Configuring Interfaces

This chapter describes the various interface modes and how to configure interfaces on the sensor. It contains the following sections:

Sensor Interfaces

This section describes the sensor interfaces, and contains the following topics:

Understanding Interfaces

The sensor interfaces are named according to the maximum speed and physical location of the interface. The physical location consists of a port number and a slot number. All interfaces that are built-in on the sensor motherboard are in slot 0, and the interface card expansion slots are numbered beginning with

slot 1 for the bottom slot with the slot numbers increasing from bottom to top. Each physical interface can be divided in to VLAN group subinterfaces, each of which consists of a group of VLANs on that interface.

There are three interface roles:

- Command and control
- Sensing
- Alternate TCP reset

There are restrictions on which roles you can assign to specific interfaces and some interfaces have multiple roles. You can configure any sensing interface to any other sensing interface as its TCP reset interface. The TCP reset interface can also serve as an IDS (promiscuous) sensing interface at the same time.:

Note The TCP reset interface that is assigned to a sensing interface has no effect in inline interface or inline VLAN pair mode, because TCP resets are always sent on the sensing interfaces in those modes.

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

Caution On the IPS 4500 series sensors, no interface-related configurations are allowed when the SensorApp is down.

Command and Control Interface

The command and control interface has an IP address and is used for configuring the sensor. It receives security and status events from the sensor and queries the sensor for statistics. The command and control interface is permanently enabled. It is permanently mapped to a specific physical interface, which depends on the specific model of sensor. You cannot use the command and control interface as either a sensing or alternate TCP reset interface.

Table 7-1 lists the command and control interfaces for each sensor.

Table 7-1 Command and Control Interfaces

Sensor	Command and Control Interface
ASA 5512-X IPS SSP	Management 0/0
ASA 5515-X IPS SSP	Management 0/0
ASA 5525-X IPS SSP	Management 0/0
ASA 5545-X IPS SSP	Management 0/0
ASA 5555-X IPS SSP	Management 0/0
IPS SSP-10	Management 0/0
IPS SSP-20	Management 0/0
IPS SSP-40	Management 0/0

Table 7-1 Command and Control Interfaces (continued)

Sensor	Command and Control Interface
IPS SSP-60	Management 0/0
IPS 4345	Management 0/0
IPS 4345-DC	Management 0/0
IPS 4360	Management 0/0
IPS 4510	Management 0/0[1]
IPS 4520	Management 0/0[1]
IPS 4520-XL	Management 0/0[1]

1. The 4500 series sensors have two management ports, Management 0/0 and Management 0/1, but Management 0/1 is reserved for future use.

Sensing Interfaces

Sensing interfaces are used by the sensor to analyze traffic for security violations. A sensor has one or more sensing interfaces depending on the sensor. Sensing interfaces can operate individually in promiscuous mode or you can pair them to create inline interfaces.

Note On appliances, all sensing interfaces are disabled by default. You must enable them to use them. On modules, the sensing interfaces are permanently enabled.

Some appliances support optional interface cards that add sensing interfaces to the sensor. You must insert or remove these optional cards while the sensor is powered off. The sensor detects the addition or removal of a supported interface card. If you remove an optional interface card, some of the interface configuration is deleted, such as the speed, duplex, description string, enabled/disabled state of the interface, and any inline interface pairings. These settings are restored to their default settings when the card is reinstalled. However, the assignment of promiscuous and inline interfaces to the Analysis Engine is not deleted from the Analysis Engine configuration, but is ignored until those cards are reinserted and you create the inline interface pairs again.

For More Information

- For the number and type of sensing interfaces available for each sensor, see Interface Support, page 7-4.
- For more information on interfaces modes, see Understanding Interface Modes, page 7-10.
- For the procedure for configuring virtual sensors, see Adding, Editing, and Deleting Virtual Sensors, page 8-12.

Interface Support

Table 7-2 describes the interface support for appliances and modules running Cisco IPS.

Table 7-2 Interface Support

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
ASA 5512-X IPS SSP	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5515-X IPS SSP	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5525-X IPS SSP	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5545-X IPS SSP	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
ASA 5555-X IPS SSP	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
IPS SSP-10	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
IPS SSP-20	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
IPS SSP-40	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
IPS SSP-60	—	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	PortChannel 0/0 by security context instead of VLAN pair or inline interface pair	Management 0/0
IPS 4345	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 GigabitEthernet 0/6 GigabitEthernet 0/7	All sensing ports can be paired together	Management 0/0

Table 7-2 Interface Support (continued)

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
IPS 4345-DC	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 GigabitEthernet 0/6 GigabitEthernet 0/7	All sensing ports can be paired together	Management 0/0
IPS 4360	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 GigabitEthernet 0/6 GigabitEthernet 0/7	All sensing ports can be paired together	Management 0/0
IPS 4510	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 TenGigabitEthernet 0/6 TenGigabitEthernet 0/7 TenGigabitEthernet 0/8 TenGigabitEthernet 0/9	All sensing ports can be paired together	Management 0/0 Management 0/1[1]

Table 7-2 Interface Support (continued)

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
IPS 4520	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 TenGigabitEthernet 0/6 TenGigabitEthernet 0/7 TenGigabitEthernet 0/8 TenGigabitEthernet 0/9	All sensing ports can be paired together	Management 0/0 Management 0/1[1]
IPS 4520-XL	—	GigabitEthernet 0/0 GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4 GigabitEthernet 0/5 TenGigabitEthernet 0/6 TenGigabitEthernet 0/7 TenGigabitEthernet 0/8 TenGigabitEthernet 0/9	All sensing ports can be paired together	Management 0/0 Management 0/1[1]

1. Reserved for future use.

TCP Reset Interfaces

This section explains the TCP reset interfaces and when to use them. It contains the following topics:

Understanding Alternate TCP Reset Interfaces

You can configure sensors to send TCP reset packets to try to reset a network connection between an attacker host and its intended target host. In some installations when the interface is operating in promiscuous mode, the sensor may not be able to send the TCP reset packets over the same sensing interface on which the attack was detected. In such cases, you can associate the sensing interface with

an alternate TCP reset interface and any TCP resets that would otherwise be sent on the sensing interface when it is operating in promiscuous mode are instead sent out on the associated alternate TCP reset interface.

If a sensing interface is associated with an alternate TCP reset interface, that association applies when the sensor is configured for promiscuous mode but is ignored when the sensing interface is configured for inline mode. Any sensing interface can serve as the alternate TCP reset interface for another sensing interface

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

Table 7-3 lists the alternate TCP reset interfaces.

