CHAPTER 1

Introducing the Sensor

This chapter introduces the sensor and provides information you should know before you install the sensor. In this guide, the term *sensor* refers to all models unless noted otherwise. For a complete list of supported sensors and their model numbers, see Supported Sensors, page 1-15. This chapter contains the following sections:

- How the Sensor Functions, page 1-1
- Supported Sensors, page 1-15
- IPS Appliances, page 1-16
- IPS Modules, page 1-18
- Time Sources and the Sensor, page 1-24
- Installation Preparation, page 1-28
- Site and Safety Guidelines, page 1-28
- Cable Pinouts, page 1-32

How the Sensor Functions

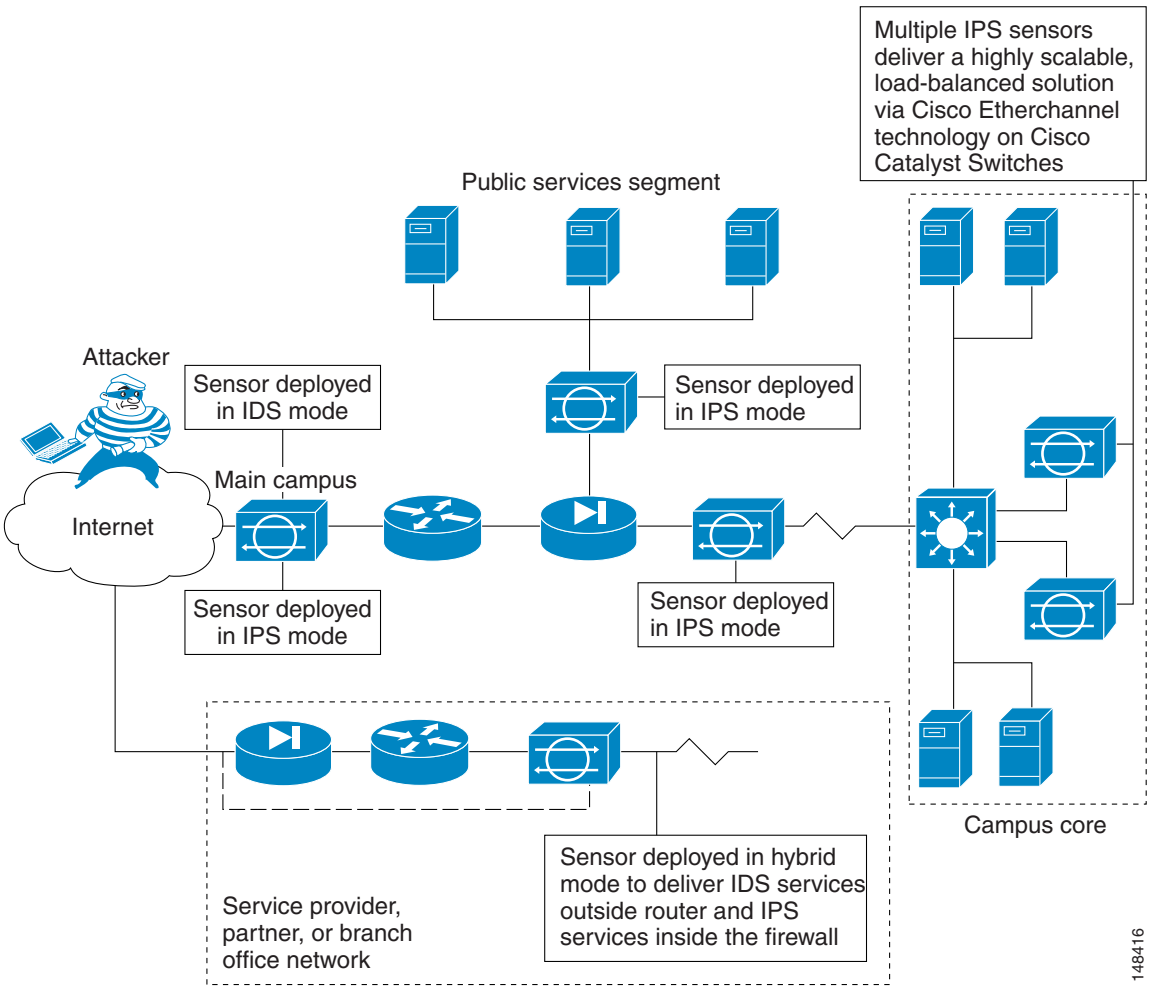
This section describes how the sensor functions, and contains the following topics:

- Capturing Network Traffic, page 1-1
- Your Network Topology, page 1-3
- Correctly Deploying the Sensor, page 1-3
- Tuning the IPS, page 1-3
- Sensor Interfaces, page 1-4
- Interface Modes, page 1-12

Capturing Network Traffic

The sensor can operate in either promiscuous or inline mode. Figure 1-1 on page 1-2 shows how you can deploy a combination of sensors operating in both inline (IPS) and promiscuous (IDS) modes to protect your network.

Figure 1-1 Comprehensive Deployment Solutions



The command and control interface is always Ethernet. This interface has an assigned IP address, which allows it to communicate with the manager workstation or network devices (Cisco switches, routers, and firewalls). Because this interface is visible on the network, you should use encryption to maintain data privacy. SSH is used to protect the CLI and TLS/SSL is used to protect the manager workstation. SSH and TLS/SSL are enabled by default on the manager workstations.

When responding to attacks, the sensor can do the following:

- Insert TCP resets via the sensing interface.

Note You should select the TCP reset action only on signatures associated with a TCP-based service. If selected as an action on non-TCP-based services, no action is taken. Additionally, TCP resets are not guaranteed to tear down an offending session because of limitations in the TCP protocol.

- Make ACL changes on switches, routers, and firewalls that the sensor manages.

Note ACLs may block only future traffic, not current traffic.

- Generate IP session logs, session replay, and trigger packets display.

  IP session logs are used to gather information about unauthorized use. IP log files are written when events occur that you have configured the appliance to look for.
- Implement multiple packet drop actions to stop worms and viruses.

Your Network Topology

Before you deploy and configure your sensors, you should understand the following about your network:

- The size and complexity of your network.
- Connections between your network and other networks (and the Internet).
- The amount and type of network traffic on your network.

This knowledge will help you determine how many sensors are required, the hardware configuration for each sensor (for example, the size and type of network interface cards), and how many managers are needed.

Correctly Deploying the Sensor

You should always position the IPS sensor behind a perimeter-filtering device, such as a firewall or adaptive security appliance. The perimeter device filters traffic to match your security policy thus allowing acceptable traffic in to your network. Correct placement significantly reduces the number of alerts, which increases the amount of actionable data you can use to investigate security violations. If you position the IPS sensor on the edge of your network in front of a firewall, your sensor will produce alerts on every single scan and attempted attack even if they have no significance to your network implementation. You will receive hundreds, thousands, or even millions of alerts (in a large enterprise environment) that are not really critical or actionable in your environment. Analyzing this type of data is time consuming and costly.

