Chapter 13

Configuring Transparent Bridging

This chapter provides an introduction to transparent bridging and describes how to configure transparent bridging on E-series routers.

This chapter contains the following sections:

Overview

This section introduces important concepts that you need to understand before configuring transparent bridging. These concepts include:

- How Transparent Bridging Works
- Bridge Groups and Bridge Group Interfaces
- Bridge Interface Types and Supported Configurations
- Subscriber Policies
- Concurrent Routing and Bridging
- Transparent Bridging and VPLS
- Unsupported Features

How Transparent Bridging Works

A *transparent bridge* is a data-link layer (layer 2) relay device that connects two or more networks or network systems. When a transparent bridge powers up, it automatically begins learning the network topology by examining the media access control (MAC) source address of every incoming packet. The bridge then creates an entry in the forwarding table consisting of the address and associated interface where the packet was received.

More specifically, a transparent bridge performs all of the following actions to learn the network topology:

- Learning—The bridge examines the MAC address of every incoming packet, records the MAC address and associated interface in the forwarding table, and manages the database of MAC addresses and their associated interfaces.
- Flooding—When a packet's destination address does not match any entries in the forwarding table, the bridge transmits (floods) the packet on all bridge interfaces to all network segments except the interface on which the packet was received.
- Forwarding—Once the bridge has learned a packet's destination address (that is, has a matching entry in its forwarding table), the bridge uses the associated port and interface information to send the packet toward its destination.
- Filtering—If the bridge detects that a packet's source and destination addresses are on the same network segment, it ignores (filters) that packet. *Filtering* is the process by which the bridge can screen network traffic for certain characteristics and determine whether to forward or discard (drop) that traffic based on user-defined criteria. On E-series routers, filtering criteria can include the MAC source address, MAC destination address, and protocol type.
- Aging—When a bridge adds a dynamic (learned) MAC address entry to the forwarding table, it assigns an age to the entry. The bridge updates this age each time it receives a packet. To manage MAC entries more efficiently, you can configure an entry's aging time, which is the maximum time that an entry can remain in the forwarding table before it "ages out."

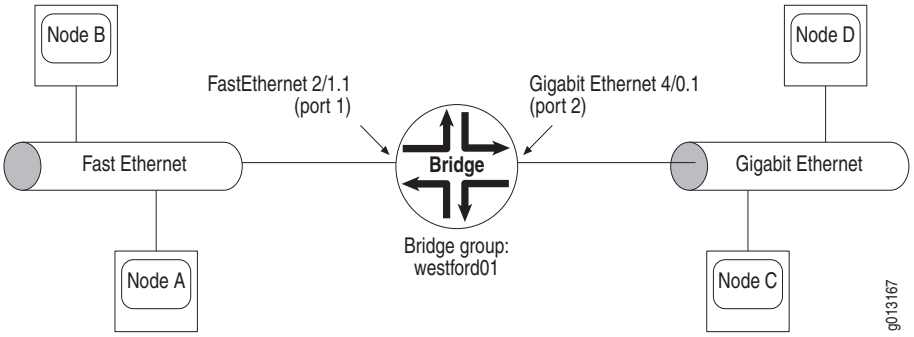
Bridge Groups and Bridge Group Interfaces

You configure transparent bridging by creating one or more bridge groups on the router. A *bridge group* is a collection of network interfaces (ports) that forms a broadcast domain. Each bridge group has its own set of forwarding tables and filters and, as such, functions as a logical transparent bridging device. For information about the maximum number of bridge groups that you can configure per E-series router, see *JUNOSe Release Notes*, *Appendix A*, *System Maximums*.

After you create a bridge group, you associate one or more network interfaces with the bridge group. This association is called a *bridge group interface*, or simply *bridge interface*. For information about the maximum number of bridge interfaces that you can configure per line module and per E-series router, see *JUNOSe Release Notes*, *Appendix A*, *System Maximums*.

Figure 38 shows an example of a simple transparent bridging network configuration that illustrates the concepts discussed so far in this section.

Figure 38: Bridge Group with Fast Ethernet and Gigabit Ethernet Bridge Interfaces



In Figure 38, a bridge group named westford01 is configured on the E-series router, which allows the router to function as a transparent bridge between a Fast Ethernet LAN segment and a Gigabit Ethernet LAN segment. The bridge group includes two bridge interfaces. The bridge interface associated with port 1 is stacked on a VLAN subinterface over a Fast Ethernet interface. The bridge interface associated with port 2 is stacked on a VLAN subinterface over a Gigabit Ethernet interface.

Table 21 presents a simple representation of the forwarding table for bridge group westford01.

Table 21: Sample Bridge Group Forwarding Table

Port	Source Address	Interface
1	Node A	Fast Ethernet 2/1.1
1	Node B	Fast Ethernet 2/1.1
2	Node C	Gigabit Ethernet 4/0.1
2	Node D	Gigabit Ethernet 4/0.1

Bridge Interface Types and Supported Configurations

A bridge interface can be configured as one of the following types:

- Subscriber (client)—A subscriber (client) bridge interface is *downstream* from the traffic flow; that is, the traffic flow direction is from the server (trunk) to the client (subscriber). This is the default bridge group interface type.

- Trunk (server)—A trunk (server) bridge interface is *upstream* from the traffic flow; that is, the traffic flow direction is from the client (subscriber) to the server (trunk). To configure a trunk bridge group interface, you must specify the **subscriber-trunk** keyword as part of the **bridge-group** command.

You can configure bridge interfaces to add transparent bridging capabilities to your existing network configurations. Currently, bridge interfaces can be stacked on:

- Bridged Ethernet over ATM 1483 subinterfaces
- Fast Ethernet interfaces
- Gigabit Ethernet interfaces
- 10-Gigabit Ethernet interfaces
- VLAN subinterfaces over Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or bridged Ethernet interfaces

For sample configurations that include bridge interfaces, see *Configuration Examples* on page 413. For information about configuring Ethernet, ATM, and bridged Ethernet interfaces, see:

- *Chapter 1, Configuring ATM*
- *Chapter 5, Configuring VLAN and S-VLAN Subinterfaces*
- *Chapter 12, Configuring Bridged Ethernet*
- *JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*

Subscriber Policies

To enable intelligent flooding of packets within a bridge group's broadcast domain, each bridge group interface you create is associated with a default subscriber policy. A *subscriber policy* is a set of forwarding and filtering rules that defines how the bridge group interface handles various packet or attribute types, as follows:

- For each packet type, the subscriber policy specifies whether you want the bridge group interface to permit (forward) or deny (filter or drop) packets of that type.
- For the relearn attribute, the subscriber policy specifies whether the bridge interface can relearn a MAC address entry on a different interface from the one initially associated with this entry in the forwarding table. Permit indicates that relearning is allowed, and deny indicates that relearning is prohibited.

The router provides two default subscriber policies: default Subscriber for subscriber (client) bridge interfaces, and default Trunk for trunk (server) bridge interfaces.

Table 22 lists the default values for each packet or attribute type defined in the default Subscriber and default Trunk policies. The only difference between the two policies is how broadcast packets and packets with unknown unicast destination addresses (DAs) are handled.

