interface interface mrru bytes
save
```

Sequence-Header Format

The sequence-header format blank and can be set to 12 or 24 bits, but 24 bits is considered the more robust value for most networks.

To configure a 12-bit sequence header format, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*interface*) > MLPPP: Select **Short-Sequence MLPPP Number**, then click **Apply**.

CLI

```
set interface interface short-sequence
save
```

Multi-Link Frame Relay Configuration Options

This section explains the additional MLFR configuration options available on some WAN interfaces.

Basic Configuration Steps

To configure MLFR on an interface that supports MLFR encapsulation:

1. Create a bundle, and configure it for MLFR encapsulation. Assign the bundle to a security zone. You can also set other options, such as a bundle identification or the MTU, for the bundle.

2. (Optional) Configure Frame Relay options for the bundle. This step is required only if you need to change the default Frame Relay options for the bundle.

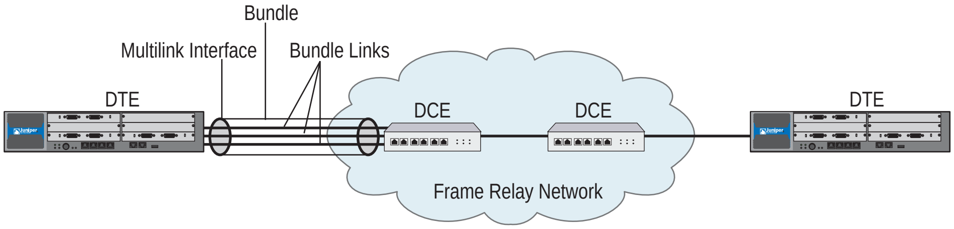
3. Assign bundle links to the bundle.

4. (Optional) Configure MLFR options for each link in the bundle. This step is required only if you need to change the default MLFR options for the link.

5. Create one or more PVCs for the bundle, and assign each PVC a Frame Relay DLCI and an IP address.

Figure 9 shows how MLFR allows multiple T1 bundle links to be aggregated into a single bundle.

Figure 9: Multilink Frame Relay Bundle



Frame Relay functions are configured on the multilink interface and not on each bundle link. (Although bundle links are visible to peer DTE and DCE devices, they are invisible to the Frame Relay Data Link Layer.) The local device and peer devices exchange Link Integrity Protocol (LIP) control messages to determine which bundle links are operational and to synchronize which bundle links are associated with each bundle.

For link management, each end of the bundle link follows the MLFR LIP and exchanges link control messages with its peer at the other end of the bundle link. To bring up a bundle link, both ends of the link must complete an exchange of ADD_LINK and ADD_LINK_ACK messages. To maintain the link, both ends periodically exchange HELLO and HELLO_ACK messages. The exchange of hello messages and acknowledgements serves as a keepalive mechanism for the link. If a device sends a hello message but does not receive an acknowledgement, it resends the hello message up to a configured maximum number of retries. If the device sends the maximum number of retries without receiving an acknowledgement, ScreenOS identifies the bundle link as down.

ScreenOS brings up the bundle link when the peer device acknowledges that it will use the link for the bundle. The link remains up when the peer device acknowledges the hello messages from the local device. When Local Management Interface (LMI) is enabled, the bundle link status is considered up when the Frame Relay Data Link Layer on the local device and on the peer device synchronize using LMI. The bundle link remains up as long as the LMI keepalives are successful.

Link Assignment for MLFR

A MLFR interface can be either DCE or DTE (the default ScreenOS configuration). The DTE acts as a master, requesting status from the DCE part of the link.

For physical links configured for MLFR encapsulation, each link endpoint in a bundle initiates a request for bundle operation with its peer by transmitting an add-link message. A hello message notifies the peer endpoint that the local endpoint is up. Both ends of a link generate a hello message periodically or as configured with the hello timer. A remove-link message notifies the peer that the local end management is removing the link from bundle operation. Endpoints respond to add-link, remove-link, and hello messages by sending acknowledgement messages.

Acknowledge Retries

For bundle links, you can configure the number of retransmission attempts to be made for consecutive hello or remove-link messages after the expiration of the acknowledgement timer. To configure the retransmission attempts, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*interface*) > MLFR: Enter a value for **Line Interface Protocol (LIP) Retransmission Count before Link-Down**, then click **Apply**.

CLI

```
set interface interface mlfr-uni-nni acknowledge-retries number
save
```

Acknowledge Timer

You can configure the maximum period to wait for an add-link acknowledgement, a hello acknowledgement, or a remove-link acknowledgement. To configure the acknowledge time, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*interface*) > MLFR: Enter a value for **Maximum Period to Wait for an Acknowledgement**, then click **Apply**.

CLI

```
set interface interface mlfr-uni-nni acknowledge-timer seconds
save
```

Hello Timer

To configure the rate at which hello messages are sent, use the WebUI or CLI:

WebUI

Network > Interfaces > Edit (*interface*) > MLFR: Enter a value for LIP Hello Keepalive Interval, then click **Apply**.

CLI

```
set interface interface mlfr-uni-nni hello-timer seconds
save
```

A hello message is transmitted after the specified period (in milliseconds) has elapsed. When the hello timer expires, a link endpoint generates an add-link message.

WAN Interface Configuration Examples

This section provides the following WAN configuration examples:

Configuring a Serial Interface

This example configures the WAN properties of a Serial interface. Once you have configured the WAN interface properties, see "Encapsulation Configuration Examples" on page 60 to configure the WAN encapsulation.

WebUI

Network > Interfaces > Edit (serial6/0) > WAN: Select the following, then click **Apply**:

```
Hold Time
    Clock Mode: Internal (select)
    Clock Rate: 8.0 (select)
DTE Options
    Line Encoding: Non-Return-To-Zero (select)
```

CLI

1. Set the clocking information

```
set interface serial6/0 serial-options clocking-mode internal
set interface serial6/0 serial-options clock-rate 8.0
```

2. Set the line encoding

```
set interface serial6/0 serial-options encoding nrz
save
```

Configuring a T1 Interface

This example configures the WAN properties of a T1 interface. Once you have configured the WAN interface properties, see "Encapsulation Configuration Examples" on page 60 to configure the WAN encapsulation.

WebUI

Network > Interfaces > Edit (serial3/0) > WAN: Select the following, then click **Apply**:

```
Hold Time
    Clock Mode: External (select)
T1 Options
    Line buildout: 0 - 132 (select)
    Line Encoding: 8-bits Zero Suppression (select)
    Byte Encoding: 8-bits per byte (select)
    Frame Checksum: 16-bits (select)
    Framing Mode: Extended Super Frame (select)
    Transmitting Flag in Idle Cycles: 0x7E (select)
    Start/End Flags on Transmission: Filter (select)
    Invert Data: (deselect)
```

CLI

1. Set the clocking source

```
set interface serial3/0 clocking external
```

2. Set the line buildout

```
set interface serial3/0 t1-options buildout 0-132
```

3. Set the line encoding

```
set interface serial3/0 t1-option line-encoding b8zs
unset interface serial3/0 t1-option invert-data
```

4. Set the byte encoding

```
set interface serial3/0 t1-option bye-encoding nx56
```

5. Set the framing options

```
set interface serial3/0 t1-options fcs 16
set interface serial3/0 t1-options framing esf
```

6. Set the flag options

```
set interface serial3/0 t1-options idle-cycle-flag flags
set interface serial3/0 t1-options start-end-flag filter
save
```

Configuring an E1 Interface

This example configures the WAN properties of a E1 interface. Once you have configured the WAN interface properties, see “Encapsulation Configuration Examples” on page 60 to configure the WAN encapsulation.

WebUI

Network > Interfaces > Edit (serial6/1) > WAN: Select the following, then click **Apply**:

```
Hold Time
    Clock Mode: External (select)
E1 Options
    Frame Checksum: 16-bits (select)
    Framing Mode: with CRC4 (select)
    Transmitting Flag in Idle Cycles: 0x7E (select)
    Start/End Flags on Transmission: Filter (select)
    Invert Data: (deselect)
    (Optional) Time slots: 2-32
```

CLI

1. Set the clocking source

```
set interface serial6/1 clocking external
```

2. Set the framing options

```
set interface serial6/1 e1-options fcs 16
set interface serial6/1 e1-options framing g704
```

3. Set the flags

```
set interface serial6/1 e1-options idle-cycle-flag flags
set interface serial6/1 e1-options start-end-flag filter
unset interface serial6/1 e1-options invert-data
```

4. (Optional) Set the time-slots

```
set interface serial6/1 e1-options timeslots 2-32
save
```

Configuring a T3 Interface

This example configures the WAN properties of a T3 interface. Once you have configured the WAN interface properties, see “Encapsulation Configuration Examples” on page 60 to configure the WAN encapsulation.

WebUI

Network > Interfaces > Edit (serial4/0) > WAN: Select the following, then click **Apply**:

```
Hold Time
    Clock Mode: External (select)
E1 Options
    Frame Checksum: 16-bits (select)
    Transmitting Flag in Idle Cycles: 0x7E (select)
    Start/End Flags on Transmission: Filter (select)
```

CLI

1. Set the clocking source

```
set interface serial4/0 clocking external
```

2. Set the framing option

```
set interface serial4/0 t3-options fcs 16
```

3. Set the flags

```
set interface serial4/0 t3-options idle-cycle-flag flags
set interface serial4/0 t3-options start-end-flag filter
save
```

Configuring your Device for ISDN Connectivity

The following steps summarize the minimum setup that is required to configure your device for ISDN using the default options:

Configuration Steps	See
1. Select the ISDN switch type.	page 53
2. Create PPP profiles.	page 53
3. Set up the ISDN Interface (BRI).	page 54
4. Route traffic through the ISDN interface (BRI).	page 58

Refer to the following sections for more details on each of the above steps.

Step 1: Selecting the ISDN Switch Type

The minimum ISDN options to configure is to select the ISDN switch type your device is connected to. For more information on other ISDN options, see “ISDN Options” on page 25.

WebUI

Network > Interfaces > List > Edit (*bri*): Select **WAN** and select the applicable option value, then click **Apply**.

```
Switch type after Reboot: etsi
```

CLI

```
set in bri0/0 isdn switch-type etsi
```

Use the **get int bri2/0 isdn** command to display the ISDN stack configuration.

Step 2: Configuring a PPP Profile

Configure a PPP profile using static or dynamic IP address.

WebUI

Network > PPP > PPP Profile > New: Enter the applicable option value, then click **OK**.

```
PPP Profile: isdn-ppp
Authentication: CHAP
Passive: Check
    Local Name: 169
    Password: 169
```

CLI

```
set ppp profile isdn-ppp
set ppp profile isdn-ppp auth local-name 169
set ppp profile isdn-ppp auth secret 169
set ppp profile isdn-ppp auth type chap
set ppp profile isdn-ppp passive
```

Step 3: Setting Up the ISDN BRI Interface

This section describes the three methods of configuring the ISDN BRI for ISDN support:

Configuring the ISDN BRI	See
Using the ISDN BRI as a dialer	"Dialing Out to a Single Destination Only" on page 54
Using the Dialer interface to dial out	"Dialing Out Using the Dialer Interface" on page 54
Using a leased line mode	"Using the Leased Line Mode" on page 58

Refer to the respective sections for examples of configuring your device for ISDN support.

Dialing Out to a Single Destination Only

In this example, you configure the ISDN interface (BRI) as the dialer to connect the endpoints at the Branch Office (see Figure 1 on page 5) to the Corporate Headquarters. Set up this configuration if you are dialing out to a single destination only when you have intermittent traffic between the two sites. The connection drops when there is no traffic.

Branch Office A on the 10.1.1.1 network dials out to Branch Office B on the 10.2.2.2/16 network or to the Corporate Headquarters on the 11.0.0.0/16 network through the bri0/0 interface.

WebUI

Network > Interfaces > List > Edit (*bri*): Select **Basic** and select the applicable option value, then click **Apply**.

BRI Mode: **Dial Using BRI**
Dialer Enable Options
  Primary Number: 16900
WAN Encapsulation: PPP

Click **Apply**

Binding a PPP Profile: isdn-ppp

CLI

```
set in bri0/0 dialer-enable
set in bri0/0 encap ppp
set in bri0/0 ppp profile isdn-ppp
set in bri0/0 primary-number 16900
```

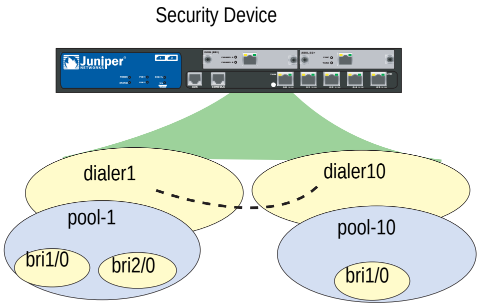
Dialing Out Using the Dialer Interface

In this example, you dial out using the dialer interface. Use this method to dial out to multiple destinations, when the number of destinations exceeds the number of available physical lines. This configuration supports dial-on-demand Routing (DDR) and bandwidth-on-demand.

The dialer pool utilizes ISDN BRI by using logical dial peers via the dialer interfaces. This separates the actual physical links from all the potential destinations. When the number of destinations exceeds the number of available physical lines, a physical interface can be configured as a member of a dialer pool. The physical interface can also belong to more than one pool, allowing the single line to be used to dial more than one destination.

Figure 10 illustrates the relationship between the dialer interface, the dialer pool and the ISDN BRI.

Figure 10: Dialing Out Using the Dialer Interface



By default, ISDN BRIs are not in any dialer pools. Also, each ISDN BRI can be added to several dialer pools.

This following section provides step-by-step instructions on configuring dialer1 and dialer10 as shown in Figure 10 on page 55 using the WebUI and CLI. At the end of the configuration, two stations at Branch Office A (see Figure 1 on page 5) can connect to Branch Office B using the dialer interface, dialer1. At the same time, another workstation at Branch Office A can dial out to the headquarters using dialer10.

1. Configure the dialer1 and dialer 10 interfaces.

   a. Create and configure the dialer interfaces.

   b. Bind the PPP profile (isdn-ppp) to the dialer interfaces.

2. Configure the dialer pools, pool-1 and pool-10.

   a. Create the two dialer pools.

   b. Bind the dialer pools to the respective dialer interfaces. Bind pool-1 to dialer1 and pool-10 to dialer10.

3. Add the ISDN interface (BRI) to the dialer pool.

   Add bri1/0 and bri2/0 to dialer pool-1.
   Add bri1/0 to dialer pool-10.

To set other BRI options, see “BRI Mode” on page 27.

WebUI

1. **Configuring the dialer1 interface**

   Network > Interface > List > New > Dialer IF: Enter the following, then click **OK**:

   Interface Name: dialer1
   Primary Number: 16900
   WAN Encapsulation: Multi-link PPP
   Zone Name: Untrust
   MTU: 1500
   Click **Apply**

   Binding a PPP Profile: isdn-ppp

   Network > Interfaces > List > Edit (*dialer1*) > **Dialer Pool**: Enter the applicable option value, then click **Apply**.

   Dialer pool: pool-1
   Click Add

   Network > Interfaces > List > Edit (*bri1/0*):

   Select **Basic** and enter the applicable option value, then click **Apply**.

   BRI Mode:
   Leased Line Mode(128kbps): uncheck
   Dial Using BRI: uncheck

   Select **Dialer Pool** and enter the applicable option value, then click **Apply**.

   Set the priority for the **pool-1** and check the Select as Member box.

   Priority: 1
   Select as Member: Check

   Network > Interfaces > List > Edit (*bri2/0*):

   Select **Basic** and enter the applicable option value, then click **Apply**.

   BRI Mode:
   Leased Line Mode(128kbps): uncheck
   Dial Using BRI: uncheck

   Select **Dialer Pool** and enter the applicable option value, then click **Apply**.

   Set the priority for the **pool-1** and check the Select as Member box.

   Priority: 1
   Select as Member: Check

2. **Configuring the dialer10 interface**

   Network > Interface > List > New > Dialer IF: Enter the following, then click **OK**:

   Interface Name: dialer10
   Primary Number: 16900
   WAN Encapsulation: Multi-link PPP

Zone Name: Untrust
MTU: 1500
Click **Apply**

Binding a PPP Profile: isdn-ppp

Network > Interfaces > List > Edit (*dialer10*) > **Dialer Pool**: Enter the applicable option value, then click **Apply**.

Dialer pool: pool-10
Click Add

Network > Interfaces > List > Edit (*bri1/0*):

Select **Basic** and enter the applicable option value, then click **Apply**.

BRI Mode:
Leased Line Mode(128kbps): uncheck
Dial Using BRI: uncheck

Select **Dialer Pool** and enter the applicable option value, then click **Apply**.

Set the priority for the **pool-10** and check the Select as Member box.
Priority: 1
Select as Member: Check

CLI

1. **Configuring the dialer1 interface**

```
set interface dialer1 zone Untrust
set interface dialer1 primary-number 16900
set interface dialer1 encap mlppp
set interface dialer1 mtu 1500
set interface dialer1 ppp profile isdn-ppp

set dialer pool name pool-1
set interface dialer1 dialer-pool pool-1

set dialer pool pool-1 member-interface bri2/0 priority 1
```

2. **Configure the dialer10 interface**

```
set interface dialer10 zone Untrust
set interface dialer10 primary-number 16900
set interface dialer10 encap mlppp
set interface dialer10 mtu 1500
set interface dialer10 ppp profile isdn-ppp

set dialer pool name pool-1
set interface dialer10 dialer-pool pool-10

set dialer pool pool-10 member-interface bri1/0 priority 1
```

As shown in Figure 1 on page 5, two stations at Branch Office A can connect to Branch Office B using the dialer interface, dialer1. At the same time, another workstation at Branch Office A can dial out to the headquarters using dialer10.

Using the Leased Line Mode

In this example, you establish ISDN connectivity using a leased line. If the BRI is configured for leased-line mode, it becomes a Layer 3 interface that can only deliver data, so the D-channel is not required. Only one channel (B + B) with a total data rate of 128Kbps is supported. The Q931 dialing is not needed to set up a channel. For more information on the Q931 and Q921 protocols, refer to the *ScreenOS Command Line Reference Guide*.

Use this configuration method to connect two sites with a cost-effective and reliable, high-speed connection as and when required.

WebUI

Network > Interfaces > List > Edit (*bri*): Select **Basic** and select the applicable option value, then click **OK**.

BRI Mode: Leased Line
WAN Encapsulation: PPP
Click **Apply**

Binding a PPP Profile: isdn-ppp

CLI

```
set in bri0/0 isdn leased-line 128kbps
set in bri0/0 encap ppp
set in bri0/0 ppp profile isdn-ppp
```

Step 3: Routing Traffic to the Destination

Configure the following at the Branch Office A security device to route the traffic through the ISDN interface (BRI) and the dialer interface.

Routing Traffic through the ISDN BRI

WebUI

Network > Routing > Destination > New: Select the applicable option value, then click **OK**.

IP Address/Netmask: 10.2.2.2/16
Next Hop: Gateway
Interface: bri1/0

Network > Routing > Destination > New: Select the applicable option value, then click **OK**.

IP Address/Netmask: 11.0.0.0/16
Next Hop: Gateway
Interface: bri1/0

Network > Routing > Destination > New: Select the applicable option value, then click **OK**.

IP Address/Netmask: 10.2.2.2/16
Next Hop: Gateway
Interface: bri2/0

Network > Routing > Destination > New: Select the applicable option value, then click **OK**.

IP Address/Netmask: 11.0.0.0/16
Next Hop: Gateway
Interface: bri2/0

CLI

```
set route 10.2.2.2/16 interface bri1/0
set route 10.2.2.2/16 interface bri2/0
set route 11.0.0.0/16 interface bri1/0
set route 11.0.0.0/16 interface bri2/0
```

Routing Traffic through the Dialer Interface

WebUI

Network > Routing > Destination > New: Select the applicable option value, then click **OK**.

IP Address/Netmask: 10.2.2.2/16
Next Hop: Gateway
Interface: dialer1

Network > Routing > Destination > New: Select the applicable option value, then click **OK**.

IP Address/Netmask: 11.0.0.0/16
Next Hop: Gateway
Interface: dialer1

Network > Routing > Destination > New: Select the applicable option value, then click **OK**.

IP Address/Netmask: 10.2.2.2/16
Next Hop: Gateway
Interface: dialer10

Network > Routing > Destination > New: Select the applicable option value, then click **OK**.

IP Address/Netmask: 11.0.0.0/16
Next Hop: Gateway
Interface: dialer10

CLI

```
set route 10.2.2.2/16 interface dialer1
set route 11.0.0.0/16 interface dialer1

set route 10.2.2.2/16 interface dialer10
set route 11.0.0.0/16 interface dialer10
```

Two stations at Branch Office A can connect to Branch Office B using the dialer interface, dialer1. At the same time, another workstation at Branch Office A can dial out to the headquarters using dialer10.

Encapsulation Configuration Examples

This section provides the following WAN encapsulation examples:

“Encapsulation Configuration Examples” on page 60

“Configuring MLPPP Encapsulation” on page 62

“Configuring Frame Relay Encapsulation” on page 63

“Configuring ML Frame Relay” on page 65

“Configuring Cisco HDLC Encapsulation” on page 66

NOTE: Configure the WAN interface properties before configure the encapsulation information.

Configuring PPP Encapsulation

This example shows the basic PPP Encapsulation configuration.

WebUI

1. Set the PPP Access Profile

   Network > PPP > Edit > New: Enter the following, then click **Apply**:

   PPP Profile: juniper1
   Authentication: CHAP (select)
   Static IP: (select)
   Local Name: local-firewall
   Password: abcd1234#B

2. Set the user information

   Objects > User > Local > New: Enter the following, the click **Apply**:

   User name: router
   WAN User: (select)
   Authentication User: (select)
   User Password: abcd1234#C
   Confirm Password: abcd1234#C

3. Assign the WAN interface the juniper1 access profile

   Network > Interfaces > List > Edit (serial2/0): Select the following, then click **Apply**:

   WAN Encapsulation: PPP (select)
   Binding a PPP Profile: juniper1 (select)
   Zone Name: untrust (select)
   Fixed IP: (select)
   IP Address/Netmask: 192.168.100.1/24
   Manageable: (select)

CLI

1. Set the PPP Access Profile

```
set ppp profile juniper1 auth type chap
set ppp profile juniper1 auth local-name local-firewall
set ppp profile juniper1 auth secret abcd1234#B
set ppp profile juniper1 static-ip
```

2. Set the user information

```
set user router password abcd1234#C
set user router type wan
```

3. Assign the WAN interface the juniper1 access profile

```
set interface serial2/0 untrust zone
set interface serial2/0 encap ppp
set interface serial2/0 ppp profile juniper1
set interface serial2/0 ip 192.168.100.1/24
set interface serial2/0 manage
save
```

Configuring MLPPP Encapsulation

This example shows the basic MLPPP Encapsulation configuration.

WebUI

1. Set the PPP Access Profile

   Network > PPP > Edit > New: Enter the following, then click **Apply**:

   PPP Profile: juniper-mlppp
   Authentication: CHAP (select)
   Static IP: (select)
   Local Name: local-firewall
   Password: abcd1234

2. Set the user information

   Objects > User > Local > New: Enter the following, the click **Apply**:

   User name: router
   WAN User: (select)
   Authentication User: (select)
   User Password: abcd1234
   Confirm Password: abcd1234

3. Set the Multi-link Interface

   Network > Interfaces > List > New Multilink IF: Enter the following, then click **Apply**:

   Interface Name: ML.1
   WAN Encapsulation: Multi-Link PPP (select)
   Zone Name: Untrust (select)

   Edit (ml1 interface): Enter the following, then click **Apply**:

   Binding a PPP Profile: juniper-mlppp (select)
   Fixed IP: (select)
   IP Address/Netmask: 192.168.100.1/24
   Manageable: (deselect)
   Service Options
   Other Services: ping (select)

4. Set the WAN interfaces in the multi-link bundle

   Network > Interfaces > List > Edit (serial1/0): Select Member link options, ml1 Multilink Interface option, then click **Apply**.

   Network > Interfaces > List > Edit (serial2/0): Select Member link options, ml1 Multilink Interface option, then click **Apply**.

CLI

1. Set the PPP Access Profile

```
set ppp profile juniper-mlppp auth type chap
set ppp profile juniper-mlppp auth local-name local-firewall
set ppp profile juniper-mlppp auth secret abcd1234
set ppp profile juniper-mlppp static-ip
```

2. Set the user information

```
set user router password abcd1234
set user router type wan
```

3. Set the Multi-link Interface

