



Configuring Router Interfaces



Note

From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

This chapter contains the following topics:

- [Basic Interface Settings on Cisco IOS Routers, page 62-1](#)
- [Router Interfaces Page, page 62-7](#)
- [Advanced Interface Settings on Cisco IOS Routers, page 62-13](#)
- [Advanced Interface Settings Page, page 62-16](#)
- [IPS Module Interface Settings on Cisco IOS Routers, page 62-22](#)
- [IPS Module Interface Settings Page, page 62-23](#)
- [CEF Interface Settings on Cisco IOS Routers, page 62-25](#)
- [CEF Interface Settings Page, page 62-26](#)
- [Dialer Interfaces on Cisco IOS Routers, page 62-28](#)
- [Dialer Policy Page, page 62-31](#)
- [ADSL on Cisco IOS Routers, page 62-34](#)
- [ADSL Policy Page, page 62-37](#)
- [SHDSL on Cisco IOS Routers, page 62-41](#)
- [SHDSL Policy Page, page 62-42](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)
- [PVC Policy Page, page 62-55](#)
- [PPP on Cisco IOS Routers, page 62-71](#)
- [PPP/MLP Policy Page, page 62-76](#)

Basic Interface Settings on Cisco IOS Routers



Note

From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

You typically add interfaces to Security Manager by performing discovery, as described in [Discovering Policies, page 5-12](#). After you have discovered the interfaces, you can modify the properties of each interface.

You can also use Security Manager to configure physical and virtual interfaces manually. This is useful when you modify interface configurations of existing devices, and makes it possible for you to configure all the interfaces of a device before you physically add the device to the network.

Related Topics

- [Available Interface Types, page 62-2](#)
- [Defining Basic Router Interface Settings, page 62-4](#)
- [Deleting a Cisco IOS Router Interface, page 62-6](#)

Available Interface Types

[Table 62-1 on page 62-2](#) describes the types of interfaces that can be configured on Cisco IOS routers.

Table 62-1 Router Interface Types

Type	Description
Null	Null interface.
Analysis-module	A Fast Ethernet interface that connects to the internal interface on the Network Analysis Module (NAM). Note You cannot configure parameters such as speed and duplex mode for this type of interface.
Async	Port line used as an asynchronous interface.
ATM	ATM interface.
BRI	ISDN BRI interface. This interface configuration propagates to each B channel. B channels cannot be configured individually. Note You must configure a dialer interface policy for calls to be placed on a BRI interface. For more information, see Dialer Interfaces on Cisco IOS Routers, page 62-28 .
BVI	Bridge-group virtual interface. BVI interfaces are used to route traffic at Layer 3 to the interfaces in a bridge group.
Content-engine	Content engine (CE) network module interface. Note You cannot configure parameters such as speed and duplex mode for this type of interface. You cannot create subinterfaces for this type of interface.
Dialer	Dialer interface.
Ethernet	Ethernet IEEE 802.3 interface.
Fast Ethernet	100-Mbps Ethernet interface.
FDDI	Fiber Distributed Data Interface.
Gigabit Ethernet	1000-Mbps Ethernet interface.

Table 62-1 Router Interface Types (continued)

Type	Description
Group-Async	Main asynchronous interface. This interface type creates a single asynchronous interfaces to which other interfaces are associated. This one-to-many configuration enables you to configure all associated member interfaces by configuring the main interface.
HSSI	High-Speed Serial Interface.
Loopback	A logical interface that emulates an interface that is always up. For example, having a loopback interface on the router prevents a loss of adjacency with neighboring OSPF routers if the physical interfaces on the router go down. The name of a loopback interface must end with a number ranging from 0-2147483647. Note This interface type is supported on all platforms. You can create an unlimited number of loopback interfaces.
Multilink	Multilink interface. A logical interface used for multilink PPP (MLP).
Port channel	Port channel interface. This interface type enables you to bundle multiple point-to-point Fast Ethernet links into one logical link. It provides bidirectional bandwidth of up to 800 Mbps.
POS	Packet OC-3 interface on the Packet-over-SONET (POS) interface processor.
PRI	ISDN PRI interface. Includes 23/30 B-channels and one D-channel.
Serial	Serial interface.
Switch	Switch interface.
Ten Gigabit Ethernet	10000-Mbps Ethernet interface.
Token Ring	Token Ring interface.
Tunnel	Tunnel interface. Note You can create an unlimited number of virtual, tunnel interfaces. Valid values range from 0-2147483647.
VG-AnyLAN	100VG-AnyLAN port adapter.
VLAN	Virtual LAN subinterface.
Virtual Template	Virtual template interface. When a user dials in, a predefined configuration template is used to configure a virtual access interface; when the user is done, the virtual access interface goes down and the resources are freed for other dial-in uses.

Related Topics

- [Defining Basic Router Interface Settings, page 62-4](#)
- [Deleting a Cisco IOS Router Interface, page 62-6](#)
- [Basic Interface Settings on Cisco IOS Routers, page 62-1](#)

Defining Basic Router Interface Settings

When you define an interface or subinterface for a Cisco IOS router, you name it, specify how it is assigned an IP address, and optionally define other properties, such as the speed, maximum transmission unit (MTU), and the encapsulation type.



Note

Basic interface settings are always local to the device on which they are configured. You cannot share this policy with other devices. You can, however, share advanced interface settings. For more information, see [Advanced Interface Settings on Cisco IOS Routers, page 62-13](#).

Related Topics

- [Deleting a Cisco IOS Router Interface, page 62-6](#)

-
- Step 1** In Device view, select **Interfaces > Interfaces** from the Policy selector. The [Router Interfaces Page, page 62-7](#) is displayed.
- Step 2** To add a new interface or subinterface, click the Add Row button to open the Create Router Interface dialog box.
- To edit an existing interface or subinterface, select it in the Interfaces table, and then click the Edit Row button to open the Edit Router Interface dialog box. Refer to [Create Router Interface Dialog Box, page 62-8](#) for descriptions of the fields in these dialog boxes.
- Step 3** Select **Enabled** to have Security Manager actively manage this interface or subinterface. If this option is deselected, the interface/subinterface definition is retained, but the interface/subinterface itself is disabled (or “shutdown”).
- Step 4** Choose **Interface** or **Subinterface** from the Type list.
- Step 5** If you are creating an interface, enter a name for the interface. You can click **Select** to open a dialog box that will help you generate a standard name based on interface type and details about the interface’s location, such as card, slot, and subinterface. For more information on using the dialog box to generate an interface name, see [Interface Auto Name Generator Dialog Box, page 62-12](#).



Note

When naming a BVI interface, use the bridge group number as the card number. Deployment will fail if you configure a BVI interface without configuring a corresponding bridge group.

- Step 6** If you are creating a subinterface, provide the following:
- Parent**—Choose the parent interface for this subinterface.
 - Subinterface ID**—Enter a number to identify the subinterface.



Note

Security Manager configures serial subinterfaces as point-to-point, not multipoint.

- Step 7** To specify a **Layer Type**, choose a Level 2 (data link) or Level 3 (network) option from this list.
- Step 8** Choose a method of **IP** address assignment for this interface/subinterface, then provide additional information, as required:
- **Static IP**—Provide an **IP Address** and **Subnet Mask**.
 - **DHCP**—No additional information is required.

- **PPPoE**—No additional information is required.
- **Unnumbered**—Provide the name of the interface from which an IP address is to be “borrowed.”



Note Layer 2 interfaces do not support IP addresses.

Step 9 Define additional properties of the interface/subinterface:

- Use the **Negotiation** check box to enable and disable auto-negotiation for the interface.

Auto-negotiation detects the capabilities of remote devices and negotiates the best possible performance between the two devices. When Negotiation is enabled, the Fast Ethernet Duplex and Speed options are disabled.



Note Auto-negotiation is available only for Fast Ethernet and Gigabit Ethernet interfaces on ASR devices.

- Choose a transmission mode from the **Duplex** list. If you choose Auto, be sure the network device to which this interface is connected is set to automatically detect the transmission mode. (Auto is not available on ASRs; use auto-negotiation instead.)



Note You must configure a fixed speed to define the duplex value. Tunnel and loopback interfaces do not support this setting.

- Choose a transmission speed from the **Speed** list. If you choose Auto, be sure the network device to which this interface is connected is set to automatically detect the transmission speed. (Auto is not available on ASRs; use auto-negotiation instead.)
- Enter the maximum transmission unit (**MTU**), which defines the largest packet size, in bytes, that this interface can support.



Note Certain interface properties are set automatically, or are unavailable, depending on the interface type and the underlying port type. For example, the Speed options are available for Fast Ethernet and Gigabit Ethernet interfaces only.

Step 10 Choose an encapsulation method from the **Encapsulation** list:

- **None**—No encapsulation; no additional parameters are required.
- (Ethernet subinterfaces only) **DOT1Q**—VLAN encapsulation, as defined by the IEEE 802.1Q standard. Provide the following VLAN parameters for this subinterface:
 - Enter a VLAN ID to associate with this subinterface.



Note All VLAN IDs must be unique among all subinterfaces configured on the same physical interface.

- If you are defining the 802.1Q trunk interface, select Native VLAN.

**Tip**

To configure DOT1Q encapsulation on an Ethernet interface without associating a VLAN with the subinterface, enter the **vlan-id dot1q** command using CLI commands or FlexConfigs. See [Understanding FlexConfig Policies and Policy Objects, page 7-2](#). Configuring VLANs on the main interface increases the number of VLANs that can be configured on the router.

- (Serial interfaces only) **Frame Relay**—IETF Frame Relay encapsulation. Provide a data-link connection identifier (DLCI) for the subinterface.

**Note**

Frame relay must be configured on the parent interface.

**Note**

IETF Frame Relay encapsulation provides interoperability between a Cisco IOS router and equipment from other vendors. To configure Cisco Frame Relay encapsulation, use CLI commands or FlexConfigs.

Step 11 (Optional) Enter a description of up to 1024 characters for the interface.

Step 12 Click **OK** to save the interface/subinterface definition and close the dialog box. The new interface is displayed on the Router Interfaces page. Subinterfaces are displayed beneath the parent interface.

Deleting a Cisco IOS Router Interface

Although you can delete the definition of a virtual interface at any time, use this option with great care. If the interface is included in any policy definitions that exist for this router, deleting the interface causes these policy definitions to fail when they are deployed to the device.

**Note**

Deleting the basic interface definition does not delete any advanced settings that are configured under **Interface > Settings > Advanced Settings**. You must delete these advanced settings separately. If you fail to do so, deployment fails.

**Note**

Deleting the definition of a physical interface from the Router Interfaces page does not remove the interface from the device. If you perform this operation by mistake, you can perform rediscovery to restore the definition to Security Manager. For more information, see [Discovering Policies on Devices Already in Security Manager, page 5-15](#).

Related Topics

- [Defining Basic Router Interface Settings, page 62-4](#)
- [Basic Interface Settings on Cisco IOS Routers, page 62-1](#)

Step 1 Click the **Device View** button on the toolbar.

Step 2 Select a router from the Device selector.

- Step 3** Select **Interfaces > Interfaces** from the Policy selector. The Router Interfaces page is displayed. See [Table 62-2 on page 62-7](#) for an explanation of the fields on this page.
- Step 4** Select an interface from the table, then click the **Delete** button. The interface is deleted.

Router Interfaces Page

Use the Router Interfaces page to view, create, edit, and delete interface definitions (physical and virtual) on a selected Cisco IOS router. The Router Interfaces page displays interfaces that were discovered by Security Manager as well as interfaces added manually after you added the device to the system.



Note

Unlike other router policies, the Interfaces policy cannot be shared among multiple devices. The Advanced Settings policy, however, may be shared. See [Local Policies vs. Shared Policies, page 5-3](#).

For more information, see [Basic Interface Settings on Cisco IOS Routers, page 62-1](#).

Navigation Path

Select a Cisco IOS router from the Device selector, then select **Interfaces > Interfaces** from the Policy selector.

Related Topics

- [Available Interface Types, page 62-2](#)
- [Deleting a Cisco IOS Router Interface, page 62-6](#)
- [Table Columns and Column Heading Features, page 1-49](#)
- [Filtering Tables, page 1-48](#)

Field Reference

Table 62-2 Router Interfaces Page

Element	Description
Interface Type	The interface type. Subinterfaces are displayed indented beneath their parent interface.
Interface Name	The name of the interface.
Enabled	Indicates whether the interface is currently enabled (managed by Security Manager) or disabled (shutdown state).
IP Address	The IP address of interfaces defined with a static address.
IP Address Type	The type of IP address assigned to the interface—static, DHCP, PPPoE, or unnumbered. (IP address is defined by a selected interface role.)
Interface Role	The interface roles that are assigned to the selected interface.
Add button	Opens the Create Router Interface Dialog Box, page 62-8 . From here you can create an interface on the selected router.
Edit button	Opens the Create Router Interface Dialog Box, page 62-8 . From here you can edit the selected interface.

Table 62-2 Router Interfaces Page (continued)

Element	Description
Delete button	Deletes the selected interfaces from the table. Ensure that the interface is not being used in any other policy before deleting it.

Create Router Interface Dialog Box

Use the Create Router Interface dialog box to create and edit physical and virtual interfaces on the selected Cisco IOS router.



Tip

Interface configuration is specific to the type of device. Many of the options on this page might be greyed out for specific device or interface types because they do not apply or they are not configurable.

Navigation Path

Go to the [Router Interfaces Page, page 62-7](#), then click the **Add** or **Edit** button beneath the table.

Related Topics

- [Basic Interface Settings on Cisco IOS Routers, page 62-1](#)
- [Deleting a Cisco IOS Router Interface, page 62-6](#)
- [Advanced Interface Settings Page, page 62-16](#)

Field Reference

Table 62-3 Create Router Interface Dialog Box

Element	Description
Enabled	Whether the interface is enabled (no shutdown). If you deselect this option, the interface is created in the configuration but it is shut down.
Type	Specifies whether you are defining an interface or subinterface.
Name	Applies only to interfaces. The name of the interface. Enter a name manually, or click Select to display a dialog box for generating a name automatically. See Interface Auto Name Generator Dialog Box, page 62-12 . Logical interfaces require a number after the name: <ul style="list-style-type: none"> • The range for dialer interfaces is 0-799. • The range for loopback interfaces is 0-2147483647. • The range for BVI interfaces is 1-255. • The only allowed value for null interfaces is 0.
Parent	Applies only to subinterfaces. The parent interface of the subinterface. Choose the parent interface from this list.

Table 62-3 Create Router Interface Dialog Box (continued)

Element	Description
Subinterface ID	<p>Applies only to subinterfaces.</p> <p>The ID number of the subinterface.</p>
IP	<p>The method of IP address assignment for the interface:</p> <ul style="list-style-type: none"> • Static IP—Defines a static IP address and subnet mask for the interface. Enter this information in the fields that appear below the option. <p>Note You can define the mask using either dotted decimal (for example, 255.255.255.255) or CIDR notation (/32). See Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-81.</p> <ul style="list-style-type: none"> • DHCP—The interface obtains its IP address dynamically from a DHCP server. • PPPoE—The router automatically negotiates its own registered IP address from a central server (via PPP/PCP). The following interface types support PPPoE: <ul style="list-style-type: none"> – Async – Serial – High-Speed Serial Interface (HSSI) – Dialer – BRI, PRI (ISDN) – Virtual template – Multilink • Unnumbered—The interface obtains its IP address from a different interface on the device. Choose an interface from the Interface list. This option can be used with point-to-point interfaces only. <p>Note Layer 2 interfaces do not support IP addresses. Deployment fails if you define an IP address on a Layer 2 interface.</p>
Layer Type	<p>The OSI layer at which the interface is defined:</p> <ul style="list-style-type: none"> • Unknown—The layer is unknown. • Layer 2—The data link layer, which contains the protocols that control the physical layer (Layer 1) and how data is framed before being transmitted on the medium. Layer 2 is used for bridging and switching. Layer 2 interfaces do not have IP addresses. • Layer 3—The network layer, which is primarily responsible for the routing of data in packets across logical internetwork paths. This routing is accomplished through the use of IP addresses.

Table 62-3 Create Router Interface Dialog Box (continued)

Element	Description
Negotiation	<p>Available on ASRs; applies to Fast Ethernet and Gigabit Ethernet interfaces only.</p> <p>Auto-negotiation detects the capabilities of remote devices and negotiates the best possible performance between the two devices. When Negotiation is enabled, the Duplex and Speed options are disabled.</p>
Duplex	<p>The interface transmission mode:</p> <ul style="list-style-type: none"> • None—The transmission mode is returned to its device-specific default setting. • Full—The interface transmits and receives at the same time (full duplex). • Half—The interface can transmit or receive, but not at the same time (half duplex). This is the default. • Auto—The router automatically detects and sets the appropriate transmission mode, either full or half duplex. Not available on ASRs; use auto-negotiation instead. <p>Note When using Auto mode, be sure that the port on the active network device to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, select the appropriate fixed mode.</p> <p>Note You can configure a duplex value only if you set the Speed to a fixed speed, not Auto.</p> <p>Note This setting does not apply to serial, HSSI, ATM, PRI, DSL, tunnel, or loopback interfaces.</p>
Speed	<p>Applies only to Fast Ethernet and Gigabit Ethernet interfaces.</p> <p>The speed of the interface:</p> <ul style="list-style-type: none"> • None—The setting is not configurable on the device. • 10—10 megabits per second (10Base-T networks). • 100—100 megabits per second (100Base-T networks). This is the default for Fast Ethernet interfaces. • 1000—1000 megabits per second (Gigabit Ethernet networks). This is the default for Gigabit Ethernet interfaces. • Auto—The router automatically detects and sets appropriate interface speed. Not available on ASRs; use auto-negotiation. <p>Note When using Auto mode, be sure that the port on the active network device to which you connect this interface is also set to automatically negotiate the transmission speed. Otherwise, select the appropriate fixed speed.</p>

Table 62-3 Create Router Interface Dialog Box (continued)

Element	Description
MTU	<p>The maximum transmission unit, which refers to the maximum packet size, in bytes, that this interface can handle.</p> <p>Valid values for serial, Ethernet, and Fast Ethernet interfaces range from 64 to 17940 bytes.</p> <p>Valid values for Gigabit Ethernet interfaces range from 1500 to 9216 bytes.</p>
Encapsulation	<p>The type of encapsulation performed by the interface:</p> <ul style="list-style-type: none"> • None—No encapsulation. • DOT1Q—VLAN encapsulation, as defined by the IEEE 802.1Q standard. Applies only to Ethernet subinterfaces. • Frame Relay—IETF Frame Relay encapsulation. Applies only to serial interfaces (not serial subinterfaces). <p>Note IETF Frame Relay encapsulation provides interoperability between a Cisco IOS router and equipment from other vendors. To configure Cisco Frame Relay encapsulation, use CLI commands or FlexConfigs.</p>
VLAN ID	<p>Applies only to subinterfaces with encapsulation type DOT1Q.</p> <p>The VLAN ID associated with this subinterface. The VLAN ID specifies where 802.1Q tagged packets are sent and received on this subinterface; without a VLAN ID, the subinterface cannot send or receive traffic. Valid values range from 1 to 4094.</p> <p>Note All VLAN IDs must be unique among all subinterfaces configured on the same physical interface.</p> <p>Tip To configure DOT1Q encapsulation on an Ethernet interface without associating the VLAN with a subinterface, enter the vlan-id dot1q command using CLI commands or FlexConfigs. See Understanding FlexConfig Policies and Policy Objects, page 7-2. Configuring VLANs on the main interface increases the number of VLANs that can be configured on the router.</p>

Table 62-3 Create Router Interface Dialog Box (continued)

Element	Description
Native VLAN	<p>Applies only when the encapsulation type is DOT1Q and you are configuring a physical interface that is meant to serve as an 802.1Q trunk interface. Trunking is a way to carry traffic from several VLANs over a point-to-point link between two devices.</p> <p>When selected, the Native VLAN is associated with this interface, using the ID specified in the VLAN ID field. (If no VLAN ID is specified for the Native VLAN, the default is 1.) The native VLAN is the VLAN to which all untagged VLAN packets are logically assigned by default. This includes the management traffic associated with the VLAN. If no VLAN ID is defined, the default is 1.</p> <p>For example, if the VLAN ID of this interface is 1, all incoming untagged packets and packets with VLAN ID 1 are received on the main interface and not on a subinterface. Packets sent from the main interface are transmitted without an 802.1Q tag.</p> <p>When deselected, the Native VLAN is not associated with this interface.</p> <p>Note The Native VLAN cannot be configured on a subinterface of the trunk interface. Be sure to configure the same Native VLAN value at both ends of the link; otherwise, traffic may be lost or sent to the wrong VLAN.</p>
DLCI	<p>Applies only to serial subinterfaces with Frame Relay encapsulation.</p> <p>Enter the data-link connection identifier to associate with the subinterface. Valid values range from 16 to 1007.</p> <p>Note Security Manager configures serial subinterfaces as point-to-point not multipoint.</p>
Description	Additional information about the interface (up to 1024 characters).
Roles	The interface roles assigned to this interface. A message is displayed if no roles have yet been assigned.

