



CHAPTER 5

Configuring Interfaces

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

- [Understanding Interfaces, page 5-1](#)
- [Understanding Interface Modes, page 5-11](#)
- [Interface Configuration Summary, page 5-15](#)
- [Configuring Interfaces, page 5-16](#)
- [Configuring Inline Interface Pairs, page 5-19](#)
- [Configuring Inline VLAN Pairs, page 5-21](#)
- [Configuring VLAN Groups, page 5-24](#)
- [Configuring Bypass Mode, page 5-27](#)
- [Configuring Traffic Flow Notifications, page 5-29](#)
- [Configuring CDP Mode, page 5-30](#)

Understanding Interfaces

This section describes the IPS interfaces and modes, and contains the following topics:

- [IPS Sensor Interfaces, page 5-1](#)
- [Command and Control Interface, page 5-2](#)
- [Sensing Interfaces, page 5-3](#)
- [Interface Support, page 5-4](#)
- [TCP Reset Interfaces, page 5-6](#)
- [Interface Configuration Restrictions, page 5-8](#)
- [Hardware Bypass Mode, page 5-10](#)

IPS Sensor 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 PCI expansion slots are numbered beginning with slot 1 for the

bottom slot with the slot numbers increasing from bottom to top (except for the IPS 4270-20, where the ports are numbered from top to bottom). Interfaces with a given slot are numbered beginning with port 0 for the right port with the port numbers increasing from right to left. For example, GigabitEthernet2/1 supports a maximum speed of 1 Gigabit and is the second-from-the-right interface in the second-from-the bottom PCI expansion slot. The IPS 4240, IPS 4255, IPS 4260, and IPS 4270-20 are exceptions to this rule. The command and control interface on these sensors is called Management0/0 rather than GigabitEthernet0/0. IPS 4270-20 has an additional interface called Management0/1, which is reserved for future use.

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. The following restrictions apply:

- Because the AIM IPS, AIP SSM, and NME IPS only have one sensing interface, you cannot configure a TCP reset interface.
- Because of hardware limitations on the Catalyst switch, both of the IDSM2 sensing interfaces are permanently configured to use System0/1 as the TCP reset interface.
- 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 Each physical interface can be divided into VLAN group subinterfaces, each of which consists of a group of VLANs on that interface.

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 5-1 lists the command and control interfaces for each sensor.

Table 5-1 *Command and Control Interfaces*

Sensor	Command and Control Interface
AIM IPS	Management0/0
AIP SSM-10	GigabitEthernet0/0
AIP SSM-20	GigabitEthernet0/0
AIP SSM-40	GigabitEthernet0/0
IDSM2	GigabitEthernet0/2

Table 5-1 *Command and Control Interfaces (continued)*

Sensor	Command and Control Interface
IPS 4240	Management0/0
IPS 4255	Management0/0
IPS 4260	Management0/0
IPS 4270-20	Management0/0
NME IPS	Management0/1

Sensing 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.

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.

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 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 5-4](#).
- For more information on interface modes, see [Understanding Interface Modes, page 5-11](#).
- For the procedure for configuring virtual sensors, see [Adding, Editing, and Deleting Virtual Sensors, page 6-11](#).

Interface Support

Table 5-2 describes the interface support for appliances and modules running Cisco IPS.

Table 5-2 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)
AIM IPS	—	GigabitEthernet0/1 by ids-service-module command in the router configuration instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by ids-service-module command in the router configuration instead of VLAN pair or inline interface pair	Management0/0
AIP SSM-10	—	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/0
AIP SSM-20	—	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/0
AIP SSM-40	—	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/0
IDSM2	—	GigabitEthernet0/7 GigabitEthernet0/8	0/7<->0/8	GigabitEthernet0/2
IPS 4240	—	GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS 4255	—	GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS 4260	—	GigabitEthernet0/1	N/A	Management0/0