Table 22: Default Subscriber Policies for Bridge Group Interfaces

Packet/Attribute Type	Default Subscriber Policy	Default Trunk Policy
ARP	Permit	Permit
Broadcast	Deny	Permit
IP	Permit	Permit
MPLS	Permit	Permit
Multicast	Permit	Permit
PPPoE	Permit	Permit
Relearn	Permit	Permit
Unicast (user-to-user)	Permit	Permit
Unknown unicast DA	Deny	Permit
Unknown protocol	Permit	Permit

You cannot change the default subscriber policy values listed in Table 22 for a trunk bridge interface. You can, however, configure a nondefault subscriber policy for a subscriber bridge interface to change the default permit or deny value for one or more packet or attribute types. For details, see *Configuring Subscriber Policies* on page 406.

Concurrent Routing and Bridging

After you create the necessary bridge groups and bridge interfaces for your network configuration, you can use the **bridge crb** command to enable concurrent routing and bridging (CRB) for all bridge groups configured on your router. When CRB is enabled, the router can route a protocol among a group of interfaces in one bridge group and concurrently bridge the same protocol among a separate group of interfaces in a different bridge group on the router.

The router does not switch the protocol between the two bridge groups. Instead, it confines routed traffic to the routed interfaces and bridged traffic to the bridged interfaces. As a result, a protocol can be either routed or bridged on a particular interface, but cannot be both routed and bridged on the same interface.

By default, CRB is disabled for all bridge groups on the router. When you use the **bridge crb** command to enable CRB, it takes effect for all bridge groups currently configured on your router; you cannot enable CRB for some bridge groups on the router but not for others.

When you first enable CRB, the router issues an implicit **bridge route** command for any IP, MPLS, or PPPoE interfaces that are currently configured in the interface stack for the bridge group. This command directs the bridge group to route traffic for these protocols. After CRB has been enabled, you must issue an explicit **bridge route** command to route any new IP, MPLS, or PPPoE interface that is the first occurrence of this protocol in the bridge group. (See *Configuring Explicit Routing* on page 411 for details about using the **bridge route** command.)

As a result, it is important that you issue the **bridge crb** command after you configure all bridge group interfaces. In this way, the router can detect all IP, MPLS, or PPPoE interfaces in your configuration and direct the bridge group to route traffic from these protocols.

Transparent Bridging and VPLS

Except for the **bridge crb** and **bridge route** commands, you can use the existing transparent bridging commands to configure one or more instances of the Virtual Private LAN Service (VPLS), referred to as *VPLS instances*, on the router. VPLS employs a layer 2 virtual private network (VPN) to connect multiple individual LANs across a service provider's MPLS core network. The geographically dispersed multiple LANs functions as a single virtual LAN.

A single VPLS instance is analogous to a bridge group, and performs similar functions. In effect, a VPLS instance is a new or existing bridge group that has additional VPLS attributes configured.

For details about configuring and using VPLS, see *JUNOSe BGP and MPLS Configuration Guide, Chapter 8, Configuring VPLS*.

Unsupported Features

The current E-series implementation of transparent bridging does not support the spanning-tree algorithm as defined in IEEE 802.1D.

NOTE: Because the spanning-tree algorithm is not currently supported, make sure that your topology avoids the creation of network loops.

Platform Considerations

You can configure transparent bridging on the following E-series routers:

- E120 router
- E320 router
- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

Module Requirements

For information about the modules that support transparent bridging on ERX-14xx models, ERX-7xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support transparent bridging.

For information about the modules that support transparent bridging on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support transparent bridging.

Interface Specifiers

The configuration task examples in this chapter use the *slot*/*port*[.*subinterface*] format to specify the physical interface on which to configure transparent bridging. However, the interface specifier format that you use depends on the router that you are using.

For ERX-7xx models, ERX-14xx models, and ERX-310 routers, use the *slot*/*port*[.*subinterface*] format. For example, the following command specifies ATM 1483 subinterface 10 on slot 0, port 1 of an ERX-7xx model, ERX-14xx model, or ERX-310 router.

```
host1(config)#interface atm 0/1.10
```

For E120 and E320 routers, use the *slot*/*adapter*/*port*[.*subinterface*] format, which includes an identifier for the bay in which the I/O adapter (IOA) resides. In the software, adapter 0 identifies the right IOA bay (E120 router) and the upper IOA bay (E320 router); adapter 1 identifies the left IOA bay (E120 router) and the lower IOA bay (E320 router). For example, the following command specifies ATM 1483 subinterface 20 on slot 5, adapter 0, port 0 of an E320 router.

```
host1(config)#interface atm 5/0/0.20
```

For more information about supported interface types and specifiers on E-series routers, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.

References

For more information about transparent bridging, consult the following resources:

- IEEE 802.1D—Media access control (MAC) bridges
- Draft Standard P802.1Q/D9 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
- RFC 1493—Definitions of Managed Objects for Bridges (July 1993)

Before You Configure Transparent Bridging

Before you configure transparent bridging on an E-series router, verify that:

- You have correctly installed a line module that supports transparent bridging. For a list of the line modules that support transparent bridging, see *ERX Module Guide, Appendix A, Module Protocol Support* or *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support transparent bridging.
- Each configured line can transmit data to and receive data from your switch connections.

Table 23 lists the prerequisite tasks for configuring transparent bridging and the resources that you can consult to learn how to perform these tasks.

Table 23: Prerequisite Tasks for Configuring Transparent Bridging

To Learn About	See
Preconfiguration and hardware diagnostic procedures	*ERX Hardware Guide* *E120 and E320 Hardware Guide*
Configuring T3 ATM line modules	*JUNOSe Physical Layer Configuration Guide, Chapter 2, Configuring T3 and E3 Interfaces*
Configuring OCx/STMx ATM line modules	*JUNOSe Physical Layer Configuration Guide, Chapter 3, Configuring Unchannelized OCx/STMx Interfaces*
Configuring Ethernet line modules	*JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*

Also have the following information available:

- A diagram of your network topology indicating the names of the bridge groups and bridge group interfaces that you need to create
- On ERX-7xx models, ERX-14xx models, and ERX-310 routers, the slot and port numbers of the line modules over which you want to configure transparent bridging
- On E120 and E320 routers, slot, adapter, and port numbers of the IOAs over which you want to configure transparent bridging
- Types and specifiers for the interfaces and subinterfaces over which you want to create bridge group interfaces

Configuration Tasks

To configure transparent bridging on an E-series router:

1. Create a bridge group.
2. (Optional) Set optional attributes for the bridge group.
3. Configure bridge group interfaces.
4. (Optional) Configure nondefault subscriber policies for bridge interfaces.
5. (Optional) Enable concurrent routing and bridging.
6. (Optional) If CRB is enabled, configure explicit routing for IP, MPLS, or PPPoE protocols.

The following sections describe how to perform each of these tasks. See *Configuration Examples* on page 413 for detailed sample configurations.

NOTE: For information about the maximum values that the router supports for transparent bridging, see *JUNOSe Release Notes*, *Appendix A*, *System Maximums*.

Creating Bridge Groups

To create a bridge group:

1. From Global Configuration mode, create a bridge group and give it an alphanumeric name.

   host1(config)#**bridge westford01**

NOTE: Do not assign the bridge group the same name as an existing VR configured on your router.