Table 7-3 Alternate TCP Reset Interfaces

Sensor	Alternate TCP Reset Interface
ASA 5512-X IPS SSP	None
ASA 5515-X IPS SSP	None
ASA 5525-X IPS SSP	None
ASA 5545-X IPS SSP	None
ASA 5555-X IPS SSP	None
IPS SSP-10	None
IPS SSP-20	None
IPS SSP-40	None
IPS SSP-60	None
IPS 4345	Any sensing interface
IPS 4345-DC	Any sensing interface
IPS 4360	Any sensing interface
IPS 4510	Any sensing interface
IPS 4520	Any sensing interface
IPS 4520-XL	Any sensing interface

Designating the Alternate TCP Reset Interface

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

You need to designate an alternate TCP reset interface in the following situations:

- When a switch is being monitored with either SPAN or VACL capture and the switch does not accept incoming packets on the SPAN or VACL capture port.
- When a switch is being monitored with either SPAN or VACL capture for multiple VLANs, and the switch does not accept incoming packets with 802.1q headers. The TCP resets need 802.1q headers to tell which VLAN the resets should be sent on.

- When a network tap is used for monitoring a connection. Taps do not permit incoming traffic from the sensor.

Caution You can only assign a sensing interface as an alternate TCP reset interface. You cannot configure the management interface as an alternate TCP reset interface.

Interface Configuration Restrictions

The following restrictions apply to configuring interfaces on the sensor:

- Physical Interfaces
  - On the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) all backplane interfaces have fixed speed, duplex, and state settings. These settings are protected in the default configuration on all backplane interfaces.
  - For nonbackplane FastEthernet interfaces the valid speed settings are 10 Mbps, 100 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit copper interfaces (1000-TX on the IPS 4345, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL), valid speed settings are 10 Mbps, 100 Mbps, 1000 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit (copper or fiber) interfaces, if the speed is configured for 1000 Mbps, the only valid duplex setting is auto.
  - The command and control interface cannot also serve as a sensing interface.
- Inline Interface Pairs
  - Inline interface pairs can contain any combination of sensing interfaces regardless of the physical interface type (copper versus fiber), speed, or duplex settings of the interface. However, pairing interfaces of different media type, speeds, and duplex settings may not be fully tested or supported.
  - The command and control interface cannot be a member of an inline interface pair.
  - You cannot pair a physical interface with itself in an inline interface pair.
  - A physical interface can be a member of only one inline interface pair.
  - You can only configure bypass mode and create inline interface pairs on sensor platforms that support inline mode.
  - A physical interface cannot be a member of an inline interface pair unless the subinterface mode of the physical interface is **none**.

    Note You can configure the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) to operate inline even though they have only one sensing interface.

- Inline VLAN Pairs
  - You cannot pair a VLAN with itself.
  - You cannot use the default VLAN as one of the paired VLANs in an inline VLAN pair.

  - For a given sensing interface, a VLAN can be a member of only one inline VLAN pair. However, a given VLAN can be a member of an inline VLAN pair on more than one sensing interface.
  - The order in which you specify the VLANs in an inline VLAN pair is not significant.
  - A sensing interface in Inline VLAN Pair mode can have from 1 to 255 inline VLAN pairs.

    Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support inline VLAN pairs.

  - For the IPS 4500 series, the maximum number of inline VLAN pairs you can create system-wide is 150. On all other platforms, the limit is 255 per interface.
  - You can enable LACP for inline VLAN pairs only on the 4500 series sensors.

- Alternate TCP Reset Interface
  - You can only assign the alternate TCP reset interface to a sensing interface. You cannot configure the command and control interface as an alternate TCP reset interface. The alternate TCP reset interface option is set to **none** as the default and is protected for all interfaces except the sensing interfaces.
  - You can assign the same physical interface as an alternate TCP reset interface for multiple sensing interfaces.
  - A physical interface can serve as both a sensing interface and an alternate TCP reset interface.
  - The command and control interface cannot serve as the alternate TCP reset interface for a sensing interface.
  - A sensing interface cannot serve as its own alternate TCP reset interface.
  - You can only configure interfaces that are capable of TCP resets as alternate TCP reset interfaces.

    Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

- VLAN Groups
  - You can configure any single interface for promiscuous, inline interface pair, or inline VLAN pair mode, but no combination of these modes is allowed.
  - You cannot add a VLAN to more than one group on each interface.
  - You cannot add a VLAN group to multiple virtual sensors.
  - An interface can have no more than 255 user-defined VLAN groups.
  - When you pair a physical interface, you cannot subdivide it; you can subdivide the pair.
  - You can use a VLAN on multiple interfaces; however, you receive a warning for this configuration.
  - You can assign a virtual sensor to any combination of one or more physical interfaces and inline VLAN pairs, subdivided or not.
  - You can subdivide both physical and logical interfaces into VLAN groups.
  - The CLI, IDM, and IME prompt you to remove any dangling references. You can leave the dangling references and continue editing the configuration.

  - The CLI, IDM, and IME do not allow configuration changes in Analysis Engine that conflict with the interface configuration.
  - The CLI allows configuration changes in the interface configuration that cause conflicts in the Analysis Engine configuration. The IDM and IME do *not* allow changes in the interface configuration that cause conflicts in the Analysis Engine configuration.
- Other Restrictions
  - For IPS standalone appliances with 1 G and 10 G fixed or add-on interfaces, the maximum jumbo frame size is 9216 bytes. For integrated IPS sensors, such as the ASA 5500-X and ASA 5585-X series, refer to the following URL for information:

    http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/interface_start.html#wp1328869
  - A jumbo frame is an Ethernet packet that is larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS).
  - On the IPS 4500 series sensors, no interface-related configurations are allowed when the SensorApp is down.

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support VLAN groups mode.

For More Information

For more information on interface pair combinations, see Interface Support, page 7-4.

Understanding Interface Modes

This section explains the various interface modes, and contains the following topics:

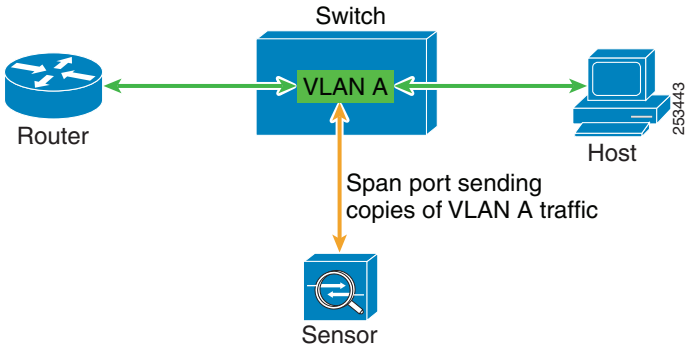
Promiscuous Mode

In promiscuous mode, packets do not flow through the sensor. The sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require assistance from other networking devices, for example, routers and firewalls, to respond to an attack. While such response actions can prevent some classes of attacks, in atomic attacks the single packet has the chance of reaching the target system before the promiscuous-based sensor can apply an ACL modification on a managed device (such as a firewall, switch, or router).

By default, all sensing interfaces are in promiscuous mode. To change an interface from inline interface mode to promiscuous mode, delete any inline interface that contains that interface and delete any inline VLAN pair subinterfaces of that interface from the interface configuration.

Figure 7-1 illustrates promiscuous mode:

Figure 7-1 Promiscuous Mode



IPv6, Switches, and Lack of VACL Capture

VACLs on Catalyst switches do not have IPv6 support. The most common method for copying traffic to a sensor configured in promiscuous mode is to use VACL capture. If you want to have IPv6 support, you can use SPAN ports.

