

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 3-1](#)
- [Understanding Promiscuous Mode, page 3-2](#)
- [Understanding Inline Interface Mode, page 3-3](#)
- [Understanding Inline VLAN Pair Mode, page 3-3](#)
- [Interface Support, page 3-4](#)
- [Interface Configuration Restrictions, page 3-5](#)
- [Understanding Hardware Bypass, page 3-7](#)
- [Summary, page 3-9](#)
- [Configuring Interfaces, page 3-10](#)
- [Configuring Inline Interface Pairs, page 3-14](#)
- [Configuring Inline VLAN Pairs, page 3-17](#)
- [Configuring Bypass Mode, page 3-20](#)
- [Configuring Traffic Flow Notifications, page 3-21](#)

Understanding Interfaces

The command and control interface is permanently mapped to a specific physical interface, which depends on the type of sensor you have. You can configure the sensing interfaces to operate in promiscuous mode, inline interface mode, or inline VLAN pair mode. For sensors that support inline interface mode, you can pair the sensing interfaces into logical interfaces called “inline pairs.” For sensors that support VLANs, you can pair the VLANs into inline VLAN pairs. You must enable the interfaces, interface pairs, or VLAN pairs before the sensor can monitor traffic.

**Note**

On appliances, the sensing interfaces are disabled by default. On modules, the sensing interfaces are always enabled and cannot be disabled.

With the addition of the inline VLAN pair feature, each sensing interface operates in one of three possible modes at any time: promiscuous, inline interface, or inline VLAN pair. On sensors with multiple sensing interfaces, any combination of modes are allowed on the same sensor:

- A sensing interface is in inline interface mode if it is paired with another sensing interface in an inline interface pair and its subinterface type is set to none (the default).
- A sensing interface is in inline VLAN pair mode if its subinterface type is set to inline VLAN pair.
- A sensing interface is in promiscuous mode by default, that is, if it is not in either of the other modes.

The sensing interface does not have an IP address assigned to it and is therefore invisible to attackers. This lets the sensor monitor the data stream without letting attackers know they are being watched. Promiscuous mode is contrasted by inline interface mode where all packets entering or leaving the network must pass through the sensor. For more information, see [Understanding Promiscuous Mode, page 3-2](#), [Understanding Inline Interface Mode, page 3-3](#), and [Understanding Inline VLAN Pair Mode, page 3-3](#).

The sensor only monitors traffic on interfaces, inline interface pairs, and inline VLAN pairs that are assigned to the default virtual sensor. For more information, see [Assigning Interfaces to the Virtual Sensor, page 4-3](#).

To configure the sensor so that traffic continues to flow through inline pairs even when SensorApp is not running, you can enable bypass mode. Bypass mode minimizes dataflow interruptions during reconfiguration, service pack installation, or software failure.

The sensor detects the interfaces of modules that have been installed while the chassis was powered off. You can configure them the next time you start the sensor. If a module is removed, the sensor detects the absence of the interfaces the next time it is started. Your interface configuration is retained, but the sensor ignores it if the interfaces are not present.

The following interface configuration events are reported as status events:

- Link up or down
- Traffic started or stopped
- Bypass mode auto activated or deactivated
- Missed packet percentage threshold exceeded

Understanding Promiscuous Mode

In promiscuous mode, packets do not flow through the IPS. 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 IPS 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, for atomic attacks, however, 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).

Understanding Inline Interface Mode

Operating in inline interface 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 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 AIP-SSM to operate inline even though it has 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.

Understanding Inline VLAN Pair Mode

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 pairs are supported on all sensors that are compatible with IPS 5.1 except NM-CIDS, AIP-SSM-10, and AIP-SSM-20.

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 any packets received on the VLAN that are not assigned to an inline VLAN pair.