2. (Optional) Repeat Step 1 to create additional bridge groups, one at a time.

   host1(config)#**bridge westford02**
   host1(config)#**bridge westford03**

3. (Optional) Use the appropriate **show** command to verify the bridge group creation.

   host1#**show bridge groups**

bridge

- Use to create a bridge group for transparent bridging.
- You must specify an alphanumeric name for the bridge group; the name can be a maximum of 32 characters and can use any combination of alphanumeric characters.

- Example

  host1(config)#**bridge westford04**

- Use the **no** version to remove the bridge group from the router.

Configuring Optional Bridge Group Attributes

After you create a bridge group, you can configure the following optional attributes for the bridge group to manage the MAC address entries in the bridge group's forwarding table:

- Enable or disable the bridge group's ability to acquire dynamically learned MAC addresses; acquiring dynamic MAC addresses is enabled by default.

  host1(config)#**bridge westford01 acquire**

- Enable or disable the bridge group's ability to filter (forward or discard) frames with a particular MAC source or destination address.

  host1(config)#**bridge westford01 address 0090.1a40.4c7c forward atm 3/0.1**
  host1(config)#**bridge westford02 address 1011.22c2.333d discard**

- Set the aging time of a dynamic (learned) entry in the forwarding table.

  host1(config)#**bridge westford01 aging-time 200**

- Set the maximum number of dynamic MAC addresses that a bridge group can learn.

  host1(config)#**bridge westford02 learn 10000**

You can also optionally enable SNMP link status processing for the bridge group. For example:

host1(config)#**bridge westford03 snmp-trap link-status**

bridge acquire

- Use to enable or disable a specified bridge group's ability to acquire dynamically learned MAC addresses; acquiring dynamic MAC addresses is enabled by default.
- Enables the bridge group to forward any frames it receives for nodes (stations) whose address it has learned dynamically.
- Example

  host1(config)#**bridge westford01 acquire**

- Use the **no** version to prevent the bridge group from acquiring dynamically learned MAC addresses and to limit forwarding only to those nodes that have a statically configured address entry in the forwarding table.

bridge address

- Use to enable or disable a specified bridge group's ability to filter (forward or discard) frames based on their MAC address.
- Enables the bridge group to filter frames by their MAC address and add static (nonlearned) address entries to the forwarding table.
- Specify the following:
  - *bridgeGroupName*—Alphanumeric name of the bridge group specified in the **bridge** command
  - *macAddress*—Unique 48-bit (6-byte) physical address or hardware address of the LAN network interface card as a dotted triple of four-digit hexadecimal numbers
- Specify one of the following filter types:
  - **forward**—Forwards frames destined for the specified MAC address out the specified interface
  - **discard**—Discards (drops) frames sent from or destined for the specified MAC address without further processing
- If you use the **forward** keyword, you must additionally specify the following:
  - *interfaceType*—One of the following bridge interface types listed in *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*:
    - **atm**
    - **fastEthernet**
    - **gigabitEthernet**
    - **tenGigabitEthernet**
  - *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide* for information
- Example 1—Forwards frames destined for the node with MAC address 0090.1a40.4c7c out the specified Fast Ethernet interface

  host1(config)#**bridge westford02 address 0090.1a40.4c7c forward fastEthernet 3/0.1**

- Example 2—Drops frames sent from or destined for the node with MAC address 1011.22b2.333c

  host1(config)#**bridge westford03 address 1011.22b2.333c discard**

- Use the **no** version to remove the static MAC address entry from the forwarding table.

bridge aging-time

- Use to set the length of time, in seconds, that a dynamic (learned) MAC address entry can remain in a specified bridge group's forwarding table.
- When a dynamic entry reaches its configured aging time, it "ages out" of the forwarding table.
- The default aging time is 300 seconds.

- The aging-time range is 1–1000000 seconds.
- Example

  host1(config)#**bridge westford04 aging-time 1000**

- Use the **no** version to restore the default value, 300 seconds.

bridge learn

- Use to set the maximum number of dynamic (learned) MAC address entries that a specified bridge group can learn.
- For information about the maximum number of learned MAC address entries combined for all bridge groups on an E-series router, see *JUNOSe Release Notes, Appendix A, System Maximums*.
- The default value is 0 (zero) learned addresses. This default implies that there is no maximum number of learned entries for an individual bridge group; that is, an individual bridge group can learn an unlimited number of MAC addresses, up to the maximum number that the router supports.
- Example

  host1(config)#**bridge westford05 learn 2000**

- Use the **no** version to restore the default value, 0 (zero) learned addresses.

bridge snmp-trap link-status

- Use to enable SNMP link status processing for a specified bridge group and to enable SNMP traps for all bridge interfaces configured in the bridge group.
- Example

  host1(config)#**bridge westford06 snmp-trap link-status**

- Use the **no** version to disable SNMP link status processing for the bridge group.

Configuring Bridge Group Interfaces

To configure a bridge group interface:

1. From Global Configuration mode, select the ATM, Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet interface or subinterface that you want to assign to the bridge group.
2. Assign the interface or subinterface to an existing bridge group to create the bridge interface.
3. (Optional) Configure the bridge group interface as a trunk (server) interface.
4. (Optional) Enable SNMP link status processing for the bridge group interface.
5. (Optional) Set the maximum number of dynamic MAC addresses that the bridge group interface can learn.

For detailed sample configurations that include bridge interfaces, see *Configuration Examples* on page 413.

bridge-group

- Use to assign a bridge interface to an existing bridge group.
- To create a subscriber (client) bridge group interface, which is the default, you must supply the alphanumeric name of the bridge group (specified in the **bridge** command) to which you want to assign the interface.
- Optionally, you can also choose one of the following keywords:
  - **subscriber-trunk**—Creates a trunk (server) bridge group interface
  - **snmp-trap link-status**—Enables SNMP link status processing for the specified interface in the specified bridge group; SNMP link status processing is disabled by default
  - **learn** *addressCount*—Sets the maximum number of MAC addresses that the bridge group interface can learn, where *addressCount* is an integer in the range 0–64000. A value of 0 indicates that an individual bridge group interface can learn an unlimited number of MAC addresses, up to the maximum number that the router supports.
- Example 1—Creates a subscriber (client) bridge group interface for a bridge group named westford02 with SNMP link status processing enabled

  host1(config-subif)#**bridge-group westford02 snmp-trap link-status**

- Example 2—Sets the maximum number of learned MAC addresses on the westford02 bridge interface to 1000

  host1(config-subif)#**bridge-group westford02 learn 1000**

- Example 3—Creates a trunk (server) interface for a bridge group named westford03

  host1(config-subif)#**bridge-group westford03 subscriber-trunk**

- Use the **no** version to remove the interface from the bridge group and to restore the default value for the keyword you specified.

interface atm

- Use to select an ATM interface or subinterface type.
- Example

  host1(config)#**interface atm 3/2.1**

- Use the **no** version to remove the interface or subinterface.

interface fastEthernet

- Use to select a Fast Ethernet interface.
- Example

  host1(config)#**interface fastEthernet 1/0.2**

- Use the **no** version to remove the interface or subinterface. You must issue the **no** version from the highest level down; you cannot remove an interface or a subinterface if the one above it still exists.

interface gigabitEthernet
interface tenGigabitEthernet

- Use to select a Gigabit Ethernet interface or a 10-Gigabit Ethernet interface.
- Examples

  host1(config)#**interface gigabitEthernet 1/0**
  host1(config)#**interface gigabitEthernet 4/0/1**
  host1(config)#**interface tenGigabitEthernet 4/0/1**

- Use the **no** version to remove the interface or subinterface. You must issue the **no** version from the highest level down; you cannot remove an interface or subinterface if the one above it still exists.