However, you can only configure up to two monitor sessions on a switch unless you use the following configuration:

- Monitor session
- Multiple trunks to one or more sensors
- Restrict per trunk port which VLANs are allowed to perform monitoring of many VLANs to more than two different sensors or virtual sensors within one IPS

The following configuration uses one SPAN session to send all of the traffic on any of the specified VLANs to all of the specified ports. Each port configuration only allows a particular VLAN or VLANs to pass. Thus you can send data from different VLANs to different sensors or virtual sensors all with one SPAN configuration line:

```
clear trunk 4/1-4 1-4094
set trunk 4/1 on dot1q 930
set trunk 4/2 on dot1q 932
set trunk 4/3 on dot1q 960
set trunk 4/4 on dot1q 962
set span 930, 932, 960, 962 4/1-4 both
```

Note The SPAN/Monitor configuration is valuable when you want to assign different IPS policies per VLAN or when you have more bandwidth to monitor than one interface can handle.

For More Information

- For more information on promiscuous mode, see Promiscuous Mode, page 7-10.
- For more information on configuring SPAN/monitor on switches, refer to the following sections in *Catalyst 6500 Series Software Configuration Guide, 8.7*:
  - Configuring SPAN, RSPAN and the Mini Protocol Analyzer
  - Configuring SPAN on the Switch
  - Configuring Ethernet VLAN Trunks
  - Defining the Allowed VLANs on a Trunk

Inline Interface Mode

Operating in inline interface pair mode puts the IPS directly into the traffic flow and affects packet-forwarding rates making them slower by adding latency. This allows the sensor to stop attacks by dropping malicious traffic before it reaches the intended target, thus providing a protective service. Not only is the inline device processing information on Layers 3 and 4, but it is also analyzing the contents and payload of the packets for more sophisticated embedded attacks (Layers 3 to 7). This deeper analysis lets the system identify and stop and/or block attacks that would normally pass through a traditional firewall device.

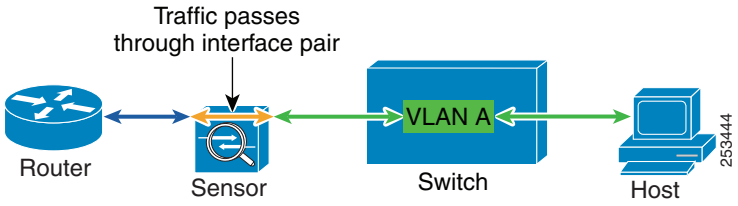
In inline interface pair mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

Note You can configure the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) to operate inline even though they have only one sensing interface.

Note If the paired interfaces are connected to the same switch, you should configure them on the switch as access ports with different access VLANs for the two ports. Otherwise, traffic does not flow through the inline interface.

Figure 7-2 illustrates inline interface pair mode.

Figure 7-2 Inline Interface Pair Mode



Inline VLAN Pair Mode

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support inline VLAN pairs.

Note For the IPS 4500 series sensors, the maximum number of inline VLAN pairs you can create system-wide is 150. On all other platforms, the limit is 255 per interface.

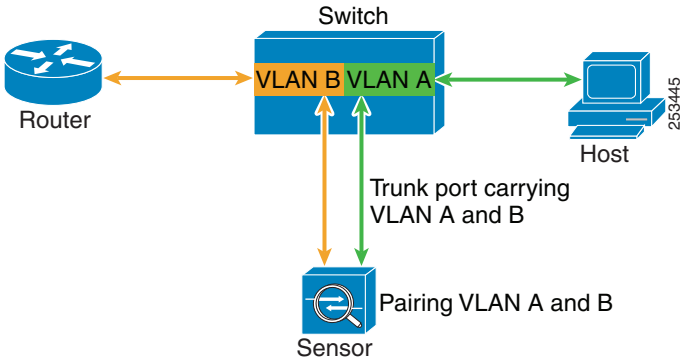
You can associate VLANs in pairs on a physical interface. This is known as inline VLAN pair mode. Packets received on one of the paired VLANs are analyzed and then forwarded to the other VLAN in the pair.

Inline VLAN pair mode is an active sensing mode where a sensing interface acts as an 802.1q trunk port, and the sensor performs VLAN bridging between pairs of VLANs on the trunk. The sensor inspects the traffic it receives on each VLAN in each pair, and can either forward the packets on the other VLAN in the pair, or drop the packet if an intrusion attempt is detected. You can configure an IPS sensor to simultaneously bridge up to 255 VLAN pairs on each sensing interface. The sensor replaces the VLAN ID field in the 802.1q header of each received packet with the ID of the egress VLAN on which the sensor forwards the packet. The sensor drops all packets received on any VLANs that are not assigned to inline VLAN pairs.

Note You cannot use the default VLAN as one of the paired VLANs in an inline VLAN pair.

Figure 7-3 illustrates inline VLAN pair mode.

Figure 7-3 Inline VLAN Pair Mode



VLAN Groups Mode

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support VLAN groups mode.

You can divide each physical interface or inline interface into VLAN group subinterfaces, each of which consists of a group of VLANs on that interface. Analysis Engine supports multiple virtual sensors, each of which can monitor one or more of these interfaces. This lets you apply multiple policies to the same sensor. The advantage is that now you can use a sensor with only a few interfaces as if it had many interfaces.

Note You cannot divide physical interfaces that are in inline VLAN pairs into VLAN groups.

VLAN group subinterfaces associate a set of VLANs with a physical or inline interface. No VLAN can be a member of more than one VLAN group subinterface. Each VLAN group subinterface is identified by a number between 1 and 255. Subinterface 0 is a reserved subinterface number used to represent the entire unvirtualized physical or logical interface. You cannot create, delete, or modify subinterface 0 and no statistics are reported for it.

An unassigned VLAN group is maintained that contains all VLANs that are not specifically assigned to another VLAN group. You cannot directly specify the VLANs that are in the unassigned group. When a VLAN is added to or deleted from another VLAN group subinterface, the unassigned group is updated.

Packets in the native VLAN of an 802.1q trunk do not normally have 802.1q encapsulation headers to identify the VLAN number to which the packets belong. A default VLAN variable is associated with each physical interface and you should set this variable to the VLAN number of the native VLAN or to 0. The value 0 indicates that the native VLAN is either unknown or you do not care if it is specified. If the default VLAN setting is 0, the following occurs:

- Any alerts triggered by packets without 802.1q encapsulation have a VLAN value of 0 reported in the alert.
- Non-802.1q encapsulated traffic is associated with the unassigned VLAN group and it is not possible to assign the native VLAN to any other VLAN group.