Table 5-2 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 4260	4GE-BP	GigabitEthernet0/1		Management0/0
	Slot 1	GigabitEthernet2/0 GigabitEthernet2/1 GigabitEthernet2/2 GigabitEthernet2/3	2/0<->2/1 ¹ 2/2<->2/3	
	Slot 2	GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet3/2 GigabitEthernet3/3	3/0<->3/1 3/2<->3/3	
IPS 4260	2SX	GigabitEthernet0/1	All sensing ports can be paired together	Management0/0
	Slot 1	GigabitEthernet2/0 GigabitEthernet2/1		
	Slot 2	GigabitEthernet3/0 GigabitEthernet3/1		
IPS 4260	10GE	GigabitEthernet0/1		Management0/0
	Slot 1	TenGigabitEthernet2/0 TenGigabitEthernet2/1	2/0<->2/1 ²	
IPS 4270-20	—	—	N/A	Management0/0 Management0/1 ³
IPS 4270-20	4GE-BP			Management0/0 Management0/1 ⁵
	Slot 1	GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet3/2 GigabitEthernet3/3	3/0<->3/1 ⁴ 3/2<->3/3	
	Slot 2	GigabitEthernet4/0 GigabitEthernet4/1 GigabitEthernet4/2 GigabitEthernet4/3	4/0<->4/1 4/2<->4/3	
IPS 4270-20	2SX		All sensing ports can be paired together	Management0/0 Management0/1 ⁶
	Slot 1	GigabitEthernet3/0 GigabitEthernet3/1		
	Slot 2	GigabitEthernet4/0 GigabitEthernet4/1		

Table 5-2 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 4270-20	10GE Slot 1 Slot 2	TenGigabitEthernet5/0 TenGigabitEthernet5/1 TenGigabitEthernet7/0 TenGigabitEthernet7/1	All sensing ports can be paired together	Management0/0 Management0/1 ⁷
NME IPS	—	GigabitEthernet0/1 by ids-service-module command in the router configuration instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by ids-service-module command in the router configuration instead of VLAN pair or inline interface pair	Management0/1

1. To disable hardware bypass, pair the interfaces in any other combination (2/0<->2/2 and 2/1<->2/3, for example).
2. To disable hardware bypass, pair the interfaces in any other combination (2/0<->2/2 and 2/1<->2/3, for example).
3. Reserved for future use.
4. To disable hardware bypass, pair the interfaces in any other combination (2/0<->2/2 and 2/1<->2/3, for example).
5. Reserved for future use.
6. Reserved for future use.
7. Reserved for future use.

**Note**

The IPS 4260 supports a mixture of 4GE-BP, 2SX, and 10GE cards. The IPS 4270-20 also supports a mixture of 4GE-BP, 2SX, and 10GE cards up to a total of either six cards, or sixteen total ports, whichever is reached first, but is limited to only two 10GE card in the mix of cards.

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, page 5-6](#)
- [Designating the Alternate TCP Reset Interface, page 5-7](#)

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.

With the exception of the IDSM2, any sensing interface can serve as the alternate TCP reset interface for another sensing interface. The alternate TCP reset interface on the IDSM2 is fixed because of hardware limitation.

Table 5-3 lists the alternate TCP reset interfaces.



Note

There is only one sensing interface on IPS modules (AIM IPS, AIP SSM, and NME IPS).

Table 5-3 *Alternate TCP Reset Interfaces*

Sensor	Alternate TCP Reset Interface
AIM IPS	None
AIP SSM-10	None
AIP SSM-20	None
AIP SSM-40	None
IDSM2	System0/1 ¹
IPS 4240	Any sensing interface
IPS 4255	Any sensing interface
IPS 4260	Any sensing interface
IPS 4270-20	Any sensing interface
NME IPS	None

1. This is an internal interface on the Catalyst backplane.

Designating the 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.



Note

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.



Note

Taps do not permit incoming traffic from the sensor.

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

**Note**

For IPS standalone appliances with 1 G and 10 G fixed or add-on interfaces, the maximum jumbo frame size is 9216 bytes. A jumbo frame is an Ethernet packet that is larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS).

The following restrictions apply to configuring interfaces on the sensor:

- Physical Interfaces
 - On modules (AIM IPS, AI P SSM, IDSM2, and NME IPS), 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 4240, IPS 4255, IPS 4260, and IPS 4270-20), 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**.
- 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.

- 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 The exception to this restriction is the IDSM2. The alternate TCP reset interface assignments for both sensing interfaces is System0/1 (protected).

- 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.
 - CLI, IDM, and IME prompt you to remove any dangling references. You can leave the dangling references and continue editing the configuration.
 - CLI, IDM, and IME do not allow configuration changes in Analysis Engine that conflict with the interface configuration.
 - 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.

For More Information

For more information on interface pair combinations, see [Interface Support, page 5-4](#).

Hardware Bypass Mode

In addition to Cisco IPS software bypass, the IPS 4260 and the IPS 4270-20 also support hardware bypass. This section describes the hardware bypass card and its configuration restrictions, and contains the following topics:

- [Hardware Bypass Card, page 5-10](#)
- [Hardware Bypass Configuration Restrictions, page 5-11](#)

Hardware Bypass Card

The IPS 4260 and the IPS 4270-20 support the 4-port GigabitEthernet card (part number IPS-4GE-BP-INT=) with hardware bypass. This 4GE bypass interface card supports hardware bypass only between ports 0 and 1 and between ports 2 and 3.

**Note**

To disable hardware bypass, pair the interfaces in any other combination, for example 2/0<->2/2 and 2/1<->2/3.

Hardware bypass complements the existing software bypass feature in Cisco IPS. The following conditions apply to hardware bypass and software bypass:

- When bypass is set to OFF, software bypass is not active.
For each inline interface for which hardware bypass is available, the component interfaces are set to disable the fail-open capability. If SensorApp fails, the sensor is powered off, reset, or if the NIC interface drivers fail or are unloaded, the paired interfaces enter the fail-closed state (no traffic flows through inline interface or inline VLAN subinterfaces).
- When bypass is set to ON, software bypass is active.
Software bypass forwards packets between the paired physical interfaces in each inline interface and between the paired VLANs in each inline VLAN subinterface. For each inline interface on which hardware bypass is available, the component interfaces are set to standby mode. If the sensor is powered off, reset, or if the NIC interfaces fail or are unloaded, those paired interfaces enter fail-open state in hardware (traffic flows unimpeded through inline interface). Any other inline interfaces enter fail-closed state.
- When bypass is set to AUTO (traffic flows without inspection), software bypass is activated if SensorApp fails.
For each inline interface on which hardware bypass is available, the component interfaces are set to standby mode. If the sensor is powered off, reset, or if the NIC interfaces fail or are unloaded, those paired interfaces enter fail-open state in hardware. Any other inline interfaces enter the fail-closed state.

**Note**

To test fail-over, set the bypass mode to ON or AUTO, create one or more inline interfaces and power down the sensor and verify that traffic still flows through the inline path.

For More Information

- For the procedure for installing and removing the hardware bypass card, for the IPS 4260 refer to [Installing and Removing Interface Cards](#), and for the IPS 4270-20 refer to [Installing and Removing Interface Cards](#).
- For the procedure for configuring bypass mode, see [Configuring Bypass Mode, page 5-27](#).

Hardware Bypass Configuration Restrictions

To use the hardware bypass feature on the 4GE bypass interface card, you must pair interfaces to support the hardware design of the card. If you create an inline interface that pairs a hardware-bypass-capable interface with an interface that violates one or more of the hardware-bypass configuration restrictions, hardware bypass is deactivated on the inline interface and you receive a warning message similar to the following:

```
Hardware bypass functionality is not available on Inline-interface pair0.  
Physical-interface GigabitEthernet2/0 is capable of performing hardware bypass only when  
paired with GigabitEthernet2/1, and both interfaces are enabled and configured with the  
same speed and duplex settings.
```

The following configuration restrictions apply to hardware bypass:

- The 4-port bypass card is only supported on the IPS 4260 and the IPS 4270-20.
- Fail-open hardware bypass only works on inline interfaces (interface pairs), not on inline VLAN pairs.
- Fail-open hardware bypass is available on an inline interface if all of the following conditions are met:
 - Both of the physical interfaces support hardware bypass.
 - Both of the physical interfaces are on the same interface card.
 - The two physical interfaces are associated in hardware as a bypass pair.
 - The speed and duplex settings are identical on the physical interfaces.
 - Both of the interfaces are administratively enabled.
- Autonegotiation must be set on MDI/X switch ports connected to the IPS 4260 and the IPS 4270-20.

You must configure both the sensor ports and the switch ports for autonegotiation for hardware bypass to work. The switch ports must support MDI/X, which automatically reverses the transmit and receive lines if necessary to correct any cabling problems. The sensor is only guaranteed to operate correctly with the switch if both of them are configured for identical speed and duplex, which means that the sensor must be set for autonegotiation too.

Understanding Interface Modes

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

- [Promiscuous Mode](#)
- [IPv6, Switches, and Lack of VACL Capture, page 5-12](#)
- [Inline Interface Mode](#)
- [Inline VLAN Pair Mode](#)
- [VLAN Group Mode](#)

Promiscuous Mode

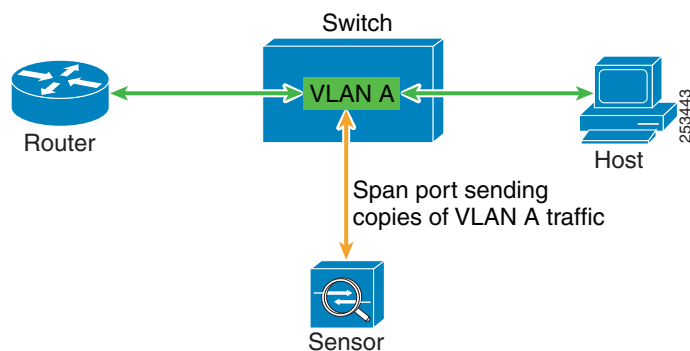
In promiscuous mode, packets do not flow through the sensor. The sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of

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 5-1 illustrates promiscuous mode.

Figure 5-1 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 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](#)
- For more information on promiscuous mode, see [Promiscuous Mode, page 5-11](#).

Inline Interface Mode

**Note**

You can configure the AIM IPS, AIP SSM, and NME IPS to operate inline even though these modules have only one sensing interface.

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.

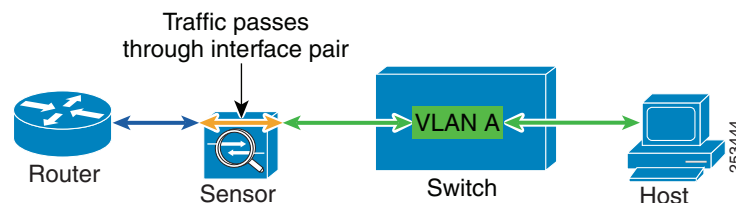
In inline interface pair mode, a packet comes in through the first interface of the pair on the sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

**Note**

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 5-2 illustrates inline interface pair mode.

Figure 5-2 *Inline Interface Pair Mode*



Inline VLAN Pair Mode


Note

Inline VLAN pairs are not supported on the AIM IPS, AIP SSM, and NME IPS.

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.

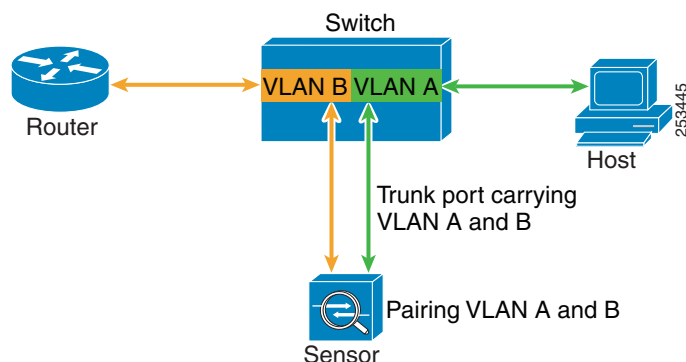
Inline VLAN pair mode is an active sensing mode where a sensing interface acts as an 802.1q trunk port, and the sensor performs VLAN bridging between pairs of VLANs on the trunk. The sensor inspects the traffic it receives on each VLAN in each pair, and can either forward the packets on the other VLAN 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 5-3 illustrates inline VLAN pair mode.