Tuning the IPS

Tuning the IPS ensures that the alerts you see reflect true actionable information. Without tuning the IPS, it is difficult to do security research or forensics on your network because you will have thousands of benign events, also known as false positives. False positives are a by-product of all IPS devices, but they occur much less frequently in Cisco IPS devices since Cisco IPS devices are stateful, normalized, and use vulnerability signatures for attack evaluation. Cisco IPS devices also provide risk rating, which identifies high risk events, and policy-based management, which lets you deploy rules to enforce IPS signature actions based on risk rating.

Follow these tips when tuning your IPS sensors:

- Place your sensor on your network behind a perimeter-filtering device.

  Proper sensor placement can reduce the number of alerts you need to examine by several thousands a day.
- Deploy the sensor with the default signatures in place.

  The default signature set provides you with a very high security protection posture. The Cisco signature team has spent many hours on testing the defaults to give your sensor the highest protection. If you think that you have lost these defaults, you can restore them.

- Make sure that the event action override is set to drop packets with a risk rating greater than 90.

  This is the default and ensures that high risk alerts are stopped immediately.
- Filter out known false positives caused by specialized software, such as vulnerability scanner and load balancers by one of the following methods:
  - You can configure the sensor to ignore the alerts from the IP addresses of the scanner and load balancer.
  - You can configure the sensor to allow these alerts and then use IME to filter out the false positives.
- Filter the Informational alerts.

  These low priority events notifications could indicate that another device is doing reconnaissance on a device protected by the IPS. Research the source IP addresses from these Informational alerts to determine what the source is.
- Analyze the remaining actionable alerts:
  - Research the alert.
  - Fix the attack source.
  - Fix the destination host.
  - Modify the IPS policy to provide more information.

For More Information

- For a detailed description of risk rating, refer to Calculating the Risk Rating.
- For information on Cisco signatures for IDM and IME, refer to Defining Signatures, and for the CLI, refer to Defining Signatures.
- For detailed information on event action overrides, for IDM and IME, refer to Configuring Event Action Overrides, and for the CLI, refer to Configuring Event Action Overrides.
- For information on using Cisco IME, refer to *Installing and Using Cisco Intrusion Prevention System Manager Express 6.1*.

Sensor Interfaces

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

- Understanding Sensor Interfaces, page 1-4
- Command and Control Interface, page 1-5
- Sensing Interfaces, page 1-6
- Interface Support, page 1-6
- TCP Reset Interfaces, page 1-9
- Interface Restrictions, page 1-10

Understanding 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 interface card 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 interface card 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 NME-IPS only have one sensing interface, you cannot configure a TCP reset interface.
- Because of hardware limitations on the Catalyst switch, both of the 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.

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

Table 1-1 Command and Control Interfaces

Sensor	Command and Control Interface
AIM-IPS	Management0/0
AIP-SSM-10	GigabitEthernet0/0
AIP-SSM-20	GigabitEthernet0/0
AIP-SSM-40	GigabitEthernet0/0
IDSM-2	GigabitEthernet0/2
IPS-4240	Management0/0

Table 1-1 Command and Control Interfaces (continued)

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

Sensing Interfaces

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

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

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

Interface Support

Table 1-2 describes the interface support for appliances and modules running Cisco IPS 6.1.

Table 1-2 Interface Support

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
AIM-IPS	—	GigabitEthernet0/1 by **ids-service-module** command in the router configuration instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by **ids-service-module** command in the router configuration instead of VLAN pair or inline interface pair	Management0/0
AIP-SSM-10	—	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by security context instead of VLAN pair or inline interface pair	GigabitEthernet0/0

Table 1-2 Interface Support (continued)

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
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
IDSM-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 Slot 1 Slot 2	GigabitEthernet0/1 GigabitEthernet2/0 GigabitEthernet2/1 GigabitEthernet2/2 GigabitEthernet2/3 GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet3/2 GigabitEthernet3/3	 2/0<->2/1[1] 2/2<->2/3 3/0<->3/1 3/2<->3/3	Management0/0
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

Table 1-2 Interface Support (continued)

Base Chassis	Added Interface Cards	Interfaces Supporting Inline VLAN Pairs (Sensing Ports)	Combinations Supporting Inline Interface Pairs	Interfaces Not Supporting Inline (Command and Control Port)
IPS-4260	10GE Slot 1	GigabitEthernet0/1 TenGigabitEthernet2/0 TenGigabitEthernet2/1	 2/0<->2/1[2]	Management0/0
IPS 4270-20	—	GigabitEthernet0/1	N/A	Management0/0 Management0/1[3]
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[4] 3/2<->3/3 4/0<->4/1 4/2<->4/3	Management0/0 Management0/1[5]
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[6]
IPS 4270-20	10GE Slot 1 Slot 2	 TenGigabitEthernet5/0 TenGigabitEthernet5/1 TenGigabitEthernet7/0 TenGigabitEthernet7/1	All sensing ports can be paired together	Management0/0 Management0/1[7]
NME-IPS	—	GigabitEthernet0/1 by **ids-service-module** command in the router configuration instead of VLAN pair or inline interface pair	GigabitEthernet0/1 by **ids-service-module** command in the router configuration instead of VLAN pair or inline interface pair	Management0/1

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

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

TCP Reset Interfaces

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

- Understanding Alternate TCP Reset Interfaces, page 1-9
- Designating the Alternate TCP Reset Interface, page 1-10

Understanding Alternate TCP Reset Interfaces

Note The alternate TCP reset interface setting is ignored in inline interface or inline VLAN pair mode, because resets are sent inline in these modes.

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 1-3 lists the alternate TCP reset interfaces.

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

Table 1-3 Alternate TCP Reset Interfaces

Sensor	Alternate TCP Reset Interface
AIM-IPS	None
AIP-SSM-10	None
AIP-SSM-20	None
AIP-SSM-40	None
IDSM-2	System0/1[1]
IPS-4240	Any sensing interface
IPS-4255	Any sensing interface
IPS-4260	Any sensing interface

Table 1-3 Alternate TCP Reset Interfaces (continued)

Sensor	Alternate TCP Reset Interface
IPS 4270-20	Any sensing interface
NME-IPS	None

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

Designating the Alternate TCP Reset Interface

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

- When a switch is being monitored with either SPAN or VACL capture and the switch does not accept incoming packets on the SPAN or VACL capture port.
- When a switch is being monitored with either SPAN or VACL capture for multiple VLANs, and the switch does not accept incoming packets with 802.1q headers.

  Note The TCP resets need 802.1q headers to tell which VLAN the resets should be sent on.

- When a network tap is used for monitoring a connection.

  Note Taps do not permit incoming traffic from the sensor.

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

Interface Restrictions

The following restrictions apply to configuring interfaces on the sensor:

- Physical Interfaces
  - On modules (AIM-IPS, AIP-SSM, IDSM-2, and NME-IPS), all backplane interfaces have fixed speed, duplex, and state settings. These settings are protected in the default configuration on all backplane interfaces.
  - For nonbackplane FastEthernet interfaces the valid speed settings are 10 Mbps, 100 Mbps, and auto. Valid duplex settings are full, half, and auto.
  - For Gigabit copper interfaces (1000-TX on 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, IDM, and IME prompt you to remove any dangling references. You can leave the dangling references and continue editing the configuration.
- CLI, IDM, and IME do not allow configuration changes in Analysis Engine that conflict with the interface configuration.
- CLI allows configuration changes in the interface configuration that cause conflicts in the Analysis Engine configuration. IDM and IME do *not* allow changes in the interface configuration that cause conflicts in the Analysis Engine configuration.