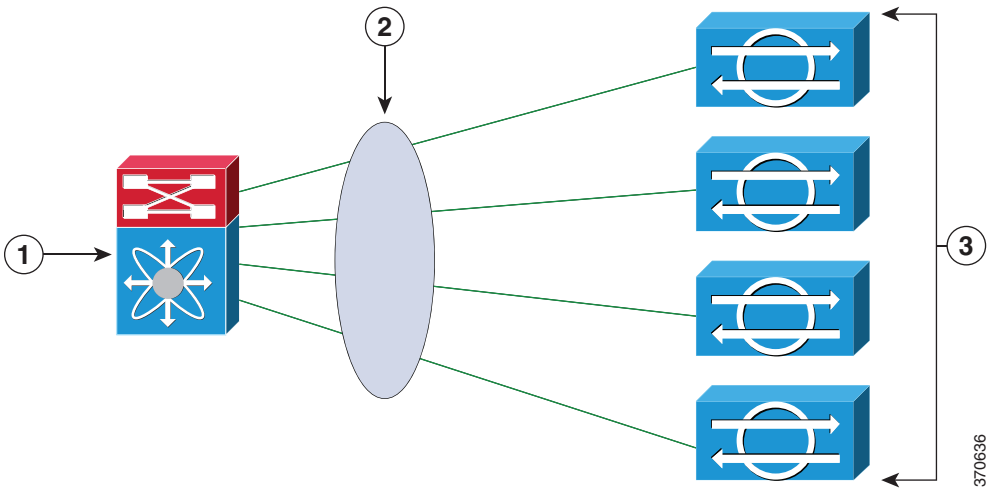
Note You can configure a port on a switch as either an access port or a trunk port. On an access port, all traffic is in a single VLAN is called the access VLAN. On a trunk port, multiple VLANs can be carried over the port, and each packet has a special header attached called the 802.1q header that contains the VLAN ID. This header is commonly referred as the VLAN tag. However, a trunk port has a special VLAN called the native VLAN. Packets in the native VLAN do not have the 802.1q headers attached.

Understanding ECLB Using LACP

Link Aggregation Control Protocol (LACP) support has been added to the IPS 4500 series sensors to meet the scalability and high availability requirements of the data center. The capability of network switches is leveraged to aggregate multiple links in a single port channel. For example, using EtherChannel, LACP can scale aggregated IPS throughput to a maximum of up to 80 Gbps with 16 IPS 4520 in an LACP group. LACP with IPS interoperates with Catalyst 6K and Nexus 7K switches in data center environments. ECLB using LACP in the Nexus 7K supports up to 16 IPS devices; with the Catalyst 6K it supports 8 IPS devices.

Figure 7-4 shows a port channel configuration that consists of a switch that is connected to four IPS sensors to achieve scalability and increase bandwidth.

Figure 7-4 IPS Port Channel Configuration with a Switch



1	Switch S1	**2**	Port Channel
3	IPS		

A port channel is created on the switch and the four physical interfaces that are connected to the IPS sensors are added to the port channel. The port channel supports load balancing to distribute the load among the members of the port channel. IPS sensors in an LACP port channel act as independent appliances. We recommend that you have the same configuration on all IPS sensors participating in the LACP port channel. You must configure each of the IPS interfaces in the LACP port channel in inline VLAN pair mode.

LACP is a point-to-point protocol and has two modes of operation—active and passive. Both are supported by the IPS. In active mode, Link Aggregation Control Protocol Data Units (LACPDUs) are periodically sent to actively probe for LACP support on the device on the other side. If the device on the other side responds to the LACP packets, an LACP connection is initiated. If LACP mode is configured as active, the connection is initiated as soon as the physical link is up.

In passive mode, the device does not actively send any LACP packets to probe the LACP device on the other end. It waits for the other side to probe and initiate an LACP connection. This can work only if the device on the other side supports LACP and is configured in active mode.

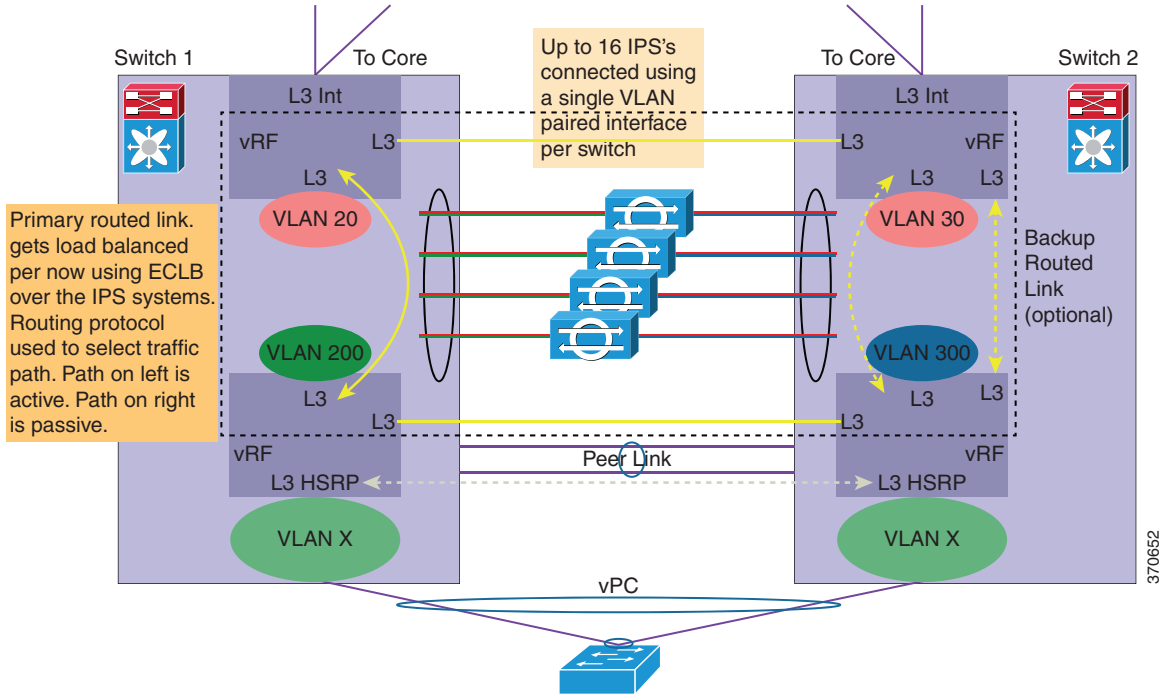
By default, LACP mode in IPS is disabled. Once LACP is enabled in the IPS, you must have it configured and operational in the switch, otherwise the LACP port will be either suspended or independent based on the switch side configuration.

Note We do not recommend that you enable LACP unless you are sure of the configuration on the other side.

Note We do not recommend that you configure UDLD with LACP.

Figure 7-5 displays the recommended IPS LACP deployment in a data center environment:

Figure 7-5 Recommended IPS LACP Configuration



For More Information

- For the procedure for configuring LACP on your 4500 series sensor, see Configuring LACP, page 7-21.
- For detailed information on monitoring LACP on your sensor, see Monitoring LACP, page 20-18.

Interface Configuration Summary

The Summary pane provides a summary of how you have configured the sensing interfaces—the interfaces you have configured for promiscuous mode, the interfaces you have configured as inline pairs, and the interfaces you have configured as inline VLAN pairs. The content of this pane changes when you change your interface configuration.