Figure 5-3 *Inline VLAN Pair Mode*



VLAN Group 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 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 to 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. The IDSM2 can read the 802.1q headers for all nonnative traffic to determine the VLAN ID for that packet. However, the IDSM2 does not know which VLAN is configured as the native VLAN for the port in the switch configuration, so it does not know what VLAN the native packets are in. Therefore, you must tell the IDSM2 which VLAN is the native VLAN for that port. Then the IDSM2 treats any untagged packets as if they were tagged with the native VLAN ID.

For More Information

For the procedures for configuring the IDSM2 for VLAN group mode, refer to [Configuring the IDSM2](#).

Interface Configuration Summary

This section describes the Summary pane, and contains the following topics:

- [Summary Pane, page 5-15](#)
- [Summary Pane Field Definitions, page 5-16](#)

Summary Pane

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.

Summary Pane Field Definitions

The following fields are found in the Summary pane:

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

Configuring Interfaces

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

- [Interfaces Pane, page 5-16](#)
- [Interfaces Pane Field Definitions, page 5-17](#)
- [Edit Interface Dialog Box Field Definitions, page 5-17](#)
- [Enabling and Disabling Interfaces, page 5-18](#)
- [Editing Interfaces, page 5-18](#)

Interfaces Pane

**Note**

You must be administrator to 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.

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 > Policies > IPS Policies > Add Virtual Sensor**.

Interfaces Pane Field Definitions

The following fields are found in the Interfaces pane:

- Interface Name—Name of the interface. The values are FastEthernet or GigabitEthernet for all interfaces.
- Enabled—Whether or not the interface is enabled.
- 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).
- Default VLAN—Indicates which VLAN the interface is assigned to.
- 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.
- Description—Lets you provide a description of the interface.

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 or GigabitEthernet 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).
- Default VLAN—VLAN ID associated with native traffic, or 0 if unknown or if you do not care which VLAN it is.
- 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.
- Description—Lets you provide a description of the interface.

Enabling and Disabling Interfaces

To enable or disable an interface, follow these steps:

-
- Step 1** Log in to the IDM using an account with administrator privileges.
 - Step 2** Choose **Configuration > 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.
-

Editing Interfaces

To edit the interface settings, follow these steps:

-
- Step 1** Log in to the IDM using an account with administrator privileges.
 - Step 2** Choose **Configuration > 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 You can change the description in the Description field, or change the state from enabled to disabled by checking the **No** or **Yes** check box. You can have the interface use the alternate TCP reset interface by checking the **Use Alternative TCP Reset Interface** check box.



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

Step 5 Click **OK**. The edited interface appears in the list in the Interfaces pane.



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

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

Configuring Inline Interface Pairs

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

- [Interface Pairs Pane, page 5-19](#)
- [Interface Pairs Pane Field Definitions, page 5-19](#)
- [Add and Edit Interface Pair Dialog Boxes Field Definitions, page 5-20](#)
- [Configuring Inline Interface Pairs, page 5-20](#)

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 AIM IPS, AIP SSM, and NME IPS 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 AIP SSM in inline mode, refer to [Configuring the AIP SSM](#).