Interface Auto Name Generator Dialog Box

Use the Interface Auto Name Generator dialog box to have Security Manager generate a name for the interface based on the interface type and its location in the router or switch.

Navigation Path

Go to the [Create Router Interface Dialog Box, page 62-8](#), select **Interface** from the Type list, then click **Select** in the Name field.

Field Reference

Table 62-4 Interface Auto Name Generator Dialog Box

Element	Description
Type	The type of interface. Your selection from this list forms the first part of the generated name, as displayed in the Result field. For more information, see Available Interface Types, page 62-2 .
Card	The card related to the interface. Note When defining a BVI interface, enter the number of the corresponding bridge group.
Slot	The slot related to the interface.
Port	The port related to the interface. Note The information you enter in these fields forms the remainder of the generated name, as displayed in the Result field.
Result	The name generated by Security Manager from the information you entered for the interface type and location. The name displayed in this field is read-only. Tip After closing this dialog box, you can edit the generated name in the Create Router Interface dialog box, if required.

Advanced Interface Settings on Cisco IOS Routers

In addition to the basic interface definitions that you can define on the Interfaces page, Security Manager provides a method for defining selected advanced settings on interfaces that support those settings.

Unlike the basic interface settings defined on the Interface page, you can share an advanced settings policy with multiple devices. This provides a convenient method for configuring multiple devices with identical settings. See [Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-37](#).

You can define a variety of advanced settings on a selected interface, subinterface, or interface role, including:

- Cisco Discovery Protocol (CDP) settings.
- Internet Control Message Protocol (ICMP) settings.
- Directed broadcast settings.
- Load interval for determining the average load.
- Throughput delay for use by routing protocols.
- Configuring TCP maximum segment size.
- Helper addresses for forwarding UDP broadcasts. For more information on helper addresses, see [Understanding Helper Addresses, page 62-14](#).
- Enabling Maintenance Operation Protocol (MOP).
- Enabling virtual fragmentation reassembly (VFR).
- Enabling proxy ARP.
- Enabling NBAR protocol discovery.

- Enabling and configuring unicast reverse path forwarding (RFP).

**Tip**

You can define these settings for multiple interfaces on a device at once by choosing an interface role instead of a specific interface. For example, if you have defined an All-Ethernets interface role, you can define identical advanced settings for every Ethernet interface on the device with a single definition. See [Understanding Interface Role Objects, page 6-73](#).

Before You Begin

- Define basic interface settings. See [Basic Interface Settings on Cisco IOS Routers, page 62-1](#).

Step 1

Do one of the following:

- (Device view) Select **Interfaces > Settings > Advanced Settings** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > Advanced Settings** from the Policy Type selector. Select an existing policy or create a new one.

The Advanced Interface Settings page is displayed (see [Advanced Interface Settings Page, page 62-16](#)).

Step 2

Do one of the following:

- Click the **Add** button to add an interface or interface role to the table. In the Advanced Interface Settings dialog box, enter the name of the interface or interface role, or click **Select** to select an existing role or to create a new role.
- Select an existing entry in the table and click the **Edit** button to change its settings.

Step 3

Configure the advanced settings required for the selected interface. For details about each setting, see [Advanced Interface Settings Dialog Box, page 62-16](#).

Step 4

Click **OK** to save your definitions. Your definitions are displayed in the Advanced Interface Settings table.

Understanding Helper Addresses

Network hosts occasionally use User Datagram Protocol (UDP) broadcasts to determine address, configuration, and name information. This presents a problem if the host is on a network segment that does not include the required server, as by default, routers do not forward UDP broadcasts beyond their subnet. You can remedy this situation by configuring the interface to forward certain classes of broadcasts to a helper address.

One common use of helper addresses is when the router acts as a relay agent for DHCP clients who need to contact a DHCP server located on a different subnet. The helper address can either represent a specific DHCP server or a network address for a segment containing multiple DHCP servers. You can also configure a helper address for each DHCP server.

In [Figure 62-1](#), hosts located on network 192.168.1.0 can use 10.44.23.7 as a helper address to forward UDP broadcasts to the other network, while hosts located on network 10.44.0.0 can use 192.168.1.19 as their helper address.

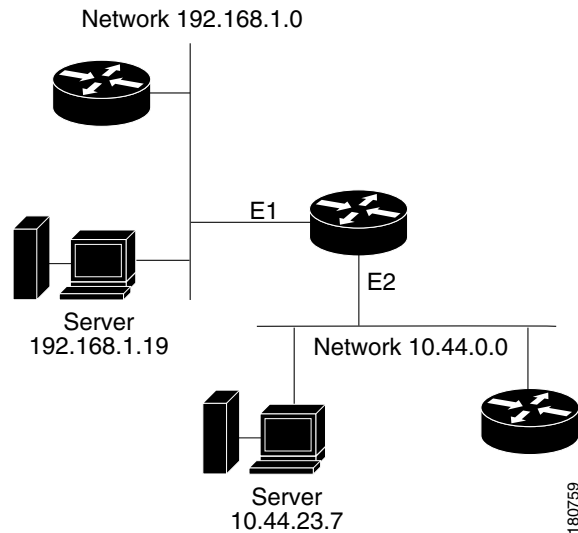
Figure 62-1 *Helper Addresses*

Table 62-5 on page 62-15 lists the default UDP services that can be forwarded to helper addresses.

Table 62-5 *Default UDP Services Forwarded to Helper Addresses*

Service	Port
BOOTP/DHCP Client	68
BOOTP/DHCP Server	67
DNS	53
NetBIOS datagram service	138
NetBIOS name service	137
TACACS	49
TFTP	69
Time	37

**Tip**

To forward additional UDP services, use the CLI or FlexConfigs to configure the `ip forward-protocol` command. Use the `no` form of this command to prevent the forwarding of any of the default services listed in Table 62-5 on page 62-15.

All of the following conditions must be met in order for a UDP or IP packet to use helper addresses:

- The MAC address of the received frame must be an all-ones broadcast address (ffff.ffff.ffff).
- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface, or major-net broadcast for the receiving interface if the `no ip classless` command is also configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).

Related Topics

- [Advanced Interface Settings on Cisco IOS Routers, page 62-13](#)
- [Basic Interface Settings on Cisco IOS Routers, page 62-1](#)

Advanced Interface Settings Page

Use the Advanced Interface Settings page to configure advanced interface definitions (physical and virtual) on a router. Examples of advanced settings include Cisco Discovery Protocol (CDP) settings, ICMP message settings, and virtual fragment reassembly settings. You can configure settings for specific interfaces or for interface roles. The columns in the table summarize the advanced settings for an entry and are explained in [Advanced Interface Settings Dialog Box, page 62-16](#).

To configure advanced settings:

- Click the **Add** button to add an interface or interface role to the table, and fill in the Advanced Interface Settings dialog box.
- Select an entry and click the **Edit** button to edit an existing entry.
- Select an entry and click the **Delete** button to delete it.

For more information, see [Advanced Interface Settings on Cisco IOS Routers, page 62-13](#).

Navigation Path

- (Device view) Select **Interfaces > Settings > Advanced Settings** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > Advanced Settings** from the Policy Type selector. Right-click **Advanced Settings** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- [Router Interfaces Page, page 62-7](#)
- [Available Interface Types, page 62-2](#)
- [Deleting a Cisco IOS Router Interface, page 62-6](#)
- [Table Columns and Column Heading Features, page 1-49](#)
- [Filtering Tables, page 1-48](#)

Advanced Interface Settings Dialog Box

Use the Advanced Interface Settings dialog box to define a variety of advanced settings on a selected interface as described in the table below.

Navigation Path

Go to the [Advanced Interface Settings Page, page 62-16](#), then click the **Add** or **Edit** button beneath the table.

Related Topics

- [Basic Interface Settings on Cisco IOS Routers, page 62-1](#)
- [Advanced Interface Settings on Cisco IOS Routers, page 62-13](#)

- [Deleting a Cisco IOS Router Interface, page 62-6](#)
- [Available Interface Types, page 62-2](#)

Field Reference

Table 62-6 *Advanced Interface Settings Dialog Box*

Element	Description
Interface	<p>The interface on which the advanced settings are defined. Enter the name of an interface or interface role, or click Select to select it. If the you want is not listed, click the Create button to create it.</p> <p>Note The only advanced settings supported on Layer 2 interfaces are Max. Bandwidth, Load Interval, and CDP.</p>
Max Bandwidth	<p>The bandwidth value to communicate to higher-level protocols in kilobits per second (kbps). The value you define in this field is an informational parameter only; it does not affect the physical interface.</p>
Load Interval	<p>The length of time, in seconds, used to calculate the average load on the interface. Valid values range from 30 to 600 seconds, in multiples of 30 seconds. The default is 300 seconds (5 minutes). Load interval is not supported on subinterfaces.</p> <p>Modify the default to shorten the length of time over which load averages are computed. You can do this if you want load computations to be more reactive to short bursts of traffic.</p> <p>Load data is gathered every 5 seconds. This data is used to compute load statistics, including input/output rate in bits and packets per second, load, and reliability. Load data is computed using a weighted-average calculation in which recent load data has more weight in the computation than older load data.</p> <p>Tip You can use this option to increase or decrease the likelihood of activating a backup interface; for example, a backup dial interface may be triggered by a sudden spike in the load on an active interface.</p>
TCP Maximum Segment Size	<p>The maximum segment size (MSS) of TCP SYN packets that pass through this interface. Valid values range from 500 to 1460 bytes. If you do not specify a value, the MSS is determined by the originating host.</p> <p>This option helps prevent TCP sessions from being dropped as they pass through the router. Use this option when the ICMP messages that perform auto-negotiation of TCP frame size are blocked (for example, by a firewall). We highly recommend using this option on the tunnel interfaces of DMVPN networks.</p> <p>For more information, see <i>TCP MSS Adjustment</i> at this URL: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t4/feature/guide/ft_a_dmss.html</p> <p>Note Typically, the optimum MSS is 1452 bytes. This value plus the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte packet that matches the MTU size for the Ethernet link.</p>

Table 62-6 Advanced Interface Settings Dialog Box (continued)

Element	Description
Helper Addresses	<p>The helper addresses that are used to forward User Datagram Protocol (UDP) broadcasts that are received on this interface. Enter one or more addresses or the names of the network/host objects, or click Select to select an object from a list or to create a new object.</p> <p>By default, routers do not forward broadcasts outside of their subnet. Helper addresses provide a solution by enabling the router to forward certain types of UDP broadcasts as a unicast to an address on the destination subnet. For more information, see Understanding Helper Addresses, page 62-14.</p>
Interface Throughput Delay	<p>The expected delay for the interface in tens of microseconds (for example, 3000 translates to 30,000 microseconds). You can enter a value between 1 and 16777215, and the default varies by the type of interface.</p> <p>Higher-level protocols might use delay information to make operating decisions. For example, IGRP can use delay information to differentiate between a satellite link and a land link. This setting is for informational purposes only and does not affect the actual delay on the interface.</p>
Cisco Discovery Protocol settings	<p>Settings related to the Cisco Discovery Protocol (CDP). CDP is a media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment including routers, access servers, bridges, and switches. It is primarily used to obtain protocol addresses of neighboring devices and to discover the platform of those devices. The options are:</p> <ul style="list-style-type: none"> • Enable CDP—Whether to enable the Cisco Discovery Protocol (CDP) on this interface. You cannot enable CDP on ATM interfaces. • Log CDP Messages—On Ethernet interfaces, whether to log duplex mismatches for this interface.
ICMP Messages Settings	
Enable Redirect Messages	<p>Whether to enable the sending of Internet Control Message Protocol (ICMP) redirect messages if the device is forced to resend a packet through the same interface on which it was received to another device on the same subnet. Redirect messages are sent when the device wants to instruct the originator of the packet to remove it from the route and substitute a different device that offers a more direct path to the destination.</p>


Table 62-6 *Advanced Interface Settings Dialog Box (continued)*

Element	Description
Enable Unreachable Messages	<p>Whether to enable the sending of ICMP unreachable messages. Unreachable messages are sent in two circumstances:</p> <ul style="list-style-type: none"> • If the interface receives a nonbroadcast packet destined for itself that uses an unknown protocol, the interface sends an ICMP unreachable message to the source. • If the device receives a packet that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it sends an ICMP host unreachable message to the originator of the packet. <p>Note This is the only advanced setting supported by the null0 interface.</p>
Enable Mask Reply Messages	Whether to enable the sending of ICMP mask reply messages. Mask reply messages are sent in response to mask request messages, which are sent when a device needs to know the subnet mask for a particular subnetwork.
Additional Settings	
Enable Maintenance Operation Protocol (MOP)	Whether to enable MOP on the interface. You can use MOP for utility services such as uploading and downloading system software, remote testing, and problem diagnosis.
Enable Virtual Fragment Reassembly (VFR)	<p>Whether to enable virtual fragmentation reassembly (VFR) on this interface. VFR is a feature that enables the Cisco IOS Firewall to create dynamic ACLs that can protect the network from various fragmentation attacks. For more information, see <i>Virtual Fragmentation Reassembly</i> at this URL:</p> <p>http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_virt_frag_reasm_ps6441_TSD_Products_Configuration_Guide_Chapter.html</p>
Enable Proxy ARP	Whether to enable proxy Address Resolution Protocol (ARP) on the interface. Proxy ARP, defined in RFC 1027, is the technique in which one host, usually a router, answers ARP requests intended for another machine, thereby accepting responsibility for routing packets to the real destination. Proxy ARP can help machines on a subnet reach remote subnets without configuring routing or a default gateway.
Enable NBAR Protocol Discovery	<p>Whether to enable network-based application recognition (NBAR) on this interface to discover traffic and keep traffic statistics for all protocols known to NBAR. Protocol discovery provides a method to discover application protocols traversing an interface so that QoS policies can be developed and applied to them. For more information, go to:</p> <p>http://www.cisco.com/en/US/products/ps6616/products_qanda_item09186a00800a3ded.shtml</p>

Table 62-6 Advanced Interface Settings Dialog Box (continued)

Element	Description
Enable Directed Broadcasts ACL	<p>Whether to have directed broadcast packets “exploded” as a link-layer broadcast when this interface is directly connected to the destination subnet. When deselected, directed broadcast packets that are intended for the subnet to which this interface is directly connected are dropped rather than being broadcast. This is the default.</p> <p>An IP directed broadcast is an IP packet whose destination address is a valid broadcast address on a different subnet from the node on which it originated. In such cases, the packet is forwarded as if it was a unicast packet until it reaches its destination subnet.</p> <p>This option affects only the final transmission of the directed broadcast on its destination subnet; it does not affect the transit unicast routing of IP directed broadcasts.</p> <p>If you enable directed broadcasts, you can apply an ACL to determine which directed broadcasts are permitted to be broadcast on the destination subnet. All other directed broadcasts destined for the subnet to which this interface is directly connected are dropped. Enter the name of a standard or extended ACL object, or click Select to select an object from a list or to create a new object.</p> <p>Tip Because directed broadcasts, and particularly ICMP directed broadcasts, have been abused by malicious persons, we recommend deselecting this option on interfaces where directed broadcasts are not needed. When you enable directed broadcasts, apply an ACL to restrict their use.</p>
Unicast Reverse Path Forwarding (RFP) Settings	
Enable Unicast RFP	<p>Whether to enable unicast reverse path forwarding (RFP) on the interface. When you enable Unicast RFP on an interface, the router examines all packets that are received on that interface. The router checks to make sure that the source address appears in the FIB, and takes action based on your unicast RFP settings. Use unicast RFP to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks based on source IP address spoofing. For more information on unicast RFP, see the description of the ip verify unicast source reachable-via command in the <i>Cisco IOS Interface and Hardware Component Command Reference</i>.</p> <p>To enable unicast RFP, you must also globally enable Cisco Express Forwarding (CEF). For more information on CEF, see CEF Interface Settings on Cisco IOS Routers, page 62-25.</p>

Table 62-6 Advanced Interface Settings Dialog Box (continued)

Element	Description
Mode	<p>How strict to make unicast RFP:</p> <ul style="list-style-type: none"> • Loose Mode—The default. Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet if the source is reachable through any interface on the router. <p>Use loose mode on interfaces where asymmetric paths allow packets from valid source networks (networks contained in the FIB). For example, routers that are in the core of an ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.</p> <ul style="list-style-type: none"> • Strict Mode—Examines incoming packets to determine whether the source address is in the FIB and permits the packet only if the source is reachable through the interface on which the packet was received. <p>Use strict mode on interfaces where only one path allows packets from valid source networks (networks contained in the FIB). Also, use strict mode when a router has multiple paths to a given network as long as the valid networks are switched through the incoming interfaces. Packets for invalid networks are dropped. For example, routers at the edge of the network of an ISP are likely to have symmetrical reverse paths. Strict mode is also applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.</p>
Allow Use Of Default Route for RFP Verification	Whether to permit Unicast RFP to successfully match on prefixes that are known through the default route when determining whether to pass packets. Normally, sources found in the FIB but only by way of the default route are dropped.
Allow Self Ping	<p>Whether to allow the router to ping its own interfaces. By default, when you enable Unicast RFP, packets that are generated by the router and destined to the router are dropped, thereby making certain troubleshooting and management tasks difficult to accomplish.</p> <p> Caution Allowing self-ping opens a potential denial of service (DoS) hole.</p>
ACL (For Unicast RFP)	If you enable unicast RFP, you can apply an ACL to refine how packets are handled when a reverse path is not found. If you specify an ACL, when (and only when) a packet fails the Unicast RFP check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Enter the name of a standard or extended ACL object, or click Select to select an object from a list or to create a new object.

IPS Module Interface Settings on Cisco IOS Routers



Note

From version 4.17, though Cisco Security Manager continues to support IPS and IOS features/functionality, it does not support any bug fixes or enhancements.

