

Private Hosts (Using PACLs)

This chapter describes the Private Hosts feature, which is being introduced for the Cisco 7600 series router in Cisco IOS Release 12.2SRB. This chapter contains the following sections:

- [Overview, page 35-1](#)
- [Configuration Guidelines and Limitations, page 35-5](#)
- [Configuring Private Hosts, page 35-7](#)
- [Command Reference, page 35-12](#)

Overview

The Private Hosts feature provides Layer 2 (L2) isolation between the hosts in a VLAN. You can use Private Hosts as an alternative to the Private VLAN isolated-trunks feature, which is currently not available on the Cisco 7600 router.

Service Providers (SPs) worldwide face increasing demand to provide their customers with triple-play services (voice, video, and data) over a single physical interface (copper or fiber). Typically, triple-play services are delivered over three different VLANs for each user, even though the VLAN for video traffic is often shared by multiple end users.

The key benefits of the Private Hosts feature are the ability to:

- Isolate traffic among hosts (subscribers) that share the same VLAN ID
- Reuse VLAN IDs across different subscribers, which improves VLAN scalability by making better use of the 4096 VLANs allowed
- Prevent MAC spoofing to prevent denial of service (DOS) attacks

The Private Hosts feature uses port-based Protocol-Independent MAC ACLs (PACLs) to provide Layer 2 isolation between hosts on trusted ports within a purely Layer 2 domain. The PACLs isolate the hosts by imposing Layer 2 forwarding constraints on the router ports.

**Note**

In Release 12.2SRB, PACLs are supported only as part of Private Hosts; you cannot configure your own PACLs. Instead, the router creates and applies PACLs based on your Private Hosts configuration.

The sections that follow provide more detail about the following Private Hosts concepts:

- [Isolating Hosts in a VLAN, page 35-2](#)
- [Restricting Traffic Flow \(Using Private Hosts Port Mode and PACLs\), page 35-3](#)
- [Port ACLs, page 35-5](#)

Isolating Hosts in a VLAN

Typically, triple-play services (voice, video, and data) are delivered over three different VLANs for each user, even though the VLANs for the same set of services could be shared among multiple end users. For example, if 10 end users all receive the same set of services, Private Hosts can be used to deliver the services to all of 10 end users over a single set of VLANs. However, to allow VLAN sharing, the service provider must be able to isolate traffic between the users (hosts) at Layer 2.

The Private Hosts feature provides Layer 2 isolation among hosts (end users) 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 Cisco 7600 router is used as a DSLAM Gigabit Ethernet (GE) aggregator, the DSLAM is connected to the router 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 35-1 shows an example of triple-play services being delivered from the Cisco 7600 router to multiple end users attached to a DSLAM. In the figure note that:

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

Figure 35-1 VC to VLAN Mapping

A	Trunk link carries: <ul style="list-style-type: none"> • One voice VLAN • One video VLAN • One data VLAN 	B	DSLAM maps voice, video, and data traffic between VLANs and VCs.
		C	Individual VCs carry voice, video, and data traffic between 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 35-2](#)):

- **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 Cisco 7600 routers. These ports can act as either an isolated port or a promiscuous port, depending on Spanning Tree Protocol (STP) topology changes. These ports allow unicast traffic to upstream devices (such as BRAS and multicast servers) only.

The following list summarizes how the Private Hosts feature restricts traffic flow:

- 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 routers (Cisco 7600 routers connected to each other) is blocked except for traffic directed toward BRAS and multicast servers.
- The unknown unicast flood blocking (UUFb) feature is used to block unknown unicast traffic on DSLAM-facing ports.

Figure 35-2 shows the different types of port modes (isolated, promiscuous, and mixed) used in a Private Hosts configuration.

Figure 35-2 Private Hosts Port Types (Modes)

A	Promiscuous ports	Permit all traffic from BRAS to hosts.
B	Mixed-mode ports	Permit broadcast traffic from BRAS. Redirect broadcast traffic from hosts to promiscuous and mixed-mode ports. Permit traffic from BRAS to hosts and from hosts to BRAS. Deny all other host to host traffic.
C	Isolated ports	Permit unicast traffic from host to BRAS only; block unicast traffic between ports. Redirect all broadcast traffic from host to BRAS. Deny traffic from BRAS (to prevent spoofing). Permit multicast traffic (IPv4 and IPv6).
Note The term BRAS represents upstream devices such as BRAS, multicast servers (such as video servers), or core network devices that provide access to these devices.		