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, GigabitEthernet0/0<->GigabitEthernet0/1).
- **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—The name you give the interface pair.
- Select two interfaces—Lets you select two interfaces from the list to pair (for example, GigabitEthernet0/0<->GigabitEthernet0/1).
- 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 IDM using an account with administrator privileges.
- Step 2** Choose **Configuration > 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, GigabitEthernet0/0 and GigabitEthernet0/1.
- 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, page 5-21](#)
- [VLAN Pairs Pane Field Definitions, page 5-22](#)
- [Add and Edit VLAN Pair Dialog Boxes Field Definitions, page 5-22](#)
- [Configuring Inline VLAN Pairs, page 5-22](#)
- [Configuring UDLD, page 5-23](#)

VLAN Pairs Pane

**Note**

You must be administrator to configure inline VLAN pairs.

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**

If your sensor does not support inline VLAN pairs, the VLAN Pairs pane is not displayed. The AIM IPS, AIP SSM, and NME IPS do not support inline VLAN pairs.

**Note**

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

VLAN Pairs Pane Field Definitions

The following fields are found in the VLAN Pairs pane:

- Interface Name—Name of the inline VLAN pair.
- Subinterface—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—Your description of the inline VLAN pair.

Add and Edit VLAN Pair Dialog Boxes Field Definitions

**Note**

You cannot pair a VLAN with itself.

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

- Interface Name—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**

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 IDM using an account with administrator privileges.
 - Step 2** Choose **Configuration > 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 UDLD

UniDirectional Link Detection (UDLD) is a protocol that Cisco switches use to prevent spanning-tree forwarding loops and to prevent single direction links in switched networks. IPS appliances configured in inline VLAN pair mode are now able to respond to UDLD packets received from the switch. You can enable UDLD protocol on the switch so that the switch can detect when the appliance has entered an error state in which packets are being sent to the appliance, but the appliance is no longer sending packets back to the switch. Before UDLD support was available, spanning tree and EtherChannel configurations were unable to detect certain appliance failures, which resulted in either spanning-tree loops or the switch not using alternate routes for the packets.



Note No special configuration is necessary on the appliance. Configure the appliance for inline VLAN pairs and make sure its interfaces are enabled.

To configure a Catalyst 6500 series switch to use UDLD with an appliance configured in inline VLAN pair mode, follow these steps:

- Step 1** Log in to the console.
- Step 2** Globally enable UDLD in aggressive mode and prevent the switch from automatically restoring an interface that has been disabled by UDLD.

```
switch(config)# udld aggressive
switch(config)# no errdisable recovery cause udld
switch(config)# errdisable detect cause udld
switch(config)# udld message time 7
```

- Step 3** Configure the switch interface connected to the sensor interface for UDLD aggressive mode.

```
switch(config)# interface gigabitethernet slot/port
switch(config-if)# udld port aggressive
```

Repeat Step 3 for each switch interface connected to the sensor interface.

