



# CHAPTER 5

## Configuring Interfaces

---

This chapter describes how to configure interfaces on the sensor. You configured the interfaces when you initialized the sensor with the **setup** command, but if you need to change or add anything to your interface configuration, use the following procedures. For more information on configuring interfaces using the **setup** command, see [Initializing the Sensor, page 3-3](#).

This chapter contains the following sections:

- [Understanding Interfaces, page 5-1](#)
- [Configuring Physical Interfaces, page 5-13](#)
- [Configuring Promiscuous Mode, page 5-16](#)
- [Configuring Inline Interface Mode, page 5-17](#)
- [Configuring Inline VLAN Pair Mode, page 5-21](#)
- [Configuring VLAN Group Mode, page 5-26](#)
- [Configuring Bypass Mode, page 5-34](#)
- [Configuring Interface Notifications, page 5-36](#)
- [Displaying Interface Statistics, page 5-37](#)

## Understanding Interfaces

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

- [IPS Sensor Interfaces, page 5-2](#)
- [Command and Control Interface, page 5-2](#)
- [Sensing Interfaces, page 5-3](#)
- [TCP Reset Interfaces, page 5-4](#)
- [Interface Support, page 5-6](#)
- [Hardware Bypass Mode, page 5-9](#)
- [Interface Configuration Restrictions, page 5-10](#)
- [Interface Configuration Sequence, page 5-12](#)

## 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 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. 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 AIM-IPS, AIP-SSM, and NM-CIDS only have one sensing interface, you cannot configure a TCP reset interface.
- Because of hardware limitations on the Catalyst switch, both of the IDSM-2 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.



**For More Information**

- For the number and type of sensing interfaces available for each sensor, see [Interface Support](#), page 5-6.
- For more information on modes, see [Understanding Promiscuous Mode](#), page 5-16, [Understanding Inline Interface Mode](#), page 5-17, [Understanding Inline VLAN Pair Mode](#), page 5-21, and [Understanding VLAN Group Mode](#), page 5-27.
- For more information creating and configuring virtual sensors, see [Chapter 6, “Configuring Virtual Sensors.”](#)

## 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 5-4
- [Designating the Alternate TCP Reset Interface](#), page 5-5

### 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 IDSM-2, any sensing interface can serve as the alternate TCP reset interface for another sensing interface. The alternate TCP reset interface on IDSM-2 is fixed because of hardware limitation.

[Table 5-2](#) lists the alternate TCP reset interfaces.

**Table 5-2** *Alternate TCP Reset Interfaces*

Sensor	Alternate TCP Reset Interface
AIM-IPS	None <sup>1</sup>
AIP-SSM-10	None <sup>2</sup>
AIP-SSM-20	None <sup>3</sup>
AIP-SSM-40	None <sup>4</sup>
IDS-4215	Any sensing interface
IDS-4235	Any sensing interface
IDS-4250	Any sensing interface
IDSM-2	System0/1 <sup>5</sup>
IPS-4240	Any sensing interface

**Table 5-2** *Alternate TCP Reset Interfaces*

Sensor	Alternate TCP Reset Interface
IPS-4255	Any sensing interface
IPS-4260	Any sensing interface
IPS 4270-20	Any sensing interface
NM-CIDS	None <sup>6</sup>

1. There is only one sensing interface on AIM-IPS.
2. There is only one sensing interface on AIP-SSM-10.
3. There is only one sensing interface on AIP-SSM-20.
4. There is only one sensing interface on AIP-SSM-40.
5. This is an internal interface on the Catalyst backplane.w
6. There is only one sensing interface on NM-CIDS.

**For More Information**

For more information on alternate TCP interfaces, see [Designating the Alternate TCP Reset Interface](#), page 5-5.

**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 Support

Table 5-3 describes the interface support for appliances and modules running IPS 6.0.

**Table 5-3** 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 <b>ids-service-module</b> command in the router configuration instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by <b>ids-service-module</b> 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
IDS-4215	—	FastEthernet0/1	N/A	FastEthernet0/0
IDS-4215	4FE	FastEthernet0/1 FastEthernetS/0 <sup>1</sup> FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3 0/1<->1/0 0/1<->1/1 0/1<->1/2 0/1<->1/3	FastEthernet0/0
IDS-4235	—	GigabitEthernet0/0	N/A	GigabitEthernet0/1
IDS-4235	4FE	GigabitEthernet0/0 FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/1
IDS-4235	TX (GE)	GigabitEthernet0/0 GigabitEthernet1/0 GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	—	GigabitEthernet0/0	N/A	GigabitEthernet0/1

Table 5-3 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)
IDS-4250	4FE	GigabitEthernet0/0 FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/1
IDS-4250	TX (GE)	GigabitEthernet0/0 GigabitEthernet1/0 GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	SX	GigabitEthernet0/0 GigabitEthernet1/0	N/A	GigabitEthernet0/1
IDS-4250	SX + SX	GigabitEthernet0/0 GigabitEthernet1/0 GigabitEthernet2/0	1/0<->2/0	GigabitEthernet0/1
IDS-4250	XL	GigabitEthernet0/0 GigabitEthernet2/0 GigabitEthernet2/1	2/0<->2/1	GigabitEthernet0/1
IDS-2	—	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
IPS-4260	4GE-BP	GigabitEthernet0/1		Management0/0
	Slot 1	GigabitEthernet2/0 GigabitEthernet2/1 GigabitEthernet2/2 GigabitEthernet2/3	2/0<->2/1 <sup>2</sup> 2/2<->2/3	
	Slot 2	GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet3/2 GigabitEthernet3/3	3/0<->3/1 3/2<->3/3	

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

1. You can install the 4FE card in either slot 1 or 2. S indicates the slot number, which can be either 1 or 2.
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 (3/0<->3/2 and 3/1<->3/3, for example).
5. Reserved for future use.
6. Reserved for future use.