On some routers, you can install IPS modules such as the Cisco Intrusion Prevention System Advanced Integration Module or Network Module. When installed and active, you must configure the IPS Module interface settings policy to define the following:

- The name of the interface between the module and the router.
- The failure mode of the module. If the module fails, you can configure it to allow all traffic or to deny all traffic.
- The router interfaces to monitor. You can name specific interfaces or use interface roles to cover more than one interface at a time. For example, if you have defined an All-Ethernets interface role, you can define identical monitoring settings for every Ethernet interface on the device with a single definition. See [Understanding Interface Role Objects, page 6-73](#).



Tip

After you have defined an IPS Module interface settings policy, you can share the policy and assign it to other devices. This provides a convenient method for configuring multiple devices with identical settings. See [Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-37](#).

Before You Begin

Define basic interface settings. See [Basic Interface Settings on Cisco IOS Routers, page 62-1](#).

Step 1

Do one of the following:

- (Device view) Select **Interfaces > Settings > IPS Module** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > IPS Module** from the Policy Type selector. Select an existing policy or create a new one.

The IPS Module Interface Settings page is displayed. See [IPS Module Interface Settings Page, page 62-23](#) for an explanation of the fields on this page.

Step 2

In the IPS Module Interface Settings fields, enter the name of the IPS interface (such as IDS-Sensor1/0) or click Select to select it from a list. Also determine whether you want to allow all traffic if the module fails (fail open) or to deny all traffic (fail closed).

Step 3

Identify the router interfaces that the module should monitor. Click the **Add** button below the IPS Module Service Module Monitoring Settings table to add interfaces to the list, or select an interface and click the **Edit** button to change the settings for an existing interface. Use the IPS Monitoring Information dialog box to define the interface name or role, monitoring mode, and access list (if any). For more information, see [IPS Monitoring Information Dialog Box, page 62-24](#).

IPS Module Interface Settings Page



Note

From version 4.17, though Cisco Security Manager continues to support IPS features/functionality, it does not support any bug fixes or enhancements.

Use the IPS Module Interface Settings page to define the settings on the Cisco Intrusion Prevention System Advanced Integration Module or Network Module. The module must be running IPS 6.0 or later. You can define the fail mode for the IPS interface, and the interfaces that the module should monitor. Configure this policy only if the router hosts an IPS module.



Caution

Cisco IOS IPS and the Cisco IPS module cannot be used together. Cisco IOS IPS must be disabled when the IPS module is installed.

Navigation Path

- (Device view) Select **Interfaces > Settings > IPS Module** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > IPS Module** from the Policy Type selector. Create a new policy or select an existing policy from the Shared Policy selector.

Related Topics

- [IPS Module Interface Settings on Cisco IOS Routers, page 62-22](#)
- [Table Columns and Column Heading Features, page 1-49](#)
- [Filtering Tables, page 1-48](#)

Field Reference

Table 62-7 *IPS Module Interface Settings Page*

Element	Description
Interface Name	The name of the IPS module interface. Enter the name or click Select to select the interface or interface role. If the object that you want is not listed, click the Create button to create it.
Fail Over Mode	How the module should handle traffic inspection during a module failure, either to fail open (passing all traffic without inspection) or fail closed (dropping all traffic). The default is fail open.

Table 62-7 *IPS Module Interface Settings Page (continued)*

Element	Description
IPS Module Service Module Monitoring Settings table	<p>The list of interfaces on the router that the IPS module should monitor. The table shows the name of the interface or interface role, whether monitoring is inline or promiscuous, and whether an ACL is used to filter traffic for inspection on the interface. Inline mode puts the IPS module directly into the traffic flow, allowing it to stop attacks by dropping malicious traffic before it reaches the intended target. In promiscuous mode, packets do not flow through the sensor; the sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. If the ACL is matched, the matched traffic is not inspected.</p> <ul style="list-style-type: none"> To add an interface to the table, click the Add button and fill in the IPS Monitoring Information Dialog Box, page 62-24. To edit the settings for an interface, select it and click the Edit button. To delete an interface, select it and click the Delete button.

IPS Monitoring Information Dialog Box



Note

From version 4.17, though Cisco Security Manager continues to support IPS features/functionality, it does not support any bug fixes or enhancements.

Use the IPS Monitoring Information dialog box to add or edit the properties of interfaces to be monitored by the IPS module.

Navigation Path

Go to the [IPS Module Interface Settings Page, page 62-23](#), then click the **Add** or **Edit** button beneath the IPS Module Service Module Monitoring Settings table.

Related Topics

- [IPS Module Interface Settings on Cisco IOS Routers, page 62-22](#)
- [Basic Interface Settings on Cisco IOS Routers, page 62-1](#)

Field Reference

Table 62-8 *IPS Monitoring Information Dialog Box*

Element	Description
Interface Name	A name of the interface or interface role that the module should monitor. Enter the name or click Select to select the interface or interface role. If the object that you want is not listed, click the Create button to create it.

Table 62-8 IPS Monitoring Information Dialog Box (continued)

Element	Description
Monitoring Mode	How the interface should be monitored: <ul style="list-style-type: none"> • Inline mode—The IPS module is directly in the traffic flow, allowing it to stop attacks by dropping malicious traffic before it reaches the intended target. • Promiscuous mode—Packets do not flow through the sensor; the sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet.
Access List	The name of the standard or extended access list policy object to use to filter traffic on this interface for inspection, if you want to apply one. A matched ACL causes traffic not to be inspected for that ACL. Click Select to select the ACL or to create a new one.

CEF Interface Settings on Cisco IOS Routers

Cisco Express Forwarding (CEF) is an advanced Layer 3 IP switching technology that optimizes network performance and scalability for all kinds of networks, from those that carry small amounts of traffic to those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions. CEF is enabled by default on most Cisco IOS routers.

Typically, you do not need to configure a CEF policy unless you want to enable CEF accounting so that you can view statistics with the **show ip cef** command on the router. You would also configure the policy if you want to disable CEF, or to configure non-default CEF behavior on specific interfaces, for example, to have CEF load balance based on packets rather than source-destination packet streams.

When configuring alternate CEF settings for interfaces, you can name specific interfaces or use interface roles to cover more than one interface at a time. For example, if you have defined an All-Ethernets interface role, you can define identical CEF settings for every Ethernet interface on the device with a single definition. See [Understanding Interface Role Objects, page 6-73](#).



Tip

After you have defined a CEF interface settings policy, you can share the policy and assign it to other devices. This provides a convenient method for configuring multiple devices with identical settings. See [Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-37](#).

Before You Begin

Define basic interface settings. See [Basic Interface Settings on Cisco IOS Routers, page 62-1](#).

Step 1

Do one of the following:

- (Device view) Select **Interfaces > Settings > CEF** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > CEF** from the Policy Type selector. Select an existing policy or create a new one.

The CEF Interface Settings page is displayed. See [CEF Interface Settings Page, page 62-26](#) for an explanation of the fields on this page.

Step 2

If you are enabling CEF, select the accounting options you desire.

- Step 3** If you want to configure non-default behavior for certain interfaces, add them to the CEF Interface Settings table. Click the **Add** button below the table to add interfaces to the list, or select an interface and click the **Edit** button to change the settings for an existing interface. For more information about the options, see [CEF Interface Settings Dialog Box, page 62-27](#).
-

CEF Interface Settings Page

Use the CEF Interface Settings page to define the settings for Cisco Express Forwarding. CEF is an advanced Layer 3 IP switching technology that optimizes network performance and scalability for all kinds of networks, from those that carry small amounts of traffic to those that carry large amounts of traffic in complex patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions. CEF is enabled by default on most Cisco IOS routers.

Navigation Path

- (Device view) Select **Interfaces > Settings > CEF** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > CEF** from the Policy Type selector. Create a new policy or select an existing policy from the Shared Policy selector.

Related Topics

- [CEF Interface Settings on Cisco IOS Routers, page 62-25](#)
- [Table Columns and Column Heading Features, page 1-49](#)
- [Filtering Tables, page 1-48](#)

Field Reference

Table 62-9 CEF Interface Settings Page

Element	Description
Enable Cisco Express Forwarding	Whether to enable CEF globally on the device. The option is greyed out if you cannot disable CEF on the device. You can configure other settings on the page only if you enable CEF globally.

Table 62-9 CEF Interface Settings Page (continued)

Element	Description
CEF Network Accounting	<p>These options are for configuring CEF accounting globally. If you collect accounting statistics, you can view them using the show ip cef command on the router. You can select the following options to enable different types of accounting:</p> <ul style="list-style-type: none"> • Enable Accounting for Traffic Through Non-Recursive Prefixes—For network prefixes with directly connected next hops, non-recursive accounting enables express forwarding of the collection of packets through a prefix. • Enable Per-Prefix Accounting—Accounting statistics based on the packet's network prefix. • Enable Prefix Length Accounting—Accounting statistics based on the network prefix length. • Enable Load Balance Hash Accounting—When you use per-destination load balancing (the default), CEF uses a series of 16 hash buckets to distribute the available paths based on the source and destination addresses. Enabling load balance hash accounting provides per-hash-bucket counters.
CEF Interface Settings table	<p>The interfaces on the router for which you are defining special CEF configurations. When you enable CEF globally, by default, all interfaces on the router enable CEF and use per-destination load balancing. Add interfaces to this table only if you want to configure different behavior for the interfaces.</p> <p>The table shows the name of the interface or interface role, whether CEF is enabled or disabled, and whether the interface is load balancing based on destination or on a per-packet basis. For a detailed explanation of the fields, see CEF Interface Settings Dialog Box, page 62-27.</p> <ul style="list-style-type: none"> • To add an interface to the table, click the Add button. • To edit the settings for an interface, select it and click the Edit button. • To delete an interface, select it and click the Delete button.

CEF Interface Settings Dialog Box

Use the CEF Interface Settings dialog box to add or edit the CEF properties of interfaces when you want to configure something different than the global default.

Navigation Path

Go to the [CEF Interface Settings Page, page 62-26](#), then click the **Add** or **Edit** button beneath the CEF Interface Settings table.

Related Topics

- [CEF Interface Settings on Cisco IOS Routers, page 62-25](#)
- [Basic Interface Settings on Cisco IOS Routers, page 62-1](#)

Field Reference**Table 62-10 CEF Interface Settings Dialog Box**

Element	Description
Interface Name	The name of the interface or interface role for which you are configuring CEF. Enter the name or click Select to select the interface or interface role. If the object that you want is not listed, click the Create button to create it.
Enable CEF on Interface	Whether to enable CEF on the interface. CEF is enabled by default.
Load Balancing	How the interface should balance traffic, either per-destination or per-packet. In per-destination load balancing, all packets for a given source-destination pair take the same path. In per-packet load balancing, packets for a given source-destination pair can take different equal-cost routes, and thus reach their destination out of order. The default is to balance the load based on the destination of the traffic.

Dialer Interfaces on Cisco IOS Routers

Before you can configure a dial backup policy for a site-to-site VPN (see [Configuring Dial Backup, page 25-40](#)), you must configure a dialer interface policy on the appropriate Cisco IOS router. The dialer interface policy uses dialer pools to associate the dialer interface used by dial backup with a physical BRI interface on the router. Each dialer interface is associated with a single dialer pool, which can contain one or more physical interfaces. Multiple dialer interfaces can reference the same dialer pool.

The following topics describe how to create dialer interfaces policies on Cisco IOS routers:

- [Defining Dialer Profiles, page 62-28](#)
- [Defining BRI Interface Properties, page 62-30](#)

Defining Dialer Profiles

When you configure a dialer profile, you must select the interface or interface role representing the dialer interface and specify the number to be dialed. You must also assign a pool ID, which you use to reference this dialer interface when configuring the physical dialer interface. Additionally, you can modify the default timeout settings for the line.

**Note**

IP is the only protocol supported for dialer profiles by Security Manager.

**Note**

Authentication parameters for the dialer profile are defined in the PPP policy.

Before You Begin


Define the virtual and physical dialer interfaces on the router. See [Basic Interface Settings on Cisco IOS Routers, page 62-1](#).

**Note**

In addition, you can optionally define interface roles for the virtual and physical dialer interfaces. See [Defining Dialer Profiles, page 62-28](#).

Related Topics

- [Defining BRI Interface Properties, page 62-30](#)
- [Dialer Interfaces on Cisco IOS Routers, page 62-28](#)

-
- Step 1** Do one of the following:
- (Device view) Select **Interfaces > Settings > Dialer** from the Policy selector.
 - (Policy view) Select **Router Interfaces > Settings > Dialer** from the Policy Type selector. Select an existing policy or create a new one.
- The Dialer page is displayed. See [Table 62-11 on page 62-31](#) for a description of the fields on this page.
- Step 2** Select a dialer profile from the upper table on the Dialer Interfaces page, then click **Edit**, or click **Add** to create a profile. The Dialer Profile dialog box appears. See [Table 62-12 on page 62-32](#) for a description of the fields in this dialog box.
- Step 3** Enter the name of the interface or interface role that represents the virtual dialer interface, or click **Select** to select an interface role object or to create a new one. For more information, see [Specifying Interfaces During Policy Definition, page 6-76](#).
- Step 4** Enter a name for the dialer profile. Having a name makes it easier for you to assign the correct dialer pool to the physical interface. See [Defining BRI Interface Properties, page 62-30](#).
-  **Tip** We recommend that you define a name that is logically associated with the site to which the dialer interface serves as a backup. For example, if the dialer interface is serving as a backup connection to the London site, define the name London for the dialer profile.
-
- Step 5** Enter an ID number for the dialer pool to associate with this dialer interface. Each dialer interface is associated with a single pool. Multiple interfaces may, however, be associated with the same dialer pool.
- Step 6** Enter the number of the dialer group to assign to the dialer interface.
- Step 7** (Optional) In the Interesting Traffic ACL field, enter the name of the extended ACL object that defines which packets are permitted to initiate calls using this dialer profile, or click **Select** to select the object from a list or to create a new one. Use this option to limit the IP traffic that can make use of the dialer.
- Step 8** Enter the dialer string, which is the phone number of the remote side of the dialer interface connection.
- Step 9** (Optional) Modify the default timeout values (Idle Timeout and Fast Idle Timeout), if required.
- Step 10** Click **OK** to save your definitions locally on the client and close the dialog box. The dialer profile appears in the Dialer Profile table on the Dialer page.
-

Defining BRI Interface Properties

You configure the properties of the physical BRI interfaces used for dialer interface policies by selecting the appropriate interface or interface role, defining the dialer pools to which the interface belongs, and defining the ISDN switch type. It is the dialer pool that connects the physical interface with the virtual dialer interface.



Note

To define other types of physical dialer interfaces, such as ATM and Ethernet, use FlexConfigs. For more information, see [Understanding FlexConfig Policies and Policy Objects, page 7-2](#).

Before You Begin

Define the virtual and physical dialer interfaces on the router. See [Basic Interface Settings on Cisco IOS Routers, page 62-1](#).



Note

In addition, you can optionally define interface roles for the virtual and physical dialer interfaces. See [Creating Interface Role Objects, page 6-74](#).

Related Topics

- [Defining Dialer Profiles, page 62-28](#)
- [Dialer Interfaces on Cisco IOS Routers, page 62-28](#)

- Step 1** Do one of the following:
- (Device view) Select **Interfaces > Settings > Dialer** from the Policy selector.
 - (Policy view) Select **Router Interfaces > Settings > Dialer** from the Policy Type selector. Select an existing policy or create a new one.
- The Dialer Interfaces page is displayed. See [Table 62-11 on page 62-31](#) for a description of the fields on this page.
- Step 2** Select a physical BRI interface from the Dialer Physical Interfaces table, then click **Edit**, or click **Add** to add an interface. The Dialer Physical Interface dialog box appears. See [Table 62-13 on page 62-33](#) for a description of the fields in this dialog box.
- Step 3** Enter the name of the interface or interface role that represents the physical dialer interface, or click **Select** to select an interface role object from a list or to create a new one. For more information, see [Specifying Interfaces During Policy Definition, page 6-76](#).
- Step 4** Enter the names of the dialer pools to associate with the physical interface, or click **Select** to display a selector. Separate multiple entries with commas.
- Step 5** Select the ISDN switch type used by the physical interface. [Table 62-13 on page 62-33](#) describes the available switch types.
- Step 6** (Optional) If you selected the Basic-DMS-100, Basic-NI, or Basic-5ess switch type, enter up to two service provider identifiers (SPIDs).



Note

We recommend that you do not enter SPIDs for the Basic-5ess switch type, even though SPIDs are supported.

- Step 7** Click **OK** to save your definitions locally on the client and close the dialog box. The interface definition appears in the Dialer Physical Interfaces table on the Dialer Interface page.

Dialer Policy Page

Use the Dialer page to define the relationship between physical Basic Rate Interface (BRI) and virtual dialer interfaces. You use these dialer interfaces when you configure the dial backup feature for site-to-site VPNs.

For more information, see [Dialer Interfaces on Cisco IOS Routers, page 62-28](#).

Navigation Path

- (Device view) Select **Interfaces > Settings > Dialer** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > Dialer** from the Policy Type selector. Right-click **Dialer** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- [Configuring Dial Backup, page 25-40](#)
- [Table Columns and Column Heading Features, page 1-49](#)
- [Filtering Tables, page 1-48](#)

Field Reference

Table 62-11 *Dialer Page*

Element	Description
Dialer Profiles table	<p>The dialer profiles that define the dialer pools. You must add profiles before you can add physical BRI interfaces. The table shows the name of the interface or interface role that the dialer interface uses, the profile name, pool, group, the ACL that defines which traffic can use this profile, the dial string, and idle times.</p> <ul style="list-style-type: none"> • To add a profile, click the Add Row button and fill in the Dialer Profile Dialog Box, page 62-32. • To edit a profile, select it and click the Edit Row button. • To delete a profile, select it and click the Delete Row button.
Dialer Physical Interfaces (BRI) table	<p>The physical interfaces that use the dialer profiles. The table shows the name of the interface or interface role, the dial pools, ISDN switch type, and first and second service provider identifiers (SPID) related to the interface.</p> <ul style="list-style-type: none"> • To add an interface, click the Add Row button and fill in the Dialer Physical Interface Dialog Box, page 62-33. • To edit an interface, select it and click the Edit Row button. • To delete an interface, select it and click the Delete Row button.

Dialer Profile Dialog Box

Use the Dialer Profile dialog box to add or edit dialer profiles.

Navigation Path

Go to the [Dialer Policy Page, page 62-31](#), then click the **Add** or **Edit** button beneath the Dialer Profile table.

Related Topics

- [Dialer Physical Interface Dialog Box, page 62-33](#)
- [Defining Dialer Profiles, page 62-28](#)
- [Dialer Interfaces on Cisco IOS Routers, page 62-28](#)
- [Basic Interface Settings on Cisco IOS Routers, page 62-1](#)
- [Creating Interface Role Objects, page 6-74](#)

Field Reference

Table 62-12 *Dialer Profile Dialog Box*

Element	Description
Name	A descriptive name for the dialer profile. This name enables you to assign the correct dialer pool to the physical interface. You can also use the profile name as a reference to the site to which this dialer interface serves as a backup.
Interface	The virtual dialer interface to associate with the dialer profile. Enter the name of an interface or interface role, or click Select to select it. If the object that you want is not listed, click the Create button to create it.
Pool ID	The dialer pool ID. Each pool can contain multiple physical interfaces and can be associated with multiple dialer interfaces. Each dialer interface, however, is associated with only one pool.
Group	The group ID, which identifies the dialer group that this dialer interface uses.
Interesting Traffic ACL	The extended, numbered ACL that defines which packets are permitted to initiate calls using this dialer profile. The valid ACL number range is 100 to 199. Enter the name of the ACL object, or click Select to select it. If the object that you want is not listed, click the Create button to create it.
Dialer String (Remote Phone Number)	The phone number of the destination that the dialer contacts.
Idle Timeout	The default amount of idle time before an uncontested line is disconnected. The default is 120 seconds.
Fast Idle Timeout	The default amount of idle time before a contested line is disconnected. The default is 20 seconds. Line contention occurs when a busy line is requested to send another packet to a different destination.