Interface Modes

The following section describes the interface modes, and contains the following topics:

- Promiscuous Mode, page 1-12
- Inline Interface Pair Mode, page 1-13
- Inline VLAN Pair Mode, page 1-13
- VLAN Group Mode, page 1-13
- Deploying VLAN Groups, page 1-14

Promiscuous Mode

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

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

Inline Interface Pair 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, AIP-SSM, and NME-IPS 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.

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.

Note Inline VLAN pairs are supported on all sensors that are compatible with Cisco IPS 6.1 except AIM-IPS, AIP-SSM, and NME-IPS.

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.

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 is in a single VLAN is called the access VLAN. On a trunk port, multiple VLANs can be carried over the port, and each packet has a special header attached called the 802.1q header that contains the VLAN ID. This header is commonly referred as the VLAN tag. However, a trunk port has a special VLAN called the native VLAN. Packets in the native VLAN do not have the 802.1q headers attached. 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.The IDSM2 also operates in this manner, because its two data ports are always connected to the same switch.

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

In the second variation, the two ports are configured as trunk ports, so they can carry multiple VLANs. In this configuration, the sensor bridges multiple VLANs between the two switches. Because multiple VLANs are carried over the inline interface pair, the VLANs can be divided into groups and each group can be assigned to a virtual sensor. The second variation does not apply to the IDSM2 because it cannot be connected in this way.

For More Information

For information on how to configure IDSM-2, refer to Configuring IDSM-2.

Supported Sensors

Caution Installing the most recent software (version 6.1) on unsupported sensors may yield unpredictable results. We do not support software installed on unsupported platforms.

Table 1-4 lists the sensors (IPS appliances and modules) that are supported by Cisco IPS 6.1.

Table 1-4 Supported Sensors

Model Name	Part Number	Optional Interfaces
Appliances		
IPS-4240	IPS-4240-K9 IPS-4240-DC-K9[1]	— —
IPS-4255	IPS-4255-K9	—
IPS-4260	IPS-4260-K9 IPS-4260-4GE-BP-K9 IPS-4260-2SX-K9 IPS-4260-2X10GE-SR-K9	IPS-4GE-BP-INT= IPS-2SX-INT= IPS-2X10GE-SR-INT= — — —
IPS 4270-20	IPS-4270-K9 IPS-4270-4GE-BP-K9 IPS-4270-2SX-K9 IPS-4270-2X10GE-SR-K9	IPS-4GE-BP-INT= IPS-2SX-INT= IPS-2X10GE-SR-INT= — — —
Modules		
AIM-IPS	AIM-IPS-K9	—
AIP-SSM-10	ASA-SSM-AIP-10-K9	—
AIP-SSM-20	ASA-SSM-AIP-20-K9	—
AIP-SSM-40	ASA-SSM-AIP-40-K9	—
IDSM-2	WS-SVC-IDSM2-K9	—
NME-IPS	NM-IPS-K9	—

1. IPS-4240-DC-K9 is a NEBS-compliant product.

The following NRS and IDS appliance models are legacy models and are not supported in this document:

- NRS-2E
- NRS-2E-DM
- NRS-2FE
- NRS-2FE-DM
- NRS-TR
- NRS-TR-DM
- NRS-SFDDI
- NRS-SFDDI-DM
- NRS-DFDDI
- NRS-DFDDI-DM
- IDS-4220-E
- IDS-4220-TR
- IDS-4230-FE
- IDS-4230-SFDDI
- IDS-4230-DFDDI
- IDS-4210
- IDS-4215
- IDS-4235
- IDS-4250
- NM-CIDS

Note The WS-X6381, the IDSM, is a legacy model and is not supported in this document.

For More Information

For instructions on how to obtain the most recent Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.

IPS Appliances

This section describes the Cisco 4200 series appliance, and contains the following topics:

- Introducing the IPS Appliance, page 1-17
- Appliance Restrictions, page 1-17
- Connecting an Appliance to a Terminal Server, page 1-17

Introducing the IPS Appliance

The IPS appliance is a high-performance, plug-and-play device. The appliance is a component of the IPS, a network-based, real-time intrusion prevention system.

You can use the IPS CLI, IDM, IME, ASDM, or CSM to configure the appliance. For a list of IPS documents and how to access them, refer to *Documentation Roadmap for Cisco Intrusion Prevention System 6.1*.

You can configure the appliance to respond to recognized signatures as it captures and analyzes network traffic. These responses include logging the event, forwarding the event to the manager, performing a TCP reset, generating an IP log, capturing the alert trigger packet, and reconfiguring a router. The appliance offer significant protection to your network by helping to detect, classify, and stop threats including worms, spyware and adware, network viruses, and application abuse.

After being installed at key points in the network, the appliance monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the system detects unauthorized activity, appliances can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the manager. Other legitimate connections continue to operate independently without interruption.

Appliances are optimized for specific data rates and are packaged in Ethernet, Fast Ethernet, and Gigabit Ethernet configurations. In switched environments, appliances must be connected to the switch's SPAN port or VACL capture port.

The Cisco IPS 4200 series appliances provide the following:

- Protection of multiple network subnets through the use of up to eight interfaces
- Simultaneous, dual operation in both promiscuous and inline modes
- A wide array of performance options—from 80 Mbps to multiple gigabits
- Embedded web-based management solutions packaged with the sensor

For More Information

For a list of supported appliances, see Supported Sensors, page 1-15.

Appliance Restrictions

The following restrictions apply to using and operating the appliance:

- The appliance is not a general purpose workstation.
- Cisco Systems prohibits using the appliance for anything other than operating Cisco IPS.
- Cisco Systems prohibits modifying or installing any hardware or software in the appliance that is not part of the normal operation of the Cisco IPS.

Connecting an Appliance to a Terminal Server

A terminal server is a router with multiple, low speed, asynchronous ports that are connected to other serial devices. You can use terminal servers to remotely manage network equipment, including appliances.

To set up a Cisco terminal server with RJ-45 or hydra cable assembly connections, follow these steps:

Step 1 Connect to a terminal server using one of the following methods:

- For terminal servers with RJ-45 connections, connect a 180 rollover cable from the console port on the appliance to a port on the terminal server.
- For hydra cable assemblies, connect a straight-through patch cable from the console port on the appliance to a port on the terminal server.

Step 2 Configure the line and port on the terminal server.

In enable mode, enter the following configuration, where # is the line number of the port to be configured:

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

Step 3 Be sure to properly close a terminal session to avoid unauthorized access to the appliance.

If a terminal session is not stopped properly, that is, if it does not receive an exit(0) signal from the application that initiated the session, the terminal session can remain open. When terminal sessions are not stopped properly, authentication is not performed on the next session that is opened on the serial port.

Caution Always exit your session and return to a login prompt before terminating the application used to establish the connection.

Caution If a connection is dropped or terminated by accident, you should reestablish the connection and exit normally to prevent unauthorized access to the appliance.