Caution You can configure any single physical interface to run in promiscuous mode, inline interface pair mode, or inline VLAN pair mode, but you cannot configure an interface in a combination of these modes.

Field Definitions

The following fields are found in the Summary pane:

- Name—Displays the name of the interface. The values are FastEthernet, GigabitEthernet, Management, or PortChannel for promiscuous interfaces. For inline interfaces, the name is whatever you assigned to the pair.
- Details—Tells you whether the interface is promiscuous, inline, or backplane and whether there are VLAN pairs.
- Assigned Virtual Sensor—Tells you whether the interface or interface pair has been assigned to a virtual sensor.
- Description—Displays your description of the interface.

Configuring Interfaces

This section describes how to configure interfaces on the sensor, and contains the following topics:

Interfaces Pane

Note You must be administrator to enable, disable, and edit the interfaces on the sensor.

The Interfaces pane lists the existing physical interfaces on your sensor and their associated settings. The sensor detects the interfaces and populates the interfaces list in the Interfaces pane. If an option is not available for an interface, the field reads N/A or is empty.

To configure the sensor to monitor traffic, you must enable the interface. When you initialized the sensor using the **setup** command, you assigned the interface or the inline pair to a virtual sensor, and enabled the interface or inline pair. If you need to change your interfaces settings, you can do so in the Interfaces pane.To add a virtual sensor and assign it an interface in the Add Virtual Sensor dialog box, choose **Configuration > *sensor_name* > Policies > IPS Policies > Add Virtual Sensor**.

Interfaces Pane Field Definitions

Note If an option is not pertinent or available for an interface, you cannot configure that option. The field is grayed out.

The following fields are found in the Interfaces pane:

- Interface Name—Indicates the name of the interface. The values are FastEthernet, GigabitEthernet, Management, or PortChannel.
- Enabled—Whether or not the interface is enabled.
- Management Interface—Whether or not this interface is a management interface.
- Media Type—Indicates the media type. The media type options are the following:
  - TX—Copper media
  - SX—Fiber media
  - XL—Network accelerator card
  - Backplane interface—An internal interface that connects the module to the backplane of the parent chassis.
- Duplex—Indicates the duplex setting of the interface. The duplex type options are the following:
  - Auto—Sets the interface to auto negotiate duplex.
  - Full—Sets the interface to full duplex.
  - Half—Sets the interface to half duplex.
- Speed—Indicates the speed setting of the interface. The speed type options are the following:
  - Auto—Sets the interface to auto negotiate speed.
  - 10 MB—Sets the interface to 10 MB (for TX interfaces only).
  - 100 MB—Sets the interface to 100 MB (for TX interfaces only).
  - 1000—Sets the interface to 1 GB (for Gigabit interfaces only).
  - 10000—Indicates the interface is set to 10 GB (for PortChannel only).
- Default VLAN—Indicates the VLAN to which the interface is assigned.

- Alternate TCP Reset Interface—If selected, sends TCP resets on an alternate interface when this interface is used for promiscuous monitoring and the reset action is triggered by a signature firing.

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

- Description—Lets you provide a description of the interface.
- LACP—Displays the LACP mode (active or passive) and the channel ID of this interface.

Enabling and Disabling Interfaces

To enable or disable an interface, follow these steps:

Step 1 Log in to the IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Interfaces > Interfaces**.

Step 3 Select the interface and click **Enable**. The interface is enabled. To have the interface monitor traffic, it must also be assigned to a virtual sensor. The Enabled column reads Yes in the list in the Interfaces pane.

Step 4 To disable an interface, select it, and click **Disable**. The Enabled column reads No in the list in the Interfaces pane.

Tip To discard your changes, click **Reset**.

Step 5 Click **Apply** to apply your changes and save the revised configuration.

Edit Interface Dialog Box Field Definitions

The following fields are found in the Edit Interface dialog box:

- Interface Name—Name of the interface. The values are FastEthernet, GigabitEthernet, Management, or PortChannel for all interfaces.
- Enabled—Whether or not the interface is enabled.
- Media Type—Indicates the media type. The media types are the following:
  - TX—Copper media
  - SX—Fiber media
  - XL—Network accelerator card
  - Backplane interface—An internal interface that connects the module to the backplane of the parent chassis.
- Duplex—Indicates the duplex setting of the interface. The duplex types are the following:
  - Auto—Sets the interface to auto negotiate duplex.
  - Full—Sets the interface to full duplex.
  - Half—Sets the interface to half duplex.

- Speed—Indicates the speed setting of the interface. The speed types are the following:
  - Auto—Sets the interface to auto negotiate speed.
  - 10 MB—Sets the interface to 10 MB (for TX interfaces only).
  - 100 MB—Sets the interface to 100 MB (for TX interfaces only).
  - 1000—Sets the interface to 1 GB (for Gigabit interfaces only).
  - 10000—Indicates the interface is set to 10 GB (for PortChannel 0/0 only).
- Default VLAN—Indicates the VLAN to which the interface is assigned.
- Management Interface—Sets this interface as the management interface.
- Use Alternate TCP Reset Interface—If checked, sends TCP resets on an alternate interface when this interface is used for promiscuous monitoring and the reset action is triggered by a signature firing.
  - Select Interface—Sets the interface that sends the TCP reset.

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

- Description—Lets you provide a description of the interface.
- LACP Settings—Lets you enable LACP if your sensor is configured as an inline VLAN pair:
  - LACP Mode—Lets you set LACP to Active, Passive, or Off mode on the interface. The default is Off.

    LACP has two modes of operation: active and passive. Because LACP is a point-to-point protocol, in active mode, LACPDUs are periodically sent to actively probe for LACP support on the device other side. If the device on the other side responds to the LACP packets, an LACP connection is initiated. If LACP mode is configured active, this is done as soon as the physical link is up.

    In passive mode, the device does not actively send any LACP packets to probe LACP devices on the other end. It waits for the other side to probe and initiate an LACP connection. This can work only if the device on the other side supports LACP and is configured in active mode.
  - LACP Channel ID—Let you create a port channel identifier. The range is 1 to 255. The default is 1.

Editing Interfaces

To edit the interface settings, follow these steps:

Step 1 Log in to the IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Interfaces > Interfaces**.

Step 3 Select the interface and click **Edit**.

Note You can also double-click the interface and the Edit Interface dialog box appears.

Step 4 Change the state from enabled to disabled by checking the **No** or **Yes** check box.

Step 5 Change the Duplex and Speed settings, but clicking the drop-down menu and choosing a new value.

Step 6 You can have the interface use the alternate TCP reset interface by checking the **Use Alternative TCP Reset Interface** check box and then choose an interface from the Select Interface drop-down menu.

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

Step 7 You can change the description in the Description field.

Note Change the LACP settings:

a. Choose Active, Passive, or Off from the LACP Mode drop-down menu. The default is Off.

b. Enter an LACP channel ID in the LACP Channel ID field. The valid value is 1 to 255. The default is 1.