Dialer Physical Interface Dialog Box

Use the Dialer Physical Interface dialog box to add or edit the properties that associate physical BRI interfaces with dialer interfaces.



Note

Use FlexConfigs to define other types of physical dialer interfaces, such as ATM and Ethernet. For more information, see [Understanding FlexConfig Policies and Policy Objects, page 7-2](#).

Navigation Path

Go to the [Dialer Policy Page, page 62-31](#), then click the **Add** or **Edit** button beneath the Dialer Physical Interfaces table.

Related Topics

- [Dialer Profile Dialog Box, page 62-32](#)
- [Defining BRI Interface Properties, page 62-30](#)
- [Dialer Interfaces on Cisco IOS Routers, page 62-28](#)
- [Basic Interface Settings on Cisco IOS Routers, page 62-1](#)
- [Understanding Interface Role Objects, page 6-73](#)

Field Reference

Table 62-13 *Dialer Physical Interface Dialog Box*

Element	Description
ISDN BRI	The physical BRI interface associated with the dialer interface. Enter the name of an interface or interface role object, or click Select to select it. If the object that you want is not listed, click the Create button to create it.
Pools	Associates dialer pools with a physical interface. Enter the names of one or more pools (as defined in the Dialer Profile Dialog Box, page 62-32), or click Select to display a selector. Use commas to separate multiple entries.

Table 62-13 *Dialer Physical Interface Dialog Box (continued)*

Element	Description
Switch Type	<p>The ISDN switch type.</p> <p>Options for North America are:</p> <ul style="list-style-type: none"> • basic-5ess—Lucent (AT&T) basic rate 5ESS switch • basic-dms100—Northern Telecom DMS-100 basic rate switch • basic-ni—National ISDN switches <p>Options for Australia, Europe, and the UK are:</p> <ul style="list-style-type: none"> • basic-1tr6—German 1TR6 ISDN switch • basic-net3—NET3 ISDN BRI for Norway NET3, Australia NET3, and New Zealand NET3 switch types; ETSI-compliant switch types for Euro-ISDN E-DSS1 signaling system • vn3—French VN3 and VN4 ISDN BRI switches <p>Option for Japan is:</p> <ul style="list-style-type: none"> • ntt—Japanese NTT ISDN switches <p>Option for Voice/PBX system is:</p> <ul style="list-style-type: none"> • basic-qsig—PINX (PBX) switches with QSIG signaling per Q.931 ()
SPID1	<p>Applies only when you select Basic-DMS-100, Basic-NI, or Basic-5ess as the switch type.</p> <p>The service provider identifier (SPID) for the ISDN service to which the interface subscribes. Some service providers in North America assign SPIDs to ISDN devices when you first subscribe to an ISDN service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid assigned SPID to the service provider when accessing the switch to initialize the connection.</p> <p>Valid SPIDs can contain up to 20 characters, including spaces and special characters.</p> <p>Note We recommend that you do not enter a SPID for interfaces using the AT&T 5ESS switch type, even though they are supported.</p>
SPID2	<p>Applies only when you select DMS-100 or NI as the switch type.</p> <p>The service provider identifier (SPID) for a second ISDN service to which the interface subscribes. Valid SPIDs can contain up to 20 alphanumeric characters (no spaces are permitted).</p>

ADSL on Cisco IOS Routers

Digital Subscriber Line (DSL) is a family of technologies that transports data over existing twisted-pair copper wire. DSL uses frequencies that are beyond the upper list used by POTS (plain old telephone service) to deliver broadband applications, such as multimedia and video, over the local loop (or *last mile*) that connects the telephone company's central office to customer sites.

Asymmetric Digital Subscriber Line (ADSL) is a form of DSL where the data flow downstream to customer sites is much greater than the data flow upstream to the central office (CO). This asymmetric setup is well-suited for applications where users typically download far more information than they send, such as web surfing, video-on-demand, and remote LAN access. With ADSL, the connection speed is related to the distance between the customer site and the digital subscriber line-access multiplexer (DSLAM) that aggregates the connections from multiple customer sites onto a high-speed line.

ADSL downstream rates range from 1.5 to 9 Mbps, whereas upstream bandwidth ranges from 16 to 640 kbps. ADSL transmissions work at distances up to 18,000 feet (5,488 meters) over a single copper twisted pair. Newer versions of ADSL technology, such as ADSL2 and ADSL2+, offer even higher data rates for short distances, as well as power management and realtime performance monitoring.

ATM is used in many ADSL implementations due to its small, fixed-length cell size, which makes it suitable for carrying time-critical traffic, such as voice and video, in conjunction with other traffic. You can use Security Manager to configure ATM over DSL on a Cisco IOS router. For more information about configuring ADSL policies in Security Manager, see [Defining ADSL Settings, page 62-36](#).

To configure ADSL in Security Manager, you must do the following:

1. Configure an ATM interface or subinterface. See [Defining Basic Router Interface Settings, page 62-4](#).
2. Configure ADSL settings on the ATM interface or subinterface. See [Defining ADSL Settings, page 62-36](#).
3. Configure PVCs on the ATM interface or subinterface. See [Defining ATM PVCs, page 62-51](#).


Note

If you perform discovery on the device, Security Manager populates the Interfaces policy with the ATM interface and subinterface and the ADSL policy with the ADSL settings for that interface. Any discovered PVCs are added to the PVC policy.

Related Topics

- [Supported ADSL Operating Modes, page 62-35](#)

Supported ADSL Operating Modes

[Table 62-14 on page 62-35](#) describes the operating modes that are supported on each ADSL interface card that can be configured with Security Manager.

Table 62-14 *ADSL Cards and Supported DSL Operating Modes*

ADSL Interface Card	Supported DSL Operating Modes
WIC-1ADSL	auto, ansi-dmt, itu-dmt, splitterless
WIC-1ADSL-I-DG	auto, etsi, itu-dmt
WIC-1ADSL-DG	auto, ansi-dmt, itu-dmt, splitterless
HWIC-1ADSL	auto, ansi-dmt, itu-dmt, adsl2, adsl2+
HWIC-1ADSLI	auto, etsi, itu-dmt, adsl2, adsl2+
HWIC-ADSL-B/ST	auto, ansi-dmt, itu-dmt, adsl2, adsl2+
HWIC-ADSLI-B/ST	auto, etsi, itu-dmt, adsl2, adsl2+

Table 62-15 on page 62-36 describes the operating modes that are supported on each ADSL device that can be configured with Security Manager.

Table 62-15 Fixed ADSL Devices and Supported DSL Operating Modes

Device	Supported DSL Operating Modes
857 Integrated Services Router	auto, ansi-dmt, itu-dmt, adsl2, adsl2+
876 Integrated Services Router	auto, etsi, itu-dmt, adsl2, adsl2+
877 Integrated Services Router	auto, ansi-dmt, itu-dmt, adsl2, adsl2+
1801 Integrated Services Router	auto, ansi-dmt, itu-dmt, adsl2, adsl2+
1802 Integrated Services Router	auto, etsi, itu-dmt, adsl2, adsl2+

Related Topics

- [Defining ADSL Settings, page 62-36](#)
- [ADSL on Cisco IOS Routers, page 62-34](#)

Defining ADSL Settings

When you configure an ADSL definition in Security Manager, you must select the ATM interface on which ADSL is being defined. In addition, we highly recommend that you specify the router type or the type of WIC (WAN interface card) installed in the router. The validity of DSL policy definitions is highly dependent on the hardware. By specifying the hardware used by this policy, you enable Security Manager to properly validate the values you define and avoid deployment failures.

You can optionally specify the following parameters:

- The DSL operating mode.
- Whether to enable dynamic VC bandwidth adjustments when using Inverse Multiplexing over ATM (IMA).
- Whether certain interface cards should use a particular set of carrier tones.

Modular Cisco IOS routers may contain multiple interface cards, each of which contains a single ATM interface. You may define only one ADSL definition per interface.

Before You Begin

- Make sure that the device contains an ADSL ATM interface. See [Basic Interface Settings on Cisco IOS Routers, page 62-1](#).

Related Topics

- [Supported ADSL Operating Modes, page 62-35](#)
- [ADSL on Cisco IOS Routers, page 62-34](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)

Step 1 Do one of the following:

- (Device view) Select **Interfaces > Settings > DSL > ADSL** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > DSL > ADSL** from the Policy Type selector. Select an existing policy or create a new one.

The ADSL page is displayed. See [Table 62-16 on page 62-38](#) for a description of the fields on this page.

- Step 2** Click the **Add** button beneath the table to display the ADSL Settings dialog box. See [Table 62-17 on page 62-39](#) for a description of the fields in this dialog box.
- Step 3** In the ATM Interface field, enter the name of the ATM interface or interface role on which you want to define ADSL settings, or click **Select** to select an interface role or create a new one. For more information, see [Specifying Interfaces During Policy Definition, page 6-76](#).



Note The interface that you select must be physically present on the device; otherwise, deployment fails.

- Step 4** (Optional) Select the interface card type installed on the router.



Note When discovering from a live device, the correct interface card type is already displayed. If you did not perform discovery on a live device, or if Security Manager cannot detect the type of interface card installed on the device, this field displays “Unknown”.

- Step 5** (Optional) When using IMA groups, select the **Allow bandwidth change on ATM PVCs** check box to enable dynamic adjustments to VC bandwidth in response to changes in group bandwidth. If this check box is left deselected, you must make these adjustments manually.

- Step 6** (Optional) Specify the DSL operating mode for this ATM interface. See [Table 62-14 on page 62-35](#) for a list of the operating modes supported for each card type.

- Step 7** (Optional) Select the **Use low tone set** check box to have the interface card use carrier tones 29 through 48.

- Step 8** Click **OK** to save your definitions locally on the client and close the dialog box. Your definitions are displayed in the ADSL table.



Note To edit an ADSL definition, select it from the table, then click **Edit**. To remove an ADSL definition, select it, then click **Delete**.

- Step 9** Repeat [Step 2](#) through [Step 8](#) to define ADSL settings on additional ATM interfaces. Only one ADSL definition may be defined on an interface.

ADSL Policy Page

Use the ADSL page to create, edit, and delete ADSL definitions on the ATM interfaces of the router. For more information, see [Defining ADSL Settings, page 62-36](#).

Navigation Path

- (Device view) Select **Interfaces > Settings > DSL > ADSL** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > DSL > ADSL** from the Policy Type selector. Right-click **ADSL** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- [PVC Policy Page, page 62-55](#)
- [SHDSL Policy Page, page 62-42](#)
- [ADSL on Cisco IOS Routers, page 62-34](#)
- [Table Columns and Column Heading Features, page 1-49](#)
- [Filtering Tables, page 1-48](#)

Field Reference**Table 62-16** *ADSL Page*

Element	Description
ATM Interface	The ATM interface on which ADSL settings are defined.
Interface Card	The type of device or ADSL interface card on which the ATM interface resides.
Bandwidth Change	Indicates whether the router makes dynamic adjustments to VC bandwidth as overall bandwidth changes. (This is relevant only when IMA groups are configured on the ATM interface.)
DSL Operating Mode	The DSL operating mode for this interface.
Tone Low	Indicates whether the interface is using the low tone set (carrier tones 29 through 48).
Add button	Opens the ADSL Settings Dialog Box, page 62-38 . From here you can define the ADSL settings for a selected ATM interface.
Edit button	Opens the ADSL Settings Dialog Box, page 62-38 . From here you can edit the selected ADSL definition.
Delete button	Deletes the selected ADSL definition from the table.

ADSL Settings Dialog Box

Use the ADSL Settings dialog box to configure ADSL settings on a selected ATM interface.

**Note**

When you configure ADSL settings, we highly recommend that you select the type of device or interface card on which the ATM interface is defined. ADSL settings are highly dependent on the hardware. Defining the hardware type in Security Manager enables proper validation of your configuration for a successful deployment to your devices.

Navigation Path

Go to the [ADSL Policy Page, page 62-37](#), then click the **Add** or **Edit** button beneath the table.

Related Topics

- [Defining ADSL Settings, page 62-36](#)
- [PVC Policy Page, page 62-55](#)

Field Reference

Table 62-17 ADSL Settings Dialog Box

Element	Description
ATM Interface	<p>The ATM interface on which ADSL settings are defined. Enter the name of an interface or interface role, or click Select to select it. If the object that you want is not listed, click the Create button to create it.</p> <p>Note We recommend that you do not define an interface role that includes ATM interfaces from different interface cards. The different settings supported by each card type may cause deployment to fail.</p> <p>Note You can create only one ADSL definition per interface.</p>
Interface Card	<p>The device type or the type of interface card installed on the router:</p> <ul style="list-style-type: none"> • [blank]—The interface card type is not defined. • WIC-1ADSL—A 1-port ADSL WAN interface card that provides ADSL over POTS (ordinary telephone lines). • WIC-1ADSL-I-DG—A 1-port ADSL WAN interface card that provides ADSL over ISDN with Dying Gasp support. (With Dying Gasp, the router warns the DSLAM of imminent line drops when the router is about to lose power.) • WIC-1ADSL-DG—A 1-port ADSL WAN interface card that provides ADSL over POTS with Dying Gasp support. • HWIC-1ADSL—A 1-port high-speed ADSL WAN interface card that provides ADSL over POTS. • HWIC-1ADSLI—A 1-port high-speed ADSL WAN interface card that provides ADSL over ISDN. • HWIC-ADSL-B/ST—A 2-port high-speed ADSL WAN interface card that provides ADSL over POTS with an ISDN BRI port for backup. • HWIC-ADSLI-B/ST—A 2-port high-speed ADSL WAN interface card that provides ADSL over ISDN with an ISDN BRI port for backup.

Table 62-17 ADSL Settings Dialog Box (continued)

Element	Description
Interface Card (continued)	<ul style="list-style-type: none"> 857 ADSL—Cisco 857 Integrated Service Router with an ADSL interface. 876 ADSL—Cisco 876 Integrated Services Router with an ADSL interface. 877 ADSL—Cisco 877 Integrated Services Router with an ADSL interface. 1801 ADSLoPOTS—Cisco 1801 Integrated Services Router that provides ADSL over POTS. 1802 ADSLoISDN—Cisco 1802 Integrated Services Router that provides ADSL over ISDN. <p>Note When discovering from a live device, the correct interface card type will already be displayed. If you did not perform discovery on a live device, or if Security Manager cannot detect the type of interface card installed on the device, this field displays “Unknown”.</p>
Allow bandwidth change on ATM PVCs	<p>When selected, the router makes dynamic adjustments to VC bandwidth in response to changes in the overall bandwidth of the Inverse Multiplexing over ATM (IMA) group defined on the ATM interface.</p> <p>When deselected, PVC bandwidth must be adjusted manually (using the CLI) whenever an individual physical link in the IMA group goes up or down.</p>
DSL Operating Mode	<p>The operating mode configured for this ADSL line:</p> <ul style="list-style-type: none"> auto—Performs automatic negotiation with the DSLAM located at the central office (CO). This is the default. ansi-dmt—The line trains in ANSI T1.413 Issue 2 mode. itu-dmt—The line trains in G.992.1 mode. splitterless—The line trains in G.992.2 (G.Lite) mode. etsi—The line trains in ETSI (European Telecommunications Standards Institute) mode. adsl2—The line trains in G.992.3 (adsl2) mode. adsl2+—The line trains in G.992.5 (adsl2+) mode. <p>Note See Table 62-14 on page 62-35 for a description of the operating modes that are supported by each card type.</p>
Use low tone set	<p>When selected, the interface card uses carrier tones 29 through 48.</p> <p>When deselected, the interface card uses carrier tones 33 through 56.</p> <p>Note Leave this option deselected when the interface card is operating in accordance with Deutsche Telekom specification U-R2.</p>

SHDSL on Cisco IOS Routers

Digital Subscriber Line (DSL) is a family of technologies that transports data over existing twisted-pair copper wire. DSL uses frequencies that are beyond the upper list used by POTS (plain old telephone service) to deliver broadband applications, such as multimedia and video, over the local loop (or *last mile*) that connects the telephone company's central office to customer sites.

Based on the International Telecommunications Union (ITU) G.991.2 global industry standard, symmetric high-speed digital subscriber line (SHDSL) delivers symmetrical data rates from 192 up to 2.3 Mbps on a single wire pair. It transports many types of signals, such as T1, E1, ISDN, ATM, and IP. In addition, the G.SHDSL signal has a greater distance reach from the central office than ADSL and proprietary SDSL connections.

To configure SHDSL in Security Manager, do the following:

1. Configure the SHDSL controller. See [Defining SHDSL Controllers, page 62-41](#).
2. Deploy the SHDSL policy. If ATM mode is activated, the router creates an ATM interface that corresponds to the controller upon deployment. See [Working with Deployment and the Configuration Archive, page 8-25](#).
3. Rediscover the device to add the new ATM interface to Security Manager. See [Discovering Policies on Devices Already in Security Manager, page 5-15](#).
4. (Optional) Create one or more subinterfaces on the ATM interface. See [Defining Basic Router Interface Settings, page 62-4](#).
5. Configure PVCs on the ATM interface or subinterface. See [Defining ATM PVCs, page 62-51](#).

**Note**

If you perform discovery on the device, Security Manager populates the SHDSL policy with the definition of the controller and the Interfaces policy with the ATM interface and subinterface. Any discovered PVCs are added to the PVC policy.

Related Topics

- [PVCs on Cisco IOS Routers, page 62-47](#)

Defining SHDSL Controllers

When you configure an SHDSL controller in Security Manager, you must enter the name of the controller that is installed in the Cisco IOS router. The following settings are then applied automatically:

- ATM mode is enabled.
- The line termination is set to CPE (customer premises equipment).
- The line mode is set to Auto.

You can optionally change the line termination to CO and specify the DSL mode and line mode. In addition, you can define signal-to-noise ratio margins to improve line stability.

A Cisco IOS router may contain multiple SHDSL controllers. You may define only one SHDSL definition per controller.

**Note**

When you deploy an SHDSL policy with ATM mode enabled, an ATM interface is created automatically on the router. Perform rediscovery to add the interface into Security Manager. You can then define PVCs on the ATM interface as required. See [Defining ATM PVCs, page 62-51](#).

Before You Begin

- Make sure that an SHDSL controller is installed on the device.

Related Topics

- [SHDSL on Cisco IOS Routers, page 62-41](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)

Step 1

Do one of the following:

- (Device view) Select **Interfaces > Settings > DSL > SHDSL** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > DSL > SHDSL** from the Policy Type selector. Select an existing policy or create a new one.

The SHDSL page is displayed. See [Table 62-18 on page 62-43](#) for a description of the fields on this page.

Step 2

Click the **Add** button beneath the table to display the SHDSL dialog box.