IPS Modules

This section describes the IPS modules, and contains the following topics:

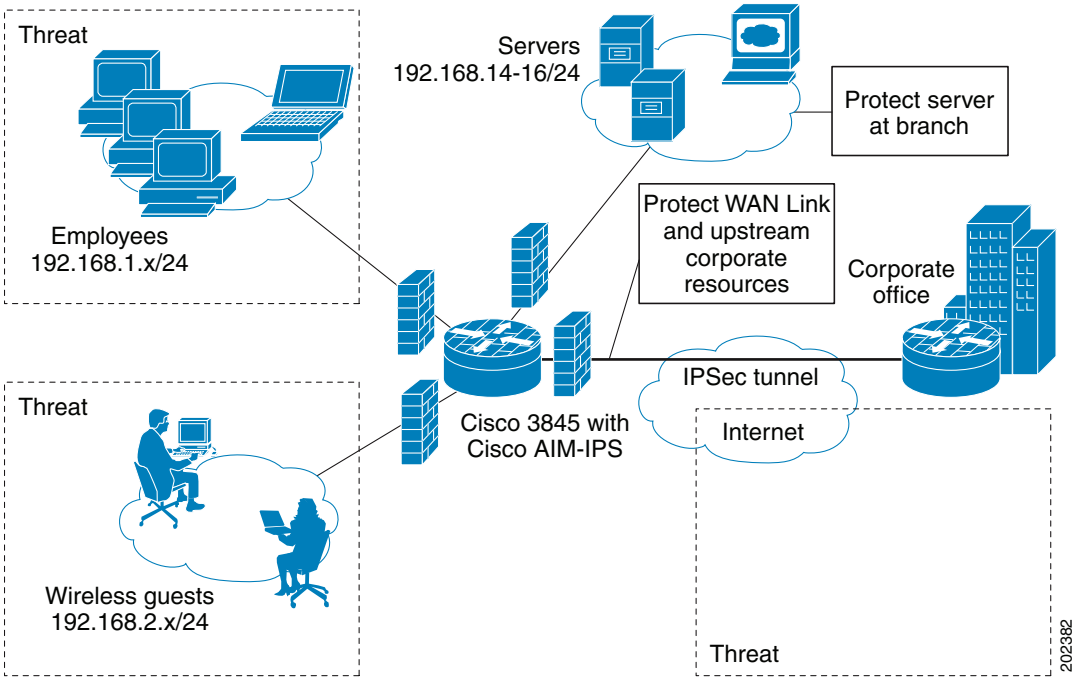
- Introducing AIM-IPS, page 1-19
- Introducing NME-IPS, page 1-20
- Introducing AIP-SSM, page 1-21
- Introducing IDSM-2, page 1-23

Introducing AIM-IPS

Cisco Intrusion Prevention System Advanced Integration Module (AIM-IPS) integrates and bring inline Cisco IPS functionality to Cisco access routers. You can install AIM-IPS in Cisco 1841, 2800 series, and 3800 series routers.

Figure 1-2 demonstrates the integration of IPS and the branch office router.

Figure 1-2 AIM-IPS and the Branch Router

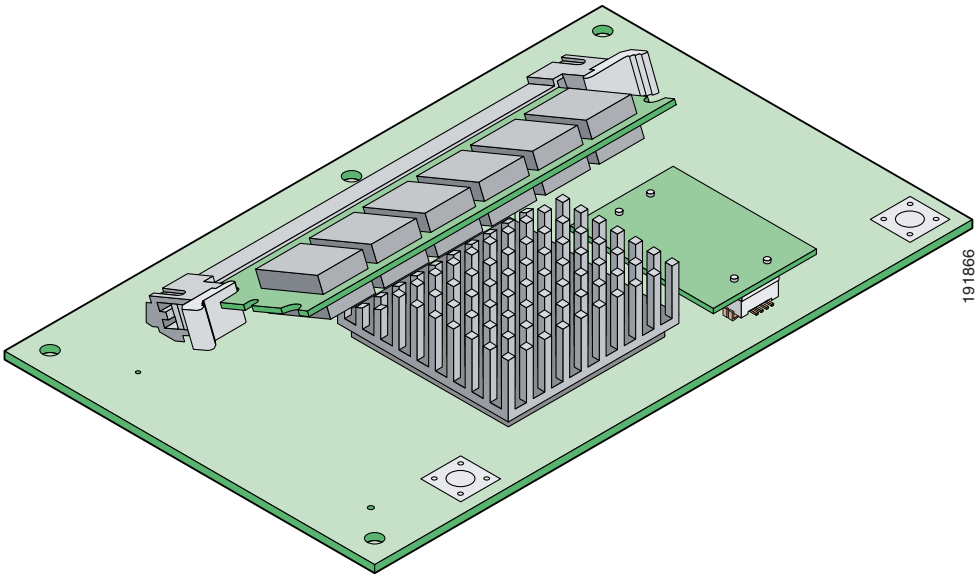


AIM-IPS has its own operating system, Cisco IPS software, startup, and run-time configurations. You launch and configure AIM-IPS through the router by means of a configuration session on the module. After the session, you return to the router CLI and clear the session.

AIM-IPS has a backplane interface, which means that all management traffic passes through the router interface rather than a dedicated port on the module. AIM-IPS does not have an external FastEthernet interface for handling management traffic. Management traffic includes all communications between applications, such as IDM, IME, CSM, and CS-MARS, and the servers on the module for exchange of IPS events, IP logs, configuration, and control messages.

AIM-IPS plugs in to a connector on the motherboard of the router and requires no external interfaces or connections. Figure 1-3 on page 1-20 shows AIM-IPS.

Figure 1-3 AIM-IPS



For More Information

- For a list of supported router and AIM-IPS combinations, see Software and Hardware Requirements, page 5-2.
- For information on installing AIM-IPS, see Installation and Removal Instructions, page 5-5.
- For more information about sessioning to AIM-IPS, see Logging In to AIM-IPS, page 10-4.

Introducing NME-IPS

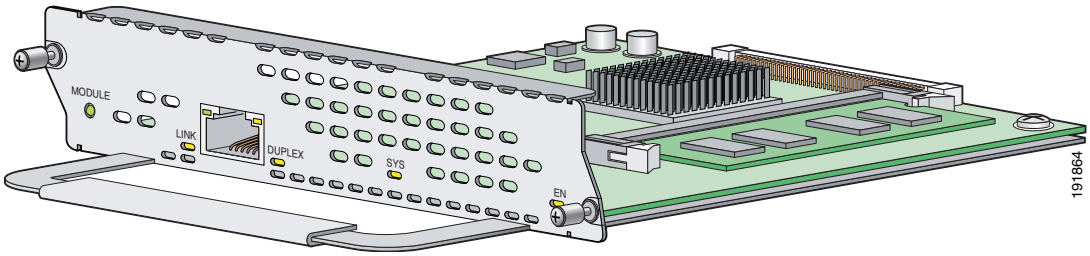
Cisco Intrusion Prevention System Network Module (NME-IPS) integrates and brings inline Cisco IPS functionality to Cisco access routers. You can install NME-IPS in any one of the network module slots in the 2800 and 3800 series router.