Note You can only apply LACP settings to interfaces that are configured in inline VLAN pairs.

Tip To discard your changes and close the Edit Interface dialog box, click **Cancel**.

Step 8 Click **OK**. The edited interface appears in the list in the Interfaces pane.

Tip To discard your changes, click **Reset**.

Step 9 Click **Apply** to apply your changes and save the revised configuration.

Configuring LACP

This section describes how to configure LACP on your 4500 series sensor, and contains the following topics:

LACP Pane

In the LACP pane, you can configure the system priority and the node identifier. Make sure you have LACP configured on your switch before setting system priority and creating a node ID on the sensor.

Note We do not recommend that you enable LACP unless you are sure of the configuration on the other side.

For More Information

For detailed information about LACP on the 4500 series sensors, see Understanding ECLB Using LACP, page 7-15.

LACP Restrictions

Note We do not recommend that you configure UDLD with LACP.

Pay attention to the following when configuring LACP on the sensor:

- The IPS 4520 is the only platform that supports the dual configuration. You can add another 4520 module to an existing 4520 or you can order the 4520-XL with two modules already installed. Mixing 4510s and 4520s is not a valid configuration.
- Make sure that in your ECLB setup, you do not have multiple links within an EtherChannel going to the same IPS device, because this can lead to a load distribution imbalance.
- When a group of IPS devices participate in an LACP ether channel as one single device, the devices should all have the same system ID. The default system ID ensures this. However, if you have a requirement to have two different IPSes to have different system IDs in order to be able to distinguish them in the show LACP neighbor output, you can configure the LACP system priority, which influences the system ID.
- Make sure that the IPS interface that is part of the same LACP port channel is configured with the same VLAN pair.
- Make sure that bypass mode is off so that IPS can failover and fallback during failure conditions.
- Make sure the TCP session tracking mode is assigned to the virtual sensor, which is the default.

Understanding Failover/Fallback

The IPS has enhanced the support for seamless failover/fallback of TCP sessions from one sensor to another (nonconnection-based traffic, such as UDP and ICMP already had seamless support). The IPS determines that a gap in the state of the sessions being monitored may have been caused by failover/bypass/link flaps. It intelligently updates its state machine to restart the inspection of the sessions and ensures that the flows do not get dropped.

LACP Link States

The LACP link state represents whether the link can forward traffic or not and does not represent the actual link state of the physical port. LACP has two link states:

- Up—When the interface is up and the LACP state is either bundled or independent.
- Down (LACP suspended)—When the LACP configuration is mismatched on both ends, which means the LACP state is suspended and the switch does not allow traffic.

The following sequence of event leads to a link being up:

1. At least two sensors are configured with the same channel ID.
2. LACP is configured on both the switch and the sensor.
3. The sensor participating in the same port channel must have the same system priority and channel ID.
4. Interfaces participating in LACP must all have the same duplex and speed configuration.
5. The physical interface is up.

The following sequence of events leads to a link going down.

1. LACP is down.
2. The SensorApp is down.
3. The physical interface is down.

LACP Field Definitions

The following fields are found in the LACP pane:

- LACP System Priority—Lets you add an LACP system priority to the sensor. The system priority is assigned to the system by the management or administration policy and is encoded as an unsigned integer. Make sure the system priority is the same number across all of the nodes in the port channel. The range is 1 to 65535. The default is 32768.
- LACP Node Identifier—Lets you add an LACP node identifier to the sensor. This ID uniquely identifies the node in the LACP group. The node is used internally to form the port number. The range is 1 to 16. The default is 1.

Enabling LACP on the Sensor

Note Make sure that you have LACP configured on a Cisco Nexus 7K or Catalyst 6K switch before configuring LACP on the sensor.

To enable LACP on a sensor, follow these steps:

Step 1 Configure LACP on your switch. Refer to your switch user documentation for the procedure.

Step 2 Configure inline VLAN pairs on the sensor.

Step 3 Log in to the IME using an account with administrator privileges.

Step 4 Choose **Configuration > *sensor_name* > Interfaces > LACP**.

Step 5 In the LACP System Priority field, assign an LACP system priority to the sensor.The range is 1 to 65535. The default is 32768.

Note Make sure the system priority is the same number across all of the nodes in the port channel.

Step 6 In the LACP Node Identifier field, assign an LACP node ID. The range is 1 to 16. The default is 1.

Note This ID uniquely identifies the node in the LACP group.

Step 7 Click **Apply**.

Step 8 Choose **Configuration** > *sensor_name* > **Interfaces**, select the interface in the list for which you want to enable LACP, and click **Edit.**

Step 9 Under LACP settings, do the following:

a. Choose **Active** from the LACP Mode drop-down menu.

b. Enter an LACP channel ID (1 to 255) in the LACP Channel ID field. The default is 1.

Note You can only apply LACP settings to interfaces that are configured in inline VLAN pairs.

Tip To discard your changes and close the Edit Interface dialog box, click **Cancel**.

Step 10 Click **OK**. The edited interface appears in the list in the Interfaces pane.

Tip To discard your changes, click **Reset**.

Step 11 Click **Apply** to apply your changes and save the revised configuration.

For More Information

For more information on monitoring LACP, see Monitoring LACP, page 20-18.

Configuring Inline Interface Pairs

This section describes how to set up inline interface pairs, and contains the following topics:

Interface Pairs Pane

Note You must be administrator to configure interface pairs.

You can pair interfaces on your sensor if your sensor is capable of inline monitoring.

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not need an inline pair for monitoring. You only need to add the physical interface to a virtual sensor.

For More Information

- For the procedure for configuring the ASA 5585-X IPS SSP in inline mode, refer to Configuring the ASA 5585-X IPS SSP.
- For the procedure for configuring the ASA 5500-X IPS SSP in inline mode, refer to Configuring the ASA 5500-X IPS SSP.

Interface Pairs Pane Field Definitions

The following fields are found in the Interface Pairs pane:

- Interface Pair Name—The name you give the interface pair.
- Paired Interfaces—The two interfaces that you have paired (for example, GigabitEthernet 0/0<->GigabitEthernet 0/1).
- Description—Lets you add a description of this interface pair.

Add and Edit Interface Pair Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Interface Pair dialog boxes:

- Interface Pair Name—Indicates the name you give the interface pair.
- Select two interfaces—Lets you select two interfaces from the list to pair (for example, GigabitEthernet 0/0<->GigabitEthernet 0/1).
- Description—Lets you add a description of this interface pair.

Configuring Inline Interface Pairs

To configure inline interface pairs, follow these steps:

Step 1 Log in to the IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Interfaces > Interface Pairs**, and then click **Add**.

Step 3 Enter a name in the Interface Pair Name field. The inline interface name is a name that you create.

Step 4 Select two interfaces to form a pair in the Select two interfaces field. For example, GigabitEthernet 0/0 and GigabitEthernet 0/1.

Step 5 You can add a description of the inline interface pair in the Description field if you want to.

Tip To discard your changes and close the Add Interface pair dialog box, click **Cancel**.

Step 6 Click **OK**. The new inline interface pair appears in the list in the Interface Pairs pane.

Step 7 To edit an inline interface pair, select it, and click **Edit**.

Step 8 You can change the name, choose a new inline interface pair, or edit the description.

Tip To discard your changes and close the Edit Interface Pair dialog box, click **Cancel**.

Step 9 Click **OK**. The edited inline interface pair appears in the list in the Interface Pairs pane.

Step 10 To delete an inline interface pair, select it, and click **Delete**. The inline interface pair no longer appears in the list in the Interface Pairs pane.

Tip To discard your changes, click **Reset**.

Step 11 Click **Apply** to apply your changes and save the revised configuration.

Configuring Inline VLAN Pairs

This section describes how to configure inline VLAN pairs, and contains the following topics:

VLAN Pairs Pane

Note You must be administrator to configure inline VLAN pairs.

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support inline VLAN pairs.

Note For the IPS 4500 series sensors, the maximum number of inline VLAN pairs you can create system-wide is 150. On all other platforms, the limit is 255 per interface.

The VLAN Pairs pane displays the existing inline VLAN pairs for each physical interface. Click **Add** to create an inline VLAN pair. To create an inline VLAN pair for an interface that is in promiscuous mode, you must remove the interface from the virtual sensor and then create the inline VLAN pair. If the interface is already paired or in promiscuous mode, you receive an error message when you try to create an inline VLAN pair.

Note You cannot create an inline VLAN pair for an interface that has already been paired with another interface or for an interface that is in promiscuous mode and assigned to a virtual sensor.

Note You cannot use the default VLAN as one of the paired VLANs in an inline VLAN pair.

For More Information

For detailed information on interface configuration restrictions, see Interface Configuration Restrictions, page 7-8.

VLAN Pairs Pane Field Definitions

The following fields are found in the VLAN Pairs pane:

- Interface Name—Displays the name of the inline VLAN pair.
- Subinterface—Displays the subinterface number of the inline VLAN pair. The value is 1 to 255.
- VLAN A—Displays the VLAN number for the first VLAN. The value is 1 to 4095.
- VLAN B—Displays the VLAN number for the second VLAN. The value is 1 to 4095.
- Description—Displays your description of the inline VLAN pair.

Add and Edit VLAN Pair Dialog Boxes Field Definitions

The following fields are found in the Add and Edit Inline VLAN Pair dialog boxes:

- Interface Name—Specifies the name of the interface you want to pair.
- Subinterface Number—Lets you assign a subinterface number. You can assign a number from 1 to 255.
- VLAN A—Lets you specify the first VLAN for this inline VLAN pair. You can assign any VLAN from 1 to 4095.
- VLAN B—Lets you specify the other VLAN for this inline VLAN pair. You can assign any VLAN from 1 to 4095.
- Description—Lets you add a description of this inline VLAN pair.

Note You cannot pair a VLAN with itself. The subinterface number and the VLAN numbers should be unique to each physical interface.

Configuring Inline VLAN Pairs

To configure inline VLAN pairs, follow these steps:

Step 1 Log in to the IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Interfaces > VLAN Pairs**, and then click **Add**.

Step 3 Choose an interface from the **Interface Name** list.

Step 4 In the Subinterface Number field, enter a subinterface number (1 to 255) for the inline VLAN pair.

Step 5 In the VLAN A field, specify the first VLAN (1 to 4095) for this inline VLAN pair.

Step 6 In the VLAN B field, specify the other VLAN (1 to 4095) for this inline VLAN pair.

Step 7 In the Description field, add a description of the inline VLAN pair if desired.

Tip To discard your changes and close the Add VLAN Pair dialog box, click **Cancel**.

Step 8 Click **OK**. The new inline VLAN pair appears in the list in the VLAN Pairs pane.

Step 9 To edit an inline VLAN pair, select it, and click **Edit**.

Step 10 You can change the subinterface number, the VLAN numbers, or edit the description.

Tip To discard your changes and close the Edit VLAN Pair dialog box, click **Cancel**.

Step 11 Click **OK**. The edited VLAN pair appears in the list in the VLAN Pairs pane.

Step 12 To delete a VLAN pair, select it, and click **Delete**. The VLAN pair no longer appears in the list in the VLAN Pairs pane.

Tip To discard your changes, click **Reset**.

Step 13 Click **Apply** to apply your changes and save the revised configuration.

Configuring VLAN Groups

This section describes how to configure VLAN groups, and contains the following topics:

VLAN Groups Pane

Note You must be administrator to configure VLAN groups.

Note The ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP) do not support VLAN groups mode.

In the VLAN Groups pane you can add, edit, or delete VLAN groups that you defined in the sensor interface configuration. A VLAN group consists of a group of VLAN IDs that exist on an interface. Each VLAN group consists of at least one VLAN ID. You can have up to 255 VLAN groups per interface

(logical or physical). Each group can contain any number of VLANs IDs. You then assign each VLAN group to a virtual sensor (but not multiple virtual sensors). You can assign different VLAN groups on the same sensor to different virtual sensors.

After you assign the VLAN IDs to the VLAN group, you must assign the VLAN group to a virtual sensor. The IME cross-validates between the interface and virtual sensor configuration. Any configuration changes in one component that could invalidate the other is blocked.

For More Information

For the procedure for assigning the VLAN group to a virtual sensor, see Adding, Editing, and Deleting Virtual Sensors, page 8-12.

Deploying VLAN Groups

Because a VLAN group of an inline pair does not translate the VLAN ID, an inline paired interface must exist between two switches to use VLAN groups on a logical interface. For an appliance, you can connect the two pairs to the same switch, make them access ports, and then set the access VLANs for the two ports differently. In this configuration, the sensor connects between two VLANs, because each of the two ports is in access mode and carries only one VLAN. In this case the two ports must be in different VLANs, and the sensor bridges the two VLANs, monitoring any traffic that flows between the two VLANs.

You can also connect appliances between two switches. There are two variations. In the first variation, the two ports are configured as access ports, so they carry a single VLAN. In this way, the sensor bridges a single VLAN between the two switches.

In the second variation, the two ports are configured as trunk ports, so they can carry multiple VLANs. In this configuration, the sensor bridges multiple VLANs between the two switches. Because multiple VLANs are carried over the inline interface pair, the VLANs can be divided into groups and each group can be assigned to a virtual sensor.

VLAN Groups Pane Field Definitions

The following fields are found in the VLAN Groups pane:

- Interface Name—Displays the physical or logical interface name of the VLAN group.
- Subinterface—Displays the subinterface number of the VLAN group. The value is 1 to 255.
- VLAN Group—Displays the VLAN number for the VLAN group. The value is 1 to 4095.
- Description—Displays your description of the VLAN group.

Add and Edit VLAN Group Dialog Boxes Field Definitions

The following fields are found in the Add and Edit VLAN Group dialog boxes:

- Interface Name—Specifies the name of the VLAN group.
- Subinterface Number—Specifies the subinterface number of the VLAN group. The value is 1 to 255.
- VLAN Group—Displays the VLAN number for the VLAN group:
  - Unassigned VLANS—Lets you choose all VLANS that have not yet been assigned to a VLAN group.