- Step 4** If UDLD disables a switch port, you must correct the sensor error and recover the switch interface manually. To recover the switch interface, shut down the interface, and then reenable it.

```
switch(config)# interface gigabit ethernet slot/port
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

For More Information

- For information on UDLD, refer to your switch documentation.
- For the procedure for configuring inline VLAN pairs on your appliance, see [Configuring Inline VLAN Pairs, page 5-22](#).

Configuring VLAN Groups

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

- [VLAN Groups Pane, page 5-24](#)
- [Deploying VLAN Groups, page 5-25](#)
- [VLAN Groups Pane Field Definitions, page 5-25](#)
- [Add and Edit VLAN Group Dialog Boxes Field Definitions, page 5-25](#)
- [Configuring VLAN Groups, page 5-26](#)

VLAN Groups Pane



Note

You must be administrator to configure VLAN groups.

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 IDM 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 6-11](#).

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. The IDSM2 also operates in this manner, because its two data ports are always connected to the same switch.

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. The second variation does not apply to the IDSM2 because it cannot be connected in this way.

For More Information

For the procedure for configuring the IDSM2 in VLAN groups, refer to [Configuring the IDSM2](#).

VLAN Groups Pane Field Definitions

The following fields are found in the VLAN Groups pane:

- Interface Name—The physical or logical interface name of the VLAN group.
- Subinterface—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—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—Name of the VLAN group.
- Subinterface Number—Subinterface number of the VLAN group. The value is 1 to 255.
- VLAN Group—Displays the VLAN number for the VLAN group.
 - Unassigned VLANS—Let you choose all VLANS that have not yet been assigned to a VLAN group.
 - Specify VLAN group number—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—Your description of the VLAN group.

Configuring VLAN Groups

To configure VLAN groups, follow these steps:

-
- Step 1** Log in to the IDM using an account with administrator privileges.
- Step 2** Choose **Configuration > 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.
-

For More Information

For the procedure for assigning a VLAN group to a virtual sensor, see [Adding, Editing, and Deleting Virtual Sensors](#), page 6-11.

Configuring Bypass Mode

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

- [Bypass Mode Pane, page 5-27](#)
- [Bypass Pane Field Definitions, page 5-27](#)
- [Adaptive Security Appliance, the AIP SSM, and Bypass Mode, page 5-28](#)

Bypass Mode Pane

**Note**

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

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, 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.

**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.

**Note**

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.

**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.

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.

Adaptive Security Appliance, the AIP SSM, and Bypass Mode

The following conditions apply to bypass mode configuration, the adaptive security appliance, and the AIP SSM.

The SensorApp Fails OR a Configuration Update is Taking Place

The following occurs when bypass is set to Auto or Off on the AIP SSM:

- Bypass Auto—Traffic passes without inspection.
- Bypass Off—If the adaptive security appliance is configured for failover, then the adaptive security appliance fails over.

If the adaptive security appliance is not configured for failover or failover is not possible:

- If set to fail-open, the adaptive security appliance passes traffic without sending it to the AIP SSM.
- If set to fail-close, the adaptive security appliance stops passing traffic until the AIP SSM is restarted or completes reconfiguration.



Note

When bypass is set to On, traffic passes without inspection regardless of the state of the SensorApp.

The AIP SSM Is Rebooted or Not Responding

The following occurs according to how the adaptive security appliance is configured for failover:

- If the adaptive security appliance is configured for failover, then the adaptive security appliance fails over.
- If the adaptive security appliance is not configured for failover or failover is not possible:
 - If set to fail-open, the adaptive security appliance passes traffic without sending it to the AIP SSM.
 - If set to fail-close, the adaptive security appliance stops passing traffic until the AIP SSM is restarted.

For More Information

- For more information on IPS software bypass mode, see [Configuring Bypass Mode, page 5-27](#).
- For more information on the adaptive security appliance and the AIP SSM, refer to [Configuring the AIP SSM](#).

Configuring Traffic Flow Notifications

This section describes how to configure traffic flow notifications, and contains the following topics:

- [Traffic Flow Notifications Pane, page 5-29](#)
- [Traffic Flow Notifications Pane Field Definitions, page 5-29](#)
- [Configuring Traffic Flow Notifications, page 5-29](#)

Traffic Flow Notifications Pane

**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.

Traffic Flow Notifications Pane Field Definitions

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

- **Missed Packets Threshold**—The percentage of packets that must be missed during a specified time before a notification is sent.
- **Notification Interval**—The interval the sensor checks for the missed packets percentage.
- **Interface Idle Threshold**—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 IDM using an account with administrator privileges.
 - Step 2** Choose **Configuration > Interfaces > Traffic Flow Notifications**.
 - Step 3** In the Missed Packets Threshold field, determine 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, determine 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, determine 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

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

- [CDP Mode Pane, page 5-30](#)
- [CDP Mode Pane Field Definitions, page 5-30](#)
- [Configuring CDP Mode, page 5-31](#)

CDP Mode Pane

**Note**

You must be administrator to configure 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.

CDP Mode Pane Field Definitions

The following fields are found in the CDP Mode pane:

- Drop CDP Packets—The sensor does not forward CDP packets.
- Forward CDP Packets—The sensor forwards CDP packets.

Configuring CDP Mode

To configure CDP mode, follow these steps:

-
- Step 1** Log in to the IDM using an account with administrator privileges.
 - Step 2** Choose **Configuration > 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.
-

