Configuring Private Hosts

This chapter describes how to configure the private hosts feature in Cisco IOS Release 12.2SX.

Note For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Master Command List, at this URL:

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

This chapter consists of these sections:

- Understanding Private Hosts, page 25-1
- Configuration Guidelines and Limitations, page 25-6
- Configuring Private Hosts, page 25-8

Understanding Private Hosts

The sections that follow provide more detail about the following private hosts concepts:

- Private Hosts Overview, page 25-2
- Isolating Hosts in a VLAN, page 25-2
- Restricting Traffic Flow (Using Private Hosts Port Mode and PACLs), page 25-3
- Port ACLs, page 25-5

Private Hosts Overview

Service providers typically deliver triple-play services (voice, video, and data) using three different VLANs over a single physical interface for each end user. The service infrastructure would be simpler and more scalable if the service provider could deploy a single set of VLANs to multiple end users for the same set of services, but the service provider must be able to isolate traffic between the users (hosts) at Layer 2. The private hosts feature provides this isolation, allowing VLAN sharing among multiple end users.

The private hosts feature provides these key benefits:

- Isolates traffic among hosts (subscribers) that share the same VLAN ID.
- Reuses VLAN IDs across different subscribers, which improves VLAN scalability by making better use of the 4096 VLANs allowed.
- Prevents media access control (MAC) address spoofing to prevent denial of service (DOS) attacks.

The private hosts feature uses protocol-independent port-based access control lists (PACLs) to provide Layer 2 isolation between hosts on trusted ports within a strictly Layer 2 domain. The PACLs isolate the hosts by imposing Layer 2 forwarding constraints on the switch ports.

Isolating Hosts in a VLAN

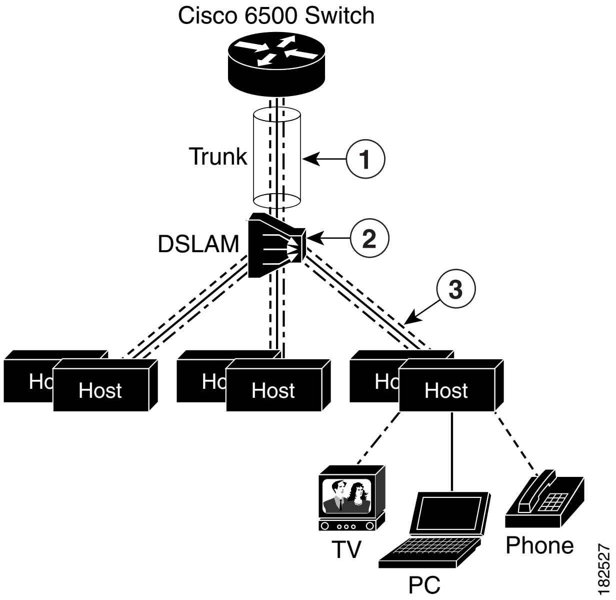
By isolating the hosts, a service provider can use a single set of VLANs to deliver the same set of broadband or metro Ethernet services to multiple end users while ensuring that none of the hosts in the VLAN can communicate directly with each other. For example, VLAN 10 can be used for voice traffic, VLAN 20 for video traffic, and VLAN 30 for data traffic.

When the switch is used as a Digital Subscriber Line Access Multiplexer (DSLAM) gigabit Ethernet aggregator, the DSLAM is connected to the switch through a trunk port that can carry data for multiple VLANs. The service provider uses a single physical port and a single set of VLANs to deliver the same set of services to different end users (isolated hosts). A separate VLAN is used for each service (voice, video, and data).

Figure 25-1 shows an example of triple-play services being delivered from the switch to multiple end users attached to a DSLAM. In the figure, note the following:

- A single trunk link between the switch and the DSLAM carries traffic for all three VLANs.
- Virtual circuits (VCs) deliver the VLAN traffic from the DSLAM to individual end users.

Figure 25-1 VC to VLAN Mapping



1	The trunk link carries: • One voice VLAN • One video VLAN • One data VLAN	**2**	The DSLAM maps voice, video, and data traffic between VLANs and VCs.
		3	Individual VCs carry voice, video, and data traffic between the DSLAM and each host.

Restricting Traffic Flow (Using Private Hosts Port Mode and PACLs)

The private hosts feature uses PACLs to restrict the type of traffic that is allowed to flow through each of the ports configured for private hosts. A port's mode (specified when you enable private hosts on the port) determines what type of PACL is applied to the port. Each type of PACL restricts the traffic flow for a different type of traffic (for example, from content servers to isolated hosts, from isolated hosts to servers, and traffic between isolated hosts).

