

# x Digital Subscriber Line Bridge Support

---

## Description

The x digital subscriber line bridge support feature enables you to configure a router for intelligent bridge flooding for x digital subscriber line and other bridge applications.

## List of Terms

**Downstream**—Indicates the traffic flow from the server to the client. In this document, downstream defines the traffic flow from the trunk port to the subscriber port.

**Subscriber Bridge Group**—Bridge group formed by the subscriber interfaces.

**Subscriber Policy**—Set of forwarding and filtering rules applied to the subscriber bridge group.

**Trunk Port**—Router interface connected to the backbone routers.

**Upstream**—Indicates the traffic flow from the client to the server. In this document, upstream defines the traffic flow from the subscriber to the trunk port.

**xDSL**—Digital subscriber line; *x* means different media.

## Platforms

This feature is supported on all platforms.

## Configuration Tasks

To configure the router for xDSL bridge support, perform the tasks in the following sections:

- Configure a Subscriber Bridge Group
- Monitor the Subscriber Bridge Group

## Configure a Subscriber Bridge Group

To configure a subscriber bridge group, perform the following tasks, beginning in global configuration mode:

Task	Command
Define the bridge Spanning-Tree Protocol.	<b>bridge</b> <i>bridge-group</i> <b>protocol</b> { <b>ieee</b>   <b>dec</b> }
Define a subscriber bridge group and specify the subscriber policy for the group.	<b>bridge</b> <i>bridge-group</i> <b>subscriber-policy</b> <i>policy</i>
Define or modify the forward and filter decisions of the subscriber policy.	<b>subscriber-policy</b> <i>policy</i> [[ <b>no</b> ] [ <b>default</b> ] <i>packet</i> [ <b>permit</b> ] [ <b>deny</b> ]]
Configure a subinterface.	<b>interface</b> <i>type number</i>
Assign a subscriber bridge group and indicate whether the interface is upstream or downstream from the traffic flow.	<b>bridge-group</b> <i>bridge-group</i> [ <b>subscriber-trunk</b> ]

---

**Note** Standard access lists can coexist with the subscriber policy. However, subscriber policy will take precedence over the access list by being checked first. A packet permitted by the subscriber policy will be checked against the access list if it is specified. A packet denied by subscriber policy will be dropped with no further access list checking.

---

## Monitor the Subscriber Bridge Group

To monitor the subscriber bridge group, perform the following task in EXEC mode:

Task	Command
Display the details of the subscriber policy.	<b>show subscriber-policy</b> <i>policy</i>
Display details of the bridge group.	<b>show bridge</b> [ <i>bridge-group</i> ] [ <i>interface</i> ]

---

**Note** You can also use the EXEC commands **show running-config** and **show startup-config**. However, those two commands display only non-default values of the packets.

---

## Configuration Examples

This section provides the following subscriber bridge group configuration examples:

- Fast Ethernet Subscriber Port, Frame Relay Trunk Example
- ATM Subscriber Ports, ATM Trunk Example

## Fast Ethernet Subscriber Port, Frame Relay Trunk Example

This example uses the Fast Ethernet subinterface as the subscriber port and Frame Relay as the trunk:

```

bridge 1 protocol ieee

# Form a subscriber bridge group using policy 1
#
bridge 1 subscriber-policy 1
bridge 1 protocol ieee
int fast0.1
encap isl 1
#
# Put fast0.1 into subscriber group 1
#
bridge-group 1
int fast0.2
encap isl 2
#
# put fast0.2 into subscriber group 1
#
bridge-group 1
int serial0
encap frame-relay
int s0.1 point-to-point
#
# Use PVC 155 as the signal channel for setting up connections with the access-server
#
frame-relay interface-dlci 155
#
# Set the trunk to go upstream
#
bridge-group 1 trunk

```

## ATM Subscriber Ports, ATM Trunk Example

The following example uses ATM subinterfaces as the subscriber ports and the ATM as the trunk:

```

bridge 1 protocol ieee
#
# Use subscriber policy 3
#
bridge 1 subscriber-policy 3
#
# Change the ARP behavior from permit to deny
#
subscriber-policy 3 arp deny
#
# Change the multicast from permit to deny
#
subscriber-policy 3 multicast deny

int atm0
int atm0.1 point-to-point
#
# Use AAL5 SNAP encapsulation
#
atm pvc 1 0 101 aal5snap
bridge group 1
int atm0.2
#
# Use AAL5 SNAP encapsulation
#
atm pvc 2 0 102 aal5snap

```

```
bridge-group 1

#
# Configure ATM trunk port
#
int atm1.1
#
# Use AAL5 SNAP encapsulation
#
atm pvc 1 0 101 aal5snap
#
# Specify trunk
#
bridge-group 1 trunk
```

## Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 11.3 command references.

- **bridge subscriber-policy**
- **bridge-group subscriber-trunk**
- **show subscriber-policy**
- **subscriber-policy**

### bridge subscriber-policy

To bind a bridge group with a subscriber policy, use the **bridge subscriber-policy** global configuration command. Use the **no** form of this command to disable the subscriber bridge group feature.

**bridge** *bridge-group* **subscriber-policy** *policy*  
**no** **bridge** *bridge-group* **subscriber-policy** *policy*

#### Syntax Description

*bridge-group* Bridge group number, in the range of 1 to 256, specified in the **bridge protocol** command.

*policy* Subscriber policy number in the range of 1 to 100.

#### Default

If no forward or filter decisions have been specified for the subscriber policy, the following defaults are applied:

Packet	Upstream
ARP	Permit
Broadcast	Deny
CDP	Deny/Disable
Multicast	Permit

<b>Packet</b>	<b>Upstream</b>
STP	Deny/Disable
Unknown Unicast	Deny

### Command Mode

Global configuration

### Usage Guidelines

Standard access lists can coexist with the subscriber policy. However, subscriber policy will take precedence over the access list by being checked first. A packet permitted by the subscriber policy will be checked against the access list if it is specified. A packet denied by subscriber policy will be dropped with no further access list checking.

### Example

The following example forms a subscriber bridge group using policy 1.

```
bridge 1 subscriber-policy 1
```

### Related Commands

**bridge protocol**  
**show subscriber-policy**  
**subscriber-policy**

## bridge-group subscriber-trunk

To specify that an interface is at the upstream point of traffic flow, use the **bridge-group subscriber-trunk** interface configuration command. Use the **no** form of this command to remove the specification and reset the interface to a non-trunking port.

**bridge-group** *bridge-group* **subscriber-trunk**  
**no bridge-group** *bridge-group* **subscriber-trunk**

### Syntax Description

*bridge-group* Bridge group number, in the range from 1 to 256, specified in the **bridge protocol** command.

### Default

The interface is set to a non-trunking port.

### Command Mode

Interface Configuration

### Example

The following example sets bridge-group 1 as the upstream point of traffic flow:

```
bridge-group 1 subscriber-trunk
```

### Related Commands

**bridge protocol**  
**bridge subscriber-policy**  
**show subscriber-policy**  
**subscriber-policy**

## show subscriber-policy

To display the details of a subscriber policy, use the **show subscriber-policy EXEC** command.

```
show subscriber-policy range
```

### Syntax Description

*range*                      Range of subscriber policy numbers (range 1 to 100).

### Default

If a range is not specified, the entire range (1 to 100) is displayed.

### Command Mode

EXEC

### Sample Display

The following is sample output from the **show subscriber-policy** command:

```
Router# show subscriber-policy 1
ARP: Permit
Broadcast: Deny
Multicast: Permit
Unknown: Deny
STP: Disable
CDP: Disable
```

### Related Commands

**bridge protocol**  
**bridge subscriber-policy**  
**show bridge**  
**subscriber-policy**

## subscriber-policy

To define or modify the forward and filter decisions of the subscriber policy, use the **subscriber-policy** global configuration command. Use the **no** or **default** form of this command to restore the default forward and filter values.

**subscriber-policy** *policy* [[**no** | **default**] *packet* [**permit** | **deny**]]

### Command Syntax

<i>policy</i>	Subscriber policy number in the range 1 to 100.
<b>no</b>	Turn off the permit for the packet (this is an equivalent of the <b>deny</b> keyword).
<b>default</b>	Deny forwarding of the packet (this is an equivalent of the <b>deny</b> keyword).
<i>packet</i>	One of the following packets: <ul style="list-style-type: none"> <li>• <i>arp</i></li> <li>• <i>broadcast</i></li> <li>• <i>cdp</i></li> <li>• <i>multicast</i></li> <li>• <i>stp</i></li> <li>• <i>unknown unicast</i></li> </ul>
<b>permit</b>	Permit forwarding of the packet.
<b>deny</b>	Deny forwarding of the packet.

### Default

If no forward or filter decisions have been specified for the subscriber policy, the following defaults are applied:

Packet	Upstream
ARP	Permit
Broadcast	Deny
CDP	Deny/Disable
Multicast	Permit
STP	Deny/Disable
Unknown Unicast	Deny

### Command Mode

Global configuration

### Usage Guidelines

As an alternative to the command syntax described above, you can enter **subscriber-policy** *policy*, followed by the specific forward or filter decisions for each packet.

### Example

The following example changes the ARP behavior and the multicast behavior from permit to deny, using the command syntax shown in the Command Syntax section:

```
subscriber-policy 3 arp deny
subscriber-policy 3 multicast deny
```

The following example changes the ARP behavior and the multicast behavior from permit to deny, using the alternative syntax shown in the Usage Guidelines section:

```
subscriber-policy 3
arp deny
multicast deny
```

### Related Commands

**bridge protocol**  
**bridge subscriber-policy**  
**show subscriber-policy**