Port ACLs

The Private Hosts software creates several types of port ACLs (PACLs) to impose Layer 2 forwarding constraints on router ports. Each type of PACL restricts traffic flow for a particular type of traffic (for example, from content servers to isolated hosts, from isolated hosts to servers, and traffic between isolated hosts).

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).

Following are examples of the different types of PACLs that are used by the Private Hosts feature.

Isolated Hosts PACL

Following is an example of 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

Following is an example of a PACL for promiscuous ports:

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

Mixed-Mode Port PACL

Following is an example of a PACL for mixed-mode 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

Observe the following guidelines and limitations as you configure the Private Hosts feature on Cisco 7600 routers:

- Software and hardware requirements:
 - Cisco IOS Release 12.2SRB or later
 - RSP720 (with PFC3C or PFC3CXL), Sup720 (with PFC3B or PFC3BXL), or Sup32
 - Supported on line cards with Fast Ethernet or Gigabit Ethernet (GE) interfaces that can be configured as switch ports (for example, SIP-600, ESM-20, and 67xx LAN cards). (Note that the SIP-400 and Enhanced FlexWAN do not support Private Hosts.)
- Private Hosts and Private VLANs cannot both be configured on the same port (interface). Both features can co-exist on the router, but each feature must be configured on different ports.
- Private Hosts is an end-to-end feature. You must enable the feature on all of the routers between the DSLAMs and upstream devices like BRAS and multicast servers.

- Currently, only trusted ports can be configured as isolated ports.
- Supported on Layer 2 interfaces that are configured as switchports (802.1q or ISL trunk ports).
- Supported on port-channel interfaces (Etherchannel, FastEtherchannel, and GigabitEtherchannel). 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.

The following protocol-independent MAC ACL restrictions also apply:

- 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 MSFC.



Note

In Release 12.2SRB, PACLs are supported only as part of Private Hosts; you cannot configure your own PACLs. Instead, the router creates and applies PACLs based on your Private Hosts configuration.

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 break the Private Hosts feature (because the router will not be able to apply a Private Hosts MAC ACL to the port).
- VLAN ACLs (VACLs) and port ACLs cannot both be applied to the same interface.
- Routing ACLs (RACLs) and PACLs cannot both be applied to the same interface. However, you can apply the ACLs to separate interfaces.

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 switchports.
- The Multicast VLAN Registration (MVR) feature can co-exist with Private Hosts as long as the multicast source exists on a promiscuous port.

Interaction with Other Features

The following list describes how the Private Hosts feature interacts with other features that are configured on the router:

- Private Hosts does not affect Layer 2 based services such as MAC limiting, unicast flood protection (UFP), or unknown unicast flood blocking (UUFb).
- Private Hosts 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. Note that this behavior 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 upstream devices (such as BRAS or multicast servers).
- When enabled on an access port, 802.1x is not affected by Private Hosts.

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, Private Hosts:

- Uses a static MAC address for the BRAS and multicast servers.
- Disables learning in the Layer 2 (L2) forwarding table.
- Alerts the router software when a BRAS or multicast server moves from one source port to another. The software then validates the move and updates the L2 forwarding table.

Multicast Operation

Multicast traffic that originates from upstream devices (such as BRAS or multicast servers) is always permitted. In addition, the Private Hosts PACLs are not applied to multicast control packets (such as IGMP query and join requests). This behavior 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, Private Hosts does the following:

- To allow other hosts (including hosts on isolated ports) to receive multicast traffic from another host, Private Hosts adds a *multicast permit* entry to the PACLs.

Configuring Private Hosts

The following sections provide information about configuring the Private Hosts feature on a Cisco 7600 series router and instructions for configuring the feature:

- [Configuration Summary, page 35-8](#)
- [Detailed Configuration Steps, page 35-9](#)
- [Configuration Examples, page 35-10](#)

Configuration Summary

Following is a summary of the steps to perform to configure the Private Hosts feature on Cisco 7600 routers. Detailed configuration instructions are provided in the next section.