Configuring Subscriber Policies

To configure a nondefault client subscriber policy:

1. From Global Configuration mode, create the subscriber policy and assign it an alphanumeric name.

   host1(config)#**subscriber-policy client01**

   This command accesses Subscriber Policy Configuration mode.

2. From Subscriber Policy Configuration mode, define the rules for each packet or attribute type for which you want to change the default value. (All other packet or attribute types will continue to use the default values listed in Table 22 on page 397.)

   host1(config-policy)#**broadcast permit**
   host1(config-policy)#**multicast deny**
   host1(config-policy)#**relearn deny**

3. Exit Subscriber Policy Configuration mode.

   host1(config-policy)#**exit**

4. From Global Configuration mode, associate the new subscriber policy with the bridge group in which the subscriber (client) interface resides.

   host1(config)#**bridge westford02 subscriber-policy client01**

5. (Optional) Use the appropriate **show** commands to verify the creation of the subscriber policy and its association with the bridge group interface.

   host1#**show subscriber-policy client01**
   host1#**show bridge westford02**

arp

- Use to modify the subscriber policy for ARP to define whether a subscriber (client) bridge interface permits (forwards) or denies (filters or drops) ARP packets.
- Specify one of the following keywords:
  - **permit**—Forwards packets of this type
  - **deny**—Filters or drops packets of this type
- ARP packets are forwarded by default.
- Example

  host1(config-policy)#**arp deny**

- Use the **no** version to restore the default value.

bridge subscriber-policy

- Use to associate a subscriber (client) bridge interface with a nondefault subscriber policy.
- Specify the following:
  - *bridgeGroupName*—Alphanumeric name of the bridge group specified in the **bridge** command
  - *subscriberPolicyName*—Alphanumeric name of the subscriber policy specified in the **subscriber-policy** command
- Example

  host1(config)#**bridge westford02 subscriber-policy client01**

- Use the **no** version to remove the association with the subscriber policy.

NOTE: You cannot change the default subscriber policy values for a trunk (server) bridge interface. As a result, you cannot use the **bridge subscriber-policy** command to associate a nondefault subscriber policy with a trunk bridge interface.

broadcast

- Use to modify the subscriber policy for the broadcast protocol to define whether a subscriber (client) bridge interface permits (forwards) or denies (filters or drops) broadcast packets.
- Specify one of the following keywords:
  - **permit**—Forwards packets of this type
  - **deny**—Filters or drops packets of this type
- Broadcast packets are filtered or dropped by default.
- Example

  host1(config-policy)#**broadcast permit**

- Use the **no** version to restore the default value.

ip

- Use to modify the subscriber policy for IP to define whether a subscriber (client) bridge interface permits (forwards) or denies (filters or drops) IP packets.
- Specify one of the following keywords:
  - **permit**—Forwards packets of this type
  - **deny**—Filters or drops packets of this type
- IP packets are forwarded by default.
- Example

  host1(config-policy)#**ip deny**

- Use the **no** version to restore the default value.

mpls

- Use to modify the subscriber policy for MPLS to define whether a subscriber (client) bridge interface permits (forwards) or denies (filters or drops) MPLS packets.
- Specify one of the following keywords:
  - **permit**—Forwards packets of this type
  - **deny**—Filters or drops packets of this type
- MPLS packets are forwarded by default.
- Example

  host1(config-policy)#**mpls deny**

- Use the **no** version to restore the default value.

multicast

- Use to modify the subscriber policy for the multicast protocol to define whether a subscriber (client) bridge interface permits (forwards) or denies (filters or drops) multicast packets.
- Specify one of the following keywords:
  - **permit**—Forwards packets of this type
  - **deny**—Filters or drops packets of this type
- Multicast packets are forwarded by default.
- Example

  host1(config-policy)#**multicast deny**

- Use the **no** version to restore the default value.

pppoe

- Use to modify the subscriber policy for PPPoE to define whether a subscriber (client) bridge interface permits (forwards) or denies (filters or drops) PPPoE packets.
- Specify one of the following keywords:
  - **permit**—Forwards packets of this type
  - **deny**—Filters or drops packets of this type
- PPPoE packets are forwarded by default.
- Example

  host1(config-policy)#**pppoe deny**

- Use the **no** version to restore the default value.

relearn

- Use to modify the relearning policy for a subscriber (client) bridge interface.
- The **relearn** command defines whether the bridge interface can relearn a MAC address entry on a different interface from the one initially associated with this entry in the forwarding table.
- Specify one of the following keywords:
  - **permit**—Enables relearning
  - **deny**—Prohibits relearning and forces the bridge interface to wait until an entry "ages out" of the forwarding table to relearn it on the new interface
- Relearning is enabled by default.
- Example

  host1(config-policy)#**relearn deny**

- Use the **no** version to restore the default value.

subscriber-policy

- Use to create a nondefault subscriber policy for a subscriber (client) bridge interface.
- A subscriber policy is a set of forwarding and filtering rules that defines how the bridge interface handles various packet types.
- You must specify an alphanumeric name for the subscriber policy; the name can be a maximum of 32 characters and can use any combination of alphanumeric characters.
- Example

  host1(config)#**subscriber-policy client01**

- Use the **no** version to remove the nondefault subscriber policy.

NOTE: You cannot change the default subscriber policy values for a trunk (server) bridge interface. As a result, you cannot use the **subscriber-policy** command to create a nondefault subscriber policy for a trunk interface.

unicast

- Use to modify the subscriber policy for the unicast (user-to-user) protocol to define whether a subscriber (client) bridge interface permits (forwards) or denies (filters or drops) unicast packets.
- Specify one of the following keywords:
  - **permit**—Forwards packets of this type
  - **deny**—Filters or drops packets of this type
- Unicast packets are forwarded by default.
- Example

  host1(config-policy)#**unicast deny**

- Use the **no** version to restore the default value.

unknown-destination

- Use to modify the subscriber policy for packets with unknown unicast DAs to define whether a subscriber (client) bridge interface permits (forwards) or denies (filters or drops) packets with unknown unicast DAs.
- Specify one of the following keywords:
  - **permit**—Forwards packets of this type
  - **deny**—Filters or drops packets of this type
- Packets with unknown unicast DAs are filtered or dropped by default.
- Example

  host1(config-policy)#**unknown-destination permit**

- Use the **no** version to restore the default value.

unknown-protocol

- Use to modify the subscriber policy for packets containing an unknown protocol to define whether a subscriber (client) bridge interface permits (forwards) or denies (filters or drops) these packets.
- An unknown protocol is any protocol other than ARP, IP, MPLS, or PPPoE.
- Specify one of the following keywords:
  - **permit**—Forwards packets of this type
  - **deny**—Filters or drops packets of this type
- Packets containing an unknown protocol are forwarded by default.
- Example

  host1(config-policy)#**unknown-protocol deny**

- Use the **no** version to restore the default value.