**Note**

IPS-4260 supports a mixture of 4GE-BP and 2SX interface cards. IPS 4270-20 also supports a mixture of 4GE-BP and 2SX interface cards, up to a total of either six cards or sixteen total ports, whichever is reached first.

## Hardware Bypass Mode

In addition to IPS 6.0 software bypass, IPS-4260 and IPS 4270-20 also support hardware bypass. This section describes the hardware bypass card and its configuration restrictions. It contains the following topics:

- [Hardware Bypass Card, page 5-9](#)
- [Hardware Bypass Configuration Restrictions, page 5-10](#)

### Hardware Bypass Card

IPS-4260 and 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 IPS 6.0. 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 more information on software bypass mode, see [Configuring Bypass Mode, page 5-34](#).
- For the procedure for installing and removing the hardware bypass card, for IPS-4260 refer to [Installing and Removing Interface Cards](#), and for IPS 4270-20 refer to [Installing and Removing Interface Cards](#).

## 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 IPS-4260 and 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 IPS-4260 and 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.

## Interface Configuration Restrictions

The following restrictions apply to configuring interfaces on the sensor:

- Physical Interfaces
  - On modules (AIM-IPS, AIP-SSM, IDSM-2, NM-CIDS) and IPS-4240, IPS-4255, IPS-4260, and IPS 4270-20, 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 fiber interfaces (1000-SX and XL on IDS-4250), valid speed settings are 1000 Mbps and auto.
  - For Gigabit copper interfaces (1000-TX on IDS-4235, IDS-4250, 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 IDSM-2. 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 and IDM prompt you to remove any dangling references. You can leave the dangling references and continue editing the configuration.
- CLI and IDM 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. IDM does *not* allow changes in the interface configuration that cause conflicts in the Analysis Engine configuration.

#### For More Information

- For a list of supported sensor interfaces, see [Interface Support, page 5-6](#).
- For more information on TCP reset, see [TCP Reset Interfaces, page 5-4](#).
- For more information on physical interfaces, see [Configuring Physical Interfaces, page 5-13](#).

## Interface Configuration Sequence

Follow these steps to configure interfaces on the sensor:

1. Configure the physical interface settings (speed, duplex, and so forth) and enable the interfaces.
2. Create or delete inline interfaces, inline VLAN subinterfaces, and VLAN groups, and set the inline bypass mode.
3. Assign the physical, subinterfaces, and inline interfaces to the virtual sensor.

#### For More Information

- For the procedure for configuring the physical interface settings, see [Configuring Physical Interfaces, page 5-13](#).
- For the procedures for configuring interfaces, see [Creating Inline Interface Pairs, page 5-17](#), [Creating Inline VLAN Pairs, page 5-22](#), [Creating VLAN Groups, page 5-28](#), and [Configuring Bypass Mode, page 5-34](#).
- For the procedure for adding interfaces to the virtual sensor, see [Editing and Deleting Virtual Sensors, page 6-6](#).

# Configuring Physical Interfaces


**Note**

For information on what you need to configure if you are using the hardware bypass card on IPS-4260 and IPS 4270-20, see [Hardware Bypass Configuration Restrictions, page 5-10](#).

Use the **physical-interfaces** *interface\_name* command in the service interface submode to configure promiscuous interfaces. The interface name is FastEthernet or GigabitEthernet.


**Note**

AIP-SSM is configured for promiscuous mode from the ASA CLI and not from the IPS CLI.

The following options apply:

- **admin-state {enabled | disabled}**—The administrative link state of the interface, whether the interface is enabled or disabled.


**Note**

On all backplane sensing interfaces on all modules (IDSM-2, NM-CIDS, and AIP-SSM), **admin-state** is set to enabled and is protected (you cannot change the setting). The **admin-state** has no effect (and is protected) on the command and control interface. It only affects sensing interfaces. The command and control interface does not need to be enabled because it cannot be monitored.

- **alt-tcp-reset-interface**—Sends TCP resets out an alternate interface when this interface is used for promiscuous monitoring and the reset action is triggered by a signature firing.


**Note**

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.


**Note**

This option is protected on modules (IDSM-2, NM-CIDS, and AIP-SSM) and appliances that only have one sensing interface (IDS-4215, IDS-4235, and IDS-4250 without any additional NIC cards).

- *interface\_name*—The name of the interface on which TCP resets should be sent when this interface is used for promiscuous monitoring and the reset action is triggered by a signature firing. This setting is ignored when this interface is a member of an inline interface.
- **none** —Disables the use of an alternate TCP reset interface. TCP resets triggered by the reset action when in promiscuous mode will be sent out of this interface instead.
- **default**—Sets the value back to the system default setting.
- **description**—Your description of the promiscuous interface.
- **duplex**—The duplex setting of the interface.
  - **auto**—Sets the interface to auto negotiate duplex.
  - **full**—Sets the interface to full duplex.
  - **half**—Sets the interface to half duplex.




---

**Note** The **duplex** option is protected on all modules.

---

- **no**—Remove an entry or selection setting.
- **speed**—The speed setting of the interface.
  - **auto**—Sets the interface to auto negotiate speed.
  - **10**—Sets the interface to 10 MB (for TX interfaces only).
  - **100**—Sets the interface to 100 MB (for TX interfaces only).
  - **1000**—Sets the interface to 1 GB (for Gigabit interfaces only).