NME-IPS has its own operating system, Cisco IPS software, startup, and run-time configurations. You launch and configure the modules through the router by means of a configuration session on the modules. After the session, you return to the router CLI and clear the session.

For NME-IPS, all management traffic passes through the external FastEthernet interface on the module. Management traffic includes all communications between applications, such as IDM, IME, CSM, and CS-MARS, and the servers on the module for exchange of IPS events, IP logs, configuration, and control messages.

NME-IPS installs in any slot in the 2800 and 3800 series access routers. Figure 1-4 shows NME-IPS.

Figure 1-4 NME-IPS



For More Information

- For a list of supported router and NME-IPS combinations, see Software and Hardware Requirements, page 8-2.
- For information on installing NME-IPS, see Installation and Removal Instructions, page 8-5.
- For more information about sessioning to NME-IPS, see Logging In to NME-IPS, page 10-9.

Introducing AIP-SSM

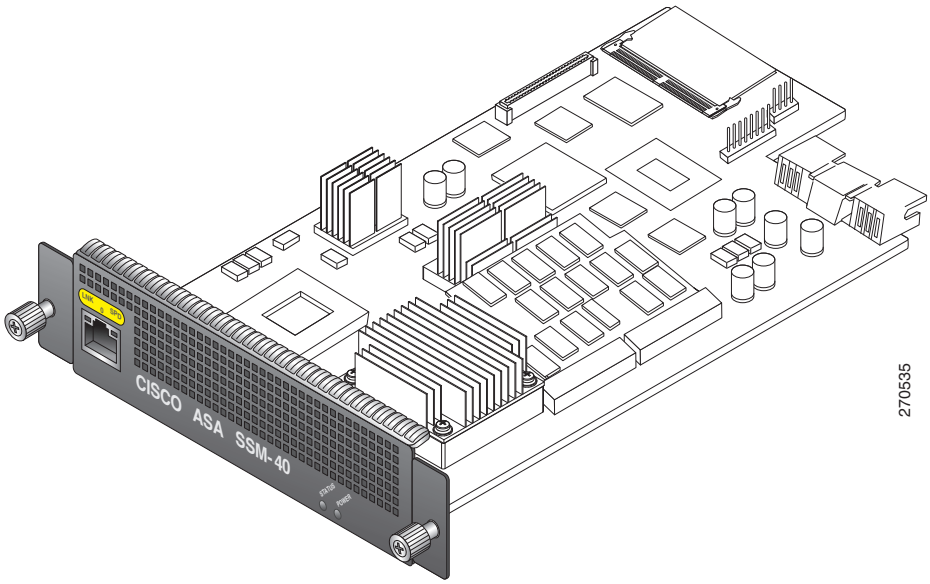
The Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM) is the IPS plug-in module in the Cisco ASA 5500 series adaptive security appliance (adaptive security appliance). The adaptive security appliance software integrates firewall, VPN, and intrusion detection and prevention capabilities in a single platform.

There are three models of AIP-SSM:

- ASA-SSM-AIP-10-K9
  - Supports 150 Mbps of IPS throughput when installed in ASA 5510
  - Supports 225 Mbps of IPS throughput when installed in ASA 5520
- ASA-SSM-AIP-20-K9
  - Supports 375 Mbps of IPS throughput when installed in ASA 5520
  - Supports 500 Mbps of IPS throughput when installed in ASA 5540
- ASA-SSM-AIP-40-K9
  - Supports 450 Mbps of IPS throughput on the ASA 5520
  - Supports 650 Mbps IPS throughput on ASA 5540

Figure 1-5 shows AIP-SSM-40.

Figure 1-5 AIP-SSM-40



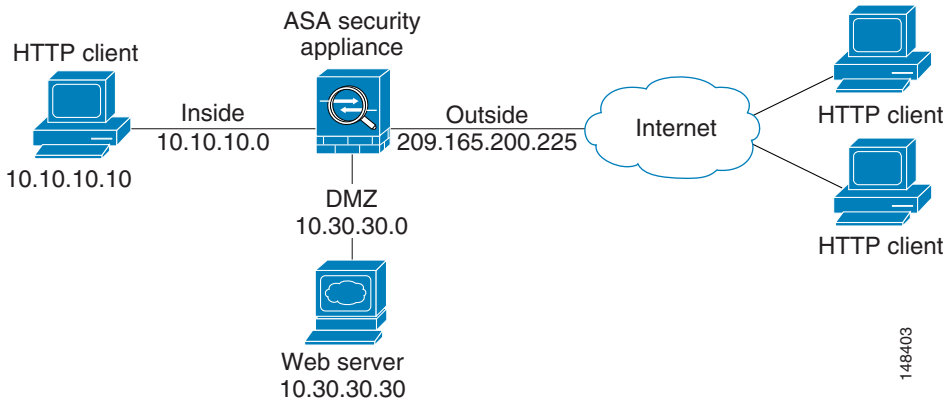
AIP-SSM runs advanced IPS software that provides further security inspection either in inline mode or promiscuous mode. The adaptive security appliance diverts packets to AIP-SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. For example, packets that are blocked by an access list are not forwarded to AIP-SSM.

In promiscuous mode, the IPS receives packets over the GigabitEthernet interface, examines them for intrusive behavior, and generates alerts based on a positive result of the examination. In inline mode, there is the additional step of sending all packets, which did not result in an intrusion, back out the GigabitEthernet interface.

Figure 1-6 on page 1-23 shows the adaptive security appliance with AIP-SSM in a typical DMZ configuration. A DMZ is a separate network located in the neutral zone between a private (inside) network and a public (outside) network. The web server is on the DMZ interface, and HTTP clients from both the inside and outside networks can access the web server securely.

In Figure 1-6 on page 1-23 an HTTP client (10.10.10.10) on the inside network initiates HTTP communications with the DMZ web server (30.30.30.30). HTTP access to the DMZ web server is provided for all clients on the Internet; all other communications are denied. The network is configured to use an IP pool (a range of IP addresses available to the DMZ interface) of addresses between 30.30.30.50 and 30.30.30.60.

Figure 1-6 DMZ Configuration



For More Information

- For more information on setting up ASA, refer to the Getting Started Guides found at this URL:

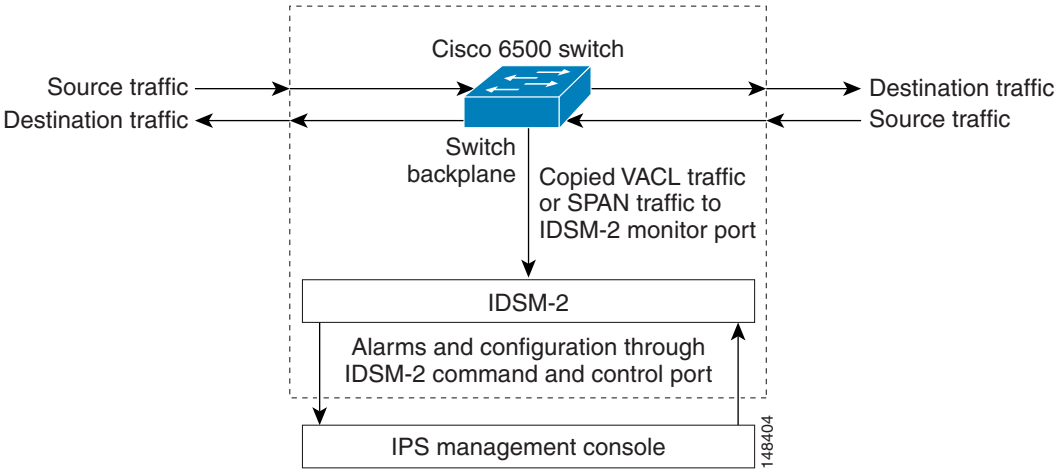
  http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html
- For more information on installing AIP-SSM, see Installing AIP-SSM, page 6-3.
- For more information on configuring AIP-SSM to receive IPS traffic, refer to Configuring AIP-SSM.

Introducing IDSM-2

The Cisco Catalyst 6500 Series Intrusion Detection System Services Module (IDSM-2) is a switching module that performs intrusion prevention in the Catalyst 6500 series switch and 7600 series router. You can use the CLI or IDSM to configure IDSM-2. You can configure IDSM-2 for promiscuous or inline mode.

IDSM-2 performs network sensing—real-time monitoring of network packets through packet capture and analysis. IDSM-2 captures network packets and then reassembles and compares the packet data against attack signatures indicating typical intrusion activity. Network traffic is either copied to IDSM-2 based on security VACLs in the switch or is copied to IDSM-2 through the SPAN port feature of the switch. These methods route user-specified traffic to IDSM-2 based on switch ports, VLANs, or traffic type to be inspected (Figure 1-7 on page 1-24).

Figure 1-7 IDSM-2 Block Diagram



IDSM-2 searches for patterns of misuse by examining either the data portion and/or the header portion of network packets. Content-based attacks contain potentially malicious data in the packet payload, whereas, context-based attacks contain potentially malicious data in the packet headers.

You can configure IDSM-2 to generate an alert when it detects potential attacks. Additionally, you can configure IDSM-2 to transmit TCP resets on the source VLAN, generate an IP log, and/or initiate blocking countermeasures on a firewall or other managed device. Alerts are generated by IDSM-2 through the Catalyst 6500 series switch backplane to the IPS manager, where they are logged or displayed on a graphical user interface.

For More Information

- For more information on installing IDSM-2, see Installing IDSM-2, page 7-5.
- For more information on configuring IDSM-2 to receive IPS traffic, refer to Configuring IDSM-2.

Time Sources and the Sensor

This section explains the importance of having a reliable time source for the sensors and how to correct the time if there is an error. It contains the following topics:

- The Sensor and Time Sources, page 1-24
- Synchronizing IPS Module System Clocks with the Parent Device System Clock, page 1-26
- Correcting the Time on the Sensor, page 1-27

The Sensor and Time Sources

The sensor requires a reliable time source. All events (alerts) must have the correct UTC and local time stamp, otherwise, you cannot correctly analyze the logs after an attack. When you initialize the sensor, you set up the time zones and summertime settings.

Here is a summary of ways to set the time on sensors:

- For appliances
  - Use the **clock set** command to set the time. This is the default.
  - Use NTP

    You can configure the appliance to get its time from an NTP time synchronization source. You need the NTP server IP address, the NTP key ID, and the NTP key value. You can set up NTP on the appliance during initialization or you can configure NTP through the CLI, IDM, IME, or ASDM.

    Note We recommend that you use an NTP time synchronization source.

- For IDSM-2
  - The IDSM-2 can automatically synchronize its clock with the switch time. This is the default.

    Note The UTC time is synchronized between the switch and the IDSM-2. The time zone and summertime settings are not synchronized between the switch and the IDSM-2.

Caution Be sure to set the time zone and summertime settings on both the switch and IDSM-2 to ensure that the UTC time settings are correct. The local time of IDSM-2 could be incorrect if the time zone and/or summertime settings do not match between IDSM-2 and the switch.

  - Use NTP

    You can configure IDSM-2 to get its time from an NTP time synchronization source. You need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure IDSM-2 to use NTP during initialization or you can set up NTP through the CLI, IDM, IME, or ASDM.

    Note We recommend that you use an NTP time synchronization source.

- For AIM-IPS and NME-IPS
  - AIM-IPS and NME-IPS can automatically synchronize their clock with the clock in the router chassis in which they are installed (parent router). This is the default.

    Note The UTC time is synchronized between the parent router and AIM-IPS and NME-IPS. The time zone and summertime settings are not synchronized between the parent router and AIM-IPS and NME-IPS.

Caution Be sure to set the time zone and summertime settings on both the parent router and AIM-IPS and NME-IPS to ensure that the UTC time settings are correct. The local time of AIM-IPS and NME-IPS could be incorrect if the time zone and/or summertime settings do not match between AIM-IPS and NME-IPS and the router.

  - Use NTP

    You can configure AIM-IPS and NME-IPS to get their time from an NTP time synchronization source, such as a Cisco router, other than the parent router. You need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure AIM-IPS and NME-IPS to use NTP during initialization or you can set up NTP through the CLI, IDM, IME, or ASDM.

    Note We recommend that you use an NTP time synchronization source.

Note AIM-IPS and NME-IPS can also use unanthenticated NTP.

- For AIP-SSM
  - AIP-SSM can automatically synchronize its clock with the clock in the adaptive security appliance in which it is installed. This is the default.

    Note The UTC time is synchronized between the adaptive security appliance and AIP-SSM. The time zone and summertime settings are not synchronized between the adaptive security appliance and AIP-SSM.

Caution Be sure to set the time zone and summertime settings on both the adaptive security appliance and AIP-SSM to ensure that the UTC time settings are correct. The local time of AIP-SSM could be incorrect if the time zone and/or summertime settings do not match between AIP-SSM and the adaptive security appliance.

  - Use NTP

    You can configure AIP-SSM to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router. You need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure AIP-SSM to use NTP during initialization or you can set up NTP through the CLI, IDM, IME, or ASDM.

    Note We recommend that you use an NTP time synchronization source.

Synchronizing IPS Module System Clocks with the Parent Device System Clock

All IPS modules (AIM-IPS, AIP-SSM, IDSM-2, and NME-IPS) synchronize their system clocks to the parent chassis clock (switch, router, or security appliance) each time the module boots up and any time the parent chassis clock is set. The module clock and parent chassis clock tend to drift apart over time. The difference can be as much as several seconds per day. To avoid this problem, make sure that both the module clock and the parent clock are synchronized to an external NTP server. If only the module clock or only the parent chassis clock is synchronized to an NTP server, the time drift occurs.

Verifying the Sensor is Synchronized with the NTP Server

In Cisco IPS, you cannot apply an incorrect NTP configuration, such as an invalid NTP key value or ID, to the sensor. If you try to apply an incorrect configuration, you receive an error message. To verify the NTP configuration, use the **show statistics host** command to gather sensor statistics. The NTP statistics section provides NTP statistics including feedback on sensor synchronization with the NTP server.

To verify the NTP configuration, follow these steps:

Step 1 Log in to the sensor.