The following list describes the port modes used by the private hosts feature (see Figure 25-2):

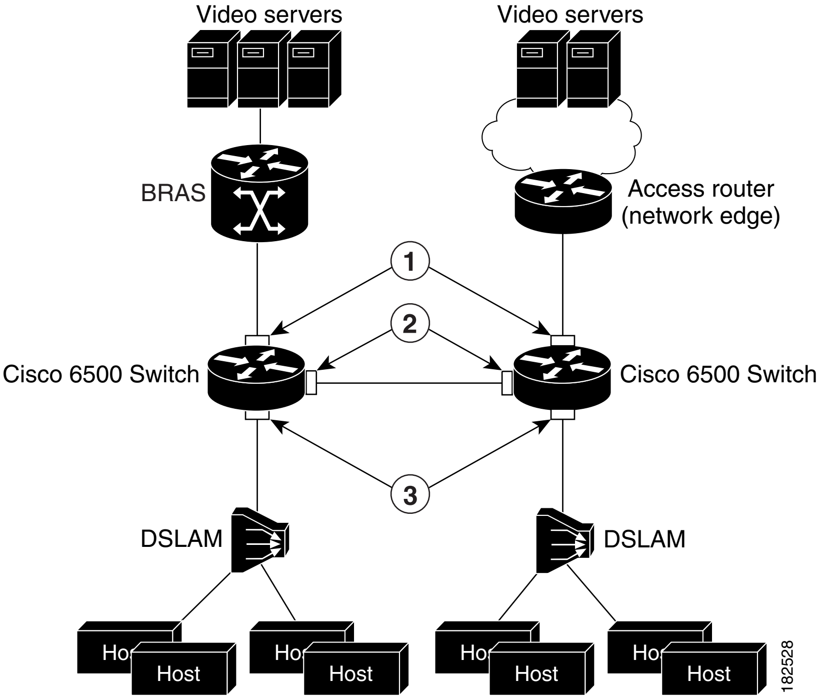
- Isolated—Ports connected to the DSLAMs that the end users (isolated hosts) are connected to. The hosts on the VLANs on these ports need to be isolated from each other. Hosts connected through these ports are allowed to pass unicast traffic to upstream devices only.
- Promiscuous—Ports that face the core network or the Broadband Remote Access Server (BRAS) devices and multicast servers that are providing the broadband services.
- Mixed—Ports that interconnect switches. These ports can function as either isolated ports or promiscuous ports, depending on Spanning Tree Protocol (STP) topology changes. These ports allow unicast traffic to upstream devices (such as a BRAS or multicast server) only.

The private hosts feature restricts traffic flow in these ways:

- Broadcast traffic at the ingress of the service provider network is redirected to BRAS and multicast servers (such as video servers).
- All unicast traffic between access switches (switches connected to each other) is blocked except for traffic directed toward a BRAS or a multicast server.
- The unknown unicast flood blocking (UUFB) feature is used to block unknown unicast traffic on DSLAM-facing ports.

Figure 25-2 shows the different types of port modes (isolated, promiscuous, and mixed) used in a private hosts configuration.

Figure 25-2 Private Hosts Port Types (Modes)



1	Promiscuous ports	Permit all traffic from a BRAS to hosts.
2	Mixed ports	Permit broadcast traffic from a BRAS. Redirect broadcast traffic from hosts to promiscuous and mixed-mode ports. Permit traffic from a BRAS to hosts and from hosts to a BRAS. Deny all other host to host traffic.
3	Isolated ports	Permit unicast traffic from host to a BRAS only; block unicast traffic between ports. Redirect all broadcast traffic from host to a BRAS. Deny traffic from a BRAS (to prevent spoofing). Permit multicast traffic (IPv4 and IPv6).

Note In this description of port types, the term BRAS represents an upstream devices such as a BRAS, a multicast server (such as a video server), or a core network device that provides access to these devices.

Port ACLs

The private hosts feature creates several types of port ACLs (PACLs) to impose Layer 2 forwarding constraints on switch ports. The software creates PACLs for the different types of private hosts ports based on the MAC addresses of the content servers providing broadband services and the VLAN IDs of the isolated hosts to deliver those services to. You specify the mode in which each private hosts port is to operate and the software applies the appropriate PACL to the port based on the port's mode (isolated, promiscuous, or mixed).

The following are examples of the different types of PACLs that are used by the private hosts feature.