Enabling Concurrent Routing and Bridging

To enable concurrent routing and bridging (CRB) for all bridge groups on the router:

1. From Global Configuration mode, issue the **bridge crb** command.

   host1(config)#**bridge crb**

2. (Optional) Use the appropriate **show** command to verify that CRB is enabled for the bridge groups on your router.

   host1#**show bridge groups details**

bridge crb

- Use to enable concurrent routing and bridging (CRB) for all bridge groups configured on an E-series router.
- CRB is disabled by default.
- When CRB is enabled, the router can route a protocol among a group of interfaces in one bridge group and concurrently bridge the same protocol among a separate group of interfaces in a different bridge group.
- The command takes effect for all bridge groups on an E-series router; you cannot enable CRB for some bridge groups on the router but not for others.
- Example

  host1(config)#**bridge crb**

- Use the **no** version to disable CRB on all bridge groups and restore the default bridging capability.

Configuring Explicit Routing

After you enable concurrent routing and bridging, you may need to issue the **bridge route** command to configure explicit routing for IP, MPLS, or PPPoE protocols if both of the following conditions are true:

- You configure new IP, MPLS, or PPPoE interfaces after you issue the **bridge crb** command to enable concurrent routing and bridging.
- The IP, MPLS, or PPPoE interface is the first occurrence of this protocol in the bridge group.

For example, assume that you want to route (rather than bridge) IP, MPLS, and PPPoE interfaces, but only IP and MPLS interfaces are configured when you issue the **bridge crb** command. The router detects the IP and MPLS interfaces and issues implicit **bridge route** commands to route these protocols.

If you subsequently add a new IP interface to a bridge group, you do not need to issue the **bridge route** command because the implicit **bridge route** command for IP is still in effect. However, if you subsequently add a new PPPoE interface to the bridge group, you must issue an explicit **bridge route** command for PPPoE to direct the bridge group to route PPPoE packets.

You can also use the **bridge route** command as a way to filter packets by routing. If you issue an explicit **bridge route** command for a protocol that is not currently configured in any of your bridge groups, the bridge group must route rather than bridge that protocol, but does not have the required interface stacking to do so. As a result, the bridge group discards (drops) those packets.

To configure explicit routing:

1. Ensure that you have enabled concurrent routing and bridging. (See *Enabling Concurrent Routing and Bridging* on page 411 for details.)

2. From Global Configuration mode, enable routing of IP, MPLS, or PPPoE packets in a specified bridge group.

   host1(config)#**bridge westford02 route ip**
   host1(config)#**bridge westford02 route mpls**
   host1(config)#**bridge westford03 route pppoe**

3. (Optional) Use the appropriate **show** command to verify that routing is enabled for the specified protocols in the bridge group.

   host1#**show bridge westford02**

bridge route

- Use to enable the routing of IP, MPLS, or PPPoE packets in a specified bridge group when concurrent routing and bridging (CRB) is enabled.
- If you issue this command for a protocol that is not configured in any bridge groups on your router, the bridge group discards (drops) those packets.
- You must specify the alphanumeric name of the bridge group specified in the **bridge** command.
- Choose one of the following keywords to indicate the protocol type that the bridge group routes: **ip**, **mpls**, or **pppoe**.
- Example

  host1(config)#**bridge westford02 route ip**

- Use the **no** version to disable routing of the specified protocol in the specified bridge group.

Configuration Examples

This section provides examples that show how to configure transparent bridging on the router. With each step, an illustration shows how the router is building the interface column.

Example 1: Bridging with Bridged Ethernet

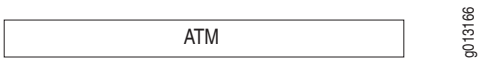
The following example illustrates how to configure transparent bridging with bridged Ethernet.

1. Create the bridge group.

   host1(config)#**bridge westford01**

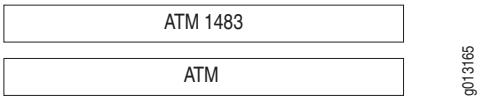
2. Create an ATM major interface.

   host1(config)#**interface atm 3/3**



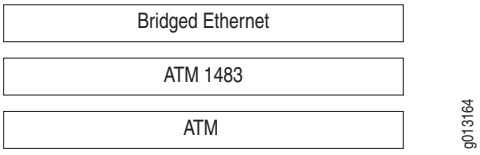
3. Create an ATM 1483 subinterface and associated PVC.

   host1(config-if)#**interface atm 3/3.1**
   host1(config-subif)#**atm pvc 1 0 10 aal5snap**



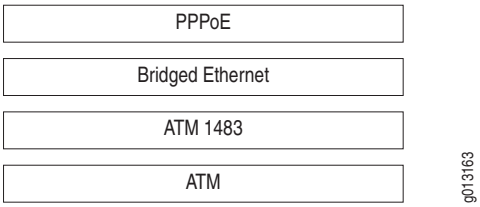
4. Specify bridged Ethernet as the encapsulation method on the subinterface. The **encapsulation** keyword implies that the bridged Ethernet interface is the only interface stacked directly above the ATM 1483 subinterface. As a result, the bridged Ethernet interface cannot have a peer interface stacked above the same lower-layer interface.

   host1(config-subif)#**encapsulation bridge1483**



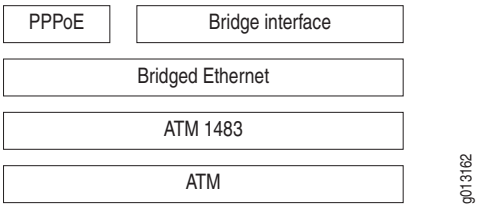
5. Create a PPPoE major interface over the bridged Ethernet interface. Because this command does not use the **encapsulation** keyword, the PPPoE interface can have one or more peer interfaces stacked above the same bridged Ethernet interface.

   host1(config-subif)#**pppoe**



6. Configure a subscriber (client) bridge group interface over the bridged Ethernet interface as a peer to the PPPoE interface. Assign the interface to the bridge group you created in Step 1.

   host1(config-subif)#**bridge-group westford01**



Example 2: Bridging with VLANs

The following example illustrates how to configure transparent bridging with VLANs over a Fast Ethernet interface.

NOTE: You can also configure transparent bridging with VLANs over a bridged Ethernet interface. For information, see *Configuring VLANs over Bridged Ethernet* in *Chapter 12, Configuring Bridged Ethernet*.

1. Create the bridge group.

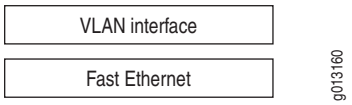
   host1(config)#**bridge westford02**

2. Create a Fast Ethernet interface.

   host1(config)#**interface fastEthernet 2/0**

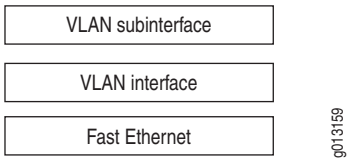
3. Create a VLAN major interface by specifying VLAN as the encapsulation method for the interface.

   host1(config-if)#**encapsulation vlan**



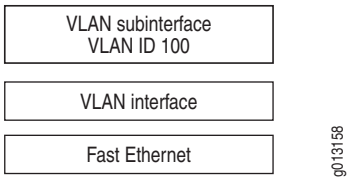
4. Create a VLAN subinterface by adding a subinterface number to the **interface fastEthernet** command.

   host1(config-if)#**interface fastEthernet 2/0.1**



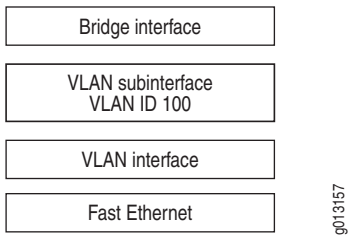
5. Assign a unique VLAN ID to the VLAN subinterface.

   host1(config-if)#**vlan id 100**



6. Configure a subscriber (client) bridge group interface over the VLAN subinterface. Assign the interface to the bridge group you created in Step 1.

   host1(config-subif)#**bridge-group westford02**



7. Exit Subinterface Configuration mode.

   host1(config-subif)#**exit**

8. (Optional) Configure additional VLAN subinterfaces and bridge group interfaces by repeating Steps 4 through 6, supplying unique values.

Monitoring Transparent Bridging

This section describes how to:

- Set a statistics baseline for bridge groups and bridge interfaces.
- Remove all dynamic MAC address entries or a specific dynamic MAC address entry from the forwarding table for bridge groups and bridge interfaces.
- Use the **show** commands to monitor bridge groups, bridge group interfaces, and subscriber policies

NOTE: The E120 router and E320 router output for **monitor** and **show** commands is identical to output from other E-series routers, except that the E120 and E320 router output also includes information about the adapter identifier in the interface specifier (*slot/adapter/port*).

Setting Statistics Baselines

You can set a statistics baseline for a bridge group (by using the **baseline bridge** command) or for a bridge interface (by using the **baseline bridge interface** command).

baseline bridge

- Use to set a statistics baseline for a specified bridge group.
- The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Example

  host1#**baseline bridge westford03**

- There is no **no** version.

baseline bridge interface

- Use to set a statistics baseline for a particular network interface belonging to a bridge group.
- The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.

- You must specify the following:
  - *interfaceType*—One of the following bridge interface types listed in *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*:
    - **atm**
    - **fastEthernet**
    - **gigabitEthernet**
    - **tenGigabitEthernet**
  - *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide* for information
- Example

  host1#**baseline bridge interface atm 3/3.1**

- There is no **no** version.

Removing Dynamic MAC Address Entries

You can remove all dynamic (learned) MAC address entries from the forwarding table for a bridge group (using the **clear bridge** command) or for a bridge interface (using the **clear bridge interface** command). You can also use the **clear bridge address** command to remove a specific dynamic MAC address entry from the forwarding table for a bridge group.

clear bridge

- Use to remove all dynamic MAC address entries from the forwarding table for the specified bridge group.
- Example

```
host1#show bridge westford01 table
  Bridge: westford01 MAC Address Table
   Address         Action         Interface          Age
--------------   ----------   -------------------   -----
0090.1a01.0205   forward      ATM3/3.1               0
1234.abcd.5678   discard      ---                    ---

host1#clear bridge westford01

host1#show bridge westford01 table
  Bridge: westford01 MAC Address Table
   Address         Action         Interface          Age
--------------   ----------   -------------------   -----
```

- There is no **no** version.

clear bridge address

- Use to remove a specific dynamic MAC address entry from the forwarding table for the specified bridge group.
- Example

```
host1#show bridge westford01 table
  Bridge: westford01 MAC Address Table
   Address         Action         Interface          Age
--------------   ----------   -------------------   -----
0090.1a01.0205   forward      ATM3/3.1               0
1234.abcd.5678   discard      ---                    ---

host1#clear bridge westford01 address 1234.abcd.5678

host1#show bridge westford01 table
  Bridge: westford01 MAC Address Table
   Address         Action         Interface          Age
--------------   ----------   -------------------   -----
0090.1a01.0205   forward      ATM3/3.1               0
```

- There is no **no** version.

clear bridge interface

- Use to remove all dynamic MAC address entries for a network interface belonging to a bridge group from the forwarding table for that bridge group.
- You must specify the following:
  - *interfaceType*—One of the following bridge interface types listed in *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*:
    - **atm**
    - **fastEthernet**
    - **gigabitEthernet**
    - **tenGigabitEthernet**
  - *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide* for information
- Example

```
host1#show bridge westford02 table dynamic
  Bridge: westford02 MAC Address Table
   Address         Action         Interface          Age
--------------   ----------   -------------------   -----
0090.1a01.0205   forward      ATM3/3.1               0
0090.1a01.0206   forward      ATM3/3.2              10
0090.1a01.0207   forward      ATM3/3.3               5

host1#clear bridge interface atm 3/3.2

host1#show bridge westford02 table dynamic
  Bridge: westford02 MAC Address Table
   Address         Action         Interface          Age
--------------   ----------   -------------------   -----
0090.1a01.0205   forward      ATM3/3.1               0
0090.1a01.0207   forward      ATM3/3.3               5
```

- There is no **no** version.

Monitoring Bridge Groups

You can use **show** commands to display information about the bridge groups configured on your router.

show bridge

- Use to display configuration and statistics information for the specified bridge group.
- To display information about the MAC address table and bridge interfaces, use the **all** keyword.
- Field descriptions
  - BridgeGroup—Name assigned to the bridge group
  - Bridge Mode—Bridging capability currently enabled, either concurrent routing and bridging (CRB) or default bridging
  - Aging Time—Length of time, in seconds, that a MAC address entry can remain in the forwarding table
  - Learning—Whether acquisition of dynamically learned MAC addresses is currently enabled or disabled
  - Max Learn—Maximum number of dynamic MAC addresses that the bridge group can learn
  - Link Status Snmp Traps—Whether SNMP link status processing is enabled or disabled for all bridge interfaces in the bridge group
  - Subscriber Policy—Name of the subscriber policy currently in effect for the bridge group
  - Protocol Actions—When CRB is enabled, displays the protocols (IP, MPLS, or PPPoE) for which explicit routing has been configured
  - Port Count—Number of ports (interfaces) currently configured for the bridge group; this value typically matches the Interface Count
  - Interface Count—Number of bridge group interfaces currently configured for the bridge group
  - Address Table—Displays the current static and dynamic entries in the MAC address table
    - Address—MAC address of the entry
    - Action—How the bridge group handles this entry: forward or discard
    - Interface—Interface type and specifier on which the entry will be forwarded; this value does not appear for entries that are discarded
    - Age—Length of time that a dynamic entry has been in the forwarding table; this value does not appear for static entries

- Interfaces—Displays statistics information for each bridge group interface; the entries for each interface are preceded by the interface type and specifier (for example, ATM3/3.1)
  - Port Number—Bridge group port number on which this interface resides
  - Operational Status—Operational status of the physical interface: Up, Down, LowerLayerDown, NotPresent
  - Admin Status—State of the physical interface: Up, Down
  - Snmp Link Status Trap—Whether SNMP link status processing is enabled or disabled for the specified bridge interface
  - Max Learn—Maximum number of dynamic MAC addresses that the bridge group interface can learn
  - Subscriber Policy—Name of the subscriber policy currently in effect for the bridge group interface
  - In Octets—Number of octets received on this interface
  - In Frames—Number of frames received on this interface
  - In Discards—Number of incoming packets discarded on this interface
  - In Errors—Number of incoming errors received on this interface
  - Out Octets—Number of octets transmitted on this interface
  - Out Frames—Number of frames transmitted on this interface
  - Out Discards—Number of outgoing packets discarded on this interface
  - Out Errors—Number of outgoing errors on this interface
  - queue—Hardware packet queue associated with the specified traffic class and interface
  - Queue length—Length of the queue, in bytes
  - Forwarded packets, Bytes—Number of packets and bytes forwarded on this queue
  - Dropped committed packets, Bytes—Number of committed packets and bytes that were dropped
  - Dropped conformed packets, Bytes—Number of conformed packets and bytes that were dropped
  - Dropped exceeded packets, Bytes—Number of exceeded packets and bytes that were dropped

- Example 1—Displays configuration settings for the specified bridge group

```
host1#show bridge westford01
  BridgeGroup: westford01
        Bridge Mode:            CRB
        Aging Time:             300 secs
        Learning:               Enabled
        Max Learn:              Unlimited
        Link Status Snmp Traps: Disabled
        Subscriber Policy:      default Subscriber
        Protocol Actions:
           Route  IP
           Route  PPPoE
        Port Count:             1
        Interface Count:        1
```

- Example 2—Displays information about configuration settings, MAC address table entries, and bridge group interfaces for the specified bridge group

```
host1#show bridge westford01 all
  BridgeGroup: westford01
        Bridge Mode:            CRB
        Aging Time:             300 secs
        Learning:               Enabled
        Max Learn:              Unlimited
        Link Status Snmp Traps: Disabled
        Subscriber Policy:      default Subscriber
        Protocol Actions:
           Route  IP
           Route  PPPoE
        Port Count:             1
        Interface Count:        1

  Address Table:
   Address         Action         Interface          Age
--------------   ----------   -------------------   -----
1011.22b2.333c   forward      ATM3/3.1               ---
1234.abcd.5678   discard      ---                    ---

  Interfaces:
    ATM3/3.1
      Port Number: 1
      Operational Status: LowerLayerDown
      Admin Status: Up
      Snmp Link Status Trap: Disabled
      Max Learn: Unlimited
      Subscriber Policy: default Subscriber
      Statistics:
         In Octets:    0
         In Frames:    0
         In Discards:  0
         In Errors:    0
         Out Octets:   0
         Out Frames:   0
         Out Discards: 0
         Out Errors:   0
      queue 0: traffic class best-effort, bound to bridge     ATM3/3.1
        Queue length 0 Bytes
        Forwarded packets 0, Bytes 0
        Dropped committed packets 0, Bytes 0
        Dropped conformed packets 0, Bytes 0
        Dropped exceeded packets 0, Bytes 0
```

show bridge groups

- Use to display configuration information for all bridge groups currently configured on your router.
- To display the configuration settings for all bridge groups on your router, use the **details** keyword.
- Field descriptions
  - BridgeGroup—Name assigned to the bridge group
  - Bridge Mode—Bridging capability currently enabled, either concurrent routing and bridging (CRB) or default bridging
  - Aging Time—Length of time, in seconds, that a MAC address entry can remain in the forwarding table
  - Learning—Whether acquisition of dynamically learned MAC addresses is currently enabled or disabled
  - Max Learn—Maximum number of dynamic MAC addresses that the bridge group can learn
  - Link Status Snmp Traps—Whether SNMP link status processing is enabled or disabled for all bridge interfaces in the bridge group
  - Subscriber Policy—Name of the subscriber policy currently in effect for the bridge group
  - Protocol Actions—When CRB is enabled, displays the protocols (IP, MPLS, or PPPoE) for which explicit routing has been configured
  - Port Count—Number of ports (interfaces) currently configured for the bridge group; this value typically matches the Interface Count
  - Interface Count—Number of bridge group interfaces currently configured for the bridge group
- Example 1—Displays the names of the bridge groups configured on your router

```
host1#show bridge groups
  BridgeGroup: westford02
  BridgeGroup: westford01
```

- Example 2—Displays the configuration settings for each bridge group on your router

```
host1#show bridge groups details
  BridgeGroup: westford02
        Bridge Mode:            CRB
        Aging Time:             300 secs
        Learning:               Enabled
        Max Learn:              Unlimited
        Link Status Snmp Traps: Disabled
        Subscriber Policy:      client01
        Protocol Actions:
           Route  IP
           Route  PPPoE
        Port Count:             0
        Interface Count:        0
```

```
BridgeGroup: westford01
      Bridge Mode:            CRB
      Aging Time:             300 secs
      Learning:               Enabled
      Max Learn:              Unlimited
      Link Status Snmp Traps: Disabled
      Subscriber Policy:      default Subscriber
      Protocol Actions:
      Port Count:             1
      Interface Count:        1
```

show bridge port

- Use to display configuration, statistics, and status information for all ports (interfaces) or for a specified port associated with a bridge group.
- To display only the port number, interface identifier, and status for each port, use the **brief** keyword.
- Field descriptions
  - Port Number—Bridge group port number on which this interface resides
  - Operational Status—Operational status of the physical interface: Up, Down, LowerLayerDown, NotPresent
  - Admin Status—State of the physical interface: Up, Down
  - Snmp Link Status Trap—Whether SNMP link status processing is enabled or disabled for the specified bridge interface
  - Max Learn—Maximum number of dynamic MAC addresses that the bridge group interface can learn
  - Subscriber Policy—Name of the subscriber policy currently in effect for the bridge group interface
  - Statistics—Displays statistics information for the specified port
    - In Octets—Number of octets received on this interface
    - In Frames—Number of frames received on this interface
    - In Discards—Number of incoming packets discarded on this interface
    - In Errors—Number of incoming errors received on this interface
    - Out Octets—Number of octets transmitted on this interface
    - Out Frames—Number of frames transmitted on this interface
    - Out Discards—Number of outgoing packets discarded on this interface
    - Out Errors—Number of outgoing errors on this interface
  - queue—Hardware packet queue associated with the specified traffic class and interface
    - Queue length—Length of the queue, in bytes
    - Forwarded packets, Bytes—Number of packets and bytes forwarded on this queue
    - Dropped committed packets, Bytes—Number of committed packets and bytes that were dropped

        - Dropped conformed packets, Bytes—Number of conformed packets and bytes that were dropped
        - Dropped exceeded packets, Bytes—Number of exceeded packets and bytes that were dropped
      - Using the **brief** keyword displays the following fields:
        - Port—Bridge group port number on which this interface resides
        - Interface—Interface type and specifier associated with the port (for example, ATM3/3.1)
        - Status—Operational status of the physical interface: Up, Down, LowerLayerDown, NotPresent
  - Example 1—Displays configuration, statistics, and status information for all ports currently associated with the bridge group

```
host1#show bridge westford01 port 1
    ATM3/3.1
      Port Number: 1
      Operational Status: LowerLayerDown
      Admin Status: Up
      Snmp Link Status Trap: Disabled
      Max Learn: Unlimited
      Subscriber Policy: default Subscriber
      Statistics:
         In Octets:    0
         In Frames:    0
         In Discards:  0
         In Errors:    0
         Out Octets:   0
         Out Frames:   0
         Out Discards: 0
         Out Errors:   0
      queue 0: traffic class best-effort, bound to bridge     ATM3/3.1
        Queue length 0 Bytes
        Forwarded packets 0, Bytes 0
        Dropped committed packets 0, Bytes 0
        Dropped conformed packets 0, Bytes 0
        Dropped exceeded packets 0, Bytes 0
```

  - Example 2—Uses the **brief** keyword to display summary information for each port

```
host1#show bridge westford01 port brief
 Port            Interface              Status
------   -------------------------   ------------
1        ATM3/3.1                    LowerLayerDown
```

show bridge table

- Use to display information about dynamic and static entries in the MAC address table for the specified bridge group.
- To display only static address entries, use the **static** keyword.
- To display only dynamic address entries, use the **dynamic** keyword.

- Field descriptions
  - Bridge—Name of the bridge group for which the MAC address table is displayed
  - Address—MAC address of the entry
  - Action—Specifies how the bridge group handles this entry: forward or discard
  - Interface—Interface type and specifier on which the entry will be forwarded; this value does not appear for entries that are discarded
  - Age—Length of time that a dynamic entry has been in the forwarding table; this value does not appear for static entries
- Example

```
host1#show bridge westford01 table static
  Bridge: westford01 MAC Address Table
   Address          Action          Interface           Age
--------------   ----------   -------------------   -----
1a11.22b2.333c   forward      ATM3/3.1               ---
1234.abcd.5678   discard      ---                    ---
```

Monitoring Bridge Interfaces

You can use the **show bridge interface** command to display information for a specified bridge interface or for all interfaces assigned to a bridge group.

show bridge interface

- Use to display configuration, statistics, and status information for a specified bridge interface or for all interfaces assigned to a bridge group.
- Field descriptions
  - BridgeGroup—Name of the bridge group to which the interface belongs
  - Port Number—Bridge group port number on which this interface resides
  - Operational Status—Operational status of the physical interface: Up, Down, LowerLayerDown, NotPresent
  - Admin Status—State of the physical interface: Up, Down
  - Snmp Link Status Trap—Whether SNMP link status processing is enabled or disabled for the specified bridge interface
  - Max Learn—Maximum number of dynamic MAC addresses that the bridge group interface can learn
  - Subscriber Policy—Name of the subscriber policy currently in effect for the bridge group interface
  - Statistics—Displays statistics information for the specified port
    - In Octets—Number of octets received on this interface
    - In Frames—Number of frames received on this interface
    - In Discards—Number of incoming packets discarded on this interface
    - In Errors—Number of incoming errors received on this interface
    - Out Octets—Number of octets transmitted on this interface

- Out Frames—Number of frames transmitted on this interface
- Out Discards—Number of outgoing packets discarded on this interface
- Out Errors—Number of outgoing errors on this interface

- queue—Hardware packet queue associated with the specified traffic class and interface
  - Queue length—Length of the queue, in bytes
  - Forwarded packets, Bytes—Number of packets and bytes forwarded on this queue
  - Dropped committed packets, Bytes—Number of committed packets and bytes that were dropped
  - Dropped conformed packets, Bytes—Number of conformed packets and bytes that were dropped
  - Dropped exceeded packets, Bytes—Number of exceeded packets and bytes that were dropped
- Using the **brief** keyword displays the following fields:
  - Interface—Interface type and specifier associated with the port (for example, FastEthernet9/1.1)
  - Port—Bridge group port number on which this interface resides
  - Status—Operational status of the physical interface: Up, Down, LowerLayerDown, NotPresent

- Example 1—Displays information about a specified interface

```
host1#show bridge interface fastEthernet 9/1.1
    fastEthernet9/1.1
      BridgeGroup: 1
      Port Number: 1
      Operational Status: Up
      Admin Status: Up
      Snmp Link Status Trap: Disabled
      Max Learn: Unlimited
      Subscriber Policy: atmfe1
      Statistics:
         In Octets:    0
         In Frames:    0
         In Discards:  0
         In Errors:    0
         Out Octets:   0
         Out Frames:   0
         Out Discards: 0
         Out Errors:   0
      queue 0: traffic class best-effort, bound to bridge
    FastEthernet9/1.1
        Queue length 0 Bytes
        Forwarded packets 0, Bytes 0
        Dropped committed packets 0, Bytes 0
        Dropped conformed packets 0, Bytes 0
        Dropped exceeded packets 0, Bytes 0
```

- Example 2—Uses the **brief** keyword to display a summary of all bridge interfaces configured on the router

```
host1#show bridge westford01 interface brief
Interface            Port       Status
-----------------  --------   ------------
FastEthernet9/1.1     1           Up
FastEthernet9/1.2     2           Up
FastEthernet9/3.1     3           Up
ATM11/0.5             4           Up
ATM11/3.2             5           Up
ATM11/0.7             6           Up
```

Monitoring Subscriber Policies

You can use the **show subscriber-policy** command to display the rules for all subscriber policies configured on your router or for a specified subscriber policy.

show subscriber-policy

- Use to display the set of forwarding and filtering rules for all default and nondefault subscriber policies configured on the router or for a specified subscriber policy.
- For all packet types except Relearn, the command displays **permit** to indicate that the bridge interface forwards the packets, or **deny** to indicate that the bridge interface filters the packets. (For information about the meaning of **permit** and **deny** for Relearn, see the field descriptions.)
- Field descriptions
  - Subscriber—Name of the subscriber policy
  - ARP—Specifies how the bridge interface handles ARP packets
  - Broadcast—Specifies how the bridge interface handles broadcast packets
  - Multicast—Specifies how the bridge interface handles multicast packets
  - Unknown Destination—Specifies how the bridge interface handles packets with unknown unicast DAs
  - Unicast—Specifies how the bridge interface handles unicast (user-to-user) packets
  - PPPoE—Specifies how the bridge interface handles PPPoE packets
  - Relearn—Specifies whether the bridge interface can relearn a MAC address entry on a different interface from the one initially associated with this entry in the forwarding table; **permit** indicates that relearning is allowed, and **deny** indicates that relearning is prohibited
  - Mpls—Specifies how the bridge interface handles MPLS packets

- Example 1—Displays the rules for all default and nondefault subscriber policies currently configured on the router

```
host1#show subscriber-policy
  Subscriber: default Subscriber
  ARP                 : Permit
  Broadcast           : Deny
  Multicast           : Permit
  Unknown Destination : Deny
  IP                  : Permit
  Unknown Protocol    : Permit
  Unicast             : Permit
  PPPoE               : Permit
  Relearn             : Permit
  Mpls                : Permit
  Subscriber: default Trunk
  ARP                 : Permit
  Broadcast           : Permit
  Multicast           : Permit
  Unknown Destination : Permit
  IP                  : Permit
  Unknown Protocol    : Permit
  Unicast             : Permit
  PPPoE               : Permit
  Relearn             : Permit
  Mpls                : Permit

  Subscriber: client01
  ARP                 : Permit
  Broadcast           : Permit
  Multicast           : Deny
  Unknown Destination : Deny
  IP                  : Permit
  Unknown Protocol    : Permit
  Unicast             : Permit
  PPPoE               : Permit
  Relearn             : Deny
  Mpls                : Permit
```

- Example 2—Displays the rules for a specified subscriber policy

```
host1#show subscriber-policy client01
  Subscriber: client01
  ARP                 : Permit
  Broadcast           : Permit
  Multicast           : Deny
  Unknown Destination : Deny
  IP                  : Permit
  Unknown Protocol    : Permit
  Unicast             : Permit
  PPPoE               : Permit
  Relearn             : Deny
  Mpls                : Permit
```