```
set interface ml1 zone untrust
set interface ml1 encap mlppp
set interface ml1 ppp profile juniper-mlppp
```

4. Set the WAN interfaces in the multi-link bundle

```
set interface serial1/0 bundle ml1
set interface serial2/0 bundle ml1
set interface ml1 ip 192.168.100.1/24
set interface ml1 manage ping
save
```

Configuring Frame Relay Encapsulation

This example shows the basic Frame Relay Encapsulation configuration.

WebUI

1. Set the Frame Relay Encapsulation

   Network > Interfaces > List > Edit (serial2/0): For WAN Encapsulation, select Frame Relay, then click **Apply**:

   Edit (serial2/0) > FR: Select the Itu type, then click Apply.

2. Set the PVC

   Network > Interfaces > List > New WAN Sub-IF: Enter the following, then click **Apply**:

```
Interface Name: serial2/0 (select) .1
Zone Name: Untrust (select)
Frame Relay DLCI: 200
Fixed IP: (select)
    IP Address/Netmask: 192.168.100.1/24
    Manageable: (deselect)
Service Options
    Other Services: ping (select)
```

NOTE: The DLCI value you specify is the DLCI that your local provider has assigned to your PVC.

CLI

1. Set the Frame Relay Encapsulation

```
set interface serial2/0 encap frame-relay
set interface serial2/0 frame-relay lmi type itu
```

2. Set the PVC

```
set interface serial2/0.1 zone untrust
set interface serial2/0.1 frame-relay dlci 200
set interface serial2/0.1 ip 192.168.100.1/24
set interface serial2/0.1 manage ping
save
```

Configuring ML Frame Relay

This example shows the basic ML Frame Relay Encapsulation configuration.

WebUI

1. Create the Multi-link Interface

   Network > Interfaces > List > New Multilink IF: Enter the following, then click **Apply**:

   ```
   Interface Name: ML 1
   WAN Encapsulation: Multi-Link FR (select)
   Zone Name: Untrust (select)
   ```

   Network > Interfaces > List > Edit (serial2/0): For WAN Encapsulation, select Frame Relay, then click **Apply**:

   Edit (serial2/0) > FR: Select the Itu type, then click **Apply**.

2. Set the WAN interfaces in a bundle

   Network > Interfaces > List > Edit (serial1/0): Select Member link options, ml1 Multilink Interface option, then click **Apply**.

   Network > Interfaces > List > Edit (serial2/0): Select Member link options, ml1 Multilink Interface option, then click **Apply**.

3. Set the Bundle PVC

   Network > Interfaces > List > New WAN Sub-IF: Enter the following, then click **Apply**:

   ```
   Interface Name: ml (select).1
   Zone Name: Untrust (select)
   Frame Relay DLCI: 200
   Frame Relay Inverse ARP: (select)
   Fixed IP: (select)
       IP Address/Netmask: 192.168.100.1/24
       Manageable: (deselect)
   Service Options
       Other Services: ping (select)
   ```

NOTE: The DLCI value you specify is the DLCI that your local provider has assigned to your PVC.

CLI

1. Create the Multi-link Interface

   ```
   set interface ml1 zone untrust
   set interface ml1 encap mlfr-uni-nni
   set interface ml1 frame-relay lmi type itu
   ```

2. Set the WAN interfaces in a bundle

```
set interface serial1/0 bundle ml1
set interface serial2/0 bundle ml1
```

3. Set the Bundle PVC

```
set interface ml1.1 zone untrust
set interface ml1.1 frame-relay dlci 200
set interface ml1.1 frame-relay inverse-arp
set interface ml1.1 ip 192.168.100.1/24
set interface ml1.1 manage ping
save
```

Configuring Cisco HDLC Encapsulation

This example shows the basic Cisco HDLC Encapsulation configuration.

WebUI

Device A

Network > Interfaces > List > Edit (serial2/0): Enter the following, then click **Apply**:

```
WAN Encapsulation: Cisco HDLC (select)
Zone Name: Trust (select)
Fixed IP: (select)
IP Address/Netmask: 192.168.3.1/24
```

Device B

Network > Interfaces > List > Edit (serial2/0): Enter the following, then click **Apply**:

```
WAN Encapsulation: Cisco HDLC (select)
Zone Name: Trust (select)
Fixed IP: (select)
    IP Address/Netmask: 192.168.3.2/24
```

CLI

Device A

1. Bind the WAN interface to a security zone

```
set interface serial2/0 zone trust
```

2. Set the encapsulation type

```
set interface serial2/0 encap cisco-hdlc
```

3. Set the interface IP Address

```
set interface serial2/0 ip 192.168.3.1/24
save
```

Device B

1. Bind the WAN interface to a security zone

   ```
   set interface serial2/0 zone trust
   ```

2. Set the encapsulation type

   ```
   set interface serial2/0 encap cisco-hdlc
   ```

3. Set the interface IP Address

   ```
   set interface serial2/0 ip 192.168.3.2/24
   save
   ```

Chapter 2

Asymmetric Digital Subscriber Line

Some Juniper Networks security devices provide an Asymmetric Digital Subscriber Line (ADSL) connection with integrated Internet Protocol Security virtual private network (IPSec VPN) and firewall services for a broadband telecommuter, a branch office, or a retail outlet. This section describes the ADSL interface on the security device and provides example configurations.

NOTE: For information about configuring IPSec VPN and firewall features on the security device, see *Volume 5: Virtual Private Networks*.

This chapter contains the following sections:

- "ADSL Overview" on this page
- "The ADSL Interface on a Security Device" on page 70
- "Configuration Examples" on page 74

ADSL Overview

Asymmetric Digital Subscriber Line (ADSL) is a Digital Subscriber Line (DSL) technology that allows existing telephone lines to carry both voice telephone service and high-speed digital transmission. A growing number of service providers offer ADSL service to home and business customers.

The transmission is *asymmetric* because the rate at which you can send data (the *upstream* rate) is considerably less than the rate at which you can receive data (the *downstream* rate). This is ideal for Internet access because most messages that you send to the Internet are small and do not require much upstream bandwidth, while most data that you receive from the Internet — such as graphic, video, or audio content — requires greater downstream bandwidth. The data transmission rates available to you depend upon the type of DSL service you obtain from your service provider. Most service providers offer several rate levels, with higher-speed transmissions being more costly than lower-rate transmissions.

Traditional telephone lines use analog signals to carry voice service through twisted-pair copper wires. However, analog transmission uses only a small portion of the available bandwidth. Digital transmission allows the service provider to use a wider bandwidth on the same media. The service provider can separate the analog and digital transmissions, using only a small portion of the available bandwidth to transmit voice. This separation allows a telephone and computer to be used simultaneously on the same line. At the central office of the service provider, the Digital Subscriber Line Access Multiplexer (DSLAM) connects many DSL lines to a high-speed network such as an Asynchronous Transfer Mode (ATM) network.

The ADSL Interface on a Security Device

The ADSL cable provided with some security devices is used to connect the ADSL port on the device to the telephone outlet. No ADSL modem is needed. Signal splitters and microfilters can also be installed once they are obtained from the service provider. Some of the security devices support port mode configuration. Refer to your Juniper Networks security appliance *Hardware Installation and Configuration Guide* for more information about connecting the security device to a network. For information on how to configure a port mode, see Port Modes in Volume 1-33.

The ADSL interface uses ATM as its Transport Layer. There are two types of ATM virtual circuits (VCs): switched virtual circuits (SVCs) are temporary logical network connections that are created and maintained for individual data transfer sessions, while permanent virtual circuits (PVCs) are continuously available logical connections to the network. The ADSL interface supports multiple PVCs on a single physical line.

To set PVC on your physical line, use the following CLI command:

```
set interface interface [ pvc number number ]  { mux [ llc | vc ] protocol [ bridge |
      routed ] [ qos { ubr | cbr | <pcr> <cdvt> | vbr-nrt < mbs> <src> <pcr> <cdvt> }
      ] zone [ Null | Trust | untrust |Self | Global | Untrust-Tun | V1-Null | V1-Trust |
      V1-Untrust | DMZ | V1-DMZ | VLAN ] }
```

The information that you configure for the adsl1 interface must match the DSLAM configuration for your ADSL connection, so you must obtain the following information from your service provider:

- Virtual Path Identifier and Virtual Channel Identifier (VPI/VCI), which identifies the VC on the DSLAM.
- ATM encapsulation method. The ADSL interface supports the following ATM Adaptation Layer 5 (AAL5) encapsulations:
  - Logical Link Control (LLC), which allows several protocols to be carried on the same ATM VC. This is the default encapsulation method.
  - Virtual circuit (VC)-based multiplexing, in which each protocol is carried over a separate ATM VC.

  Check with your service provider for the type of multiplexing used on the ADSL line.

- Point-to-Point Protocol (PPP) is a standard protocol for transmitting IP packets over serial point-to-point links, such as an ATM PVC. The security device supports the following methods of transporting PPP packets:
    - PPP over Ethernet (PPPoE). RFC 2516 describes the encapsulation of PPP packets over Ethernet. For more information about PPPoE, see “System Parameters” on page **2**-229.
    - PPP over AAL5 (PPPoA). RFC 1483 describes the encapsulation of network traffic over AAL5. For more information about PPPoA, see “Point-to-Point Protocol over Adaptation Layer 5” on page 72.

  If the network of the service provider uses PPPoE or PPPoA, the service provider needs to provide the username and password for the connection, the authentication method used, and any other protocol-specific parameters.

- The service provider may give the network a static IP address or a range of IP addresses. The service provider should also provide the address of the DNS server to use for DNS name and address resolution.
- Discrete multitone (DMT) is a method for encoding digital data in an analog signal. By default, the ADSL interface automatically negotiates the DMT operating mode with the DSLAM of the service provider. The mode on the adsl1 interface can be changed to cause the interface to use only one of the following DMT standards:
    - American National Standards Institute (ANSI) TI.413 Issue 2, which supports data rates up to 8 Mbps downstream and 1 Mbps upstream.
    - International Telecommunications Union (ITU) G.992.1 (also known as G.dmt), which supports data rates of 6.144 Mbps downstream and 640 kbps upstream.
    - ITU 992.2 (also known as *G.lite*), which supports data rates up to 1.536 Mbps downstream and 512 kbps upstream. This standard is also called *splitterless DSL*, because you do not have to install a signal splitter on your ADSL line; the service provider’s equipment remotely splits the signal.
    - ITU 992.3 (also known as ADSL2), which supports data rates up to 1.2 Mbps upstream and 12 Mbps downstream.
    - ITU 992.5 (also known as ADSL2+), which supports data rates up to 1.2 Mbps upstream and 24 Mbps downstream.

To set the DMT operating mode, use the following CLI command:

```
set interface interface phy operating-mode [ adsl2 | adsl2plus | ansi-dmt | auto |
    glite | itu-dmt ]
```

NOTE: Contact your ISP for operational mode compatibility. We recommend using auto mode to determine which operational mode is supported with your connection.

Point-to-Point Protocol over Adaptation Layer 5

Point-to-Point Protocol over Adaptation Layer 5 (PPPoA) is usually used for PPP sessions that are to be terminated on a security device with an ADSL interface. PPPoA is primarily used for business class services as it does not require a desktop client.

The following are configuration parameters for a PPPoA client instance:

- Username and password for the PPPoA connection.
- Interface to which the PPPoA instance is bound (the ADSL interface or subinterface) and the netmask for the interface (the default is 255.255.255.255).
- Authentication method: Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or any authentication protocol (any is the default).
- Auto connect: The number of seconds before a previously closed connection is automatically reinitiated. The default (0) disables this function.
- Clear on disconnect: Specifies that IP information is cleared when a connection is closed. This is disabled by default.
- Idle interval: Specifies the number of minutes that the connection is idle before the security device terminates the connection. The default is 30 minutes.
- PPP Link Control Protocol (LCP) parameters for sending LCP-Echo requests.

When the security device initiates a PPPoA connection, the PPPoA server automatically provides the IP addresses for the Untrust zone interface and for the Domain Name System (DNS) servers. When the security device receives DNS server addresses from PPPoA, it updates the DHCP server on the device with these DNS server addresses. If you do not want the DNS server addresses updated on the DHCP server, you can disable the automatic updating of DNS parameters received through the PPPoA connection.

To display the state of the PPPoA instance, use the WebUI (Network > PPPoA) or the CLI (using the **get pppoa all** command). The **get pppoa all** command also shows the state of the physical interface.

The default timeout value for a PPP session on a security device is 1800 seconds (30 minutes). This value is based on the default number of times that an LCP-Echo request is retried (10) multiplied by the interval between each request (180 seconds). You can configure the number of times an LCP-Echo request is retried and the interval between requests.

To set the number of times an LCP-Echo request is retried to 12 and the interval between requests to 190:

WebUI

Network > PPPoA > Edit (for PPPoA instance): Enter the following, then click **OK**:

PPP Lcp Echo Retries: 12
PPP Lcp Echo Timeout: 190

CLI

```
set pppoa name poa1 ppp lcp-echo-retries 12
set pppoa name poa1 ppp lcp-echo-timeout 190
save
```

Multi-Link PPP

Some security devices allow you to configure Multi-Link Point to Point Protocol (MLPPP) over ADSL which is used to bundle two or more ADSL channels into one high-speed ADSL connection. This bundle doubles the downstream and upstream bandwidth. When two ADSL interfaces are bundled to a Multi-Link (ML) interface while the ADSL interfaces are up, Link Control Protocol (LCP) starts. The ML interface does not change its status to up until the LCP negotiation successfully finishes. If the ML interface does not use a static IP address, the ML interface gets a dynamic IP address after the LCP negotiation is finished.

The following restrictions apply for MLPPP to work with ADSL2/2+ mini physical interface modules (PIMs):

- Two ADSL2/2+ PIMs must connect to the same BRAS
- Only two ADSL2/2+ interfaces can be bundled for ADSL MLPPP
- ADSL interface must be in the same security zone as the ML interface

Asynchronous Transfer Mode Quality of Service

The Asynchronous Transfer Mode (ATM) Quality of Service (QoS) shapes ATM traffic that the user transmits, limiting the rate of transmission. ATM QoS has many benefits:

- Ensures that traffic from one VC does not consume the entire bandwidth of an interface, thus adversely impacting other VCs with resulting data loss.
- Controls bandwidth access when policy dictates that the rate of a given VC on average not exceed a certain rate.
- Match the transmission rate of the local interface to the speed of a remote target interface. For example, suppose one end of a link transmits at 256 Kbps and the other end transmits at 128 Kbps. Without an even, end-to-end pipe, an intermediate switch may have to drop some packets at the lower-speed end, disrupting applications using the link.

Juniper Networks supports three ATM QoS services on the ADSL2/2+:

- Constant Bit Rate (CBR)
- Unspecified Bit Rate (UBR)
- Variable Bit Rate Non-Real-Time (VBR-NRT)

Configuration Examples

This section contains the following configuration examples:

- “Example 1: (Small Business/Home) PPPoA on ADSL Interface” on this page. Configure the security device as a firewall with an Internet connection through the ADSL interface with PPPoA (or PPPoE).
- “Example 2: (Small Business/Home) 1483 Bridging on ADSL Interface” on page 77. Configure the security device as a firewall with an Internet connection through the ADSL interface with 1483 Bridging.
- “Example 3: (Small Business) 1483 Routing on ADSL Interface” on page 79. Configure the security device as a firewall with an Internet connection through the ADSL interface, using RFC 1483 Routing.
- “Example 4: (Small Business/Home) Dialup Backup” on page 81. Configure the security device as a firewall with the primary Internet connection through the ADSL interface using PPPoE with dialup as the backup connection.
- “Example 5: (Small Business/Home) Ethernet Backup” on page 84. Configure the security device as a firewall with the primary Internet connection through the ADSL interface using PPPoE with Ethernet as the backup connection.
- “Example 6: (Small Business/Home) ADSL Backup” on page 88. Configure the security device as a firewall with the primary Internet connection through the ADSL interface using PPPoE with another ADSL interface as the backup connection.
- “Example 7: (Small Business) MLPPP ADSL” on page 91. Configure the security device as a firewall with an Internet connection through a MultiLink PPP ADSL connection.
- “Example 8: (Small Business) Allow Access to Local Servers” on page 93. Configure the security device as a firewall with an Internet connection through the ADSL interface. Allow Internet access to local webservers while protecting other internal hosts from being directly accessible from the Internet.
- “Example 9: (Branch Office) VPN Tunnel Through ADSL” on page 96. Configure the security device as a firewall with a VPN tunnel to corporate headquarters through the ADSL interface. Allow Internet access to local webservers while protecting other internal hosts from being directly accessible from the Internet.
- “Example 10: (Branch Office) Secondary VPN Tunnel” on page 100. Configure the security device as a firewall with both an Internet connection and a connection to corporate headquarters through the ADSL interface. Configure a

VPN tunnel through the Internet to corporate headquarters as a secondary connection.

Example 1: (Small Business/Home) PPPoA on ADSL Interface

This example, as shown in Figure 11, explains how to configure a security device as a firewall with an Internet connection through the ADSL interface using PPPoA. Some security devices act as both a PPPoA client and a DHCP server.

To configure PPPoA on an ADSL interface, doing the following:

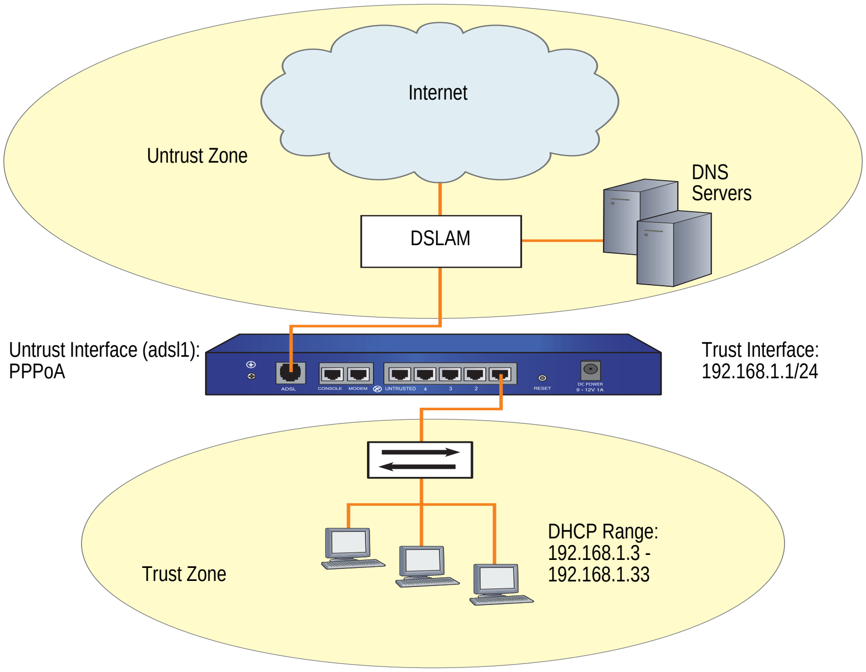
1. Configure the trust interface and set it as the DHCP Server. When the security device assigns IP addresses to the hosts in the Trust zone, it also provides to the hosts the DNS server address obtained from the service provider.

2. Configure a PVC on the ADSL interface with the VPI/VCI pair value 0/35 that uses LLC encapsulation, and a PPPoA instance named “poa1,” which is bound to the ADSL interface. When the security device receives the IP address for the ADSL interface, it also receives one or more IP addresses for DNS servers.

3. Activate PPPoA on the security device. The security device receives a dynamically assigned IP address for its ADSL interface (adsl1) from the service provider through PPPoA, and the security device also dynamically assigns IP addresses for the hosts in its Trust zone.

4. Activate DHCP on the internal network.

Figure 11: ADSL Interface Using PPPoA



WebUI

1. **Trust Interface and DHCP Server**

   Network > Interfaces > Edit (for trust interface): Enter the following, then click **OK**:

   Zone: Trust
   Static IP: (select)
   IP Address/Netmask: 192.168.1.1/24

   Network > DHCP > Edit (for trust interface) > DHCP Server: Select **Apply**.

   > Addresses > New: Enter the following, then click **OK**:

   Dynamic: (select)
   IP Address Start: 192.168.1.3
   IP Address End: 192.168.1.33

2. **ADSL Interface and PPPoA**

   Network > Interfaces > Edit (for adsl1 interface): Enter the following, then click **OK**:

   VPI/VCI: 0/35
   Encapsulation: LLC (select)
   Zone Name: Untrust

   Network > PPPoA > New: Enter the following, then click **OK**:

   PPPoA Instance: poa1
   Bound to Interface: adsl1 (selected)
   Username: alex
   Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
   Automatic Update of DHCP Server's DNS Parameters: (select)

3. **Activating PPPoA on the Security Device**

   Turn off the power to the security device and the workstations in the Trust zone.

   Turn on the security device.

   The security device makes a PPPoA connection to the DSLAM, and obtains the IP address for the ADSL interface and the IP addresses for the DNS servers.

4. **Activating DHCP on the Internal Network**

   Turn on the workstations.

   The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

CLI

1. **Trust Interface and DHCP Server**

```
set interface trust zone trust
set interface trust ip 192.168.1.1/24
set interface trust dhcp server service
set interface trust dhcp server ip 192.168.1.3 192.168.1.33
```

2. **ADSL Interface and PPPoA**

```
set interface adsl1 pvc 0 35 mux llc zone untrust
set pppoa name poa1 username alex password
    tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoa name poa1 interface adsl1
set pppoa update-dhcpserver
save
```

3. **Activating PPPoA on the Security Device**

   Turn off the power to the security device and the workstations in the Trust zone.

   Turn on the security device.

   The security device makes a PPPoA connection to the DSLAM, and obtains the IP address for the ADSL interface and the IP addresses for the DNS servers.

4. **Activating DHCP on the Internal Network**

   Turn on the workstations.

   The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

Example 2: (Small Business/Home) 1483 Bridging on ADSL Interface

RFC 1483 describes methods of transporting bridged protocol data units (PDUs) over AAL5 links. The bridged PDUs do not require the overhead of IPSec processing, thus allowing more usable bandwidth to be available for data traffic. Such traffic is not secured at the IP Packet l Layer and should only be used where you have a private VC (the service provider assigns you a static IP address for your ADSL interface).

This example, as shown in Figure 12, explains how to configure the security device as a firewall with an Internet connection through the ADSL interface using 1483 bridging. A service provider assigns the static IP address 1.1.1.1/32 for your network, as well as an IP address for the DNS server.

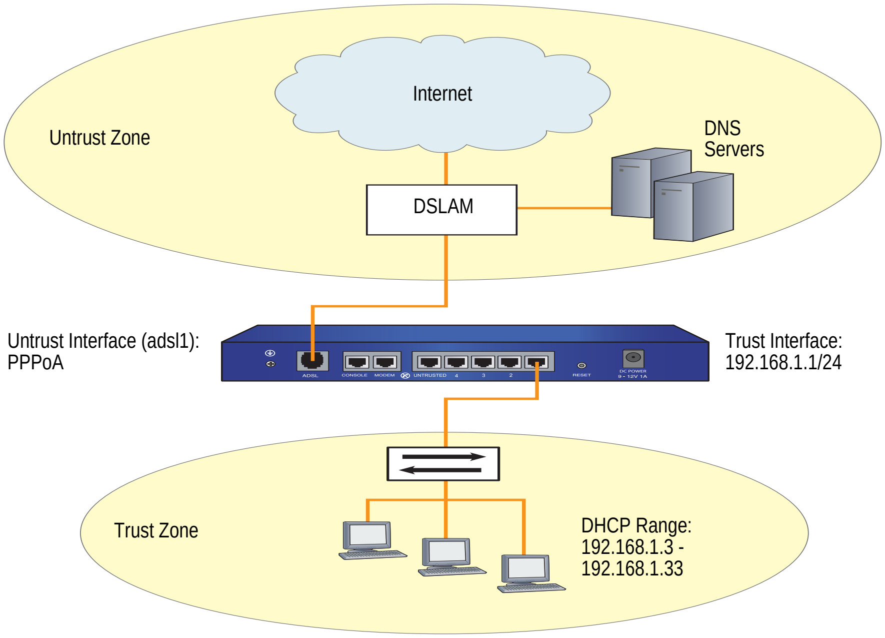
To configure 1483 Bridging on an ADSL interface, do the following:

1. Configure the trust interface and set it as the DHCP server.

2. Configure a PVC on the ADSL interface with the VPI/VCI pair 0/35 and the static IP address 1.1.1.1/32 which is assigned by the service provider.

3. Activate DHCP on the internal network. The security device also dynamically assigns IP addresses for the hosts in its Trust zone. When the security device assigns IP addresses to the hosts in the Trust zone, it also provides the DNS server address from the service provider.

Figure 12: ADSL Interface Using RFC 1483 Bridging


Internet
Untrust Zone
DNS Servers
DSLAM
Untrust Interface (adsl1): PPPoA
Trust Interface: 192.168.1.1/24
Trust Zone
DHCP Range: 192.168.1.3 - 192.168.1.33

WebUI

1. **Trust Interface and DHCP Server**

   Network > Interfaces > Edit (for trust interface): Enter the following, then click **OK**:

   Zone: Trust
   Static IP: (select)
   IP Address/Netmask: 192.168.1.1/24
   Interface Mode: NAT

   Network > DHCP > Edit (for trust interface) > DHCP Server: Enter the following, then click **Apply**.

   Gateway: 1.1.1.1
   Netmask: 255.255.255.0
   DNS#1: 1.1.1.221

   > Addresses > New: Enter the following, then click **OK**:

   Dynamic: (select)
   IP Address Start: 192.168.1.3
   IP Address End: 192.168.1.33

2. **ADSL Interface**

   Network > Interfaces > Edit (for adsl1 interface): Enter the following, then click **Apply**:

   ```
   VPI/VCI: 0/35
   Zone Name: Untrust
   Static IP: (select)
   IP Address/Netmask: 1.1.1.1/32
   ```

3. **Activating DHCP on the Internal Network**

   Turn off the workstations.

   The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

CLI

1. **Trust Interface and DHCP Server**

   ```
   set interface trust zone trust
   set interface trust ip 192.168.1.1/24
   set interface trust dhcp server service
   set interface trust dhcp server ip 192.168.1.3 192.168.1.33
   ```

2. **ADSL Interface**

   ```
   set interface adsl1 pvc 0 35 mux llc zone untrust
   set interface adsl1 ip 1.1.1.1/32
   save
   ```

3. **Activating DHCP on the Internal Network**

   Turn off the workstations.

   The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

Example 3: (Small Business) 1483 Routing on ADSL Interface

RFC 1483 describes methods of transporting routed protocol data units (PDUs) over AAL5 links. Use this configuration to enable the device to exchange routing information with another router through the ADSL interface.

This example, as shown in Figure 13, explains how to configure the security device as a firewall with an Internet connection through the ADSL interface using 1483 routing and LLC encapsulation.

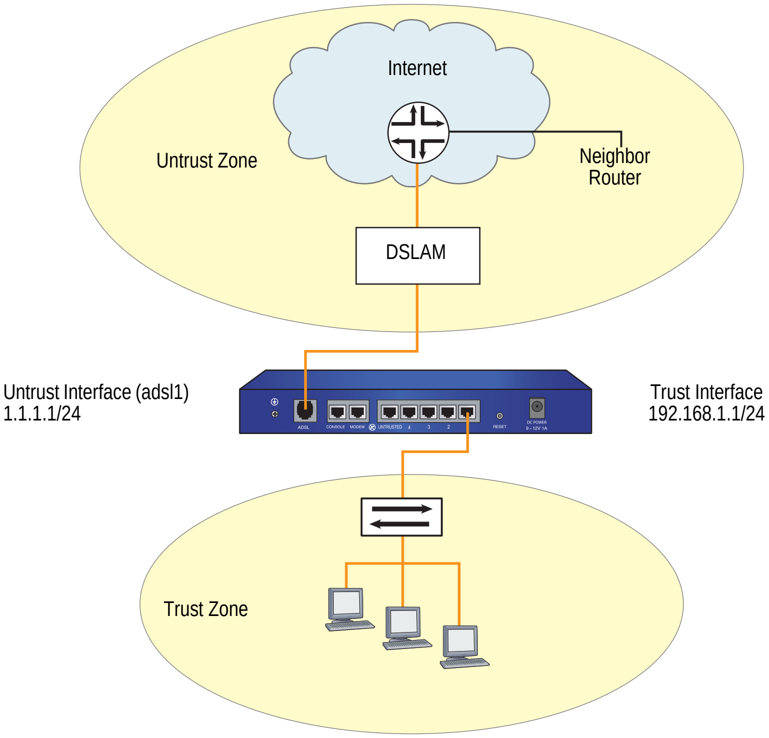
To configure 1483 routing on an ADSL interface, do the following:

1. Configure the ADSL interface. Set a PVC on the ADSL interface with the VPI/VCI pair 0/35 and the static IP address 1.1.1.1/24. You can also configure the ADSL interface to be a DHCP client which receives its IP address from a DHCP server running on the neighbor router.

2. Configure the trust interface. Set the trust interface IP address to 192.168.1.1/24 and the trust interface mode to route.

3. Enable the dynamic routing protocol—which can be either RIP, OSPF, or BGP—in the trust-vr virtual router and on the ADSL and trust interfaces; in the example, the dynamic routing protocol is RIP. The interface on the neighbor router is also configured for LLC encapsulation and 1483 routing.

Figure 13: 1483 Routing on an ADSL Interface



WebUI

1. ADSL Interface

Network > Interfaces > Edit (for adsl1 interface): Enter the following, then click **OK**:

VPI/VCI: 0/35
Multiplexing Method: LLC (select)
RFC1483 Protocol Mode: Routed (select)
Zone: Untrust
Static IP: (select)
IP Address/Netmask: 1.1.1.1/24

2. Trust Interface

Network > Interfaces > Edit (for trust interface): Enter the following, then click **OK**:

Zone: Trust
Static IP: (select)
IP Address/Netmask: 192.168.1.1/24
Interface Mode: Route

3. **Dynamic Routing Protocol**

   Network > Routing > Virtual Router (trust-vr) > Edit: Select Create RIP Instance.

   Select Enable RIP, then click **OK**.

   Network > Interface > Edit (for adsl1 interface) > RIP: Select Protocol RIP Enable, then click **Apply**.

   Network > Interface > Edit (for trust interface) > RIP: Select Protocol RIP Enable, then click **Apply**.

CLI

1. **ADSL Interface**

```
set int adsl1 pvc 0 35 mux llc protocol routed zone untrust
set int adsl1 ip 1.1.1.1/24
```

2. **Trust Interface**

```
set interface trust zone trust
set interface trust ip 192.168.1.1/24
set interface trust route
```

3. **Dynamic Routing Protocol**

```
set vr trust-vr protocol rip
set vr trust-vr protocol rip enable
set interface adsl1 protocol rip
set interface adsl1 protocol rip enable
set interface trust protocol rip
set interface trust protocol rip enable
save
```

Example 4: (Small Business/Home) Dialup Backup

This example, as shown in Figure 14, explains how to configure the security device as a firewall with the primary Internet connection through the ADSL interface using PPPoE, and a backup Internet connection through a dialup connection.

NOTE: Some security devices require that the port mode be set to Home/Work for this example. You can configure a backup link using either the Untrusted Ethernet port or the Modem port on the device. You must bind the backup interface to the Untrust zone and configure the interface appropriately. For port mode information, see “Failover” on page **11**-79.

NOTE: On some devices you can configure only one backup interface.

To configure the primary connection through the ADSL interface and the backup connection through dialup, do the following:

1. Configure the ADSL interface and PPPoE. Configure a PVC on the ADSL interface with the VPI/VCI pair value 0/35 that uses LLC encapsulation, and a PPPoE instance named “poe1,” which is bound to the ADSL interface.

NOTE: Some security devices also acts as DHCP servers to the Home and Work zones with the combined port mode, assigning IP addresses to hosts in both zones.

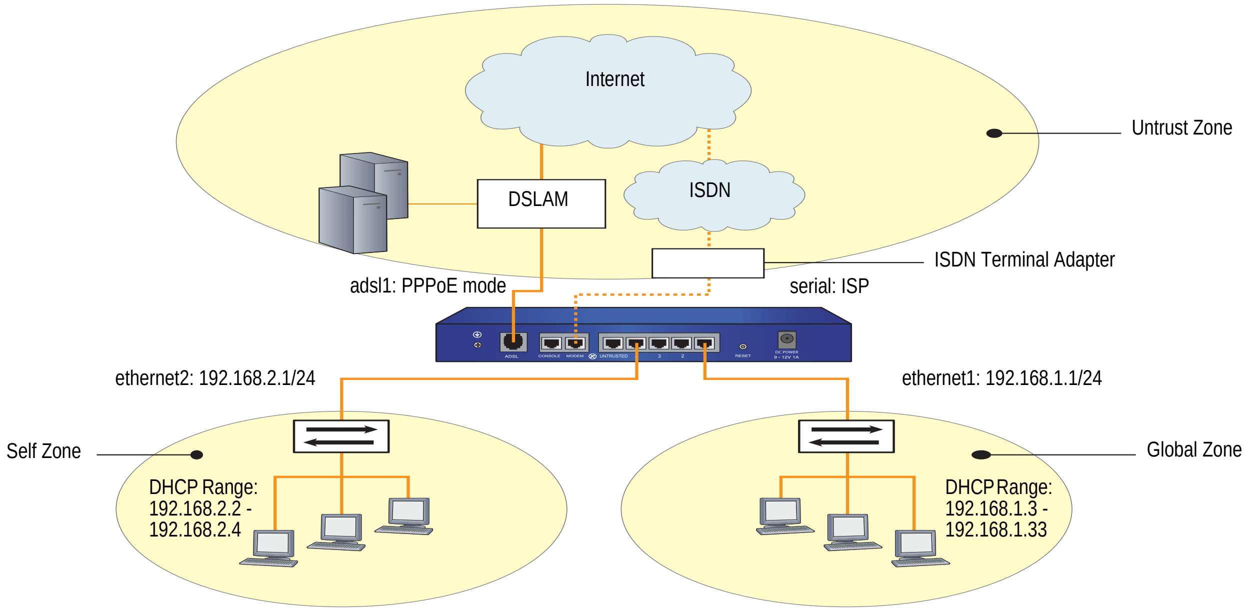
2. Configure a backup connection to the Internet using the serial interface on the Modem port. When the adsl1 and serial interface are both bound to the Untrust zone, interface failover is automatically configured. This means that if the ADSL interface becomes unavailable, the security device automatically sends outgoing traffic to the serial interface, dialing through the Integrated Services Digital Network (ISDN) terminal adapter or modem to your ISP account. When the ADSL interface is again available, the security device automatically sends outgoing traffic to the adsl1 interface. For information about interface failover, see "Failover" on page **11**-79. For information about ISDN configuration, see "ISP Failover and Dial Recovery" on page 107.

3. Configure the Global zone. Set the static IP of the Global zone as 192.168.1.1/24 and set the interface mode to NAT.

4. Configure the Self zone. Set the static IP of the Self zone as 192.168.2.1/24 and set the interface mode to NAT.

5. Activate DHCP on the Self and Global zones.

Figure 14: ADSL with Dialup Backup



To configure the serial interface, you need the following information:

- Login and password for your account to the dialup service provider
- Primary phone connection for dialing into the account
- Modem initialization string

WebUI

1. **ADSL Interface and PPPoE**

   Network > Interfaces > Edit (for adsl1/0 interface): Enter the following, then click **OK**:

   > VPI/VCI: 0/35
   > Encapsulation: LLC (selected)
   > Zone Name: Untrust

   Network > PPPoE > New: Enter the following, then click **OK**:

   > PPPoE Instance: poe1
   > Bound to Interface: adsl1/0 (select)
   > Username: alex
   > Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
   > Automatic Update of DHCP Server's DNS Parameters: (select)

2. **Backup Dialup Interface**

   Network > Interfaces > Backup: Enter the following, then click **OK**:

   > Primary Interface: adsl1/0
   > Backup Interface: serial0/0
   > Type: track ip

   Network > Interfaces > Edit > Monitor (for adsl1/0 interface): Enter the following, then click **OK**:

   > Enable Track IP: (select)
   > Threshold: 1
   > Weight: 255

   Network > Interfaces > Edit > Monitor > Track IP > Click **ADD**: Enter the following, then click **OK**:

   > Dynamic: (select)

3. **Global Interface**

   Network > Interfaces > Edit (for ethernet1 interface): Enter the following, then click **OK**:

   > Zone: Work (already selected)
   > Static IP: (select)
   > IP Address/Netmask: 192.168.1.1/24
   > Interface Mode: NAT

   Network > DHCP > Edit (for ethernet1 interface) > DHCP Server: Select **Apply**.

   > \> Addresses > New: Enter the following, then click **OK**:
   >
   > > Dynamic: (select)
   > > IP Address Start: 192.168.1.3
   > > IP Address End: 192.168.1.33

4. **Self Interface**

   Network > Interfaces > Edit (for ethernet2 interface): Enter the following, then click **OK**:

Zone: Home (already selected)
Static IP: (select)
IP Address/Netmask: 192.168.2.1/24
Interface Mode: NAT

Network > DHCP > Edit (for ethernet2 interface) > DHCP Server: Select **Apply**.

> Addresses > New: Enter the following, then click **OK**:

Dynamic: (select)
IP Address Start: 192.168.2.2
IP Address End: 192.168.2.5

5. **Activating DHCP on the Home and Work Zones**

   Turn off the workstations.

   The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

CLI

1. **ADSL Interface and PPPoE**

```
set interface adsl1 pvc 0 35 mux llc zone untrust
set pppoe name poe1 username alex password
    tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoe name poe1 interface adsl1
```

2. **Backup Dialup Interface**

```
set interface adsl1/0 backup interface serial0/0 type track-ip
set interface adsl1/0 monitor track ip
set interface adsl1/0 monitor track-ip dynamic
```

3. **Global Interface**

```
set interface ethernet1 ip 192.168.1.1/24
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 192.168.1.3 192.168.1.33
```

4. **Self Interface**

```
set interface ethernet2 ip 192.168.2.1/24
set interface ethernet2 dhcp server service
set interface ethernet2 dhcp server ip 192.168.2.2 192.168.2.5
save
```

5. **Activating DHCP on the Home and Work Zones**

   Turn off the workstations.

   The workstations automatically receive the IP address for the DNS server and obtain an IP address for themselves when they attempt a TCP/IP connection.

Example 5: (Small Business/Home) Ethernet Backup

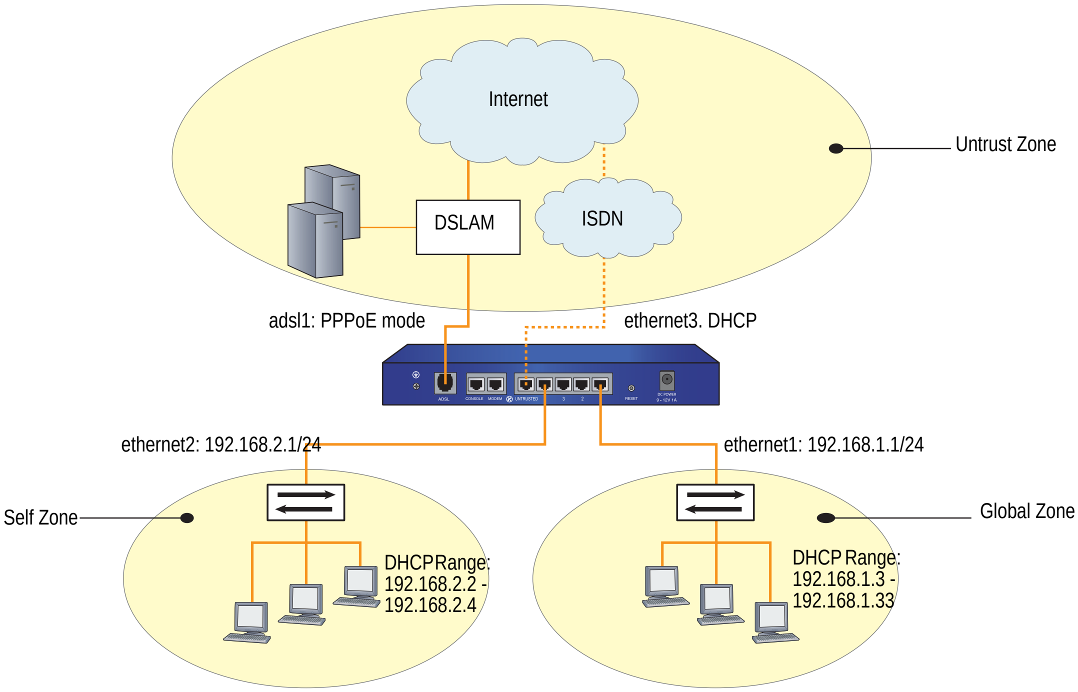
This example, as shown in Figure 15, explains how to configure the security device as a firewall with the primary Internet connection through the ADSL interface using PPPoE, and a backup Internet connection through an Ethernet connection.

NOTE: This example is similar to the configuration shown in "Example 4: (Small Business/Home) Dialup Backup" on page 81, except that the backup connection to the Internet is through the Untrusted Ethernet port.

To configure the primary connection through the ADSL interface and the backup connection through an Ethernet connection, do the following:

1. Configure the ADSL interface with PPPoE. Configure a PVC on the ADSL interface with the VPI/VCI pair value 0/35 that uses LLC encapsulation, and a PPPoE instance named "poe1," which is bound to the ADSL interface.
2. Configure the backup interface as ethernet3.
3. Configure the Global zone.
4. Configure the Self zone.

Figure 15: ADSL with Ethernet Backup


Internet
Untrust Zone
DSLAM
ISDN
adsl1: PPPoE mode
ethernet3. DHCP
ethernet2: 192.168.2.1/24
ethernet1: 192.168.1.1/24
Self Zone
Global Zone
DHCPRange: 192.168.2.2 - 192.168.2.4
DHCP Range: 192.168.1.3 - 192.168.1.33

WebUI

1. **ADSL Interface and PPPoE**

   Network > Interfaces > Edit (for adsl1 interface): Enter the following, then click **OK**:

   VPI/VCI: 0/35
   Encapsulation: LLC (selected)
   Zone: Untrust

   Network > PPPoE > New: Enter the following, then click **OK**:

   PPPoE Instance: poe1
   Bound to Interface: adsl1 (select)
   Username: alex
   Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
   Automatic Update of DHCP Server's DNS Parameters: (select)

2. **Backup Ethernet Interface**

   Network > Interfaces > Edit (for ethernet3 interface): Enter the following, then click **OK**:

   Zone Name: Untrust (select)
   Obtain IP using DHCP: (select)
   Automatic update DHCP server parameters: (select)

3. **Global Zone**

   Network > Interfaces > Edit (for ethernet1 interface): Enter the following, then click **OK**:

   Zone: Global
   Static IP: (select)
   IP Address/Netmask: 192.168.1.1/24
   Interface Mode: NAT

   Network > DHCP > Edit (for ethernet1 interface) > DHCP Server: Select **Apply**.

   > Addresses > New: Enter the following, then click **OK:**
   Dynamic: (select)
   IP Address Start: 192.168.1.3
   IP Address End: 192.168.1.33

4. **Self Zone**

   Network > Interfaces > Edit (for ethernet2 interface): Enter the following, then click **OK**:

   Zone: Self
   Static IP: (select)
   IP Address/Netmask: 192.168.2.1/24
   Interface Mode: NAT

Network > DHCP > Edit (for ethernet 2interface) > DHCP Server: Select **Apply**.

> Addresses > New: Enter the following, then click **OK**:

Dynamic: (select)
IP Address Start: 192.168.2.2
IP Address End: 192.168.2.5

CLI

1. **ADSL Interface and PPPoE**

```
set interface adsl1 pvc 0 35 mux llc zone untrust
set pppoe name poe1 username alex password
    tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoe name poe1 interface adsl1
```

2. **Backup Ethernet Interface**

```
set interface ethernet3 zone untrust
set interface ethernet3 dhcp client
set interface ethernet3 update-dhcpserver
```

3. **Global Zone**

```
set interface ethernet1 ip 192.168.1.1/24
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 192.168.1.3 192.168.1.33
```

4. **Self Zone**

```
set interface ethernet2 ip 192.168.2.1/24
set interface ethernet2 dhcp server service
set interface ethernet2 dhcp server ip 192.168.2.2 192.168.2.5
save
```

Example 6: (Small Business/Home) ADSL Backup

This example, as shown in Figure 16, explains how to configure the security device as a firewall with the primary Internet connection through the ADSL interface using PPPoE, and a backup Internet connection through a second ADSL connection.

NOTE: This example is similar to the configuration shown in “Example 4: (Small Business/Home) Dialup Backup” on page 81, except that the backup connection to the Internet is through the ADSL 2/2+ mini PIM.

To configure the primary connection through the ADSL interface and the backup connection through an Ethernet connection, do the following:

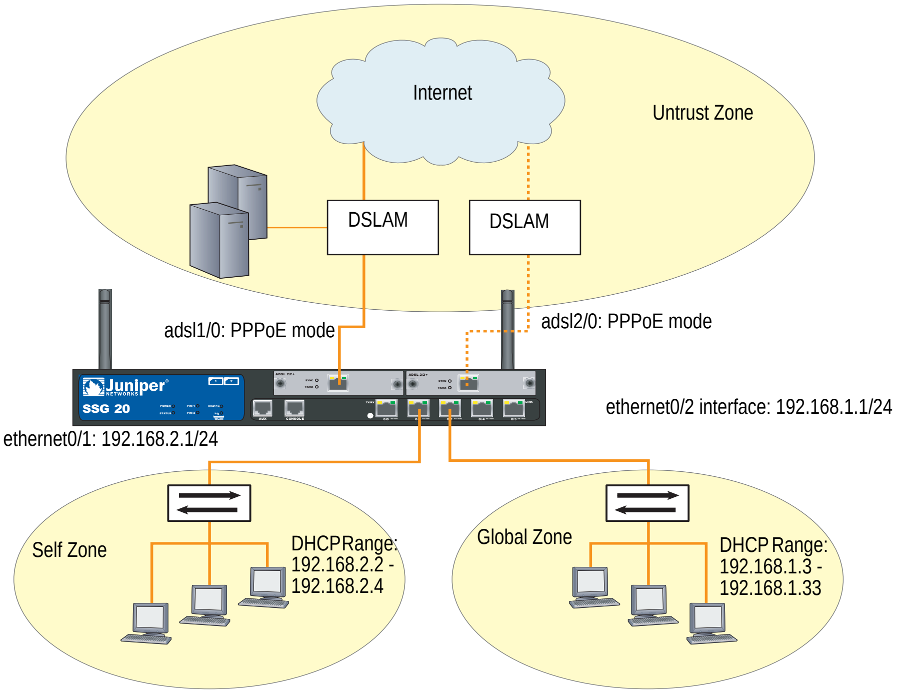
1. Configure the ADSL interfaces with PPPoE. Configure a PVC on the ADSL interface with the VPI/VCI pair value 0/35 that uses LLC encapsulation, and a PPPoE instance named “poe1,” which is bound to the ADSL interface.

2. Configure the backup ADSL interface as adsl2/0.

3. Configure the Global zone.

4. Configure the Self zone.

Figure 16: ADSL with ADSL Backup



WebUI

1. **ADSL Interface and PPPoE**

   Network > Interfaces > Edit (for adsl1/0 interface): Enter the following, then click **OK**:

   VPI/VCI: 0/35
   Encapsulation: LLC (selected)
   Zone: Untrust

   Network > PPPoE > New: Enter the following, then click **OK**:

   PPPoE Instance: poe1
   Bound to Interface: adsl1/0 (select)
   Username: alex
   Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
   Automatic Update of DHCP Server's DNS Parameters: (select)

2. **Backup ADSL Interface**

   Network > Interfaces > Edit (for adsl2/0 interface): Enter the following, then click **OK**:

   VPI/VCI: 8/35
   Encapsulation: LLC (selected)
   Zone: Untrust

   Network > PPPoE > New: Enter the following, then click **OK**:

   PPPoE Instance: poe2
   Bound to Interface: adsl2/0 (select)
   Username: alex
   Password: tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
   Automatic Update of DHCP Server's DNS Parameters: (select)

   Network > Interfaces > Backup: Enter the following, then click **OK**:

   Primary Interface: adsl1/0
   Backup Interface: adsl2/0
   Type: track ip

   Network > Interfaces > Edit > Monitor (for adsl1/0 interface): Enter the following, then click **OK**:

   Enable Track IP: (select)
   Threshold: 1
   Weight: 255

3. **Global Zone**

   Network > Interfaces > Edit (for ethernet0/2 interface): Enter the following, then click **OK**:

   Zone: Global
   Static IP: (select)
   IP Address/Netmask: 192.168.1.1/24
   Interface Mode: NAT

Network > DHCP > Edit (for ethernet0/2 interface) > DHCP Server: Select **Apply**.

> Addresses > New: Enter the following, then click **OK**:
Dynamic: (select)
IP Address Start: 192.168.1.3
IP Address End: 192.168.1.33

4. **Self Zone**

Network > Interfaces > Edit (for ethernet0/1 interface): Enter the following, then click **OK**:

Zone: Self
Static IP: (select)
IP Address/Netmask: 192.168.2.1/24
Interface Mode: NAT

Network > DHCP > Edit (for ethernet0/1 interface) > DHCP Server: Select **Apply**.

> Addresses > New: Enter the following, then click **OK**:

Dynamic: (select)
IP Address Start: 192.168.2.2
IP Address End: 192.168.2.5

CLI

1. **ADSL Interface and PPPoE**