Step 3

Enter the name of the controller, or click **Select** to display the utility for generating the name. See [Controller Auto Name Generator Dialog Box, page 62-46](#).

**Note**

The controller that you select must be physically present on the device; otherwise, deployment fails.

Step 4

Define the SHDSL controller as required. For more information, see [Table 62-19 on page 62-44](#).

Step 5

Click **OK** to save your definitions locally on the client and close the dialog box. Your definitions are displayed in the SHDSL table.

**Note**

To edit an SHDSL controller, select it from the table, then click **Edit**. To remove an SHDSL controller, select it, then click **Delete**.

Step 6

Repeat [Step 2](#) through [Step 5](#) to define additional SHDSL controllers. Only one definition may be defined per controller.

SHDSL Policy Page

Use the SHDSL page to create, edit, and delete DSL controller definitions on the router. For more information, see [Defining SHDSL Controllers, page 62-41](#).

Navigation Path

- (Device view) Select **Interfaces > Settings > DSL > SHDSL** from the Policy selector.

- (Policy view) Select **Router Interfaces > Settings > DSL > SHDSL** from the Policy Type selector. Right-click **SHDSL** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- [PVC Policy Page, page 62-55](#)
- [ADSL Policy Page, page 62-37](#)
- [SHDSL on Cisco IOS Routers, page 62-41](#)
- [Table Columns and Column Heading Features, page 1-49](#)
- [Filtering Tables, page 1-48](#)

Field Reference

Table 62-18 *SHDSL Page*

Element	Description
Name	The name of the DSL controller.
Description	An optional description of the controller.
Shutdown	Indicates whether the DSL controller is in shutdown mode.
Configure ATM Mode	Indicates whether the DSL controller has been set into ATM mode.
Line Termination	The line termination set for the router (CPE or CO).
DSL Mode	The operating mode defined for the DSL controller.
Line Mode	The line mode defined for the DSL controller.
Line Rate	The line rate (in kbps) defined for the DSL controller. Note A value is displayed in this column only if the line mode is not set to Auto.
SNR Margin Current	The current signal-to-noise ratio on the controller.
SNR Margin Snext	The self near-end crosstalk (Snext) signal-to-noise ratio on the controller.
Add button	Opens the SHDSL Controller Dialog Box, page 62-43 . From here you can define the settings for a DSL controller.
Edit button	Opens the SHDSL Controller Dialog Box, page 62-43 . From here you can edit the selected DSL controller definition.
Delete button	Deletes the selected DSL controller definition from the table.

SHDSL Controller Dialog Box

Use the SHDSL Controller dialog box to configure SHDSL controllers.

Navigation Path

Go to the [SHDSL Policy Page, page 62-42](#), then click the **Add** or **Edit** button beneath the table.

Related Topics

- [Defining SHDSL Controllers, page 62-41](#)
- [PVC Policy Page, page 62-55](#)

- [Discovering Policies on Devices Already in Security Manager, page 5-15](#)

Field Reference

Table 62-19 SHDSL Dialog Box

Element	Description
Name	The name of the controller. Enter a name manually, or click Select to display a dialog box for generating a name. See Controller Auto Name Generator Dialog Box, page 62-46 .
Description	Additional information about the controller (up to 80 characters).
Shutdown	When selected, the DSL controller is in shutdown state. However, its definition is not deleted. When deselected, the DSL controller is enabled. This is the default.
Configure ATM mode	When selected, sets the controller into ATM mode and creates an ATM interface with the same ID as the controller. This is the default. You must enable ATM mode and then perform rediscovery to configure ATM or PVCs on the device. When deselected, ATM mode is disabled. No ATM interface is created on deployment. Note You cannot remove ATM mode from a controller after it has been saved in Security Manager.
Line Termination	The line termination that is set for the router: <ul style="list-style-type: none"> • CPE—Customer premises equipment. This is the default. • CO—Central office.
DSL Mode	The DSL operating mode, including regional operating parameters, used by the controller: <ul style="list-style-type: none"> • [blank]—The operating mode is not defined. (When deployed, the Annex A standard for North America is used.) • A—Supports Annex A of the G.991.2 standard for North America. • A-B—Supports Annex A or Annex B. Available only when the Line Term is set to CPE. The appropriate mode is selected when the line trains. • A-B-ANFP—Supports Annex A or Annex B-ANFP. Available only when the Line Term is set to CPE. The appropriate mode is selected when the line trains. • B—Supports Annex B of the G.991.2 standard for Europe. • B-ANFP—Supports Annex B-ANFP (Access Network Frequency Plan). Note The available DSL modes are dependent on the selected line termination.
Line Mode settings	

Table 62-19 SHDSL Dialog Box (continued)

Element	Description
Line Mode	<p>The line mode used by the controller:</p> <ul style="list-style-type: none"> • auto—The controller operates in the same mode as the other line termination (2-wire line 0, 2-wire line 1, or 4-wire enhanced). This is the default for CPE line termination. • 2-wire—The controller operates in two-wire mode. This is the default for CO line termination. • 4-wire—The controller operates in four-wire mode. <p>Note You can select Auto only when you configure the controller as the CPE.</p>
Line	<p>Applies only when the Line Mode is defined as 2-wire.</p> <p>The pair of wires to use:</p> <ul style="list-style-type: none"> • line-zero—RJ-11 pin 1 and pin 2. This is the default for CO line termination. • line-one—RJ-11 pin 3 and pin 4.
Exchange Handshake	<p>Applies only when the Line Mode is defined as 4-wire.</p> <p>The type of handshake mode to use:</p> <ul style="list-style-type: none"> • [blank]—The handshake mode is not specified. (When deployed, the enhanced option is used.) This is the default. • enhanced—Exchanges handshake status on both wire pairs. • standard—Exchanges handshake status on the main wire pair only.
Line Rate	<p>Does not apply when the Line Mode is defined as Auto.</p> <p>The DSL line rate (in kbps) available for the SHDSL port:</p> <ul style="list-style-type: none"> • auto—The controller selects the line rate. This is available only in 2-wire mode. • Supported line rates: <ul style="list-style-type: none"> – For 2-wire mode: 192, 256, 320, 384, 448, 512, 576, 640, 704, 768, 832, 896, 960, 1024, 1088, 1152, 1216, 1280, 1344, 1408, 1472, 1536, 1600, 1664, 1728, 1792, 1856, 1920, 1984, 2048, 2112, 2176, 2240, and 2304. – For 4-wire mode: 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1536, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2560, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480, and 4608. <p>Note Third-party equipment may use a line rate that includes an additional SHDSL overhead of 8 kbps for 2-wire mode or 16 kbps for 4-wire mode.</p>
SNR Margin settings	

Table 62-19 SHDSL Dialog Box (continued)

Element	Description
Current	<p>The current signal-to-noise (SNR) ratio on the controller, in decibels (dB). Valid values range from -10 to 10 dB.</p> <p>This option can create a more stable line by making the line train more than current noise margin plus SNR ratio threshold during training time. If any external noise is applied that is less than the set SNR margin, the line will be stable.</p> <p>Note Select disable to disable the current SNR.</p>
Snext	<p>The Self Near-End Crosstalk (SNEXT) signal-to-noise ratio on the controller, in decibels. Valid values range from -10 to 10 dB.</p> <p>This option can create a more stable line by making the line train more than SNEXT threshold during training time. If any external noise is applied that is less than the set SNEXT margin, the line will be stable.</p> <p>Note Select disable to disable the SNEXT SNR.</p>

Controller Auto Name Generator Dialog Box

Use the Controller Auto Name Generator dialog box to have Security Manager generate a name for the DSL controller based on its location in the router.

Navigation Path

Go to the [SHDSL Controller Dialog Box, page 62-43](#), then click **Select** in the Name field.

Related Topics

- [Defining SHDSL Controllers, page 62-41](#)
- [SHDSL Policy Page, page 62-42](#)
- [PVC Policy Page, page 62-55](#)

Field Reference

Table 62-20 Controller Auto Name Generator Dialog Box

Element	Description
Type	The type of interface. This field displays the value DSL and is read-only.
Card	The card related to the controller.
Slot	The slot related to the controller.
Port	The port related to the controller.
	<p>Note The information you enter in these fields forms the remainder of the generated name, as displayed in the Result field.</p>

Table 62-20 Controller Auto Name Generator Dialog Box (continued)

Element	Description
Result	<p>The name generated by Security Manager from the information you entered for the controller location. The name displayed in this field is read-only.</p> <p>Tip After closing this dialog box, you can edit the generated name in the SHDSL dialog box, if required.</p>

PVCs on Cisco IOS Routers

Asynchronous Transfer Mode (ATM) is an International Telecommunication Union (ITU-T) standard designed for the high-speed transfer of voice, video, and data through public and private networks using cell relay technology. A cell switching and multiplexing technology, ATM combines the benefits of circuit switching (constant transmission delay, guaranteed capacity) with those of packet switching (flexibility, efficiency for intermittent traffic). An ATM network is made up of one or more ATM switches and ATM endpoints, such as a Cisco IOS router.

There are three general types of ATM services, permanent virtual connections (PVCs), switched virtual connections (SVCs), and connectionless service. PVCs allow direct and permanent connections between sites to provide a service that is similar to a leased line. Advantages of PVCs are the guaranteed availability of a connection and that no call setup procedures are required between switches. Each piece of equipment between the source and destination must be manually provisioned for the PVC.

For more information about ATM PVCs, see:

- [Understanding Virtual Paths and Virtual Channels, page 62-47](#)
- [Understanding ATM Service Classes, page 62-48](#)
- [Understanding ATM Management Protocols, page 62-49](#)

For more information about defining PVCs in Security Manager, see:

- [Defining ATM PVCs, page 62-51](#)
- [Defining OAM Management on ATM PVCs, page 62-54](#)

Related Topics

- [ADSL on Cisco IOS Routers, page 62-34](#)
- [SHDSL on Cisco IOS Routers, page 62-41](#)

Understanding Virtual Paths and Virtual Channels

ATM networks are fundamentally connection oriented. This means that a virtual connection needs to be established across the ATM network before any data transfer. Two types of ATM connections exist:

- Virtual path connections (VPCs), identified by a virtual path identifier (VPI).
- Virtual channel connections (VCCs), identified by the combination of a VPI and a VCI (virtual channel identifier). PVCs are a type of VCC where a permanent connection is defined between two sites.

As shown in [Figure 62-2](#), a virtual path is a bundle of virtual channels, all of which are switched transparently across the ATM network on the basis of the common VPI. A VPC can be thought of as a bundle of VCCs with the same VPI value.

Figure 62-2 ATM Virtual Path and Virtual Channel Connections



Every cell header contains a VPI field and a VCI field, which explicitly associate a cell with a given virtual channel on a physical link. It is important to remember the following attributes of VPIs and VCIs:

- VPIs and VCIs are not addresses, such as MAC addresses used in LAN switching.
- VPIs and VCIs are explicitly assigned at each segment of a connection and, as such, have only local significance across a particular link. They are remapped, as appropriate, at each switching point.

Using the VPI/VCI identifier, the ATM layer can multiplex (interleave), demultiplex, and switch cells from multiple connections. Certain VPI/VCI identifiers are reserved for particular uses, such as the Integrated Local Management Interface (ILMI).

Related Topics

- [Understanding ATM Service Classes, page 62-48](#)
- [Understanding ATM Management Protocols, page 62-49](#)
- [Defining ATM PVCs, page 62-51](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)

Understanding ATM Service Classes

Version 4.0 of the Traffic Management Specification published by the ATM Forum defines five service classes that describe the user traffic transmitted on a network and the quality of service that a network needs to provide for that traffic. Security Manager supports the following ATM service classes:

- *Available Bit Rate (ABR)* This is a service class where ATM switches make no guarantee of cell delivery, but do guarantee a minimum bit rate and that cell loss is kept as low as possible with the use of a feedback mechanism. The ABR service category is designed for VCs that carry file transfers and other bursty, non-real-time traffic that requires a minimum amount of bandwidth. This bandwidth is specified via a minimum cell rate that must be available while the VC is configured and active. For more details, see *Understanding the Available Bit Rate (ABR) Service Category for ATM VCs* at: http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a00800fbc76.shtml.
- *Constant Bit Rate (CBR)* This is a service class where cells are transmitted in a continuous bitstream to meet voice and video QoS needs. The CBR service class is designed for ATM virtual circuits (VCs) that need a static amount of bandwidth that is continuously available for the duration of the active connection. An ATM VC configured as CBR can send cells at peak cell rate (PCR) at any time and for any duration. It also can send cells at a rate less than the PCR or even emit no cells. The

configuration on CBR may vary with different platforms. For more details, see *Understanding the CBR Service Category for ATM VCs* at:

http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080094e6a.shtml.

- *Unspecified Bit Rate (UBR)* This is a service class where the network management makes no Quality of Service (QoS) commitment. It models the best-effort service that the Internet normally provides and is suitable for applications tolerant to delay that do not require real-time responses. Examples include email, fax transmission, file transfers, Telnet, LAN and remote office interconnections. For more details, see *Understanding the UBR Service Category for ATM Virtual Circuits* at: http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a00800a4837.shtml.
- *Unspecified Bit Rate (UBR+)* Cisco provides a variant of the UBR service class called UBR+. The main advantage of the UBR+ service class is that it allows an ATM end-system to signal a minimum cell rate to an ATM switch in a connection request, and the ATM network attempts to maintain this minimum as an end-to-end guarantee. For more details, see *Understanding the UBR+ Service Category for ATM VCs* at: http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080094b40.shtml.
- *Variable Bit Rate - Non-Real Time (VBR-nrt)* This service class is used to transmit non-real-time applications that are bursty in nature. The traffic characteristics are defined in terms of the Peak Cell Rate (PCR), Sustained Cell Rate (SCR), and Minimum Burst Size (MBS). For more details, see *Understanding the VBR-nrt Service Category and Traffic Shaping for ATM VCs* at: http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080102a42.shtml.
- *Variable Bit Rate - Real Time (VBR-rt)* This service class is used to transmit real-time data that is sensitive to time delays, like compressed voice over IP and video conferencing. As with VBR-nrt, VBR-rt traffic is defined in terms of a PCR, SCR, and MBS. For more details, see *Understanding the Variable Bit Rate Real Time (VBR-rt) Service Category for ATM VCs* at: http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080094cd0.shtml.

You can use these service classes to define ATM quality of service (QoS) guarantees, such as traffic shaping. Traffic shaping is the use of queues to constrain data bursts, limit peak data rate, and smooth jitter so that traffic fits within the envelope defined by the traffic contract. ATM devices use traffic shaping to adhere to the terms of the traffic contract.

Related Topics

- [Understanding Virtual Paths and Virtual Channels, page 62-47](#)
- [Understanding ATM Management Protocols, page 62-49](#)
- [Defining ATM PVCs, page 62-51](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)

Understanding ATM Management Protocols

ATM uses two different types of signaling for tracking the status of PVCs:

- Integrated Local Management Interface (ILMI). For more information, see [Understanding ILMI, page 62-50](#).
- Flow 4 (F4) and Flow 5 (F5) Operation, Administration, and Maintenance (OAM) cells. For more information, see [Understanding OAM, page 62-51](#).

Security Manager can be used to enable and disable ILMI on specific PVCs and to configure F5 OAM functionality.

Related Topics

- [Understanding Virtual Paths and Virtual Channels, page 62-47](#)
- [Understanding ATM Service Classes, page 62-48](#)
- [Defining ATM PVCs, page 62-51](#)
- [Defining OAM Management on ATM PVCs, page 62-54](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)

Understanding ILMI

The Integrated Local Management Interface (ILMI) is a protocol defined by the ATM Forum for setting and capturing physical layer, ATM layer, virtual path, and virtual circuit parameters on ATM interfaces. ILMI facilitates network-wide autoconfiguration by enabling devices to determine the status of components at the other end of a physical link and to negotiate a common set of operational parameters to ensure interoperability. The ATM routing protocols, PNNI (Private Network to Network Interface) and IISP (Interim-Interswitch Signaling Protocol), use this information to discover and bring up a network of interconnected ATM switch routers.

When two ATM interfaces run the ILMI protocol, they exchange ILMI packets across the physical connection. These packets consist of SNMP messages as large as 484 octets. ATM interfaces encapsulate these messages in an ATM adaptation layer 5 (AAL5) trailer, segment the packet into cells, and schedule the cells for transmission. ATM interfaces use the SNMP object IDs in network functions such as permanent virtual circuit (PVC) autodiscovery, which is particularly useful in digital subscriber line (DSL) applications.

ILMI organizes managed objects into multiple information bases (MIBs), including one for link management. This MIB contains the following object groups for all ATM interfaces:

- Physical layer—ILMI 4.0 discontinues or "deprecates" earlier physical-layer ILMI values and specifies the use of the standard Interface MIB (RFC 1213).
- ATM layer—Indicates the number of available bits for VPI and VCI values in the ATM cell header, maximum number of virtual path connections (VPCs) and virtual channel connections (VCCs) allowed, number of configured PVCs, and so on.
- Virtual path connection—Indicates the up or down status of a VPC and its Quality of Service (QoS) parameters.
- Virtual channel connection—Indicates the up or down status of the VCC and its QoS parameters.

Administrators may enable or disable ILMI at will, but we highly recommend you enable it. Without ILMI, you must manually configure many of the parameters otherwise managed by ILMI for the ATM devices to operate correctly. ILMI operates over a reserved PVC of VPI=X, VCI=16.

Related Topics

- [Understanding ATM Management Protocols, page 62-49](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)

Understanding OAM

The Operation, Administration, and Maintenance (OAM) feature provides fault management and performance management for ATM and is based on the standard defined in ITU recommendation I.610. OAM detects network connectivity failures on a PVC and reacts by bringing down the PVC. Without OAM, a PVC would remain up after network connectivity is lost. In such a situation, routing table entries would continue to point to the PVC, resulting in lost packets.

Security Manager enables the use of F5 OAM, which operates at the virtual circuit (VC) level. To detect a failure along the PVC path on an end-device, such as a Cisco IOS router, OAM uses the following cells:

- Loopback cells—At regular intervals, routers configured for OAM send loopback cells which must be looped in the network. This looping point can be the machine at the end of the PVC (end-to-end loopback cells) or a device on the path (segment loopback cells). A failure occurs when the loopback cell fails to return to its point of origin.
- Continuity Check (CC) cells—CC cells are sent regularly by routers configured for OAM to check the integrity of the link. CC cells can be sent either end-to-end or confined to a particular segment of the PVC. Activation and deactivation cells are used to initiate and suspend continuity checking. Any connectivity failures are reported in special SNMP notifications.
- Alarm Indication Signal (AIS) cells—In the event of a failure at the physical layer, AIS cells are sent to downstream devices to report a virtual connection failure at the ATM layer. The PVC moves to the down state after a defined number of AIS cells are received and does not come up again until a defined interval passes without additional AIS cells.
- Remote Detection Indication (RDI) cells—When AIS cells are sent to warn downstream devices of a connectivity failure, RDI cells are sent upstream in response as a control and feedback mechanism for the network.

AIS/RDI cells are sent using the same VPI/VCI as the user cells on the affected PVC until the failure is resolved.

Related Topics

- [Understanding ATM Management Protocols, page 62-49](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)
- [Defining OAM Management on ATM PVCs, page 62-54](#)

Defining ATM PVCs

You define an ATM permanent virtual circuit (PVC) by selecting an ATM interface and then defining the following settings:

- The PVC ID.
- The type of encapsulation to use.
- Whether ILMI management is enabled on this PVC.
- Whether Inverse ARP (InARP) is used to learn the IP addresses of the destination devices.
- Options related to PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA).
- Quality-of-service settings, such as traffic shaping.
- Static IP address mappings in place of InARP.

For information about defining F5 Operation, Administration, and Maintenance (OAM) management, such as loopbacks and continuity checks, on PVCs, see [Defining OAM Management on ATM PVCs, page 62-54](#).

Before You Begin

- When configuring ATM over DSL, make sure that you have configured either an ADSL policy (see [ADSL on Cisco IOS Routers, page 62-34](#)) or an SHDSL policy ([SHDSL on Cisco IOS Routers, page 62-41](#)).
- Make sure that the device contains an ATM interface and subinterface. (PVCs are typically configured on ATM subinterfaces.) See [Basic Interface Settings on Cisco IOS Routers, page 62-1](#).



Note

When configuring ATM for SHDSL, the ATM interface is created when you define the SHDSL controller and enable ATM mode. You must then rediscover the device to add the ATM interface to Security Manager. See [Defining SHDSL Controllers, page 62-41](#).

Related Topics

- [Defining OAM Management on ATM PVCs, page 62-54](#)
- [Understanding Policing and Shaping Parameters, page 66-6](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)

Step 1

Do one of the following:

- (Device view) Select **Interfaces > Settings > PVC** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > PVC** from the Policy Type selector. Select an existing policy or create a new one.

The PVC page is displayed. See [Table 62-21 on page 62-56](#) for a description of the fields on this page.

Step 2

Click the **Add** button beneath the table to display the PVC dialog box. See [Table 62-22 on page 62-57](#) for a description of the fields in this dialog box.

Step 3

In the Interface field, enter the name of the ATM interface, ATM subinterface, or interface role on which you want to define the PVC, or click **Select** to select an interface role or to create a new one.

Step 4

Select the type of device or DSL WAN interface card that contains the ATM interface.



Note

We highly recommend that you define this setting to ensure the proper validation of your PVC policy, as the settings in this policy are highly hardware-dependent.

Step 5

On the Settings tab of the PVC dialog box, define the basic settings of the PVC:

- Enter the VPI/VCI identifier and an optional text handle. If you are defining the management PVC, select the **Management PVC (ILMI)** check box.



Note

An error occurs if two users attempt to define PVCs with the same identifiers at the same time.

- Select the type of ATM encapsulation to use. If you select aal5autoppp or aal5ciscoppp, you must define the virtual template to use for PPPoA, or click **Select** to display a selector. If you select aal5mux as the encapsulation type, you must select the protocol that is carried by the PVC.



Note Do not select an encapsulation type when defining the management PVC.



Note If you modify the virtual template settings on an existing PVC, you must enter the **shutdown** command followed by the **no shutdown** command on the ATM subinterface to restart the interface. This causes the newly configured parameters to take effect.

- c. Select the Enable ILMI check box to enable the ILMI to manage this PVC. For more information, see [Understanding ILMI, page 62-50](#).



Note You cannot configure the management PVC on a subinterface.

- d. Select the Inverse ARP check box to enable the PVC to dynamically learn the Layer 3 addresses that are required to forward traffic to those devices.



Note Alternatively, you can create static address mappings, as described in [Step 7](#).

- e. In the PPPoE Max Sessions field, define the maximum number of PPPoE sessions allowed on the PVC.
- f. In the VPN Service Name field, define the static domain name to use for PPPoA sessions on the PVC.

See [Table 62-23 on page 62-58](#) for a description of the fields on the Settings tab.

Step 6 (Optional) On the QoS tab of the PVC dialog box, define the type of ATM traffic shaping to perform on the traffic carried by this PVC. Traffic shaping regulates the flow of traffic carried by the PVC by queuing traffic that exceeds the defined bit rates. See [Table 62-24 on page 62-62](#) for a description of the fields on the QoS tab.

Step 7 (Optional) On the Protocol tab of the PVC dialog box, create static mappings for the IP addresses at the other end of the PVC:

- a. Click **Add** to display the Define Mapping dialog box. See [Table 62-26 on page 62-66](#) for a description of the fields in this dialog box.
- b. Select IP Address, then enter the address or network/host object that you want to map, or click **Select** to select a network/host object from a list or to create a new one.
- c. Click **OK**. The static mapping is displayed on the Protocol tab.
- d. Repeat [a.](#) through [c.](#) to define additional static mappings.



Note You can also use the Protocol tab to change the type of InARP to use, broadcast or non-broadcast.

Step 8 Click **Advanced** to configure OAM management on the PVC. See [Defining OAM Management on ATM PVCs, page 62-54](#).

Step 9 Click **OK** to save your definitions locally on the client and close the dialog box. Your definitions are displayed in the PVC table.



Note To edit a PVC, select it from the table, then click **Edit**. To remove a PVC, select it, then click **Delete**.

Step 10 Repeat [Step 2](#) through [Step 9](#) to define additional PVCs.

Defining OAM Management on ATM PVCs

Security Manager enables you to configure the following F5 (VC level) Operation, Administration, and Maintenance (OAM) cells for detecting PVC failures in a Cisco IOS router:

- Loopback cells
- Continuity Check (CC) cells
- Alarm Indication Signal (AIS) cells
- Remote Detection Indication (RDI) cells

You can enable and disable each of these cell types and define settings that determine how each cell type affects the PVC when a failure is detected.

Before You Begin

- Select the ATM interface on which the PVC is defined.
- Define the general settings and the QoS settings of the PVC. See [Defining ATM PVCs, page 62-51](#).

Related Topics

- [Defining ATM PVCs, page 62-51](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)

Step 1 In the PVC dialog box, click **Advanced** to display the PVC Advanced Settings dialog box. See [Table 62-27 on page 62-66](#) for a description of the fields in this dialog box.

Step 2 Enable OAM loopback cells on the selected PVC:

- a. Click the **OAM-PVC** tab. See [Table 62-29 on page 62-69](#) for a description of the fields on this tab.
- b. Select the **Enable OAM Management** check box.
- c. Define the frequency of loopback cell transmissions.

Step 3 (Optional) Enable segment CC cells on the PVC:

- a. Under Segment Continuity Check, select **Configure Continuity Check**.
- b. Choose whether the router should act as the sink, source, or both. This determines the direction in which CC cells are sent.
- c. Choose whether the PVC should remain up after segment or end-to-end failures are detected.



Note Select **Deny Activation Requests** to have the router reject CC activation requests received from peers.

- Step 4** (Optional) Enable end-to-end CC cells on the PVC, using the procedure described in [Step 3](#) for segment CC cells.
- Step 5** (Optional) Configure additional loopback cell parameters:
- Click the **OAM** tab.
 - Select the **Enable OAM Retry** check box, then define the down count, up count, and retry frequency. See [Table 62-28 on page 62-67](#) for a description of the available options.
- Step 6** (Optional) Configure additional CC cell parameters:
- Select the **Enable** check box for segment CC cells, then define the activation count, deactivation count, and retry frequency. These fields determine how many activation and deactivation requests are sent to peers and how often the router waits between each attempt. See [Table 62-28 on page 62-67](#) for a description of the available options.
 - Repeat **a.** for end-to-end CC cells.
- Step 7** (Optional) Configure AIS/RDI cells on the PVC:
- On the OAM tab, select the **Enable AIS-RDI Detection** check box.
 - Define how many AIS/RDI cells are required to move the PVC to the down state.
 - Define how many seconds must elapse without receiving AIS/RDI cells before moving the PVC to the up state.
- Step 8** Click **OK** to close the dialog box and return to PVC dialog box.
-

PVC Policy Page

Use the PVC page to create, edit, and delete permanent virtual connections (PVCs) on the router. PVCs allow direct and permanent connections between sites to provide a service that is similar to a leased line. These PVCs can be used in ADSL, SHDSL, or pure ATM environments. For more information, see [Defining ATM PVCs, page 62-51](#).

Navigation Path

- (Device view) Select **Interfaces > Settings > PVC** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > PVC** from the Policy Type selector. Right-click **PVC** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- [ADSL Policy Page, page 62-37](#)
- [SHDSL Policy Page, page 62-42](#)
- [PVCs on Cisco IOS Routers, page 62-47](#)
- [Table Columns and Column Heading Features, page 1-49](#)
- [Filtering Tables, page 1-48](#)

Field Reference**Table 62-21 PVC Page**

Element	Description
ATM Interface	The ATM interface on which the PVC is defined.
Interface Card	The type of device or WAN interface card on which the ATM interface resides.
PVC ID	The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) of the PVC.
Settings	Additional settings configured for the PVC, including encapsulation, the number of PPPoE sessions, and the VPN service name.
QoS	Quality-of-service settings defined for the PVC, such as traffic shaping.
Protocol	The IP protocol mappings (static maps or Inverse ARP) configured for the PVC.
OAM	The F5 Operation, Administration, and Maintenance (OAM) loopback, continuity check, and AIS/RDI definitions configured for the PVC.
OAM-PVC	The OAM management cells that are configured for the PVC.
Add button	Opens the PVC Dialog Box, page 62-56 . From here you can define a PVC.
Edit button	Opens the PVC Dialog Box, page 62-56 . From here you can edit the selected PVC.
Delete button	Deletes the selected PVC from the table.

PVC Dialog Box

Use the PVC dialog box to configure ATM permanent virtual circuits (PVCs).

You can configure the following types of interface cards:

- Unknown—The interface card type is not defined.
- WIC-1ADSL—A 1-port ADSL WAN interface card that provides ADSL over POTS (ordinary telephone lines).
- WIC-1ADSL-I-DG—A 1-port ADSL WAN interface card that provides ADSL over ISDN with Dying Gasp support. (With Dying Gasp, the router warns the DSLAM of imminent line drops when the router is about to lose power.)
- WIC-1ADSL-DG—A 1-port ADSL WAN interface card that provides ADSL over POTS with Dying Gasp support.
- HWIC-1ADSL—A 1-port high-speed ADSL WAN interface card that provides ADSL over POTS.
- HWIC-1ADSLI—A 1-port high-speed ADSL WAN interface card that provides ADSL over ISDN.
- HWIC-ADSL-B/ST—A 2-port high-speed ADSL WAN interface card that provides ADSL over POTS with an ISDN BRI port for backup.
- HWIC-ADSLI-B/ST—A 2-port high-speed ADSL WAN interface card that provides ADSL over ISDN with an ISDN BRI port for backup.
- WIC-1-SHDSL-V2—A 1-port multiline G.SHDSL WAN interface card with support for 2-wire mode and enhanced 4-wire mode.

- WIC-1-SHDSL-V3—A 1-port multiline G.SHDSL WAN interface card with support for 2-wire mode and 4-wire mode (standard & enhanced).
- NM-1A-T3—A 1-port ATM network module with a T3 link.
- NM-1A-OC3-POM—A 1-port ATM network module with an optical carrier level 3 (OC-3) link and three operating modes (multimode, single-mode intermediate reach (SMIR), and single-mode long-reach (SMLR)).
- NM-1A-E3—A 1-port ATM network module with an E3 link.
- 857 ADSL—Cisco 857 Integrated Service Router with an ADSL interface.
- 876 ADSL—Cisco 876 Integrated Services Router with an ADSL interface.
- 877 ADSL—Cisco 877 Integrated Services Router with an ADSL interface.
- 878 888 G.SHDSL—Cisco 878 Integrated Services Router with a G.SHDSL interface.
- 1801 ADSLoPOTS—Cisco 1801 Integrated Services Router that provides ADSL over POTS.
- 1802 ADSLoISDN—Cisco 1802 Integrated Services Router that provides ADSL over ISDN.
- 1803 G.SHDSL—Cisco 1803 Integrated Services Router that provides 4-wire G.SHDSL.

Navigation Path

Go to the [PVC Policy Page, page 62-55](#), then click the **Add** or **Edit** button beneath the table.

Related Topics

- [Defining ATM PVCs, page 62-51](#)

Field Reference

Table 62-22 PVC Dialog Box

Element	Description
ATM Interface	<p>The ATM interface on which the PVC is defined. Enter the name of an interface, subinterface, or interface role, or click Select to select it. If the object that you want is not listed, click the Create button to create it.</p> <p>Note We strongly recommend not defining an interface role that includes ATM interfaces from different interface cards. The different settings supported by each card type may cause deployment to fail.</p>
Interface Card	<p>The type of WAN interface card installed on the router or the router type. Supported card types are listed above.</p> <p>Note To ensure proper policy validation, we highly recommend that you define a value in this field. When you discover a live device, the correct interface card type will already be displayed. If you did not perform discovery on a live device, or if Security Manager cannot detect the type of interface card installed on the device, this field displays “Unknown”.</p>
Settings tab	<p>Defines basic PVC settings, such as the VPI/VCI and encapsulation. See PVC Dialog Box—Settings Tab, page 62-58.</p>
QoS tab	<p>Defines ATM traffic shaping and other quality-of-service settings for the PVC. See PVC Dialog Box—QoS Tab, page 62-61.</p>

Table 62-22 PVC Dialog Box (continued)

Element	Description
Protocol tab	Defines the IP protocol mappings configured for the PVC (static maps or Inverse ARP). See PVC Dialog Box—Protocol Tab, page 62-64 .
Advanced button	Defines F5 Operation, Administration, and Maintenance (OAM) settings for the PVC. See PVC Advanced Settings Dialog Box—OAM Tab, page 62-67 .

PVC Dialog Box—Settings Tab

Use the Settings tab of the PVC dialog box to configure the basic settings of the PVC, including:

- ID settings.
- Encapsulation settings.
- Whether ILMI and Inverse ARP are enabled.
- The maximum number of PPPoE sessions.
- The static domain (VPN service) name to use for PPPoA.

Navigation Path

Go to the [PVC Dialog Box, page 62-56](#), then click the **Settings** tab.

Related Topics

- [PVC Dialog Box—QoS Tab, page 62-61](#)
- [PVC Dialog Box—Protocol Tab, page 62-64](#)
- [PVC Advanced Settings Dialog Box, page 62-66](#)
- [Defining ATM PVCs, page 62-51](#)

Field Reference

Table 62-23 PVC Dialog Box—Settings Tab

Element	Description
PVC ID settings	
VPI	<p>The virtual path identifier of the PVC. In conjunction with the VCI, identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination. Valid values for most platforms range from 0 to 255.</p> <p>For Cisco 2600 and 3600 Series routers using Inverse Multiplexing for ATM (IMA), valid values range from 0 to 15, 64 to 79, 128 to 143, and 192 to 207.</p> <p>Note VPI/VCI values must be unique for all the PVCs configured on a selected interface. VPI/VCI values are unique to a single link only and might change as cells traverse the ATM network.</p>

Table 62-23 PVC Dialog Box—Settings Tab (continued)

Element	Description
VCI	<p>The 16-bit virtual channel identifier of the PVC. In conjunction with the VPI, identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination. Valid values vary by platform. Typically, values up to 31 are reserved for special traffic (such as ILMI) and should not be used. 3 and 4 are invalid.</p> <p>Note VPI/VCI values must be unique for all the PVCs configured on a selected interface. VPI/VCI values are unique to a single link only and might change as cells traverse the ATM network.</p>
Handle	<p>An optional name to identify the PVC. The maximum length is 15 characters.</p>
Management PVC (ILMI)	<p>Does not apply when configuring the PVC on a subinterface.</p> <p>When selected, designates this PVC as the management PVC for this ATM interface by enabling communication with the Interim Local Management Interface (ILMI). ILMI is a protocol defined by the ATM Forum for setting and capturing physical layer, ATM layer, virtual path, and virtual circuit parameters on ATM interfaces. See Understanding ILMI, page 62-50.</p> <p>When deselected, this PVC does not act as the management PVC. This is the default.</p> <p>Note The VPI/VCI for the management PVC is typically set to 0/16.</p>
Encapsulation settings	

Table 62-23 PVC Dialog Box—Settings Tab (continued)

Element	Description
Type	<p>Does not apply when the Management PVC (ILMI) check box is enabled.</p> <p>The ATM adaptation layer (AAL) and encapsulation type to use on the PVC:</p> <ul style="list-style-type: none"> • [blank]—The encapsulation type is not defined. (When deployed, aal5snap is applied.) • aal2—For PVCs dedicated to AAL2 Voice over ATM. AAL2 is used for variable bit rate (VBR) traffic, which can be either realtime (VBR-RT) or non-realtime (VBR-NRT). • aal5autopp—Enables the router to distinguish between incoming PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) sessions and create virtual access for both PPP types based on demand. • aal5ciscopp—For the proprietary Cisco version of PPP over ATM. • aal5mux—Enables you to dedicate the PVC to a single protocol, as defined in the Protocol field. • aal5nlpid—Enables ATM interfaces to work with High-Speed Serial Interfaces (HSSI) that are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). • aal5snap—Supports Inverse ARP and incorporates the Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) that precedes the protocol datagram. This allows multiple protocols to traverse the same PVC.
Virtual Template	<p>The virtual template used for PPP over ATM on this PVC. Enter the name of a virtual template interface or interface role, or click Select to select it. If the object that you want is not listed, click the Create button to create it.</p> <p>When a user dials in, the virtual template is used to configure a virtual access interface. When the user is done, the virtual access interface goes down and the resources are freed for other dial-in users.</p> <p>Note If you modify the virtual template settings on an existing PVC, you must enter the shutdown command followed by the no shutdown command on the ATM subinterface to restart the interface. This causes the newly configured parameters to take effect.</p>

Table 62-23 PVC Dialog Box—Settings Tab (continued)

Element	Description
Protocol	<p>Applies only when aal5mux is the defined encapsulation type.</p> <p>The protocol carried by the MUX-encapsulated PVC:</p> <ul style="list-style-type: none"> • frame-relay—Frame-Relay-ATM Network Interworking (FRF.5) on the Cisco MC3810. • fr-atm-srv—Frame-Relay-ATM Service Interworking (FRF.8) on the Cisco MC3810. • ip—IP protocol. • ppp—IETF-compliant PPP over ATM. You must specify a virtual template when using this protocol type. • voice—Voice over ATM.
Additional settings	
Enable ILMI	<p>When selected, enables ILMI management on this PVC.</p> <p>When deselected, ILMI management on this PVC is disabled.</p>
Inverse ARP	<p>When selected, the Inverse Address Resolution Protocol (Inverse ARP) is enabled on the PVC.</p> <p>When deselected, Inverse ARP is disabled. This is the default.</p> <p>Inverse ARP is used to learn the Layer 3 addresses at the remote ends of established connections. These addresses must be learned before the virtual circuit can be used.</p> <p>Note Use the Protocol tab to define static mappings of IP addresses instead of dynamically learning the addresses using Inverse ARP. See PVC Dialog Box—Protocol Tab, page 62-64.</p>
PPPoE Max Sessions	The maximum number of PPP over Ethernet sessions that are permitted on the PVC.
VPN Service Name	<p>The static domain name to use on this PVC. The maximum length is 128 characters.</p> <p>Use this option when you want PPP over ATM (PPPoA) sessions in the PVC to be forwarded according to the domain name supplied, without starting PPP.</p>

PVC Dialog Box—QoS Tab

Use the QoS tab of the PVC dialog box to configure the ATM traffic shaping and other quality-of-service settings of the PVC, including:

- The limit on packets placed on transmission rings.
- The QoS service.
- Whether random detection is enabled.

These settings regulate the flow of traffic over the PVC by queuing traffic that exceeds the defined allowable bit rates.

**Note**

QoS values are highly hardware dependent. Please refer to your router documentation for additional details about the settings that can be configured on your device.

Navigation Path

Go to the [PVC Dialog Box](#), page 62-56, then click the **QoS** tab.

Related Topics

- [PVC Dialog Box—Settings Tab](#), page 62-58
- [PVC Dialog Box—Protocol Tab](#), page 62-64
- [PVC Advanced Settings Dialog Box](#), page 62-66
- [Defining ATM PVCs](#), page 62-51
- [Quality of Service Policy Page](#), page 66-19
- [Understanding Policing and Shaping Parameters](#), page 66-6

Field Reference

Table 62-24 *PVC Dialog Box—QoS Tab*

Element	Description
Tx Ring Limit	<p>The maximum number of transmission packets that can be placed on a transmission ring on the WAN interface card (WIC) or interface.</p> <p>The range of valid values depends on the type of interface card selected in the Settings tab. See PVC Dialog Box—Settings Tab, page 62-58.</p>
Traffic Shaping settings	
Traffic Shaping	<p>The type of service to define on the PVC:</p> <ul style="list-style-type: none"> • [null]—The bit rate is not defined. • ABR—Available Bit Rate. A best-effort service suitable for applications that do not require guarantees against cell loss or delays. • CBR—Constant Bit Rate service. Delay-sensitive data, such as voice or video, is sent at a fixed rate, providing a service similar to a leased line. • UBR—Unspecified Bit Rate service. A best-effort service suitable for applications that are tolerant to delay and do not require realtime responses. • UBR+—Unspecified Bit Rate service. Unlike UBR, UBR+ attempts to maintain a guaranteed minimum rate. • VBR-NRT—Variable Bit Rate - Non-Real Time service. A service suitable for non-realtime applications that are bursty in nature. VBR is more efficient than CBR and more reliable than UBR. • VBR-RT—Variable Bit Rate - Real Time service. A service suitable for realtime applications that are bursty in nature. <p>For more information about each service class, see Understanding ATM Service Classes, page 62-48.</p>

Table 62-24 PVC Dialog Box—QoS Tab (continued)

Element	Description
ABR	<p>The following fields are displayed when ABR is selected as the Bit Rate:</p> <ul style="list-style-type: none"> • PCR—The peak cell rate in kilobits per second (kbps). It specifies the maximum value of the ABR. • MCR—The minimum cell rate in kilobits per second (kbps). It specifies the minimum value of the ABR. <p>The ABR varies between the MCR and the PCR. It is dynamically controlled using congestion control mechanisms.</p>
CBR	<p>The following field is displayed when CBR is selected as the Bit Rate:</p> <ul style="list-style-type: none"> • Rate—The constant bit rate (also known as the average cell rate) for the PVC in kilobits per second (kbps). An ATM VC configured for CBR can send cells at this rate for as long as required.
UBR	<p>The following field is displayed when UBR is selected as the Bit Rate:</p> <ul style="list-style-type: none"> • PCR—The peak cell rate for output in kilobits per second (kbps). Cells in excess of the PCR may be discarded.
UBR+	<p>The following fields are displayed when UBR+ is selected as the Bit Rate:</p> <ul style="list-style-type: none"> • PCR—The peak cell rate for output in kilobits per second (kbps). Cells in excess of the PCR may be discarded. • MCR—The minimum guaranteed cell rate for output in kilobits per second (kbps). Traffic is always allowed to be sent at this rate. <p>Note UBR+ requires Cisco IOS Software Release 12.4(2)XA or later, or version 12.4(6)T or later.</p>
VBR-NRT	<p>The following fields are displayed when VBR-NRT is selected as the Bit Rate:</p> <ul style="list-style-type: none"> • PCR—The peak cell rate for output in kilobits per second (kbps). Cells in excess of the PCR may be discarded. • SCR—The sustained cell rate for output in kilobits per second (kbps). This value, which must be lower than or equal to the PCR, represents the maximum rate at which cells can be transmitted without incurring data loss. • MBS—The maximum burst cell size for output. This value represents the number of cells that can be transmitted above the SCR but below the PCR without penalty.

Table 62-24 PVC Dialog Box—QoS Tab (continued)

Element	Description
VBR-RT	<p>The following fields are displayed when VBR-RT is selected as the Bit Rate:</p> <ul style="list-style-type: none"> • Peak Rate—The peak information rate for realtime traffic in kilobits per second (kbps). • Average Rate—The average information rate for realtime traffic in kilobits per second (kbps). This value must be lower than or equal to the peak rate. • Burst—The burst size for realtime traffic, in number of cells. Configure this value if the PVC carries bursty traffic. <p>These values configure traffic shaping between realtime traffic (such as voice and video) and data traffic to ensure that the carrier does not discard realtime traffic, for example, voice calls.</p>
IP QoS settings	
Random Detect	<p>When selected, enables Weighted Random Early Detection (WRED) or VIP-distributed WRED (DWRED) on the PVC.</p> <p>When deselected, WRED and DWRED are disabled. This is the default.</p> <p>WRED is a queue management method that selectively drops packets as the interface becomes congested. See Tail Drop vs. WRED, page 66-4.</p>

PVC Dialog Box—Protocol Tab

Use the Protocol tab of the PVC dialog box to add, edit, or delete the protocol mappings configured for the PVC. You may configured static mappings or Inverse ARP (broadcast or nonbroadcast) for each PVC, but not both.



Note

IP is the only protocol supported by Security Manager for protocol mapping on ATM networks. You cannot define protocol mappings on the Management PVC (ILMI).

Navigation Path

Go to the [PVC Dialog Box](#), page 62-56, then click the **Protocol** tab.

Related Topics

- [PVC Dialog Box—Settings Tab](#), page 62-58
- [PVC Dialog Box—QoS Tab](#), page 62-61
- [PVC Advanced Settings Dialog Box](#), page 62-66
- [Defining ATM PVCs](#), page 62-51

Field Reference**Table 62-25 PVC Dialog Box—Protocol Tab**

Element	Description
IP Protocol Mapping	Displays the IP protocol mappings configured for the PVC.
Add button	Opens the Define Mapping Dialog Box, page 62-65 . From here you can define an IP protocol mapping.
Edit button	Opens the Define Mapping Dialog Box, page 62-65 . From here you can edit the selected mapping.
Delete button	Deletes the selected mapping from the table.

Define Mapping Dialog Box

Use the Define Mapping dialog box to configure the IP protocol mappings to use on the ATM PVC. Mappings are required by the PVC to discover which IP address is reachable at the other end of a connection. Mappings can either be learned dynamically using Inverse ARP (InARP) or defined statically. Static mappings are best suited for simple networks that contain only a few nodes.

**Note**

Inverse ARP is only supported for the aal5snap encapsulation type. See [PVC Dialog Box—Settings Tab, page 62-58](#).

**Tip**

Use the CLI or FlexConfigs to configure mappings for protocols other than IP.

Navigation Path

Go to the [PVC Dialog Box—Protocol Tab, page 62-64](#), then click **Add** or **Edit**.

Related Topics

- [PVC Dialog Box, page 62-56](#)
- [Defining ATM PVCs, page 62-51](#)

Field Reference**Table 62-26** *Define Mapping Dialog Box*

Element	Description
IP Options	<p>The type of IP protocol mapping to use:</p> <ul style="list-style-type: none"> IP Address—Select this option when using static mapping. Enter the address or the name of a network/host object, or click Select to select it. If the object that you want is not listed, click the Create button to create it. InARP—Inverse ARP. Select this option when using dynamic mapping. This allows the PVC to resolve its own network addresses without configuring a static map. Dynamic mappings age out and are refreshed periodically every 15 minutes by default. <p>Note InARP can be used only when aal5snap is the defined encapsulation type for the PVC. See PVC Dialog Box—Settings Tab, page 62-58.</p>
Broadcast Options	<p>Indicates whether to use this map entry when sending IP broadcast packets (such as EIGRP updates):</p> <ul style="list-style-type: none"> Broadcast—The map entry is used for broadcast packets. No Broadcast—The map entry is used only for unicast packets. None—Broadcast options are disabled.

PVC Advanced Settings Dialog Box

Use the PVC Advanced Settings dialog box to configure F5 Operation, Administration, and Maintenance (OAM) functionality on an ATM PVC. OAM is used to detect connectivity failures at the ATM layer.

For more information, see [Defining OAM Management on ATM PVCs, page 62-54](#).

Navigation Path

Go to the [PVC Dialog Box, page 62-56](#), then click **Advanced**.

Related Topics

- [PVC Policy Page, page 62-55](#)

Field Reference**Table 62-27** *PVC Advanced Settings Dialog Box*

Element	Description
OAM tab	Defines loopback, connectivity check, and AIS/RDI settings. See PVC Advanced Settings Dialog Box—OAM Tab, page 62-67 .
OAM-PVC tab	Enables OAM loopbacks and connectivity checks on the PVC. See PVC Advanced Settings Dialog Box—OAM-PVC Tab, page 62-69 .

PVC Advanced Settings Dialog Box—OAM Tab

Use the OAM tab of the PVC Advanced Settings dialog box to define:

- The number of loopback cell responses that move the PVC to the down or up state.
- The number of alarm indication signal/remote defect indication (AIS/RDI) cells that move the PVC to the down or up state.
- The number and frequency of segment/end continuity check (CC) activation and deactivation requests that are sent on this PVC.

For more information, see [Defining OAM Management on ATM PVCs, page 62-54](#).



Note

The settings defined in this tab are dependent on the settings defined in the OAM-PVC tab. See [PVC Advanced Settings Dialog Box—OAM-PVC Tab, page 62-69](#).

Navigation Path

Go to the [PVC Advanced Settings Dialog Box, page 62-66](#), then click the **OAM** tab.

Related Topics

- [PVC Dialog Box, page 62-56](#)

Field Reference

Table 62-28 PVC Advanced Settings Dialog Box—OAM Tab

Element	Description
Retry settings	
Enable OAM Retry	<p>When selected, OAM management settings can be defined.</p> <p>When deselected, OAM management settings cannot be defined.</p> <p>Note If Enable OAM Management is deselected in the OAM-PVC tab, these settings are saved in the device configuration but are not applied.</p>
Down Count	The number of consecutive, unreceived, end-to-end loopback cell responses that cause the PVC to move to the down state. The default is 3.
Up Count	The number of consecutive end-to-end loopback cell responses that must be received in order to move the PVC to the up state. The default is 5.
Retry Frequency	<p>The interval between loopback cell verification transmissions in seconds. The default is 1 second.</p> <p>If a PVC is up and a loopback cell response is not received within the specified interval (as defined in the Frequency field of the PVC-OAM tab), loopback cells are transmitted at the frequency defined here to verify whether the PVC is down. If the number of consecutive cells that do not receive a response matches the defined down count, the PVC is moved to the down state.</p>
AIS-RDI settings	

Table 62-28 PVC Advanced Settings Dialog Box—OAM Tab (continued)

Element	Description
Enable AIS-RDI Detection	<p>When selected, alarm indication signal (AIS) cells and remote defect indication (RDI) cells are used to report connectivity failures at the ATM layer of the PVC.</p> <p>When deselected, AIS/RDI cells are disabled.</p> <p>AIS cells notify downstream devices of the connectivity failure. The last ATM switch then generates RDI cells in the upstream direction towards the device that sent the original failure notification.</p>
Down Count	The number of consecutive AIS/RDI cells that cause the PVC to go down. Valid values range from 1 to 60. The default is 1.
Up Count	The number of seconds after which a PVC is brought up if no AIS/RDI cells are received. Valid values range from 3 to 60 seconds. The default is 3.
Segment Continuity Check settings	
Enable Segment Continuity Check	<p>When selected, OAM F5 continuity check (CC) activation and deactivation requests are sent to a device at the other end of a segment.</p> <p>When deselected, segment CC activation and deactivation requests are disabled.</p> <p>Note If Configure Continuity Check is deselected in the OAM-PVC tab, these settings are saved in the device configuration but are not applied.</p>
Activation Count	The maximum number of times that the activation request is sent before the receipt of an acknowledgement. Valid values range from 3 to 600. The default is 3.
Deactivation Count	The maximum number of times that the deactivation request is sent before the receipt of an acknowledgement. Valid values range from 3 to 600. The default is 3.
Retry Frequency	The interval between activation/deactivation retries, in seconds. The default is 30 seconds.
End-to-End Continuity Check settings	
Enable End-to-End Continuity Check	<p>When selected, OAM F5 continuity check (CC) activation and deactivation requests are sent to a device at the other end of the PVC.</p> <p>When deselected, segment CC activation and deactivation requests are disabled.</p> <p>Note If Configure Continuity Check is deselected in the OAM-PVC tab, these settings are saved in the device configuration but are not applied.</p>
Activation Count	The maximum number of times that the activation request is sent before the receipt of an acknowledgement. Valid values range from 3 to 600. The default is 3.
Deactivation Count	The maximum number of times that the deactivation request is sent before the receipt of an acknowledgement. Valid values range from 3 to 600. The default is 3.

Table 62-28 PVC Advanced Settings Dialog Box—OAM Tab (continued)

Element	Description
Retry Frequency	The interval between activation/deactivation retries, in seconds. The default is 30 seconds.

PVC Advanced Settings Dialog Box—OAM-PVC Tab

Use the OAM-PVC tab of the PVC Advanced Settings dialog box to enable loopback cells and connectivity checks (CCs) on the PVC. These functions test the connectivity of the virtual connection.

For more information, see [Defining OAM Management on ATM PVCs, page 62-54](#).



Note

Use the OAM tab to define additional settings related to the settings on this tab. See [PVC Advanced Settings Dialog Box—OAM Tab, page 62-67](#).

Navigation Path

Go to the [PVC Advanced Settings Dialog Box, page 62-66](#), then click the **OAM-PVC** tab.

Related Topics

- [PVC Dialog Box, page 62-56](#)

Field Reference

Table 62-29 PVC Advanced Settings Dialog Box—OAM-PVC Tab

Element	Description
OAM settings	
Enable OAM Management	When selected, OAM loopback cell generation and OAM management are enabled on the PVC. When deselected, OAM loopback cells and OAM management are disabled. However, continuity checks can still be performed.
Frequency	The interval between loopback cell transmissions. Valid values range from 0 to 600 seconds.
Segment Continuity Check settings	
Segment Continuity Check	The current configuration of OAM F5 continuity checks performed on PVC segments: <ul style="list-style-type: none"> • None—Segment continuity checks (CC) are disabled. • Deny Activation Requests—The PVC rejects activation requests from peer devices, which prevents OAM F5 CC management from being activated on the PVC. • Configure Continuity Check—Segment CCs are enabled on the PVC. The router on which CC management is configured sends a CC activation request to the router at the other end of the segment, directing it to act as either a source or a sink. Segment CCs occur on a PVC segment between the router and a first-hop ATM switch.

Table 62-29 PVC Advanced Settings Dialog Box—OAM-PVC Tab (continued)

Element	Description
Direction	<p>Applies only when CC management is enabled.</p> <p>The direction in which CC cells are transmitted:</p> <ul style="list-style-type: none"> • both—CC cells are transmitted in both directions. • sink—CC cells are transmitted toward the router that initiated the CC activation request. • source—CC cells are transmitted away from the router that initiated the CC activation request.
Keep VC up after segment failure	<p>When selected, the PVC is kept in the up state when CC cells detect connectivity failure.</p> <p>When deselected, the PVC is brought down when CC cells detect connectivity failure.</p>
Keep VC up after end-to-end failure	<p>When selected, specifies that if AIS/RDI cells are received, the PVC is not brought down because of end CC failure or loopback failure.</p> <p>When deselected, the PVC is brought down because of end CC failure or loopback failure.</p>
End-to-End Continuity Check settings	
End-to-End Continuity Check	<p>The current configuration of OAM F5 end-to-end continuity checks on the PVC:</p> <ul style="list-style-type: none"> • None—End-to-end continuity checks (CC) are disabled. • Deny Activation Requests—The PVC rejects activation requests from peer devices, which prevents OAM F5 CC management from being activated on the PVC. • Configure Continuity Check—End-to-end CCs are enabled on the PVC. The router on which CC management is configured sends a CC activation request to the router at the other end of the connection, directing it to act as either a source or a sink. <p>End-to-end CC monitoring is performed on the entire PVC between two ATM end stations.</p>
Direction	<p>Applies only when CC management is enabled.</p> <p>The direction in which CC cells are transmitted:</p> <ul style="list-style-type: none"> • both—CC cells are transmitted in both directions. • sink—CC cells are transmitted toward the router that initiated the CC activation request. • source—CC cells are transmitted away from the router that initiated the CC activation request.
Keep VC up after end-to-end failure	<p>When selected, the PVC is kept in the up state when CC cells detect connectivity failure.</p> <p>When deselected, the PVC is brought down when CC cells detect connectivity failure.</p>

Table 62-29 PVC Advanced Settings Dialog Box—OAM-PVC Tab (continued)

Element	Description
Keep VC up after segment failure	When selected, specifies that if AIS/RDI cells are received, the PVC is not brought down because of a segment CC failure. When deselected, the PVC is brought down because of a segment CC failure.

PPP on Cisco IOS Routers

The Point-to-Point Protocol (PPP), as defined in RFC 1661, provides a method for transporting packets between two devices or hosts using physical or logical links. PPP is a Layer 2 data-link protocol that can work with multiple Layer 3 network-layer protocols, including IP, IPX, and AppleTalk.

PPP is used in many common scenarios, such as:

- Connecting remote users to a central network over dial-in connections.
- Connecting the gateway of an enterprise network to an ISP for internet access.
- Connecting two LANs (for example, a central office and a branch office) to exchange data between them.

PPP connectivity is established in stages:

1. First, a Link Control Protocol (LCP) establishes, configures, and tests the data-link connection.
2. (Optional) Authentication verifies the identity of the two parties.
3. A family of Network Control Protocols (NCPs) establishes and configures the necessary network-layer protocols.

The PPP policy in Security Manager provides a method for configuring selected parameters that are negotiated between the two nodes during the LCP stage, including authentication (typically CHAP or PAP) and Multilink PPP (MLP). For more information about MLP, see [Defining Multilink PPP Bundles, page 62-75](#).

The following topics describe the tasks you perform to create PPP policies on Cisco IOS routers:

- [Defining PPP Connections, page 62-72](#)
- [Defining Multilink PPP Bundles, page 62-75](#)

Understanding Multilink PPP (MLP)

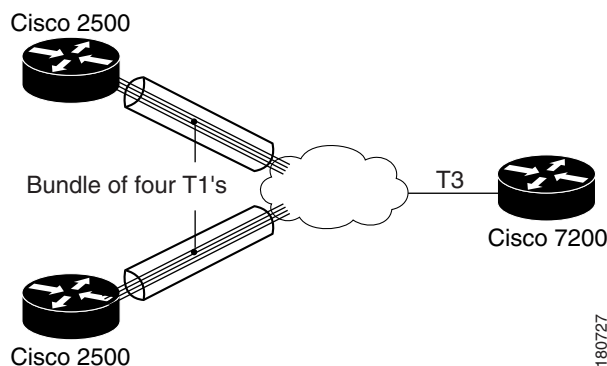
MLP, as defined in RFC 1990, is a method for splitting, recombining, and sequencing datagrams across multiple logical data links. MLP was originally designed to exploit multiple bearer channels in ISDN, but it can be used whenever multiple PPP links connect two systems, including asynchronous links.