---

**Note** The **speed** option is protected on all modules.

---

To configure the promiscuous interface settings on the sensor, follow these steps:

---

**Step 1** Log in to the CLI using an account with Administrator privileges.

**Step 2** Enter interface submode:

```
sensor# configure terminal
sensor(config)# service interface
```

**Step 3** Display the list of available interfaces:

```
sensor(config-int)# physical-interfaces ?
GigabitEthernet0/0    GigabitEthernet0/0 physical interface.
GigabitEthernet0/1    GigabitEthernet0/1 physical interface.
GigabitEthernet0/2    GigabitEthernet0/2 physical interface.
GigabitEthernet0/3    GigabitEthernet0/3 physical interface.
Management0/0        Management0/0 physical interface.
sensor(config-int)# physical-interfaces
```

**Step 4** Specify the interface for promiscuous mode:

```
sensor(config-int)# physical-interfaces GigabitEthernet0/2
```

**Step 5** Enable the interface:

```
sensor(config-int-phy)# admin-state enabled
```

You must assign the interface to a virtual sensor and enable it before it can monitor traffic.

**Step 6** Add a description of this interface:

```
sensor(config-int-phy)# description INT1
```

**Step 7** Specify the duplex settings:

```
sensor(config-int-phy)# duplex full
```

This option is not available on modules.

**Step 8** Specify the speed:

```
sensor(config-int-phy)# speed 1000
```

This option is not available on modules.

**Step 9** Enable TCP resets for this interface if desired:

```
sensor(config-int-phy) # alt-tcp-reset-interface interface-name GigabitEthernet2/0
```

**Step 10** Repeat Steps 4 through 9 for any other interfaces you want to designate as promiscuous interfaces.

**Step 11** Verify the settings:



**Note** Make sure the `subinterface-type` is `none`, the default. You use the `subinterface-type` command to configure inline VLAN pairs.

```
sensor(config-int-phy) # show settings
<protected entry>
name: GigabitEthernet0/2
-----
media-type: tx <protected>
description: INT1 default:
admin-state: enabled default: disabled
duplex: full default: auto
speed: 1000 default: auto
alt-tcp-reset-interface
-----
interface-name: GigabitEthernet2/0
-----
subinterface-type
-----
none
-----
-----
sensor(config-int-phy) #
```

**Step 12** To remove TCP resets from an interface:

```
sensor(config-int-phy) # alt-tcp-reset-interface none
```

**Step 13** Verify the settings:

```
sensor(config-int-phy) # show settings
<protected entry>
name: GigabitEthernet0/0
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <protected>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
-----
sensor(config-int-phy) #
```

**Step 14** Exit interface submode:

```
sensor(config-int-phy)# exit
sensor(config-int)# exit
Apply Changes:?[yes]:
```

**Step 15** Press **Enter** to apply the changes or enter **no** to discard them.

---

#### For More Information

- For a list of possible interfaces for your sensor, see [Interface Support, page 5-6](#).
- For the procedure for configuring traffic on AIP-SSM, see [Sending Traffic to AIP-SSM, page 18-9](#).
- For more information on the alternate TCP reset interface, see [TCP Reset Interfaces, page 5-4](#), and [Designating the Alternate TCP Reset Interface, page 5-5](#).
- For the procedure for creating and configuring a virtual sensor, see [Adding Virtual Sensors, page 6-4](#).
- For the procedure for configuring inline VLAN pairs, see [Creating Inline VLAN Pairs, page 5-22](#).

## Configuring Promiscuous Mode

This section describes promiscuous mode on the sensor, and contains the following topics:

- [Understanding Promiscuous Mode, page 5-16](#)
- [Configuring Promiscuous Mode, page 5-16](#)

## Understanding 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).

## Configuring Promiscuous Mode

By default, all sensing interfaces are in promiscuous mode. To change an interface from inline mode to promiscuous mode, delete the inline interface that contains that interface from the interface configuration.

# Configuring Inline Interface Mode

This section describes inline mode on the sensor, and contains the following topics:

- [Understanding Inline Interface Mode, page 5-17](#)
- [Creating Inline Interface Pairs, page 5-17](#)

## Understanding 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 AIM-IPS and AIP-SSM to operate inline even though these modules 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.

## Creating Inline Interface Pairs

**Note**

For information on what you need to configure if you are using the hardware bypass card on IPS-4260 and IPS 4270-20, see [Hardware Bypass Configuration Restrictions, page 5-10](#).

Use the **inline-interfaces** *name* command in the service interface submode to create inline interface pairs.

**Note**

AIP-SSM is configured for Inline Interface mode from the ASA CLI and not from the IPS CLI.

The following options apply:

- **inline-interfaces** *name*—Name of the logical inline interface pair.
- **default**—Sets the value back to the system default setting.
- **description**—Your description of the inline interface pair.
- **interface1** *interface\_name*—The first interface in the inline interface pair.

- **interface2** *interface\_name*—The second interface in the inline interface pair.
- **no**—Removes an entry or selection setting.
- **admin-state {enabled | disabled}**—The administrative link state of the interface, whether the interface is enabled or disabled.



**Note** On all backplane sensing interfaces on all modules (IDSM-2 NM-CIDS, and AIP-SSM), **admin-state** is set to enabled and is protected (you cannot change the setting). The **admin-state** has no effect (and is protected) on the command and control interface. It only affects sensing interfaces. The command and control interface does not need to be enabled because it cannot be monitored.

To create inline interface pairs, follow these steps:

**Step 1** Log in to the CLI using an account with Administrator privileges.

**Step 2** Enter interface submode:

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)#
```

**Step 3** Verify that the subinterface mode is “none” for both of the physical interfaces you are pairing in the inline interface:

```
sensor(config-int)# show settings
  physical-interfaces (min: 0, max: 999999999, current: 2)
  -----
  <protected entry>
  name: GigabitEthernet0/0 <defaulted>
  -----
  media-type: tx <protected>
  description: <defaulted>
  admin-state: disabled <protected>
  duplex: auto <defaulted>
  speed: auto <defaulted>
  alt-tcp-reset-interface
  -----
  none
  -----
  -----
  subinterface-type
  -----
  none
  -----
  -----
  -----
```

**Step 4** Name the inline pair:

```
sensor(config-int)# inline-interfaces PAIR1
```

**Step 5** Display the available interfaces:

```
sensor(config-int)# interface1 ?
GigabitEthernet0/0    GigabitEthernet0/0 physical interface.
GigabitEthernet0/1    GigabitEthernet0/1 physical interface.
GigabitEthernet0/2    GigabitEthernet0/2 physical interface.
```

```
GigabitEthernet0/3      GigabitEthernet0/3 physical interface.
Management0/0          Management0/0 physical interface.
```

**Step 6** Configure two interfaces into a pair:

```
sensor(config-int-inl)# interface1 GigabitEthernet0/0
sensor(config-int-inl)# interface2 GigabitEthernet0/1
```

You must assign the interface to a virtual sensor and enable it before it can monitor traffic (see Step 10).

**Step 7** Add a description of the interface pair:

```
sensor(config-int-inl)# description PAIR1 Gig0/0 and Gig0/1
```

**Step 8** Repeat Steps 4 through 7 for any other interfaces that you want to configure into inline interface pairs.

**Step 9** Verify the settings:

```
sensor(config-int-inl)# show settings
name: PAIR1
-----
description: PAIR1 Gig0/0 & Gig0/1 default:
interface1: GigabitEthernet0/0
interface2: GigabitEthernet0/1
-----
```

**Step 10** Enable the interfaces assigned to the interface pair:

```
sensor(config-int)# exit
sensor(config-int)# physical-interfaces GigabitEthernet0/0
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# exit
sensor(config-int)# physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# exit
sensor(config-int)#
```

**Step 11** Verify that the interfaces are enabled:

```
sensor(config-int)# show settings
physical-interfaces (min: 0, max: 999999999, current: 5)
-----
<protected entry>
name: GigabitEthernet0/0
-----
media-type: tx <protected>
description: <defaulted>
admin-state: enabled default: disabled
duplex: auto <defaulted>
speed: auto <defaulted>
default-vlan: 0 <defaulted>
alt-tcp-reset-interface
-----
none
-----
subinterface-type
-----
none
-----
-----
<protected entry>
name: GigabitEthernet0/1
```

```

-----
media-type: tx <protected>
description: <defaulted>
admin-state: enabled default: disabled
duplex: auto <defaulted>
speed: auto <defaulted>
default-vlan: 0 <defaulted>
alt-tcp-reset-interface
-----
    none
-----
-----
subinterface-type
-----
    none
-----
-----
<protected entry>
name: GigabitEthernet0/2 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
default-vlan: 0 <defaulted>
alt-tcp-reset-interface
-----
    none
-----
-----
subinterface-type
-----
    none
-----
-----
<protected entry>
name: GigabitEthernet0/3 <defaulted>
-----
media-type: tx <protected>
--MORE--

```

**Step 12** To delete an inline interface pair and return the interfaces to promiscuous mode:

```
sensor(config-int)# no inline-interfaces PAIR1
```

You must also delete the inline interface pair from the virtual sensor to which it is assigned.

**Step 13** Verify the inline interface pair has been deleted:

```

sensor(config-int)# show settings
-----
command-control: Management0/0 <protected>
inline-interfaces (min: 0, max: 999999999, current: 0)
-----
bypass-mode: auto <defaulted>
interface-notifications
-----

```

**Step 14** Exit interface configuration submode:

```
sensor(config-int)# exit  
Apply Changes:[yes]:
```

**Step 15** Press **Enter** to apply the changes or enter **no** to discard them.

---

#### For More Information

- For a list of possible interfaces for your sensor, see [Interface Support, page 5-6](#).
- For the procedure for configuring traffic on AIP-SSM, see [Sending Traffic to AIP-SSM, page 18-9](#).
- For the procedure for editing and deleting virtual sensors, see [Editing and Deleting Virtual Sensors](#).

## Configuring Inline VLAN Pair Mode

This section describes inline VLAN pair mode and how to configure inline VLAN pairs. It contains the following topics:

- [Understanding Inline VLAN Pair Mode, page 5-21](#)
- [Creating Inline VLAN Pairs, page 5-22](#)

## Understanding Inline VLAN Pair Mode



#### Note

For IPS-4260 and IPS 4270-20, fail-open hardware bypass is not supported on inline VLAN pairs. For more information, see [Hardware Bypass Configuration Restrictions, page 5-10](#).

---

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.



#### Note

AIM-IPS, AIP-SSM, and NME-IPS do not support inline VLAN pairs.

---

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.

---

## Creating Inline VLAN Pairs



### 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.

Use the **physical-interfaces** *interface\_name* command in the service interface submode to configure inline VLAN pairs. The interface name is FastEthernet or GigabitEthernet.

The following options apply:

- **admin-state {enabled | disabled}**—The administrative link state of the interface, whether the interface is enabled or disabled.



### Note

On all backplane sensing interfaces on all modules (IDS-M-2, NM-CIDS, and AIP-SSM), **admin-state** is set to enabled and is protected (you cannot change the setting). The **admin-state** has no effect (and is protected) on the command and control interface. It only affects sensing interfaces. The command and control interface does not need to be enabled because it cannot be monitored.

- **default**—Sets the value back to the system default setting.
- **description**—Your description of the interface.
- **duplex**—The duplex setting of the interface.
  - **auto**—Sets the interface to auto negotiate duplex.
  - **full**—Sets the interface to full duplex.
  - **half**—Sets the interface to half duplex.



### Note

The **duplex** option is protected on all modules.

- **no**—Removes an entry or selection setting.
- **speed**—The speed setting of the interface.
  - **auto**—Sets the interface to auto negotiate speed.
  - **10**—Sets the interface to 10 MB (for TX interfaces only).
  - **100**—Sets the interface to 100 MB (for TX interfaces only).
  - **1000**—Sets the interface to 1 GB (for Gigabit interfaces only).



### Note

The **speed** option is protected on all modules.

- **subinterface-type**—Specifies that the interface is a subinterface and what type of subinterface is defined.
  - **inline-vlan-pair**—Lets you define the subinterface as an inline VLAN pair.
  - **none**—No subinterfaces defined.

- **subinterface** *name*—Defines the subinterface as an inline VLAN pair.
  - **vlan1**—The first VLAN in the inline VLAN pair.
  - **vlan2**—The second VLAN in the inline VLAN pair.

To configure the inline VLAN pair settings on the sensor, follow these steps:

---

**Step 1** Log in to the CLI using an account with Administrator privileges.

**Step 2** Enter interface submode:

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)#
```

**Step 3** Verify if any inline interfaces exist (the subinterface type should read “none” if no inline interfaces have been configured):

```
sensor(config-int)# show settings
physical-interfaces (min: 0, max: 999999999, current: 5)
-----
<protected entry>
name: GigabitEthernet0/0 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
subinterface-type
-----
none
-----
-----
<protected entry>
name: GigabitEthernet0/1 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
subinterface-type
-----
none
-----
-----
```

```

<protected entry>
name: GigabitEthernet0/2 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
subinterface-type
-----
none
-----
-----
<protected entry>
name: GigabitEthernet0/3 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
subinterface-type
-----
none
-----
-----
<protected entry>
name: Management0/0 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <protected>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
subinterface-type
-----
none
-----
-----

```

```

command-control: Management0/0 <protected>
inline-interfaces (min: 0, max: 999999999, current: 0)
-----
-----
bypass-mode: auto <defaulted>
interface-notifications
-----
missed-percentage-threshold: 0 percent <defaulted>
notification-interval: 30 seconds <defaulted>
idle-interface-delay: 30 seconds <defaulted>
-----
sensor(config-int)#

```

- Step 4** If there are inline interfaces that are using this physical interface, remove them:

```
sensor(config-int)# no inline-interfaces interface_name
```

You must also delete the inline interface from the virtual sensor to which it is assigned.

- Step 5** Display the list of available interfaces:

```

sensor(config-int)# physical-interfaces ?
GigabitEthernet0/0    GigabitEthernet0/0 physical interface.
GigabitEthernet0/1    GigabitEthernet0/1 physical interface.
GigabitEthernet0/2    GigabitEthernet0/2 physical interface.
GigabitEthernet0/3    GigabitEthernet0/3 physical interface.
Management0/0        Management0/0 physical interface.
sensor(config-int)# physical-interfaces

```

- Step 6** Designate an interface:

```
sensor(config-int)# physical-interfaces GigabitEthernet0/2
```

- Step 7** Enable the interface:

```
sensor(config-int-phy)# admin-state enabled
```

You must assign the interface to a virtual sensor and enable it before it can monitor traffic.

- Step 8** Add a description of this interface:

```
sensor(config-int-phy)# description INT1
```

- Step 9** Configure the duplex settings:

```
sensor(config-int-phy)# duplex full
```

This option is not available on modules.

- Step 10** Configure the speed:

```
sensor(config-int-phy)# speed 1000
```

This option is not available on modules.

- Step 11** Set up the inline VLAN pair:

```

sensor(config-int-phy)# subinterface-type inline-vlan-pair
sensor(config-int-phy-inl)# subinterface 1
sensor(config-int-phy-inl-sub)# vlan1 52
sensor(config-int-phy-inl-sub)# vlan2 53

```

- Step 12** Add a description for the inline VLAN pair:

```
sensor(config-int-phy-inl-sub)# description INT1 vlans 52 and 53
```

**Step 13** Verify the inline VLAN pair settings:

```
sensor(config-int-phy-inl-sub)# show settings
subinterface-number: 1
-----
description: INT1 vlans 52 and 53 default:
vlan1: 52
vlan2: 53
-----
sensor(config-int-phy-inl-sub)#
```

**Step 14** To delete VLAN pairs:

e. To delete one VLAN pair:

```
sensor(config-int-phy-inl-sub)# exit
sensor(config-int-phy-inl)# no subinterface 1
```

If this VLAN pair is the last one on the sensor, you receive the following error message:

```
Error: This "subinterface-type" contains less than the required number of
"subinterface" entries. Please add entry(s) to reach the minimum required entries or
select a different "subinterface-type".
```

Go to Step b to remove the last VLAN pair.

f. To delete all VLAN pairs:

```
sensor(config-int-phy-inl-sub)# exit
sensor(config-int-phy-inl)# exit
sensor(config-int-phy)# subinterface-type none
```

You must also delete the interface from the virtual sensor to which it is assigned.

**Step 15** Exit interface submode:

```
sensor(config-int-phy-inl-sub)# exit
sensor(config-int-phy-inl)# exit
sensor(config-int-phy)# exit
sensor(config-int)# exit
Apply Changes:[yes]:
```

**Step 16** Press **Enter** to apply the changes or enter **no** to discard them.

---

#### For More Information

- For the procedure for editing and deleting virtual sensors, see [Editing and Deleting Virtual Sensors, page 6-6](#).
- For the procedure for assigning interfaces to virtual sensors, see [Adding Virtual Sensors, page 6-4](#).

## Configuring VLAN Group Mode

This section describes VLAN group mode and how to configure VLAN groups. It contains the following topics:

- [Understanding VLAN Group Mode, page 5-27](#)
- [Deploying VLAN Groups, page 5-27](#)
- [Creating VLAN Groups, page 5-28](#)

## Understanding 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 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. IDSM-2 can read the 802.1q headers for all nonnative traffic to determine the VLAN ID for that packet. However, IDSM-2 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 IDSM-2 which VLAN is the native VLAN for that port. Then IDSM-2 treats any untagged packets as if they were tagged with the native VLAN ID.

## 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.

IDS-2 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 IDS-2 because it cannot be connected in this way.

#### For More Information

For more information on configuring IDS-2 in VLAN groups, see [Chapter 19, “Configuring IDS-2.”](#)

## Creating VLAN Groups



#### Note

For information on what you need to configure if you are using the hardware bypass card on IPS-4260 and IPS 4270-20, see [Hardware Bypass Configuration Restrictions, page 5-10.](#)

Use the **physical-interfaces** *interface\_name* command in the service interface submode to configure inline VLAN groups. The interface name is FastEthernet or GigabitEthernet.

The following options apply:

- **admin-state {enabled | disabled}**—The administrative link state of the interface, whether the interface is enabled or disabled.



#### Note

On all backplane sensing interfaces on all modules (IDS-2, NM-CIDS, and AIP-SSM), **admin-state** is set to enabled and is protected (you cannot change the setting). The **admin-state** has no effect (and is protected) on the command and control interface. It only affects sensing interfaces. The command and control interface does not need to be enabled because it cannot be monitored.

- **default**—Sets the value back to the system default setting.
- **description**—Your description of the interface.
- **duplex**—The duplex setting of the interface.
  - **auto**—Sets the interface to auto negotiate duplex.
  - **full**—Sets the interface to full duplex.
  - **half**—Sets the interface to half duplex.



**Note** The **duplex** option is protected on all modules.

- **no**—Removes an entry or selection setting.

- **speed**—The speed setting of the interface.
  - **auto**—Sets the interface to auto negotiate speed.
  - **10**—Sets the interface to 10 MB (for TX interfaces only).
  - **100**—Sets the interface to 100 MB (for TX interfaces only).
  - **1000**—Sets the interface to 1 GB (for Gigabit interfaces only).




---

**Note** The **speed** option is protected on all modules.

---

- **subinterface-type**—Specifies that the interface is a subinterface and what type of subinterface is defined.
  - **vlan-group**—Lets you define the subinterface as a VLAN group.
  - **none**—No subinterfaces defined.
- **subinterface name**—Defines the subinterface as a VLAN group.
  - **vlan {range | unassigned}**—The set of VLANs in the VLAN group




---

**Note** The value for **range** is 1 to 4095 in a comma-separated pattern of individual VLAN IDs or ranges: 1,5-8,10-15. There are no spaces between the entries.

---

To configure the inline VLAN group settings on the sensor, follow these steps:

---

**Step 1** Log in to the CLI using an account with Administrator privileges.

**Step 2** Enter interface submode:

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)#
```

**Step 3** Verify if any inline interfaces exist (the subinterface type should read “none” if no inline interfaces have been configured):

```
sensor(config-int)# show settings
physical-interfaces (min: 0, max: 999999999, current: 5)
-----
<protected entry>
name: GigabitEthernet0/0 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
-----
subinterface-type
-----
none
-----
-----
```

```

-----
-----
<protected entry>
name: GigabitEthernet0/1 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
-----
subinterface-type
-----
none
-----
-----
-----
<protected entry>
name: GigabitEthernet0/2 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
-----
subinterface-type
-----
none
-----
-----
-----
<protected entry>
name: GigabitEthernet0/3 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <defaulted>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
-----
subinterface-type
-----
none
-----
-----
-----

```

```

-----
<protected entry>
name: Management0/0 <defaulted>
-----
media-type: tx <protected>
description: <defaulted>
admin-state: disabled <protected>
duplex: auto <defaulted>
speed: auto <defaulted>
alt-tcp-reset-interface
-----
none
-----
subinterface-type
-----
none
-----
-----
command-control: Management0/0 <protected>
inline-interfaces (min: 0, max: 999999999, current: 0)
-----
bypass-mode: auto <defaulted>
interface-notifications
-----
missed-percentage-threshold: 0 percent <defaulted>
notification-interval: 30 seconds <defaulted>
idle-interface-delay: 30 seconds <defaulted>
-----
sensor(config-int)#

```

**Step 4** If there are inline interfaces that are using this physical interface, remove them:

```
sensor(config-int)# no inline-interfaces interface_name
```

**Step 5** Display the list of available interfaces:

```

sensor(config-int)# physical-interfaces ?
GigabitEthernet0/0    GigabitEthernet0/0 physical interface.
GigabitEthernet0/1    GigabitEthernet0/1 physical interface.
GigabitEthernet0/2    GigabitEthernet0/2 physical interface.
GigabitEthernet0/3    GigabitEthernet0/3 physical interface.
Management0/0        Management0/0 physical interface.
sensor(config-int)# physical-interfaces

```

**Step 6** Specify an interface:

```
sensor(config-int)# physical-interfaces GigabitEthernet0/2
```

**Step 7** Enable the interface:

```
sensor(config-int-phy)# admin-state enabled
```

You must also assign the interface to a virtual sensor and enable it before it can monitor traffic.

**Step 8** Add a description of this interface:

```
sensor(config-int-phy)# description INT1
```

**Step 9** Specify the duplex settings:

```
sensor(config-int-phy) # duplex full
```

This option is not available on modules.

**Step 10** Specify the speed:

```
sensor(config-int-phy) # speed 1000
```

This option is not available on modules.

**Step 11** Set up the VLAN group:

```
sensor(config-int-phy) # subinterface-type vlan-group
sensor(config-int-phy-vla) # subinterface 1
```

**Step 12** Assign the VLANs to this group:

a. For specific VLANs:

```
sensor(config-int-phy-vla-sub) # vlans range 1,5-8,10-15
sensor(config-int-phy-vla-sub) #
```

b. Verify the settings:

```
sensor(config-int-phy-vla-sub) # show settings
subinterface-number: 1
-----
description: <defaulted>
vlans
-----
range: 1,5-8,10-15
-----
sensor(config-int-phy-vla-sub) #
```

c. For unassigned VLANs:

```
sensor(config-int-phy-vla-sub) # vlans unassigned
sensor(config-int-phy-vla-sub) #
```

d. Verify the settings:

```
sensor(config-int-phy-vla-sub) # show settings
subinterface-number: 1
-----
description: <defaulted>
vlans
-----
unassigned
-----
-----
sensor(config-int-phy-vla-sub) #
```



**Note**

Assigning the unassigned VLANs to a separate virtual sensor allows you to specify a policy for all VLANs that you have not specifically assigned to other groups. For example, you can group your important internal VLANs in one group and apply a stringent security policy to that group. You can group the other less important unassigned VLANs into another group, and apply the default security policy to that group, so that only very serious alerts are reported.

**Step 13** Add a description for the VLAN group:

```
sensor(config-int-phy-inl-sub)# description INT1 vlans 52 and 53
```

**Step 14** Verify the VLAN group settings:

```
sensor(config-int-phy-vla-sub)# show settings
subinterface-number: 1
-----
description: GROUP1 default:
vlans
-----
unassigned
-----
-----
-----
-----
sensor(config-int-phy-vla-sub)#
```

**Step 15** To delete VLAN groups:

a. To delete one VLAN group:

```
sensor(config-int-phy-vla-sub)# exit
sensor(config-int-phy-vla)# no subinterface 1
```

If this VLAN group is the last one on the sensor, you receive the following error message:

```
Error: This "subinterface-type" contains less than the required number of
"subinterface" entries. Please add entry(s) to reach the minimum required entries or
select a different "subinterface-type".
```

Go to Step b to remove the last VLAN group.

b. To delete all VLAN groups:

```
sensor(config-int-phy-vla-sub)# exit
sensor(config-int-phy-vla)# exit
sensor(config-int-phy)# subinterface-type none
```

You must also delete the VLAN group from the virtual sensor to which it is assigned.

**Step 16** Exit interface submode:

```
sensor(config-int-phy-vla-sub)# exit
sensor(config-int-phy-vla)# exit
sensor(config-int-phy)# exit
sensor(config-int)# exit
Apply Changes:[yes]:
```

**Step 17** Press **Enter** to apply the changes or enter **no** to discard them.

### For More Information

- For the procedure for editing and deleting virtual sensors, see [Editing and Deleting Virtual Sensors, page 6-6](#).
- For the procedure for assigning interfaces to virtual sensors, see [Adding Virtual Sensors, page 6-4](#).

# Configuring Bypass Mode

This section describes bypass mode for sensors configured as inline interface and inline VLAN pairs, and contains the following topics:

- [Understanding Bypass Mode, page 5-34](#)
- [Configuring Bypass Mode, page 5-34](#)
- [Adaptive Security Appliance, AIP-SSM, and Bypass Mode, page 5-35](#)

## Understanding Bypass Mode



### Note

For more information on using hardware bypass mode with software bypass mode, see [Hardware Bypass Mode, page 5-9](#).

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.

## Configuring Bypass Mode

Use the **bypass-mode** command in the service interface submode to configure bypass mode.

The following options apply:

- **off**—Turns off inline bypassing. Packet inspection is performed on inline data traffic. However, inline traffic is interrupted if Analysis Engine is stopped.
- **on**—Turns on inline bypassing. No packet inspection is performed on the traffic. Inline traffic continues to flow even if Analysis Engine is stopped.
- **auto**—Automatically begins bypassing inline packet inspection if Analysis Engine stops processing packets. This prevents data interruption on inline interfaces. This is the default.

To configure bypass mode, follow these steps:

**Step 1** Log in to the CLI using an account with Administrator privileges.

**Step 2** Enter interface submode:

```
sensor# configure terminal
sensor(config)# service interface
```

**Step 3** Configure bypass mode:

```
sensor(config-int)# bypass-mode off
```

**Step 4** Verify the settings:

```
sensor(config-int)# show settings
-----
bypass-mode: off default: auto
interface-notifications
-----
missed-percentage-threshold: 0 percent <defaulted>
notification-interval: 30 seconds <defaulted>
idle-interface-delay: 30 seconds <defaulted>
-----
sensor(config-int)#
```

**Step 5** Exit interface submode:

```
sensor(config-int)# exit
Apply Changes:[yes]:
```

**Step 6** Press **Enter** to apply the changes or enter **no** to discard them.

## Adaptive Security Appliance, AIP-SSM, and Bypass Mode

The following conditions apply to bypass mode, adaptive security appliance, and AIP-SSM:

- Bypass Auto or Off
 

The adaptive security appliance permits or blocks traffic from going through according to the configured fail-open or fail-close rules when AIP-SSM is shut down or reset.
- Bypass Auto
 

If SensorApp stops in AIP-SSM, the adaptive security appliance permits all traffic through regardless of the configured fail-open or fail-close rules, because the AIP-SSM NIC driver is still functioning and passing heartbeat packets.
- Bypass Off
 

If SensorApp stops in AIP-SSM, the adaptive security appliance stops all traffic from going through regardless of the configured fail-open or fail-close rules.

### For More Information

- For more information on IPS software bypass mode, see [Configuring Bypass Mode, page 5-34](#).
- For more information on the adaptive security appliance and AIP-SSM, see [Chapter 18, “Configuring AIP-SSM.”](#)

# Configuring Interface 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.

Use the **interface-notifications** command in the service interface submode to configure traffic notifications.

The following options apply:

- **default**—Sets the value back to the system default setting.
- **idle-interface-delay**—The number of seconds an interface must be idle before sending a notification. The valid range is 5 to 3600. The default is 30 seconds.
- **missed-percentage-threshold**—The percentage of packets that must be missed during a specified interval before notification will be sent. The valid range is 0 to 100. The default is 0.
- **notification-interval**—Interval to check for missed packet percentage. The valid range is 5 to 3600. The default is 30 seconds

To configure the interface notification settings, follow these steps:

---

**Step 1** Log in to the CLI using an account with Administrator privileges.

**Step 2** Enter global configuration mode:

```
sensor# configure terminal
```

**Step 3** Enter interface submode:

```
sensor(config)# service interface
```

**Step 4** Enter interface notifications submode:

```
sensor(config-int)# interface-notifications
```

**Step 5** Specify the idle interface delay:

```
sensor(config-int-int)# idle-interface-delay 60
```

**Step 6** Specify the missed percentage threshold:

```
sensor(config-int-int)# missed-percentage-threshold 1
```

**Step 7** Specify the notification interval:

```
sensor(config-int-int)# notification-interval 60
```

**Step 8** Verify the settings:

```
sensor(config-int-int)# show settings
interface-notifications
-----
missed-percentage-threshold: 1 percent default: 0
notification-interval: 60 seconds default: 30
idle-interface-delay: 60 seconds default: 30
-----
sensor(config-int-int)#
```

**Step 9** Exit interface notifications submode:

```
sensor(config-int-int)# exit
sensor(config-int)# exit
Apply Changes:[yes]:
```

**Step 10** Press **Enter** to apply the changes or enter **no** to discard them.

## Displaying Interface Statistics

Use the **show interfaces [clear | brief]** command in EXEC mode to display statistics for all system interfaces. Use the **show interfaces {FastEthernet | GigabitEthernet | Management} [slot/port]** command to display statistics for specific interfaces.

The following options apply:

- **clear**—(Optional) Clears the diagnostics.
- **brief**—(Optional) Displays a summary of the usability status information for each interface.
- **FastEthernet**—Displays statistics for FastEthernet interfaces.
- **GigabitEthernet**—Displays statistics for GigabitEthernet interfaces.
- **Management**—Displays statistics for Management interfaces.



**Note** Only platforms with external ports marked *Management* support this keyword.

- **slot/port**—Displays statistics for the specific slot/port of the interface.



**Note** For information on slot and port numbers and which platforms have a Management port, refer to [Installing Cisco Intrusion Prevention System Appliances and Modules 6.0](#).

To display interface statistics, follow these steps:

**Step 1** Log in to the CLI.

**Step 2** Display statistics for all interfaces:

```
sensor# show interfaces
Interface Statistics
Total Packets Received = 0
Total Bytes Received = 0
Missed Packet Percentage = 0
Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/0
Statistics From Subinterface 12
Vlans in this group = 12
Total Packets Received On This Vlan Group = 0
Total Bytes Received On This Vlan Group = 0
Total Packets Transmitted On This Vlan Group = 0
Total Bytes Transmitted On This Vlan Group = 0
Statistics From Subinterface 16
Vlans in this group = 10
Total Packets Received On This Vlan Group = 0
Total Bytes Received On This Vlan Group = 0
```

```

Total Packets Transmitted On This Vlan Group = 0
Total Bytes Transmitted On This Vlan Group = 0
Statistics From Subinterface 25
Vlans in this group = 11
Total Packets Received On This Vlan Group = 0
Total Bytes Received On This Vlan Group = 0
Total Packets Transmitted On This Vlan Group = 0
Total Bytes Transmitted On This Vlan Group = 0
--MORE--

```

**Step 3** Show a brief summary of the interfaces:

```

sensor# show interfaces brief
CC  Interface                Sensing State  Link  Inline Mode  Pair Status
*   GigabitEthernet0/0      Disabled      Down  Unpaired     N/A
    Management0/0          Disabled      Up    Unpaired     N/A
    GigabitEthernet0/1     Disabled      Down  Unpaired     N/A
    GigabitEthernet0/2     Disabled      Down  Unpaired     N/A
    GigabitEthernet0/3     Disabled      Down  Unpaired     N/A
sensor#

```

The \* indicates that the interface is the command and control interface.

**Step 4** Display the statistics for a specific interface:

```

sensor# show interfaces Management0/0
MAC statistics from interface Management0/0
Interface function = Command-control interface
Description =
Media Type = TX
Default Vlan = 0
Link Status = Up
Link Speed = Auto_100
Link Duplex = Auto_Full
Total Packets Received = 4305909
Total Bytes Received = 280475712
Total Multicast Packets Received = 0
Total Receive Errors = 0
Total Receive FIFO Overruns = 0
Total Packets Transmitted = 973627
Total Bytes Transmitted = 437632618
Total Transmit Errors = 0
Total Transmit FIFO Overruns = 0
sensor#

```

**Step 5** To clear the statistics:

```

sensor# show interfaces clear
Interface Statistics
Total Packets Received = 0
Total Bytes Received = 0
Missed Packet Percentage = 0
Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/0
Statistics From Subinterface 12
Vlans in this group = 12
Total Packets Received On This Vlan Group = 0
Total Bytes Received On This Vlan Group = 0
Total Packets Transmitted On This Vlan Group = 0
Total Bytes Transmitted On This Vlan Group = 0
Statistics From Subinterface 16
Vlans in this group = 10
Total Packets Received On This Vlan Group = 0
Total Bytes Received On This Vlan Group = 0
Total Packets Transmitted On This Vlan Group = 0

```

```
Total Bytes Transmitted On This Vlan Group = 0
Statistics From Subinterface 25
Vlans in this group = 11
Total Packets Received On This Vlan Group = 0
Total Bytes Received On This Vlan Group = 0
Total Packets Transmitted On This Vlan Group = 0
Total Bytes Transmitted On This Vlan Group = 0
--MORE--
```

---