Interface Support

Table 3-1 describes the interface support for appliances and modules running IPS 5.1:

Table 3-1 *Interface Support*

Base Chassis	Added PCI Cards	Interfaces Supporting Inline	Possible Port Combinations	Interfaces Not Supporting Inline
IDS-4210	—	None	N/A	All
IDS-4215	—	None	N/A	All
IDS-4215	4FE	FastEthernet0/1 4FE FastEthernetS/0 ¹ 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	—	None	N/A	All
IDS-4235	4FE	4FE 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	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4235	TX (GE)	TX onboard + TX PCI GigabitEthernet0/0 + GigabitEthernet1/0 or GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	—	None	N/A	All
IDS-4250	4FE	4FE 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	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4250	TX (GE)	TX onboard + TX PCI GigabitEthernet0/0 + GigabitEthernet1/0 or GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	SX	None	N/A	All
IDS-4250	SX + SX	2 SX GigabitEthernet1/0 GigabitEthernet2/0	1/0<->2/0	GigabitEthernet0/0 GigabitEthernet0/1

Table 3-1 *Interface Support (continued)*

Base Chassis	Added PCI Cards	Interfaces Supporting Inline	Possible Port Combinations	Interfaces Not Supporting Inline
IDS-4250	XL	2 SX of the XL GigabitEthernet2/0 GigabitEthernet2/1	2/0<->2/1	GigabitEthernet0/0 GigabitEthernet0/1
IDS-2	—	port 7 and 8 GigabitEthernet0/7 GigabitEthernet0/8	0/7<->0/8	GigabitEthernet0/2
IPS-4240	—	4 onboard GE 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	—	4 onboard GE 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	—	4 onboard GE 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
NM-CIDS	—	None	N/A	All
AIP-SSM-10	—	GigabitEthernet0/1	By security context	GigabitEthernet0/0
AIP-SSM-20	—	GigabitEthernet0/1	By security context	GigabitEthernet0/0

1. The 4FE card can be installed in either slot 1 or 2. S indicates the slot number, which can be either 1 or 2.

Interface Configuration Restrictions

The following restrictions apply to configuring interfaces on the sensor:

- Physical Interfaces
 - On modules (IDS-2, NM-CIDS, AIP-SSM-10, and AIP-SSM-20) and IPS-4240, IPS-4255, and IPS-4260 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 the IDS-4250), valid speed settings are 1000 Mbps and auto.

- For Gigabit copper interfaces (1000-TX on the IDS-4235, IDS-4250, IPS-4240, IPS-4255, and IPS-4260), 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 officially supported. For more information, see [Interface Support, page 3-4](#).
 - 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.
 - 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).

Understanding Hardware Bypass

In addition to IPS 5.1 software bypass, IPS-4260 also supports hardware bypass.

This section describes the 4GE bypass interface card and its configuration restrictions. For the procedure for installing and removing PCI cards, refer to [Installing and Removing PCI Cards](#).

This section contains the following topics:

- [4GE Bypass Interface Card](#), page 3-7
- [Hardware Bypass Configuration Restrictions](#), page 3-8

4GE Bypass Interface Card

IPS-4260 supports 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. [Figure 3-1](#) shows the 4GE bypass interface card.

Figure 3-1 4GE Bypass Interface Card



Hardware bypass complements the existing software bypass feature in IPS 5.1. For more information on software bypass mode, see [Configuring Bypass Mode](#), page 3-20. The following conditions apply to hardware bypass and software bypass on IPS-4260:

- 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.

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 GigabitEthernet1/0 is capable of performing hardware bypass only when
paired with GigabitEthernet1/1, 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.
- 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 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.

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.

Summary

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

- [Overview, page 3-9](#)
- [Supported User Role, page 3-9](#)
- [Field Definitions, page 3-9](#)

Overview

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 pair mode, or inline VLAN pair mode, but you cannot configure an interface in a combination of these modes.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

Field Definitions

The following fields and buttons are found on the Summary pane.

Field Descriptions:

- 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.
- Description—Your description of the interface.
- Assigned Virtual Sensor—Whether the interface or interface pair has been assigned to the virtual sensor, vs0.

Configuring Interfaces

**Note**

For information on what you need to configure if you are using the hardware bypass card on IPS-4260, see [Interface Configuration Restrictions, page 3-5](#).