```
set interface adsl1/0 pvc 0 35 mux llc zone untrust
set pppoe name poe1 username alex password
    tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoe name poe1 interface adsl1/0
```

2. **Backup ADSL Interface**

```
set interface adsl2/0 pvc 8 35 mux llc zone untrust
set pppoe name poe1 username alex password
    tSOCbme4NW5iYPshGxCy67Ww48ngtHC0Bw==
set pppoe name poe2 interface adsl2/0
set interface adsl1/0 backup interface adsl2/0 type track-ip
set interface adsl1/0 monitor track ip
set interface adsl1/0 monitor track-ip dynamic
```

3. **Global Zone**

```
set interface ethernet0/2 ip 192.168.1.1/24
set interface ethernet0/2 dhcp server service
set interface ethernet0/2 dhcp server ip 192.168.1.3 192.168.1.33
```

4. **Self Zone**

```
set interface ethernet0/1 ip 192.168.2.1/24
set interface ethernet0/1 dhcp server service
set interface ethernet0/1 dhcp server ip 192.168.2.2 192.168.2.5
save
```

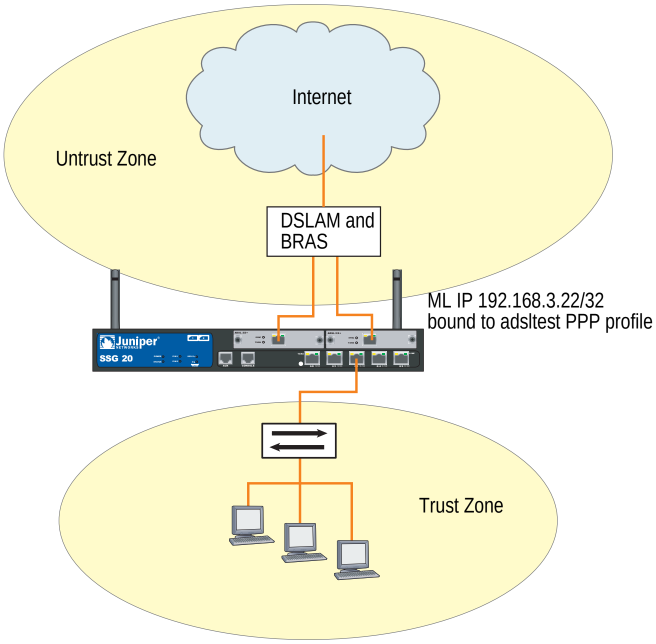
Example 7: (Small Business) MLPPP ADSL

This example, as shown in Figure 14, explains how to configure a PVC on the ADSL interface with the VPI/VCI pair value 8/35 that uses MLPPP encapsulation, and a PPP profile named "adsltest," which is bound to the ML interface.

To configure MLPPP over ADSL, do the following:

1. Configure the multi-link interface.
2. Configure a PPP profile with a dynamic IP address.
3. Bind the PPP profile to the multi-link interface.
4. Bundle the ADSL interface to the multi-link interface.

Figure 17: MLPPP over ADSL



WebUI

1. **Multi-Link Interface**

   Network > Interfaces > New (multi-link interface): Enter the following, then click **OK**:

   Interface Name: 1
   WAN Encapsulation: Multi-Link PPP (select)
   Zone Name: Untrust (select)

2. **PPP Profile with Dynamic IP Address**

   Network > PPP > Edit: Enter the following, then click **OK**:

   PPP Profile: adsltest
   Authentication: CHAP (select) and PAP (select)
   Static IP: (deselect)
   Netmask: 255.255.255.255

Passive: Don't challenge peer (deselect)
Local Name: root
Password: 123456 (does not display)

PPP Profile with Static IP Address (Optional)

Static IP: (select)

3. **Bind PPP Profile to ML Interface**

   Network > Interfaces > Edit (ml1 interface) > Basic properties: Enter the following, then click **OK**:

   WAN Encapsulation: Multi-Link PPP (select)
   Binding a PPP Profile: adsltest (select)
   Fixed IP: (select)
   IP Address/Netmask: 192.168.3.22/24
   Manage IP: 0.0.0.0
   Interface Mode: Route (select)
   Maximum Transfer Unit (MTU): 1500

4. **Bundle ADSL Interface to ML Interface**

   Network > Interfaces > Edit (for adsl1/0 interface): Enter the following, then click **OK**:

   VPI/VCI: 8/35
   QoS Options: UBR (select)
   Multiplexing Method: LLC (select)
   RFC1483 Protocol Mode: Bridged (select)
   Operating Mode: Auto (select)
   Bind to a multilink interface: ml1 (select)
   DNS Proxy: (select)

CLI

1. **Multi-Link Interface**

```
set interface ml1 zone untrust
set interface ml1 encapsulation mlppp
```

2. **PPP Profile with Dynamic IP Address**

```
set ppp profile adsltest
set ppp profile adsltest authentication type any
set ppp profile adsltest authentication local-name root
set ppp profile adsltest authentication secret 123456
```

PPP Profile with Static IP Address (Optional)

```
set ppp profile adsltest static-ip
set interface ml1 ip 192.168.3.22/32
```

3. **Bind PPP Profile to ML Interface**

```
set interface ml1 ppp profile adsltest
```

4. **Bundle ADSL Interface to ML Interface**

```
set interface adsl1/0 pvc 8 35 zone untrust
set interface adsl2/0 pvc 8 35 zone untrust
set interface adsl1/0 bundle ml1
set interface adsl2/0 bundle ml1
```

5. **Remove a Member Link from the Bundle**

```
unset interface adsl1/0 bundle
unset interface adsl2/0 bundle
```

Example 8: (Small Business) Allow Access to Local Servers

This example, as shown in Figure 18, explains how to configure the security device to allow internal hosts to access the Internet through the ADSL interface and allow Internet users to access a local webserver while protecting other internal hosts.

NOTE: Some devices require the configuration of the Trust/Untrust/DMZ (Extended) port mode.

To segregate traffic flow to the webserver from the rest of your internal network, do the following:

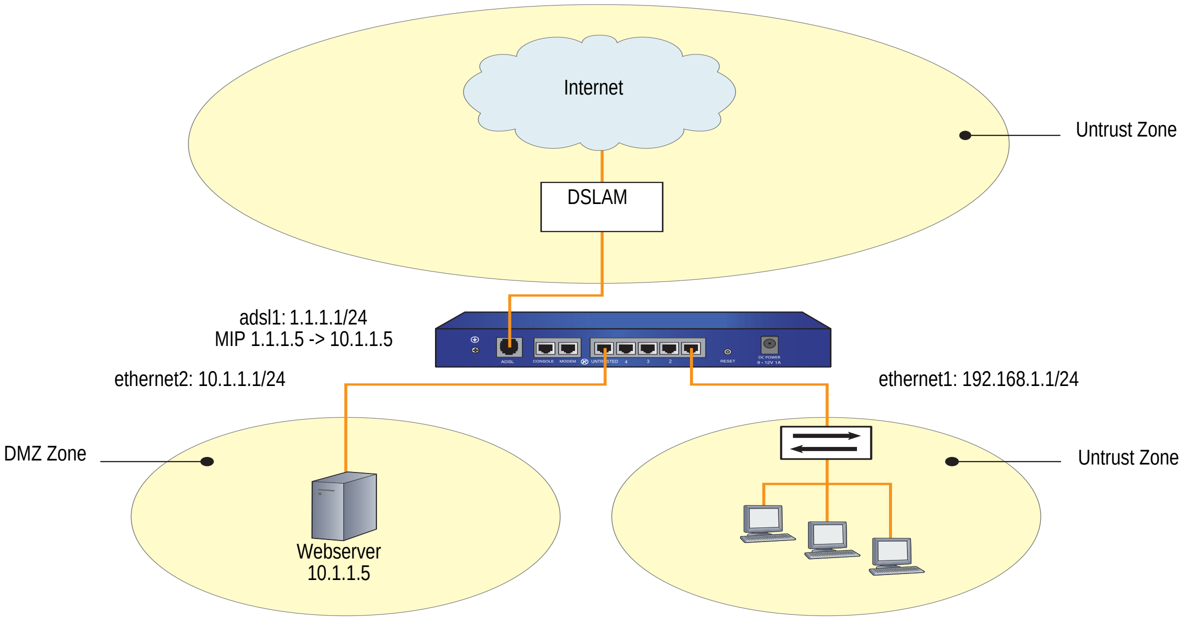
1. Configure the trust and dmz interfaces.

2. Configure the ADSL interface and Mapped IP (MIP). Set a PVC on the ADSL interface with the VPI/VCI pair 0/35 and the static IP address 1.1.1.1/24 which is assigned by the service provider. You bind the Trust interface to the Trust zone and assign it IP address 192.168.1.1/24. You configure a MIP to direct incoming HTTP traffic destined for the host 1.1.1.5 to the webserver at 10.1.1.5 in the DMZ zone.

3. Create a policy to allow only HTTP traffic to the zone in which the webserver resides.

   (Default policies allow all traffic from the Trust zone to the Untrust Zone and block all traffic from the Untrust zone to the Trust zone.)

Figure 18: ADSL Interface Allowing Access to Local Servers



WebUI

1. **Trust and DMZ Interfaces**

   Network > Interfaces > Edit (for ethernet1 interface): Enter the following, then click **OK**:

   Static IP: (select)
   IP Address/Netmask: 192.168.1.1/24
   Interface Mode: NAT

   Network > DHCP > Edit (for ethernet1 interface) > DHCP Server: Select **Apply**.

   > Addresses > New: Enter the following, then click **OK**:

   Dynamic: (select)
   IP Address Start: 192.168.1.3
   IP Address End: 192.168.1.33

   Network > Interfaces > Edit (for ethernet2 interface): Enter the following, then click **OK**:

   Static IP: (select)
   IP Address/Netmask: 10.1.1.1/24
   Interface Mode: NAT

2. **ADSL Interface and MIP**

   Network > Interfaces > Edit (for adsl1 interface): Enter the following, then click **Apply**:

   VPI/VCI: 0/35
   Zone Name: Untrust
   Static IP: (select)
   IP Address/Netmask: 1.1.1.1/24

   > MIP > New: Enter the following, then click **OK**:

   Mapped IP: 1.1.1.5
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.5
   Host Virtual Router Name: trust-vr

3. **Policy**

   Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

   Source Address:
   Address Book Entry: (select) Any
   Destination Address:
   Address Book Entry: (select), MIP(1.1.1.5)
   Service: HTTP
   Action: Permit

CLI

1. **Trust and DMZ Interfaces**

```
set interface ethernet1 ip 192.168.1.1/24
set interface ethernet1 nat
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 192.168.1.3 192.168.1.33
set interface ethernet2 ip 10.1.1.1/24
set interface ethernet2 nat
```

2. **ADSL Interface and MIP**

```
set interface adsl1 pvc 0 35 zone untrust
set interface adsl1 ip 1.1.1.1/24
set interface adsl1 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255 vrouter
    trust-vr
```

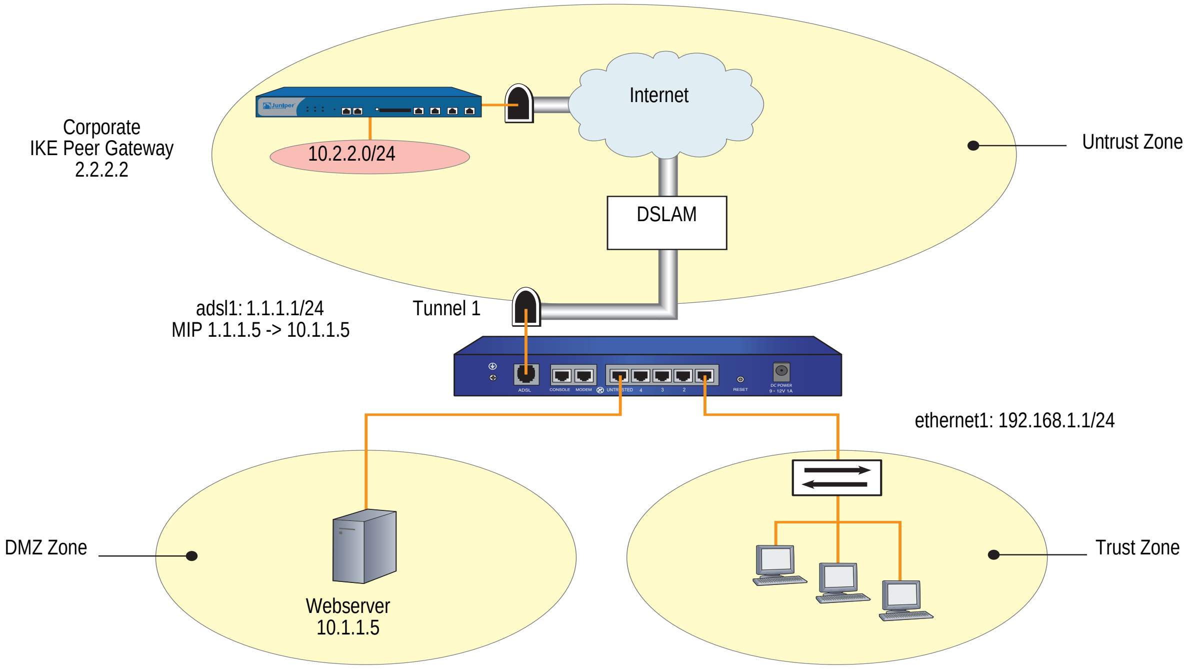
3. **Policy**

```
set policy from untrust to dmz any mip(1.1.1.5) http permit
save
```

Example 9: (Branch Office) VPN Tunnel Through ADSL

This example, as shown in Figure 19, explains how to configure a VPN tunnel to corporate headquarters through the ADSL interface on the security device and how to allow Internet access to local webservers while protecting other internal hosts from being directly accessible from the Internet, as described in “Example 7: (Small Business) MLPPP ADSL” on page 91.

Figure 19: VPN Tunnel Through ADSL Interface



This example also explains how to configure a route-based AutoKey IKE tunnel using a preshared secret. For the Phase 1 and 2 security levels, configure pre-g2-3des-sha for the Phase 1 proposal and the predefined “Compatible” set of proposals for Phase 2. To configure a VPN tunnel through the ADSL interface, do the following:

1. Configure the trust and dmz interfaces.

2. Configure the ADSL interface and Mapped IP (MIP). Set a PVC on the ADSL interface with the VPI/VCI pair 0/35 and the static IP address 1.1.1.1/24 which is assigned by the service provider. You bind the Trust interface to the Trust zone and assign it IP address 192.168.1.1/24. You configure a MIP to direct incoming HTTP traffic destined for the host 1.1.1.5 to the webserver at 10.1.1.5 in the DMZ zone.

3. Create a tunnel interface and bind it to the Untrust security zone. To create a tunnel, do the following:

   a. Configure the tunnel interface to borrow the IP address from the adsl1 interface, which is also bound to the Untrust security zone (this is known as an “unnumbered” interface).

b. Configure the VPN tunnel, designate the adsl1 interface as its outgoing interface in the Untrust zone, bind it to the tunnel interface, and configure its proxy-ID.

c. Enter a route to the Corporate LAN through the tunnel interface.

d. Set up policies for VPN traffic to pass between the branch office and corporate headquarters.

4. Create a policy to allow only HTTP traffic to the zone in which the webserver resides.

   (Default policies allow all traffic from the Trust zone to the Untrust Zone and block all traffic from the Untrust zone to the Trust zone.)

WebUI

1. Trust and DMZ Interfaces

Network > Interfaces > Edit (for ethernet1 interface): Enter the following, then click **OK**:

Static IP: (select)
IP Address/Netmask: 192.168.1.1/24
Interface Mode: NAT

Network > DHCP > Edit (for ethernet1 interface) > DHCP Server: Select **Apply**.

> Addresses > New: Enter the following, then click **OK**:

Dynamic: (select)
IP Address Start: 192.168.1.3
IP Address End: 192.168.1.33

Network > Interfaces > Edit (for ethernet2 interface): Enter the following, then click **OK**:

Static IP: (select)
IP Address/Netmask: 10.1.1.1/24
Interface Mode: NAT

2. ADSL Interface and MIP

Network > Interfaces > Edit (for adsl1 interface): Enter the following, then click **Apply**:

VPI/VCI: 0/35
Zone Name: Untrust
Static IP: (select)
IP Address/Netmask: 1.1.1.1/24

> MIP > New: Enter the following, then click **OK**:

Mapped IP: 1.1.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

3. **VPN Tunnel**

   Network > Interfaces > New Tunnel IF: Enter the following, then click **OK**:

   Tunnel Interface Name: tunnel.1
   Zone (VR): Untrust (trust-vr)
   Unnumbered: (select)
   Interface: adsl1 (trust-vr)

   VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

   Gateway Name: To_Corp
   Security Level: Custom
   Remote Gateway Type:
   Static IP Address: (select), IP Address/Hostname: 2.2.2.2
   Preshared Key: h1p8A24nG5

   > Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

   Security Level: Custom
   Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha
   Mode (Initiator): Main (ID Protection)

   VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

   VPN Name: Branch1_Corp
   Security Level: Compatible
   Remote Gateway:
   Predefined: (select), To_Corp

   > Advanced: Enter the following advanced settings, then click Return to return to the basic AutoKey IKE configuration page:

   Security Level: Compatible
   Bind to: Tunnel Interface, tunnel.1
   Proxy-ID: (select)
   Local IP/Netmask: 192.168.1.1/24
   Remote IP/Netmask: 10.2.2.0/24
   Service: ANY

   Network > Routing > Routing Entries > trust vr > New: Enter the following, then click **OK**:

   Network Address/Netmask: 10.2.2.0/24
   Gateway: (select)
   Interface: Tunnel.1

4. **Policies**

   Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

   ```
   Source Address:
           Address Book Entry: (select) Any
   Destination Address:
           Address Book Entry: (select), MIP(1.1.1.5)
   Service: HTTP
   Action: Permit
   ```

   Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

   ```
   Name: To_Corp
   Source Address: 192.168.1.1/24
   Destination Address: 10.2.2.0/24
   Service: ANY
   Action: Permit
   Position at Top: (select)
   ```

   Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

   ```
   Name: From_Corp
   Source Address: 10.2.2.0/24
   Destination Address: 192.168.1.1/24
   Service: ALL
   Action: Permit
   Position at Top: (select)
   ```

CLI

1. **Trust and DMZ Interfaces**

   ```
   set interface ethernet1 ip 192.168.1.1/24
   set interface ethernet1 nat
   set interface ethernet1 dhcp server service
   set interface ethernet1 dhcp server ip 192.168.1.3 192.168.1.33
   set interface ethernet2 ip 10.1.1.1/24
   set interface ethernet2 nat
   ```

2. **ADSL Interface and MIP**

   ```
   set interface adsl1 pvc 0 35 zone untrust
   set interface adsl1 ip 1.1.1.1/24
   set interface adsl1 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255 vrouter
       trust-vr
   ```

3. **VPN Tunnel**

   ```
   set interface tunnel.1 zone untrust
   set interface tunnel.1 ip unnumbered interface adsl1
   set ike gateway To_Corp address 2.2.2.2 main outgoing-interface adsl1 preshare
       hlp8A24nG5 proposal pre-g2-3des-sha
   set vpn Branch1_Corp gateway To_Corp sec-level compatible
   set vpn Branch1_Corp bind interface tunnel.1
   set vpn Branch1_Corp proxy-id local-ip 192.168.1.1/24 remote-ip 10.2.2.0/24
       any
   set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
   ```

4. **Policies**