MLP spreads inbound and outbound traffic across multiple physical WAN links (known collectively as a bundle) while providing the following benefits:

- Packet fragmentation and reassembly
- Proper sequencing
- Multivendor interoperability
- Load balancing

As shown in [Figure 62-3](#), traffic routed across an MLP link is fragmented, with the fragments being sent across the different physical links. At the remote end of the link, the fragments are reassembled and forwarded to the next hop toward their ultimate destination. By using multiple physical links, MLP provides a way to temporarily use the additional bandwidth afforded by these links.

Figure 62-3 Multilink PPP



Every MLP bundle is controlled by a single interface, the bundle director, which is a virtual-access interface. This interface is created in the background when the bundle is first created. The physical interface becomes part of the bundle that is managed by the bundle director. Bundles are also used when you create a multilink group consisting of a multilink interface and its associated serial interfaces, which is a setup that is often found in static, leased-line environments.

MLP uses an endpoint discriminator to identify the system transmitting a packet. By default, this discriminator is based on the hostname of the router, but it can also be based on other criteria, such as the IP address or MAC address of the interface, a telephone number, or a user-defined string. If the endpoint discriminator matches the discriminator of an existing link, the new link is added to the matching bundle. If no match exists, a new bundle is created. When authentication is used, a new bundle is established whenever there is a mismatch in either the discriminator or the authentication information exchanged between the two nodes.

Related Topics

- [Defining Multilink PPP Bundles, page 62-75](#)
- [PPP on Cisco IOS Routers, page 62-71](#)

Defining PPP Connections

When you define a PPP connection, the first step is to select the interface on which PPP should be enabled. You must select one of the following interface types:

- Async
- Group-Async
- Serial
- High-Speed Serial Interface (HSSI)
- Dialer
- BRI, PRI (ISDN)
- Virtual template

- Multilink

You cannot define PPP connections on:

- Subinterfaces.
- Serial interfaces with Frame Relay encapsulation.
- Virtual template interfaces defined as Ethernet or tunnel types (serial is supported).

**Note**

You cannot configure PPP on serial interfaces that are configured for Frame Relay encapsulation. See [Defining Basic Router Interface Settings, page 62-4](#).

**Note**

Deployment might fail if you define PPP on a virtual template that is also used in an 802.1x policy. See [Defining 802.1x Policies, page 64-4](#).

You can select one or more authentication protocols and define when authentication should be performed.

In addition, you can configure the authentication and authorization methods to use when performing AAA on a remote security server. You can either define a default method list to use for all PPP connections on the device or define a customized method list that applies to a specific connection.

Before You Begin

- Make sure that the device contains an interface on which PPP can be configured. See [Basic Interface Settings on Cisco IOS Routers, page 62-1](#).

Related Topics

- [Defining Multilink PPP Bundles, page 62-75](#)
- [PPP on Cisco IOS Routers, page 62-71](#)

-
- Step 1** Do one of the following:
- (Device view) Select **Interfaces > Settings > PPP/MLP** from the Policy selector.
 - (Policy view) Select **Router Interfaces > Settings > PPP/MLP** from the Policy Type selector. Select an existing policy or create a new one.
- The PPP/MLP page is displayed. See [Table 62-30 on page 62-76](#) for a description of the fields on this page.
- Step 2** Click the **Add** button beneath the table to display the PPP dialog box.
- Step 3** In the Interface field, enter the name of the interface or interface role on which you want to define the PPP connection, or click **Select** to select an interface role from a list or to create a new one.
- Step 4** (Optional) On the PPP tab, define authentication for the PPP connection:
- a. Select one or more authentication protocols.
 - b. Select one or more authentication options. These options determine when to perform authentication (callin, callout, and callback), whether to use one-time passwords, and whether to allow a mobile station in a PDSN configuration to receive Simple IP and Mobile IP services without using CHAP or PAP.



Note The Call Back option only enables authentication during callback. Use the CLI or FlexConfigs to configure the callback feature on the device.

c. See [PPP Dialog Box—PPP Tab, page 62-78](#) for a description of the fields on this tab.

Step 5 (Optional) When using a remote AAA server to perform authentication, select Default List or Custom Method List in the Authenticate Using field, then define the methods to use in the Prioritized Method List field.



Note If you modify the default list, your changes affect all PPP connections on the devices that use this list. If you leave this field blank, authentication is performed using the local database on the device.

Step 6 (Optional) When using a remote AAA server to perform authorization, select AAA Policy Default List or Custom Method List, then define the methods to use in the Prioritized Method List field.



Note If you choose AAA Policy Default List, the device uses the default authorization methods defined in the AAA policy. See [Defining AAA Services, page 63-4](#).

Step 7 (Optional) Define the username and password to send in response to PAP authentication requests.



Note If you entered the encrypted version of the password, select the **Encrypted** check box.

Step 8 (Optional) Define a different hostname to send in all CHAP challenges and responses in place of the router's own hostname.



Note If you entered the encrypted version of the password, select the **Encrypted** check box.

Step 9 (Optional) To enable Multilink PPP on this connection, click the **MLP** tab. See [Defining Multilink PPP Bundles, page 62-75](#).

Step 10 Click **OK** to save your definitions locally on the client and close the dialog box. Your definitions are displayed in the PPP table.



Note To edit a PPP connection, select it from the table, then click **Edit**. To remove a PPP connection, select it, then click **Delete**.

Step 11 Repeat [Step 2](#) to [Step 10](#) to define PPP connections on additional interfaces. Only one PPP connection may be defined on an interface.

Defining Multilink PPP Bundles

You enable Multilink PPP (MLP) on the selected interface by selecting the check box at the top of the Multilink tab in the PPP dialog box. You can optionally enable Multiclass Multilink PPP (MCMP), which prevents delay-sensitive traffic from fragmentation, and interleaving, which enables packets to be interspersed among the fragments of larger packets. If you want to restrict a serial interface to a specific bundle, you can select the multilink interface that represents that bundle.

In addition, you can optionally modify the following default settings:

- The maximum fragment delay.
- The endpoint discriminator that identifies the router when negotiating the use of MLP.
- The maximum receive reconstructed unit (MRRU) permitted by the router and its peers.
- The maximum queue depth for first-in, first-out (FIFO) and non-FIFO queues.

Before You Begin

- Select the interface on which the PPP connection should be enabled.

Related Topics

- [Defining PPP Connections, page 62-72](#)
- [PPP on Cisco IOS Routers, page 62-71](#)

-
- Step 1** In the PPP dialog box, click the **MLP** tab. See [PPP Dialog Box—MLP Tab, page 62-80](#) for a description of the fields on this tab.
- Step 2** Select the **Enable Multilink Protocol (MLP)** check box.
- Step 3** (Optional) Configure one or more of the following options:
- a. Whether to enable the multiclass feature that prevents delay-sensitive traffic from being fragmented. This is achieved by placing delay-sensitive traffic in a separate class from regular traffic.
 - b. Whether to enable the interleaving of packets among the fragments of larger packets on the MLP bundle.
 - c. Whether to restrict the physical link to joining only a designated multilink-group (defined by selecting a multilink interface). If a peer at the other end of the link tries to join a different bundle, the connection is severed.
 - d. Whether to modify the default amount of time required to transmit a fragment on the MLP bundle. The default is 30 milliseconds.



Note If you enable interleaving without defining a fragment delay, the default delay of 30 seconds is configured. This value does not appear in Security Manager or in the device configuration.

- Step 4** (Optional) Under Endpoint, modify the default endpoint discriminator used on the MLP bundle. The endpoint discriminator is used to identify the router on the MLP bundle. The default endpoint discriminator is either the globally configured hostname, or the PAP username or CHAP hostname (depending on the authentication protocol being used), if you configured those values on the PPP tab. See [Defining PPP Connections, page 62-72](#).
- Step 5** (Optional) In the MRRU fields, modify the default maximum packet size that the router (local) or the peer (remote) is capable of receiving.

- Step 6** (Optional) Modify the default maximum size of link transmit queues when using FIFO and non-FIFO (QoS) queuing.
- Step 7** Click **OK** to close the dialog box. Your definitions are displayed on the PPP page.

PPP/MLP Policy Page

Use the PPP/MLP page to create, edit, and delete PPP connections on the router. For more information, see [Defining PPP Connections, page 62-72](#).

Navigation Path

- (Device view) Select **Interfaces > Settings > PPP/MLP** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > PPP/MLP** from the Policy Type selector. Right-click **PPP/MLP** to create a policy, or select an existing policy from the Shared Policies selector.

Related Topics

- [PPP on Cisco IOS Routers, page 62-71](#)
- [Table Columns and Column Heading Features, page 1-49](#)
- [Filtering Tables, page 1-48](#)

Field Reference

Table 62-30 *PPP/MLP Page*

Element	Description
Interface	The interface that is configured for PPP/MLP.
Authentication	The types of authentication used on the PPP connection.
Authorization	The method list used for AAA authorization on the PPP connection.
Multilink	Indicates whether Multilink PPP (MLP) is enabled on this PPP connection.
Endpoint	The type of default endpoint discriminator to use when negotiating the use of MLP with the peer.
Multiclass	Indicates whether the Multiclass Multilink PPP (MCMP) feature is enabled on this PPP connection.
Group	The number of the multilink-group interface to which the physical link is restricted.
Interleave	Indicates whether the PPP multilink interleave feature is enabled on this PPP connection.
Add button	Opens the PPP Dialog Box, page 62-77 . From here you can define the authentication and multilink settings for the PPP connection.
Edit button	Opens the PPP Dialog Box, page 62-77 . From here you can edit the selected PPP connection.
Delete button	Deletes the selected PPP connection from the table.

PPP Dialog Box

Use the PPP dialog box to configure PPP connections on the router. When you configure a PPP connection, you can define the type of authentication and authorization to perform and define multilink parameters.

Navigation Path

Go to the [PPP/MLP Policy Page, page 62-76](#), then click the **Add** or **Edit** button beneath the table.

Related Topics

- [Defining PPP Connections, page 62-72](#)

Field Reference

Table 62-31 PPP Dialog Box

Element	Description
Interface	<p>The interface on which PPP encapsulation is enabled. Enter the name of an interface or interface role, or click Select to select it. If the object that you want is not listed, click the Create button to create it.</p> <p>The following interface types support PPP:</p> <ul style="list-style-type: none"> • Async • Group-Async • Serial • High-Speed Serial Interface (HSSI) • Dialer • BRI, PRI (ISDN) • Virtual template • Multilink <p>You cannot define PPP on:</p> <ul style="list-style-type: none"> • Subinterfaces. • Serial interfaces with Frame Relay encapsulation. • Virtual template interfaces defined as Ethernet or tunnel types (serial is supported). <p>Note You can define only one PPP connection per interface.</p> <p>Note Deployment might fail if you define PPP on a virtual template that is also used in an 802.1x policy. See 802.1x Policy Page, page 64-5.</p>
PPP tab	<p>Defines the type of authentication and authorization to perform on the PPP connection. See PPP Dialog Box—PPP Tab, page 62-78.</p>

Table 62-31 *PPP Dialog Box (continued)*

Element	Description
MLP tab	<p>Defines how to split and recombine sequential datagrams across multiple logical data links using Multilink PPP (MLP). See PPP Dialog Box—MLP Tab, page 62-80.</p> <p>This tab is greyed out and cannot be opened for devices that do not support the configuration settings.</p>

PPP Dialog Box—PPP Tab

Use the PPP tab of the PPP dialog box to define the types of authentication and authorization to perform on the PPP connection.

Navigation Path

Go to the [PPP Dialog Box, page 62-77](#), then click the **PPP** tab.

Related Topics

- [PPP Dialog Box—MLP Tab, page 62-80](#)

Field Reference

Table 62-32 *PPP Dialog Box—PPP Tab*

Element	Description
Authentication settings	
PPP Encapsulation	When selected, indicates that PPP encapsulation is enabled for the selected interface. This field is read-only.
Protocol	<p>The authentication protocols to use:</p> <ul style="list-style-type: none"> • CHAP—Challenge-Handshake Authentication Protocol. • PAP—Password Authentication Protocol. • MS-CHAP—Version 1 of the Microsoft version of CHAP (RFC 2433). • MS-CHAP-2—Version 2 of the Microsoft version of CHAP (RFC 2759). • EAP—Extensible Authentication Protocol. <p>You may select one or more authentication protocols, as required.</p>

Table 62-32 PPP Dialog Box—PPP Tab (continued)

Element	Description
Options	<p>The authentication options to use:</p> <ul style="list-style-type: none"> • Call In—When selected, authentication is performed on incoming calls. • Call Out—When selected, authentication is performed on outgoing calls. • Call Back—When selected, authentication is performed on callback. • One Time—When selected, one-time passwords are used for authentication. One-time passwords are considered highly secure since each one is used only once. When deselected, one-time passwords are not used. <p>Note AAA authentication must be enabled in order to use one-time passwords. See AAA Policy Page, page 63-6. One-time passwords cannot be used with CHAP.</p> <ul style="list-style-type: none"> • Optional—When selected, allows a mobile station in a Packet Data Serving Node (PDSN) configuration to receive Simple IP and Mobile IP services without using CHAP or PAP. <p>When deselected, mobile stations must use CHAP or PAP to receive Simple IP and Mobile IP services.</p>
Authenticate Using	<p>AAA authentication settings for the PPP connection:</p> <ul style="list-style-type: none"> • PPP Default List—Defines a default list of methods to be queried when authenticating a user for PPP. Enter the names of one or more AAA server group objects (up to four) in the Prioritized Method List field, or click Select to select it. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the Create button to create it. <p>The device tries initially to authenticate users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received.</p> <p>Tip After you create the default list for one PPP connection, you can use it for other PPP connections on this device.</p> <ul style="list-style-type: none"> • Prioritized Method List—Defines a sequential list of methods to be queried when authenticating a user for this PPP connection only. <p>Note Leave this field blank to perform authentication using the local database on the router.</p>
PAP Authentication settings	
Username	The username to send in PAP authentication requests. The username is case sensitive.

Table 62-32 PPP Dialog Box—PPP Tab (continued)

Element	Description
Password	<p>The password to send in PAP authentication requests. Enter the password again in the Confirm field. The password can contain 1 to 25 uppercase or lowercase alphanumeric characters. The password is case sensitive.</p> <p>The username and password are sent if the peer requests the router to authenticate itself using PAP.</p>
Encrypted Password	<p>When selected, this indicates that the password you entered is already encrypted.</p> <p>When deselected, this indicates that the password you entered is in clear text.</p>
CHAP Authentication settings	
Hostname	By default, the router uses its hostname to identify itself to the peer. If required, you can enter a different hostname to use for all CHAP challenges and responses. For example, use this field to specify a common alias for all routers in a rotary group.
Secret	The secret used to compute the response value for any CHAP challenge from an unknown peer. Enter the secret again in the Confirm field.
Encrypted Secret	When selected, this indicates that the password you entered is already encrypted. When deselected, this indicates that the password you entered is in clear text.
Authorization settings	
Authorize Using	<p>AAA authorization settings for the PPP connection:</p> <ul style="list-style-type: none"> AAA Policy Default List—Uses the default authorization method list that is defined in the device's AAA policy. See AAA Policy Page, page 63-6. Prioritized Method List—Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click Select to select it. Use the up and down arrows to define the order in which selected server groups should be used. If the object that you want is not listed, click the Create button to create it. <p>The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received.</p> <p>Note Leave this field blank to perform authorization using the local database on the router.</p>

PPP Dialog Box—MLP Tab

Use the MLP tab of the PPP dialog box to define Multilink PPP (MLP) parameters for the selected PPP connection.

Navigation Path

Go to the [PPP Dialog Box, page 62-77](#), then click the **MLP** tab.

Related Topics

- [PPP Dialog Box—PPP Tab, page 62-78](#)

Field Reference**Table 62-33** *PPP Dialog Box—MLP Tab*

Element	Description
Enable Multilink PPP (MLP)	When selected, MLP is enabled on this PPP connection. When deselected, MLP is disabled.
Allow Multiple Data Classes	When selected, enables multiple data classes on the MLP bundle. Delay-sensitive traffic is placed into Class 1, where it can be interleaved but never fragmented. Normal data traffic is placed into Class 0, which is subject to fragmentation just as regular multilink packets are. When deselected, all traffic is subject to fragmentation.
Enable Interleaving of Packets Among Fragments of Larger Packets	When selected, enables the interleaving of packets among the fragments of larger packets on the MLP bundle. Note If you enable interleaving without defining a fragment delay, the default delay of 30 seconds is configured. This value does not appear in Security Manager or in the device configuration. When deselected, interleaving is disabled. Note Serial interfaces do not support interleaving.
Multilink Group	Applies only to serial, Group-Async, and multilink interfaces. Restricts the physical link to the selected multilink-group interface. Enter the name of a multilink interface or interface role, or click Select to select it. If the object that you want is not listed, click the Create button to create it. This option is typically used in static leased-line environments, where the remote systems to which the device's serial lines are connected are known in advance. In effect, this option dedicates a specific interfaces to a particular user, even when that user is not connected. If a peer at the other end of the link tries to join a different bundle, the connected is severed.
Maximum Fragment Delay	The maximum amount of time that should be required to transmit a fragment on the MLP bundle. Valid values range from 1 to 1000 milliseconds. Fragment size is determined by the defined fragment delay and the bandwidth of the links. Note Serial interfaces do not support this feature.

Table 62-33 PPP Dialog Box—MLP Tab (continued)

Element	Description
Endpoint Type	<p>The identifier used by the router when transmitting packets on the MLP bundle:</p> <ul style="list-style-type: none"> • [null]—Negotiation is conducted without using an endpoint discriminator. (No CLI command is generated.) • Hostname—The hostname of the router. This option is useful when multiple routers are using the same username to authenticate but have different hostnames. • IP—A defined IP address. Enter the address or the name of a network/host object, or click Select to select it. If the object that you want is not listed, click the Create button to create it. • MAC—The MAC address of a specific interface. Enter the name of the interface or interface role, or click Select to select it. If the object that you want is not listed, click the Create button to create it. • None—Negotiation is conducted without using an endpoint discriminator. (The relevant CLI command is generated, but no endpoint discriminator is provided.) This option is useful when the router is connected to a malfunctioning peer that does not handle the endpoint discriminator properly. • Phone—An E.164-compliant telephone number. Enter the number in the field displayed. • String—A character string. Enter the string in the field displayed. <p>The default endpoint discriminator is either the globally configured hostname, or the PAP username or CHAP hostname (depending on the authentication protocol being used), if you have configured those values on the PPP tab.</p>
MRRU Local Peer	<p>The maximum receive reconstructed unit (MRRU) value of the local peer. This value represents the maximum size packet that the local router is capable of receiving.</p> <p>Valid values range from 128 to 16384 bytes. The default is the maximum transmission unit (MTU) of the multilink group interface and 1524 bytes for all other interfaces.</p>
MRRU Remote Peer	<p>The maximum receive reconstructed unit (MRRU) value of the remote peer. This value represents the maximum size packet that the remote peer is capable of receiving.</p> <p>Valid values range from 128 to 16384 bytes. The default is 1524 bytes.</p>
Maximum FIFO Queue Size	<p>The maximum queue depth when the bundle uses first-in, first-out (FIFO) queuing. Valid values range from 2 to 255 packets. The default is 8.</p>
Maximum QoS Queue Size	<p>The maximum queue depth when the bundle uses non-FIFO queuing. Valid values range from 2 to 255 packets. The default is 2.</p>