1. Determine which router ports (interfaces) to use for the Private Hosts feature. You can configure the feature on switchports (802.1q or ISL trunk ports) or port-channel interfaces (Etherchannel, FastEtherchannel, and GigabitEtherchannel). Note that 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. Note that you can configure the VLANs now 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 Broadband Remote Access Servers (BRAS) 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 router, 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 DSLAM and isolated hosts), or is connected to another Cisco 7600 router (typically, in a ring topology). See [Restricting Traffic Flow \(Using Private Hosts Port Mode and ACLs\)](#), page 35-3.

After you enable the feature on individual ports, the router 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 ACLs for your configuration. The software then applies the appropriate ACL to each Private Hosts port based on the port's mode.

Detailed Configuration Steps

Perform the following steps to configure the Private Hosts feature. Note that these steps assume that you have already configured the Layer 2 interfaces that you plan for Private Hosts. See the “[Command Reference](#)” section on page 35-12 for detailed descriptions of the commands in the following table.


Note

You can configure Private Hosts only on switchports (802.1q or ISL trunk ports) or Etherchannel ports. In addition, you must enable Private Hosts on all of the routers between the DSLAMs and upstream devices.

	Command or Action	Purpose
Step 1	Router(config)# configure terminal	Enters global configuration mode.
Step 2	Router(config)# private-hosts mac-list <i>mac-list-name</i> <i>mac-address</i> [remark <i>device-name</i> <i>comment</i>] Example: Router(config)# private-hosts mac-list BRAS_list 0000.1111.1111 remark BRAS_SanJose	Creates a list of MAC addresses that identify the BRAS and multicast servers providing broadband services, where: <ul style="list-style-type: none"> <i>mac-list-name</i> specifies a name to assign to this list of content servers. <i>mac-address</i> 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 router, specify the MAC address of the core network device that provides access to the server.
Step 3	Router(config)# private-hosts vlan-list <i>vlan-ids</i> Example: Router(config)# private-hosts vlan-list 10,12,15,200-300	Creates a list of the VLANs (<i>vlan-ids</i>) 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.

	Command or Action	Purpose
Step 4	<pre>Router(config)# private-hosts promiscuous mac-list-name [vlan-list vlan-ids]</pre> <p>Example:</p> <pre>Router(config)# private-hosts promiscuous BRAS_list vlan-list 1,2,3</pre>	<p>Identifies the content servers for broadband services and the end users (isolated hosts) to deliver the services to, where:</p> <ul style="list-style-type: none"> <i>mac-list-name</i> 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. <i>vlan-ids</i> 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). <p>Note You can issue this command multiple times to configure multiple MAC and VLAN combinations, each defining the server and receiving hosts for a particular type of service.</p>
Step 5	<pre>Router(config)# private-hosts</pre>	Globally enables Private Hosts on the router.
Step 6	<pre>Router(config)# interface interface</pre>	Selects the switchport (802.1Q or ISL trunk port) or Etherchannel port to enable for Private Hosts.
Step 7	<pre>Router(config-if)# private-hosts mode {promiscuous isolated mixed}</pre> <p>Example:</p> <pre>Router(config-if)# private-hosts mode isolated</pre>	<p>Enables Private Hosts on the port. Use one of the following keywords to define the mode that the port is to operate in:</p> <ul style="list-style-type: none"> 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 Cisco 7600 routers, typically in a ring topology. <p>Note You must perform this step on each port being used for Private Hosts.</p>
Step 8	<pre>Router(config-if)# end</pre>	Exits interface and global configuration modes and returns to privileged EXEC mode. Private Hosts configuration is complete.