Isolated Hosts PACL

This example shows a PACL for isolated ports:

```
deny host BRAS_MAC any
permit any host BRAS_MAC
redirect any host FFFF.FFFF.FFFF to LTLIndex 6
permit any 0100.5E00.0000/0000.007F.FFFF
permit any 3333.0000.0000/000.FFFF.FFFF
deny any any
```

Promiscuous Port PACL

This example shows a PACL for promiscuous ports:

```
permit host BRAS_MAC any
deny any any
```

Mixed Port PACL

This example shows a PACL for mixed ports:

```
permit host BRAS_MAC ffff.ffff.ffff
redirect any host FFFF.FFFF.FFFF to LTLIndex 6
permit host BRAS_MAC any
permit any host BRAS_MAC
deny any any
```

Configuration Guidelines and Limitations

General Restrictions

When you configure the private hosts feature, observe the following guidelines and limitations:

- The SIP-400 and Enhanced FlexWAN modules do not support private hosts.
- Private hosts and private VLANs cannot both be configured on the same port (interface). Both features can coexist on the switch, but the features must be configured on different ports.
- Private hosts is an end-to-end feature. You must enable the feature on all of the switches between the DSLAMs and an upstream device such as a BRAS or a multicast server.
- Only trusted ports can be configured as isolated ports.
- The private hosts feature is supported on Layer 2 interfaces that are configured as trunking switch ports (802.1Q or ISL trunk ports).
- The private hosts feature is supported on port-channel interfaces (EtherChannel, Fast EtherChannel, and Gigabit EtherChannel). You must enable private hosts on the port-channel interface; you cannot enable the feature on member ports.
- DAI and DHCP snooping cannot be enabled on a private hosts port unless all of the VLANs on the port are configured for snooping.

ACL Guidelines

The following configuration guidelines and limitations apply to access control lists (ACLs):

- This release of the private hosts feature uses protocol-independent MAC ACLs.

  Do not apply IP-based ACLs to any port configured for private hosts or you will defeat the private hosts feature (because the switch will not be able to apply a private hosts MAC ACL to the port).
- You can configure the following interface types for protocol-independent MAC ACL filtering:
  - VLAN interfaces with no IP address
  - Physical LAN ports that support EoMPLS
  - Logical LAN subinterfaces that support EoMPLS
- Protocol-independent MAC ACL filtering applies MAC ACLs to all ingress traffic types (for example, IPv4 traffic, IPv6 traffic, and MPLS traffic, in addition to MAC-layer traffic).
- Ingress traffic that is permitted or denied by a protocol-independent MAC ACL is processed by egress interfaces as MAC-layer traffic. You cannot apply egress IP ACLs to traffic permitted or denied by a MAC ACL on an interface configured for protocol-independent MAC ACL filtering.

- Do not configure protocol-independent MAC ACL filtering on VLAN interfaces where you have configured an IP address.
- Do not configure protocol-independent MAC ACL filtering with microflow policing when the permitted traffic would be bridged or Layer 3 switched in hardware by the PFC3.
- Protocol-independent MAC ACL filtering supports microflow policing when the permitted traffic is routed in software by the route processor (RP).
- Do not apply any VACLs or RACLs to a port configured for private hosts. To prevent any existing VLAN ACLs (VACLs) and routing ACLs (RACLs) from interfering with a PACL, configure the **access-group mode prefer port** command on the port.

VLANs on the Trunk Port

The following guidelines and limitations apply to VLANs:

- You can enable IGMP snooping on VLANs that use trunk ports configured for private hosts.
- You cannot enable IP multicast on a VLAN that uses a trunk port that is configured for private hosts.
- Because PACLs operate in override mode on trunk ports, you cannot apply VLAN-based features to switch ports.
- The Multicast VLAN Registration (MVR) feature can coexist with private hosts as long as the multicast source exists on a promiscuous port.

Interaction with Other Features

The private hosts feature interacts with other features that are configured on the switch as follows:

- Private hosts do not affect Layer 2-based services such as MAC limiting, unicast flood protection (UFP), or unknown unicast flood blocking (UUFB).
- The private hosts features does not affect IGMP snooping. However, if IGMP snooping is globally disabled, IGMP control packets will be subject to ACL checks. To permit IGMP control packets, the private hosts software adds a multicast permit statement to the PACLs for isolated hosts. This operation occurs automatically and no user intervention is required.
- Port security can be enabled on isolated ports to provide added security to those ports.
- When enabled on promiscuous or mixed-mode ports, the port security feature may restrict a change in source port for an upstream device (such as a BRAS or a multicast server).
- When enabled on an access port, 802.1X is not affected by the private hosts feature.