```
set policy from untrust to dmz any mip(1.1.1.5) http permit
set policy top name "To Corp" from trust to untrust 192.168.1.1/24 10.2.2.0/24
     any permit
set policy top name "From Corp" from untrust to trust 10.2.2.0/24
     192.168.1.1/24 any permit
save
```

Example 10: (Branch Office) Secondary VPN Tunnel

This example, as shown in Figure 20, explains how to configure the security device as a firewall with both an Internet connection and a connection to corporate headquarters through the ADSL interface. This example is similar to the configuration shown in "Example 9: (Branch Office) VPN Tunnel Through ADSL" on page 96, but you create two PVCs: one to the Internet and another to corporate headquarters. You also configure a VPN tunnel through the Internet to corporate headquarters as a secondary connection.

To configure and primary and secondary VPN tunnel through ADSL, do the following:

1. Configure the trust and dmz interfaces.

2. Configure the ADSL interface and Mapped IP (MIP). Set a PVC on the ADSL interface with the VPI/VCI pair 0/35 and the static IP address 1.1.1.1/24 which is assigned by the service provider. You bind the Trust interface to the Trust zone and assign it IP address 192.168.1.1/24. You configure a MIP to direct incoming HTTP traffic destined for the host 1.1.1.5 to the webserver at 10.1.1.5 in the DMZ zone.

3. Configure the Headquarter (HQ) custom zone.

4. Configure an ADSL subinterface. Set an additional PVC on the security device by creating the ADSL subinterface adsl1.1. The adsl1.1 subinterface with the VPI/VCI pair value 1/35 that uses LLC encapsulation and a PPPoE instance named poe1, which is bound to the subinterface. You then need to define policies to allow the flow of traffic to and from the HQ zone.

NOTE: You can bind the ADSL interface and each of its subinterfaces to different security zones; you bind the ADSL subinterface to the custom zone "HQ" (the main ADSL interface is bound to the Untrust zone by default).

5. Create a tunnel interface and bind it to the Untrust security zone. To create a tunnel, do the following:

   a. Configure the tunnel interface to borrow the IP address from the adsl1 interface, which is also bound to the Untrust security zone (this is known as an "unnumbered" interface).

   b. Configure the IKE gateway.

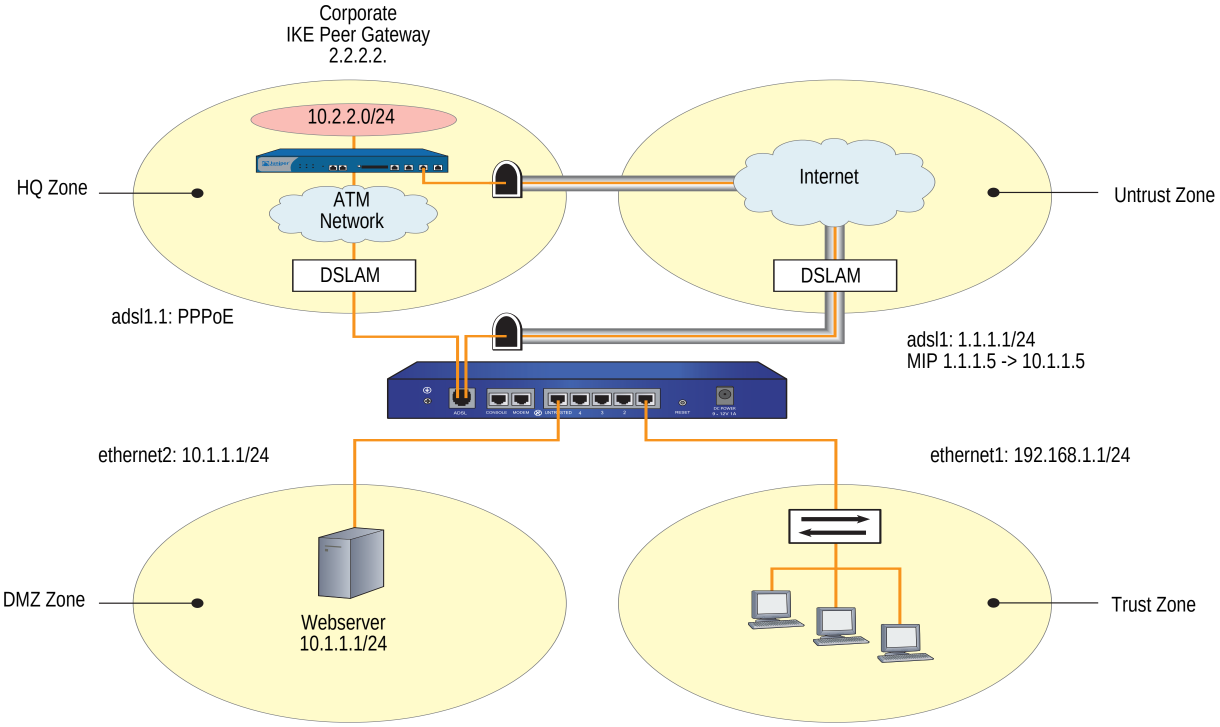
   c. Configure the VPN tunnel, designate the adsl1 interface as its outgoing interface in the Untrust zone, bind it to the tunnel interface, and configure its proxy-ID.

6. Create virtual route (trust-vr).

7. Set up policies for VPN traffic to pass between the branch office and corporate headquarters.

   (Default policies allow all traffic from the Trust zone to the Untrust Zone and block all traffic from the Untrust zone to the Trust zone.)

Figure 20: ADSL Interface with a Secondary Tunnel



Because you have two different routes between workstations in the Trust zone and corporate headquarters—one using the adsl1.1 interface and another using the VPN tunnel interface—you need to specify which route is “preferred.” This is done by setting the metric for the route through the VPN tunnel higher than the route through the adsl1.1 interface.

WebUI

1. Trust and DMZ Interfaces

Network > Interfaces > Edit (for ethernet1 interface): Enter the following, then click **OK**:

Static IP: (select)
IP Address/Netmask: 192.168.1.1/24
Interface Mode: NAT

Network > DHCP > Edit (for ethernet1 interface) > DHCP Server: Select **Apply**.

> Addresses > New: Enter the following, then click **OK**:

Dynamic: (select)
IP Address Start: 192.168.1.3
IP Address End: 192.168.1.33

Network > Interfaces > Edit (for ethernet2 interface): Enter the following, then click **OK**:

Static IP: (select)
IP Address/Netmask: 10.1.1.1/24
Interface Mode: NAT

2. **ADSL Interface and MIP**

Network > Interfaces > Edit (for adsl1 interface): Enter the following, then click **Apply**:

VPI/VCI: 0/35
Zone Name: Untrust
Static IP: (select)
IP Address/Netmask: 1.1.1.1/24

> MIP > New: Enter the following, then click **OK**:

Mapped IP: 1.1.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

3. **HQ Zone**

Network > Zones > New: Enter the following, then click **OK**:

Zone Name: HQ
Block Intra-Zone Traffic: (select)

4. **ADSL Subinterface**

Network > Interfaces > New ADSL Sub-IF: Enter the following, then click **OK**:

Interface Name: adsl1.1
VPI/VCI: 1/35
Encapsulation: LLC (selected)
Zone: HQ (select)

Network > PPPoE > New: Enter the following, then click **OK**:

PPPoE Instance: poe1
Bound to Interface: adsl1.1 (select)
Username: felix
Password: ioP936QNlwab48Rc

5. **VPN Tunnel**

Network > Interfaces > New Tunnel IF: Enter the following, then click **OK**:

Tunnel Interface Name: tunnel.1
Zone (VR): Untrust (trust-vr)
Unnumbered: (select)
Interface: adsl1 (trust-vr)

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: To_Corp
Security Level: Custom
Remote Gateway Type:
Static IP Address: (select), IP Address/Hostname: 2.2.2.2
Preshared Key: h1p8A24nG5

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom
Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID Protection)

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: Branch1_Corp
Security Level: Compatible
Remote Gateway:
Predefined: (select), To_Corp

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic AutoKey IKE configuration page:

Security Level: Compatible
Bind to: Tunnel Interface, tunnel.1
Proxy-ID: (select)
Local IP/Netmask: 192.168.1.1/24
Remote IP/Netmask: 10.2.2.0/24
Service: ANY

6. **Routes**

Network > Routing > Routing Entries > trust vr > New: Enter the following, then click **OK**:

Network Address/Netmask: 10.2.2.0/24
Gateway: (select)
Interface: adsl1.1
Metric: 1

Network > Routing > Routing Entries > trust vr > New: Enter the following, then click **OK**:

Network Address/Netmask: 10.2.2.0/24
Gateway: (select)
Interface: Tunnel.1
Metric: 5

7. **Policies**

Policies (From: Trust, To: HQ) > New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select) Any
Destination Address:
Address Book Entry: (select) Any
Service: ANY
Action: Permit

Policies (From: HQ, To: Trust) > New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select) Any
Destination Address:
Address Book Entry: (select) Any
Service: ANY
Action: Permit

Policies (From: DMZ, To: HQ) > New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select) Any
Destination Address:
Address Book Entry: (select) Any
Service: ANY
Action: Permit

Policies (From: HQ, To: DMZ) > New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select) Any
Destination Address:
Address Book Entry: (select) Any
Service: ANY
Action: Permit

Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select) Any
Destination Address:
Address Book Entry: (select), MIP(1.1.1.5)
Service: HTTP
Action: Permit

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Name: To_Corp
Source Address: 192.168.1.1/24
Destination Address: 10.2.2.0/24
Service: ANY
Action: Permit
Position at Top: (select)

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Name: From_Corp
Source Address: 10.2.2.0/24
Destination Address: 192.168.1.1/24
Service: ALL
Action: Permit
Position at Top: (select)

CLI

1. **Trust and DMZ Interfaces**

```
set interface ethernet1 ip 192.168.1.1/24
set interface ethernet1 nat
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 192.168.1.3 192.168.1.33
set interface ethernet2 ip 10.1.1.1/24
set interface ethernet2 nat
```

2. **ADSL Interface and MIP**

```
set interface adsl1 pvc 0 35 zone untrust
set interface adsl1 ip 1.1.1.1/24
set interface adsl1 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255 vrouter
    trust-vr
```

3. **HQ Zone**

```
set zone name HQ
set zone HQ block
set zone HQ vrouter trust-vr
```

4. **ADSL Subinterface**

```
set interface adsl1.1 pvc 1 35 mux llc zone HQ
set pppoe name poe1 username felix password ioP936QNlwab48Rc
set pppoe name poe1 interface adsl1.1
```

5. **VPN Tunnel**

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface adsl1
set ike gateway To_Corp address 2.2.2.2 main outgoing-interface adsl1 preshare
    hlp8A24nG5 proposal pre-g2-3des-sha
set vpn Branch1_Corp gateway To_Corp sec-level compatible
set vpn Branch1_Corp bind interface tunnel.1
set vpn Branch1_Corp proxy-id local-ip 192.168.1.1/24 remote-ip 10.2.2.0/24
    any
```

6. **Routes**

```
set vrouter trust-vr route 10.2.2.0/24 interface adsl1.1 metric 1
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1 metric 5
```

7. **Policies**

```
set policy from trust to HQ any any any permit
set policy from HQ to trust any any any permit
set policy from dmz to HQ any any any permit
set policy from HQ to dmz any any any permit
set policy from untrust to dmz any mip(1.1.1.5) http permit
set policy top name “To Corp” from trust to untrust 192.168.1.1/24 10.2.2.0/24
    any permit
set policy top name “From Corp” from untrust to trust 10.2.2.0/24
    192.168.1.1/24 any permit
save
```

Chapter 3

ISP Failover and Dial Recovery

The NS-5GT and NS-5XT platforms each have an inband modem port. This port is not used for incoming calls; instead, it is used to connect to an external modem or an ISDN terminal adapter (TA) for dialup disaster-recovery purposes.

This chapter contains the following sections:

- "Setting ISP Priority for Failover" on this page
- "Defining Conditions for ISP Failover" on page 108
- "Configuring a Dialup Recovery Solution" on page 109

For information about configuring trustee administrator accounts, see "Example: Configuring Admin Accounts for Dialup Connections" on page 3-34.

Setting ISP Priority for Failover

You, as a root administrator (not a trustee admin), can configure a total of four ISPs. The priority of each ISP must be a unique number. You can also configure one or more ISP entries with a priority of zero for testing (monitoring) purposes; however, any ISP entry assigned a zero will not be used for failover.

When using a modem connection, a trustee administrator can manually change an ISP priority. If a failover situation occurs, the priority assigned to an ISP indicates in what order relative to other ISPs that a particular ISP will be contacted. The lower the value, the higher the priority of the ISP. Trustee admins can also check the availability of an ISP with a priority setting of zero (0).

WebUI

Home > Interface link status: Click **more**. Then click **edit** for the serial interface.

CLI

```
set modem isp “pac-bell-1” priority 1
set modem isp “pac-bell-1” primary-number “555-55-55” alternative-number
    “666-66-66”
set modem isp “pacbell-1” account login “rbrockie” password “!2005fb”
set modem isp “pac-bell-2” priority 2
set modem isp “pac-bell-2” primary-number “777-77-77” alternative-number
    “888-88-88”
set modem isp “pacbell-2” account login “rbrockie” password “!2005fb”
save
```

Defining Conditions for ISP Failover

After setting up the ISP information and priorities, you can selectively monitor a route in the untrust-vr that can trigger a failover to the next highest priority ISP (next lowest priority number) when the monitored route disappears from the untrust-vr routing table. When the failover to ISP 2 occurs, it does not necessarily mean that ISP 1 went down or failed. It means that a particular route that you want to access that is beyond ISP 1 became unavailable and you want the device to wait a specified number of seconds before giving up and calling the backup ISP.

To use this feature you specify a particular route with an IP address that currently appears in the untrust-vr. Optionally, you can specify the number of seconds for the device to wait before it calls the backup ISP. The default holddown time is 30 seconds.

In the previous example you, as root administrator, set up a priority 1 ISP and a backup ISP. In this example, you set the security device to monitor the route 1.1.1.1/24, which you have identified as an interesting or important route. This route currently exists in the untrust-vr. You set the holddown timer to be 100 seconds. You must use the CLI to set which route in the Untrust-vr you want to monitor. If the specified route becomes unavailable, failover to the next ISP (priority 2) occurs.

WebUI

This feature is not available in the WebUI.

CLI

```
set modem isp-failover type route vrouter untrust 1.1.1.1/24
set modem isp-failover holddown 100
save
```

Configuring a Dialup Recovery Solution

You can set up a dialup disaster-recovery solution for your network by configuring the following items:

- NS-5GT or NS-5XT security device
- Modem or ISDN terminal adapter (TA)
- An interface-failover trigger mechanism
- A method for the far-end device (another router or firewall device) to identify a return path to the sending device

NOTE: You need to configure a method of advertising the route back to the NS-5GT device; otherwise, the failover will occur, but the NS-5GT device will be unable to receive responses from the server. If the VPN tunnel terminates at the firewall, you can use static routes configured with different metrics or a dynamic routing protocol, such as BGP or RIP, to facilitate route learning.

For more information about dynamic routing protocols, see *Volume 7: Routing*.

You can choose one of three different failover mechanisms to trigger an interface failover:

- **Track IP** monitors the availability of a specified IPv4 address to determine failover. To use IP tracking, enter the **set failover type track-ip** command.
- **Tunnel tracking** monitors VPN tunnel status to determine failover. To track by tunnel interface, enter the **set failover type tunnel-if** command.
- **Route tracking** monitors a known route’s status. The route entry can be propagated by a dynamic routing protocol, such as BGP or OSPF. If a BGP adjacency is lost, the security device removes all routes learned from that BGP peer. If the route entry is not active for a period that exceeds the hold-down time, the security device triggers an interface failover to a backup interface. This feature requires an exact address match to an active route in the routing table of the specified vrouter to avoid failover. To achieve failover by route, enter the **set failover type route** command.

In the following example (see Figure 21), a computer located in downtown San Jose, California is networked to a server in a remote office in another part of San Jose. The NS-5GT device always uses tunnel.1, a VPN tunnel bound to ethernet3 (e3), to send traffic from the computer (PC) across the Internet to the firewall to access a remote server. The traffic uses static routes and VPN monitoring (default settings). Tunnel.1 has a metric of 1 that ensures it will always be the preferred route to the firewall; tunnel.2 has a higher metric, 180, so that does not become a preferred route.

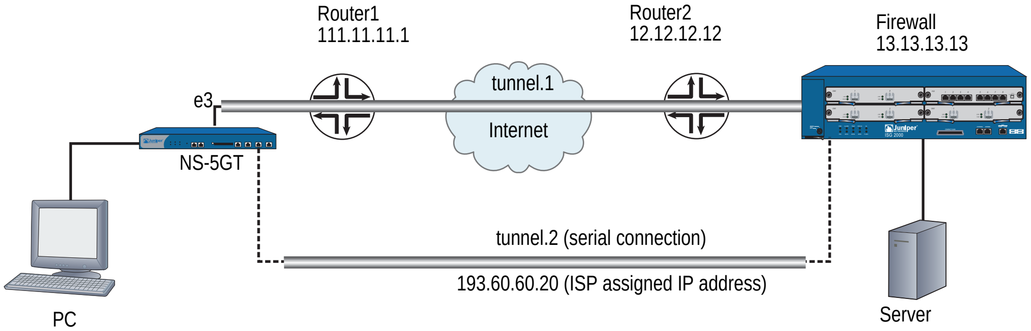
If tunnel.1 goes down, the NS-5GT device brings up tunnel.2, bound to the serial interface, to contact the firewall. In this example, tunnel tracking is preferred over IP tracking to achieve the interface failover. With IP tracking, if the link goes down, failover occurs; but it will be unknown if failover occurred because the VPN tunnel is actually down or not. The tunnel-tracking feature fails over only when the tunnel interface bound to the primary Untrust interface goes down. The primary Untrust interface can fail if a cable is unplugged or if the VPN monitor is triggered, which also means that the tunnel failed.

The NS-5GT device tunnel.2 (serial) interface uses an ISP-assigned IP address to connect over ISDN to the firewall.

The failover is set to "auto" so that when e3 becomes usable again, failback to tunnel.1 occurs.

VPN monitoring becomes active when you enter the **set vpn <name> monitor rekey** command. If necessary, you can choose to change the default interval and threshold settings by entering the **set vpnmonitor { interval | threshold }** command. You can view VPN monitoring settings by entering the **get vpnmonitor** command.

Figure 21: Dial Recovery Configuration



Following is the configuration for the NetScreen-5GT as shown in Figure 21.

WebUI

Configure the serial and tunnel interfaces

Network > Interfaces: Select **Edit** for the serial interface, and bind the interface to the **Untrust** zone. Click **Apply**.

Network > Interfaces: Select **New** for a tunnel interface (tunnel.1) and bind the interface to the **Untrust** zone. Configure settings as applicable, then click **Apply**.

Network > Interfaces: Select **New** for a tunnel interface (tunnel.2) and bind the interface to the **Untrust** zone. Configure settings as applicable, then click **Apply**.

Set static routes and metrics

Network > Routing > Routing Entries: Select **New** route for the untrust-vr, set the IP address, gateway information, metric, then click **OK**.

Network > Routing > Routing Entries: Select **New** route for the untrust-vr, set the IP address from that the ISP assigned for the serial connection, gateway information (if applicable), metric (higher number than previous entry), then click **OK**.

Set the IKE gateway

VPNs > Autokey IKE > Edit: Enter IKE requirements, then click **OK**.

Bind the VPNs to the IKE gateways

VPNs > Autokey IKE > Edit: Select Advanced and bind the VPN to the IKE gateway for tunnel.1. Click **OK**.

VPNs > Autokey IKE > Edit: Select Advanced and bind the VPN to the IKE gateway for tunnel.2. Click **OK**.

Configure interface failover

Configure from CLI.

Configure the inband modem port settings

Network > Interface (Modem)

Setting the primary ISP account

Network > Interface (ISP)

CLI (NS-5GT)

Configure the serial and tunnel interfaces

```
set interface serial zone untrust

set interface tunnel.1 zone untrust
set interface tunnel.1 ip 13.13.13.13

set interface tunnel.2 zone untrust
set interface tunnel.2 ip 13.13.13.13
```

Set static routes and metrics

```
set route 13.13.13.13/24 gateway 11.11.11.11 metric 1
set route 13.13.13.13/24 gateway 193.60.60.20 metric 180
```

Set the IKE gateway

```
set ike gateway "eth" address 13.13.13.13 Main outgoing-interface "ethernet3"
    preshare "jZ1xRY6iNJ8grrsmquC/bs0kYGnATekk8w==" sec-level standard

set ike gateway "serial" address 13.13.13.13 Main outgoing-interface "serial"
    preshare "jZ1xRY6iNJ8grrsmquC/bs0kYGnATekk8w==" sec-level standard
```

Bind the VPNs to the IKE gateways

```
set vpn "eth" gateway "eth" no-replay tunnel idletime 0 sec-level standard
set vpn "eth" monitor rekey
set vpn "eth" id 1 bind interface tunnel.1

set vpn "serial" gateway "serial" no-replay tunnel idletime 0 sec-level standard
set vpn "serial" monitor rekey
set vpn "serial" id 1 bind interface tunnel.2
```

Configure interface failover

```
set failover auto
set failover holddown 5
set failover type tunnel-if
```

Configure the inband modem port settings

```
set modem settings "port1" active
set modem settings "port1" init-strings
    AT&F1E1Q0V1S7=60S19=0M1&M4&K1&H1&R1&I0B0X4
```

Setting the primary ISP account

```
set modem isp “pac-bell-1” priority 1
set modem isp “pac-bell-1” primary-number “555-55-55” alternative-number
    “666-66-66”
set modem isp “pacbell-1” account login “rbrockie” password “!2005fb”
```

Chapter 4

Wireless Local Area Network

Juniper Networks wireless devices and systems provide wireless local area network (WLAN) connections with integrated Internet Protocol Security Virtual Private Network (IPSec VPN) and firewall services for wireless clients, such as telecommuters, branch offices, or retail outlets.

This chapter explains how to configure wireless interfaces and provides example configurations.

This chapter contains the following sections:

Overview

Wireless security devices and systems connect wireless users or other wireless devices to wired or wireless networks. A device that enables a wireless device to access a local area network is a wireless access point (AP). The features listed in this chapter require security devices or systems with built-in wireless interfaces.

NOTE: All wireless platforms can support up to four active wireless interfaces at one time (additional licenses might be required for some platforms).

ScreenOS runs on wireless security devices to provide routing and firewall services to interface with your existing or planned wired networks.

As with wired interfaces, you can configure the following for a wireless interface:

- IP address/netmask and manage IP address
- Management options, such as WebUI, SNMP, Telnet, SSH, or SSL
- Address translation
- Domain Name Services (DNS) Proxy
- WebAuth
- Dynamic Host Configuration Protocol (DHCP) server functionality (DHCP client or relay functionality is not supported)

NOTE: See *Volume 2: Fundamentals* and *Volume 8: Address Translation*.

The following wireless ScreenOS features enable you to manage and secure a WLAN:

- Up to four WLANs per system, depending on the number of wireless interfaces supported on the wireless security device (some devices require additional licenses for more wireless interfaces)
- Depending on the security device, up to 8 or 16 service set identifier (SSIDs)

- Authentication
  - Open
  - Wired Equivalent Privacy (WEP) (shared-key)
  - WEP (802.1X)
  - Wi-Fi Protected Access (WPA) (pre-shared key)
  - WPA (802.1X)
  - WPA2 (pre-shared key)
  - WPA2 (802.1X)
- Encryption
  - Advanced Encryption Standard (AES)
  - Temporal Key Integrity Protocol (TKIP)
  - WEP
- Wi-Fi™ Multimedia (WMM) Quality of Service feature
- Turbo mode with nearly double the performance per radio band

NOTE: Refer to the datasheet that accompanied the product for capacity statements.

Security Zones and Port Modes

Port and security zone assignments vary by hardware platform. Refer to your hardware manual for information about port modes and security zones.

Wireless Product Interface Naming Differences

Wireless products support up to four WLANs. Entering commands in the WebUI and CLI differ by product.

Some wireless products have two radio transceivers:

- 2.4 GHz
- 5 GHz

When configuring the wireless device, you differentiate between the two transceivers by indicating zero (0) for the 2.4 GHz transceiver or 1 for the 5 GHz transceiver.

Transceiver-specific parameters automatically appear in the WebUI or CLI.

To configure a wireless product with one radio, you do not specify a zero (0) to indicate the 2.4 GHz transceiver.

In the WebUI, the two radios are shown if a security device has them, and you configure parameters for the radio you want. If the security device has only one radio, no radio differentiation is shown, and changes apply to the one radio.

For example, in the CLI, to enable Super G for a security device with two radios, you need to specify which radio on which to enable Super G:

```
set wlan 1 super-g
```

For a security device with one radio, you do not need to specify a radio:

```
set wlan super-g
```

Basic Wireless Network Feature Configuration

Certain wireless features must be configured, but other features are optional. Each time you make changes to a wireless interface, however, you must reactivate the WLAN (for more information, see “Reactivating a WLAN Configuration” on page 120).

This section explains how to do the following tasks:

- “Creating a Service Set Identifier” on page 116
- “Setting the Operation Mode for a 2.4 GHz Radio Transceiver” on page 117
- “Setting the Operation Mode for a 5 GHz Radio Transceiver” on page 118
- “Reactivating a WLAN Configuration” on page 120

Creating a Service Set Identifier

A wireless network is identified by a service set identifier (SSID). SSIDs allow you to maintain multiple WLANs using one wireless security device. You must bind an SSID to a wireless interface, which can be bound to a security zone. The SSID is a unique name that can be up to 32 text characters in length. To use spaces in the name, you must enclose the name in double quotation marks.

You can create 8 SSIDs for security devices with one radio. For security devices with two radios, you can create 16 SSIDs.

NOTE: You are not constrained by the number of wireless interfaces in the security device when creating SSIDs. You can have more SSIDs than the number of wireless interfaces. You can bind a maximum of four SSIDs to wireless interfaces. You can activate site- or time-specific WLANs by binding and unbinding SSIDs to wireless interfaces as your network needs change.

In the following example, you configure an SSID with the name “My Home Network.” For increased security, you can make the name difficult to guess and not include the location of the device in the SSID name.

WebUI

Wireless > SSID > New: Enter the name in the SSID field, then click **OK**.

CLI

```
set ssid name “My Home Network”
```

Suppressing SSID Broadcast

After creating and SSID, you can disable the broadcasting of SSIDs in beacons that are advertised by the security device. If SSID broadcasting is disabled, only wireless clients that know of the SSID are able to associate. By default, SSIDs are broadcast in beacons.

To suppress an SSID broadcast, use one of the following procedures:

WebUI

Wireless > SSID > Edit (for *name_str*): Select **Disable SSID Broadcast**, then click **OK**.

CLI

set ssid *name_str* ssid-suppression

Isolating a Client

By isolating the client, you prohibit wireless clients in the same subnet from communicating directly with each other. This forces each client to communicate through the firewall. By default, this option is disabled.

To prohibit wireless clients in the same subnet from communicating directly with each other, use one of the following procedures.

WebUI

Wireless > SSID > Edit (for *name_str*): Select **SSID Client Isolation**, then click **OK**.

CLI

set ssid *name_str* client-isolation enable

Setting the Operation Mode for a 2.4 GHz Radio Transceiver

You can configure WLAN 0 to operate in one of the following modes:

- 802.11b mode (11b)
- 11g mode with 802.11b compatibility (11g)
- 11g mode without 802.11b compatibility (11g 11g-only)
- turbo static 11g-only mode

The **11g** mode without 802.11b compatibility (**11g-only**) option prevents the security device to associate with 802.11b clients. When the **11g** option is selected, the device allows association with 802.11b and 802.11g clients. The **11b** option sets the device to only allow association with 802.11b clients. **Turbo** mode is a high performance option.

NOTE: Only 11g-turbo-supported clients can connect when turbo mode is enabled for the security device.

The default mode is set to 802.11g; this mode allows 802.11g and 802.11b clients.

To set the operational mode to 802.11g, use one of the following procedures:

WebUI

Wireless > WLAN > General Settings: Select 802.11g from the Operation Mode list, then click **Apply**. (If the security device has more than one radio, make the selection for the 2.4 GHz radio.)

CLI

To set the operational mode to 802.11g for a security device with one radio, enter the following command:

```
set wlan mode 11g
```

To set the operational mode to 802.11g for a security device with two radios, enter the following command:

```
set wlan 0 mode 11g
```

Setting the Operation Mode for a 5 GHz Radio Transceiver

For security devices with two radios, you can configure WLAN 1, the 5 GHz transceiver, to operate in 802.11a mode or in turbo mode. **802.11a** mode operates within a 5 GHz frequency band and is the default operational mode.

NOTE: Only 11a-turbo-supported clients can associate when turbo mode is enabled on the security device.

By enabling **turbo** mode, you can increase the performance of downloads.

In the following example, you enable **turbo** mode for WLAN 1.

WebUI

Wireless > WLAN > General Settings: Select Turbo mode from the **Operation Mode** list, then click **Apply**.

CLI

To enable turbo mode for WLAN 1, enter the following command:

```
set wlan 1 mode turbo
```

Configuring Minimum Data Transmit Rate

You can set the minimum data transmit rate in megabits per second (Mbps) for sending frames. The data transmit rate depends on the radio type and can be one of the following.

- 802.11a: 6, 9, 12, 18, 24, 36, 48, 54
- 802.11a with XR enabled: 0.25, 0.5, 3, 6, 9, 12, 18, 24, 36, 48, 54
- 802.11b: 1, 2, 5.5, 11
- 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
- 802.11g with XR enabled: .0.25, 0.5, 1, 2, 3, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54
- If turbo is enabled: 12, 18, 24, 36, 48, 72, 96, 108

The **auto** rate, which is the default value, uses the best rate first and then automatically falls back to the next rate if transmission fails.

To configure the data transmit rate, use one of the following procedures:

WebUI

Wireless > General Settings: Select the rate from the Transmit Data Rate list (if the security device has more than one radio, make the selection for the radio you want).

CLI

To set the data transmit rate to 11 Mbps on a security device with one radio, enter the following command:

```
set wlan transmit rate 11
```

To set the data transmit rate to 54 Mbps for the 5GHz radio on a security device with two radios, enter the following command:

```
set wlan 1 transmit rate 54
```

Configuring Transmit Power

You can set the power transmission and adjust the radio range for the security device. You can set the power level to an eighth, full, half, minimum, or quarter of the maximum transmit power, which is the maximum power allowed in the country the security device is operating in. The default is full power.

To configure the transmit power, use one of the following procedures:

WebUI

Wireless > General Settings: Select the power level from the Transmit Power list (if the security device has more than one radio, make the selection for the radio you want).

CLI

To set the transmit power to half on a security device with one radio, enter the following command:

```
set wlan transmit power half
```

To set the transmit per to half for the 5GHz radio on a security device with two radios, enter the following command:

```
set wlan 1 transmit power half
```

Reactivating a WLAN Configuration

After making any changes to a WLAN configuration, you must reactivate the WLAN subsystem within the device, which reboots the wireless interfaces. Any WLAN-related configuration changes take effect only after you reactivate this subsystem.

Depending on the network, the reactivation process can take 60 seconds or more to complete. Wireless traffic is disrupted, and all wireless client sessions are terminated. Wireless clients must reconnect to the wireless network to reestablish connectivity.

To reactivate the system, use one of the following procedures:

WebUI

For security devices with one radio:

Wireless > Activate Changes: Click the Activate Changes button.

For security devices with two radios:

Click the Activate Changes button at the top of any wireless page.

CLI

To reactivate the WLAN, enter the following command:

```
exec wlan reactivate
```

Configuring Authentication and Encryption for SSIDs

The settings for authentication and encryption are specific to each SSID. You can configure different authentication and encryption preferences for each SSID.

ScreenOS supports the following authentication and encryption mechanisms for WLANs:

- Authentication
  - Open
  - WEP (shared-key)
  - WEP (802.1X)

  - WPA (pre-shared key)
  - WPA (802.1X)
  - WPA2 (pre-shared key)
  - WPA2 (802.1X)
- Encryption
  - Advanced Encryption Standard (AES)
  - Temporal Key Integrity Protocol (TKIP)
  - WEP

The following sections describe WEP, WPA, and WPA2 and explain how to configure them in an SSID. For more information about EAP and 802.1X, see “Extensible Authentication for Wireless and Ethernet Interfaces” on page **9**-81.

Configuring Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) provides confidentiality for wireless communication. It uses the Rivest Cipher 4 (RC4) stream cipher algorithm to encrypt and decrypt data as it travels over the wireless link. You can store the WEP key locally or negotiate a key dynamically with an external authentication server. Wireless clients in turn store this key on their systems.

ScreenOS supports two WEP key lengths: 40 and 104 bits. The keys are concatenated with a 24-bit initialization vector (IV) and result in 64 and 128 bit lengths.

NOTE: Some third-party wireless clients include the 24 bits from the IV when specifying their WEP key lengths. To avoid connectivity issues, the same WEP key length described as 40 or 104 bits on the wireless device might actually be the same length as a key described as 64 or 128 bits on a client.

Multiple WEP Keys

You can create up to four WEP keys per SSID.

If you create only one WEP key, the wireless device uses that key to authenticate wireless clients in that SSID and to encrypt and decrypt traffic sent between itself and the clients.

You can also define multiple WEP keys on the wireless device—up to four keys for a single SSID. Using multiple keys allows you to adjust the level of security for different wireless clients within the same SSID. You can use longer keys to provide greater security for some traffic and shorter keys to reduce processing overhead for other, less critical, traffic. The wireless devices use the WEP key specified as **default** for encryption, and another key (or the default key again) for authenticating and decrypting. If you do not specify a key as the default, the first key you define becomes the default.

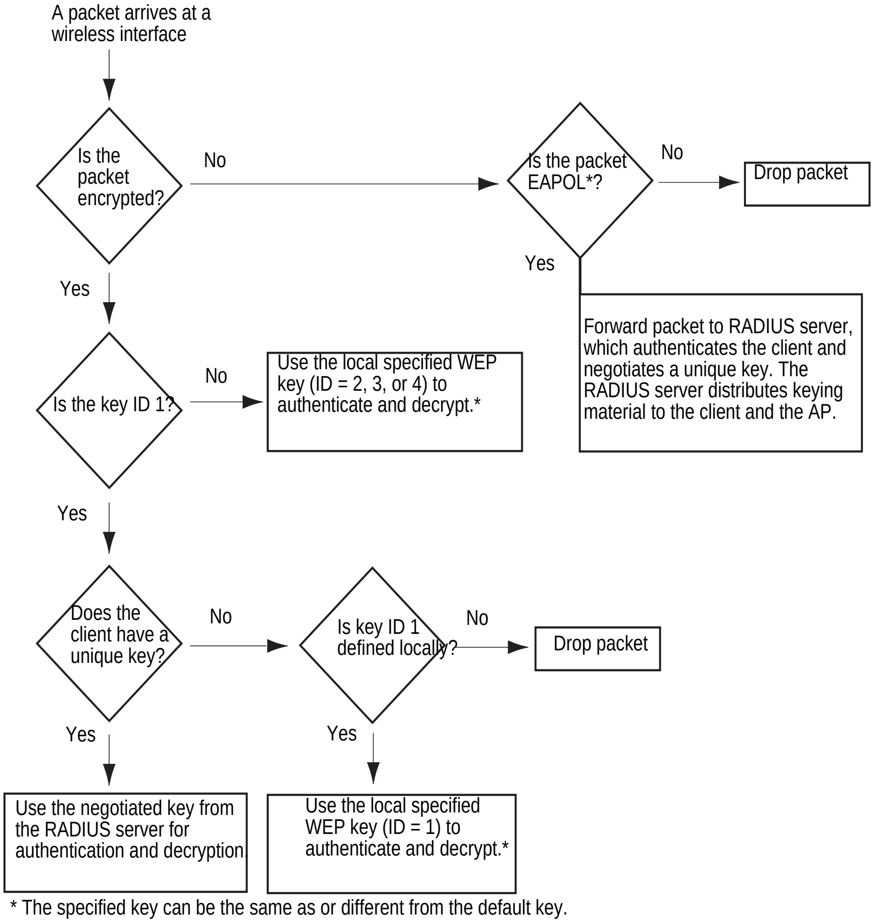
Keep the following in mind about WEP key storage and key ID numbers:

- When clients use a unique, dynamically created WEP key from an external RADIUS server, the wireless device uses this unique specific key—which it also receives from the RADIUS server—for bidirectional communication.
- When wireless clients use statically defined WEP keys stored locally on the wireless device, the device uses the default key to encrypt all wireless traffic that it transmits. The clients must also have this key loaded to be able to decrypt traffic from the wireless device.
- If you store multiple WEP keys on the wireless device, the default key ID can be 1, 2, 3, or 4.
- If you store some WEP keys on the wireless device and use dynamically created WEP keys from an external RADIUS server, the ID for the default WEP key on the wireless device cannot be 1, because the RADIUS server uses 1 as the ID for all of its keys. The wireless device can use a default WEP key with key ID 2, 3, or 4 for encryption, and it can use a statically defined WEP key with ID 1, 2, 3, or 4 for authentication and decryption.
- If you exclusively use WEP keys from a RADIUS server, the server uses a key ID of 1 for all its keys. RADIUS creates and distributes a different key per session for each client.
- You can specify a different locally stored key for the wireless device to use when authenticating and decrypting traffic it receives from wireless clients. The clients must have this key and its ID number loaded to be able to authenticate themselves and encrypt traffic sent to the device. (If a client does not supply a key ID, the device tries to use the default WEP key to authenticate the client and decrypt its traffic.)

NOTE: If a client uses only one key for encrypting, decrypting, and authenticating, then it must use the default WEP key.

Figure 22 shows how the wireless device processes a wireless connection request when WEP keys are stored locally and when they come from a RADIUS server.

Figure 22: Connectivity Process with WEP on RADIUS Server


A packet arrives at a wireless interface
Is the packet encrypted?
No
Is the packet EAPOL*?
No
Drop packet
Yes
Yes
Forward packet to RADIUS server, which authenticates the client and negotiates a unique key. The RADIUS server distributes keying material to the client and the AP.
Is the key ID 1?
No
Use the local specified WEP key (ID = 2, 3, or 4) to authenticate and decrypt.*
Yes
Does the client have a unique key?
No
Is key ID 1 defined locally?
No
Drop packet
Yes
Yes
Use the negotiated key from the RADIUS server for authentication and decryption
Use the local specified WEP key (ID = 1) to authenticate and decrypt.*
* The specified key can be the same as or different from the default key.

Configuring Open Authentication

You can configure open authentication, which specifies that no authentication is performed. The wireless client provides the SSID and is connected to the wireless network. When using open authentication, you can specify the following encryption key options:

- No encryption
- WEP encryption
  - Local key source: The WEP key is stored on the security device. You must specify a default key.
  - Server: The WEP key is a dynamic key negotiated from a RADIUS server.
  - Both: Only available for security devices with one radio, the WEP key is stored on the device and a RADIUS server. You must specify a default key.

You can specify up to four WEP keys per SSID.

Configuring Open Authentication with WEP Keys from RADIUS Server

The following examples use the following parameters for the SSID named hr:

- Open authentication
- WEP encryption
- Dynamically generated WEP key obtained from RADIUS server named rs1

WebUI

Use the following procedure if you have a security device with one radio:

```
Wireless>SSID > Edit: Enter the following, then click OK.
WEP Based Authentication and Encryption Methods: Open, WEP Encryption
Key Source: Server
Auth Server: rs1(click Create new Auth Server to define RADIUS server if it does
    not already exist)
```

Use the following procedure if you have a security device with two radios:

```
Wireless>SSID > Edit: Enter the following, then click OK.
802.1X Based Authentication and Encryption Methods: 802.1X
Auth Server: rs1 (click Create new Auth Server to define RADIUS server if it does
    not already exist)
```

CLI

Use the following command if you have a security device with one radio:

```
set ssid hr authentication open encryption wep key-source server rs1
```

Use the following command if you have a security device with two radios:

```
set ssid hr authentication 802.1x auth-server rs1
```

Configuring Open Authentication with Local WEP Keys

The following examples use the following parameters for the SSID named hr:

- Open authentication
- WEP encryption
- WEP key stored locally on security device
- Key ID: 1
- Key length: 40-bit
- ASCII text: 1a2i3
- Key with ID 1 is default key

WebUI

Use the following procedure if you have a security device with one radio:

```
Wireless>SSID > Edit: Enter the following, then click OK.
WEP Based Authentication and Encryption Methods: Open, WEP Encryption
Click WEP Key, enter the following, then click Add:
    Key ID: 1
    Key Length: 40
    Key String: Select ASCII and enter 1a2i3 (provide again in Confirm field)
    Default Key (select)
```

Use the following procedure if you have a security device with two radios:

```
Wireless>SSID > Edit: Enter the following, then click OK.
WEP Based Authentication and Encryption Methods: Open, WEP Encryption
Click WEP Key, enter the following, then click Add:
    Key ID: 1
    Key Length: 40
    Key String: Select ASCII and enter 1a2i3 (provide again in Confirm field)
    Default Key (select)
```

CLI

Use the following command if you have a security device with one radio:

```
set ssid hr key-id 1 length 40 method asciitext 1a2i3 default
set ssid hr authentication open wep key-source local
```

Use the following command if you have a security device with two radios:

```
set ssid hr key-id 1 length 40 method asciitext 1a2i3 default
set ssid hr authentication open encryption wep
```

Configuring WEP Shared-Key Authentication

You can configure a static WEP key that is stored on the security device that is used to authenticate clients, who also have the static WEP key configured on their wireless devices. You can create up to four WEP keys per SSID.

You can specify a 40-bit encryption by providing a 5-digit hexadecimal number or a string consisting of 5 ASCII characters. Specify 104-bit encryption by providing a 26-digit hexadecimal number or a string consisting of 13 ASCII characters.

The following examples use the following parameters for the SSID named hr:

- WEP shared-key
- Key ID: 1
- Key length: 40-bit
- ASCII text: 1a2i3
- Key with ID 1 is default key

WebUI

Wireless>SSID > Edit: Enter the following, then click OK.
WEP Based Authentication and Encryption Methods: WEP Shared Key
Click WEP Key, enter the following, then click Add:
Key ID: 1
Key Length: 40
Key String: Select ASCII and enter 1a2i3 (provide again in Confirm field)
Default Key (select)

CLI

```
set ssid hr authentication shared-key
set ssid hr key-id 1 length 40 method asciitext 1a2i3 default
```

ScreenOS provides a mechanism for automatically negotiating with a wireless client whether it authenticates itself with a WEP shared key. Using this option can improve compatibility if you want to allow access to wireless clients using various operating systems that support different implementations of WEP.

To enable automatic negotiation, do one of the following:

WebUI

Wireless > SSID > Edit (for *name_str)*: Select **Auto**.

CLI

set ssid *name_str* authentication auto

NOTE: Although you can configure WEP for all of the SSIDs, the device intentionally restricts its use to only one interface at a time. For this reason, we recommend using WPA or WPA2.

Configuring Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a more secure solution for WLAN authentication and encryption and was designed in response to many of the weaknesses in WEP. ScreenOS supports WPA and WPA2.

WPA and WPA2 support 802.1X authentication, which use an Extensible Authentication Protocol (EAP) method for authentication through a RADIUS server. EAP is an encapsulation protocol used for authentication and operates at the Data Link Layer (Layer 2). For more information, refer to RFC 2284, *PPP Extensible Authentication Protocol (EAP)*.

ScreenOS interoperates with 802.1X-compliant RADIUS servers, such as the Juniper Networks Steel-Belted RADIUS server and the Microsoft Internet Authentication Service (IAS) RADIUS server.

When using WPA or WPA2 with a RADIUS server, the security device forwards authentication requests and replies between the wireless clients and the RADIUS server. After successfully authenticating a client, the RADIUS server sends an encryption key to the client and the security device. From that point, the security device manages the encryption process, including the encryption type—Temporal

Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES)—and the rekey interval. For information about TKIP, see the IEEE Standard 802.11. For information about AES, see RFC 3268, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.

You can also use WPA or WPA2 with a pre-shared key, which is a static key that is configured on the security device and the client's device. Both devices use the key to generate a unique key (group key) for the session. You can specify the pre-shared key by using an ASCII passphrase (password) or in hexadecimal format. You also use the same encryption types as with 802.1X authentication: TKIP or AES.

If you want to allow WPA and WPA2 as the authentication type, you can specify the wpa-auto keyword (or WebUI option) if you are using 802.1X as the authentication method or the wpa-auto-psk keyword (or WebUI option) if you are using a pre-shared key as the authentication method.

Configuring 802.1X Authentication for WPA and WPA2

To configure 802.1X authentication for WPA and WPA2, you specify the following:

- RADIUS server
- Encryption type: In addition to TKIP or AES, you can specify auto, which specifies TKIP and AES as the encryption type.
- Rekey interval: Time that elapses before the group key for clients is updated. By default, the rekey interval is 1800 seconds (30 minutes). The value range is 30 through 4294967295 seconds. Use the **disable** CLI keyword or specify zero (0) in the WebUI to disable the rekey interval.

In addition to specifying WPA or WPA2 as the authentication type, you can also specify the auto option, which allows WPA and WPA2 as the authentication type.

The following examples use the following parameters for an SSID named hr:

- WPA (auto option)
- RADIUS server named rs1
- Rekey interval of 3600 seconds
- Encryption type of AES

WebUI

Wireless > SSID > (select hr SSID): Enter the following information, then click **OK**.

WPA Based Authentication and Encryption Methods: WPA Auto Pre-shared Key
Auth Server: rs1 (click Create new Auth Server to define RADIUS server if it does not already exist)
Rekey Interval: 3600
Encryption Type: AES

CLI

```
set ssid hr authentication wpa-auto rekey-interval 3600 encryption aes auth-server
    rs1
```

Configuring Pre-Shared Key Authentication for WPA and WPA2

To configure pre-shared key authentication for WPA and WPA2, you specify the following:

- Pre-shared key
  - Hexadecimal format: Specifies the key in raw format, which is a 256-bit (64 characters) hexadecimal value.
  - ASCII passphrase: Specifies a passphrase to access the SSID and consists of 8 to 63 ASCII characters.
- Encryption type: In addition to TKIP or AES, you can specify auto, which specifies TKIP and AES as the encryption type.
- Rekey interval: Time that elapses before the group key for clients is updated. By default, the rekey interval is 1800 seconds (30 minutes). The value range is 30 through 4294967295 seconds. Use the **disable** CLI keyword or specify zero (0) in the WebUI to disable the rekey interval.

In addition to specifying WPA or WPA2 as the authentication type, you can also specify the auto option, which allows WPA and WPA2 as the authentication type.

The following examples use the following parameters for an SSID named hr:

- WPA2
- Pre-shared key using ASCII passphrase of $FKwinnisJamesTown8fg4
- Rekey interval of 3600 seconds
- Encryption type of TKIP

WebUI

Wireless > SSID > (select hr SSID): Enter the following information, then click **OK**.

WPA Based Authentication and Encryption Methods: WPA2 Pre-shared Key
Key by Password: $FKwinnisJamesTown8fg4 (provide passphrase again in Confirm Key by Password field)
Rekey Interval: 3600
Encryption Type: TKIP

CLI

```
set ssid hr authentication wpa2-psk passphrase $FKwinnisJamesTown8fg4
    encryption tkip rekey-interval 3600
```

Specifying Antenna Use

The wireless security device allows you to choose a specific antenna or enable antenna diversity. Antenna A or antenna B, whichever has the stronger signal, is used when diversity is selected. The default setting is diversity. The diversity setting adapts in most situations. To use an external unidirectional antenna, you can specify antenna A or antenna B. For some security devices, antenna A is antenna closest to the power inlet. Antennae A and B are labeled on some security devices. See your hardware manual for more information.

To change the antenna setting, use one of the following procedures:

WebUI

Wireless > General Settings: Select the antenna setting from the Antenna Diversity list, then click **OK**.

CLI

To select antenna A on a security device with one radio, enter the following command:

```
set wlan antenna a
```

To select antenna A for the 5GHz radio on a security device with two radios, enter the following command:

```
set wlan 1 antenna a
```

Setting the Country Code, Channel, and Frequency

The regulatory domains used for channel assignments come preset as FCC (US), TELEC (Japan), ETSI (Europe), or WORLD (all countries). The ETSI regulatory domain is available only for security devices with two radios. You cannot change a preset regulatory domain. If the regulatory domain is preset to FCC or TELEC, you cannot select a country. If the regulatory domain is WORLD or ETSI, you must select a country. If you do not set a country for a device preset to WORLD or ETSI, a warning message appears, and wireless capabilities will not function.

The wireless security device uses the same channel and frequency for all SSIDs in one radio transceiver. The device automatically selects the appropriate channel based on the country code that you enter (unless you manually selected a specific channel). The channel in use appears in the channel list in the WebUI. The device can select the channel if you leave the setting at auto.

For the list of available country codes, channels, and frequencies, see “Wireless Information” on page A-I.

To configure the country code and channel, use one of the following procedures:

WebUI

Wireless > General Settings: Select the country, channel, and frequency from the dropdown lists, then click **Apply**.

CLI

```
set wlan country-code country_abbreviation
set wlan { 0 | 1 } channel { auto | 1 | 2 | 3 | ... }
```

Using Extended Channels

If the security device is located in a regulatory domain that allows the use of channels 12 and 13, you can enable the 2.4 GHz radio transceiver to use them.

WebUI

WIreless > General Settings > Select the Extended Channel Mode checkbox.

CLI

For a security device with one radio, enter the following command:

```
set wlan extended-channel
```

For a security device with two radios, enter the following command:

```
set wlan 0 extended-channel
```

Performing a Site Survey

You can scan the broadcast vicinity to see if there are any other access points broadcasting nearby. Running a site survey allows you to see if there are any rogue access points in the area. A site survey detects any access points emitting a beacon in the area and records the following details about each detected access point:

- Service Set Identifier (SSID)
- MAC address
- Received signal strength indicator (RSSI)

  The RSSI numbers are measured in decibels (dBs), which indicate the signal-to-noise ratio (SNR). The SNR is the signal level divided by the noise level, which results in a value representing signal strength.
- Broadcast channel

In addition to performing an initial site survey, you might want to perform surveys occasionally to ensure that no rogue access points are in the area. To perform a site survey:

WebUI

WIreless > Statistics > Site Survey

CLI

```
exec wlan site-survey
```

NOTE: Depending on your network, a site survey can take up to 60 seconds to complete and disrupts wireless network traffic.

Locating Available Channels

Using the CLI, you can find the best radio channel for the device to use for transmission. Use this command if you do not want to use the default setting that automatically select channels and want to find the channel with the least interference.

To find the best channel available, use the following command:

```
exec wlan find-channel
```

NOTE: This feature is not available from the WebUI.

Setting an Access Control List Entry

You can control which wireless clients have access to the network through an access control list (ACL). The ACL identifies clients by their MAC addresses and specifies whether the wireless device allows or denies access for each address. The ACL can operate in one of three access modes:

- Disabled: The wireless device does not filter any MAC addresses. This is the default mode.
- Enabled: The wireless device allows access to all clients except those marked with a **Deny** action.
- Strict: The wireless device denies access to all clients except those marked with an **Allow** action.

NOTE: The ACL settings apply globally to all SSIDs*.*

You can define up to 64 denied clients and 64 allowed clients.

To add a MAC address to the ACL, use one of the following procedures:

WebUI

Wireless > MAC Access List: Enter the following, then click **Add**:

Access Mode: (select one of the three modes from the list)
Input a new MAC address: (type the MAC address of a wireless client)
Control Status: (select either **Allow** or **Deny**)

In the WebUI, you can also select a MAC address from the Select a learned MAC address list. Entries appear in this list when a wireless client makes an association with the wireless device. The list is a dynamic display of all currently associated wireless clients, regardless of the SSID to which they belong.

NOTE: You can also set the access mode through the MAC Address Access Control list on the Wireless > General Settings page.

CLI

```
set wlan acl mode { disable | enable | strict }
set wlan acl mac_addr { deny | allow }
```

Configuring Super G

In wireless devices that have an Atheros Communications chipset with Super G® feature, you can enable Super G, which can increase user data throughput rate up to 4 Mbps for 802.11a and 802.11g clients by using the following methods:

- Bursting: Allows the device to transmit multiple frames in a burst rather than pausing after each frame.
- Fast frames: Allows for more information per frame to be transmitted by allowing a larger-than-standard frame size.
- Compression: Link-level hardware compression is performed by a built-in data compression engine.

By default, this feature is disabled.

If wireless clients do not support Super G and the security device has Super G enabled, they can still connect to the wireless network, but the Super G feature is not available.

NOTE: You can read more about Atheros Communications Super G chipset at www.atheros.com

To enable Super G, use one of the following procedures:

WebUI

Wireless > General Settings: Select the Super-G checkbox (if the security device has more than one radio, make the selection for the radio you want).

CLI

To enable Super G on a security device with one radio, enter the following command:

```
set wlan super-g
```

To enable Super G for the 5GHz radio on a security device with two radios, enter the following command:

```
set wlan 1 super-g
```

Configuring Atheros XR (Extended Range)

You can enable Atheros Communications eXtended Range (XR) technology. XR processes 802.11 signals, defined by IEEE 802.11a and 802.11g standards, so that wireless networks to have fewer “dead spots” and greater range than usual. XR processes weaker signals more effectively and allows greater coverage. XR provides increased coverage at a lower data transmission rate.