Configuration Examples

The following example shows the interface configuration of a Private Hosts isolated port:

```
Router# show run int gi 5/2
Building configuration...

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

The following example shows the interface configuration of a Private Hosts promiscuous port:

```
Router# show run int gi 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
```

Command Reference

This section documents the commands related to the Private Hosts feature, all of which are new. The commands are:

- **private-hosts**
- **private-hosts mac-list**
- **private-hosts mode**
- **private-hosts promiscuous**
- **private-hosts vlan-list**
- **show fm private-hosts**
- **show private-hosts access-lists**
- **show private-hosts configuration**
- **show private-hosts interface configuration**
- **show private-hosts mac-list**
- **debug fm private-hosts**
- **debug private-hosts**

private-hosts

To globally enable the Private Hosts feature, use the **private-hosts** command in global configuration mode. Use the **no** form of the command to disable the feature.

private-hosts

no private-hosts

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.

Usage Guidelines Issue this command to enable Private Hosts on the router. Then, use the **private-hosts mode** command to enable Private Hosts on individual interfaces (ports).

Examples The following command example globally enables the Private Hosts feature on the router:

```
Router(config)# private-hosts
```

Related Commands	Command	Description
	private-hosts mac list	Creates a MAC address list that identifies the content servers that are being used to provide broadband services to isolated hosts.
	private-hosts mode	Specifies the operating mode for a Private Hosts port.
	private-hosts promiscuous	Identifies the content servers and receiving hosts for broadband services.
	private-hosts vlan-list	Identifies the VLANs whose hosts need to be isolated.
	show private-hosts configuration	Displays Private Hosts configuration information for the router.
	show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

private-hosts mac-list

To identify the content servers that provide broadband services to isolated hosts, create a MAC address list by using the **private-hosts mac-list** command in global configuration mode. To delete an address from the MAC address list and remove that device from the list of content servers providing services for the Private Hosts feature, use the **no** form of the command.

```
private-hosts mac-list mac-list-name mac-address [remark device-name | comment]
```

```
no private-hosts mac-list mac-list-name mac-address
```

Syntax Description

<i>mac-list-name</i>	A name to assign to the address list (up to 80 characters).
<i>mac-address</i>	The MAC address of a Broadband Remote Access Server (BRAS), multicast server, or video server that provides broadband services for the Private Hosts feature. Note If the server is not directly connected to the router, specify the MAC address of the core network device that provides access to the server.
remark <i>device-name</i> <i>comment</i>	(Optional) Specifies an optional device name or comment to assign to this MAC address list.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

This command creates a list of MAC addresses that identify the content servers being used to provide broadband services to isolated hosts in the Private Hosts configuration.

Use this command to specify the MAC address of every content server that provides broadband services for the Private Hosts feature. A *content server* is any Broadband Remote Access Server (BRAS), multicast server, or video server that provides services to the isolated hosts in your network.

You can assign all of the content servers to a single MAC address list or you can create multiple MAC address lists, each identifying the content server for a particular type of broadband service or set of services. When you configure the promiscuous ports for Private Hosts, you specify a MAC address list and VLAN list to identify the server and receiving hosts for broadband services.

If you plan to deliver different types of broadband services to different sets of hosts, create multiple MAC address lists to identify the servers for each type of service. You can also create multiple VLAN lists to identify different sets of isolated hosts. When you configure promiscuous ports, you can specify different combinations of MAC address lists and VLAN lists to identify the servers and receiving hosts for each type of service.

**Note**

The MAC address list is deleted when the last address in the list is deleted.

Examples

This example creates a MAC address list named BRAS_list that identifies the MAC address of the upstream BRAS. The optional remark indicates that the BRAS is in San Jose.

```
Router(config)# private-hosts mac-list BRAS_list 0000.1111.1111 remark BRAS_San-Jose
```

Related Commands

Command	Description
show private-hosts mac-list	Displays a list of the MAC addresses that identify the content servers that are providing broadband defined for Private Hosts.

private-hosts mode

To enable Private Hosts on an interface (port) and specify the mode in which the port is to operate, use the **private-hosts mode** command in interface configuration mode. Use the **no** form of the command to disable Private Hosts on the port.

private-hosts mode { **promiscuous** | **isolated** | **mixed** }

no private-hosts

Syntax Description

promiscuous	Configures the port for promiscuous mode. Use this mode for ports that face upstream. These are the ports that connect the router to the servers providing broadband services (BRAS, multicast, or video), or to the core network devices providing access to the servers.
isolated	Configures the port for isolated mode. Use this mode for ports that face the DSLAM to which the isolated hosts are connected.
mixed	Configures the port for mixed mode. Use this mode for ports that connect to other Cisco 7600 routers, typically in a ring topology. The behavior of this port can change depending on the Spanning Tree Protocol (STP) topology.

Defaults

This command is disabled by default.
The default for **mode** is promiscuous.

Command Modes

Interface configuration (switchport or port-channel)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

Before you can use this command, you must globally enable the Private Hosts feature on the router by issuing the **private-hosts** command.

Use this command to enable the Private Hosts feature on individual ports and to define the mode of operation for the port. A port's mode determines which type of PACL will be assigned to the port in order to restrict the type of traffic that is allowed to pass through 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). Use the **show private-hosts interface configuration** command to display the mode assigned to Private Hosts ports.

Examples

The following command example enables Private Hosts on an interface (port) and configures the port for isolated mode:

```
Router(config-if)# private-hosts mode isolated
```

Related Commands

Command	Description
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

private-hosts promiscuous

To identify the content servers and receiving hosts for broadband services, use the **private-hosts promiscuous** command in global configuration mode. Use the **no** form of the command to remove a promiscuous ports setting.

private-hosts promiscuous *mac-list-name* [**vlan** *vlan-ids*]

no private-hosts promiscuous *mac-list-name*

Syntax Description

<i>mac-list-name</i>	The name of MAC address list that identifies the content servers (BRAS, multicast, or video) providing broadband services for Private Hosts.
vlan <i>vlan-ids</i>	(Optional) The VLAN or set of VLANs whose hosts will be allowed to receive services from the content servers identified by the MAC address list. Use commas to separate individual VLANs or specify a range of VLANs (for example, 1,3,5,20-25).
Note	If no VLAN list is specified, the global VLAN list is used.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

The MAC address list and VLAN list define the content servers and receiving hosts for broadband services. If no VLAN list is specified, the system uses the global VLAN list created with the **private-hosts vlan-list** command.

You can issue this command multiple times to specify multiple combinations of MAC and VLAN lists, each defining the server and receiving hosts for a particular type of service. 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.

Examples

The following command example configures the broadband services provided by the content servers defined in the BRAS_list address list to be delivered to the isolated hosts in VLANs 10, 12, 15, and 200 through 300:

```
Router(config)# private-hosts promiscuous BRAS_list vlan 10,12,15,200-300
```

Related Commands

Command	Description
show private-hosts configuration	Displays Private Hosts configuration information for the router.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

private-hosts vlan-list

To identify the VLANs whose hosts need to be isolated from each other (so that the VLANs can be used to deliver broadband services), create a VLAN list by using the **private-hosts vlan-list** command in global configuration mode. Use the **no** form of the command to remove a VLAN from the list of VLANs requiring host isolation.

private-hosts vlan-list *vlan-ids*

no private-hosts vlan-list *vlan-ids*

Syntax Description	<i>vlan-ids</i>	A list of the VLANs whose hosts need to be isolated from each other. Use commas to separate individual VLANs or specify a range of VLANs (for example, 1,3,5,20-25).
---------------------------	-----------------	--

Defaults This command has no default settings.

Command Modes Global configuration

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.

Usage Guidelines This command creates a list of VLANs whose hosts need to be isolated through the Private Hosts feature. The VLAN list should include all of the VLANs that are being used to deliver broadband services to multiple end users (isolated hosts).

If you plan to deliver different types of broadband services to different sets of hosts, you can create multiple VLAN lists and multiple MAC address lists. When you configure promiscuous ports, you can specify different combinations of MAC and VLAN lists to identify the content servers and receiving hosts for each type of service.

If you do not specify a VLAN list when you configure promiscuous ports, the system uses the global VLAN list created by this command.



Note

The Private Hosts feature isolates the hosts in all of the VLANs included in VLAN lists; therefore, VLAN lists should include only those VLANs that are being used to deliver broadband services.

Examples

This command configures the Private Hosts feature to isolate the hosts in VLANs 10, 12, 15, and 200 through 300:

```
Router(config)# private-hosts vlan-list 10,12,15,200-300
```

Related Commands

Command	Description
show private-hosts configuration	Displays Private Hosts configuration information for the router.

show fm private-hosts

To display information about the Private Hosts feature manager, use the **show fm private-hosts** command in privileged EXEC mode.