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

- [Overview, page 3-10](#)
- [Understanding Alternate TCP Reset, page 3-10](#)
- [Supported User Role, page 3-11](#)
- [Field Definitions, page 3-11](#)
- [Configuring Interfaces, page 3-14](#)

Overview

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 on 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 the default virtual sensor, vs0, and enabled the interface or inline pair. If you need to change your interfaces settings, you can do so on the Interfaces pane. To assign the interface or inline pair to the virtual sensor, vs0, in the Edit Virtual Sensor dialog box, choose **Configuration > Analysis Engine > Virtual Sensor > Edit**.

TCP Reset Interfaces

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

- [Understanding Alternate TCP Reset, page 3-10](#)
- [Designating the Alternate TCP Reset Interface, page 3-11](#)

Understanding Alternate TCP Reset

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 allow 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.

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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to edit the interfaces on the sensor.

Field Definitions

This section lists the field definitions for interfaces, and contains the following topics:

- [Interfaces Pane, page 3-12](#)
- [Edit Interface Dialog Box, page 3-13](#)

Interfaces Pane

The following fields and buttons are found on the Interfaces pane.

Field Descriptions:

- 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 parent chassis' backplane.
- 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).
- 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.

Button Functions:

- Select All—Lets you select all entries in the list.
- Edit—Opens the Edit Interface dialog box. From this dialog box, you can change some of the values associated with this interface.
- Enable—Enables this interface.
- Disable—Disables this interface.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Edit Interface Dialog Box

The following fields and buttons are found in the Edit Interface dialog box.

Field Descriptions:

- Interface Name—Name of the interface.
The values are FastEthernet or GigabitEthernet for all interfaces.
- Description—Lets you provide a description of the interface.
- 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 parent chassis' backplane.
- Enabled—Whether or not the interface is enabled.
- 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).
- Use 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.
 - Select Interface—Sets the interface that will send the TCP reset.
For more information on the alternate TCP reset interface, see [TCP Reset Interfaces, page 3-10](#).

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Interfaces

To enable or disable the interface or edit its settings, follow these steps:

-
- Step 1** Log in to IDM using an account with administrator privileges.
- Step 2** Choose **Configuration > Interface Configuration > Interfaces**.
The Interfaces pane appears.
- Step 3** Select the row or double-click it and then click **Enable**.
The interface is enabled. To have the interface monitor traffic, it must also be assigned to a virtual sensor. For the procedure, see [Assigning Interfaces to the Virtual Sensor, page 4-3](#).
- Step 4** To edit some of the values associated with the interface, select the interface, and then click **Edit**.
The Edit Interface dialog box appears.
- Step 5** 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 **Use Alternative TCP Reset Interface** check box.
- Step 6** Click **OK**.
The changes appear in the list on the Interfaces pane.



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

- Step 7** Click **Apply** to apply your changes and save the revised configuration.
-

Configuring Inline Interface Pairs



Note For information on what you need to configure if you are using the hardware bypass card on IPS-4260, see [Interface Configuration Restrictions, page 3-5](#).

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

- [Overview, page 3-15](#)
- [Supported User Role, page 3-15](#)
- [Field Definitions, page 3-15](#)
- [Configuring Inline Interface Pairs, page 3-16](#)

Overview

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

**Note**

AIP-SSM does not need an inline pair for monitoring. You only need to add the physical interface to the virtual sensor.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure interface pairs.

Field Definitions

This sections lists field definitions for interface pairs, and contains the following topics:

- [Interface Pairs Pane, page 3-15](#)
- [Add and Edit Interface Pair Dialog Boxes, page 3-16](#)

Interface Pairs Pane

The following fields and buttons are found on the Interface Pairs pane.

Field Descriptions:

- 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.

Button Functions:

- Select All—Selects all interface pairs.
- Add—Opens the Add Interface Pair dialog box. From this dialog box, you can add an interface pair.
- Edit—Opens the Edit Interface Pair dialog box. From this dialog box, you can edit the values of the interface pair.
- Delete—Deletes the selected interface pair.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit Interface Pair Dialog Boxes

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

Field Descriptions:

- Interface Pair Name—The name you give the interface pair.
- Select two interfaces—Select two interfaces from the list to pair (for example, GigabitEthernet0/0<->GigabitEthernet0/1).
- Description—Lets you add a description of this interface pair.