Step 2 Generate the host statistics:

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
         LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f014   yes   yes   ok     reject   reachable  1
          2 10373  9014   yes   yes  none    reject   reachable  1
        status = Not Synchronized
     ...
```

Step 3 Generate the hosts statistics again after a few minutes:

```
  sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
        *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
         LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f624   yes   yes   ok   sys.peer   reachable  2
          2 10373  9024   yes   yes  none    reject   reachable  2
        status = Synchronized
```

Step 4 If the status continues to read `Not Synchronized`, check with the NTP server administrator to make sure the NTP server is configured correctly.

Correcting the Time on the Sensor

If you set the time incorrectly, your stored events will have the incorrect time because they are stamped with the time the event was created.

The Event Store time stamp is always based on UTC time. If during the original sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events might have times older than old events.

For example, if during the initial setup, you configure the sensor as central time with daylight saving time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error: the clock shows 21:00:23 CDT. You then change the time to 9:00 a.m. and now the clock shows 09:01:33 CDT. Because the offset from UTC has not changed, it requires that the UTC time now be 14:01:33 UTC, which creates the time stamp problem.

To ensure the integrity of the time stamp on the event records, you must clear the event archive of the older events by using the **clear events** command.

Note You cannot remove individual events.

For More Information

For the procedure for clearing events, refer to Clearing Events from Event Store.

Installation Preparation

To prepare for installing sensors, follow these steps:

Step 1 Review the safety precautions outlined in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

Step 2 To familiarize yourself with the IPS and related documentation and where to find it on Cisco.com, read *Documentation Roadmap for Cisco Intrusion Prevention System 6.1*.

Step 3 Before proceeding with sensor installation, read the *Release Notes for Cisco Intrusion Prevention System 6.1*.

Step 4 Unpack the sensor.

Step 5 Place the sensor in an ESD-controlled environment.

Step 6 Place the sensor on a stable work surface.

Step 7 In this book, *Installing and Using Cisco Intrusion Prevention System Sensors and Modules 6.1*, see the chapter that pertains to your sensor model.

For More Information

For ESD guidelines, see Electrical Safety Guidelines, page 1-29.

Site and Safety Guidelines

This section describes site guidelines and safety precautions to take when working with electricity, with power supplies, and in an ESD environment. It contains the following topics:

- Site Guidelines, page 1-29
- Rack Configuration Guidelines, page 1-29
- Electrical Safety Guidelines, page 1-29

- Power Supply Guidelines, page 1-30
- Working in an ESD Environment, page 1-31

Site Guidelines

Place the appliance on a desktop or mount it in a rack. The location of the appliance and the layout of the equipment rack or wiring room are extremely important for proper system operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause system malfunctions and shutdowns, and can make appliance maintenance difficult.

When planning the site layout and equipment locations, keep in mind the following precautions to help avoid equipment failures and reduce the possibility of environmentally-caused shutdowns. If you are experiencing shutdowns or unusually high errors with your existing equipment, these precautions may help you isolate the cause of failures and prevent future problems.

- Electrical equipment generates heat. Ambient air temperature might not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Make sure that the room in which you operate your system has adequate air circulation.
- Always follow the ESD-prevention procedures to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Make sure that the chassis top panel is secure. The chassis is designed to allow cooling air to flow effectively within it. An open chassis allows air leaks, which can interrupt and redirect the flow of cooling air from the internal components.

Rack Configuration Guidelines

Follow these guidelines to plan your equipment rack configuration:

- Enclosed racks must have adequate ventilation. Make sure the rack is not overly congested because each chassis generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, make sure the rack frame does not block the intake or exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, excessive heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Make sure you provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack. Experiment with different arrangements to position the baffles effectively.

Electrical Safety Guidelines

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.**

Follow these guidelines when working on equipment powered by electricity:

- Before beginning procedures that require access to the interior of the chassis, locate the emergency power-off switch for the room in which you are working. Then, if an electrical accident occurs, you can act quickly to turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your work space.
- Never assume that power is disconnected from a circuit; always check the circuit.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- If an electrical accident occurs, proceed as follows:
  - Use caution; do not become a victim yourself.
  - Disconnect power from the system.
  - If possible, send another person to get medical aid. Otherwise, assess the condition of the victim and then call for help.
  - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.
- Use the chassis within its marked electrical ratings and product usage instructions.
- Install the sensor in compliance with local and national electrical codes as listed in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.