```
show fm private-hosts {all | interface intf}
```

Syntax Description	all	Displays the feature manager information for all of the interfaces that are configured for Private Hosts.
	interface <i>intf</i>	Specifies the interface to display feature manager information for.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.

Examples The following example shows sample command output:

```
Router# show fm private-hosts interface GigabitEthernet 1/2
-----
FM_FEATURE_PVT_HOST_INGRESS      i/f: Gi1/2      map name:
PVT_HOST_ISOLATED
=====

-----
MAC Seq. No: 10          Seq. Result : PVT_HOSTS_ACTION_DENY
-----
Indx - VMR index      T      - V(Value)M(Mask)R(Result)
EtTy - Ethernet Type  EtCo - Ethernet Code
+---+---+-----+-----+-----+
|Indx|T|   Dest Node   | Source Node |EtTy|EtCo|
+---+---+-----+-----+-----+

  1   V 0000.0000.0000 0000.1111.4001    0 0
      M 0000.0000.0000 ffff.ffff.ffff    0 0
      TM_PERMIT_RESULT

  2   V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT

-----
MAC Seq. No: 20          Seq. Result : PVT_HOSTS_ACTION_PERMIT
-----
+---+---+-----+-----+-----+
|Indx|T|   Dest Node   | Source Node |EtTy|EtCo|
+---+---+-----+-----+-----+
```

```

1    V 0000.1111.4001 0000.0000.0000    0 0
    M ffff.ffff.ffff 0000.0000.0000    0 0
    TM_PERMIT_RESULT

```

```

2    V 0000.0000.0000 0000.0000.0000    0 0
    M 0000.0000.0000 0000.0000.0000    0 0
    TM_L3_DENY_RESULT

```

```

-----
MAC Seq. No: 30          Seq. Result : PVT_HOSTS_ACTION_REDIRECT
-----

```

```

+---+---+---+---+---+---+---+---+---+
|Indx|T|   Dest Node   | Source Node |EtTy|EtCo|
+---+---+---+---+---+---+---+---+---+

```

```

1    V ffff.ffff.ffff 0000.0000.0000    0 0
    M ffff.ffff.ffff 0000.0000.0000    0 0
    TM_PERMIT_RESULT

```

```

2    V 0000.0000.0000 0000.0000.0000    0 0
    M 0000.0000.0000 0000.0000.0000    0 0
    TM_L3_DENY_RESULT

```

```

-----
MAC Seq. No: 40          Seq. Result : PVT_HOSTS_ACTION_PERMIT
-----

```

```

+---+---+---+---+---+---+---+---+---+
|Indx|T|   Dest Node   | Source Node |EtTy|EtCo|
+---+---+---+---+---+---+---+---+---+

```

```

1    V 0100.5e00.0000 0000.0000.0000    0 0
    M ffff.ff80.0000 0000.0000.0000    0 0
    TM_PERMIT_RESULT

```

```

2    V 3333.0000.0000 0000.0000.0000    0 0
    M ffff.0000.0000 0000.0000.0000    0 0
    TM_PERMIT_RESULT

```

```

3    V 0000.0000.0000 0000.0000.0000    0 0
    M 0000.0000.0000 0000.0000.0000    0 0
    TM_L3_DENY_RESULT

```

```

-----
MAC Seq. No: 50          Seq. Result : PVT_HOSTS_ACTION_DENY
-----

```

```

+---+---+---+---+---+---+---+---+---+
|Indx|T|   Dest Node   | Source Node |EtTy|EtCo|
+---+---+---+---+---+---+---+---+---+

```

```

1    V 0000.0000.0000 0000.0000.0000    0 0
    M 0000.0000.0000 0000.0000.0000    0 0
    TM_PERMIT_RESULT

```

```

2    V 0000.0000.0000 0000.0000.0000    0 0
    M 0000.0000.0000 0000.0000.0000    0 0
    TM_L3_DENY_RESULT

```

```

Interfaces using this pvt host feature in ingress dir.:
-----

```

```

    Interfaces (I/E = Ingress/Egress)

```

```

Router#

```

Related Commands	Command	Description
	show private-hosts configuration	Displays Private Hosts configuration information for the router.
	show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

show private-hosts access-lists

To display the access lists for your Private Hosts configuration, use the **show private-hosts access-lists** command in privileged EXEC mode.

show private-hosts access-lists

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.

Examples The following example shows how to display the Private Hosts access lists for your configuration:

```
Router# show private-hosts access-lists

Promiscuous ACLs
Action Permit Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Deny Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Isolated ACLs
Action Deny Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000 Action
Redirect Sequence # 030 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0100.5e00.0000 0000.007f.ffff
    Source:0000.0000.0000 ffff.ffff.ffff Destination:3333.0000.0000 0000.ffff.ffff
Action Deny Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Mixed ACLs
Action Permit Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:ffff.ffff.ffff 0000.0000.0000 Action
Redirect Sequence # 020 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit Sequence # 030
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000
Action Deny Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff

Router#
```

Related Commands	Command	Description
	show fm private-hosts	Displays information about the Private Hosts feature manager.
	show private-hosts configuration	Displays Private Hosts configuration information for the router.
	show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

show private-hosts configuration

To display information about the Private Hosts configuration on the router, use the **show private-hosts configuration** command in privileged EXEC mode.

show private-hosts configuration

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.

Examples The following example shows sample command output:

```
Router# show private-hosts configuration

Private hosts enabled. BR INDEX 6 State 0000000F
Privated hosts vlans lists:
200
Privated promiscuous MAC configuration:
A '*' mark behind the mac list indicates non-existent mac-list
-----
MAC-list                VLAN list
-----
bras-list                *** Uses the isolated vlans (if any) ***
```

Related Commands	Command	Description
	show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

show private-hosts interface configuration

To display information about the Private Hosts configuration on individual interfaces (ports), use the **show private-hosts interface configuration** command in privileged EXEC mode.

show private-hosts interface configuration

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.

Examples The following example shows sample command output:

```
Router# show private-hosts interface configuration

Private hosts enabled
Debug Events: 0 Acl: 0 API: 0
Promiscuous interface list
-----
GigabitEthernet4/2
Isolated interface list
-----
GigabitEthernet5/2
Mixed mode interface list
-----
```

Related Commands	Command	Description
	show private-hosts configuration	Displays Private Hosts configuration information for the router.

show private-hosts mac-list

To display the contents of the MAC address lists defined for Private Hosts, use the **show private-hosts mac-list** command in privileged EXEC mode.

```
show private-hosts mac-list [list-name]
```

Syntax Description	<i>list-name</i>	(Optional) The name of the MAC address list whose contents you want to display.
--------------------	------------------	---

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.

Examples The following example shows sample command output:

```
Router# show private-hosts mac-list
```

```
MAC-List: bras-list
-----
MAC address      Description
-----
0000.1111.1111  BRAS-SERVER
```

Related Commands	Command	Description
	private-hosts mac-list	Creates a MAC address list that identifies a content server that is being used to provide broadband services to isolated hosts.

debug fm private-hosts

To enable debug messages for the Private Hosts feature manager, use the **debug fm private-hosts** command in privileged EXEC mode.

```
debug fm private-hosts {all | vmr | unusual | events}
```

Syntax Description	all	Enable debug messages for all Private Hosts errors and events.
	vmr	Enable debug messages for the Multicast VLAN Registration (MVR) feature.
	unusual	Enable debug messages for unexpected Private Hosts behavior.
	events	Enable debug messages for Private Hosts events.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.

Examples The following example shows sample command output:

```
Router# debug fm private-hosts all
fm private-hosts vmr debugging is on
fm private-hosts unusual debugging is on
fm private-hosts events debugging is on
Router#
```

Related Commands	Command	Description
	debug private-hosts	Enables debug messages for Private Hosts.

debug private-hosts

To enable debug messages for the Private Hosts feature, use the **debug private-hosts** command in privileged EXEC mode.

debug private-hosts {all | events | acl | api}

Syntax Description

all	Enable debug messages for all Private Hosts errors and events.
events	Enable debug messages for issues related to Private Hosts events.
acl	Enable debug messages for issues and events related to ACLs.
api	Enable debug messages for issues related to the application programming interface.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Examples

The following example shows sample command output:

```
Router# debug private-hosts all
private-hosts events debugging is on
private-hosts api debugging is on
private-hosts acl debugging is on
Router#
```

Related Commands

Command	Description
debug fm private-hosts	Enables debug messages for the Private Hosts feature manager.

■ debug private-hosts