  - Specify VLAN Group—Lets you specify the VLAN IDs that you want to assign to this VLAN group. The value is 1 to 4095 in a comma-separated pattern of individual VLAN IDs or ranges: 1, 5-8, 10-15.
- Description—Lets you add a description of the VLAN group.

Configuring VLAN Groups

To configure VLAN groups, follow these steps:

Step 1 Log in to the IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Interfaces > VLAN Groups**, and then click **Add**.

Step 3 From the Interface Name drop-down list, choose an interface.

Step 4 In the Subinterface Number field, enter a subinterface number (1 to 255) for the VLAN group.

Step 5 Under VLAN Group, specify the VLAN group for this interface by checking one of the following check boxes:

a. **Unassigned VLANs**—Lets you assign all the VLANs that are not already specifically assigned to a subinterface.

b. **Specify VLAN Group**—Lets you specify the VLANs that you want to assign to this subinterface. You can assign more than one VLAN (1 to 4096) in this pattern: 1, 5-8, 10-15. This lets you set up different policies based on VLAN ID. For example, you can make VLANs 1-10 go to one virtual sensor (VS0) and VLANs 20-30 go to another virtual sensor (VS1).

Note You need to have the VLAN IDs that are set up on your switch to enter in the Specify VLAN Group field.

Step 6 You can add a description of the VLAN group in the Description field if you want to.

Tip To discard your changes and close the Add VLAN Group dialog box, click **Cancel**.

Step 7 Click **OK**. The new VLAN group appears in the list in the VLAN Groups pane. You must assign this VLAN group to a virtual sensor.

Step 8 To edit a VLAN group, select it, and click **Edit**.

Step 9 You can change the subinterface number, the VLAN group, or edit the description.

Tip To discard your changes and close the Edit VLAN Group dialog box, click **Cancel**.

Step 10 Click **OK**. The edited VLAN group appears in the list in the VLAN Groups pane.

Step 11 To delete a VLAN group, select it, and click **Delete**. The VLAN group no longer appears in the list in the VLAN Groups pane.

Tip To discard your changes, click **Reset**.

Step 12 Click **Apply** to apply your changes and save the revised configuration.

Configuring Bypass Mode

This section describes how to configure bypass mode, and contains the following topics:

Bypass Pane

Note You must be administrator to configure bypass mode on the sensor.

Note The ASA 5500-X IPS SSP and ASA 5585-X IPS SSP do not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.

Caution There are security consequences when you put the sensor in bypass mode. When bypass mode is on, the traffic bypasses the sensor and is not inspected; therefore, the sensor cannot prevent malicious attacks.

Caution As with signature updates, when the sensor applies a global correlation update, it may trigger bypass. Whether or not bypass is triggered depends on the traffic load of the sensor and the size of the signature/global correlation update. If bypass mode is turned off, an inline sensor stops passing traffic while the update is being applied.

You can use inline bypass as a diagnostic tool and a failover protection mechanism. Normally, the sensor Analysis Engine performs packet analysis. When inline bypass is activated, the Analysis Engine is bypassed, allowing traffic to flow through the inline interfaces and inline VLAN pairs without inspection. Inline bypass ensures that packets continue to flow through the sensor when the sensor processes are temporarily stopped for upgrades or when the sensor monitoring processes fail. There are three modes: on, off, and automatic. By default, bypass mode is set to automatic.

The inline bypass functionality is implemented in software, so it only functions when the operating system is running. If the sensor is powered off or shut down, inline bypass does not work—traffic does not flow through the sensor.

For IPS 4500 series sensors, when the SensorApp is not running or if bypass mode is on, the following occurs:

- The output from the **packet capture/display** command does not show any packets.
- The **show interface** and **show interface** *interface_name* commands do not show VLAN statistics.

Bypass Pane Field Definitions

The following fields are found in the Bypass pane:

- Auto—Traffic flows through the sensor for inspection unless the monitoring process of the sensor is down. If the monitoring process of the sensor is down, traffic bypasses the sensor until the sensor is running again. The sensor then inspects the traffic. Auto mode is useful during sensor upgrades to ensure that traffic is still flowing while the sensor is being upgraded. Auto mode also helps to ensure traffic continues to pass through the sensor if the monitoring process fails.
- Off—Disables bypass mode. Traffic flows through the sensor for inspection. If the monitoring process of the sensor is down, traffic stops flowing. This means that inline traffic is always inspected.
- On—Traffic bypasses the Analysis Engine and is not inspected. This means that inline traffic is never inspected.

Configuring Traffic Flow Notifications

Note You must be administrator to configure traffic flow notifications.

You can configure the sensor to monitor the flow of packets across an interface and send notification if that flow changes (starts/stops) during a specified interval. You can configure the missed packet threshold within a specific notification interval and also configure the interface idle delay before a status event is reported.

Field Definitions

The following fields are found in the Traffic Flow Notifications pane:

- Missed Packets Threshold—Specifies the percentage of packets that must be missed during a specified time before a notification is sent.
- Notification Interval—Specifies the interval the sensor checks for the missed packets percentage.
- Interface Idle Threshold—Specifies the number of seconds an interface must be idle and not receiving packets before a notification is sent.

Configuring Traffic Flow Notifications

To configure traffic flow notifications, follow these steps:

Step 1 Log in to the IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Interfaces > Traffic Flow Notifications**.

Step 3 In the Missed Packets Threshold field, specify the percent of missed packets that has to occur before you want to receive notification and enter that amount.

Step 4 In the Notification Interval field, specify the amount of seconds that you want to check for the percentage of missed packets and enter that amount.

Step 5 In the Interface Idle Threshold field, specify the amount of seconds that you will allow an interface to be idle and not receiving packets before you want to be notified and enter that.

Tip To discard your changes, click **Reset**.

Step 6 Click **Apply** to apply your changes and save the revised configuration.

Configuring CDP Mode

Note You must be administrator to configure CDP mode.

Note The ASA 5500-X IPS SSP and ASA 5585-X IPS SSP do not support CDP mode.

You can configure the sensor to enable or disable the forwarding of CDP packets. This action applies globally to all interfaces.

Cisco Discovery Protocol is a media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. CDP runs on all media that support SNAP, including LANs, Frame Relay, and ATM media.

Field Definitions

The following fields are found in the CDP Mode pane:

- Drop CDP Packets—Specifies that the sensor does not forward CDP packets.
- Forward CDP Packets—Specifies that the sensor forwards CDP packets.

Configuring CDP Mode

To configure CDP mode, follow these steps:

Step 1 Log in to the IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Interfaces > CDP Mode**.

Step 3 From the CDP Mode drop-down list, choose either Drop CDP Packets (default) or Forward CDP Packets.

Tip To discard your changes, click **Reset**.

Step 4 Click **Apply** to apply your changes and save the revised configuration.