Only the first active SSID per radio can support XR. When XR is enabled, the first active SSID per radio uses the XR feature.

To enable XR, use one of the following procedures:

WebUI

Wireless > General Settings: Select the XR Support checkbox (if the security device has more than one radio, make the selection for the radio you want).

CLI

To enable XR on a security device with one radio, enter the following command:

```
set wlan xr
```

To enable XR for the 5GHz radio on a security device with two radios, enter the following command:

```
set wlan 1 xr
```

Configuring Wi-Fi Multimedia Quality of Service

Wi-Fi™ Multimedia (WMM) quality of service (QoS) feature enables you to enhance the performance of your wireless network by adjusting the transmission priorities of audio, video, and voice applications to accommodate the different latency and throughput requirements of each application. By default, WMM is disabled.

WMM is based on Enhanced Distributed Channel Access (EDCA) as defined in 802.11e. For more information about WMM, see http://www.wi-fi.org.

This feature is not available for all security devices.

Enabling WMM

You can enable WMM on the 2.4 GHz radio (WLAN 0) or 5 GHz radio (WLAN 1).

To enable WMM, use one of the following procedures:

WebUI

Wireless > WMM Settings > Select the **Enable** radio button for the radio, then click **Apply**.

CLI

```
set wlan [ 0 | 1 ] wmm enable
```

Configuring WMM Quality of Service

After you enable WMM, you can configure WMM parameters accommodate your network requirements. You configure WMM to operate from each end of the connection: access point (ap) and station (sta).

- *ap* is the WMM configuration for the security device.
- *station* is the WMM configuration for the client. Clients internally queue traffic according to the four ACs and then send packets as they detect transmit opportunities based on the parameters you set.

The WMM settings are used only when the security device or clients (stations) send a packet.

Access Categories

Based on Internet Engineering Task Force (IETF) Differentiated Services Code Point (DSCP) headers, the security device and client sort traffic into one of four access categories (AC):

- Best effort (0)—traffic that cannot process QoS levels and traffic that is less sensitive to latency but that can be affected by long delays.
- Background priority (1)—low-priority traffic
- Video (2)—video traffic gets a higher priority than other data traffic
- Voice (3)—voice traffic gets the highest priority

Table 3 lists the mappings between access categories and Type of Service (TOS).

Table 3: Access Category and TOS Mappings

Access Category	TOS Value
Voice	0xC0, 0xB8, 0xE0
Video	0x80, 0xA0, 0x88
Best effort	0x00, 0x60, or other
Background	0x40, 0x20

NOTE: 802.1d tags are not supported.

Although specific priorities and settings are associated with each AC, you can override these settings through the WebUI or the CLI.

WMM Default Settings

The following terms describe the configurable WMM parameters and appear as column headings in Table 4 and Table 5, which list the default settings for access point (security device) and station (client) configuration:

- *aifs*

  Arbitrary Inter-Frame Space Number (AIFSN) specifies the number of slots, after a SIFS duration, that the security device or client for an AC will check the medium-idle before transmitting or executing a backoff.

- *logcwmin* and *logcwmax*

  WMM defines a Contention Window (CW), which is equivalent to a random backoff period.

  The CWmin parameter specifies the minimum number of slots of the contention window used by the security device or client for a particular AC to generate a random number for the backoff. If logcwmin is x, then CWmin is 2^x-1.

  The CWmax parameter specifies the maximum number of slots of the window used by the security device or client for a particular AC to generate a random number for the backoff. If logcwmax is x, then CWmax is 2^x-1.

  ScreenOS does not support contention-free or scheduled access.

- *txoplimit*

  Transmit Opportunity specifies the maximum amount of time the security device or client can initiate transmissions. If you set txoplimit to x, the maximum time is 32*x microseconds.

- *ackpolicy*

  You can enable or disable an acknowledgement policy for the access point. This parameter does not apply to clients.

Table 4 lists the default values for all supported wireless modes for a security device in application type WMM. By default, *ackpolicy* is disabled for all wireless modes.

Table 4: Access Point WMM Default Values Organized by AC

AC	Wireless Mode	aifs	logcwmin	logcwmax	txoplimit
Best Effort (0)	802.11a	3	4	6	0
	802.11a Turbo	2	3	5	0
	802.11b	3	5	7	0
	802.11g	3	4	6	0
	802.11g Turbo	2	3	5	0
	XR	0	3	3	0
Background (1)	802.11a	7	4	10	0
	802.11a Turbo	7	3	10	0
	802.11b	7	5	10	0
	802.11g	7	4	10	0
	802.11g Turbo	7	4	10	0
	XR	0	3	3	0
Video (2)	802.11a	1	3	4	94
	802.11a Turbo	1	2	3	94
	802.11b	1	4	5	188
	802.11g	1	3	4	94
	802.11g Turbo	1	2	3	94
	XR	0	3	3	0
Voice (3)	802.11a	1	2	3	47
	802.11a Turbo	1	2	2	47
	802.11b	1	3	4	102
	802.11g	1	2	3	47
	802.11g Turbo	1	2	2	47
	XR	0	3	3	0

Table 5 lists the default values for all supported wireless modes for the WMM configuration for a client (sta).

Table 5: Station WMM Default Values Organized by AC

AC	Wireless Mode	aifs	logcwmin	logcwmax	txoplimit
Best Effort	802.11a	3	4	10	0
	802.11a Turbo	2	3	10	0
	802.11b	3	5	10	0
	802.11g	3	4	10	0
	802.11g Turbo	2	3	10	0
	XR	0	3	3	0
Background	802.11a	7	4	10	0
	802.11a Turbo	7	3	10	0
	802.11b	7	5	10	0
	802.11g	7	4	10	0
	802.11g Turbo	7	4	10	0
	XR	0	3	3	0
Video	802.11a	2	3	4	94
	802.11a Turbo	2	2	3	94
	802.11b	2	4	5	188
	802.11g	2	3	4	94
	802.11g Turbo	2	2	3	94
	XR	0	3	3	0
Voice	802.11a	2	2	3	47
	802.11a Turbo	1	2	2	47
	802.11b	2	3	4	102
	802.11g	2	2	3	47
	802.11g Turbo	1	2	2	47
	XR	0	3	3	0

Example

In the following example, you use the station configuration of WMM on the 5 GHz transceiver and change the settings for voice traffic (A = 0) as follows:

- logcwmin: zero (0)
- logcwmax: 15
- aifs: 4
- txoplimit: 10

To configure WMM with these settings:

WebUI

Wireless > WMM Settings: Enter the desired settings, then click **Apply**.

CLI

```
set wlan 1 wmm sta 0 logcwmin 0
set wlan 1 wmm sta logcwmax 15
set wlan 1 aifs 4
set wlan 1 txoplimit 10
save
```

Configuring Advanced Wireless Parameters

This section contains information about advanced wireless parameters. You might need to make small changes to increase performance in certain type of wireless deployments.

The following advanced wireless features are discussed in this section:

- "Configuring Aging Interval" on page 138
- "Configuring Beacon Interval" on page 139
- "Configuring Delivery Traffic Indication Message Period" on page 140
- "Configuring Burst Threshold" on page 140
- "Configuring Fragment Threshold" on page 140
- "Configuring Request To Send Threshold" on page 141
- "Configuring Clear To Send Mode" on page 141
- "Configuring Clear To Send Rate" on page 142
- "Configuring Clear To Send Type" on page 142
- "Configuring Slot Time" on page 142
- "Configuring Preamble Length" on page 143

Configuring Aging Interval

You can specify the amount of time that elapses before a wireless client is disconnected if there is no traffic to or from the client. This value can be between 60 seconds and 1,000,000 seconds. The default value is 300 seconds. To disable aging, use the **set wlan advanced aging-interval disable** command.

After the aging-interval elapses and a client is disconnected, its MAC information is deleted from a MAC table on the security device. The MAC table for each radio can contain up to 60 client MAC addresses. Because new clients are denied connectivity when the MAC table is full, set the aging-interval so that existing clients whose connections are not being used are disconnected and their MAC addresses are removed from the MAC table in a timely manner.

To set the aging interval to 500 seconds for the 2.4 GHz radio, use one of the following procedures:

WebUI

Wireless > General Settings > Advanced: Enter the following, then click Return.
Aging Interval: 500 (for devices with two radios, specify the aging interval for WLAN0)

CLI

To change the aging interval for a security device with one radio, enter the following command:

```
set wlan advanced aging-interval 500
```

To change the aging interval to 500 seconds for the 2.4 GHz radio on a security device with two radios, enter the following command:

```
set wlan 0 advanced aging-interval 500
```

Configuring Beacon Interval

You can configure the interval at which beacons are sent. The value range is 20 to 1,000 time units (1 time unit equals 1024 μs) The default value is 100 time units.

To set the beacon interval to 200 time units (2048 μs) for the 2.4 GHz transceiver, use one of the following procedures:

WebUI

Wireless > General Settings > Advanced: Enter the following, then click Return.
Beacon Interval: 200 (for devices with two radios, specify the beacon interval for WLAN0)

CLI

To change the beacon interval for a security device with one radio, enter the following command:

```
set wlan advanced beacon-interval 200
```

To change the beacon interval for the 2.4 GHz radio on a security device with two radios, enter the following command:

```
set wlan 0 advanced beacon-interval 200
```

Configuring Delivery Traffic Indication Message Period

You can set the number of beacons that are sent before the delivery traffic indication map (DTIM) is sent. Increasing the DTIM period decreases the number of broadcasts sent to clients. The value range is 1 to 255. The default value is 1 beacon interval.

To set the DTIM period to 2, use one of the following procedures:

WebUI

Wireless > General Settings > Advanced: Enter the following, then click Return.
DTIM Period: 2 (for devices with two radios, specify the DTIM period for WLAN0)

CLI

To change the DTIM period for a security device with one radio, enter the following command:

```
set wlan advanced dtim-period 2
```

To change the DTIM period for the 2.4 GHz radio on a security device with two radios, enter the following command:

```
set wlan 0 advanced dtim-period 2
```

Configuring Burst Threshold

You can set a maximum number of frames in a burst. The valid range is between 2 and 255. The default value is 3. This feature is not available on all security devices.

To change the burst threshold to 5, use one of the following procedures:

WebUI

Wireless > General Settings > Advanced: Enter the following, then click Return.
Burst Threshold: 5

CLI

```
set wlan advanced burst-threshold 5
```

Configuring Fragment Threshold

You can set the maximum length of a frame before it is fragmented into multiple frames before transmission. Value range is even numbers between 256 and 2346. The default value is 2346.

To set the fragment threshold to 500 for the 2.4 GHz radio, use one of the following procedures:

WebUI

Wireless > General Settings > Advanced: Enter the following, then click Return.
Fragment Threshold: 500 (for devices with two radios, specify the fragment threshold for WLAN0)

CLI

To change the fragment threshold for a security device with one radio, enter the following command:

```
set wlan advanced fragment-threshold 500
```

To set the fragment threshold for the 2.4 GHz radio on a security device with two radios, enter the following command:

```
set wlan 0 advanced fragment-threshold 500
```

Configuring Request To Send Threshold

You can set the maximum length a frame is before using the Request to Send (RTS) method to send the frame. The value range is 256 to 2346. The default value is 2346.

To set the RTS threshold to 500 for the 2.4 GHz radio, use one of the following procedures:

WebUI

Wireless > General Settings > Advanced: Enter the following, then click Return.
RTS Threshold: 500 (for devices with two radios, specify the RTS threshold for WLAN0)

CLI

To change the RTS threshold for a security device with one radio, enter the following command:

```
set wlan advanced rts-threshold 500
```

To set the RTS threshold of the 2.4 GHz radio on a security device with two radios, enter the following command:

```
set wlan 0 advanced rts-threshold 500
```

Configuring Clear To Send Mode

Clear To Send (CTS) protection blocks acknowledgement (ACK) packets to reduce some of the overhead required to run 802.11. The default setting is *auto*. By default the security device detects the CTS setting of clients. You can also select *on* to always use CTS or *off* to never use CTS.

NOTE: This feature does not work in 802.11b wireless mode and is not available on all security devices.

When modifying default behavior of the security device, you might also have to modify the CTS rate and type, as described in “Configuring Clear To Send Rate” and “Configuring Clear To Send Type.”

To turn off CTS protection, use one of the following procedures:

WebUI

Wireless > General Settings > Advanced: Select the following, then click Return.
CTS Mode: Off

CLI

```
set wlan advanced cts-mode off
```

Configuring Clear To Send Rate

You can set the rate (in Mbps) at which CTS frames are sent. This feature does not work in 802.11b wireless mode and is not available on all security devices. Valid values are 1, 2, 5.5, and 11 Mbps. The default is 11 Mbps.

To set the CTS rate to 5.5, use one of the following procedures:

WebUI

Wireless > General Settings > Advanced: Select the following, then click Return.
CTS Rate: 5.5

CLI

```
set wlan advanced cts-rate 5.5
```

Configuring Clear To Send Type

ScreenOS provides two Clear To Send (CTS) protection types: CTS-only and CTS-RTS. The purpose of CTS is to decrease collisions between two wireless clients. The CTS-only option (default) forces the security device to wait for a CTS frame before forwarding any data. The CTS-RTS (Request to Send) option forces the security device to complete a RTS -CTS handshake before forwarding data.

This feature is not available on all security devices.

To set the CTS type to CTS-only, use one of the following procedures:

WebUI

Wireless > General Settings > Advanced: Select the following, then click Return.
CTS Type: CTS Only

CLI

```
set wlan advanced cts-type cts-only
```

Configuring Slot Time

When the slot time is set to long, the security device uses only long slot time. By default, the security devices uses short slot time. This feature is used only in 802.11g mode.

To enable long slot time for the 2.4 GHz radio, use one of the following procedures:

WebUI

Wireless > General Settings > Advanced: Select the Long Slot Time checkbox, then click Return.

CLI

To enable long slot time for a security device with one radio, enter the following command:

```
set wlan advanced slot-time long
```

To enable long slot time for the 2.4 GHz radio on a security device with two radios, enter the following command:

```
set wlan 0 advanced slot-time long
```

Configuring Preamble Length

You can modify the transmit preamble from short to long. When set to long, only long preambles are used. When short is enabled, both short and long preambles are used. The default is short. This command only applies when setting the 2.4 GHz transceiver for 802.11b and 802.11g modes.

WebUI

Wireless > General Settings > Advanced: Select the Long Transmit Preamble checkbox, then click Return.

CLI

To enable long preambles for a security device with one radio, enter the following command:

```
set wlan advanced long-preamble
```

To enable long preambles for the 2.4 GHz radio on a security device with two radios, enter the following command:

```
set wlan 0 advanced long-preamble
```

Working with Wireless Interface

This section describes the following tasks you can perform with wireless interfaces.

Binding an SSID to a Wireless Interface

When the security device initially boots, several wireless interfaces exist, but they are not associated with SSIDs. After creating an SSID, you need to bind the interface to an SSID to activate the interface.

For security devices with one radio, after you create an SSID, you must bind it to a wireless interface that is bound to a specific security zone. For security devices with two radios, wireless interfaces can be bound to a zone or placed in a bridge group (brgoup). For more information about bridge groups, see “Creating Wireless Bridge Groups” on page 145.

To bind an SSID to a wireless interface, use one of the following procedures:

WebUI

Wireless > SSID > Edit (for the SSID that you want to bind to an interface): Select an interface from the Wireless Interface Binding list, then click **OK**.

or

For security devices with one radio, do the following:

Network > Interfaces > Edit: Select the SSID from the Bind to SSID list, then click **OK**.

For security devices with two radios, do the following:

Network > Interfaces > List > Edit: Select the SSID from the Bind to SSID list, then click **OK**.

CLI

set ssid *name_str* interface *interface*

Binding a Wireless Interface to a Radio

On some security devices, you can specify the radio a wireless interface uses. By default, wireless interfaces are bound to two radios and can run in 802.11a, 802.11b, or 802.11g modes.

You can enable the following options:

- 0, which enables only the 2.4 GHz transceiver for 802.11b and 802.11g.
- 1, which enables only the 5 GHz transceiver for 802.11a.
- both, which enables both transceivers (2.4 GHz and 5 GHz) on the interface (802.11a/b/g).

For example, if you specify 802.11b as the operation mode with the **set wlan mode** command and select the **0** option, only 802.11b is available for the wireless interface.

To specify that a wireless0/0 interface use the 2.4 GHz radio, use one of the following procedures:

WebUI

Network > Interface > List > Edit (for the wireless interface): Select 2.4G(802.11b/g) from the Wlan list, then click **OK**.

CLI

set interface wireless0/0 wlan 0

Creating Wireless Bridge Groups

Some security devices support bridge groups (bgroup). A bgroup allows network users to switch between wired/wireless traffic without having to reconfigure or reboot the device. You can configure multiple SSIDs to operate one bgroup or configure an SSID to operate in the same subnet as the wired subnet. Each grouped interface is noted as bgroup*x*, with *x* being 0 through 3.

To set an Ethernet and wireless interface to the same bgroup, use one of the following procedures:

WebUI

Network > Interfaces > List > Edit (for bgroup) > Bind Port: Select **Bind to Current Bgroup** for the interface, then click **Apply**

CLI

To set an Ethernet and wireless interface to the same bridge group interface, do the following:

```
set interface bgroup_name port wireless_interface
set interface bgroup_name port ethernet_interface
```

NOTE: The *bgroup_name* can be bgroup0—bgroup3.
The *ethernet_interface* can be ethernet0/0—ethernet0/4.
The *wireless_interface* can be wireless0/0—wireless0/3.

Disabling a Wireless Interface

You can disable a particular wireless interface from the WebUI or the CLI. By default, when you bind an interface to an SSID, it is activated. This feature is not available on all platforms.

To disable a wireless interface, use one of the following procedures:

WebUI

Network > Interfaces > List > Deactivate (for wireless interface to be disabled)

CLI

```
set interface wlan_if_name shutdown
```

Viewing Wireless Configuration Information

You can view details of wireless configurations and statistics. These command are available from the CLI and not the WebUI.

To view a WLAN configuration, enter the following command:

```
device-> get wlan
AP software version: 5.0
AP bootrom version: 1..1
     Regulatory Domain is World,  Country Code is China
     ACL mode is disabled
```

```
WLAN    Mode    Antenna     Channel     Rate    Power   Super G
0       b/g     Diversity   AUTO        11      full    Enabled
1       a       a           116 (5580)  54      full    Disabled
```

To view wireless interface association information, enter the following command:

```
get interface wlan_if_name association [ mac_addr ]
```

To view the Access Control List (ACL) for a WLAN, enter the following command:

```
get wlan acl
```

To view interface details for a WLAN interface, enter the following command:

```
get interface wlan_if_name
```

Configuration Examples

This section contains configurations for the following examples:

- “Example 1: Open Authentication and WEP Encryption” on this page
- “Example 2: WPA-PSK Authentication with Passphrase and Automatic Encryption” on page 147
- “Example 3: WLAN in Transparent Mode” on page 147
- “Example 4: Multiple and Differentiated Profiles” on page 151

Example 1: Open Authentication and WEP Encryption

In this example for a security device with one radio, you create a BSS with the SSID named **openwep,** which you then bind to the wireless2 interface. This configuration sets the WEP key-id to 1 with an input ASCII string of 40-bits. This configuration allows anyone to authenticate but encrypts communication using the WEP key.

WebUI

Wireless > SSID > New: Enter the following, then click OK:

SSID: openwep

> WEP Key: Enter the following, then click **Back to SSID Edit**:

Key ID:1
Key Length: 40
Key String
ASCII: (select), abcde
Add: (select)

> WEP Based Authentication and Encryption Methods

Open: (select)
WEP Encryption: (select); Key Source: Local
Wireless Interface Binding: wirelesse2

Wireless > Activate Changes: Click on the **Activate Changes** button.

CLI

```
set ssid name openwep
set ssid openwep key-id 1 length 40 method ascii abcde
set ssid openwep authentication open encryption wep
set ssid openwep interface wireless2
exec wlan reactivate
```

Example 2: WPA-PSK Authentication with Passphrase and Automatic Encryption

In this example for a security device with one radio, you create an SSID named **wpapsk**, which you then bind to the wireless2 interface. The configuration sets Wi-Fi Protected Access (WPA) authentication with a preshared key and automatic encryption. Wireless clients who want to connect to the wireless2 interface to access the network must use the WPA passphrase i7BB92-5o23iJ when establishing a wireless connection.

WebUI

Wireless > SSID > New: Enter the following, then click **OK**:

SSID: wpapsk

> WPA Based Authentication Methods

WPA Pre-shared Key: (select)
  Key by Password: (select), i7BB92-5o23iJ
  Confirm key by Password: i7BB92-5o23iJ
  Encryption Type: Auto
Wireless Interface Binding: wireless2

Wireless > Activate Changes: Click the **Activate Changes** button.

CLI

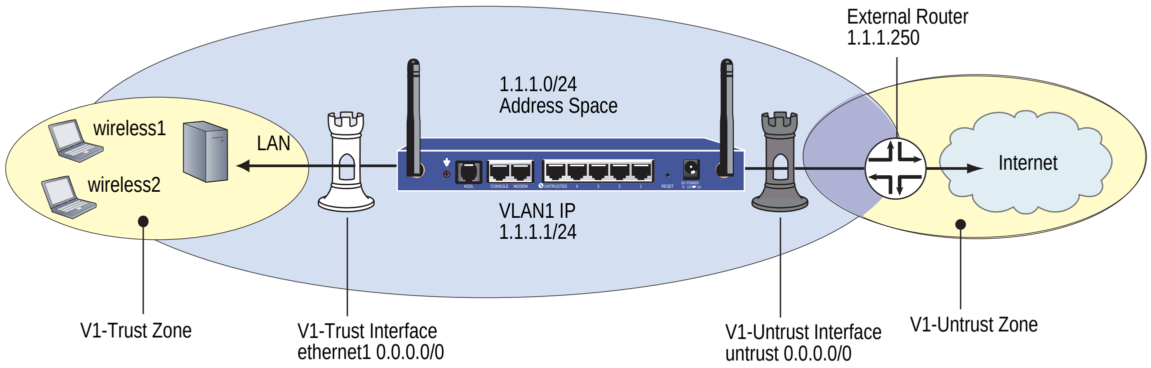
```
set ssid name wpapsk
set ssid wpapsk authentication wpa-psk passphrase i7BB92-5o23iJ encryption
    auto
set ssid wpapsk interface wireless2
exec wlan reactivate
```

Example 3: WLAN in Transparent Mode

In this example, a single WLAN is protected by a security device with one radio in Transparent mode. To increase the security of management traffic, do the following

1. Change the HTTP port number for WebUI management from 80 to 5555, and the Telnet port number for CLI management from 23 to 4646.
2. Use the VLAN1 IP address—1.1.1.1/24—to manage the security device from the V1-Trust security zone.
3. Configure a default route to the external router at 1.1.1.250, so that the security device can send outbound VPN traffic to it. (The default gateway on all hosts in the V1-Trust zone is also 1.1.1.250.)

Table 6: WLAN Device in Transparent Mode



WebUI

1. **VLAN1 Interface**

   Network > Interfaces > Edit (for the VLAN1 interface): Enter the following, then click **OK**:

   IP Address/Netmask: 1.1.1.1/24
   Management Services: WebUI, Telnet (select)
   Other Services: Ping (select)

2. **Port Mode**

   Configuration > Port Mode: Select Trust-Untrust in the Port Mode drop-down menu.

3. **HTTP Port**

   Configuration > Admin > Management: In the HTTP Port field, type 5555, then click **Apply**.

NOTE: The default port number is 80. Changing this to any number between 1024 and 32,767 is advised for discouraging unauthorized access to the configuration. When logging in to manage the device later, enter the following in the URL field of your browser: http://1.1.1.1:5555.

4. **Interfaces**

   Network > Interfaces > Edit (for trust): Enter the following, then click **OK**:

   Zone Name: V1-Trust
   IP Address/Netmask: 0.0.0.0/0

   Network > Interfaces > Edit (for untrust): Enter the following, then click **OK**:

   Zone Name: V1-Untrust
   IP Address/Netmask: 0.0.0.0/0

Network > Interfaces > Edit (for wireless1): Enter the following, then click **OK**:

Zone Name: V1-Trust
IP Address/Netmask: 0.0.0.0/0

Network > Interfaces > Edit (for wireless2): Enter the following, then click **OK**:

Zone Name: V1-Trust
IP Address/Netmask: 0.0.0.0/0

5. **Zones**

   The default virtual router for the V1-Trust, V1-Untrust, and VLAN zones is trust-vr.