Spoofing Protection

The private hosts feature prevents MAC address spoofing but does not validate the customer MAC or IP address. To prevent MAC address spoofing, the private hosts feature does the following:

- Uses a static MAC address for a BRAS or a multicast server.
- Disables learning in the Layer 2 forwarding table.
- Alerts the switch software when a BRAS or multicast server moves from one source port to another. The software then validates the move and updates the Layer 2 forwarding table.

Multicast Operation

Multicast traffic that originates from an upstream device (such as a BRAS or a multicast server) is always permitted. In addition, the private hosts PACLs are not applied to multicast control packets (such as IGMP query and join requests). This operation allows isolated hosts to participate in multicast groups, respond to IGMP queries, and receive traffic from any groups of interest.

Multicast traffic that originates from a host is dropped by the private hosts PACLs. However, if other hosts need to receive multicast traffic originating from a host, the private hosts feature adds a *multicast permit* entry to the PACLs.

Configuring Private Hosts

The following sections provide information about configuring the private hosts feature in Cisco IOS Release 12.2SX:

- Configuration Summary, page 25-8
- Detailed Configuration Steps, page 25-9
- Configuration Examples, page 25-11
- Enabling Index Learning on Isolated Mode Ports, page 25-12

Configuration Summary

The following is a summary of the steps to configure the private hosts feature. Detailed configuration instructions are provided in the next section.

1. Determine which switch ports (interfaces) to use for the private hosts feature.
   - You can configure the feature on switch ports (802.1Q or ISL trunk ports)
   - You can configure the feature on port-channel interfaces. Private hosts must be enabled on the port-channel interface; you cannot enable the feature on member ports.
2. Configure each port (interface) for normal, non-private hosts service. Configure the **access-group mode prefer port** command on the port. You can configure the VLANs at this step or later.
3. Determine which VLAN or set of VLANs will be used to deliver broadband services to end users. The private hosts feature will provide Layer 2 isolation among the hosts in these VLANs.
4. Identify the MAC addresses of all of the BRASs and multicast servers that are being used to provide broadband services to end users (isolated hosts).

Note If a server is not connected directly to the switch, determine the MAC address of the core network device that provides access to the server.

5. (Optional) If you plan to offer different types of broadband service to different sets of isolated hosts, create multiple MAC and VLAN lists.
   - Each MAC address list identifies a server or set of servers providing a particular type of service.
   - Each VLAN list identifies the isolated hosts to deliver that service to.
6. Configure promiscuous ports and specify a MAC and VLAN list to identify the server and receiving hosts for a particular type of service.

Note You can specify multiple MAC and VLAN combinations to allow different types of services to be delivered to different sets of hosts. For example, the BRAS at xxxx.xxxx.xxxx could be used to deliver a basic set of services over VLANs 20, 25, and 30, and the BRAS at yyyy.yyyy.yyyy could be used to deliver a premium set of services over VLANs 5, 10, and 15.

7. Globally enable private hosts.
8. Enable private hosts on individual ports (interfaces) and specify the mode in which the port is to operate. To determine port mode, you need to know if the port faces upstream (toward content servers or core network), faces downstream (toward DSLAMs), or is connected to another switch (typically, in a ring topology). See the "Restricting Traffic Flow (Using Private Hosts Port Mode and PACLs)" section on page 25-3.

After you enable the feature on individual ports, the switch is ready to run the private hosts feature. The private hosts software uses the MAC and VLAN lists you defined to create the isolated, promiscuous, and mixed-mode PACLs for your configuration. The software then applies the appropriate PACL to each private hosts port based on the port's mode.

Detailed Configuration Steps

To configure the private hosts feature, perform the following steps. These steps assume that you have already configured the Layer 2 interfaces that you plan for private hosts.

Note You can configure private hosts only on trunking switch ports (802.1Q or ISL trunk ports) or EtherChannel ports. In addition, you must enable private hosts on all of the switches between the DSLAMs and upstream devices.

	Command or Action	Purpose
Step 1	`Router# `**`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)# `**`private-hosts mac-list`** *`mac-list-name mac-address`* `[`**`remark`** *`device-name`* `|` *`comment`*`]`	Creates a list of MAC addresses that identify the BRAS and multicast servers providing broadband services. • *mac-list-name* specifies a name to assign to this list of content servers. • *mac-address* identifies the BRAS or multicast server (or set of servers) providing a particular broadband service or set of services. • **remark** allows you to specify an optional device name or comment to assign to this MAC list. Specify the MAC address of every content server being used to deliver services. If you plan to offer different types of services to different sets of hosts, create a separate MAC list for each server or set of servers providing a particular service. **Note** If a server is not directly connected to the switch, specify the MAC address of the core network device that provides access to the server.