Button Functions:

- OK—Accepts your changes and closes the dialog box.
- Cancel—Discards your changes and closes the dialog box.
- Help—Displays the help topic for this feature.

Configuring Inline Interface Pairs

To configure inline interface pairs, follow these steps:

-
- Step 1** Log in to IDM using an account with administrator privileges.
 - Step 2** Choose **Configuration > Interface Configuration > Interface Pairs**.
The Interface Pairs pane appears.
 - Step 3** Click **Add** to add inline interface pairs.
The Add Interface Pair dialog box appears.
 - Step 4** Enter a name in the Interface Pair Name field.
The inline interface name is a name that you create.
 - Step 5** Select two interfaces to form a pair in the Select two interfaces field.
For example, GigabitEthernet0/0 and GigabitEthernet0/1.
 - Step 6** You can add a description of the inline interface pair in the Description field if you want to.
 - Step 7** Click **OK**.
The new inline interface pair appears in the list on the Interface Pairs pane.
 - Step 8** To edit an inline interface pair, select it, and click **Edit**.
The Edit Interface Pair dialog box appears.
 - Step 9** You can change the name, choose a new inline interface pair, or edit the description.
 - Step 10** Click **OK**.
The edited inline interface pair appears in the list on the Interface Pairs pane.

- Step 11** To delete an inline interface pair, select it, and click **Delete**.
The inline interface pair no longer appears in the list on the Interface Pairs pane.



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

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

Configuring Inline VLAN Pairs



Note For information on what you need to configure if you are using the hardware bypass card on IPS-4260, see [Interface Configuration Restrictions, page 3-5](#).

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

- [Overview, page 3-17](#)
- [Supported User Role, page 3-18](#)
- [Field Definitions, page 3-18](#)
- [Configuring Inline VLAN Pairs, page 3-19](#)

Overview

The VLAN Pairs pane displays the existing inline VLAN pairs for each physical interface. Click **Add** 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 the virtual sensor.

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 If your sensor does not support inline VLAN pairs, the VLAN Pairs pane is not displayed. AIP-SSM and NM-CIDS do not support inline VLAN pairs.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure inline VLAN pairs.

Field Definitions

This sections lists field definitions for inline VLAN pairs, and contains the following topics:

- [VLAN Pairs Pane, page 3-18](#)
- [Add and Edit VLAN Pair Dialog Boxes, page 3-19](#)

VLAN Pairs Pane

The following fields and buttons are found on the Interface Pairs pane.

Field Descriptions:

- Interface Name—Name of the inline VLAN pair.
- Subinterface (VLAN Pair)—Subinterface number of the inline VLAN pair.
The value is 1 to 255.
- VLAN1—Displays the VLAN number for VLAN1.
The value is 1 to 4095.
- VLAN2—Displays the VLAN number for VLAN2.
The value is 1 to 4095.
- Description—Your description of the inline VLAN pair.

Button Functions:

- Select All—Selects all VLAN pairs.
- Add—Opens the Add VLAN Pair dialog box. From this dialog box, you can add a VLAN pair.
- Edit—Opens the Edit VLAN Pair dialog box.
From this dialog box, you can edit the values of the VLAN pair.
- Delete—Deletes the selected VLAN pair.
- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Add and Edit VLAN Pair Dialog Boxes

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

Field Descriptions:



Note

You cannot pair a VLAN with itself.

- **Interface Name**—Lets you choose the available interface to make an inline VLAN pair.
- **Subinterface Number**—Lets you assign a subinterface number.
You can assign a number from 1 to 255.
- **VLAN 1**—Lets you specify the first VLAN for this inline VLAN pair.
You can assign any VLAN from 1 to 4095.
- **VLAN 2**—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.


Button Functions:

- **OK**—Accepts your changes and closes the dialog box.
- **Cancel**—Discards your changes and closes the dialog box.
- **Help**—Displays the help topic for this feature.

Configuring Inline VLAN Pairs

To configure inline VLAN pairs, follow these steps:

-
- Step 1** Log in to IDM using an account with administrator privileges.
 - Step 2** Choose **Configuration > Interface Configuration > VLAN Pairs**.
The VLAN Pairs pane appears.
 - Step 3** Click **Add** to add inline VLAN pairs.
The Add Inline VLAN Pair dialog box appears.
 - Step 4** Select an interface from the Interface Name list.
 - Step 5** Enter a subinterface number (1 to 255) for the inline VLAN pair in the Subinterface Number field.
 - Step 6** Specify the first VLAN (1 to 4095) for this inline VLAN pair in the VLAN 1 field.
 - Step 7** Specify the other VLAN (1 to 4095) for this inline VLAN pair in the VLAN 2 field.
 - Step 8** You can add a description of the inline VLAN pair in the Description field if you want to.
 - Step 9** Click **OK**.
The new inline VLAN pair appears in the list on the VLAN Pairs pane.

- Step 10** To edit an inline VLAN pair, select it, and click **Edit**.
The Edit Inline VLAN Pair dialog box appears.
- Step 11** You can change the subinterface number, the VLAN numbers, or edit the description.
- Step 12** Click **OK**.
The edited VLAN pair appears in the list on the VLAN Pairs pane.
- Step 13** To delete a VLAN pair, select it, and click **Delete**.
The VLAN pair no longer appears in the list on the VLAN Pairs pane.
-  **Tip** To discard your changes, click **Reset**.
- Step 14** Click **Apply** to apply your changes and save the revised configuration.

Configuring Bypass Mode



Note

For information on what you need to configure if you are using the hardware bypass card on IPS-4260, see [Interface Configuration Restrictions, page 3-5](#).

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

- [Overview, page 3-20](#)
- [Supported User Role, page 3-21](#)
- [Field Definitions, page 3-21](#)

Overview

You can use the bypass mode as a diagnostic tool and a failover protection mechanism. You can set the sensor in a mode where all the IPS processing subsystems are bypassed and traffic is permitted to flow between the inline pairs directly. The bypass mode ensures that packets continue to flow through the sensor when the sensor's processes are temporarily stopped for upgrades or when the sensor's monitoring processes fail. There are three modes: on, off, and automatic. By default, bypass mode is set to automatic.



Note

Bypass mode was originally intended to only be applicable to inline-paired interfaces. Because of a defect, it does affect promiscuous mode. A future version may address this defect. We recommend you configure bypass mode to automatic or off for promiscuous mode and not use the on mode.



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**

Bypass mode only functions when the operating system is running. If the sensor is powered off or shut down, bypass mode does not work—traffic is not passed to the sensor.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

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

Field Definitions

The following fields and buttons are found on the Bypass pane.

Field Descriptions:

- Auto—Traffic flows through the sensor for inspection unless the sensor's monitoring process is down.

If the sensor's monitoring process 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 sensor's monitoring process is down, traffic stops flowing. This means that inline traffic is always inspected.

- On—Traffic bypasses the SensorApp and is not inspected. This means that inline traffic is never inspected.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Configuring Traffic Flow Notifications

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

- [Overview, page 3-22](#)
- [Supported User Role, page 3-22](#)
- [Field Definitions, page 3-22](#)
- [Configuring Traffic Flow Notifications, page 3-22](#)

Overview

You can configure the sensor to monitor the flow of packets across an interface and send notification if that flow changes (starts and 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.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

You must be Administrator to configure traffic flow notifications.

Field Definitions

The following fields and buttons are found on the Traffic Flow Notifications pane.

Field Descriptions:

- 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.

Button Functions:

- Apply—Applies your changes and saves the revised configuration.
- Reset—Refreshes the pane by replacing any edits you made with the previously configured value.

Configuring Traffic Flow Notifications

To configure traffic flow notification, follow these steps:

-
- Step 1** Log in to IDM using an account with administrator privileges.
 - Step 2** Choose **Configuration > Interface Configuration > Traffic Flow Notifications**.
The Traffic Flow Notifications pane appears.
 - Step 3** Choose the percent of missed packets that has to occur before you want to receive notification and enter that amount in the Missed Packets Threshold field.
 - Step 4** Choose the amount of seconds that you want to check for the percentage of missed packets and enter that amount in the Notification Interval field.
 - Step 5** Choose 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 in the Interface Idle Threshold field.

**Tip**

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

Step 6

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