- The sensor models equipped with AC-input power supplies are shipped with a 3-wire electrical cord with a grounding-type plug that fits only a grounding-type power outlet. This is a safety feature that you should not circumvent. Equipment grounding should comply with local and national electrical codes.
- The sensor models equipped with DC-input power supplies must be terminated with the DC input wiring on a DC source capable of supplying at least 15 amps. A 15-amp circuit breaker is required at the 48 VDC facility power source. An easily accessible disconnect device should be incorporated into the facility wiring. Be sure to connect the grounding wire conduit to a solid earth ground. We recommend that you use a Listed closed-loop ring to terminate the ground conductor at the ground stud. The DC return connection to this system is to remain isolated from the system frame and chassis.

  Other DC power guidelines are listed in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

Power Supply Guidelines

Follow these guidelines for power supplies:

- Check the power at the site before installing the chassis to ensure that the power is free of spikes and noise. Install a power conditioner if necessary, to ensure proper voltages and power levels in the source voltage.
- Install proper grounding for the site to avoid damage from lightning and power surges.
- The following applies to a chassis equipped with an AC-input power supply:
  - The chassis does not have a user-selectable operating range. Refer to the label on the chassis for the correct AC-input power requirement.

  - Several types of AC-input power supply cords are available; make sure you have the correct type for your site.
  - Install a UPS for your site.
  - Install proper site-grounding facilities to guard against damage from lightning or power surges.
- The following applies to a chassis equipped with a DC-input power supply:
  - Each DC-input power supply requires dedicated 15-amp service.
  - For DC power cables, we recommend a minimum of 14 AWG wire cable.
  - The DC return connection to this system is to remain isolated from the system frame and chassis.

Working in an ESD Environment

Work on ESD-sensitive parts only at an approved static-safe station on a grounded static dissipative work surface, for example, an ESD workbench or static dissipative mat.

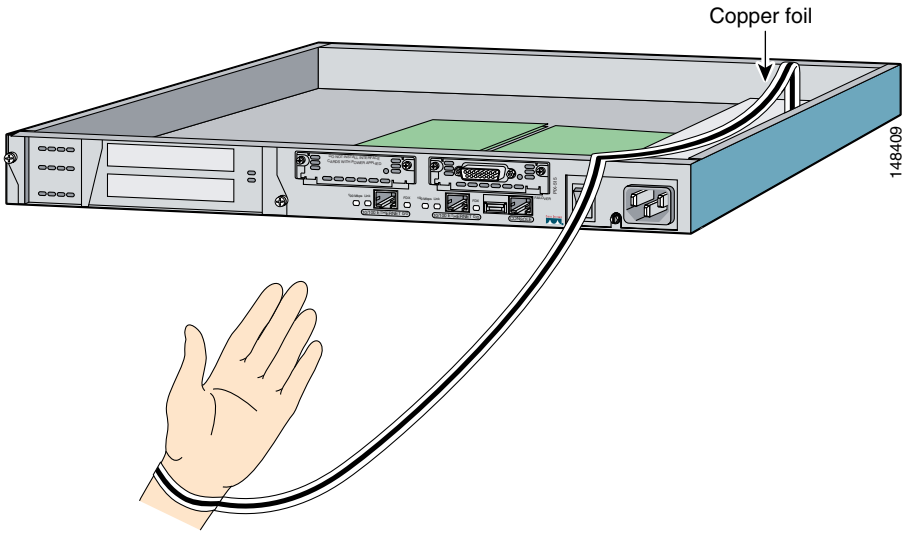
To remove and replace components in a sensor, follow these steps:

Step 1 Remove all static-generating items from your work area.

Step 2 Use a static dissipative work surface and wrist strap.

Note Disposable wrist straps, typically those included with an upgrade part, are designed for one time use.

Step 3 Attach the wrist strap to your wrist and to the terminal on the work surface. If you are using a disposable wrist strap, connect the wrist strap directly to an unpainted metal surface of the chassis.



Step 4 Connect the work surface to the chassis using a grounding cable and alligator clip.

Caution Always follow ESD-prevention procedures when removing, replacing, or repairing components.

Note If you are upgrading a component, do not remove the component from the ESD packaging until you are ready to install it.

Cable Pinouts

This section describes pinout information for 10/100/1000BaseT, console, and RJ 45 to DB 9 ports, and the MGMT 10/100 Ethernet port. It contains the following topics:

- 10/100BaseT and 10/100/1000BaseT Connectors, page 1-32
- Console Port (RJ-45), page 1-33
- RJ-45 to DB-9 or DB-25, page 1-34

10/100BaseT and 10/100/1000BaseT Connectors

Sensors support 10/100/1000BaseT ports. You must use at least a Category 5 cable for 100/1000Base-TX operations. You can use a Category 3 cable for 10Base-TX operations.

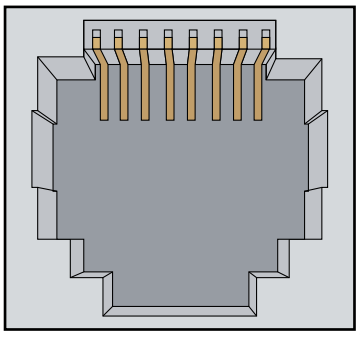
Note Some sensors support 10/100BaseT (IDS-4210, IDS-4215, and the optional 4FE card) while others support 10/100/1000BaseT (IDS-4235, IDS-4250-TX, IPS-4240, and IPS-4255). This only applies to the copper appliances. The fiber appliances support 1000Base-SX only.

The 10/100/1000BaseT ports use standard RJ-45 connectors and support MDI and MDI-X connectors. Ethernet ports normally use MDI connectors and Ethernet ports on a hub normally use MDI-X connectors.

An Ethernet straight-through cable is used to connect an MDI to an MDI-X port. A cross-over cable is used to connect an MDI to an MDI port, or an MDI-X to an MDI-X port.

Figure 1-8 shows the 10/100BaseT (RJ-45) port pinouts.

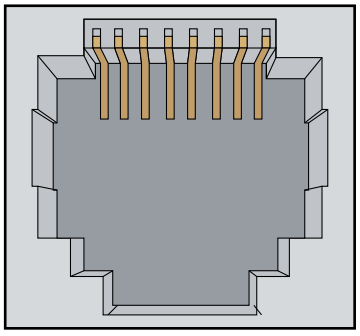
Figure 1-8 10/100 Port Pinouts

Pin	Label	1 2 3 4 5 6 7 8
1	TD+	
2	TD-	
3	RD+	
4	NC	
5	NC	
6	RD-	
7	NC	
8	NC	

148407

Figure 1-9 shows the 10/100/1000BaseT (RJ-45) port pinouts.

Figure 1-9 10/100/1000 Port Pinouts

Pin	Label	1 2 3 4 5 6 7 8
1	TP0+	
2	TP0-	
3	TP1+	
4	TP2+	
5	TP2-	
6	TP1-	
7	TP3+	
8	TP3-	

148410

Console Port (RJ-45)

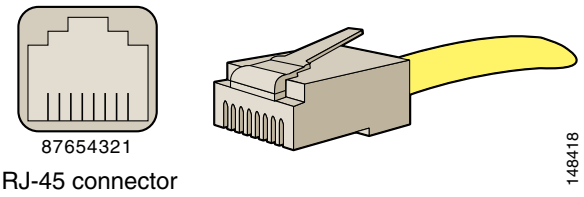
Cisco products use the following types of RJ-45 cables:

- Straight-through
- Cross-over
- Rolled (console)

Note Cisco does not provide these cables; however, they are widely available from other sources.

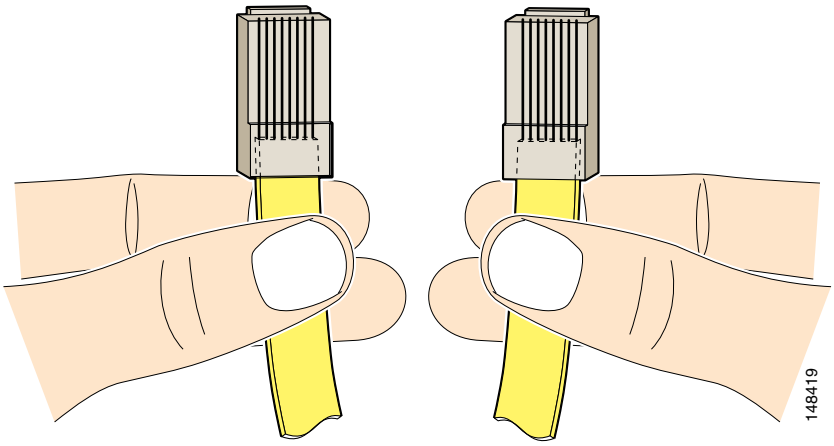
Figure 1-10 shows the RJ 45 cable.

Figure 1-10 RJ-45 Cable



To identify the RJ-45 cable type, hold the two ends of the cable next to each other so that you can see the colored wires inside the ends, as shown in Figure 1-11.

Figure 1-11 RJ-45 Cable Identification



Examine the sequence of colored wires to determine the type of RJ-45 cable, as follows:

- Straight-through—The colored wires are in the same sequence at both ends of the cable.
- Cross-over—The first (far left) colored wire at one end of the cable is the third colored wire at the other end of the cable.
- Rolled—The colored wires are in the opposite sequence at either end of the cable.

RJ-45 to DB-9 or DB-25

Table 1-5 lists the cable pinouts for RJ-45 to DB-9 or DB-25.

Table 1-5 Cable Pinouts for RJ-45 to DB-9 or DB-25

Signal	RJ-45 Pin	DB-9 /DB-25 Pin
RTS	8	8
DTR	7	6
TxD	6	2
GND	5	5

Table 1-5 Cable Pinouts for RJ-45 to DB-9 or DB-25

Signal	RJ-45 Pin	DB-9 /DB-25 Pin
GND	4	5
RxD	3	3
DSR	2	4
CTS	1	7