6. **SSIDs**

   Wireless > SSID > New: Enter the following, then click **OK**:

   SSID: xparent-wpa

   > WPA Based Authentication Methods

   WPA Pre-shared Key: (select)
   Key by Password: (select), 12345678
   Confirm key by Password: 12345678
   Encryption Type: TKIP
   Wireless Interface Binding: wireless2

   Wireless > SSID > New: Enter the following, then click **OK**:

   SSID: xparent-share

   > WEP Based Authentication and Encryption Methods

   > WEP Key: Enter the following, then click **Back to SSID Edit**:

   Key ID:1
   Key Length: 40
   Key String
   ASCII: (select), abcde
   Default Key: (select)
   Add: (select)

   > WEP Based Authentication and Encryption Methods

   WEP Shared Key: (select)
   Wireless Interface Binding: wireless1

7. **Route**

   Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

   Network Address/Netmask: 0.0.0.0/0
   Gateway: (select)
   Interface: vlan1(trust-vr)
   Gateway IP Address: 1.1.1.250
   Metric: 1

8. **Policies**

   Policies > (From: V1-Trust, To: V1-Untrust) New: Enter the following and then click **OK**:

   ```
   Source Address:
       Address Book Entry: (select), Any
   Destination Address:
       Address Book Entry: (select), Any
   Service: Any
   Action: Permit
   ```

9. **WLAN Configuration Activation**

   Wireless > Activate Changes: Click the **Activate Changes** button.

CLI

1. **VLAN1**

   ```
   set interface vlan1 ip 1.1.1.1/24
   set interface vlan1 manage web
   set interface vlan1 manage telnet
   set interface vlan1 manage ping
   ```

2. **Port Modes**

   ```
   exec port-mode trust-untrust
   ```

3. **HTTP Port**

   ```
   set admin telnet port 4646
   ```

NOTE: The default port number for Telnet is 23. Changing this to any number between 1024 and 32,767 is advised for discouraging unauthorized access to the configuration. When logging in to manage the device later through Telnet, enter the following address: 1.1.1.1 4646.

4. **Interfaces**

   ```
   set interface trust ip 0.0.0.0/0
   set interface trust zone v1-trust
   set interface untrust ip 0.0.0.0/0
   set interface untrust zone v1-untrust
   set interface wireless1 ip 0.0.0.0/0
   set interface wireless1 zone v1-trust
   set interface wireless2 ip 0.0.0.0/0
   set interface wireless2 zone v1-trust
   ```

5. **Zones**

   ```
   set zone V1-Trust vrouter trust-vr
   set zone V1-Untrust vrouter trust-vr
   set zone VLAN vrouter trust-vr
   ```

6. **SSID**

```
set ssid name xparent-wpa
set ssid xparent-wpa authentication wpa-psk passphrase 12345678 encryption
    tkip
set ssid xparent-wpa interface wireless2
set ssid name xparent-share
set ssid xparent-share key-id 1 length 40 method asciitext abcde default
set ssid xparent-share authentication shared-key
set ssid xparent-share interface wireless1
exec wlan reactivate
```

7. **Route**

```
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 1.1.1.250 metric 1
```

8. **Policies**

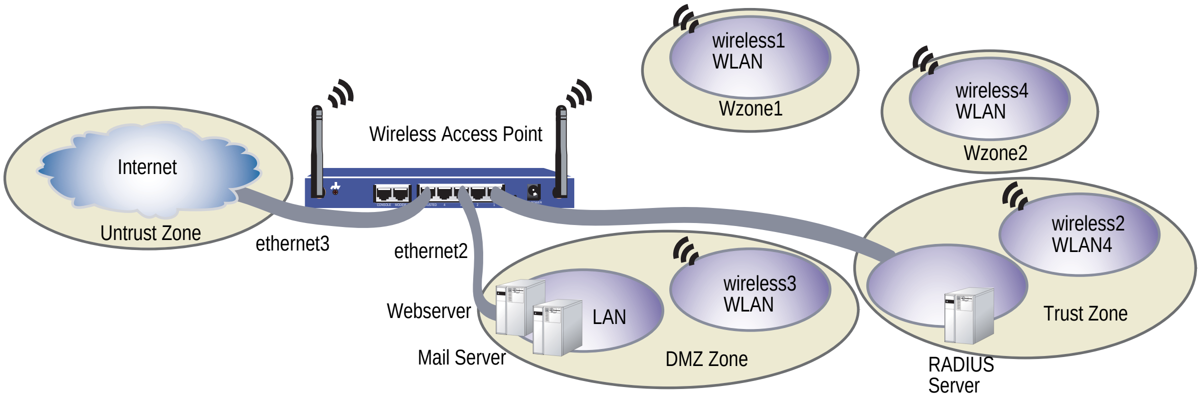
```
set policy from v1-trust to v1-untrust any any any permit
save
```

Example 4: Multiple and Differentiated Profiles

In this example, you create four SSIDs, each with a different name and authentication and encryption scheme for a wireless security device with one radio in Extended port mode. This mode provides the following port, interface, and zone bindings:

Interface	Security Zones	Basic Service Sets Names
ethernet1 (ports 1 and 2)	Trust	NA
ethernet2 (ports 3 and 4)	DMZ	NA
ethernet3 (Untrust port)	Untrust	NA
wireless1	Wzone1	SSID: wzone1-wpa with WPA preshared-key
wireless2	Trust	SSID: trust-wpa with WPA using RADIUS server
wireless3	DMZ	SSID: dmz-share with WEP shared key
wireless4	Wzone2	SSID: wzone2-open with WEP open/no encryption

Figure 23: Wireless with Multiple and Differentiated Profiles



In this example, you do the following:

1. Set your Basic Service Sets (BSS) by assigning SSID names, setting the encryption and authentication methods, and binding the SSID to a wireless interface.
2. Set each wireless interface to act as a DHCP server to assign addresses dynamically to the wireless clients for each SSID.
3. Enable wireless device management on the wireless1 interface.
4. Configure the wireless device to use a RADIUS server for WPA encryption.
5. Create policies for each wireless interface.
6. Reactivate the WLAN.

You can configure this example with either the WebUI or CLI:

WebUI

1. Setting the Basic Service Sets

Wireless > SSID > New: Enter the following, then click **OK**:

```
SSID: wzone1-wpa

> WPA Based Authentication Methods

WPA Pre-shared Key: (select)
    Key by Password: (select), 12345678
    Confirm key by Password: 12345678
    Encryption Type: Auto
Wireless Interface Binding: wireless1
```

Wireless > SSID > New: Enter the following, then click **OK**:

```
SSID: trust-wpa

> WPA Based Authentication Methods

    WPA: (select)
    Encryption Type: Auto
    Wireless Interface Binding: wireless2
```

Wireless > SSID > New: Enter the following, then click **OK**:

```
SSID: dmz-share

> WEP Based Authentication and Encryption Methods

    WEP Key: Enter the following, then click Back to SSID Edit:
    Key ID:1
    Key Length: 40
    Key String
      ASCII: (select), abcde
    Add: (select)
    WEP Shared Key: (select)
    Wireless Interface Binding: wireless3
```

Wireless > SSID > New: Enter the following, then click **OK**:

SSID: wzone2-open

> WEP Based Authentication and Encryption Methods

Open: (select)
No Encryption: (select)
Wireless Interface Binding: wireless4

2. **Interfaces**

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Obtain IP using DHCP: (select)
Automatic update DHCP server parameters: (select)

Network > Interfaces > Edit (for wireless1): Enter the following, then click **OK**:

IP Address/Netmask: 192.168.5.1/24

> Management Options

Management Services: WebUI, Telent, SSH, SNMP, SSL
Other Services: Ping

Network > DHCP > Edit (for wireless1) > DHCP Server: Enter the following, then click **OK**:

DHCP Server: (select)
DHCP Server Mode: Enable
Lease: Unlimited
DNS#1: 192.168.5.30

> Addresses > New: Enter the following, then click **OK**:

Dynamic: (select)
IP Address Start: 192.168.5.2
IP Address End: 192.168.5.22

NOTE: By default, device management is enabled for wireless2 with the default IP address of 192.168.2.1/24.

Network > DHCP > Edit (for wireless2) > DHCP Server: Enter the following, then click **OK**:

DHCP Server: (select)
DHCP Server Mode: Enable
Lease: Unlimited

> Addresses > New: Enter the following, then click **OK**:

Dynamic: (select)
IP Address Start: 192.168.2.2
IP Address End: 192.168.2.22

Network > Interfaces > Edit (for wireless3): Enter **192.168.3.1/24** in the IP Address/Netmask fields, then click **OK**.

Network > DHCP > Edit (for wireless3) > DHCP Server: Enter the following, then click **OK**:

DHCP Server: (select)
DHCP Server Mode: Enable
Lease: Unlimited

> Addresses > New: Enter the following, then click **OK**:

Dynamic: (select)
IP Address Start: 192.168.3.2
IP Address End: 192.168.3.22

Network > Interfaces > Edit (for wireless4): Enter **192.168.4.1/24** in the IP Address/Netmask fields, then click **OK**.

Network > DHCP > Edit (for wireless4) > DHCP Server: Enter the following, then click **OK**:

DHCP Server: (select)
DHCP Server Mode: Enable
Lease: Unlimited

> Addresses > New: Enter the following, then click **OK**:

Dynamic: (select)
IP Address Start: 192.168.4.2
IP Address End: 192.168.4.22

3. **RADIUS Auth Server**

Configuration > Auth > Servers > New: Enter the following, then click **OK**:

Name: radius1
IP/Domain Name: 192.168.1.50
Backup1: 192.168.1.60
Backup2: 192.168.1.61
Timeout: 30
Account Type: 802.1X
RADIUS: (select)
Shared Secret: 456htYY97kl

4. **Policies**

Policies > (From: Wzone1, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Any
Destination Address:
Address Book Entry: (select), Any
Service: ANY
Action: Permit

Policies > (From: Wzone1, To: DMZ) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Any
Destination Address:
Address Book Entry: (select), Any

Service: ANY
Action: Permit

Policies > (From: Wzone2, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
  Address Book Entry: (select), Any
Destination Address:
  Address Book Entry: (select), Any
Service: ANY
Action: Permit

Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

Source Address:
  Address Book Entry: (select), Any
Destination Address:
  Address Book Entry: (select), Any
Service: HTTP
Action: Permit

Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

Source Address:
  Address Book Entry: (select), Any
Destination Address:
  Address Book Entry: (select), Any
Service: MAIL
Action: Permit

5. **WLAN Configuration Activation**

   Wireless > Activate Changes: Click the **Activate Changes** button.

CLI

1. **Basic Service Sets**

```
set ssid name wzone1-wpa
set ssid wzone1-wpa authentication wpa-psk passphrase 12345678 encryption
    auto
set ssid wzone1-wpa interface wireless1

set ssid name trust-wpa
set ssid trust-wpa authentication wpa encryption auto
set ssid trust-wpa interface wireless2

set ssid name dmz-share
set ssid dmz-share key-id 1 length 40 method ascii abcde
set ssid dmz-share authentication shared-key
set ssid dmz-share interface wireless3

set ssid name wzone2-open
set ssid wzone2-open authentication open encryption none
set ssid wzone2-open interface wireless4
```

2. **Interfaces**

```
set interface ethernet3 dhcp client settings update-dhcp server
set interface ethernet3 dhcp client

set interface wireless1 ip 192.168.5.1/24
set interface wireless1 route
set interface wireless1 ip manageable
set interface wireless1 dhcp server service
set interface wireless1 dhcp server enable
set interface wireless1 dhcp server option gateway 192.168.5.1
set interface wireless1 dhcp server option netmask 255.255.255.0
set interface wireless1 dhcp server option dns1 192.168.5.30
set interface wireless1 dhcp server ip 192.168.5.2 to 192.168.5.22

set interface wireless2 dhcp server ip 192.168.2.2 to 192.168.2.22

set interface wireless3 ip 192.168.3.1/24
set interface wireless3 dhcp server ip 192.168.3.2 to 192.168.3.22

set interface wireless4 ip 192.168.4.1/24
set interface wireless4 dhcp server ip 192.168.4.2 to 192.168.4.22
```

3. **RADIUS Auth Server**

```
set auth-server radius1 server-name 192,168.1.50
set auth-server radius1 type radius
set auth-server radius1 account-type 802.1X
set auth-server radius1 backup1 192.168.1.60
set auth-server radius1 backup2 192. 168.1.61
set auth-server radius1 timeout 30
set auth-server radius1 radius secret A56htYY97kl
```

4. **Policies**

```
set policy from wzone1 to untrust any any any permit
set policy from wzone1 to dmz any any any permit
set policy from wzone2 to untrust any any any permit
set policy from untrust to dmz any any http permit
set policy from untrust to dmz any any mail permit
```

5. **WLAN Configuration Activation**

```
exec wlan reactivate
```

Appendix A

Wireless Information

This appendix lists information that might affect your deployment of a wireless LAN (WLAN). It contains the following sections:

- “Country Codes” on page A-I
- “802.11a Channel Numbers” on page A-IV
- “802.11b and 802.11g Channels” on page A-VI
- “Turbo-Mode Channel Numbers” on page A-VI

Country Codes

Table 7 lists the country names and country codes for wireless security devices with one radio. Table 8 lists the country names and country codes for wireless security devices with two radios.

NOTE: At this time, Argentina (AR), Brazil (BR), Czech Republic (CZ), and Ecuador (EC) are not supported for security devices with one radio.

Table 7: Country Codes for Wireless Security Devices with One Radio

Country	Code	Country	Code
NO_COUNTRY_SET	NA	Jordan	JO
Albania	AL	Kazakhstan	KZ
Algeria	DZ	North Korea	KP
Argentina	AR	Korea Republic2	K2
Armenia	AM	Kuwait	KW
Australia	AU	Latvia	LV
Austria	AT	Lebanon	LB
Azerbaijan	AZ	Liechtenstein	LI
Bahrain	BH	Lithuania	LT
Belarus	BY	Luxembourg	LU
Belgium	BE	Macao	MO
Belize	BZ	Macedonia	MK

Country	Code	Country	Code
Bolivia	BO	Malaysia	MY
Brazil	BR	Mexico	MX
Brunei Darussalam	BN	Monaco	MC
Bulgaria	BG	Morocco	MA
Canada	CA	Netherlands	NL
Chile	CL	New Zealand	NZ
Colombia	CO	Norway	NO
Costa Rica	CR	Oman	OM
Croatia	HR	Pakistan	PK
Cyprus	CY	Panama	PA
Czech Republic	CZ	Peru	PE
Denmark	DK	Philippines	PH
Dominican Republic	DO	Poland	PL
Ecuador	EC	Portugal	PT
Egypt	EG	Puerto Rico	PR
El Salvador	SV	Qatar	QA
Estonia	EE	Romania	RO
Finland	FI	Russia	RU
France	FR	Saudi Arabia	SA
France_Res	F2	Slovak Republic	SK
Georgia	GE	Slovenia	SI
Germany	DE	South Africa	ZA
Greece	GR	Spain	ES
Guatemala	GT	Sweden	SE
Honduras	HN	Switzerland	CH
Hong Kong	HK	Syria	SY
Hungary	HU	Thailand	TH
Iceland	IS	Trinidad & Tobago	TT
India	IN	Tunisia	TN
Indonesia	ID	Turkey	TR
Iran	IR	Ukraine	UA
Ireland	IE	United Arab Emirates	AE
Israel	IL	United Kingdom	GB
Italy	IT	United States	US
Japan	JP	Uruguay	UY

Country	Code	Country	Code
Japan1	J1	Uzbekistan	UZ
Japan2	J2	Venezuela	VE
Japan3	J3	Vietnam	VN
Japan4	J4	Yemen	YE
Japan5	J5	Zimbabwe	ZW

Table 8: Country Codes for Wireless Security Devices with Two Radios

Country	Code	Country	Code
NO_COUNTRY_SET	NA	Luxembourg	LU
Argentina	AR	Malta	MT
Australia	AU	Mexico	MX
Austria	AT	Monaco	MC
Belgium	BE	Netherlands	NL
Bulgaria	BG	New Zealand	NZ
Chile	CL	Norway	NO
Colombia	CO	Panama	PA
Cyprus	CY	Peru	PE
Czech Republic	CZ	Philippines	PH
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Saudi Arabia	SA
France	FR	Slovak Republic	SK
Germany	DE	Slovenia	SI
Greece	GR	South Africa	ZA
Hong Kong	HK	Spain	ES
Hungary	HU	Sweden	SE
Iceland	IS	Switzerland	CH
India	IN	Thailand	TH
Ireland	IE	Turkey	TR
Italy	IT	Ukraine	UA
Jordan	JO	United Kingdom	GB
Latvia	LV	United States	US
Liechtenstein	LI	Venezuela	VE
Lithuania	LT		

802.11a Channel Numbers

This section applies only to security devices with two radios.

The regulatory domains are as follows:

- Telecom Engineering Center (TELEC)—Japan
- Federal Communications Commission (FCC)—US
- European Telecommunications Standards Institute (ETSI)—Europe
- WORLD—All countries

Table 9 lists the countries and channel numbers for 802.11a.

Table 9: 802.11a Channel Numbers

Country	Country Code	Regulatory Domain	Channel
Argentina	AR	WORLD	56, 60, 64, 149, 153, 157, 161
Australia	AU	WORLD	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
Austria	AT	ETSI	36, 40, 44, 48
Belgium	BE	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Bulgaria	BG	ETSI	36, 40, 44, 48, 52, 56, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Canada	CA	FCC	36, 40, 44, 48, 52, 56, 60, 64
Chile	CL	WORLD	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
Colombia	CO	WORLD	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
Cyprus	CY	ETSI	36, 40, 44, 48, 52, 56, 60, 64
Czech Republic	CZ	ETSI	36, 40, 44, 48, 52, 56, 60, 64
Denmark	DK	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Estonia	EE	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Finland	FI	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
France	FR	ETSI	36, 40, 44, 48, 52, 56, 60, 64
Germany	DE	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Greece	GR	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Hong Kong	HK	WORLD	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
Hungary	HU	ETSI	36, 40, 44, 48, 52, 56, 60, 64
Iceland	IS	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
India	IN	WORLD	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
Ireland	IE	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140

Country	Country Code	Regulatory Domain	Channel
Italy	IT	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Japan	JP	TELEC	36, 40, 44, 48, 52, 56, 60, 64
Latvia	LV	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Liechtenstein	LI	ETSI	36, 40, 44, 48, 52, 56, 60, 64
Lithuania	LT	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Luxembourg	LU	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Malta	MT	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Mexico	MX	WORLD	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
Monaco	MC	ETSI	36, 40, 44, 48, 52, 56, 60, 64
Netherlands	NL	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
New Zealand	NZ	WORLD	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
Norway	NO	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Panama	PA	WORLD	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
Peru	PE	WORLD	149, 153, 157, 161, 165
Philippines	PH	WORLD	149, 153, 157, 161, 165
Poland	PL	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Portugal	PT	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Saudi Arabia	SA	WORLD	Not available
Slovak Republic	SK	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Slovenia	SI	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
South Africa	ZA	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Spain	ES	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Sweden	SE	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
Switzerland	CH	ETSI	36, 40, 44, 48, 52, 56, 60, 64
Thailand	TH	WORLD	Not available
Turkey	TR	WORLD	36, 40, 44, 48, 52, 56, 60, 64
Ukraine	UA	WORLD	Not available
United Kingdom	GB	ETSI	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140

Country	Country Code	Regulatory Domain	Channel
United States	US	FCC	36, 40, 44, 48, 52, 56, 60, 64
Venezuela	VE	WORLD	149, 153, 157, 161

802.11b and 802.11g Channels

All supported countries listed in Table 7 and Table 8, except for the following list, support channels 1 through 13 for 802.11b and 802.11g. The listed countries support channels 1 through 11 for 802.11b and 802.11g.

- Canada
- Colombia
- Dominican Republic
- Guatemala
- Mexico
- Panama
- Puerto Rico
- United States
- Uzbekistan

Turbo-Mode Channel Numbers

Table 10 lists the channels for 802.11a Turbo and 802.11g Turbo modes. The 802.11a Turbo column applies only to wireless security devices with two radios. The 802.11g Turbo column applies to security devices with one or two radios.

Table 10: Channels for 802.11a Turbo and 802.11g Turbo Modes

Country	Country Code	802.11a Turbo	802.11g Turbo
Albania	AL	Not available	6
Algeria	DZ	Not available	6
Argentina	AR	Not available	Not available
Armenia	AM	Not available	6
Australia	AU	42. 50. 58. 152. 160	6
Austria	AT	Not available	6
Azerbaijan	AZ	Not available	6
Bahrain	BH	Not available	6
Belarus	BY	Not available	6
Belgium	BE	Not available	6
Belize	BZ	Not available	6

Country	Country Code	802.11a Turbo	802.11g Turbo
Bolivia	BO	Not available	6
Brazil	BR	Not available	6
Brunei Darussalam	BN	Not available	6
Bulgaria	BG	Not available	6
Canada	CA	42, 50, 58	6
Chile	CL	42, 50, 58, 152, 160	Not available
Colombia	CO	Not available	6
Costa Rica	CR	Not available	6
Croatia	HR	Not available	6
Cyprus	CY	Not available	6
Czech Republic	CZ	Not available	6
Denmark	DK	Not available	6
Dominican Republic	DO	Not available	6
Ecuador	EC	Not available	6
Egypt	EG	Not available	6
El Salvador	SV	Not available	6
Estonia	EE	Not available	6
Finland	FI	Not available	6
France	FR	Not available	6
France_Res	F2	Not available	6
Georgia	GE	Not available	6
Germany	DE	Not available	6
Greece	GR	Not available	6
Guatemala	GT	Not available	6
Honduras	HN	Not available	6
Hong Kong	HK	42, 50, 58, 152, 160	6
Hungary	HU	Not available	6
Iceland	IS	Not available	6
India	IN	Not available	6
Indonesia	ID	Not available	6
Iran	IR	Not available	6
Ireland	IE	Not available	6
Israel	IL	Not available	6
Italy	IT	Not available	6
Japan	JP	Not available	Not available
Japan1	J1	Not available	Not available
Japan2	J2	Not available	Not available
Japan3	J3	Not available	Not available
Japan4	J4	Not available	Not available

Country	Country Code	802.11a Turbo	802.11g Turbo
Japan5	J5	Not available	Not available
Jordan	JO	Not available	6
Kazakhstan	KZ	Not available	6
North Korea	KP	Not available	6
Korea Republic2	K2	Not available	6
Kuwait	KW	Not available	6
Latvia	LV	Not available	6
Lebanon	LB	Not available	6
Liechtenstein	LI	Not available	6
Lithuania	LT	Not available	6
Luxembourg	LU	Not available	6
Macao	MO	Not available	6
Macedonia	MK	Not available	6
Malaysia	MY	Not available	6
Malta	MT	Not available	6
Mexico	MX	42, 50, 58, 152, 160	6
Monaco	MC	Not available	6
Morocco	MA	Not available	6
Netherlands	NL	Not available	6
New Zealand	NZ	Not available	6
Norway	NO	Not available	6
Oman	OM	Not available	6
Pakistan	PK	Not available	6
Panama	PA	42, 50, 58, 152, 160	6
Peru	PE	Not available	6
Philippines	PH	Not available	6
Poland	PL	Not available	6
Portugal	PT	Not available	6
Puerto Rico	PR	Not available	6
Qatar	QA	Not available	6
Romania	RO	Not available	6
Russia	RU	Not available	6
Saudi Arabia	SA	Not available	6
Slovak Republic	SK	Not available	6
Slovenia	SI	Not available	6
South Africa	ZA	Not available	6
Spain	ES	Not available	6
Sweden	SE	Not available	6
Switzerland	CH	Not available	6

Country	Country Code	802.11a Turbo	802.11g Turbo
Syria	SY	Not available	6
Thailand	TH	Not available	6
Trinidad & Tobago	TT	Not available	6
Tunisia	TN	Not available	6
Turkey	TR	Not available	6
Ukraine	UA	Not available	6
United Arab Emirates	AE	Not available	6
United Kingdom	GB	Not available	6
United States	US	42, 50, 58	6
Uruguay	UY	Not available	6
Uzbekistan	UZ	Not available	6
Venezuela	VE	Not available	6
Vietnam	VN	Not available	6
Yemen	YE	Not available	6
Zimbabwe	ZW	Not available	6

Index