	Command or Action	Purpose
Step 3	Router(config)# **private-hosts vlan-list** *vlan-IDs*	Creates a list of the VLANs (*vlan-IDs*) whose hosts need to be isolated so that the hosts can receive broadband services. Create separate VLAN lists if you plan to offer particular services to different sets of hosts. Otherwise, all of the broadband services will be delivered to all isolated hosts.
Step 4	Router(config)# **private-hosts promiscuous** *mac-list-name* [**vlan-list** *vlan-IDs*]	Identifies the content servers for broadband services and the end users (isolated hosts) to which to deliver the services. • *mac-list-name* specifies the name of the MAC address lists that identifies the BRAS or multicast server (or set of servers) providing a particular type of broadband service or set of services. • *vlan-IDs* identifies the VLAN or set of VLANs whose hosts are to receive services from the above servers. If no VLAN list is specified, the software uses the global VLAN list (configured in Step 3). **Note** You can enter this command multiple times to configure multiple MAC and VLAN combinations, each defining the server and receiving hosts for a particular type of service.
Step 5	Router(config)# **private-hosts**	Globally enables private hosts on the switch.
Step 6	Router(config)# **interface** *interface*	Selects the switch port (802.1Q or ISL trunk port) or EtherChannel port to enable for private hosts.
Step 7	Router(config-if)# **access-group mode prefer port**	Specifies that any existing VACLs or RACLs on the port will be ignored.
Step 8	Router(config-if)# **private-hosts mode** {**promiscuous** | **isolated** | **mixed**}	Enables private hosts on the port. Use one of the following keywords to define the mode that the port is to operate in: • **promiscuous**—Upstream-facing ports that connect to broadband servers (BRAS, multicast, or video) or to core network devices providing access to the servers. • **isolated**—Ports that connect to DSLAMs. • **mixed**—Ports that connect to other switches, typically in a ring topology. **Note** You must perform this step on each port being used for private hosts.
Step 9	Router(config-if)# **end**	Exits interface and global configuration modes and returns to privileged EXEC mode. Private Hosts configuration is complete.

Configuration Examples

The following example creates a MAC address list and a VLAN list and isolates the hosts in VLANs 10, 12, 15, and 200 through 300. The BRAS-facing port is made promiscuous and two host-connected ports are made isolated:

```
Router# configure terminal
Router(config)# private-hosts mac-list BRAS_list 0000.1111.1111 remark BRAS_SanJose
Router(config)# private-hosts vlan-list 10,12,15,200-300
Router(config)# private-hosts promiscuous BRAS_list vlan-list 10,12,15,200-300
Router(config)# private-hosts
Router(config)# interface gig 4/2
Router(config-if)# private-hosts mode promiscuous
Router(config-if)# exit
Router(config)# interface gig 5/2
Router(config-if)# private-hosts mode isolated
Router(config-if)# exit
Router(config)# interface gig 5/3
Router(config-if)# private-hosts mode isolated
Router(config-if)# end
Router#
```

The following example shows the interface configuration of a private hosts isolated port:

```
Router# show run interface gig 5/2
Building configuration...

Current configuration : 200 bytes
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 access-group mode prefer port
 private-hosts mode isolated
end
```

The following example shows the interface configuration of a private hosts promiscuous port:

```
Router# show run interface gig 4/2
Building configuration...

Current configuration : 189 bytes
!
interface GigabitEthernet4/2
 switchport
 switchport access vlan 200
 switchport mode access
 private-hosts mode promiscuous
end

private-hosts
private-hosts vlan-list 200
private-hosts promiscuous bras-list
private-hosts mac-list bras-list 0000.1111.1111 remark BRAS-SERVER
```

Enabling Index Learning on Isolated Mode Ports

By default, MAC address movement (index learning) is disabled between isolated-mode ports.

When wireless access points are connected to isolated-mode ports, a wireless user can make an initial connection, but with the default private hosts configuration (index learning disabled), the MAC address of the wireless user will not be learned on any other isolated-mode ports, which prevents connection through any other wireless access point that is connected to an isolated-mode port.

To allow wireless users to move from one wireless access point to another, enable index learning on isolated mode ports, which enables MAC address movement between isolated-mode ports.

To enable index learning on the switch, perform this task:

	Command or Action	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# private-hosts index learning`	Enables index learning on the switch.

This example shows how to enable index learning on the switch:

```
Router# configure terminal
Router(config)# private-hosts index learning
```

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum