Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 5.1

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-8677-01

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 5.1

CONTENTS

Preface

Revised: March 27, 2012, OL-8677-01

Contents

This guide describes how to install appliances and modules that support Cisco IPS 5.1. It includes a glossary that contains expanded acronyms and pertinent IPS terms. It is part of the documentation set for Cisco Intrusion Prevention System 5.1. Use this guide in conjunction with the documents listed in Related Documentation, page iv. This preface contains the following topics:

Audience

This guide is for experienced network security administrators who install and maintain Cisco IPS sensors, including the supported IPS appliances and modules.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

These documents support Cisco Intrusion Prevention System 5.1 and can be found on Cisco.com at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

- *Documentation Roadmap for Cisco Intrusion Prevention System 5.1*
- *Release Notes for Cisco Intrusion Prevention System 5.1*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*
- *Command Reference for Cisco Intrusion Prevention System 5.1*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

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 1-11. This chapter contains the following sections:

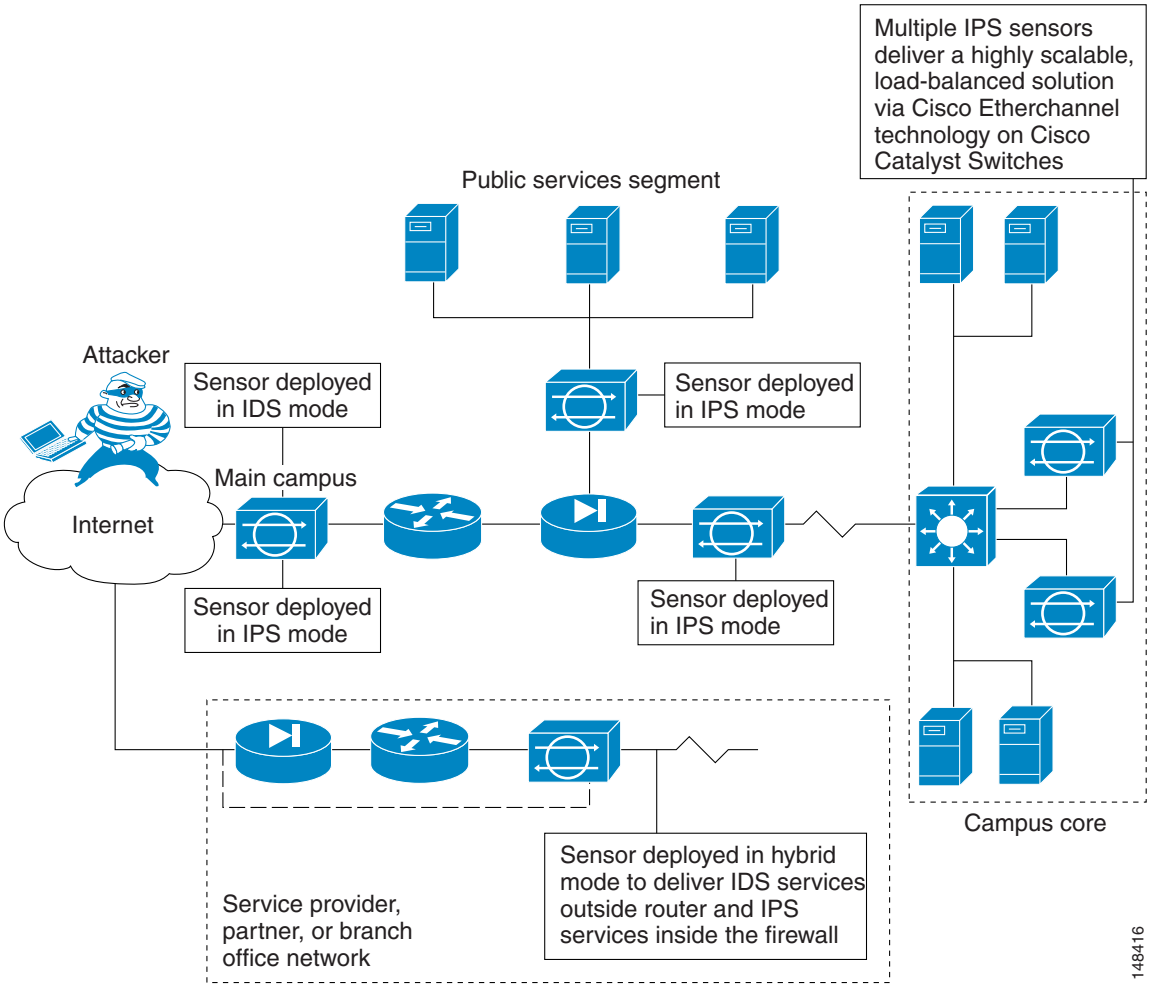
How the Sensor Functions

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

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



Note IDS-4210 and NM-CIDS do not operate in inline mode.

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. On the IDS-4250-XL, TCP resets are sent through the TCP reset interface.

- 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.

Sensor Interfaces

The sensor interfaces are named according to the maximum speed and physical location of the interface. The physical location consists of a port number and a slot number. All interfaces that are built-in on the sensor motherboard are in slot 0, and the PCI expansion slots are numbered beginning with slot 1 for the bottom slot with the slot numbers increasing from bottom to top. Interfaces with a given slot are numbered beginning with port 0 for the right port with the port numbers increasing from right to left. For example, GigabitEthernet2/1 supports a maximum speed of 1 Gigabit and is the second-from-the-right interface in the second-from-the bottom PCI expansion slot. IPS-4240, IPS-4255, and IPS-4260 are exceptions to this rule. The command and control interface on these sensors is called Management0/0 rather than GigabitEthernet0/0.

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 NM-CIDS and AIP-SSM 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.

This section contains the following topics:

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
IDS-4210	FastEthernet0/1
IDS-4215	FastEthernet0/0
IDS-4235	GigabitEthernet0/1
IDS-4250	GigabitEthernet0/1
IPS-4240	Management0/0
IPS-4255	Management0/0
IPS-4260	Management0/0
NM-CIDS	FastEthernet0/0
AIP-SSM-10	GigabitEthernet0/0
AIP-SSM-20	GigabitEthernet0/0
IDSM-2	GigabitEthernet0/2

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. For the number and type of sensing interfaces available for each sensor, see Interface Support, page 1-5.

Sensing interfaces can operate individually in promiscuous mode or you can pair them to create inline interfaces for inline sensing mode. For more information, see Promiscuous Mode, page 1-9, Inline Interface Mode, page 1-10, and Inline VLAN Pair Mode, page 1-10.

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 PCI 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 PCI card, some of the interface configuration is deleted, such as the speed, duplex, description string, enabled/disabled state of the interface, and any inline interface pairings. These settings are restored to their default settings when the card is reinstalled. However, the assignment of promiscuous and inline interfaces to the Analysis Engine is not deleted from the Analysis Engine configuration, but is ignored until those cards are reinserted and you create the inline interface pairs again. For the IDM procedure, refer to Analysis Engine. For the CLI procedure, refer to Assigning Interfaces to the Virtual Sensor.

Interface Support

Table 1-2 describes the interface support for appliances and modules running IPS 5.1:

Table 1-2 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 1-2 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
IDSM-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.

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.

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

- Understanding Alternate TCP Reset Interfaces, page 1-7
- Designating the Alternate TCP Reset Interface, page 1-8

Understanding Alternate TCP Reset Interfaces

You can configure sensors to send TCP reset packets to try to reset a network connection between an attacker host and its intended target host. In some installations when the interface is operating in promiscuous mode, the sensor may not be able to send the TCP reset packets over the same sensing interface on which the attack was detected. In such cases, you can associate the sensing interface with an alternate TCP reset interface and any TCP resets that would otherwise be sent on the sensing interface when it is operating in promiscuous mode, are instead sent out on the associated alternate TCP reset interface. For more information, see Designating the Alternate TCP Reset Interface, page 1-8.

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 limitations.

Table 1-3 lists the alternate TCP reset interfaces.

Table 1-3 Alternate TCP Reset Interfaces

Sensor	Alternate TCP Reset Interface
IDS-4210	None[1]
IDS-4215	Any sensing interface
IDS-4235	Any sensing interface
IDS-4250	Any sensing interface
IPS-4240	Any sensing interface
IPS-4255	Any sensing interface
IPS-4260	Any sensing interface
NM-CIDS	None[2]
AIP-SSM-10	None[3]
AIP-SSM-20	None[4]
IDSM-2	System0/1[5]

1. There is only one sensing interface on IDS-4210.
2. There is only one sensing interface on NM-CIDS.
3. There is only one sensing interface on AIP-SSM-10.
4. There is only one sensing interface on AIP-SSM- 20.
5. 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 (IDSM-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 1-5.
  - 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).

Interface Modes

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

Promiscuous Mode

In promiscuous mode, packets do not flow through the sensor. The sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in promiscuous mode is that the sensor does not affect the packet flow with the forwarded traffic. The disadvantage of operating in promiscuous mode, however, is the sensor cannot stop malicious traffic from reaching its intended target for certain types of attacks, such as atomic attacks (single-packet attacks). The response actions implemented by promiscuous sensor devices are post-event responses and often require

assistance from other networking devices, for example, routers and firewalls, to respond to an attack. While such response actions can prevent some classes of attacks, in atomic attacks the single packet has the chance of reaching the target system before the promiscuous-based sensor can apply an ACL modification on a managed device (such as a firewall, switch, or router).

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.

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 all packets received on any VLANs that are not assigned to inline VLAN pairs.

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.

Supported Sensors

Table 1-4 lists the sensors (appliances and modules) that are supported by Cisco IPS 5.1.

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

Caution Installing the most recent software (version 5.1) on unsupported sensors may yield unpredictable results. We do not support software installed on unsupported platforms.

Table 1-4 Supported Sensors

Model Name	Part Number	Optional Interfaces
Appliances		
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	— — —
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9[1]	IDS-4FE-INT= —
IDS-4235	IDS-4235-K9 IDS-4235-TX-K9	IDS-4FE-INT= IDS-TX-INT=
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	IDS-4FE-INT= IDS-4250-SX-INT=[2] IDS-XL-INT= IDS-TX-INT= — —

Table 1-4 Supported Sensors (continued)

Model Name	Part Number	Optional Interfaces
Appliances		
IPS-4240	IPS-4240-K9 IPS-4240-DC-K9[3]	— —
IPS-4255	IPS-4255-K9	—
IPS-4260	IPS-4260-K9 IPS-4260-4GE-BP-K9 IPS-4260-2SX-K9	IPS-4GE-BP-INT= IPS-2SX-INT= — —
Modules		
AIP-SSM-10	ASA-SSM-AIP-10-K9	—
AIP-SSM-20	ASA-SSM-AIP-20-K9	—
IDSM-2	WS-SVC-IDSM2-K9	—
NM-CIDS	NM-CIDS-K9	—

1. IDS-4215-4FE-K9 is the IDS-4215-K9 with the optional 4FE card (IDS-4FE-INT=) installed at the factory.
2. You can install one or two IDS-4250-SX-INT cards in the IDS-4250.
3. 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

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

Note IDS-4210 requires a memory upgrade to support the most recent IPS software. For more information, see Upgrading the Memory, page 2-3.

Appliances

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

Introducing the Appliance

The 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. For a list of supported appliances, see Supported Sensors, page 1-11.

You can use the CLI, IDM, or ASDM to configure the appliance. Refer to the *Documentation Roadmap for Cisco Intrusion Prevention System 5.1* that shipped with your appliance for the list of IPS documents and how to access them.

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 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

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.

Setting Up 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 IDS-4215, IPS-4240, IPS-4255, and IPS-4260:
  - For 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.
- For all other appliances, connect the M.A.S.H. adapter (part number 29-4077-01) to COM1 on the appliance and:
  - For RJ-45 connections, connect a 180 rollover cable from the M.A.S.H. adapter to a port on the terminal server.
  - For hydra cable assemblies, connect a straight-through patch cable from the M.A.S.H. adapter to a port on the terminal server.

Step 2 Configure the line and port on the terminal server as follows:

a. In enable mode, type 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
```

b. If you are configuring a terminal server for an IDS-4215, IPS-4240, IPS-4255, or IPS-4260 go to Step 3.

Otherwise, for all other supported appliances, to direct all output to the terminal server, log in to the CLI and type the following commands:

```
sensor# configure terminal
sensor(config)# display-serial
```

Output is directed to the serial port. Use the **no display-serial** command to redirect output to the keyboard and monitor.

Note You can set up a terminal server and use the **display-serial** command to direct all output from the appliance to the serial port. This option lets you view system messages on a console connected to the serial port, even during the boot process. When you use this option, all output is directed to the serial port and any local keyboard and monitor connection is disabled. However, BIOS and POST messages are still displayed on the local keyboard and monitor. For the procedure, refer to Directing Output to a Serial Connection.

Note There are no keyboard or monitor ports on an IDS-4215, IPS-4240, IPS-4255, or IPS-4260; therefore, the **display-serial** and **no display-serial** commands do not apply to those platforms.

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.

Modules

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

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 (ASA). The ASA software combines firewall, VPN concentrator, and intrusion detection and prevention software functionality into one software image.

There are two models of AIP-SSM: ASA-SSM-AIP-K9-10 and ASA-SSM-AIP-K9-20. ASA-SSM-AIP-K9-10 supports approximately 100 Mbps throughput and ASA-SSM-AIP-K9-20 supports approximately 200 Mbps. Only one module can populate the slot in an ASA at a time.

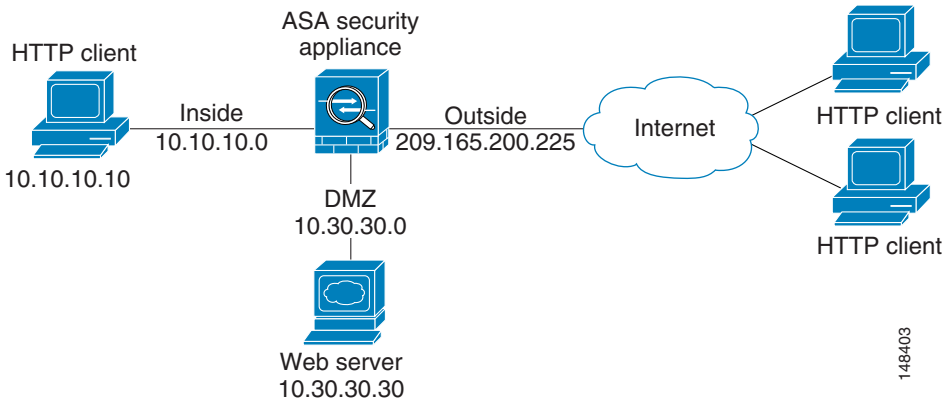
AIP-SSM runs advanced IPS software that provides further security inspection in either inline mode or promiscuous mode. The ASA diverts packets to AIP-SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. 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 1-2 shows ASA 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 1-2 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 1-2 DMZ Configuration



Refer to *Cisco ASA 5500 Quick Start Guide*for more information on setting up ASA. For more information on installing AIP-SSM, see Installing AIP-SSM, page 7-3. For more information on configuring AIP-SSM to receive IPS traffic, refer to Configuring AIP-SSM.

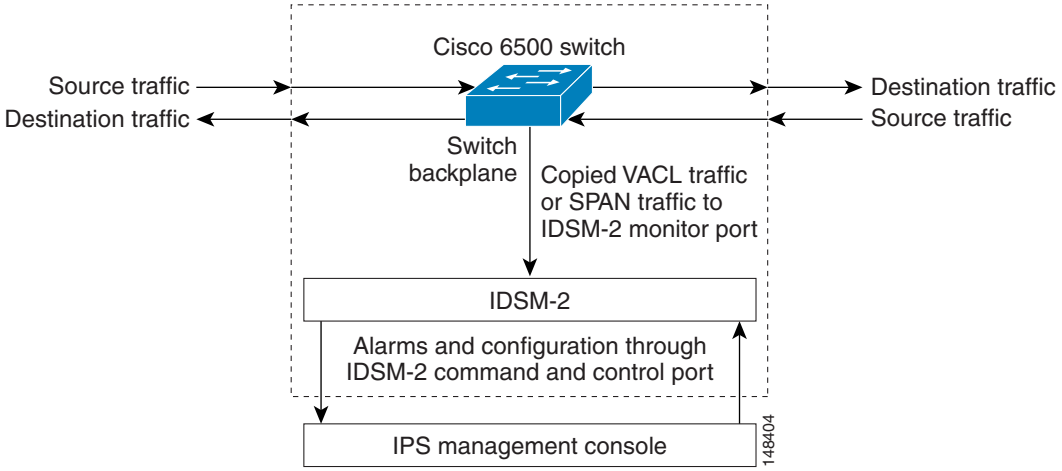
Introducing IDSM-2

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 switch's SPAN port feature. These methods route user-specified traffic to IDSM-2 based on switch ports, VLANs, or traffic type to be inspected. (See Figure 1-3.)

Figure 1-3 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.

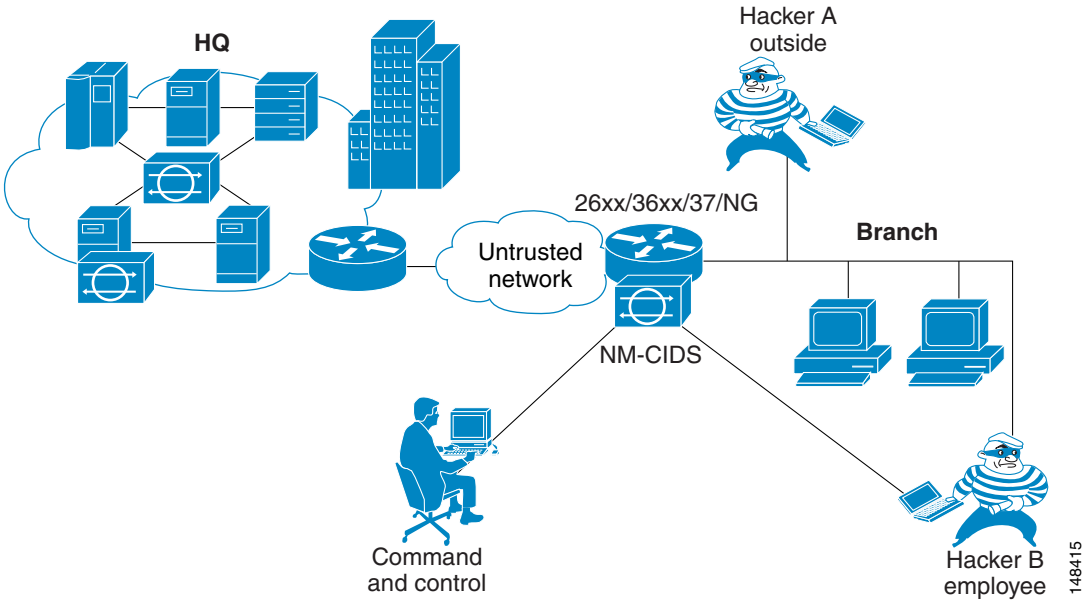
You can configure IDSM-2 to generate an alert when it detects potential attacks. Additionally, you can configure IDSM-2 to transmit TCP resets on the source VLAN, generate an IP log, and/or initiate blocking countermeasures on a firewall or other managed device. Alerts are generated by IDSM-2 through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

Introducing NM-CIDS

The Cisco Intrusion Detection System Network Module (NM-CIDS) integrates the Cisco IDS functionality into a branch office router. With NM-CIDS, you can implement full-featured IDS at your remote branch offices. You can install NM-CIDS in any one of the network module slots on the Cisco 2600, 3600, and 3700 series routers. NM-CIDS can monitor up to 45 Mbps of network traffic. For a list of supported routers, see Software and Hardware Requirements, page 9-2. Only one NM-CIDS is supported per router. Figure 1-4 on page 1-18 shows the router in a branch office environment.

Note NM-CIDS operates in promiscuous mode (IDS mode) only.

Figure 1-4 NM-CIDS in the Branch Office Router



NM-CIDS has one internal 10/100 Ethernet port that connects to the router's backplane. There is also one external 10/100-based Ethernet port that is used for device management (management of other routers and/or PIX Firewalls to perform blocking) and command and control of NM-CIDS by IDS managers.

NM-CIDS communicates with the router to exchange control and state information for bringing up and shutting down NM-CIDS and to exchange version and status information. NM-CIDS processes packets that are forwarded from selected interfaces on the router to the IDS interface on NM-CIDS. NM-CIDS analyzes the captured packets and compares them against a rule set of typical intrusion activity called signatures. If the captured packets match a defined intrusion pattern in the signatures, NM-CIDS can take one of two actions: it can make ACL changes on the router to block the attack, or it can send a TCP reset packet to the sender to stop the TCP session that is causing the attack.

In addition to analyzing captured packets to identify malicious activity, NM-CIDS can also perform IP session logging that can be configured as a response action on a per-signature basis. When the signature fires, session logs are created over a specified time period in a tcpdump format. You can view these logs using Ethereal or replay the IP session using tools such as TCP Replay.

You can manage and retrieve events from NM-CIDS through the CLI or IDM.

The IDS requires a reliable time source. All the events (alerts) must have the correct time stamp, otherwise, you cannot correctly analyze the logs after an attack. You cannot manually set the time on NM-CIDS. NM-CIDS gets its time from the Cisco router in which it is installed. Routers do not have a battery so they cannot preserve a time setting when they are powered off. You must set the router's clock each time you power up or reset the router, or you can configure the router to use NTP time synchronization. We recommend NTP time synchronization. You can configure either NM-CIDS itself or the router it is installed in to use NTP time synchronization. For more information, see Time Sources and the Sensor, page 1-19.

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:

Understanding Time on the Sensor

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. For more information, see Initializing the Sensor, page 10-2.

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.

    For the procedure, refer to Manually Setting the Clock.
  - Use NTP

    You can configure the appliance to get its time from an NTP time synchronization source. For the procedure, refer to Configuring a Cisco Router to be an NTP Server. You will 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, 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. IDSM-2's local time could be incorrect if the time zone and/or summertime settings do not match between IDSM-2 and the switch. For more information, see Synchronizing IPS Module System Clocks with Parent Device System Clocks, page 1-21.

- Use NTP

  You can configure IDSM-2 to get its time from an NTP time synchronization source. For the procedure, refer to Configuring a Cisco Router to be an NTP Server. You will 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, or ASDM.

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

- For NM-CIDS
  - NM-CIDS can automatically synchronize its clock with the clock in the router chassis in which it is installed (parent router). This is the default.

    Note The UTC time is synchronized between the parent router and NM-CIDS. The time zone and summertime settings are not synchronized between the parent router and NM-CIDS.

Caution Be sure to set the time zone and summertime settings on both the parent router and NM-CIDS to ensure that the UTC time settings are correct. NM-CIDS's local time could be incorrect if the time zone and/or summertime settings do not match between NM-CIDS and the router. For more information, see Synchronizing IPS Module System Clocks with Parent Device System Clocks, page 1-21.

  - Use NTP

    You can configure NM-CIDS to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router. For the procedure, refer to Configuring a Cisco Router to be an NTP Server. You will need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure NM-CIDS to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

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

- For AIP-SSM:
  - AIP-SSM can automatically synchronize its clock with the clock in the ASA in which it is installed. This is the default.

    Note The UTC time is synchronized between ASA and AIP-SSM. The time zone and summertime settings are not synchronized between ASA and AIP-SSM.

Caution Be sure to set the time zone and summertime settings on both ASA and AIP-SSM to ensure that the UTC time settings are correct. AIP-SSM's local time could be incorrect if the time zone and/or summertime settings do not match between AIP-SSM and ASA. For more information, see Synchronizing IPS Module System Clocks with Parent Device System Clocks, page 1-21.

– 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. For the procedure, refer to Configuring a Cisco Router to be an NTP Server. You will 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, or ASDM.

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

Synchronizing IPS Module System Clocks with Parent Device System Clocks

All IPS modules (IDSM-2, NM-CIDS, and AIP-SSM) synchronize their system clocks to the parent chassis clock (switch, router, or firewall) 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. For more information on NTP, refer to Configuring NTP.

Verifying the Sensor is Synchronized with the NTP Server

In IPS 5.1, 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. For more information on the **clear events** command, refer to Clearing Events from the Event Store.

Caution You cannot remove individual events.

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* that shipped with your sensor.

Step 2 To familiarize yourself with the IPS and related documentation and where to find it on Cisco.com, read the *Documentation Roadmap for Cisco Intrusion Prevention System 5.1* that shipped with your sensor.

Step 3 Obtain the *Release Notes for Cisco Intrusion Prevention System 5.1* from Cisco.com and completely read them before proceeding with the installation.

Step 4 Unpack the sensor.

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

For more information, see Site and Safety Guidelines, page 1-23.

Step 6 Place the sensor on a stable work surface.

Step 7 Refer to the chapter that pertains to your sensor model.

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

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.

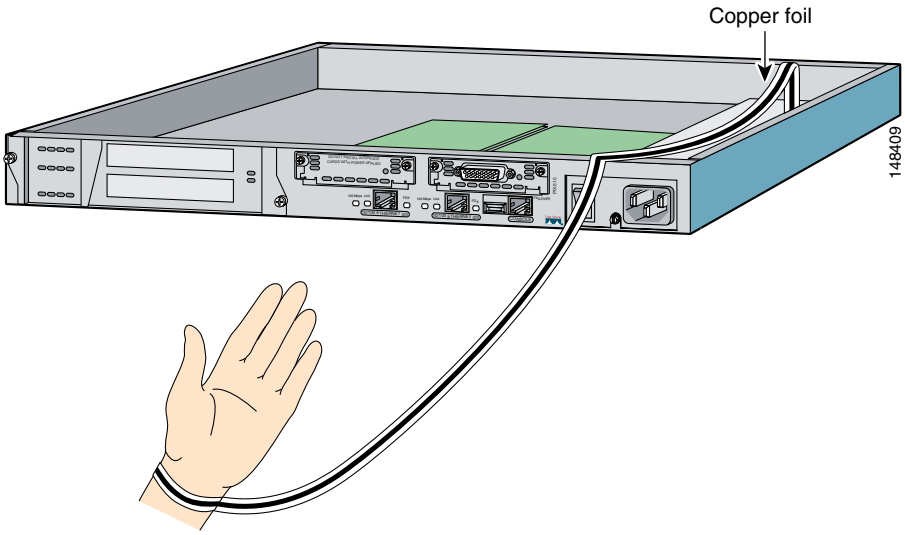
To remove and replace components in a sensor, follow these steps:

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. This section contains the following topics:

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, IPS-4255, and IPS-4260). 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 1-5 shows the 10/100BaseT (RJ-45) port pinouts.

Figure 1-5 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	

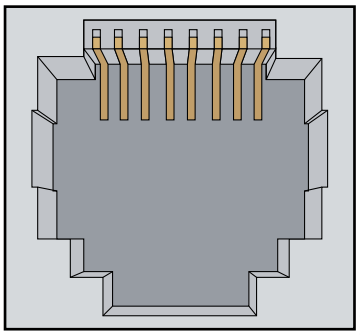
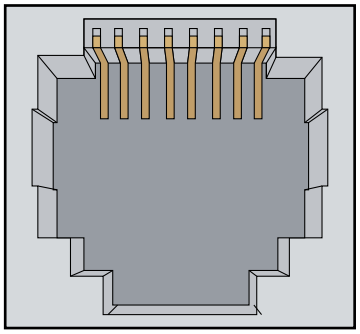


Figure 1-6 shows the 10/100/1000BaseT (RJ-45) port pinouts.

Figure 1-6 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-	



Console Port (RJ-45)

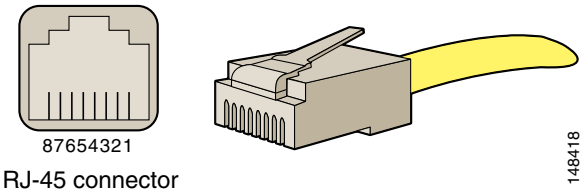
Cisco products use the following types of RJ-45 cables:

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

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

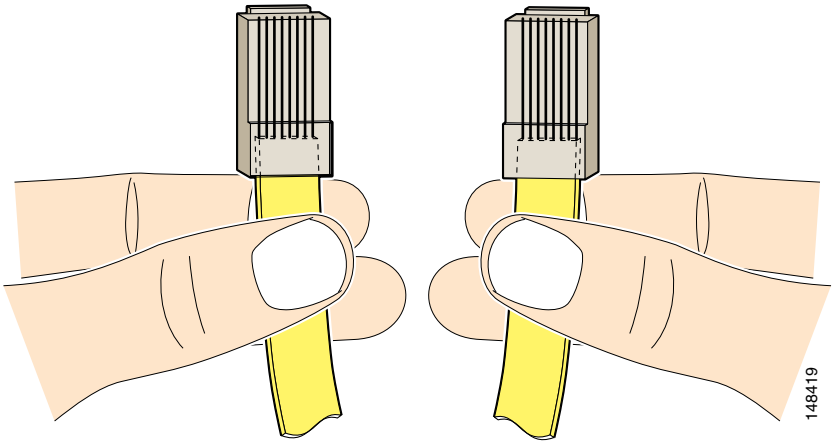
Figure 1-7 shows the RJ 45 cable.

Figure 1-7 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 1-8.

Figure 1-8 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
GND	4	5
RxD	3	3
DSR	2	4
CTS	1	7

CHAPTER 2

Installing IDS-4210

This chapter describes IDS-4210 and how to install it and its accessories.

Note IDS-4215 replaced IDS-4210, which is no longer sold.

Note If you purchased an IDS-4210 before July 2003, you must upgrade the memory to 512 MB to install Cisco IPS 5.x. for more information, see Upgrading the Memory, page 2-3.

Note IDS-4210 does not support inline (IPS) mode.

Caution The BIOS on IDS-4210 is specific to IDS-4210 and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on IDS-4210 voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Obtaining Cisco IPS Software, page 11-1.

This chapter contains the following sections:

Front and Back Panel Features and Indicators

Figure 2-1 shows the front panel indicators on IDS-4210.

Figure 2-1 Front Panel Features

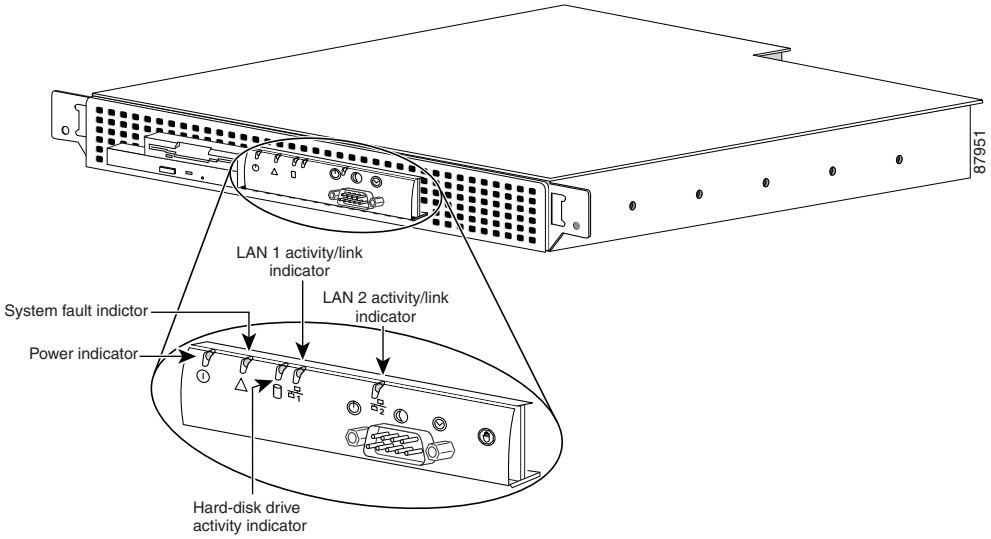


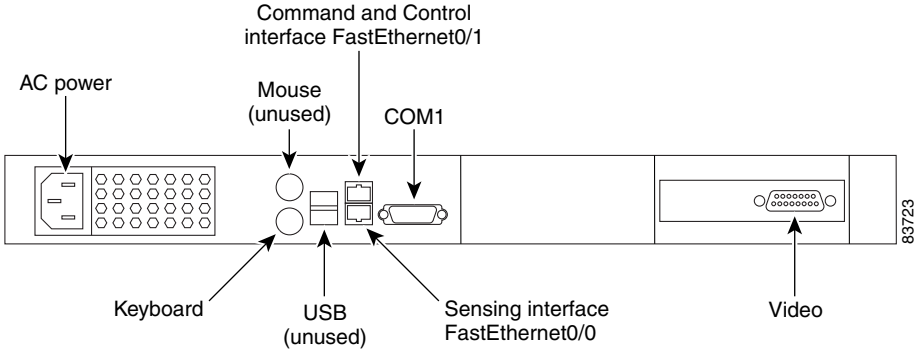
Table 2-1 describes the appearance and function of the front panel indicators.

Table 2-1 Front Panel Indicators

Indicator	Color	Function
Power	Green	Lights up when the system is connected to an AC power source; blinks when the system is in sleep mode.
System fault	Amber	Blinks during system startup or when a system fault is detected.
Hard-disk drive activity	Green	Blinks when hard-disk drive activity occurs.
LAN1 activity/link	Amber	Lights up when the LAN1 connector is linked to an Ethernet port; blinks when activity occurs on this channel.
LAN2 activity/link	Amber	Lights up when the LAN2 connector is linked to an Ethernet port; blinks when activity occurs on this channel.

Figure 2-2 shows the back panel features on IDS-4210.

Figure 2-2 Back Panel Features



Upgrading the Memory

IDS-4210, IDS-4210-K9, and IDS-4210-NFR must have 512 MB of RAM to support Cisco IPS 5.1. If you are upgrading an existing IDS-4210, IDS-4210-K9, or IDS-4210-NFR to 5.1, you must insert one additional 256-MB DIMM (part number IDS-4210-MEM-U) to upgrade the memory to the required 512 MB minimum.

Note Do not install an unsupported DIMM. Doing so nullifies the warranty.

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

To upgrade the memory, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare the appliance to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down the sensor from IDM or ASDM.

Step 3 Power off the appliance.

Step 4 Remove the power cord and other cables from the appliance.

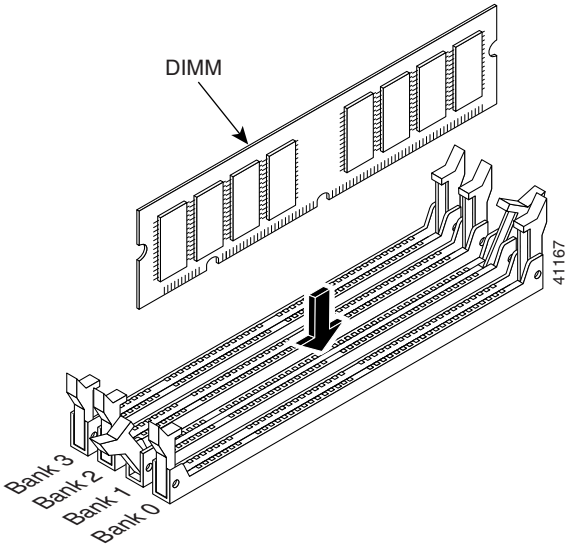
Step 5 Place the appliance in an ESD-controlled environment.

For more information, see Working in an ESD Environment, page 1-25.

Step 6 Remove the chassis cover by unscrewing the screw on the front of the cover and sliding the cover straight back.

Step 7 Locate the DIMM sockets and select the empty DIMM socket next to the existing DIMM.

Note The existing DIMM is installed in socket 0. The angled position of the DIMM sockets make installing an additional DIMM in socket 1 difficult if a DIMM occupies socket 0. Therefore, you should first remove the existing DIMM from socket 0, place the new DIMM in socket 1, and then replace the existing DIMM in socket 0.



Step 8 Locate the ejector tabs on either side of the DIMM socket. Press down and out on tabs to open the slot in the socket.

Step 9 Install the new DIMM, by positioning the DIMM into the socket and pressing it into place.

Note Do not force the DIMM into the socket. Alignment keys on the DIMM ensure that it only fits in the socket one way. If you need additional leverage, you can gently press down on the DIMM with your thumbs while pulling up on the ejector tabs.

Step 10 Replace the chassis cover and reconnect the power.

Step 11 Power on the sensor and make sure the new memory total is correct.

Note If the memory total does not reflect the added DIMMs, repeat Steps 1 through 4 to ensure the DIMMs are seated correctly in the socket.

Installing IDS-4210

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

Note If you purchased an IDS-4210 before July 2003, you must upgrade the memory to 512 MB to install Cisco IPS 5.x. For more information, see Upgrading the Memory, page 2-3.

To install IDS-4210 on the network, follow these steps:

Step 1 Position IDS-4210 on the network.

Step 2 Attach the power cord to IDS-4210 and plug it in to a power source (a UPS is recommended).

Note When you first plug an IDS-4210 into a power source, it powers on momentarily and then powers off leaving the NIC link lights lit. This is normal behavior. Press the power switch to boot the system into operation.

Step 3 Use the dual serial communication cable (PN 72-1847-01, included in the accessory kit) to attach a laptop to the COM1 port of IDS-4210 (see Table 2-2 for a list of the terminal settings), or connect a keyboard and monitor to IDS-4210.

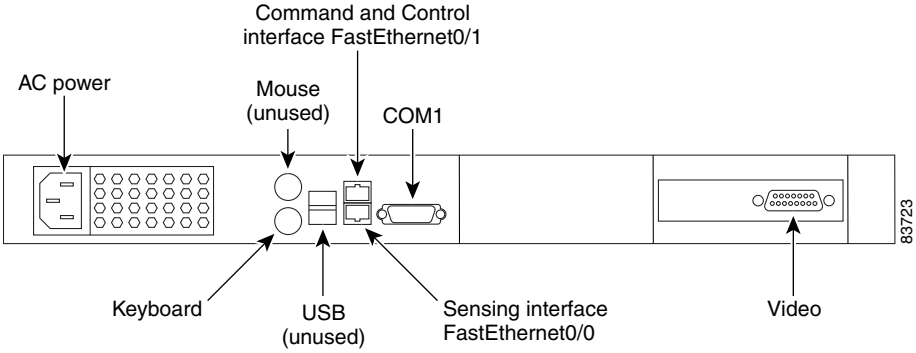
Table 2-2 Terminal Settings

Terminal	Setting
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware or RTS/CTS

Caution We recommend that you use the dual serial communication cable (PN 72-1847-01, included in the accessory kit) rather than a keyboard and monitor, because some keyboards and monitors may be incompatible with IDS-4210.

Note You can use a 180 rollover or straight-through patch cable to connect IDS-4210 to a port on a terminal server with RJ-45 or hydra cable assembly connections. Use a M.A.S.H adapter (part number 29-4077-02) to connect the appropriate cable to a port on the terminal server. For the instructions for setting up a terminal server, see Setting Up a Terminal Server, page 1-14.

Step 4 Attach the network cables.



IDS-4210 has the following interfaces:

- FastEthernet0/0 is the sensing port.
- FastEthernet0/1 is the command and control port.

Caution Management and console ports are privileged administrative ports. Connecting them to an untrusted network can create security concerns.

Step 5 Upgrade the memory on IDS-4210.

For the procedure, see Upgrading the Memory, page 2-3.

Caution You must upgrade the memory on IDS-4210 to a minimum of 512 MB before you can install the most recent Cisco IPS software.

Step 6 Power on IDS-4210.

Step 7 Initialize IDS-4210.

For the procedure, see Initializing the Sensor, page 10-2.

Step 8 Upgrade IDS-4210 to the latest Cisco IPS software.

For the procedure, see Obtaining Cisco IPS Software, page 11-1.

You are now ready to configure intrusion detection on the appliance.

For More Information

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

Installing the Accessories

You can install a bezel, and center or front mounting brackets for the IDS-4210.

This section contains the following topics:

Accessories Package Contents

The following items are shipped in the accessories package for IDS-4210:

- Cisco IDS-4210 bezel
- Power cable
- Network patch cable
- Computer interconnection cable
- Dual serial communication cable
- Rack mounting brackets
- Documentation and software
  - Cisco IDS recovery/upgrade CD
  - Cisco Documentation CD
  - *Documentation Roadmap for Cisco Intrusion Prevention System 5.1*
  - *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*

Installing and Removing the Bezel

You can install a Cisco bezel for IDS-4210.

To install and remove the bezel on IDS-4210, follow these steps:

Step 1 To insert the bezel on IDS-4210, follow these steps:

a. Align the bottom tabs on the bezel with the slots on IDS-4210.

b. Align the side tabs on the bezel with the slots on IDS-4210.

c. Press the bezel into IDS-4210.

Step 2 To remove the bezel from IDS-4210, press the side tabs and pull.

Installing Center Mount Brackets

You need the following tools and supplies to install the brackets in a two-post, open-frame relay rack:

- #2 Phillips screwdriver
- Masking tape or felt-tip pen to mark the mounting holes to be used

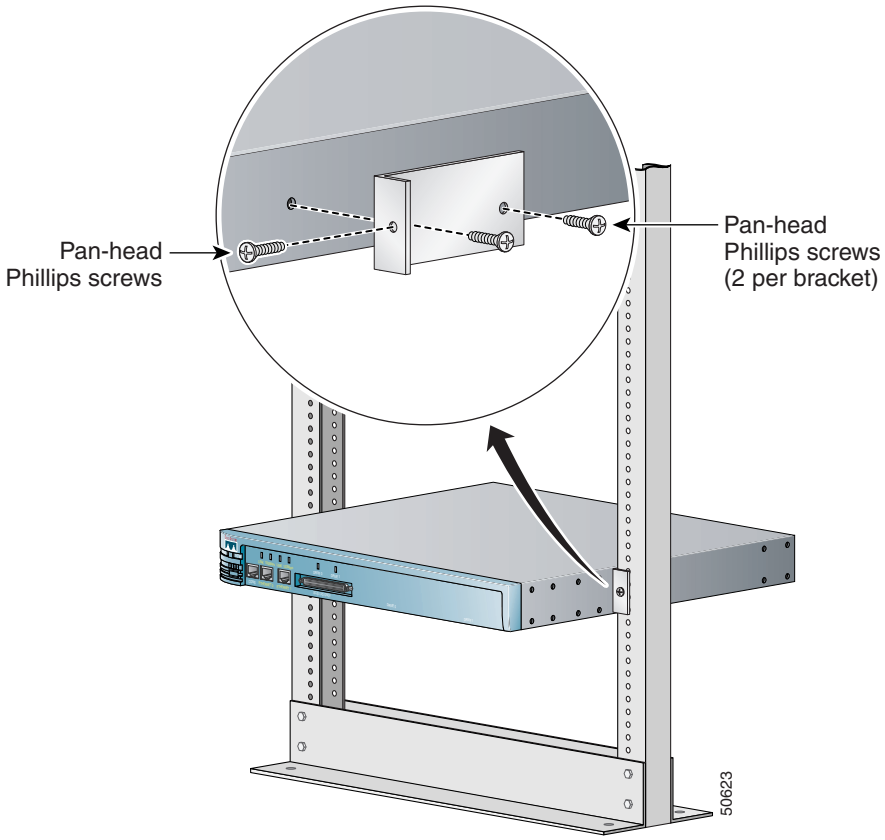
To install the center mount brackets in a two-post, open-frame relay rack, follow these steps:

Step 1 Determine where you want to place IDS-4210.

Step 2 Mark the upper and lower mounting positions on the two posts.

Step 3 Locate one of the two brackets and align it over the two threaded holes on the side of IDS-4210 (see Figure 2-3).

Figure 2-3 Installing Center Mount Brackets



Step 4 Secure the bracket to IDS-4210 chassis using two screws (see Figure 2-3 on page 2-9).

Step 5 Repeat Step 4 to install the remaining bracket on the other side of IDS-4210.

Step 6 Lift IDS-4210 into position between the two posts with the hole in the mounting bracket aligned one hole above the mark you made in the two posts (see Figure 2-3 on page 2-9).

Step 7 Secure IDS-4210 to the rack using a screw through the mounting bracket to the front of the left and right posts (see Figure 2-3 on page 2-9).

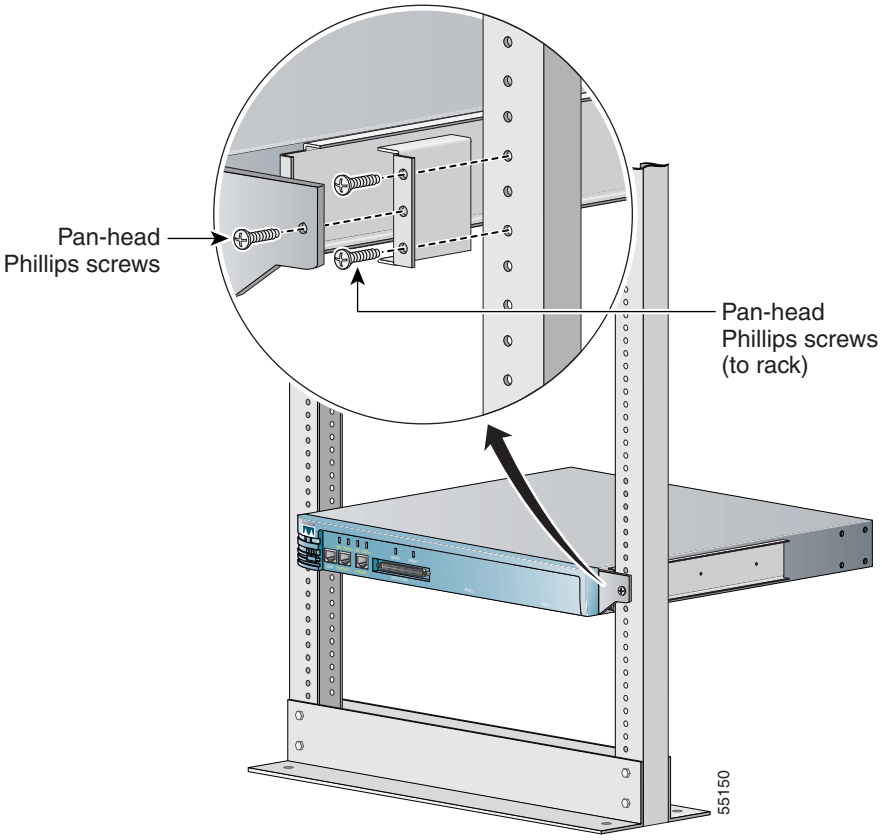
Installing Front Mount Brackets

Make sure you have the following supplies (found in the front mount bracket assembly kit) and tools to install the front mount brackets in a two-post, open-frame relay rack:

- Two chassis support brackets
- Two rack-mounting brackets
- Six screws
- #2 Phillips screwdriver

Note The front mount bracket assembly is not intended for use as a slide rail system. The server must be firmly attached to the rack, as shown in Figure 2-4.

Figure 2-4 Front Mount Brackets



Caution The chassis support brackets included in this kit are rated for 50 pounds of load per pair of brackets for general use for 10,000 cycles of opening and closing. Higher cycles or frequency will lower the load rating. The chassis support brackets are meant to support the weight of only one IDS-4210.

To install the front mount brackets, follow these steps:

Step 1 Make sure IDS-4210 is turned off and is not plugged in to an electrical outlet.

Step 2 Use the screws provided to attach one chassis support bracket to each side of IDS-4210. Use three screws on each side.

Step 3 Use the screws provided with the rack to attach the rack mounting brackets to the rack.

Step 4 Slide the chassis support brackets on IDS-4210 into the rack mounting brackets attached to the rack.

Step 5 Use the bolts provided with the rack to fasten the front flanges of IDS-4210 to the rack.

Note When you are done, IDS-4210 should not slide on the channel bar.

CHAPTER 3

Installing IDS-4215

This chapter describes IDS-4215 and how to install it. It also describes the accessories and how to install them. This chapter contains the following sections:

Warning **Port numbering for onboard interfaces was reversed from IDS 4.x to IPS 5.0 and later. The port naming convention changed within the IPS application only; the physical chassis label remains unchanged. To correlate chassis port labels to software port names, refer to Figure 3-2 on page 3-2.**

Introducing IDS-4215

IDS-4215 can monitor up to 80 Mbps of aggregate traffic and is suitable for T1/E1 and T3 environments. With the addition of the four-port fast Ethernet (4FE) card, IDS-4215 supports five sensing interfaces (10/100BASE-TX), which provide simultaneous protection for multiple subnets.

Note The 80-Mbps performance for IDS-4215 is based on the following conditions: aggregation of traffic from all five sensing interfaces, 800 new TCP connections per second, 800 HTTP transactions per second, average packet size of 445 bytes, and system running Cisco IPS 5.1 software.

The sensing interfaces and the command and control interface are all 10/100BASE-TX.

Front and Back Panel Features

This section describes the IDS-4215 front and back panel features and indicators.

Figure 3-1 shows the front view of IDS-4215.

Figure 3-1 IDS-4215 Front Panel Features

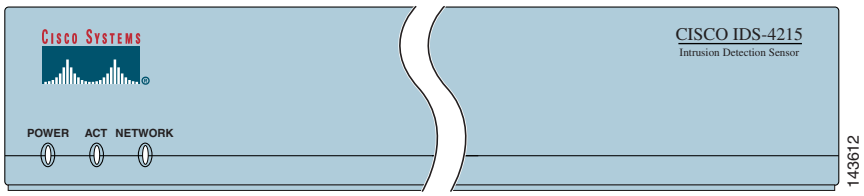


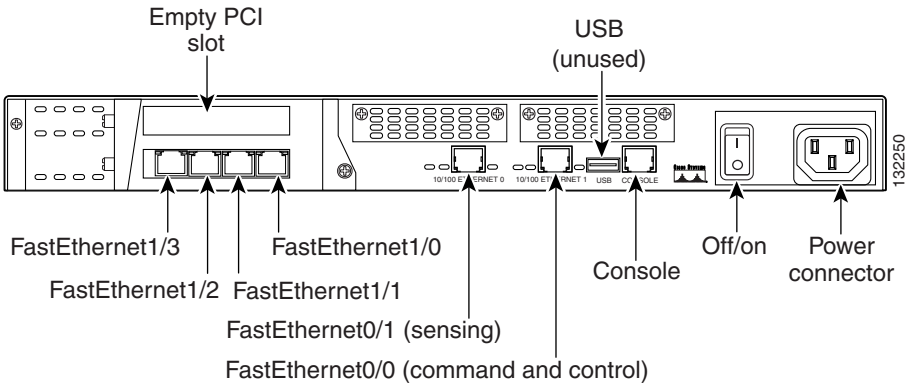
Table 3-1 describes the front panel indicators on IDS-4215.

Table 3-1 Front Panel Indicators

Indicator	Description
POWER	Lights up when power supply is running.
ACT	Lights up when IDS-4215 has completed power-up self-test and has started the operating system and application software loading process.
NETWORK	Blinks when network traffic is passing over either of the two built-in Ethernet ports; does not indicate traffic on any of the four ports of the 4FE card.

Figure 3-2 shows the back view of IDS-4215.

Figure 3-2 IDS-4215 Back Panel Features



Warning **Port numbering for onboard interfaces was reversed from IDS 4.x to IPS 5.0 and later. The port naming convention changed within the IPS application only; the physical chassis label remains unchanged. To correlate chassis port labels to software port names, refer to Figure 3-2.**

The built-in Ethernet ports have three indicators per port and the 4FE card has two indicators per port. Figure 3-3 shows the back panel indicators.

Figure 3-3 IDS-4215

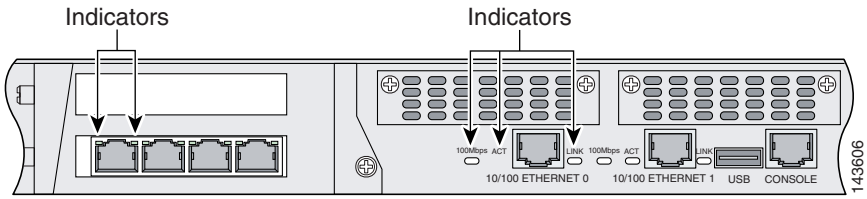


Table 3-2 lists the back panel indicators.

Table 3-2 Back Panel Indicators

Indicator	Description
Built-in Ethernet	—
100 Mbps	Lights up when the port is running in 100-Mbps mode; off when it is running in 10-Mbps mode.
Link	Lights up when the port is connected to another Ethernet port and traffic can be passed between them.
ACT	Blinks when network traffic is being received on the port.
4FE Card	—
LINK/activity	Lights up when the port is connected to another operational Ethernet port but no traffic is being passed between them; blinks off when Ethernet packets are being received.
100 Mbps	Lights up when the port is running in 100-Mbps mode; off when the port is running in 10-Mbps mode.

Specifications

Table 3-3 lists the specifications for IDS-4215.

Table 3-3 IDS-4215 Specifications

Dimensions and Weight	
Height	1.72 in. (4.37 cm)
Width	16.8 in. (42.72 cm)
Depth	11.8 in. (29.97 cm)
Weight	11.5 lb (4.11 kg)
Form factor	1 RU, standard 19-inch rack-mountable
Expansion	Two 32-bit/33-MHz PCI slots
Power	
Autoswitching	100V to 240V AC

Table 3-3 IDS-4215 Specifications (continued)

Frequency	50 to 60 Hz, single phase
Operating current	1.5 A
Steady state	50W
Maximum peak	65W
Maximum heat dissipation	410 BTU/hr, full power usage (65W)
Environment	
Temperature	Operating +41°F to +104°F (+5°C to +40°C) Nonoperating -13°F to +158°F (-25°C to +70°C)
Relative humidity	Operating 5% to 95% (noncondensing) Nonoperating 5% to 95% (noncondensing)
Altitude	Operating 0 to 9843 ft (3000 m) Nonoperating 0 to 15,000 ft (4750 m)
Shock	Operating 1.14 m/sec (45 in./sec) 1/2 sine input Nonoperating 30 G
Vibration	0.41 Grms2 (3-500 Hz) random input
Acoustic noise	54 dBa maximum

Note Only one PCI expansion slot can be used for the 4FE card. We recommend you install the 4FE card in the lower PCI expansion slot.

Accessories

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

IDS-4215 accessories kit contains the following:

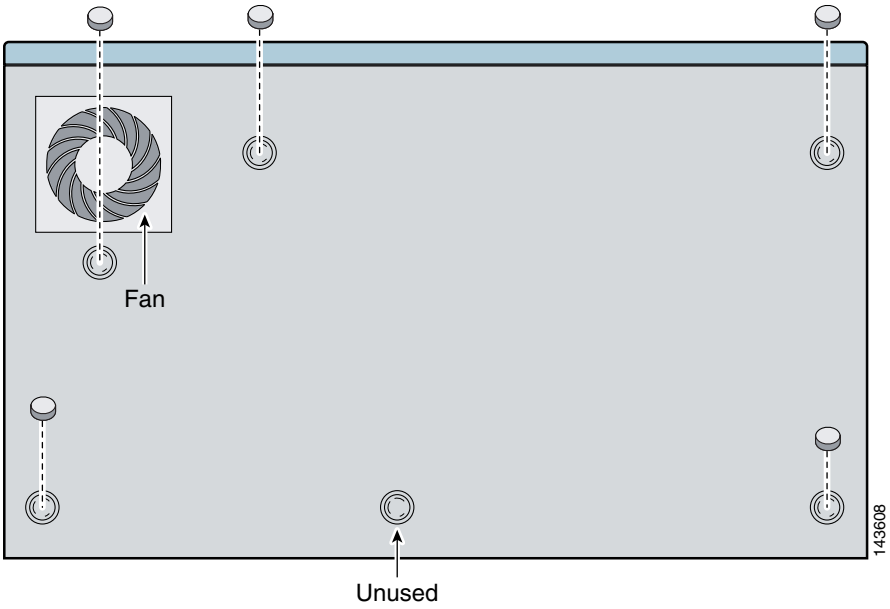
- DB25F/RJ45F adaptor
- DB9F/RJ45F adaptor
- Rubber mounting feet

- Rack mounting kit—screws, washers, and metal bracket
- RJ45 console cable
- 6-ft Ethernet cable

Surface Mounting

If you are not rack mounting IDS-4215, you must attach the rubber feet to the bottom of IDS-4215 as shown in Figure 3-4. The rubber feet are shipped in the accessories kit.

Figure 3-4 Surface Mounting IDS-4215



Caution For proper cooling and reliability, the rubber feet must be installed on IDS-4215 when it is on a flat surface and not mounted in a rack. The rubber feet allow proper airflow around IDS-4215 and they also absorb vibration so that the hard-disk drive is less impacted.

Rack Mounting

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety: This unit should be mounted at the bottom of the rack if it is the only unit in the rack. When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack. If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.**

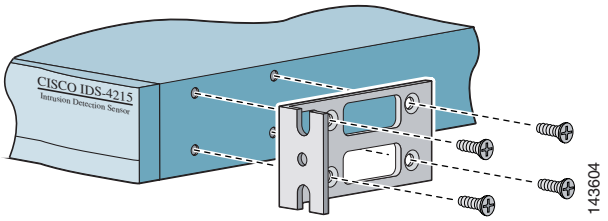
If you are installing the 4FE card in IDS-4215, do not install the mounting brackets until after you have installed the 4FE card.

Note You must remove the chassis cover of IDS-4215 to properly install or remove the 4FE card. For information on how to remove and replace the chassis cover, see Removing and Replacing the Chassis Cover, page 3-11. For information on installing the 4FE card in IDS-4215, see Installing the 4FE Card, page 3-22.

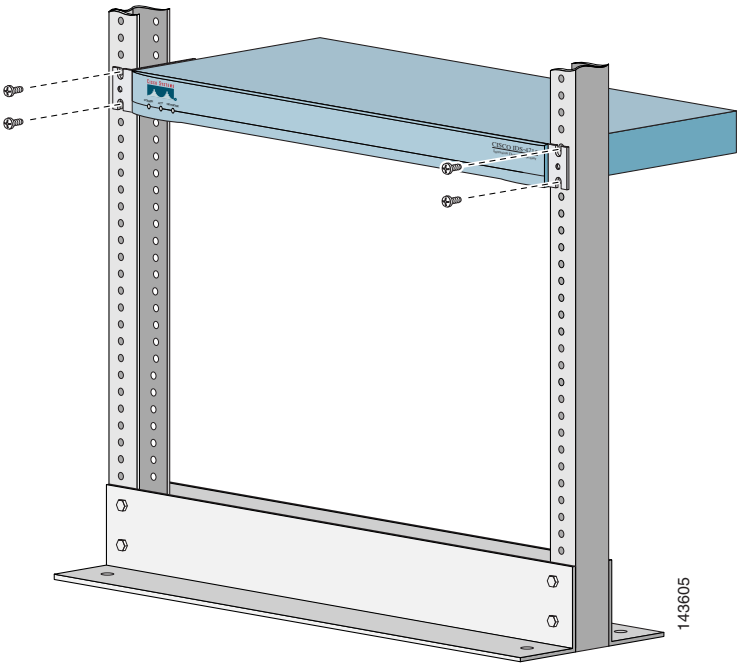
To rack mount IDS-4215, follow these steps:

Step 1 Use the supplied screws to attach the bracket to IDS-4215.

You can attach the brackets to the holes near the front of IDS-4215.



Step 2 Attach IDS-4215 to the equipment rack



Installing IDS-4215

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

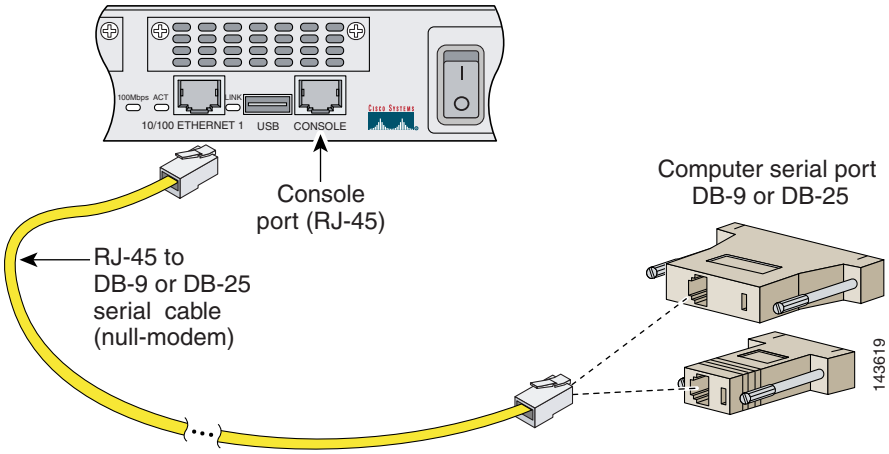
Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

To install IDS-4215 on the network, follow these steps:

Step 1 Position IDS-4215 on the network.

Step 2 Attach the power cord to IDS-4215 and plug it into a power source (a UPS is recommended).

Step 3 Connect the cable so that you have either a DB-9 or DB-25 connector on one end as required by the serial port for your computer, and the other end is the RJ-45 connector.

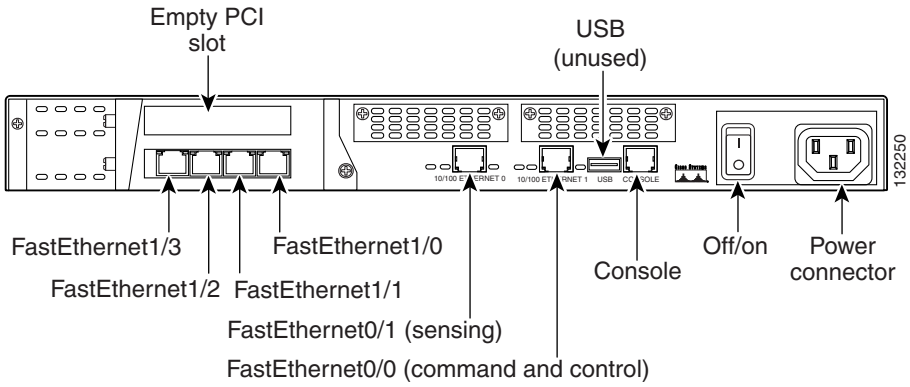


Note Use the console port to connect to a computer to enter configuration commands. Locate the serial cable from the accessory kit. The serial cable assembly consists of a 180/rollover cable with RJ-45 connectors (DB-9 connector adapter PN 74-0495-01 and DB-25 connector adapter PN 29-0810-01).

Note You can use a 180/rollover or straight-through patch cable to connect IDS-4215 to a port on a terminal server with RJ-45 or hydra cable assembly connections. Connect the appropriate cable from the console port on IDS-4215 to a port on the terminal server. For the instructions for setting up a terminal server, see Setting Up a Terminal Server, page 1-14.

Step 4 Connect the RJ-45 connector to the console port and connect the other end to the serial port connector on your computer.

Step 5 Attach the network cables.



Warning **Port numbering for onboard interfaces was reversed from IDS 4.x to IPS 5.0 and later. The port naming convention changed within the IPS application only; the physical chassis label remains unchanged. To correlate chassis port labels to software port names, refer to the figure above.**

IDS-4215 has the following interfaces:

- FastEthernet0/0 is the command and control port.
- FastEthernet0/1 is the sensing port.
- FastEthernet1/0, FastEthernet1/1, FastEthernet1/2, and FastEthernet1/3 are the optional sensing ports available if you have the 4FE card installed.

Caution Management and console ports are privileged administrative ports. Connecting them to an untrusted network can create security concerns.

Step 6 Power on IDS-4215.

Make sure the BIOS version is 5.1.7 and the ROMMON version is 1.4 before upgrading IDS-4215 to 5.x. For the procedure, see Upgrading the BIOS and ROMMON, page 3-9.

Note The BIOS/ROMMON upgrade is necessary to install the 4.1(4) system image, but not the 5.0(2) system image. The 5.0(2) system image is smaller than the size limitation that applied to earlier versions of ROMMON, while the 4.1(4) system image was larger.

Step 7 Initialize IDS-4215.

For the procedure, see Initializing the Sensor, page 10-2.

Step 8 Upgrade IDS-4215 to the most recent Cisco IPS software.

For the procedure, see Obtaining Cisco IPS Software, page 11-1.

You are now ready to configure intrusion prevention on IDS-4215.

For More Information

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

Upgrading the BIOS and ROMMON

Some TFTP servers limit the maximum file size that can be transferred to ~32 MB. Therefore, we recommend the following TFTP servers:

- For Windows:

  Tftpd32 version 2.0, available at:

  http://tftpd32.jounin.net/
- For UNIX:

  Tftp-hpa series, available at:

  http://www.kernel.org/pub/software/network/tftp/

The BIOS/ROMMON upgrade utility (IDS-4215-bios-5.1.7-rom-1.4.bin) upgrades the BIOS of IDS-4215 to version 5.1.7 and the ROMMON to version 1.4.

To upgrade the BIOS and ROMMON on IDS-4215, follow these steps:

Step 1 Download the BIOS ROMMON upgrade utility (IDS-4215-bios-5.1.7-rom-1.4.bin) to the TFTP root directory of a TFTP server that is accessible from IDS-4215.

For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of IDS-4215.

Step 2 Boot IDS-4215.

While rebooting, IDS-4215 runs the BIOS POST. After the completion of POST, the console displays the message: `Evaluating Run Options ...` for about 5 seconds.

Step 3 Press **Ctrl-R** while this message is displayed to display the ROMMON menu.

The console display resembles the following:

```
CISCO SYSTEMS IDS-4215
Embedded BIOS Version 5.1.3 05/12/03 10:18:14.84
Compiled by ciscouser
Evaluating Run Options ...
Cisco ROMMON (1.2) #0: Mon May 12 10:21:46 MDT 2003
Platform IDS-4215
0: i8255X @ PCI(bus:0 dev:13 irq:11)
1: i8255X @ PCI(bus:0 dev:14 irq:11)
Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.c0ff.ee01
Use ? for help.
rommon>
```

Step 4 If necessary, change the port number used for the TFTP download:

```
rommon> interface port_number
```

The port in use is listed just before the rommon prompt. Port 1 (default port) is being used as indicated by the text, `Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.c0ff.ee01`.

Note Ports 0 (monitoring port) and 1 (command and control port) are labeled on the back of the chassis.

Step 5 Specify an IP address for the local port on IDS-4215:

```
rommon> address ip_address
```

Note Use the same IP address that is assigned to IDS-4215.

Step 6 Specify the TFTP server IP address:

```
rommon> server ip_address
```

Step 7 Specify the gateway IP address:

```
rommon> gateway ip_address
```

Step 8 Verify that you have access to the TFTP server by pinging it from the local Ethernet port:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 9 Specify the filename on the TFTP file server from which you are downloading the image:

```
rommon> file filename
```

Example:

```
rommon> file IDS-4215-bios-5.1.7-rom-1.4.bin
```

Note The syntax of the file location depends on the type of TFTP server used. Contact your system or network administrator for the appropriate syntax if the above format does not work.

Step 10 Download and run the update utility:

```
rommon> tftp
```

Step 11 Type **y** at the upgrade prompt and the update is executed.

IDS-4215 reboots when the update is complete.

Caution Do not remove power to IDS-4215 during the update process, otherwise the upgrade can get corrupted. If this occurs, IDS-4215 will be unusable and require an RMA.

Removing and Replacing the Chassis Cover

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 120 VAC, 20 A U.S. (240 VAC, 16-20 A International). Statement 1005**

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024**

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Statement 1029**

Warning **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028**

Caution Follow proper safety procedures when removing and replacing the chassis cover by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

This section describes how to remove and replace IDS-4215 chassis cover.

This section contains the following topics:

- Removing the Chassis Cover, page 3-11
- Replacing the Chassis Cover, page 3-13

Removing the Chassis Cover

Note Removing the appliance chassis cover does not affect your Cisco warranty. Upgrading IDS-4215 does not require any special tools and does not create any radio frequency leaks.

To remove the chassis cover, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IDS-4215 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down IDS-4215 using IDM.

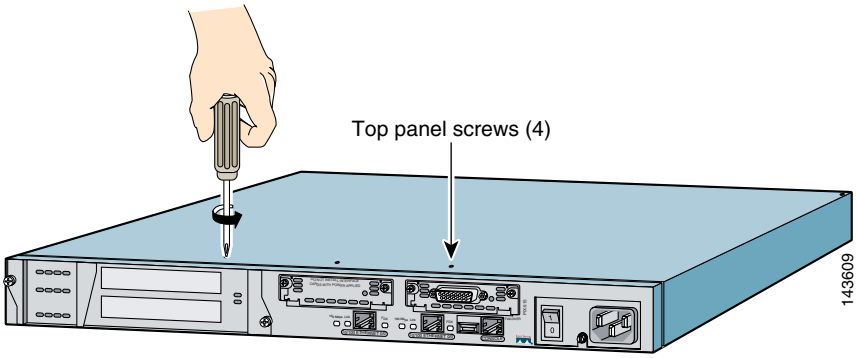
Step 3 Power off IDS-4215.

Step 4 Remove the power cord and other cables from IDS-4215.

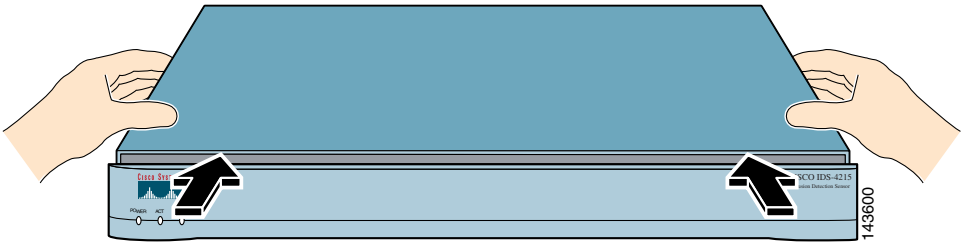
Step 5 Place IDS-4215 in an ESD-controlled environment.

For more information, see Working in an ESD Environment, page 1-25.

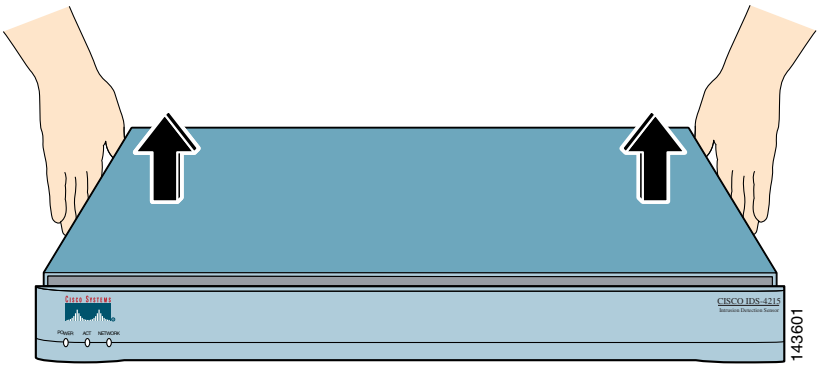
Step 6 Remove the screws from the back of the chassis.



Step 7 With the front of IDS-4215 facing you, push the top panel back one inch.



Step 8 Pull the top panel up and put it in a safe place.



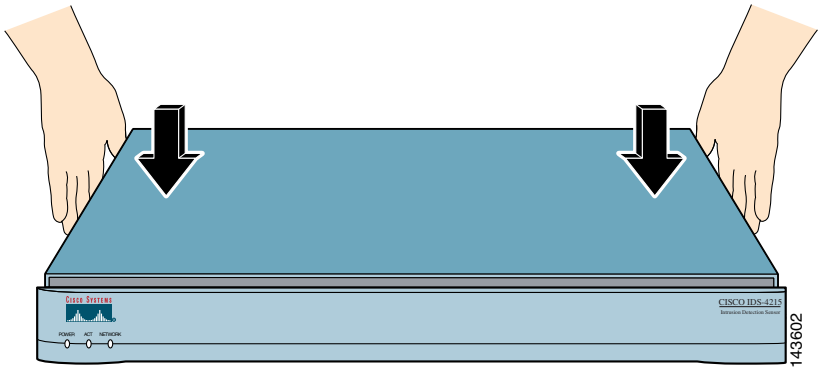
Replacing the Chassis Cover

Caution Do not operate IDS-4215 without the chassis cover installed. The chassis cover protects the internal components, prevents electrical shorts, and provides proper air flow for cooling the electronic components.

To replace the chassis cover, follow these steps:

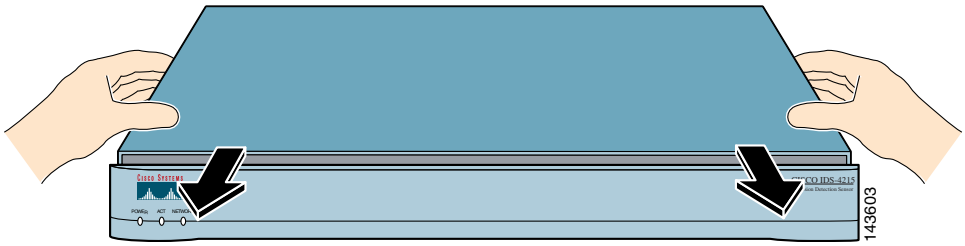
Step 1 Place the chassis on a secure surface with the front panel facing you.

Step 2 Hold the top panel so the tabs at the rear of the top panel are aligned with the chassis bottom.

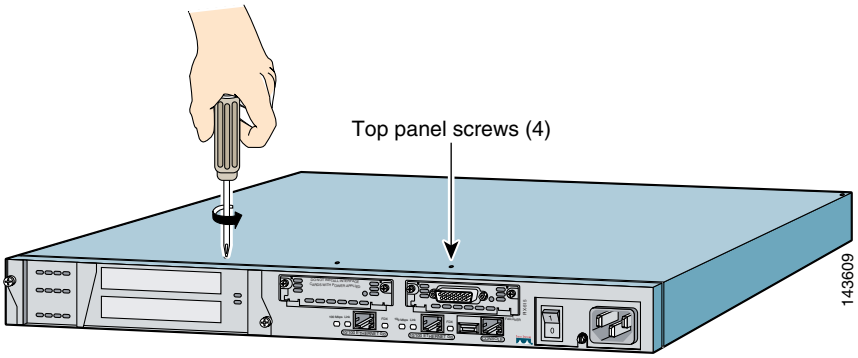


Step 3 Lower the front of the top panel onto the chassis, making sure that the top panel side tabs fit under the chassis side panels.

Step 4 Slide the top panel toward the front, making sure that the top panel tabs fit under the chassis back panel and the back panel tabs fit under the top panel.



Step 5 Fasten the top panel with the screws you set aside earlier.



Step 6 Reinstall the chassis on a rack, desktop, or table.

If you are reinstalling in a rack, see Rack Mounting, page 3-5.

Step 7 Reinstall the network interface cables.

For the procedure, see Installing IDS-4215, page 3-7.

Removing and Replacing the IDE Hard-Disk Drive

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Only use the replacement IDE hard-disk drive from Cisco. We cannot guarantee that other hard-disk drives will operate properly with the IPS.

Caution Follow proper safety procedures when removing and replacing the hard-disk drive by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

This section describes how to remove and replace the IDE hard-disk drive. It contains the following topics:

- Removing the Hard-Disk Drive, page 3-15
- Replacing the Hard-Disk Drive, page 3-16

Removing the Hard-Disk Drive

To remove the hard-disk drive from IDS-4215, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IDS-4215 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down IDS-4215 using IDM.

Step 3 Power off IDS-4215.

Step 4 Remove the power cord and other cables from IDS-4215.

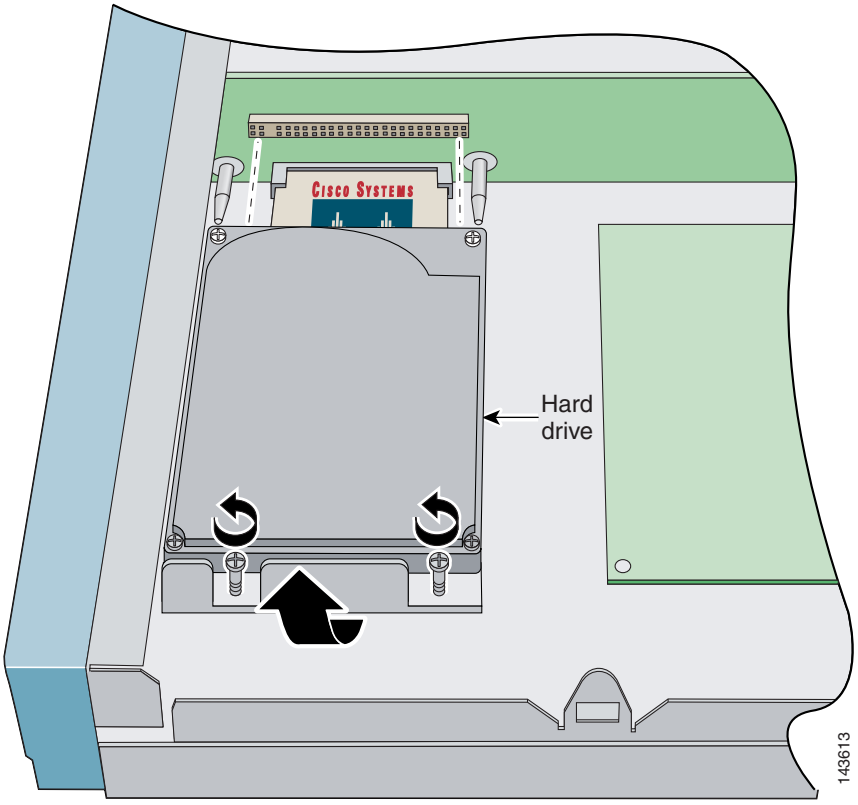
Step 5 Place IDS-4215 in an ESD-controlled environment.

For more information, see Working in an ESD Environment, page 1-25.

Step 6 Remove the chassis cover.

For the procedure, see Removing the Chassis Cover, page 3-11.

Step 7 Loosen the two captive screws from the hard-disk drive carrier.



Step 8 Grasp the hard-disk drive and pull straight backwards until it is free of the riser card connector. Do not lift or wiggle the hard-disk drive side to side until it is completely free of the connector.

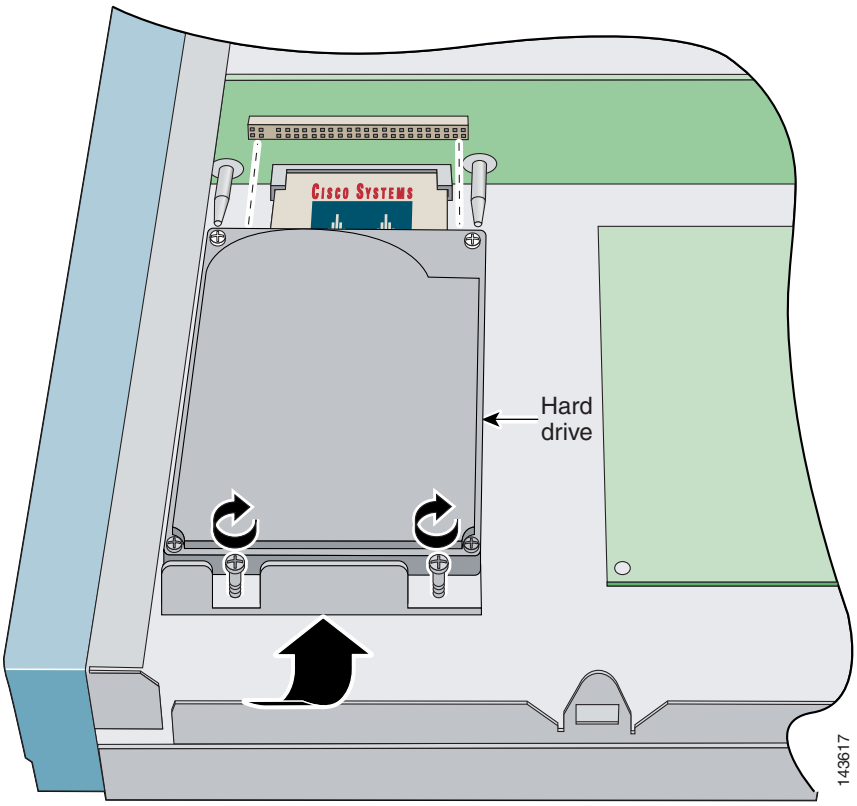
Replacing the Hard-Disk Drive

To replace the hard-disk drive in IDS-4215, follow these steps:

Step 1 Place IDS-4215 in an ESD-controlled environment.

For more information, see Working in an ESD Environment, page 1-25.

Step 2 Align the hard-disk drive connector with the two guide pins on the riser card.



Step 3 Push the hard-disk drive straight into the riser card connector. Do not lift or wiggle the hard-disk drive side to side. Push carefully until the hard-disk drive is seated.

Step 4 Tighten the two captive screws.

Step 5 Replace the chassis cover.

For the procedure, see Replacing the Chassis Cover, page 3-13.

Removing and Replacing the Compact Flash Device

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Follow proper safety procedures when removing and replacing the compact flash by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

This section describes how to remove and replace the compact flash device in IDS-4215, and contains the following topics:

- Removing the Compact Flash Device, page 3-17
- Replacing the Compact Flash Device, page 3-18

Removing the Compact Flash Device

To remove the compact flash device from IDS-4215, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IDS-4215 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down IDS-4215 using IDM.

Step 3 Power off IDS-4215.

Step 4 Remove the power cord and other cables from IDS-4215.

Step 5 Place IDS-4215 in an ESD-controlled environment.

For more information, see Working in an ESD Environment, page 1-25.

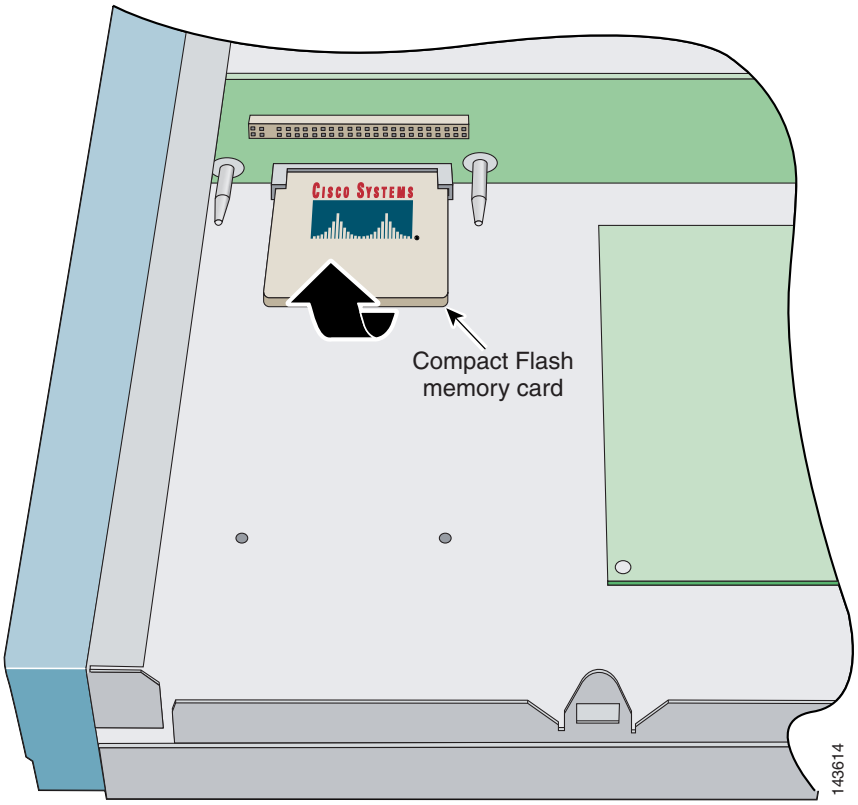
Step 6 Remove the chassis cover.

For the procedure, see Removing the Chassis Cover, page 3-11.

Step 7 Remove the hard-disk drive.

For the procedure, see Removing the Hard-Disk Drive, page 3-15.

Step 8 Grasp the compact flash device and carefully remove it from the connector on the riser card.



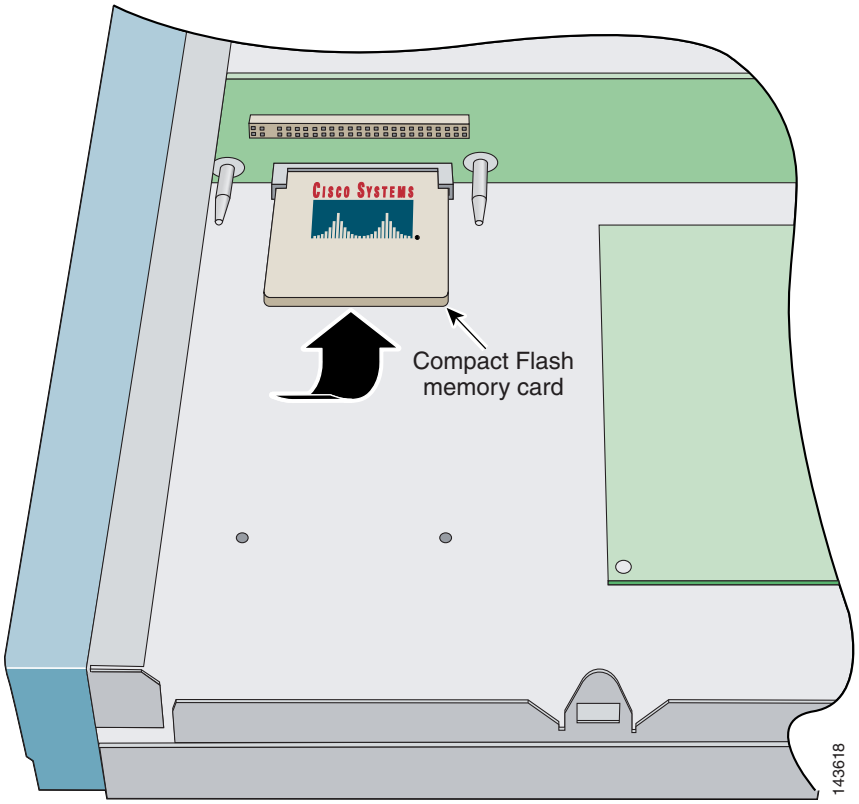
Replacing the Compact Flash Device

To replace the compact flash device in IDS-4215, follow these steps:

Step 1 Place IDS-4215 in an ESD-controlled environment.

For more information, see Working in an ESD Environment, page 1-25.

Step 2 Align the compact flash device with the connector on the riser card.



Step 3 Press until the compact flash device is fully seated in the connector.

Step 4 Replace the hard-disk drive.

For the procedure, see Replacing the Hard-Disk Drive, page 3-16.

Step 5 Replace the chassis cover.

For the procedure, see Replacing the Chassis Cover, page 3-13.

Removing and Installing the 4FE Card

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Follow proper safety procedures when installing and removing the 4FE card by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

You can order IDS-4215 with the 4FE card already installed or you can upgrade IDS-4215 with the 4FE card to have four additional interfaces.

This section contains the following topics:

Removing the 4FE Card

To remove the 4FE card, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IDS-4215 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down IDS-4215 using IDM.

Step 3 Power off IDS-4215.

Step 4 Remove the power cord and other cables from IDS-4215.

Step 5 Place IDS-4215 in an ESD-controlled environment.

For more information, see Working in an ESD Environment, page 1-25.

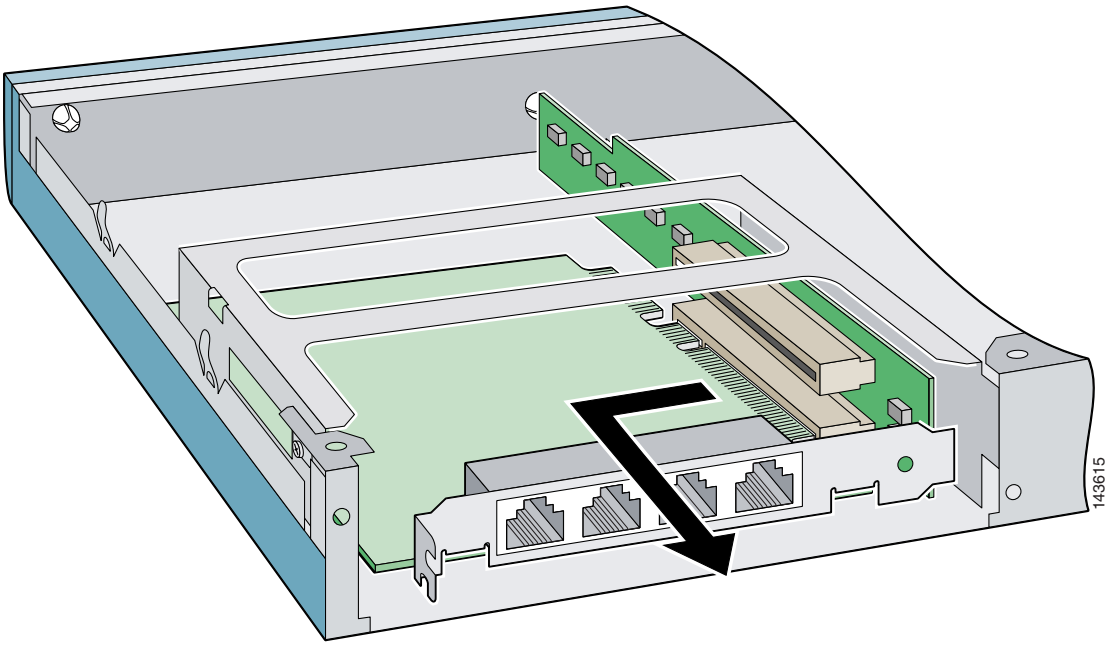
Step 6 Remove the chassis cover.

For the procedure, see Removing the Chassis Cover, page 3-11.

Step 7 Loosen the single captive screw that holds the 4FE card's connecting flange to the back cover plate.

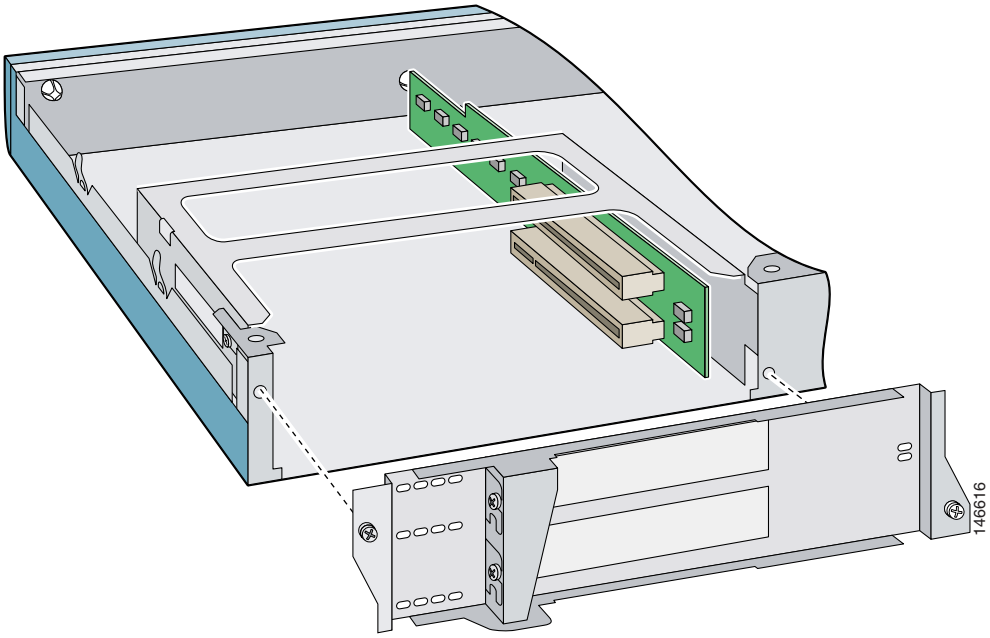
Step 8 Loosen the two captive screws from the back cover on the left and put the back cover aside.

Step 9 Grasp the 4FE card and pull it out of the slot and through the cage opening.



Step 10 Replace the lower slot cover from the back cover plate.

Step 11 Replace the back cover plate and tighten the two captive screws.



Step 12 Replace the chassis cover.

For the procedure, see Replacing the Chassis Cover, page 3-13.

Installing the 4FE Card

We recommend that you install the 4FE card in the bottom slot. We do not support installation of the 4FE card in the top slot.

Note Only one 4FE card is supported on IDS-4215.

To install a 4FE card in IDS-4215, follow these steps:

Step 1 Prepare IDS-4215 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 2.

Step 2 Power off IDS-4215.

Step 3 Remove the power cord and other cables from IDS-4215.

Step 4 Place IDS-4215 in an ESD-controlled environment.

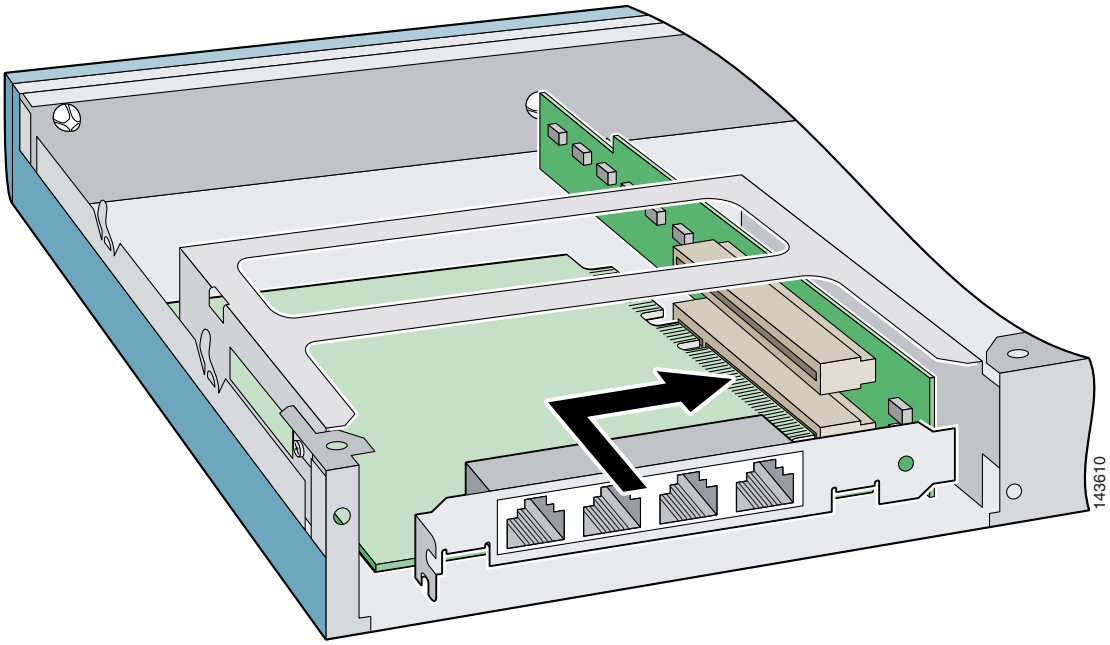
For more information, see Working in an ESD Environment, page 1-25.

Step 5 Remove the chassis cover.

For the procedure, see Removing the Chassis Cover, page 3-11.

Step 6 Loosen the two captive screws from the back cover plate on the left and put the back cover plate aside.

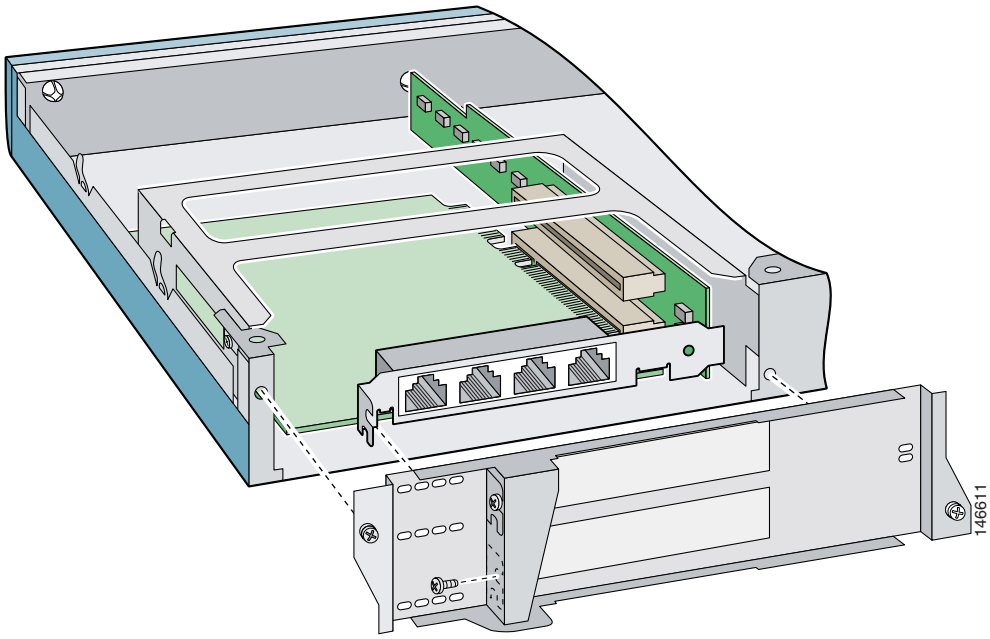
Step 7 Insert the 4FE card through the cage opening and into the lower slot.



Note When you insert a 4FE card in the slot, the end of the card's connector extends past the end of the slot. This does not affect the use or operation of the card.

Step 8 Remove the lower slot cover from the back cover plate.

Step 9 Attach the back cover plate making sure that the connecting flange on the 4FE card goes through the slot on the back cover plate.



Step 10 Tighten the single captive screw to hold the 4FE card's connecting flange to the back cover plate, and tighten the captive screws to attach the back cover plate to the appliance.

Step 11 Replace the chassis cover.

For the procedure, see Replacing the Chassis Cover, page 3-13.

You will need to assign the new interfaces (FastEthernet1/0, FastEthernet1/1, FastEthernet1/2, and FastEthernet1/3). For the CLI procedure, refer to Configuring Interfaces. For the IDM procedure, refer to Configuring Interfaces.

CHAPTER 4

Installing IDS-4235 and IDS-4250

This chapter describes IDS-4235 and IDS-4250 and how to install them. It also describes the accessories and how to install them.

Note IDS-4235 and IDS-4250 are being replaced by IPS-4240 and IPS-4255. They do not ship with IPS 5.1 installed. You must upgrade them to IPS 5.1.

Caution The BIOS on IDS-4235 and IDS-4250 is specific to IDS-4235 and IDS-4250 and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on IDS-4235 and IDS-4250 voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Cisco IPS Software, page 11-1.

This chapter contains the following sections:

Introducing IDS-4235 and IDS-4250

You can deploy IDS-4235 at 250 Mbps to provide protection in switched environments and on multiple T3 subnets. With the support of 10/100/1000 interfaces you can also deploy it on partially utilized gigabit links. The sensing interface and the command and control interface are both 10/100/1000BASE-TX. You can install the 4FE card to provide an additional four sensing interfaces. You can also install the optional 10/100/1000BASE-TX adapter card, which allows additional options for inline functionality beyond the 4FE card. For the procedure for installing optional PCI cards, see Installing Optional PCI Cards, page 4-14.

Note The 250-Mbps performance for IDS-4235 is based on the following conditions: 2500 new TCP connections per second, 2500 HTTP transactions per second, average packet size of 445 bytes, system running Cisco IPS 5.1 sensor software.

IDS-4250 supports a 500-Mbps speed and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets. The sensing interface and the command and control interface are both 10/100/1000BASE-TX. The optional interface is 1000BASE-SX (fiber). You can now install a second SX card in the IDS-4250. In addition, you can upgrade IDS-4250 to full line-rate gigabit performance with the IDS Accelerator (XL) card. You can also install the 4FE card to provide an additional four sensing interfaces. There is also an optional 10/100/1000TX adapter card that allows additional options for inline functionality beyond the 4FE card. For the procedure for installing optional PCI cards, see Installing Optional PCI Cards, page 4-14.

Note The 500-Mbps performance for IDS-4250 is based on the following conditions: 2700 new TCP connections per second, 2700 HTTP transactions per second, average packet size of 595 bytes, system running Cisco IPS 5.1 software.

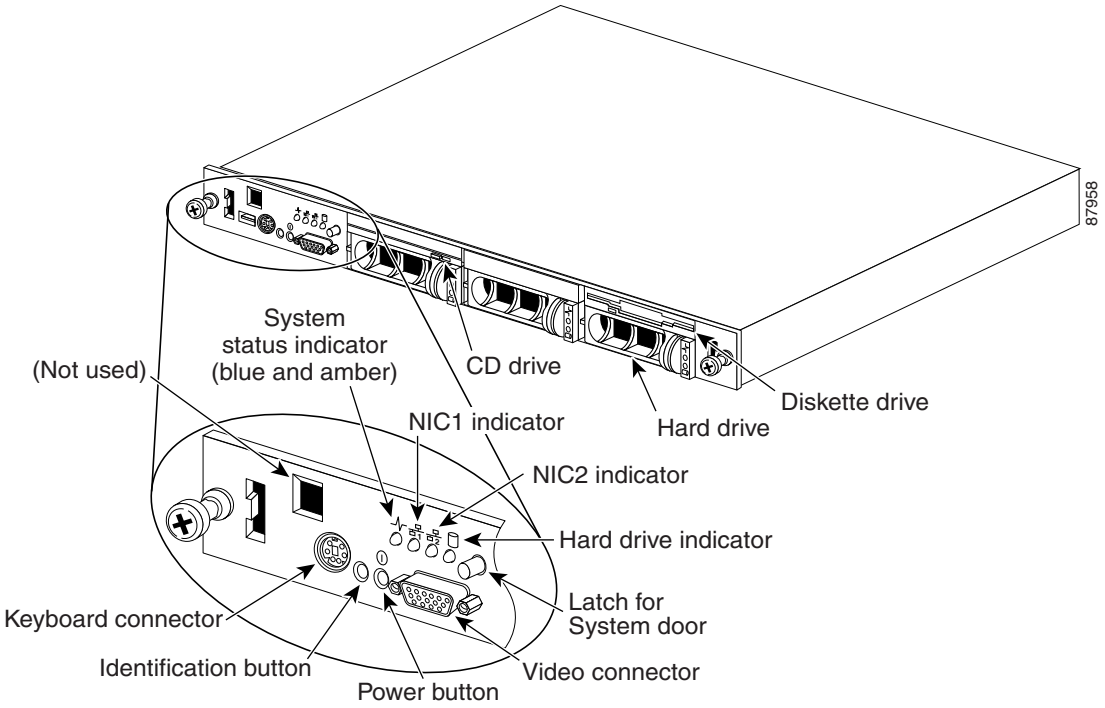
Or you can order IDS-4250-XL with the XL card already installed. At 1 Gbps, IDS 4250-XL provides customized hardware acceleration to protect fully saturated gigabit links as well as multiple partially utilized gigabit subnets.

Note The 1000-Mbps performance for IDS-4250-XL is based on the following conditions: 5000 new TCP connections per second, 5000 HTTP transactions per second, average packet size of 595 bytes, system running Cisco IPS 5.1 software.

Front-Panel Features and Indicators

Figure 4-1 shows the controls, indicators, and connectors located behind the bezel on the front panel of IDS-4235 and IDS-4250.

Figure 4-1 Front-Panel Features and Indicators



The power button controls the AC power input to the power supplies of IDS-4235 and IDS-4250.

You can use the identification buttons on the front and back panels to locate a particular IDS-4235 or IDS-4250 in a rack. When you push one of these buttons, the blue system status indicator on the front and back blinks until you push one of the buttons again.

The front panel also has a video connector for connecting a monitor and a PS/2 connector for connecting a keyboard.

Table 4-1 describes the appearance of the front panel indicators for IDS-4235 and IDS-4250.

Table 4-1 Front-Panel Indicators

LED Indicator	Icon	Description
Blue and amber system status indicator		The blue system status indicator lights up during normal system operation. The amber system status indicator flashes when the system needs attention due to a problem with power supplies, fans, system temperature, or hard drives.[1]
NIC1 and NIC2 link and activity indicators	1	The link and activity indicators for the two integrated NICs light up when the NICs are in use.

Table 4-1 Front-Panel Indicators (continued)

LED Indicator	Icon	Description
Hard-disk drive indicator		The green hard-disk drive activity indicator flashes when the hard-disk drive is in use.
Power button		The power button lights up when the system power is on.

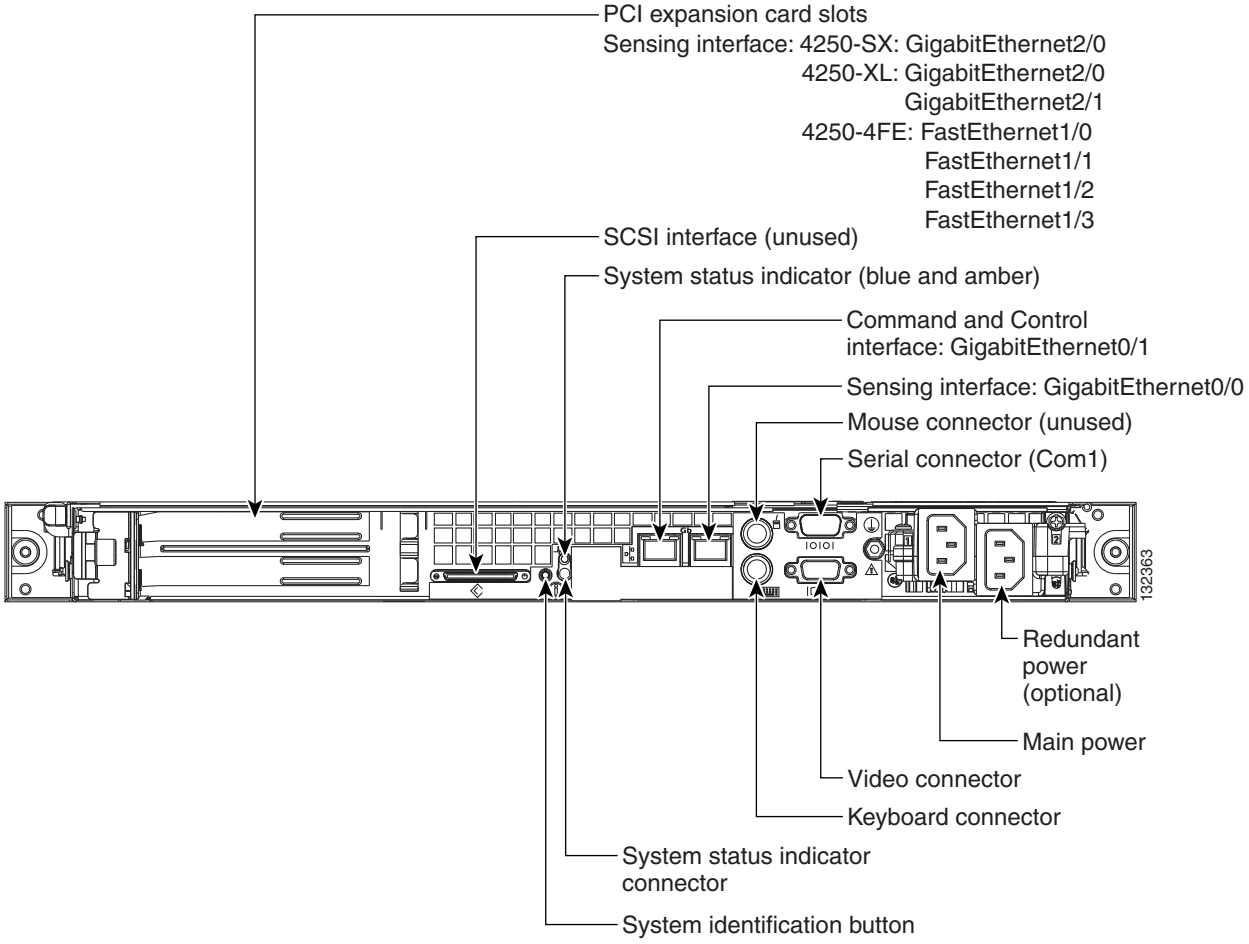
1. If the system is connected to AC power and an error has been detected, the amber system status indicator will flash regardless of whether the system has been powered on

Back-Panel Features and Indicators

Figure 4-2 shows the controls, indicators, and connectors located on the back panel of the IDS-4235 or IDS-4250.

Note Appliances with only one power supply should connect the power cable to connector PS1.

Figure 4-2 Back-Panel Features and Indicators



Specifications

Table 4-2 lists IDS-423 and IDS-4250 specifications.

Table 4-2 IDS-4235 and IDS-4250 Specifications

Dimensions and Weight	
Height	1.67 in. (4.24 cm)
Width	17.6 in. (44.70 cm)
Depth	27.0 in. (68.58 cm)
Weight	35 lb (15.88 kg)
Form factor	1 RU, standard 19-inch rack-mountable
Power	
Autoswitching	110V to 220 VAC
Frequency	50 to 60 Hz, single phase
Operating current	2.7A at 115V 1.3A at 220V
Maximum heat dissipation	983 Btu/hr (maximum)
Environment	
Temperature	Operating +50° to +95°F (+10° to +35°C) Nonoperating -40° to +149°F (-40° to +65°C)
Relative humidity	Operating 8 to 80% (noncondensing) Nonoperating 5 to 95% (noncondensing)

Installing Spare Hard-Disk Drives

Do not install a second hard-disk drive in IDS-4235 or IDS-4250. The spare hard-disk drives are meant to replace the original hard-disk drives and are not meant to be used in conjunction with the original hard-disk drive. If you install two hard-disk drives in IDS-4235 or IDS-4250, they may not recognize the **recover** command used to recover the application partition.

If the original hard-disk drive becomes unusable, remove the hard-disk drive and insert the replacement hard-disk drive. For the procedure, see Removing and Replacing the SCSI Hard-Disk Drive, page 4-16.

The replacement hard-disk drive is shipped blank from the factory. You must reimage it. For the procedure, refer to Upgrading, Downgrading, and Installing System Images.

Upgrading the BIOS

If the BIOS version is earlier than A04 on IDS-4235 or IDS-4250, you must upgrade the BIOS before you install IPS 5.1 software.

Caution The BIOS on IDS-4235 and IDS-4250 is specific to IDS-4235 and IDS-4250 and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on IDS-4235 and IDS-4250 voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Cisco IPS Software, page 11-1.

Caution Do not apply this BIOS upgrade to appliance models other than IDS-4235 and IDS-4250.

Check the BIOS version before performing the following procedure. Reboot the appliance and watch for the BIOS version number. The following example shows BIOS version A03:

```
Phoenix ROM BIOS PLUS Version 1.10 A03
Cisco Systems IDS-4235/4250
www.cisco.com
Testing memory. Please wait.
```

If the version is A01, A02, or A03, you must upgrade the BIOS to version A04.

To create and boot the IDS-4235 and IDS-4250 BIOS upgrade diskette, follow these steps:

Step 1 Copy BIOS_A04.exe to a Windows system.

You can find the file in the /BIOS directory on the recovery/upgrade CD, or you can download it from Cisco.com. For the procedure for downloading IPS software from the Software Center on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

Note You must have a Cisco.com account with cryptographic access before you can download software from the Software Center. For the procedure, see Obtaining Cisco IPS Software, page 11-1.

Step 2 Insert a blank 1.44-MB diskette in the Windows system.

Step 3 Double-click the downloaded BIOS update file, BIOS_A04.exe, on the Windows system to generate the BIOS update diskette.

Step 4 Insert the new BIOS update diskette in IDS-4235.

Caution Do not power off or manually reboot the appliance during Step 5.

Caution You cannot upgrade the BIOS from a console connection. You must connect a keyboard and monitor to the appliance so that you can see the output on the monitor.

Step 5 Boot the appliance and follow the on-screen instructions.

Step 6 Remove the BIOS update diskette from the appliance while it is rebooting, otherwise the BIOS upgrade will be started again.

Using the TCP Reset Interface

IDS-4250-XL has a TCP reset interface—INT0. IDS-4250-XL has a specific TCP reset interface because it cannot send TCP resets on its sensing ports.

If you have reset problems with IDS-4250-XL, try the following:

- Make sure the TCP reset interface of IDS-4250-XL (int0) is connected to the same switch as the sensing ports (int2 and int3) of the XL card.
- If the sensing ports are access ports (a single VLAN), you need to configure the reset port to be in the same VLAN.

  Note If the two XL ports are access ports for different VLANs, you can only configure the reset port for one of these VLANs. You can use dot1q trunk ports to overcome this limitation.

- If the sensing ports are dot1q trunk ports (multi-VLAN), the sensing ports and reset port all need to have the same native VLAN, and the reset port needs to trunk all the VLANs being trunked by both the sensing ports.

Installing IDS-4235 and IDS-4250

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

To install IDS-4235 and IDS-4250 on the network, follow these steps:

Step 1 Position the appliance on the network.

Step 2 Attach the power cord to IDS-4235 and plug it in to a power source (a UPS is recommended).

Step 3 Use the dual serial communication cable (PN 72-1847-01, included in the accessory kit) to attach a laptop to the COM1 (serial) port of the appliance (see Table 4-3 on page 4-9 for a list of the terminal settings), or connect a keyboard and monitor to the appliance.

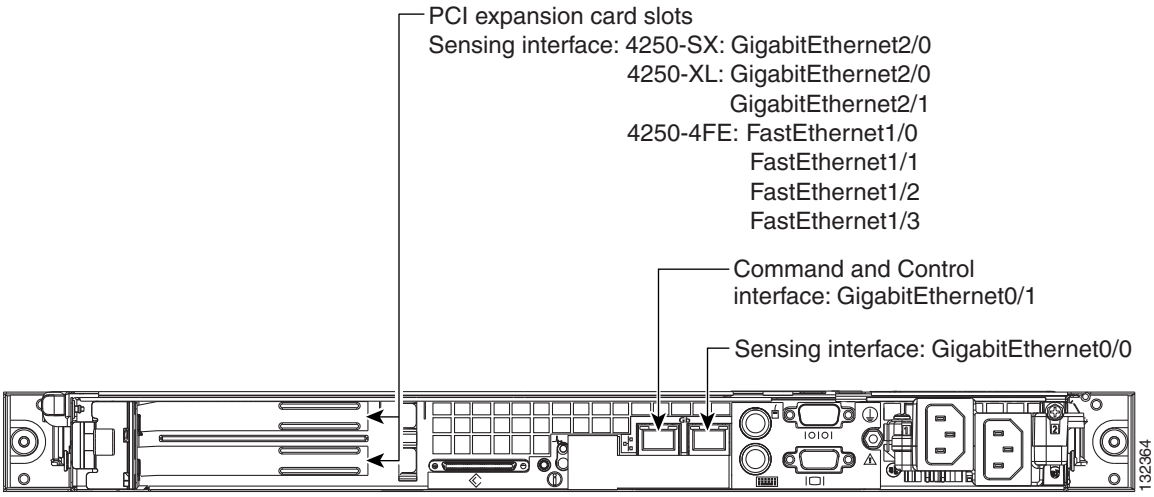
Table 4-3 Terminal Settings

Terminal	Setting
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware or RTS/CTS

Caution We recommend that you use the dual serial communication cable included in the accessory kit, because some keyboards and monitors are incompatible with IDS-4235 and IDS-4250.

Note You can use a 180 rollover or straight-through patch cable to connect the appliance to a port on a terminal server with RJ-45 or hydra cable assembly connections. Use a M.A.S.H adapter (part number 29-4077-02) to connect the appropriate cable to a port on the terminal server. For the instructions for setting up a terminal server, see Setting Up a Terminal Server, page 1-14.

Step 4 Attach the network cables.



IDS-4225 and IDS-4250 have the following interfaces:

- GigabitEthernet0/0 is the sensing port.
- GigabitEthernet0/1 is the command and control port.
- GigabitEthernet1/0 and GigabitEthernet2/0 are the optional SX (fiber NIC) sensing ports (with two SX cards installed).
- GigabitEthernet2/0 and GigabitEthernet2/1 are the optional XL card sensing ports.

- FastEthernet1/0, FastEthernet1/1, FastEthernet1/2, and FastEthernet1/3 are the optional 4FE card sensing ports.
- GigabitEthernet1/0 or GigabitEthernet2/0 (depending on the slot it is installed in) is the optional (copper NIC) sensing port (with one TX card installed). Only one optional TX adapter is supported.

Caution Management and console ports are privileged administrative ports. Connecting them to an untrusted network can create security concerns.

Step 5 Power on the appliance.

Caution If the BIOS version is earlier than A04, you must apply the BIOS upgrade before installing IPS 5.1 on the appliance. For the procedure, see Upgrading the BIOS, page 4-7.

Step 6 Initialize the appliance.

For the procedure, see Initializing the Sensor, page 10-2.

Step 7 Upgrade the appliance to the most recent Cisco IPS software.

For the procedure, see Obtaining Cisco IPS Software, page 11-1.

You are now ready to configure intrusion prevention on the appliance.

For More Information

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

Installing the Accessories

This section describes the contents of the IDS-4235 and IDS-4250 accessories package and how to install the accessories. It contains these topics:

Accessories Package Contents

The following items are shipped in the accessories kit for IDS-4235 and IDS-4250:

- Cisco IDS-4235 or IDS-4250 bezel
- Power cable
- Network patch cable
- Dual serial communication cable
- Serial extension adapter
- M.A.S.H adapter
- Documentation and software
  - Cisco IDS recovery/upgrade CD
  - Cisco Documentation CD
  - *Documentation Roadmap for Cisco Intrusion Prevention System 4.x*

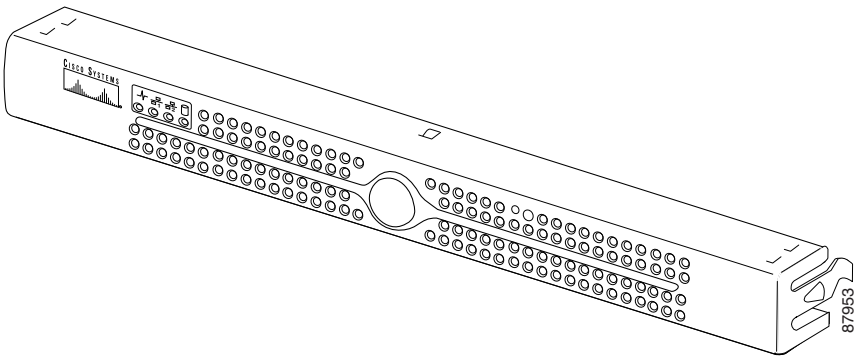
    Note 5.1 documentation is not included in the accessories kits for IDS-4235 and IDS-4250. These systems are no longer being actively manufactured so the newest documentation is not shipped. You can find 5.1 documentation at this URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

  - *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*

Installing and Removing the Bezel

Figure 4-3 shows the Cisco bezel that you can install on IDS-4235 and IDS-4250.

Figure 4-3 Cisco Bezel



To install and remove the bezel on IDS-4235 and IDS-4250, follow these steps:

Step 1 To install the bezel, follow these steps:

a. Align the right side tab on the bezel with the slot on the appliance mounting tab.

b. Press the left side of the bezel into place on the appliance.

Step 2 To remove the bezel, press the left side tab and pull.

Installing the Power Supply

You can install a second, redundant power supply and power-supply cooling fan (part number IDS-PWR=) in IDS-4235 and IDS-4250.

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

To install a power supply and fan, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare the appliance to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down the appliance from IDM.

Step 3 Power off the appliance.

Step 4 Remove the power cord and other cables from the appliance.

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

For more information, see Working in an ESD Environment, page 1-25.

Step 6 Remove the cover.

a. Remove the single screw at the front of the chassis.

b. Press the chassis release button to release the left side of the cover.

c. Lift the left side of the cover using the tab at the back of the appliance.

d. Lift the right side of the cover using the tab at the back of the appliance.

Step 7 Place the new power supply cooling fan in the back of the power supply bay (see Figure 4-4 on page 4-13).

Note Ensure that the finger guard on the fan faces the back of the appliance and that the fan power cable is pointing toward the fan power connector on the system board (see Figure 4-4 on page 4-13).

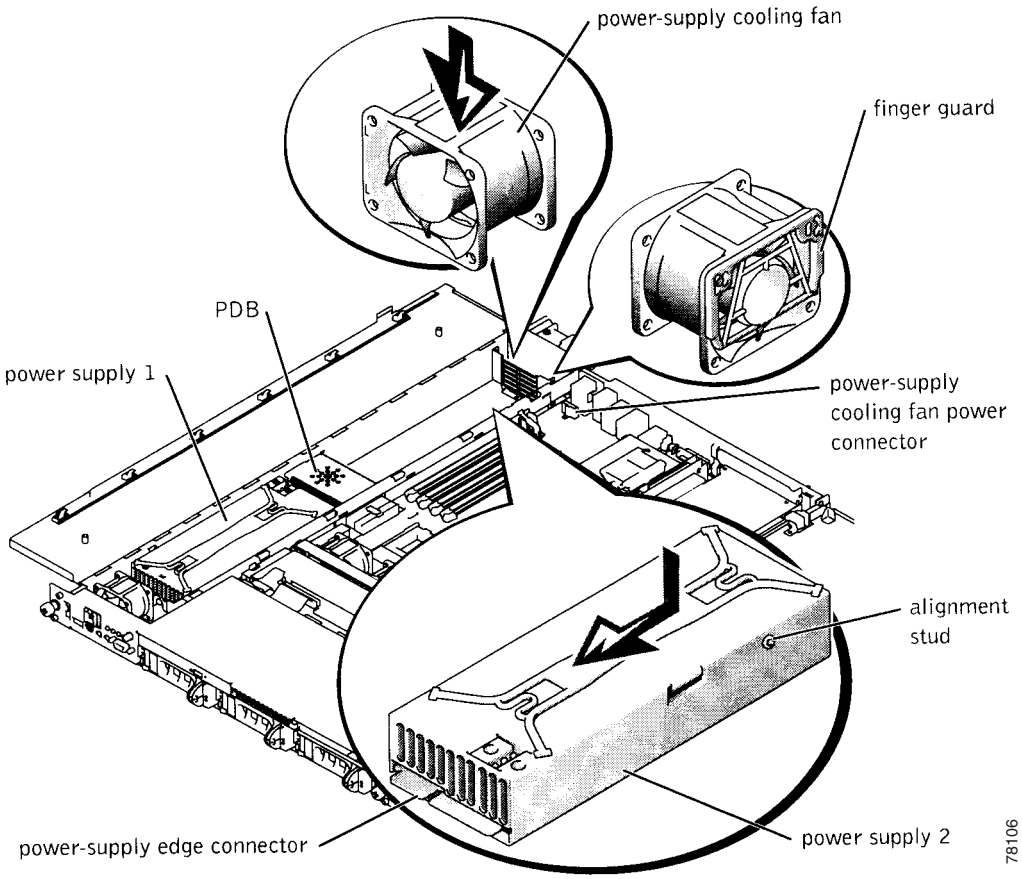
Step 8 Route the fan power cable through the rectangular opening in the power supply bay partition, and then connect the cable to the fan power connector on the system board (see Figure 4-4 on page 4-13).

Step 9 To install the new power supply, align the stud on the side of the power supply with the corresponding notch in the chassis, and then lower the power supply into the chassis (see Figure 4-4 on page 4-13).

Warning **The connectors on the Power Distribution Board (PDB) contain high voltages. Do not remove the metal cover from the PDB or touch the connectors on the PDB or power supplies.**

Step 10 Slide the power supply toward the PDB until the power-supply edge connector is fully seated in the PDB connector (see Figure 4-4 on page 4-13).

Figure 4-4 Power Supply and Power-Supply Cooling Fan



Step 11 Close the cover.

a. Close the right side of the cover.

b. Close the left side of the cover, and press firmly along the edge to lock in place.

c. Replace the screw at the front of the chassis.

Step 12 Connect the new system power cable to the power-supply 2 cable connector (PS2) on the back panel of the appliance.

Installing Optional PCI Cards

You can install the following optional PCI cards in IDS-4235 and IDS-4250 as indicated in Table 1-4 on page 1-11. The optional PCI cards provide additional sensing interfaces.

- SX card (1000BASE-SX sensing interface, part number, IDS-4250-SX-INT=)

  You can install one or two SX cards in the IDS-4250.

- TX card (10/100/1000TX sensing interface, part number, IDS-TX-INT=)

  You can install the TX card in the upper PCI slot in the IDS-4235 and IDS-4250.

- XL card (accelerated 1000BASE-SX interface with MTRJ, part number IDS-XL-INT=)

  You can install the XL card in the upper PCI slot in the IDS-4250. The XL card accelerates the performance of IDS-4250 up to 1 Gbps. You can use an MTRJ cable (part number CAB-MTRJ-SC-MM-3M=) to connect the fiber port on the XL card to the switch on the network. You can order this cable when you order the XL card.

  For information about disconnecting the fiber ports the first time you boot IDS-4250 after upgrading with the XL card, see Disconnecting the XL Card Fiber Ports, page 4-16.

- 4FE card (four-port 10/100BASE-TX fast Ethernet sensing interface, part number IDS-4FE-INT=)

  You can install the 4FE card in the lower PCI slot in the IDS-4235 and IDS-4250.

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

Note None of the PCI cards are supported as a command and control interface.

To install the PCI card, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare the appliance to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down the appliance from IDM.

Step 3 Power off the appliance.

Step 4 Remove the power cord and other cables from the appliance.

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

For more information, see Working in an ESD Environment, page 1-25.

Step 6 Remove the cover.

a. Remove the single screw at the front of the chassis.

b. Press the chassis release button to release the left side of the cover.

c. Use the tab at the rear of the system to lift the left side of the cover.

d. Use the tab at the rear of the system to lift the right side of the cover.

Step 7 Remove the PCI slot cover.

a. Pull the slot release pin at the back of the chassis to unlock the PCI slot covers and pull the slot release toward you.

b. Remove the PCI slot cover.

Step 8 Insert the PCI card into the proper PCI slot of the riser card (according to which card you have), using enough pressure so that the card pops securely into place.

Caution Be sure to support the riser card while inserting the PCI card, otherwise, you could cause the riser card to flex and damage the riser card or main board.

Step 9 Check the back of the chassis to be sure the card is flush with the PCI slot, and then return the PCI slot release to its original position to lock the PCI slot card in place.

Step 10 Close the cover.

a. Close the right side of the cover.

b. Close the left side of the cover, and press firmly along the edge to lock in place.

c. Replace the screw at the front of the chassis.

Step 11 Replace the power and network connections.

Note The sensing interface connector is now on the XL card.

Step 12 Reboot the appliance.

Caution Make sure the fiber ports are not connected the first time you boot the appliance after you have installed the XL card. For more information, see Disconnecting the XL Card Fiber Ports, page 4-16.

Step 13 Assign the new interfaces:

- SX card—GigabitEthernet1/0 or GigabitEthernet2/0 (1 SX card), GigabitEthernet1/0 and GigabitEthernet2/0 (2 SX cards)
- TX card—GigabitEthernet1/0 or GigabitEthernet2/0
- XL card—GigabitEthernet2/0 and GigabitEthernet2/1
- 4FE card—FastEthernet1/0, FastEthernet1/1, FastEthernet1/2, and FastEthernet1/3

For the CLI procedure, refer to Configuring Interfaces. For the IDM procedure, refer to Configuring Interfaces.

Disconnecting the XL Card Fiber Ports

When you upgrade IDS-4250-TX and IDS-4250-SX with the XL card, they may not boot up the first time if the fiber ports are connected. Disconnect the fiber ports before you boot them. After they start for the first time, the firmware version is upgraded and the problem is not seen again.

Note You will not experience this problem if you order IDS-4250-XL—with the XL card already installed—because it is rebooted at the factory.

To allow IDS-4250 to reboot after installing the XL card, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IDS-4250 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down IDS-4250 from IDM.

Step 3 Power off IDS-4250.

Step 4 Remove the fiber connections from the XL card.

Step 5 Boot IDS-4250.

Wait until IDS-4250 has completed bootup and you see a login prompt.

Step 6 Plug the fiber connections back into the XL card.

During the startup of the IPS applications, the XL card is upgraded to the latest firmware.

Removing and Replacing the SCSI Hard-Disk Drive

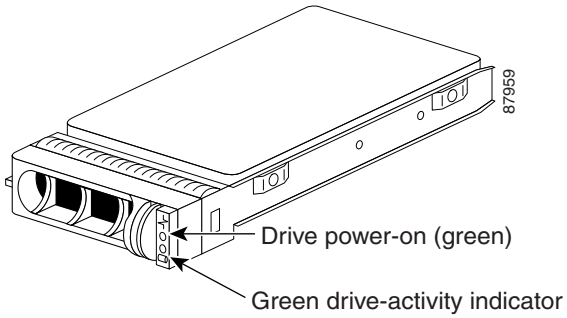
IDS-4235 and IDS-4250 has a removable SCSI hard-disk drive. You can replace the hard-disk drive in case of drive failure. Or you can order a spare drive (part number IDS-SCSI=), apply your configuration, and ship the drive to a remote site. The administrator at the remote site can then install the configured drive.

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in the *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

Caution Do not install a second hard-disk drive in IDS-4235 and IDS-4250. The spare hard-disk drives are meant to replace the original hard-disk drives and are not meant to be used with the original hard-disk drive. If you install two hard-disk drives in the appliance, the appliance may not recognize the **recover** command used to recover the application partition of the appliance.

Figure 4-5 on page 4-17 shows the SCSI hard-disk drive indicators.

Figure 4-5 SCSI Hard-Disk Drive



When you have installed the new hard-disk drive, you must reimage it with the recovery/upgrade CD. For the procedure, refer to Using the Recovery/Upgrade CD.

This section contains the following topics:

- Removing the SCSI Hard-Disk Drive, page 4-17
- Replacing the SCSI Hard-Disk Drive, page 4-18

Removing the SCSI Hard-Disk Drive

To remove the SCSI hard-disk drive, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare the appliance to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down the sensor from IDM.

Step 3 Power off the appliance by pressing the power button.

Step 4 Remove the front bezel.

For the procedure, see Installing and Removing the Bezel, page 4-11.

Step 5 Open the hard-disk drive handle to release the drive.

Step 6 Slide the hard-disk drive out until it is free of the drive bay.

Replacing the SCSI Hard-Disk Drive

To replace the SCSI hard-disk drive, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare the appliance to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down the sensor from IDM.

Step 3 Power off the appliance by pressing the power button.

Step 4 Remove the front bezel.

For the procedure, see Installing and Removing the Bezel, page 4-11.

Step 5 Open the hard-disk drive handle.

Step 6 Insert the hard-disk drive into the drive bay.

Step 7 Close the hard-disk drive handle to lock the drive into place.

Step 8 Power on the appliance by pressing the power button.

Step 9 Replace the front bezel.

For the procedure, see Installing and Removing the Bezel, page 4-11.

Note Replacement drives are shipped without an image. You must reimage the hard-disk drive. For more information, refer to Upgrading, Downgrading, and Installing System Images.

Four-Post Rack Installation

You can install the appliance in a four-post rack (part number IDS-RAIL-4=).

Caution Do not install rack kit components designed for another system. Use only the rack kit for the appliance. Using the rack kit for another system may damage the appliance and cause injury to yourself and others.

This section contains the following topics:

Recommended Tools and Supplies

You need these tools and supplies to install the appliance in a four-post rack cabinet:

- #2 Phillips screwdriver
- Masking tape or felt-tip pen for marking the mounting holes to be used

Rack Kit Contents

The four-post rack kit includes the following items:

- One pair of slide assemblies
- One cable-management arm
- One stop block
- One status-indicator cable assembly
- Ten 10-32 x 0.5-inch flange-head Phillips screws
- Releaseable tie wraps

Installing the Slide Assemblies

The rack is measured in rack units (RU). An RU is equal to 44 mm or 1.75 inches.

To install the slide assemblies, follow these steps:

Step 1 Remove the rack doors according to the documentation provided with the rack cabinet.

Step 2 Place a mark on the rack's front vertical rails where you want to locate the bottom of the appliance that you are installing in the rack cabinet.

Note The bottom of each 1-RU space is at the middle of the narrowest metal area between holes (marked with a horizontal line on some rack cabinets).

Step 3 Place a mark 44 mm (1.75 inches) above the original mark you made (or count up three holes) and mark the rack's front vertical rails to indicate where the appliance's upper edge will be located on the vertical rails.

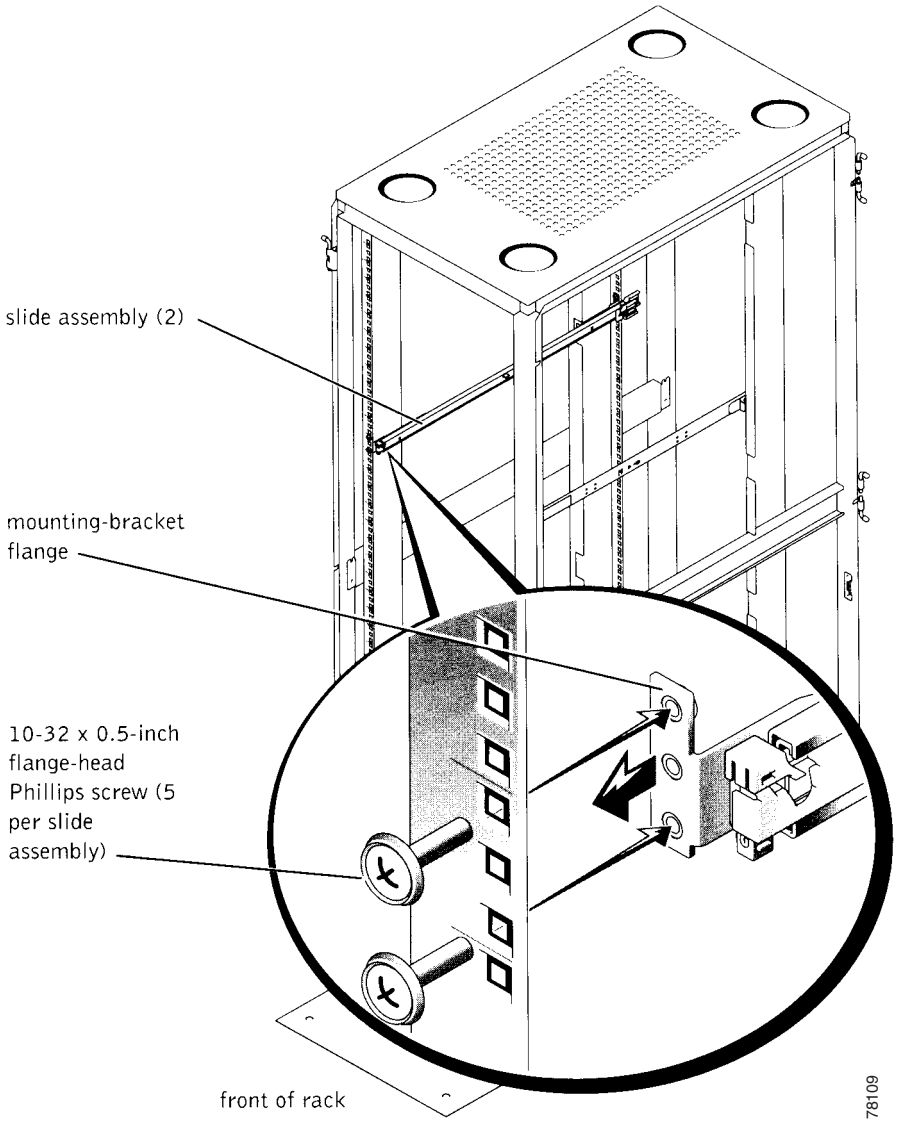
Note Mark 1 RU (44 mm or 1.75 inches) of vertical space for each appliance you install in the rack.

Step 4 At the front of the rack cabinet, position one of the slide assemblies so that its mounting-bracket flange fits between the marks you made on the rack (see Figure 4-6 on page 4-20).

Note The three holes on the front of the mounting bracket should align with the 3 holes between the marks you made on the vertical rails.

Step 5 Install two 10-32 x 0.5-inch flange-head Phillips screws in the mounting flange's top and bottom holes to secure the slide assembly to the front vertical rail (see Figure 4-6 on page 4-20).

Figure 4-6 Slide Assemblies



Step 6 At the back of the cabinet, pull back on the mounting-bracket flange until the mounting holes align with their respective holes on the back vertical rail.

Step 7 Install three 10-32 x 0.5-inch flange-head Phillips screws in the mounting flange's holes to secure the slide assembly to the back vertical rail.

Step 8 Repeat Steps 3 through 7 for the remaining slide assembly on the other side of the rack.

Step 9 Ensure that the slide assemblies are mounted at the same position on the vertical rails on each side of the rack.

Installing the Appliance in the Rack

If you are installing more than one appliance, install the first appliance in the lowest available position in the rack.

Caution Never pull more than one component out of the rack at a time.

To install the appliance in the rack, follow these steps:

Step 1 Pull the two slide assemblies out of the rack until they lock in the fully extended position.

Caution Because of the size and weight of the appliance, never attempt to install the appliance in the slide assemblies by yourself.

Step 2 Remove the appliance front bezel by pressing the left side tab and pulling.

Step 3 Lift the appliance into position in front of the extended slides.

Step 4 Place one hand on the front-bottom of the appliance and the other hand on the back-bottom of the appliance.

Step 5 Tilt the back of the appliance down while aligning the back shoulder screws on the sides of the appliance with the back slots on the slide assemblies.

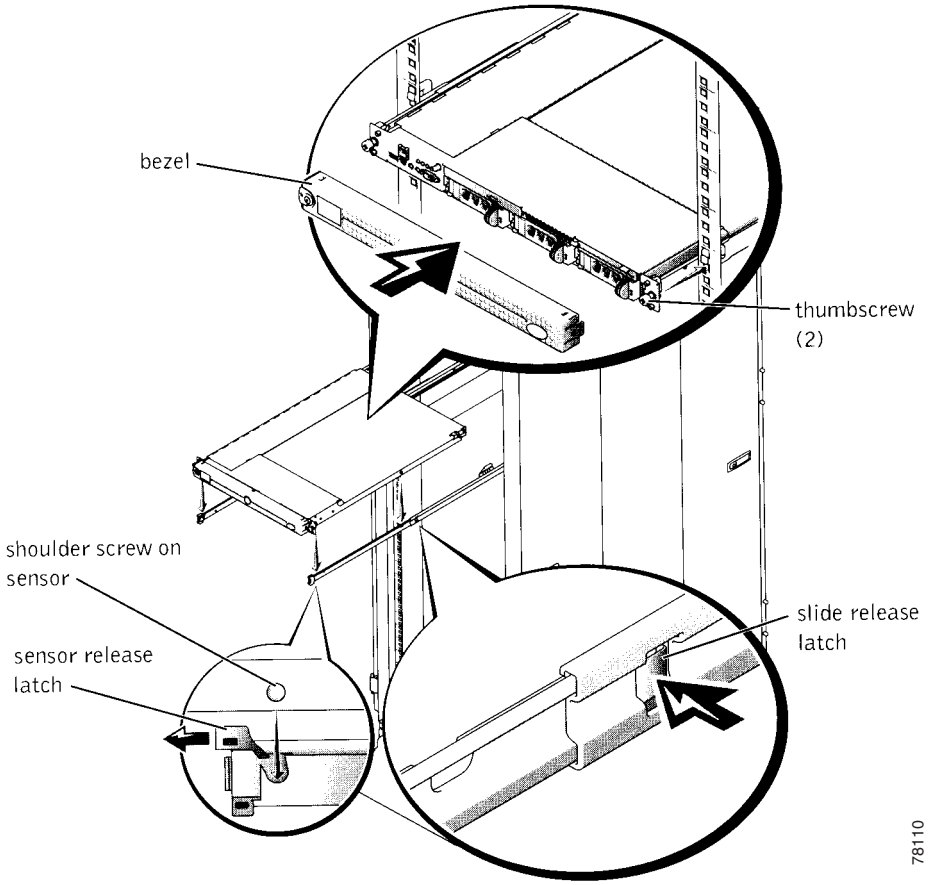
Step 6 Engage the back shoulder screws into their slots.

Step 7 Lower the front of the appliance and engage the front shoulder screws in the front slot behind the appliance release latch (see Figure 4-7 on page 4-22).

The appliance release latch moves forward and then snaps back as the shoulder screw passes into the front slot.

Note Use the appliance release latch when you want to remove the appliance from the slide assemblies.

Figure 4-7 Installing the Appliance in the Rack



Step 8 Press the slide release latch at the side of each latch to slide the appliance completely into the rack (see Figure 4-7).

Step 9 Push in and turn the captive thumbscrews on each side of the front chassis panel to secure the appliance to the rack.

Installing the Cable-Management Arm

You can install the cable-management arm on the right or left of the rack cabinet. This procedure describes installing the cable-management arm in the right side of the rack cabinet, as viewed from the back.

Tip If you are installing several appliances in the rack, consider installing the cable management arms on alternating sides of the rack for ease in cable routing.

To install the cable-management arm, follow these steps:

Step 1 Facing the back of the rack cabinet, locate the latch on the end of the right slide assembly that you secured to the back vertical rail.

Step 2 Push the tab on the back end of the cable-management arm into the latch on the end of the slide assembly (see Figure 4-8 on page 4-24).

Note The latch clicks when locked.

Step 3 Push the tab on the remaining free end (the front) into a mating latch on the inner segment of the slide assembly (see Figure 4-8 on page 4-24).

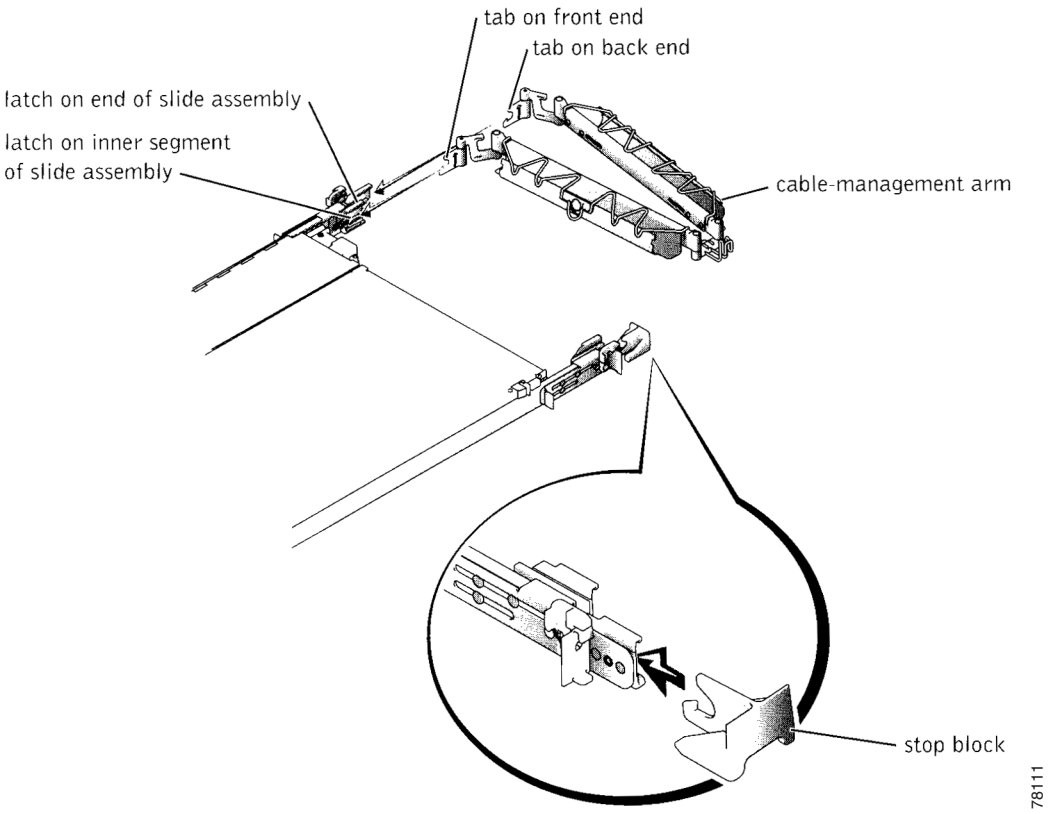
Note The latch clicks when locked.

Step 4 Install a stop block on the latch on the end of the opposite slide assembly (see Figure 4-8 on page 4-24).

Note The stop block prevents the backward travel of the cable-management arm and supports the weight of the arm with its load of installed cables.

Note The two-post rack kit has two stop blocks: one for right-side mounting, and one for left-side mounting. You can only install the proper stop block.

Figure 4-8 Cable-Management Arm



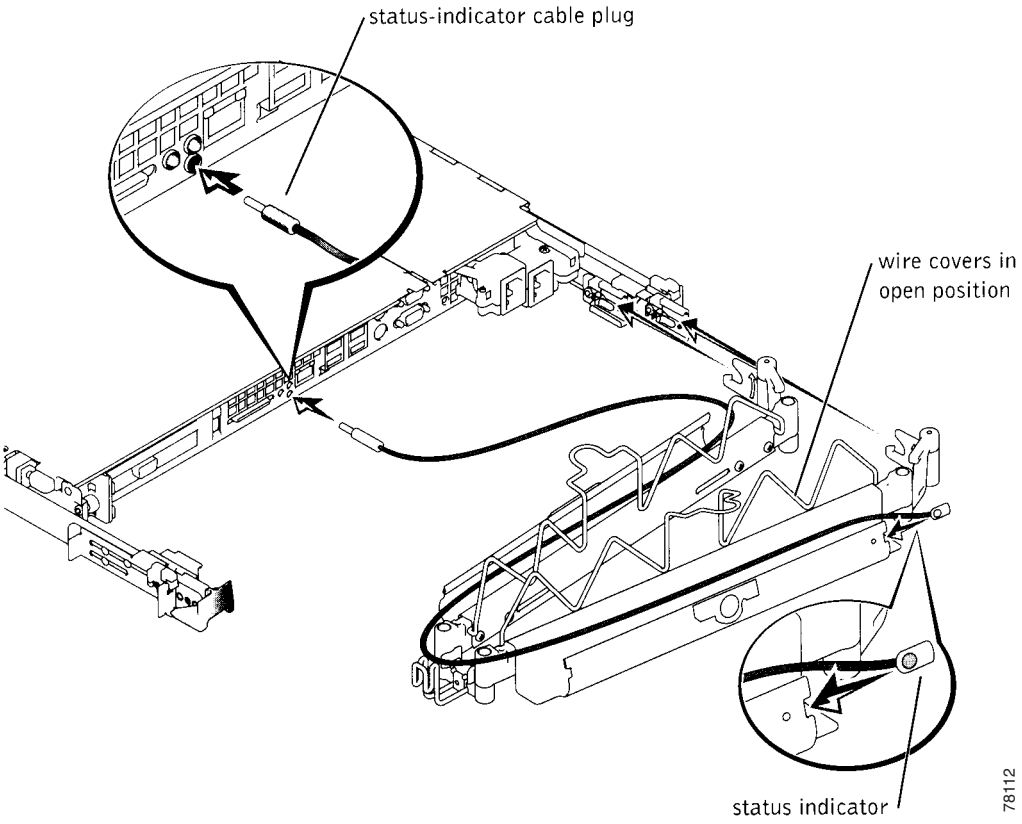
Step 5 Install the status-indicator cable plug into its connector (see Figure 4-9 on page 4-25).

Step 6 Open the wire covers on the cable-management arm by lifting the center of the wire over the top of the embossed round button on the front of the forward part of the arm, and lifting the wire over the top of a similar round button on the back part of the arm.

The wire cover swings open to enable cables to be routed within the arm.

Step 7 Route the status-indicator end of the cable assembly through the cable-management arm, and install the indicator in its slot at the back end of the cable-management arm (see Figure 4-9 on page 4-25).

Figure 4-9 Installing the Cable-Management Arm



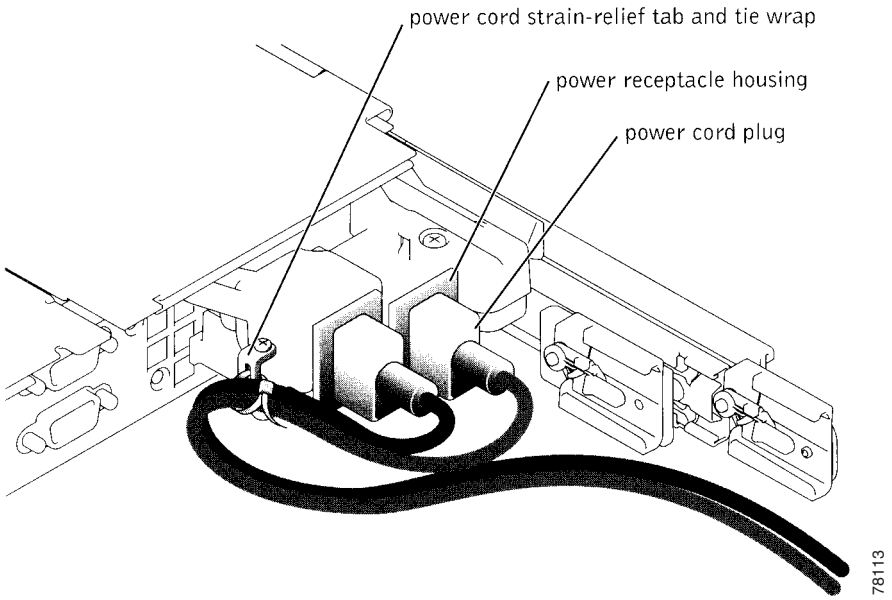
Step 8 Connect the power cords to their receptacles on the back panel.

Note Although the strain-relief can accommodate power cords with a bend radius of up to 19 millimeters (0.75 inch), use only the power cords provided with the appliance.

Step 9 Install a tie-wrap through the slot on the strain-relief tab (see Figure 4-10 on page 4-26).

Step 10 Bend the power cords back beside the power receptacle housing and form a tight loop. Install the strain-relief tie-wrap loosely around the looped power cord (see Figure 4-10 on page 4-26).

Figure 4-10 Power Cord Strain Relief



Routing the Cables

To route the cables, follow these steps:

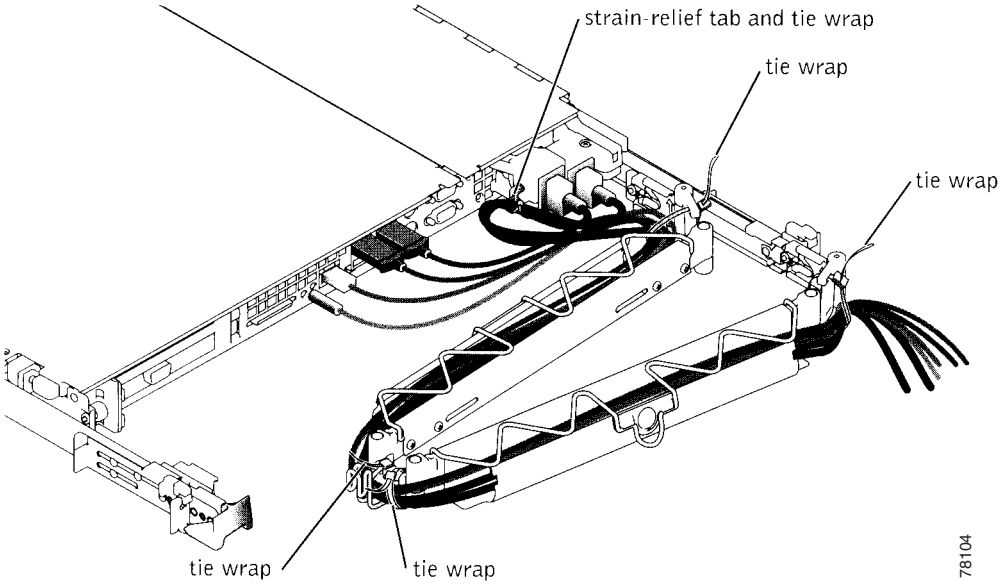
Step 1 Attach the I/O cable connectors to their respective connectors on the appliance back panel.

For details on the cable connections, see Installing IDS-4235 and IDS-4250, page 4-8.

Step 2 Route the power and I/O cables through the cable-management arm, using four loosely secured releaseable tie-wraps (two in the middle and on each end of the cable-management arm).

Note Do not fully tighten the tie-wraps at this time (see Figure 4-11 on page 4-27). Allow some cable slack in the cable-management arm to prevent damage to the cables.

Figure 4-11 Routing Cables



Step 3 Secure the cables to the cable-management arm:

a. After connecting the cables to the appliance, unscrew the thumbscrews that secure the front of the appliance to the front vertical rail.

b. Slide the appliance forward to the fully extended position.

c. Route the cables along the cable-management arm, making any adjustments to the cable slack at the hinge positions, and secure the cables to the cable-management arm with the releaseable tie-wraps and the wire covers over the cable-management arm.

Note As you pull the appliance out to its farthest extension, the slide assemblies lock in the extended position. To push the appliance back into the rack, press the slide release latch on the side of the slide, and then slide the appliance completely into the rack.

Step 4 Slide the appliance in and out of the rack to verify that the cables are routed correctly and do not bind, stretch, or pinch with the movement of the cable-management arm.

Step 5 Make any necessary adjustments to ensure that the cable slack is neither too tight nor too loose, yet keeps the cables in place as the appliance is moved in and out of the rack.

Step 6 Replace the rack doors.

Note Refer to the procedures for replacing the rack doors in the documentation provided with the rack cabinet.

Warning **Because of the size and weight of the rack cabinet doors, never attempt to remove or install them by yourself.**

Two-Post Rack Installation

You can install the two-post rack (part number IDS-RAIL-2=) in a center-mount or flush-mount configuration. The two-post kit incorporates slide assemblies that enable the appliance to be pulled out of the rack for servicing.

You must properly secure the two-post, open frame relay rack to the floor, the ceiling or upper wall, and where applicable, to adjacent racks, using floor and wall fasteners and bracing specified or approved by the rack manufacturer.

Warning **Do not attempt to install the appliance into a two-post, open-frame relay rack that has not been securely anchored in place. Damage to the appliance and injury to yourself and to others may result.**

This section contains these topics:

Recommended Tools and Supplies

You need the following tools and supplies to install the appliance in a two-post, open-frame relay rack:

- #2 Phillips screwdriver
- 11/32-inch wrench or nut driver (if changing bracket to flush-mount configuration)
- Masking tape or felt-tip pen to mark the mounting holes

Rack Kit Contents

The two-post rack kit includes:

- One pair of slide assemblies (two-post)
- One cable-management arm
- One status-indicator cable assembly
- Two stop blocks
- Eight 12-24 x 0.5-inch pan-head Phillips screws
- Releaseable tie wraps

Marking the Rack

You must allow 1 RU (44 mm or 1.75 inches) of vertical space for each appliance you install in the two-post rack.

To mark the rack, follow these steps:

Step 1 Place a mark on the rack's front vertical rails where you want to locate the bottom of the appliance that you are installing in the two-post rack.

Note The bottom of each 1-RU space is at the middle of the narrowest metal area between holes.

Step 2 Place a mark 44 mm (1.75 inches) above the original mark you made.

Note Each 1 RU (44 mm, or 1.75 inches) of vertical space on a rack with universal-hole spacing has three holes with center-to-center spacing between the holes (beginning at the top of a 1-RU space) of 15.9 mm, 15.9 mm, and 12.7 mm (0.625 inches, 0.625 inches, and 0.5 inches).

Installing the Slide Assemblies in the Rack

You can install the slide assemblies in a two-post, open-frame relay rack having either universal-hole spacing or wide-hole spacing. You can install the 1-RU slide assemblies in either a flush-mount or center-mount configuration.

This section contains these topics:

- Center-Mount Installation, page 4-29
- Flush-Mount Installation, page 4-30

Center-Mount Installation

The two-post rack kit is shipped with brackets configured for center-mount installation.

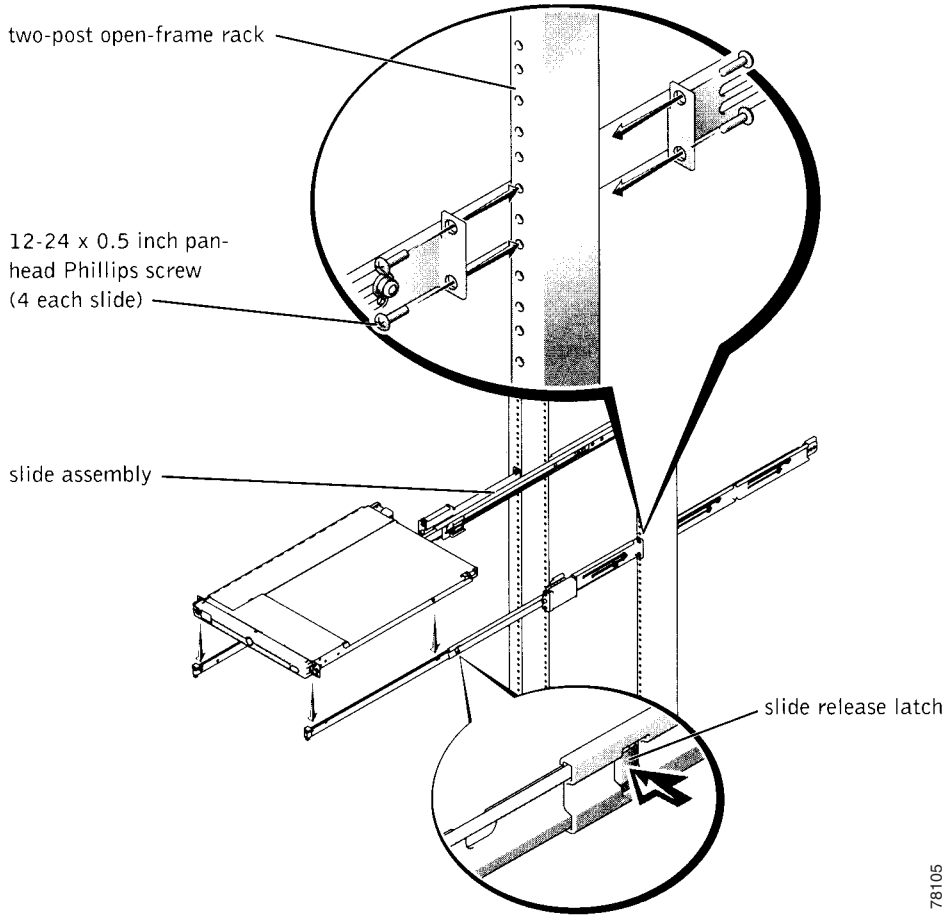
To install the center-mount brackets, follow these steps:

Step 1 Locate the right slide assembly and push the back bracket toward the back of the slide assembly (see Figure 4-12 on page 4-30).

Step 2 Position the right slide assembly in the two-post rack at the location you marked, push the back bracket forward against the vertical two-post rack, and secure the front and rear center-mounting brackets to the rack with two 12-24 x 0.5-inch pan-head Phillips screws (Figure 4-12 on page 4-30).

Step 3 Repeat Steps 1 and 2 to install the left side assembly in the rack.

Figure 4-12 Slide Assemblies for Center-Mount Configuration



Flush-Mount Installation

To install the flush-mount brackets, follow these steps:

Step 1 Locate the two slide assemblies and place them, side by side, on a smooth work surface, with the front ends of the slide assemblies toward you. Position both slide assemblies so that the center brackets are facing upward (see Figure 4-13 on page 4-31).

Note To prepare the slides for flush-mount installation, remove the front mounting bracket, rotate it 180 degrees, and reinstall it on the opposite slide assembly.

Step 2 Using a #2 Phillips screwdriver and an 11/32-inch wrench or nut driver, remove two 12-24 x 0.5-inch pan-head Phillips screws, two nuts, and two shoulder washers from each front center bracket (see Figure 4-13 on page 4-31).

Step 3 Remove the front bracket from both slide assemblies.

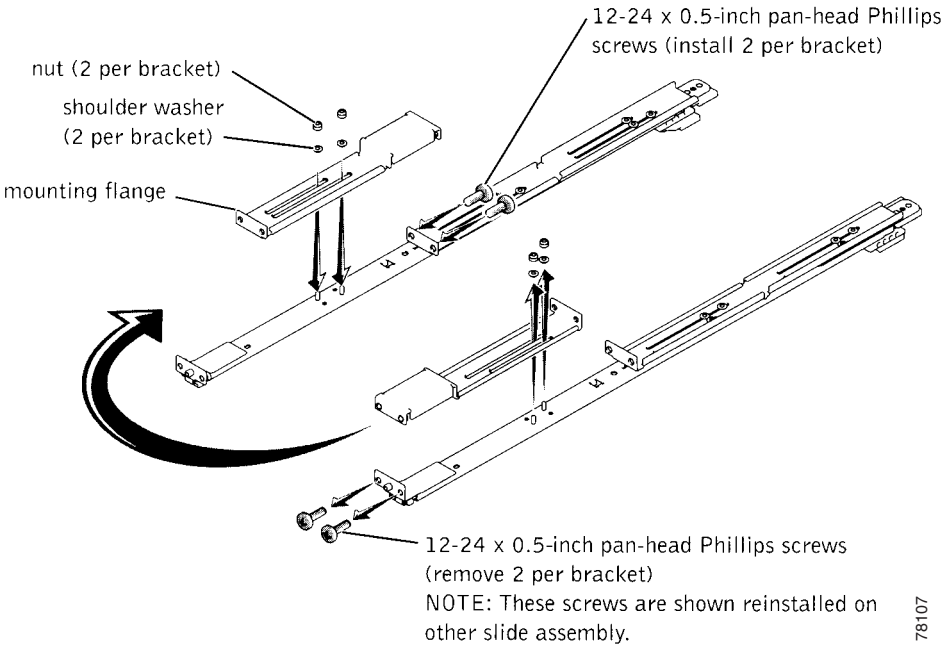
Step 4 Place the bracket from one slide assembly onto the threaded studs on the opposite slide assembly, with the bracket turned 180 degrees so that the mounting flange faces forward (see Figure 4-13 on page 4-31).

Step 5 Secure each front center mount bracket (by its nuts and shoulder washers) and tighten them by hand on their opposite slide assemblies using the two shoulder washers and two nuts you removed in Step 2 (see Figure 4-13).

Step 6 Join the front brackets you just installed to the bracket on the slide assembly with the two 12-24 x 0.5-inch pan-head Phillips screws you removed in Step 2 (see Figure 4-13).

The joined bracket becomes the new extended rear bracket.

Figure 4-13 Rotating the Front-Mounting Bracket for Flush-Mount Installation



Step 7 Repeat Steps 4 though 6 to configure the other slide assembly.

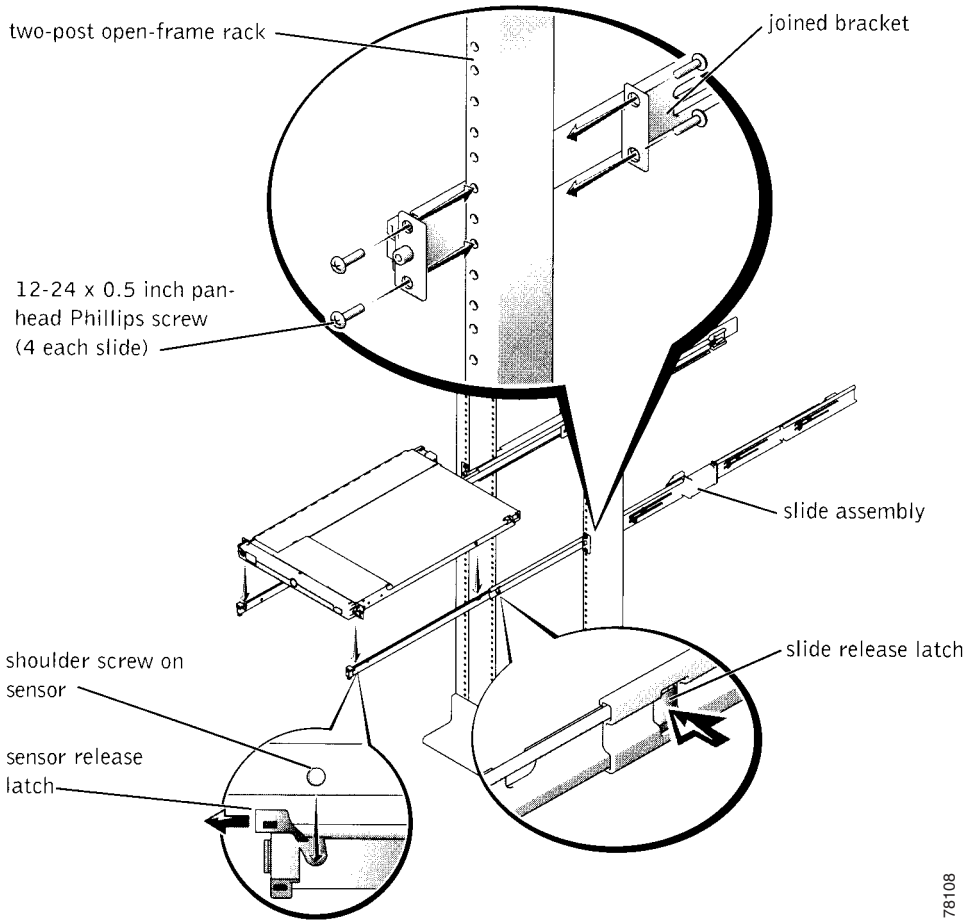
Step 8 Holding the left slide assembly into position in the two-post rack at the location you marked, adjust the extended rear bracket tightly against the back of the vertical two-post rack and secure it to the two-post rail with two 12-24 x 0.5-inch pan-head Phillips screws (see Figure 4-14 on page 4-32).

Step 9 Secure the front bracket on the slide assembly to the two-post rail with two 12-24 x 0.5-inch pan-head Phillips screws (see Figure 4-14 on page 4-32).

Step 10 Repeat Steps 8 and 9 to install the right slide assembly in the rack.

Step 11 Use and 11/32-inch wrench or nut driver to fully tighten the nuts on the mounting brackets on both slide assemblies that you tightened with your fingers.

Figure 4-14 Installing the Slide Assemblies for Flush-Mount Configuration



CHAPTER 5

Installing IPS-4260

This chapter describes IPS-4260 and how to install it. It also describes the accessories and how to install them. This chapter contains the following sections:

Caution The BIOS on IPS-4260 is specific to IPS-4260 and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on IPS-4260 voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Cisco IPS Software, page 11-1.

Introducing IPS-4260

IPS-4260 delivers 1 Gigabit of intrusion prevention performance. You can use IPS-4260 to protect both Gigabit subnets and aggregated traffic traversing switches from multiple subnets. IPS-4260 is a purpose-built device that provides support for both copper and fiber NIC environments providing flexibility of deployment in any environment.

IPS-4260 has two built-in Gigabit Ethernet network ports and six expansion slots. The network port numbers increase from right to left and the expansion slot numbers increase from bottom to top and from right to left as shown in Figure 5-4 on page 5-6. Slots 2 and 3 are PCI-Express connectors and the other expansion slots are PCI-X slots. Slots 1 through 3 are full-height slots and slots 4 though 6 are half-height slots. The built-in management port is called Management0/0 and the built-in sensing interface is Gigabit-Ethernet0/1. For more information on sensor interfaces, see Sensor Interfaces, page 1-3.

Note Only expansion slots 2 and 3 are supported at this time.

For improved reliability, IPS-4260 uses a flash device for storage rather than a hard-disk drive. IPS-4260 supports two optional network interface cards, the 2SX Fiber card, and the 4GE bypass interface card that contains the hardware-bypass feature. Initially IPS-4260 supports only the built-in interfaces and these two interface cards. For more information on the 4GE bypass interface card, see Hardware Bypass, page 5-3.

IPS-4260 monitors greater than 1 Gbps of aggregate network traffic on multiple sensing interfaces and is also inline ready. It replaces IDS-4250-XL. It supports both copper and fiber interfaces.

Note The 1-Gbps performance for IPS-4260 is based on the following conditions: 10,000 new TCP connections per second, 100,000 HTTP transactions per second, average packet size of 450 bytes, and the system running Cisco IPS 5.1 software. The 1-Gbps performance is traffic combined from all sensing interfaces.

IPS-4260 ships with one power supply, but it supports redundant power supplies. For more information, see Installing and Removing the Power Supply, page 5-21.

Note IPS-4260 operates in load-sharing mode when the optional redundant power supply is installed.

Supported PCI Cards

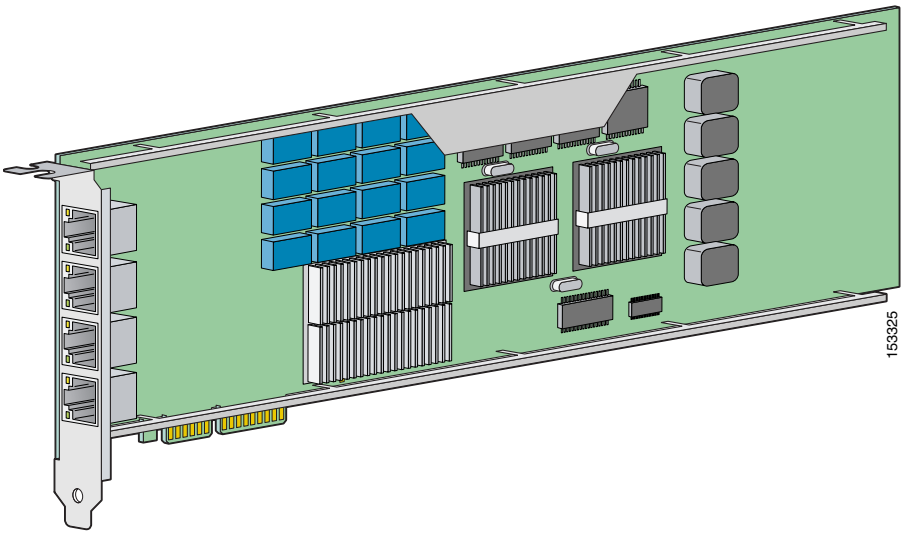
IPS-4260 supports the following PCI cards:

- 4GE bypass interface card (part number IPS-4GE-BP-INT=)

  Provides four 10/100/1000BASE-T (4GE) monitoring interfaces (allowing up to 9 total monitoring interfaces). The 4GE bypass interface card support hardware bypass.

Figure 5-1 shows the 4GE bypass interface card.

Figure 5-1 4GE Bypass Interface Card

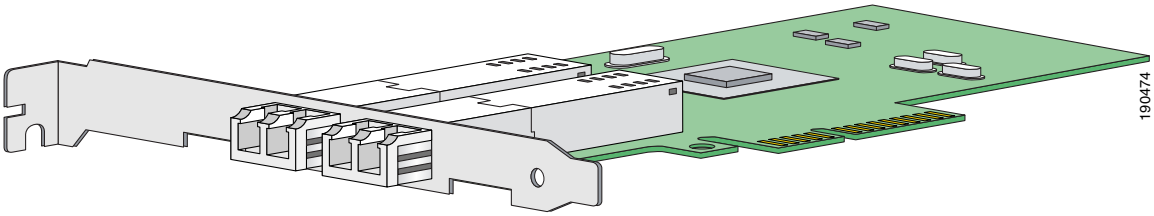


- 2SX Card (part number IPS-2SX-INT=)

  Provides two 1000BASE-SX (fiber) monitoring interfaces (allowing up to 4 total fiber monitoring interfaces). The 2SX interface cards does not support hardware bypass.

  Figure 5-2 shows the 2SX card.

Figure 5-2 2SX Interface Card



Hardware Bypass

This section describes the 4GE bypass interface card and its configuration restrictions. For the procedure for installing and removing the 4GE bypass interface card, see Installing and Removing PCI Cards, page 5-19.

This section contains the following topics:

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 5-1 on page 5-3 shows the 4GE bypass interface card.

Hardware bypass complements the existing software bypass feature in IPS 5.1. For more information on software bypass mode, refer to Configuring Bypass Mode. 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 GigabitEthernet2/0 is capable of performing hardware bypass only when
paired with GigabitEthernet2/1, and both interfaces are enabled and configured with the
same speed and duplex settings.
```

The following configuration restrictions apply to hardware bypass:

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

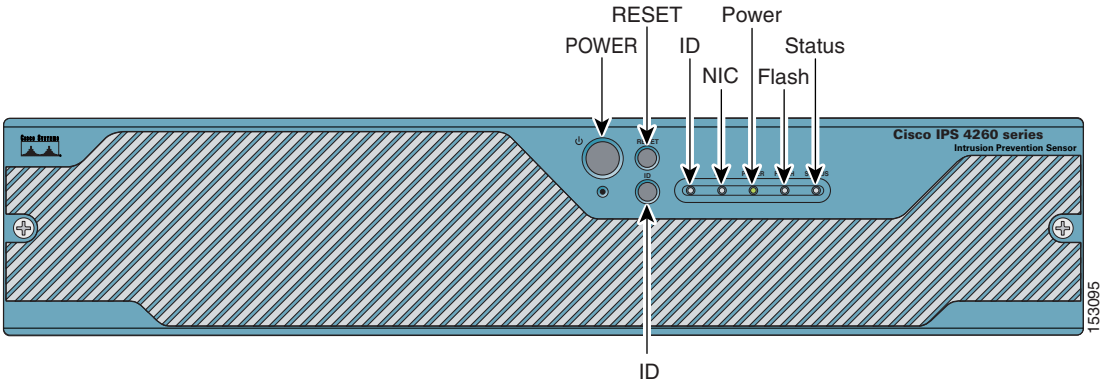
  You must configure both the sensor ports and the switch ports for autonegotiation for hardware bypass to work. The switch ports must support MDI/X, which automatically reverses the transmit and receive lines if necessary to correct any cabling problems. The sensor is only guaranteed to operate correctly 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.

Front and Back Panel Features

This section describes the IPS-4260 front and back panel features and indicators.

Figure 5-3 shows the front view of IPS-4260.

Figure 5-3 IPS-4260 Front Panel Features



There are three switches on the front panel of IPS-4260:

- Power—Toggles the system power.
- Reset—Resets the system.
- ID—Toggles the system ID indicator.

Table 5-1 describes the front panel indicators on IPS-4260.

Table 5-1 Front Panel Indicators

Indicator	Description
ID (blue)	Continuously lit when activated by the front panel ID switch.
NIC (green)	Indicates activity on either the GigabitEthernetO/1 or MGMT interfaces.
Power (green)	When continuously lit, indicates DC power. The indicator is off when power is turned off or the power source is disrupted.
Flash (green/amber)	Off when the compact flash device is not being accessed. Blinks green when the compact flash device is being accessed. Solid amber when a device has failed.
Status (green/amber)	Blinks green while the power-up diagnostics are running or the system is booting. Solid green when the system has passed power-up diagnostics. Solid amber when the power-up diagnostics have failed.

Figure 5-4 shows the back view of the IPS-4260.

Figure 5-4 IPS-4260 Back Panel Features

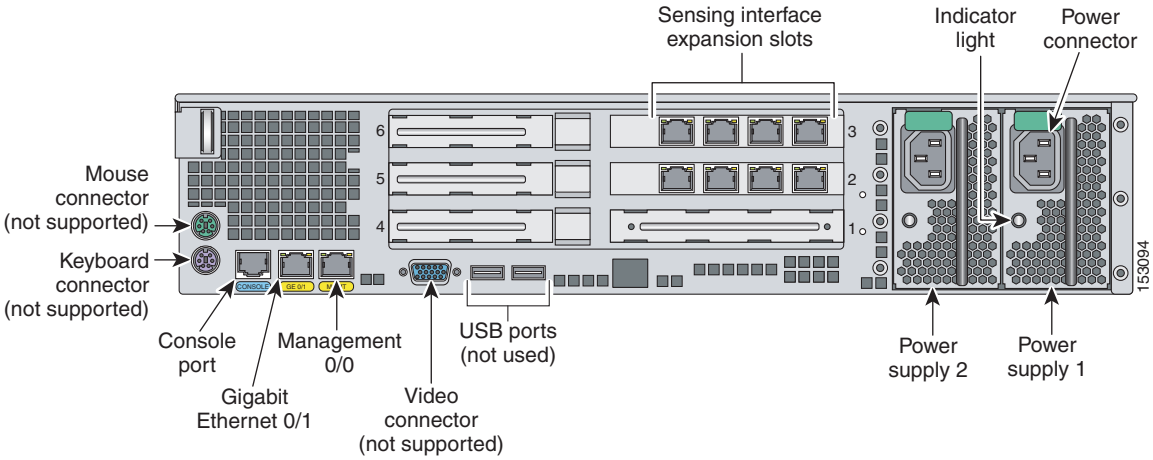


Figure 5-5 shows the two built-in Ethernet ports, which have two indicators per port.

Figure 5-5 Ethernet Port Indicators

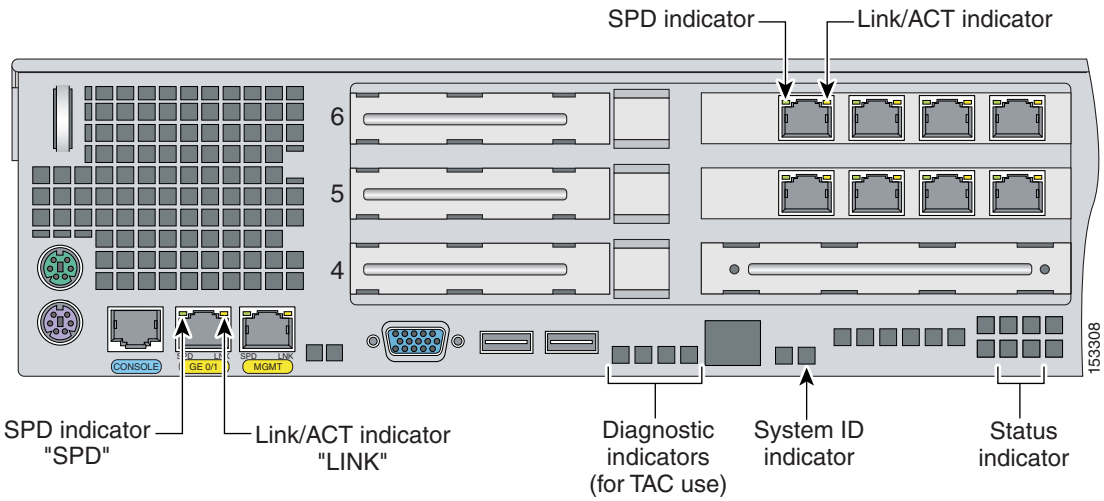


Table 5-2 lists the back panel indicators.

Table 5-2 Back Panel Indicators

Indicator	Color	Description
Left side	Green solid Green blinking	Physical link Network activity
Right side	Not lit Green Amber	10 Mbps 100 Mbps 1000 Mbps

Table 5-3 lists the power supply indicator.

Table 5-3 Power Supply Indicators

Color	Description
Off	No AC power to all power supplies.
Green solid	Output on and ok.
Green blinking	AC present, only 5Vsb on (power supply off).
Amber	No AC power to this power supply (for 1+1 configuration) or power supply critical event causing a shutdown: failure, fuse blown (1+1 only), OCP 12 V, OVP 12 V, or fan failed.
Amber blinking	Power supply warning events where the power supply continues to operate: high temperature, high power/high current, or slow fan.

Specifications

Table 5-4 lists the specifications for IPS-4260.

Table 5-4 IPS-4260 Specifications

Dimensions and Weight	
Height	3.45 in. (87.6 cm)
Width	17.14 in. (435.3 cm)
Depth	20 in. (508 cm)
Weight	40.0 lb (18.14 kg)
Form factor	2 RU, standard 19-inch rack-mountable
Power	
Autoswitching	100V to 240V AC
Frequency	47 to 63 Hz, single phase
Operating current	8.9 A
Steady state	588 W max continuous
Maximum peak	657 W
Maximum heat dissipation	648 BTU/hr
Environment	
Temperature	Operating +32°F to +104°F (+0°C to +40°C) Nonoperating -104°F to +158°F (-40°C to +70°C)
Relative humidity	Operating 10% to 85% (noncondensing) Nonoperating 5% to 95% (noncondensing)
Altitude	Operating 0 to 9843 ft (3000 m) Nonoperating 0 to 15,000 ft (4750 m)
Shock	Operating Half-sine 2 G, 11 ms pulse, 100 pulses Nonoperating 25 G, 170 inches/sec delta V
Vibration	2.2 Grms, 10 minutes per axis on all three axes

Accessories

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

IPS-4260 accessories kit contains the following:

- DB25 connector
- DB9 connector
- Rack mounting kit—screws, washers, and metal bracket
- RJ45 console cable
- Two 6-ft Ethernet cables

Rack Mounting

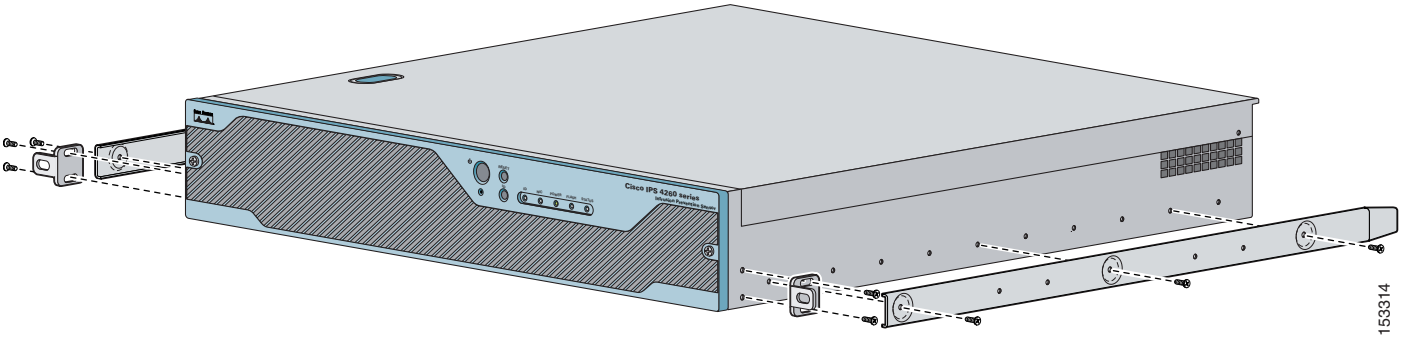
You can rack mount IPS-4260 in a 2- or 4-post rack. This section describes how to rack mount IPS-4260 and contains the following topics:

- Installing IPS-4260 in a 4-Post Rack, page 5-9
- Installing IPS-4260 in a 2-Post Rack, page 5-12

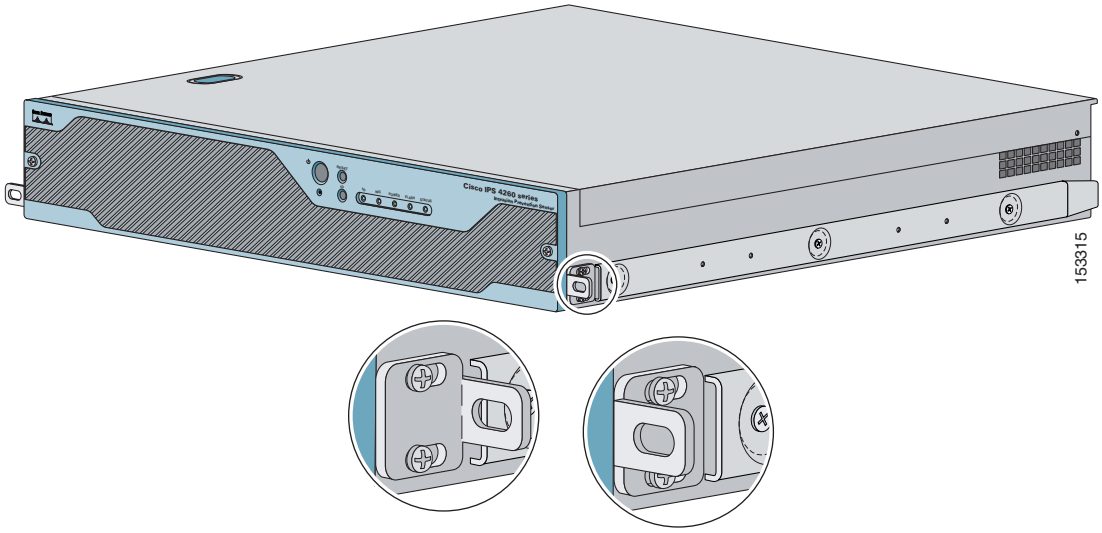
Installing IPS-4260 in a 4-Post Rack

To rack mount IPS-4260 in a 4-post rack, follow these steps:

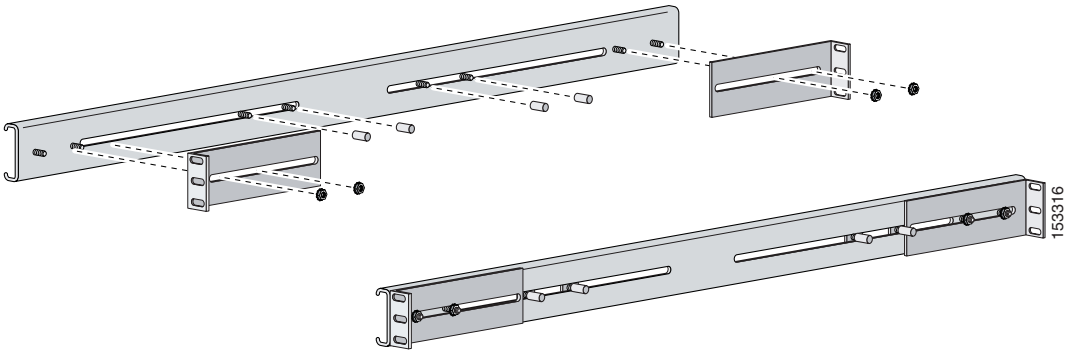
Step 1 Attach each inner rail to each side of the chassis with three 8-32x1/4” SEMS screws.



Step 2 Attach the front-tab mounting bracket to the chassis with two 8-32x1/4' SEMS screws. You can flip the bracket to push the system forward in the rack.

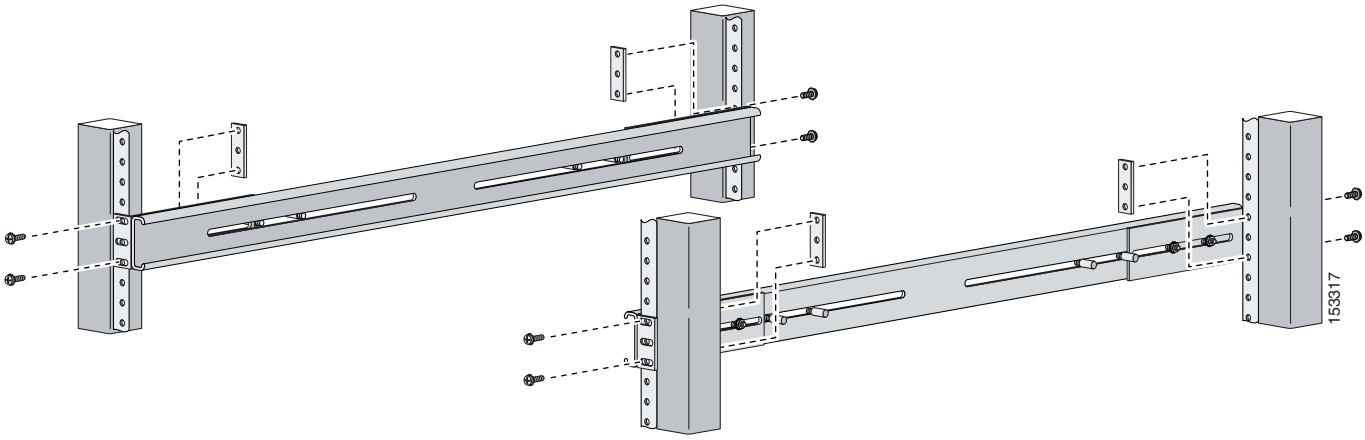


Step 3 Using the four inner studs, install the mounting brackets to the outer rail with four 8-32 KEPS nuts. Insert four thread covers over the four outer studs on each side.

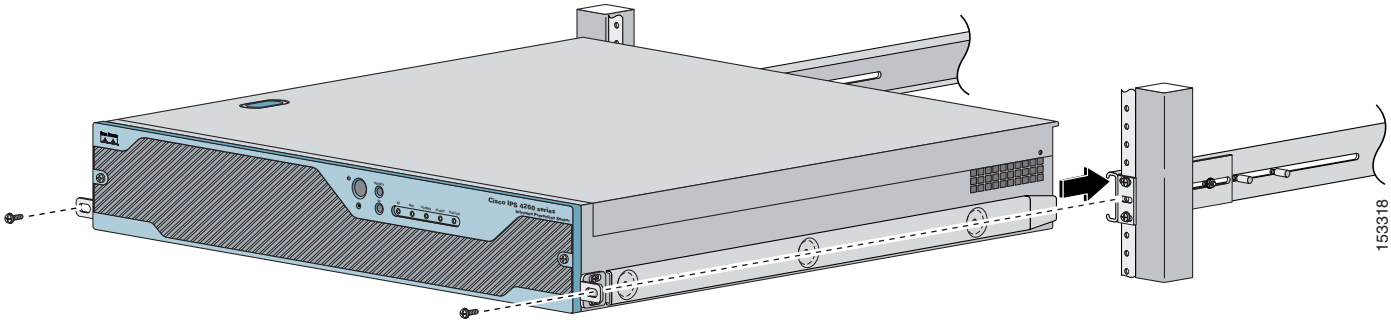


Step 4 Install the two outer rail subassemblies in the rack using eight 10-32x1/2” SEMS screws. You can use four bar nuts if necessary.

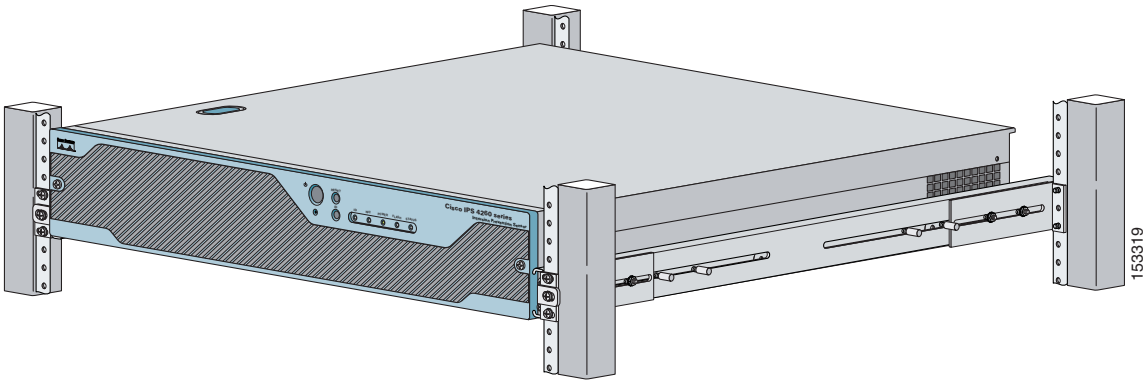
Note Adjust the mounting brackets based on rack depth.



Step 5 Slide IPS-4260 into the rack making sure the inner rail is aligned with the outer rail.



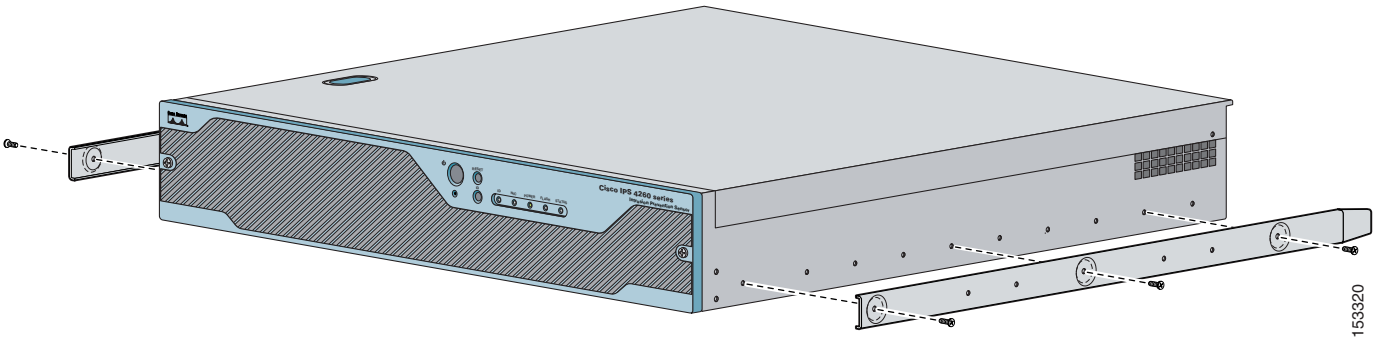
Step 6 Install two 10-32x1/2” SEMS screws to hold the front-tab mounting bracket to the rail.



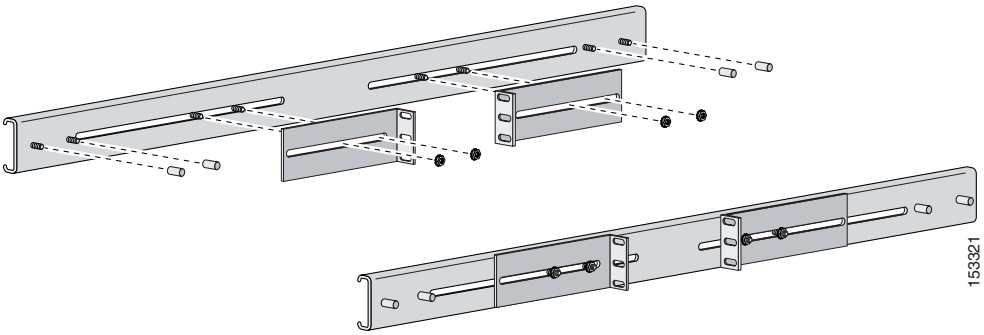
Installing IPS-4260 in a 2-Post Rack

To rack mount IPS-4260 in a 2-post rack, follow these steps:

Step 1 Attach the inner rail to each side of the chassis with three 8-32x1/4” SEMS screws.

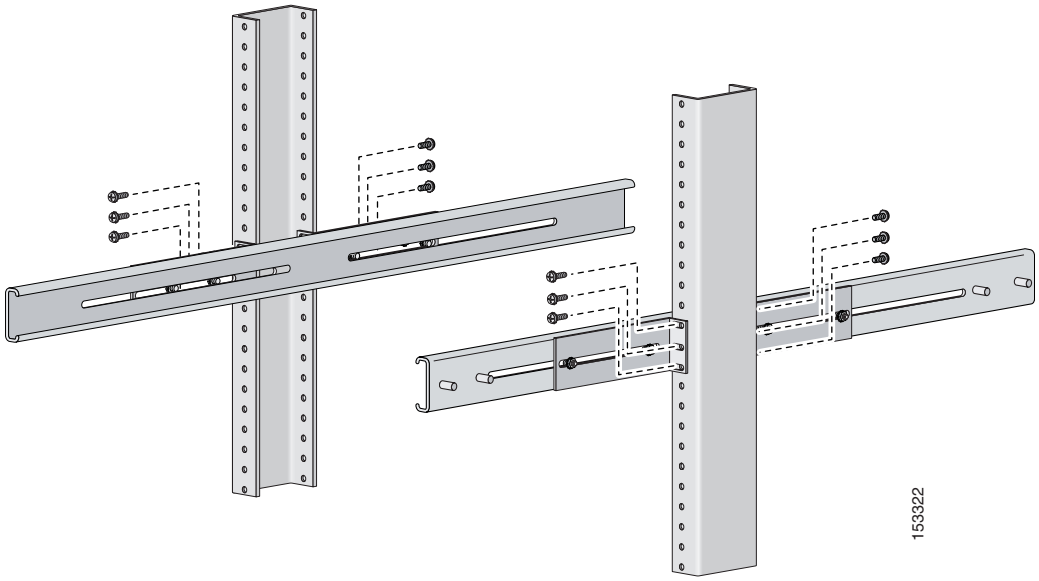


Step 2 Using the four inner studs, install the mounting brackets to the outer rail with four 8-32 KEPS nuts. Insert four thread covers over the four outer studs on each side.

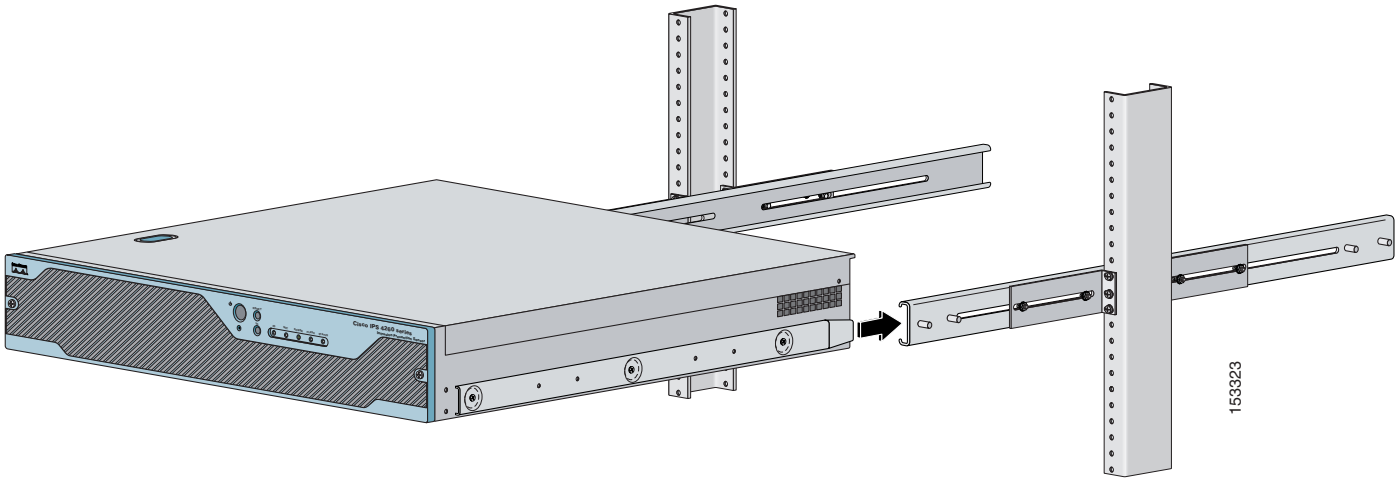


Step 3 Install the two outer rail subassemblies in the rack using twelve 10-32x1/2” SEMS screws or whatever rack hardware is necessary.

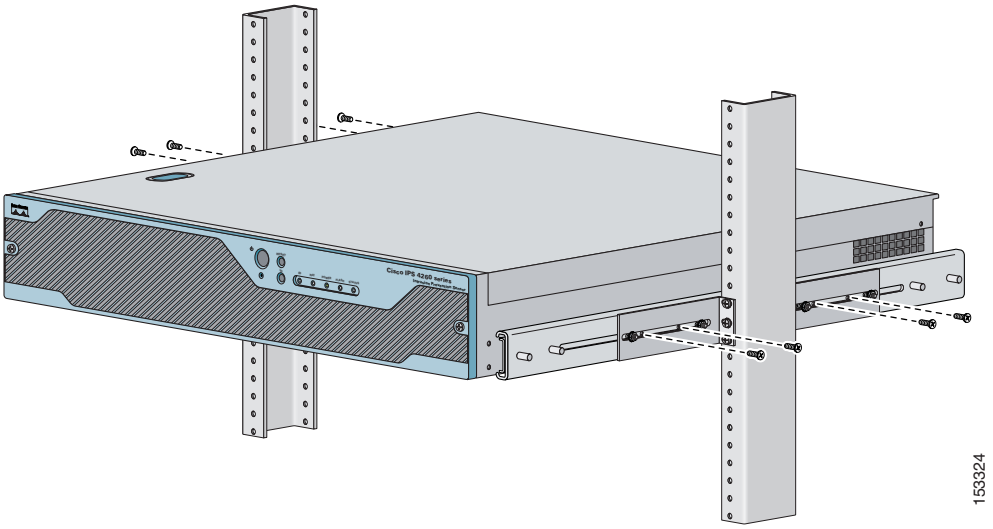
Note Adjust the mounting brackets based on the rack-channel depth.



Step 4 Slide IPS-4260 into the rack making sure the inner rail is aligned with the outer rail.



Step 5 Install four 8-32x7/16” SEMS screws through the clearance slots in the side of each outer rail assembly into the inner rail.



Installing IPS-4260

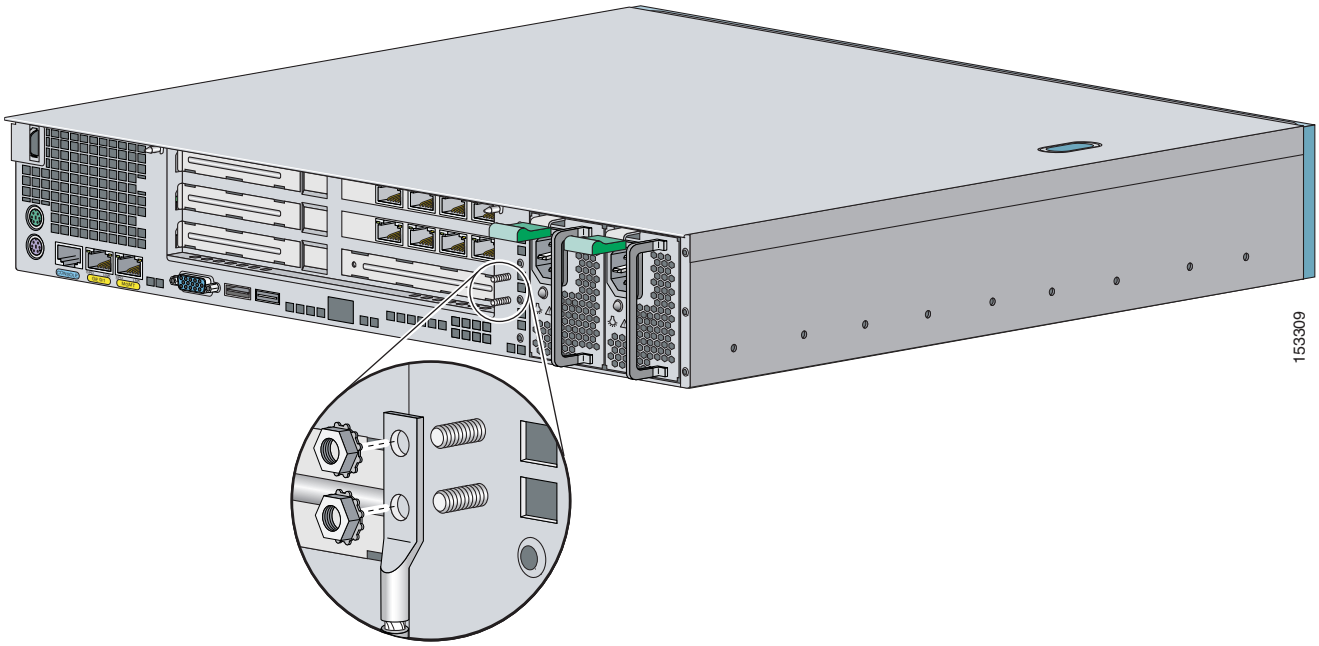
Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*. For more information on working with electrical power and in an ESD environment, see Site and Safety Guidelines, page 1-23.

To install IPS-4260 on the network, follow these steps:

Step 1 Position IPS-4260 on the network.

Step 2 Attach the grounding lugs to the back of IPS-4260.



Note Use 8-32 locknuts to connect a copper standard barrel grounding lug to the holes. The appliance requires a lug where the distance between the center of each hole is 0.56 inches. The ground lug must be NRTL listed or recognized. In addition, the copper conductor (wires) must be used and the copper conductor must comply with the NEC code for ampacity. A lug is not supplied with the appliance.

Step 3 Place IPS-4260 in a rack, if you are rack mounting it.

For the procedure, see Rack Mounting, page 5-9.

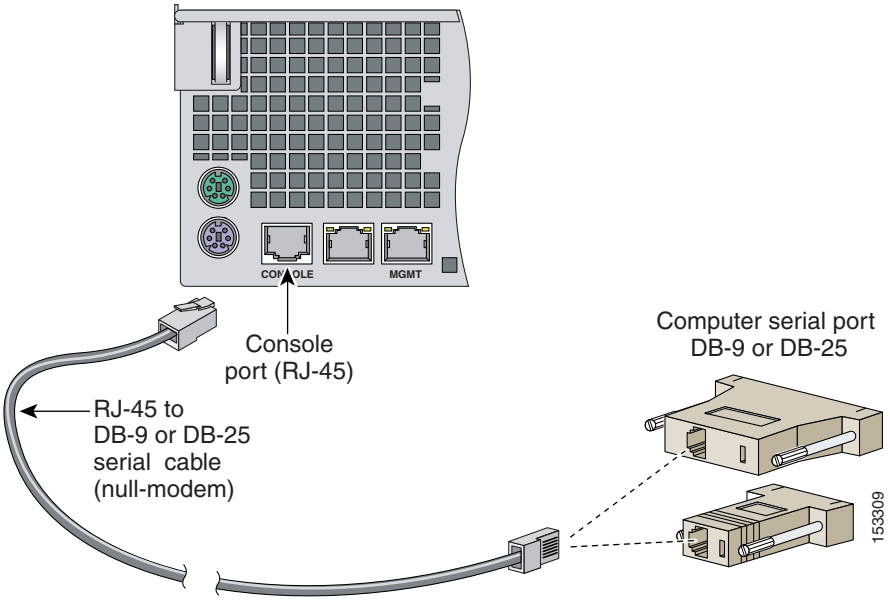
Step 4 Attach the power cord to IPS-4260 and plug it in to a power source (a UPS is recommended).

Step 5 Connect the cable as shown in Step 6 so that you have either a DB-9 or DB-25 connector on one end as required by the serial port for your computer, and the other end is the RJ-45 connector.

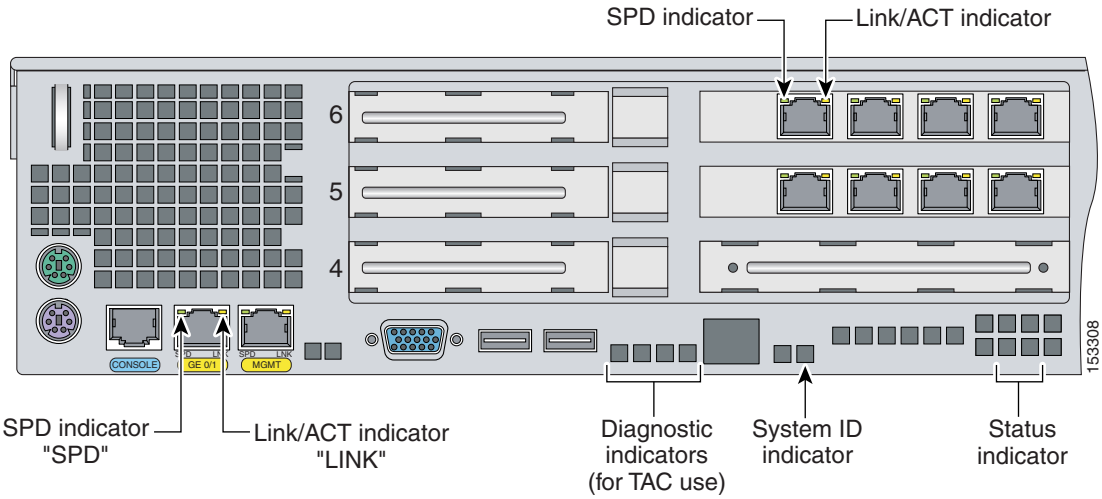
Note Use the console port to connect to a computer to enter configuration commands. Locate the serial cable from the accessory kit. The serial cable assembly consists of a 180/rollover cable with RJ-45 connectors (DB-9 connector adapter PN 74-0495-01 and DB-25 connector adapter PN 29-0810-01).

Note You can use a 180/rollover or straight-through patch cable to connect the appliance to a port on a terminal server with RJ-45 or hydra cable assembly connections. Connect the appropriate cable from the console port on the appliance to a port on the terminal server. For the instructions for setting up a terminal server, see Setting Up a Terminal Server, page 1-14.

Step 6 Connect the RJ-45 connector to the console port and connect the other end to the DB-9 or DB-25 connector on your computer.



Step 7 Attach the network cables.



IPS-4260 has the following interfaces:

- GigabitEthernet0/1 (GE 0/1) is the sensing port.
- Management0/0 (MGMT) is the command and control port.
- GigabitEthernet2/0 through GigabitEthernet2/3 and GigabitEthernet3/0 through 3/3 are the additional expansion port slots.

Caution Management and console ports are privileged administrative ports. Connecting them to an untrusted network can create security concerns.

Step 8 Power on IPS-4260.

Step 9 Initialize IPS-4260.

For the procedure, see Initializing the Sensor, page 10-2.

Step 10 Upgrade IPS-4260 with the most recent Cisco IPS software.

For the procedure, see Obtaining Cisco IPS Software, page 11-1.

You are now ready to configure intrusion prevention on IPS-4260.

For More Information

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

Removing and Replacing the Chassis Cover

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 120 VAC, 20 A U.S. (240 VAC, 16-20 A International). Statement 1005**

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024**

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Statement 1029**

Warning **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit. Statement 1028**

Caution Follow proper safety procedures when removing and replacing the chassis cover by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*.

Note Removing the appliance chassis cover does not affect your Cisco warranty. Upgrading IPS-4260 does not require any special tools and does not create any radio frequency leaks.

To remove and replace the chassis cover, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IPS-4260 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down IPS-4260 using IDM. For the procedure, refer to Resetting the Appliance.

Step 3 Power off IPS-4260.

Step 4 Remove the power cord and other cables from IPS-4260.

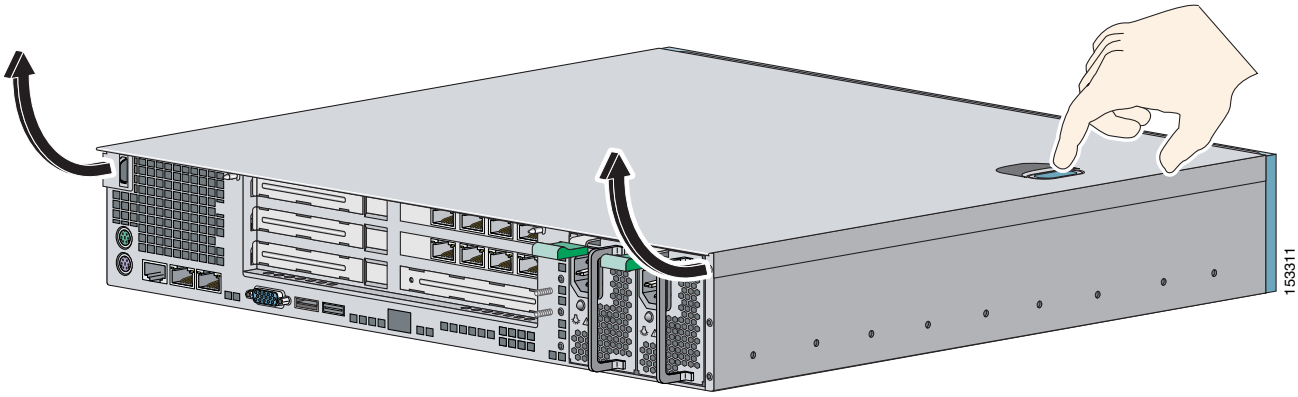
Step 5 If rack-mounted, remove IPS-4260 from the rack.

For the procedure, see Rack Mounting, page 5-9.

Step 6 Place IPS-4260 in an ESD-controlled environment.

For more information, see Working in an ESD Environment, page 1-25.

Step 7 Press the blue button on the top of the chassis cover and slide the chassis cover back.



Caution Do not operate IPS-4260 without the chassis cover installed. The chassis cover protects the internal components, prevents electrical shorts, and provides proper air flow for cooling the electronic components.

Step 8 To replace the chassis cover, position it at the back of the chassis and slide it on until it snaps into place.

Step 9 Reattach the power cord and other cables to IPS-4260.

For the procedure, see Installing IPS-4260, page 5-14.

Step 10 Reinstall IPS-4260 on a rack, desktop, or table.

If you are reinstalling in a rack, see Rack Mounting, page 5-9.

Step 11 Power on IPS-4260.

Installing and Removing PCI Cards

IPS-4260 has 6 expansion card slots, three full-height and three half-height slots. You can install the optional network interface cards in the two top full-height slots, slots 2 and 3. IPS-4260 supports up to two network interface cards. For an illustration of the expansion card slots, see Figure 5-5 on page 5-7. For an illustration of the supported PCI cards, see Supported PCI Cards, page 5-2.

Note We recommend that you install the 4GE bypass interface card in slot 2 if you are installing only one 4GE bypass card. This improves accessibility to the RJ45 cable connectors.

To install and remove PCI cards, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IPS-4260 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

Note You can also power down IPS-4260 using IDM. For the procedure, refer to Resetting the Appliance.

Step 3 Power off IPS-4260.

Step 4 Remove the power cord and other cables from IPS-4260.

Step 5 If rack-mounted, remove IPS-4260 from the rack.

For the procedure, see Rack Mounting, page 5-9.

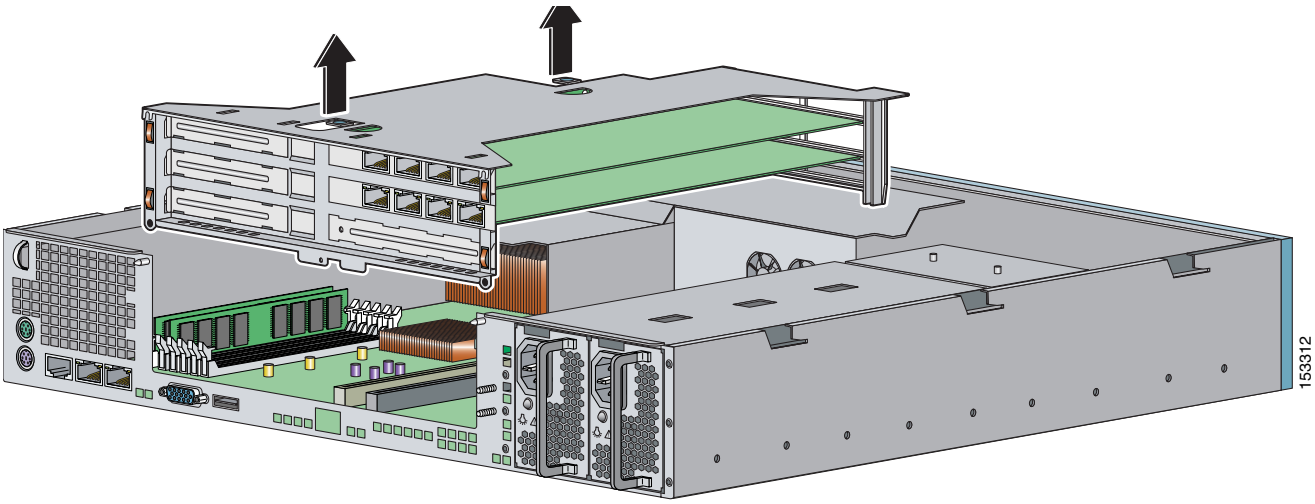
Step 6 Place IPS-4260 in an ESD-controlled environment.

For more information, see Working in an ESD Environment, page 1-25.

Step 7 Remove the chassis cover.

For the procedure, see Removing and Replacing the Chassis Cover, page 5-17.

Step 8 Remove the card carrier by pulling up on the two blue release tabs. Use equal pressure and lift the card carrier out of the chassis.

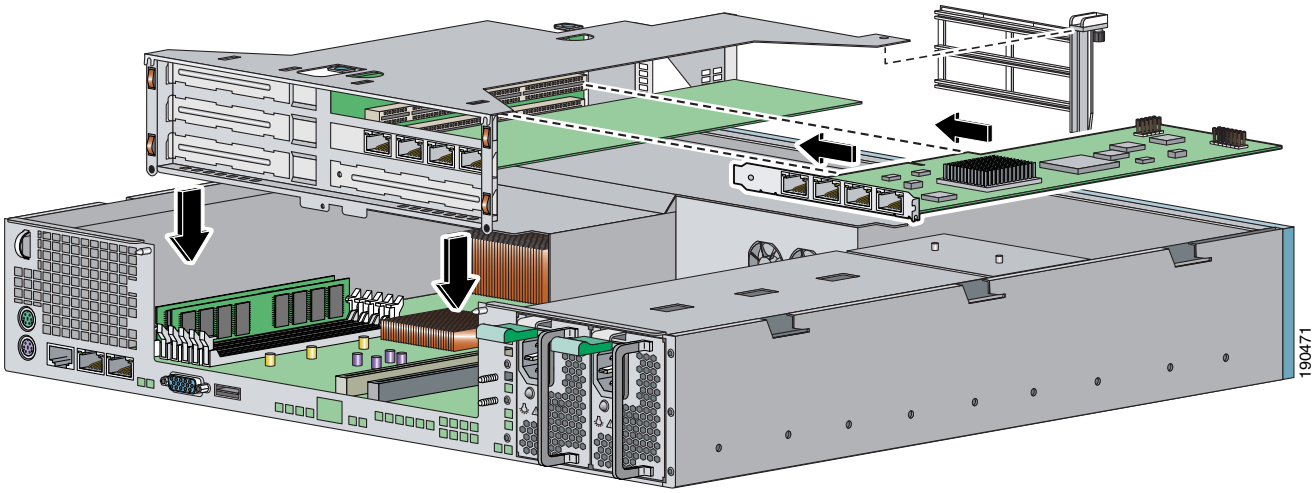


Step 9 With a screw driver, remove the screw from the desired slot cover.

Step 10 Remove the slot cover by pressing on it from inside the chassis.

If the card is full length, use a screw driver to remove the blue thumb screw from the card support at the back of the card carrier.

Step 11 Carefully align the PCI card with the PCI-Express connector and alignment grooves for the appropriate slot. Apply firm even pressure until the card is fully seated in the connector.



Step 12 Reinstall the slot cover screw to hold the card to the carrier. If necessary, reinstall the card support at the back of the card carrier.

Step 13 Replace the card carrier in the chassis.

Step 14 Replace the chassis cover.

Installing and Removing the Power Supply

IPS-4260 ships with one power supply, but you can order it with two power supplies so that you have a redundant power supply.

To install and remove power supplies, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare IPS-4260 to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

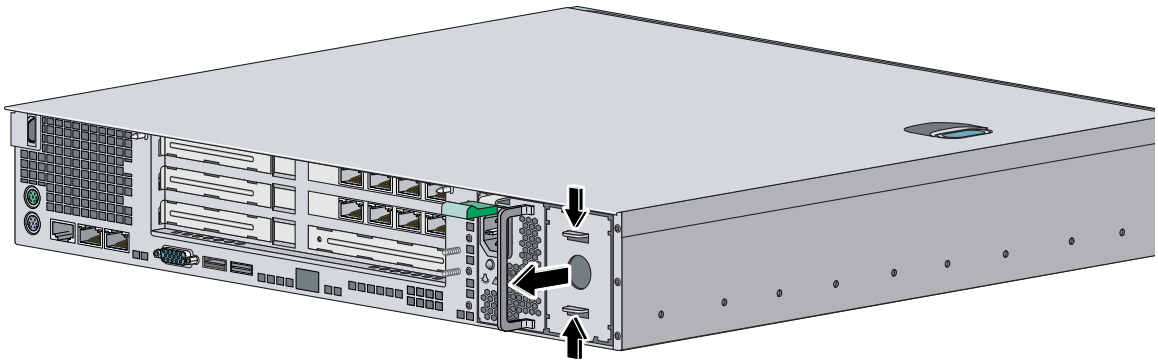
Note You can also power down IPS-4260 using IDM. For the procedure, refer to Resetting the Appliance.

Step 3 Power off IPS-4260.

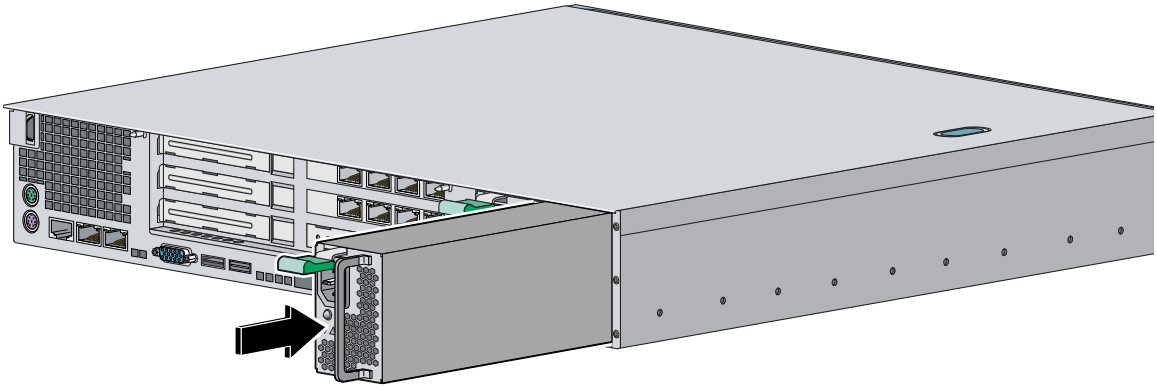
Step 4 Remove the power cord and other cables from IPS-4260.

Note Power supplies are hot-swappable. You can replace a power supply while IPS-4260 is running, if you are replacing a redundant power supply.

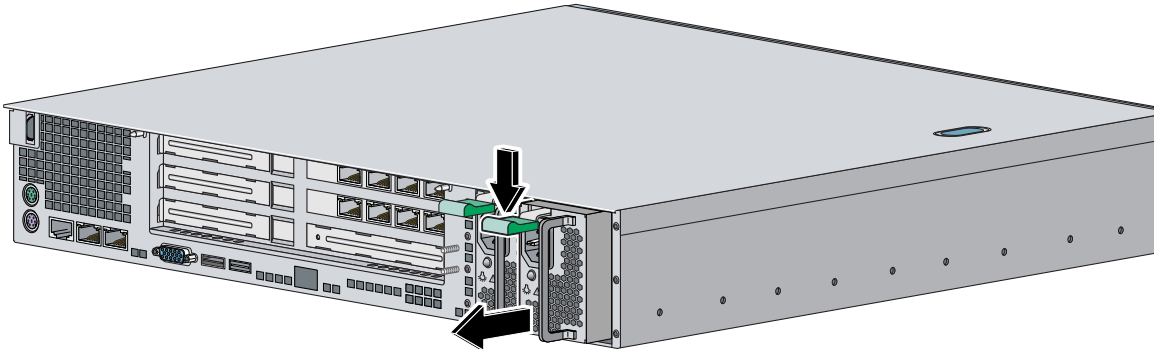
Step 5 Squeeze the tabs to remove the filler plate.



Step 6 Install the power supply.



Step 7 To remove the power supply, push down the green tab and pull out the power supply.



Step 8 After installing or removing the power supply, replace the power cord and other cables.

Step 9 Power on IPS-4260.

CHAPTER 6

Installing IPS-4240 and IPS-4255

This chapter describes IPS-4240 and IPS-4255 and how to install them. It also describes the accessories and how to install them. This chapter contains the following sections:

Introducing IPS-4240 and IPS-4255

IPS-4240 and IPS-4255 deliver high port density in a small form factor. They use a compact flash device for storage rather than the hard-disk drives used in other sensor models.

IPS-4240 monitors up to 250 Mbps of aggregate network traffic on multiple sensing interfaces and is inline ready. It replaces IDS-4235. There are four 10/100/1000 copper sensing interfaces.

Note The 250-Mbps performance for IPS-4240 is based on the following conditions: 2500 new TCP connections per second, 2500 HTTP transactions per second, average packet size of 445 bytes, and the system running Cisco IPS 5.1 software. The 250-Mbps performance is traffic combined from all four sensing interfaces.

IPS-4255 monitors up to 600 Mbps of aggregate network traffic on multiple sensing interfaces and is also inline ready. It replaces IDS-4250-TX. There are four 10/100/1000 copper sensing interfaces.

Note IDS-4250-SX and the IDS-4250-XL are not being replaced by IPS-4255 at this time.

Note The 600-Mbps performance for IPS-4255 is based on the following conditions: 6000 new TCP connections per second, 6000 HTTP transactions per second, average packet size of 445 bytes, and the system running Cisco IPS 5.1 software. The 600-Mbps performance is traffic combined from all four sensing interfaces.

Note IPS-4240 and the IPS-4255 do not support redundant power supplies.

Note IPS-4240 is available with either AC or DC power.

Front and Back Panel Features

This section describes the IPS-4240 and IPS-4255 front and back panel features and indicators.

Note Although the graphics show IPS-4240, the IPS-4255 has the same front and back panel features and indicators.

Figure 6-1 shows the front view of IPS-4240 and IPS-4255.

Figure 6-1 IPS-4240/IPS-4255 Front Panel Features

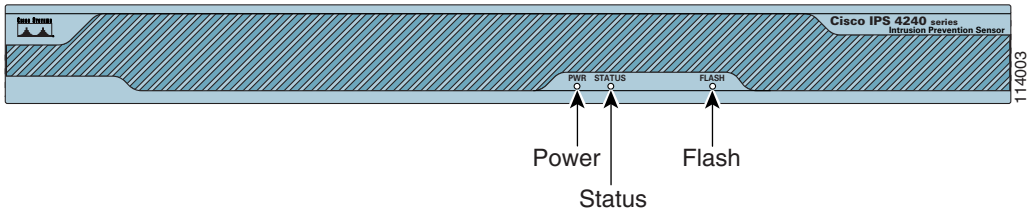


Table 6-1 describes the front panel indicators on IPS-4240 and IPS-4255.

Table 6-1 Front Panel Indicators

Indicator	Description
Power	Off indicates no power. Green when the power supply is running.
Status	Blinks green while the power-up diagnostics are running or the system is booting. Solid green when the system has passed power-up diagnostics. Solid amber when the power-up diagnostics have failed.
Flash	Off when the compact flash device is not being accessed. Blinks green when the compact flash device is being accessed.

Figure 6-2 shows the back view of the IPS-4240 and IPS-4255.

Figure 6-2 IPS-4240 and IPS-4255 Back Panel Features

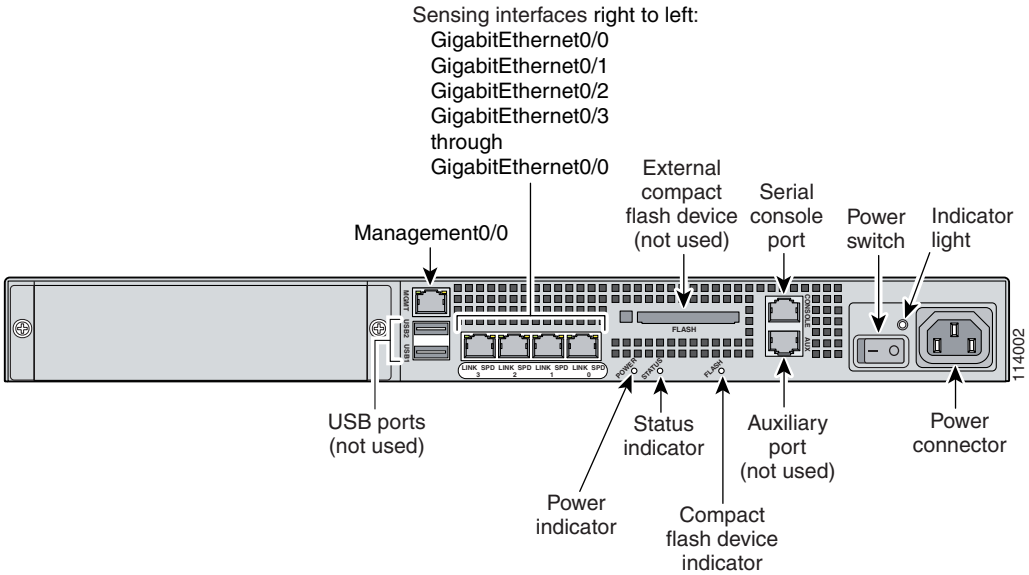


Figure 6-3 shows the four built-in Ethernet ports, which have two indicators per port.

Figure 6-3 Ethernet Port Indicators

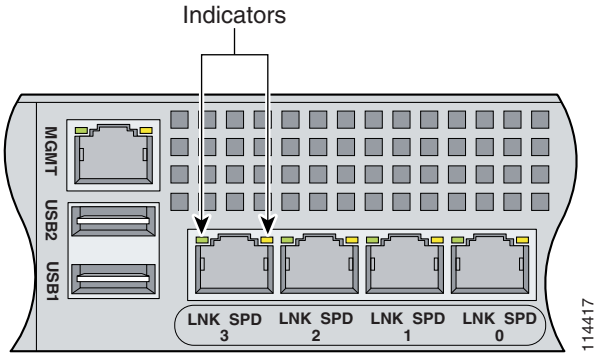


Table 6-2 lists the back panel indicators.

Table 6-2 Back Panel Indicators

Indicator	Color	Description
Left side	Green solid Green blinking	Physical link Network activity
Right side	Not lit Green Amber	10 Mbps 100 Mbps 1000 Mbps

Specifications

Table 6-3 lists the specifications for IPS-4240 and IPS-4255.

Table 6-3 IPS-4240 and IPS-4255 Specifications

Dimensions and Weight	
Height	1.75 in. (4.45 cm)
Width	17.5 in. (44.45 cm)
Depth	14.5 in. (36.83 cm)
Weight	20.0 lb (9.07 kg)
Form factor	1 RU, standard 19-inch rack-mountable
Expansion	One chassis expansion slot (not used)
Power	
Autoswitching	100V to 240V AC
Frequency	47 to 63 Hz, single phase
Operating current	3.0 A
Steady state	150 W
Maximum peak	190 W
Maximum heat dissipation	648 BTU/hr, full power usage (65 W)
Environment	
Temperature	Operating +32°F to +104°F (+0°C to +40°C) Nonoperating -13°F to +158°F (-25°C to +70°C)
Relative humidity	Operating 5% to 95% (noncondensing) Nonoperating 5% to 95% (noncondensing)
Altitude	Operating 0 to 9843 ft (3000 m) Nonoperating 0 to 15,000 ft (4750 m)
Shock	Operating 1.14 m/sec (45 in./sec) ½ sine input Nonoperating 30 G
Vibration	0.41 Grms2 (3 to 500 Hz) random input
Acoustic noise	60 dBa (maximum)

Connecting IPS-4240 to a Cisco 7200 Series Router

When an IPS-4240 is connected directly to a 7200 series router and both the IPS-4240 and the router interfaces are hard-coded to speed 100 with duplex Full, the connection does not work. If you set IPS-4240 to speed Auto and duplex Auto, it connects to the router but only at speed 100 and duplex Half.

To connect correctly at speed 100 and duplex Full, set the interfaces of both IPS-4240 and the router to speed Auto and duplex Auto. Also, if either interface is hard-coded, you must make the connection using a crossover cable.

Accessories

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

IPS-4240 and IPS-4255 accessories kit contains the following:

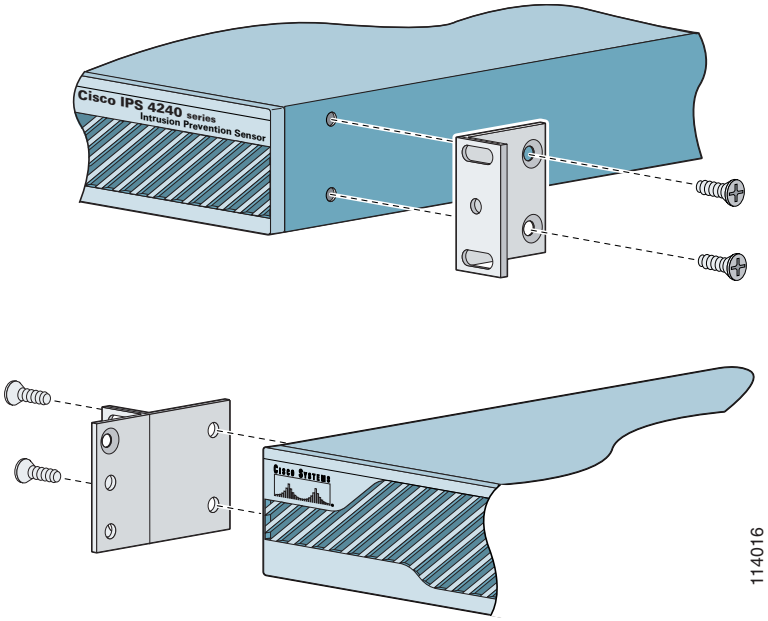
- DB25 connector
- DB9 connector
- Rack mounting kit—screws, washers, and metal bracket
- RJ45 console cable
- Two 6-ft Ethernet cables

Rack Mounting

To rack mount IPS-424 and IPS-4255, follow these steps:

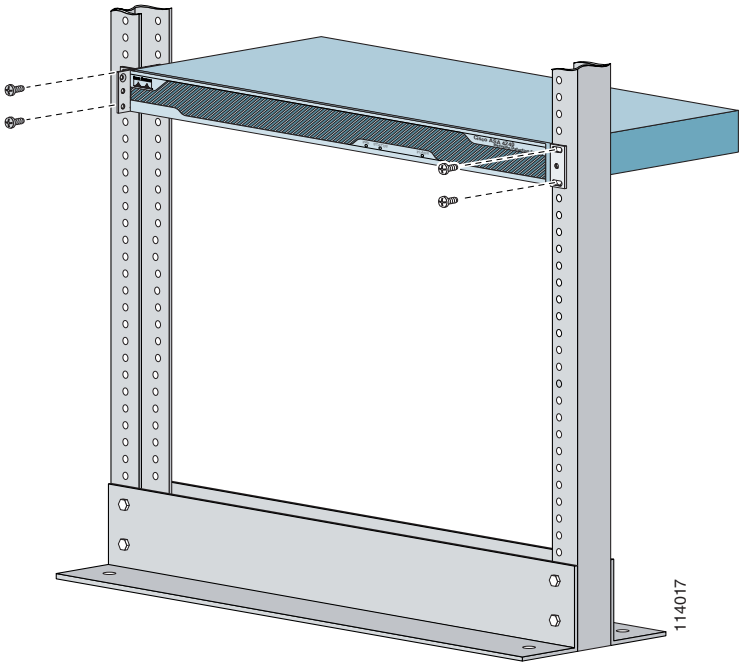
Step 1 Attach the bracket to the appliance using the supplied screws.

You can attach the brackets to the holes near the front of the appliance.



Note The top hole on the left bracket is a banana jack you can use for ESD grounding purposes when you are servicing the system. You can use the two threaded holes to mount a grounding lug to ground the chassis.

Step 2 Use the supplied screws to attach the appliance to the equipment rack.



Step 3 To remove the appliance from the rack, remove the screws that attach the appliance to the rack, and then remove the appliance.

Installing IPS-4240 and IPS-4255

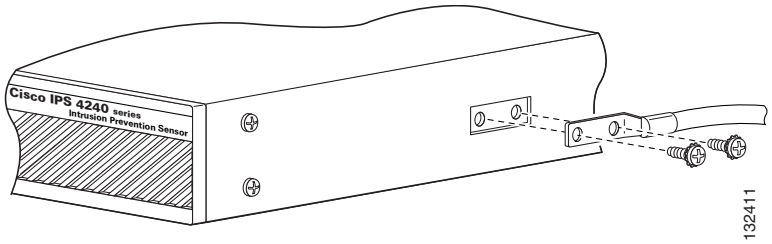
Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Follow proper safety procedures when performing these steps by reading the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*. For more information on working with electrical power and in an ESD environment, see Site and Safety Guidelines, page 1-23.

To install IPS-4240 and IPS-4255 on the network, follow these steps:

Step 1 Position the appliance on the network.

Step 2 Attach the grounding lug to the side of the appliance.



Note Use 8-32 screws to connect a copper standard barrel grounding lug to the holes. The appliance requires a lug where the distance between the center of each hole is 0.56 inches. The ground lug must be NRTL listed or recognized. In addition, the copper conductor (wires) must be used and the copper conductor must comply with the NEC code for ampacity. A lug is not supplied with the appliance.

Step 3 Place the appliance in a rack, if you are rack mounting it.

For the procedure, see Rack Mounting, page 6-5.

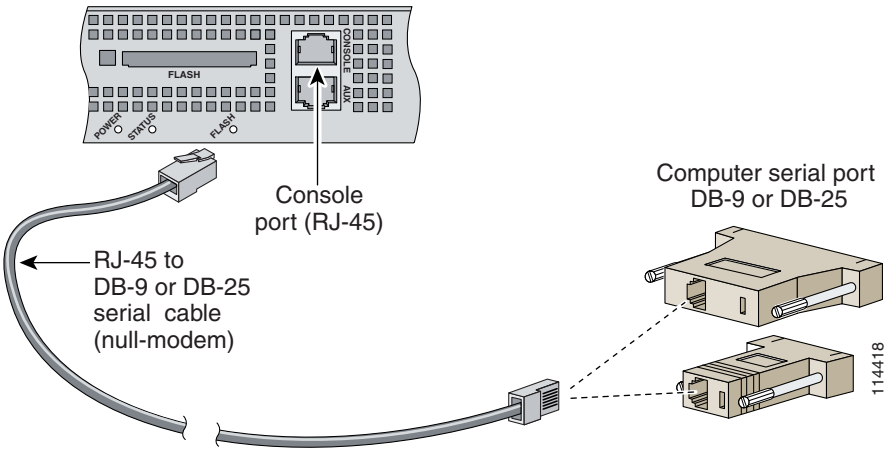
Step 4 Attach the power cord to the appliance and plug it in to a power source (a UPS is recommended).

Step 5 Connect the cable as shown in Step 6 so that you have either a DB-9 or DB-25 connector on one end as required by the serial port for your computer, and the other end is the RJ-45 connector.

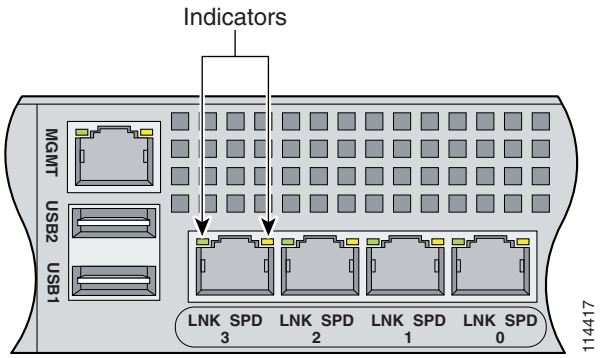
Note Use the console port to connect to a computer to enter configuration commands. Locate the serial cable from the accessory kit. The serial cable assembly consists of a 180/rollover cable with RJ-45 connectors (DB-9 connector adapter PN 74-0495-01 and DB-25 connector adapter PN 29-0810-01).

Note You can use a 180/rollover or straight-through patch cable to connect the appliance to a port on a terminal server with RJ-45 or hydra cable assembly connections. Connect the appropriate cable from the console port on the appliance to a port on the terminal server. For the instructions for setting up a terminal server, see Setting Up a Terminal Server, page 1-14.

Step 6 Connect the RJ-45 connector to the console port and connect the other end to the DB-9 or DB-25 connector on your computer.



Step 7 Attach the network cables.



IPS-4240 and IPS-4255 have the following interfaces:

- GigabitEthernet0/0, GigabitEthernet0/1, GigabitEthernet0/2, and GigabitEthernet0/3 (from right to left) are sensing ports.
- Management0/0 is the command and control port.

Caution Management and console ports are privileged administrative ports. Connecting them to an untrusted network can create security concerns.

Step 8 Power on the appliance.

Step 9 Initialize the appliance.

For the procedure, see Initializing the Sensor, page 10-2.

Step 10 Upgrade the appliance with the most recent Cisco IPS software.

For the procedure, see Obtaining Cisco IPS Software, page 11-1.

You are now ready to configure intrusion prevention on the appliance.

If you have the IPS-4240 DC model, see Installing IPS-4240-DC, page 6-9.

For More Information

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

Installing IPS-4240-DC

The IPS-4240-DC-K9 (NEBS-compliant) model equipped with DC-input power supply 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.

DC power guidelines are listed in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*. For more information on working with electrical power and in an ESD environment, see Site and Safety Guidelines, page 1-23.

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

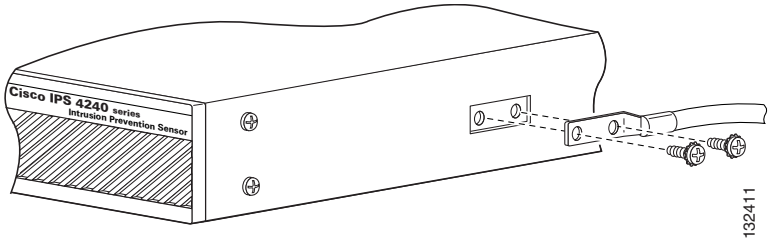
Note The DC return connection should remain isolated from the system frame and chassis (DC-I). This equipment is suitable for connection to intra-building wiring only.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

To install IPS-4240-DC, follow these steps:

Step 1 Position IPS-4240-DC on the network.

Step 2 Attach the grounding lug to the side of the appliance.



Note Use 8-32 screws to connect a copper standard barrel grounding lug to the holes. The appliance requires a lug where the distance between the center of each hole is 0.56 inches. The ground lug must be NRTL listed or recognized. In addition, the copper conductor (wires) must be used and the copper conductor must comply with the NEC code for ampacity. A lug is not supplied with the appliance.

Step 3 Place the appliance in a rack, if you are rack mounting it.

For the procedure, see Rack Mounting, page 6-5.

Step 4 Terminate 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.

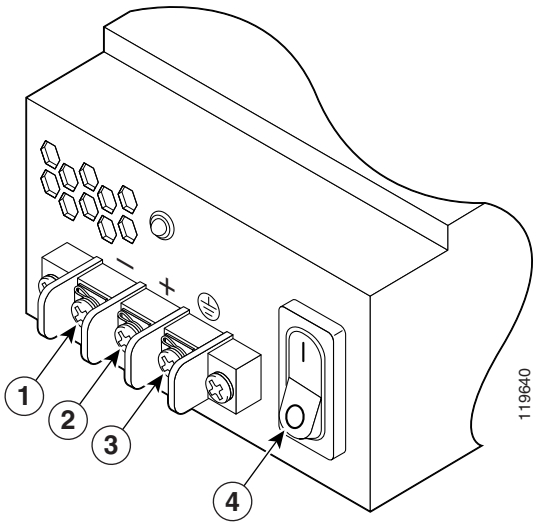
Step 5 Locate the DC-input terminal box.

Step 6 Power off IPS-4240-DC.

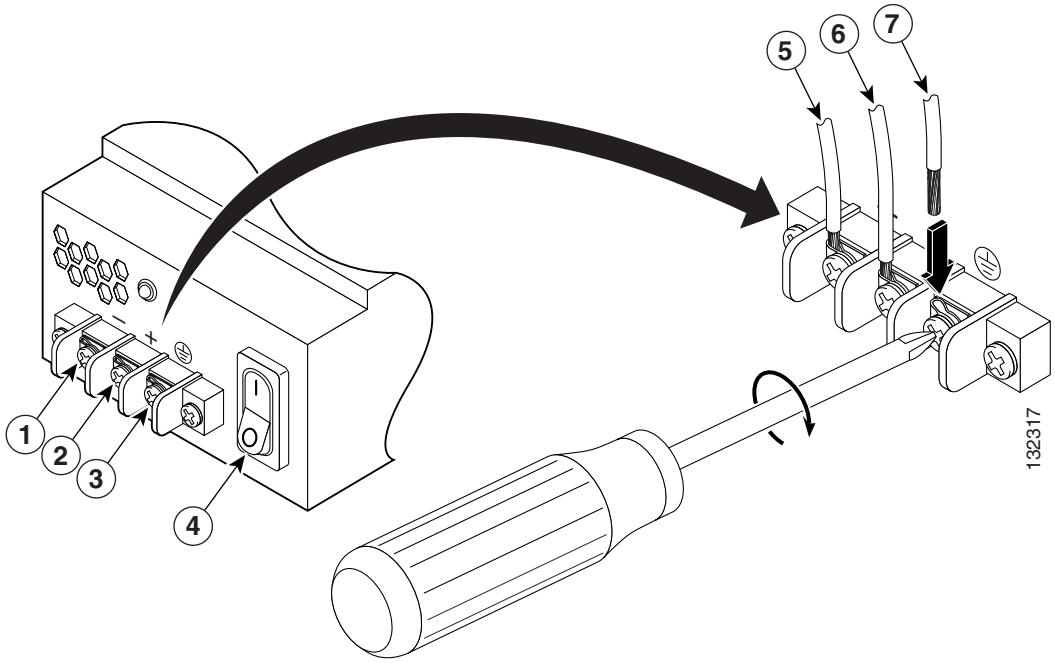
Make sure that power is removed from the DC circuit. To make sure all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

Step 7 Remove the DC power supply plastic shield.

Step 8 Strip the ends of the wires for insertion into the power connect lugs on IPS-4240-DC.



Step 9 Insert the ground wire into the connector for the earth ground and tighten the screw on the connector. Using the same method as for the ground wire, connect the negative wire and then the positive wire.



1	Negative	**5**	Negative
2	Positive	**6**	Positive
3	Ground	**7**	Ground
4	On/Off Switch		

Note The DC return connection to this system is to remain isolated from the system frame and chassis.

Step 10 After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.

Step 11 Replace the DC power supply plastic shield.

Step 12 Power on IPS-4240-DC from the switch at the back of the chassis.

Note If you need to power cycle IPS-4240-DC, wait at least 5 seconds between powering it off and powering it back on.

Step 13 Initialize IPS-4240-DC.

For the procedure, see Initializing the Sensor, page 10-2.

Step 14 Upgrade IPS-4240-DC with the most recent Cisco IPS software.

For the procedure, see Obtaining Cisco IPS Software, page 11-1.

You are now ready to configure intrusion prevention on the appliance.

For More Information

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

CHAPTER 7

Installing AIP-SSM

This chapter describes how to install AIP-SSM. It contains the following sections:

Specifications

Table 7-1 lists the specifications for AIP-SSM:

Table 7-1 AIP-SSM Specifications

Specification	Description
Dimensions (H x W x D)	1.70 x 6.80 x 11.00 inches
Weight	Minimum: 2.50 lb Maximum: 3.00 lb[1]
Operating temperature	+32° to +104°F (+0° to +40°C)
Nonoperating temperature	–40° to +167°F (–40° to +75°C)
Humidity	10% to 90%, noncondensing

1. 2.70 lbs for 45 c heatsink, approximately 3.00 lbs for the 55c maximum

Memory Specifications

Table 7-2 lists the memory specifications for AIP-SSM.

Table 7-2 AIP-SSM Memory Specifications

Model	CPU	DRAM
ASA-SSM-AIP-10-K9	2.0 GHz Celeron	1.0 GB
ASA-SSM-AIP-20-K9	2.4 GHz Pentium 4	2.0 GB

Hardware and Software Requirements

AIP-SSM has the following hardware and software requirements:

- Cisco ASA 5500 series adaptive security appliance
  - ASA 5510 (ASA-SSM-AIP-10-K9 and ASA-SSM-AIP-20-K9)
  - ASA 5520 (ASA-SSM-AIP-10-K9 and ASA-SSM-AIP-20-K9)
  - ASA 5540 (ASA-SSM-AIP-20-K9)
- Cisco Adaptive Security Appliance Software 7.0 or higher
- Cisco Intrusion Prevention System Software 5.0(2) or higher
- DES or 3DES-enabled

Indicators

Figure 7-1 shows the AIP-SSM indicators.

Figure 7-1 AIP-SSM Indicators

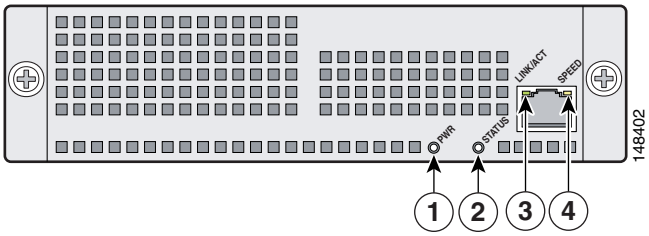


Table 7-3 describes the AIP-SSM indicators.

Table 7-3 AIP-SSM Indicators

	LED	Color	State	Description
1	PWR	Green	On	The system has power.
2	STATUS	Green	Flashing	The system is booting.
			Solid	The system has passed power-up diagnostics.
3	LINK/ACT	Green	Solid	There is Ethernet link.
			Flashing	There is Ethernet activity.
4	SPEED	Green	100 MB	There is network activity.
		Amber	1000 MB (GigabitEthernet)	There is network activity.

Installation and Removal Instructions

This section describes how to install and remove AIP-SSM, and contains the following topics:

Installing AIP-SSM

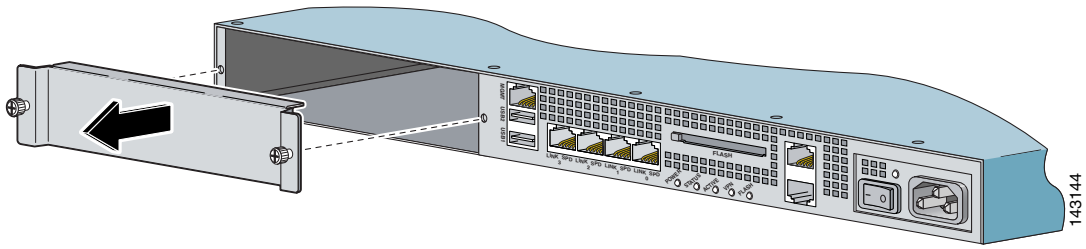
To install AIP-SSM, follow these steps:

Step 1 Power off ASA.

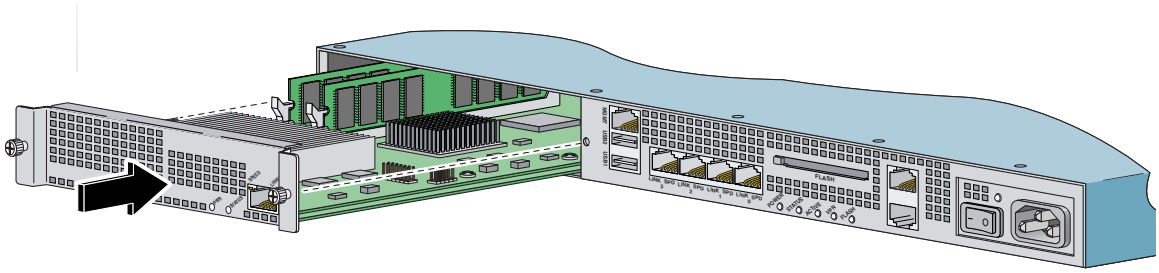
Step 2 Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.

For more information, see Working in an ESD Environment, page 1-25.

Step 3 Remove the two screws at the left back end of the chassis, and remove the slot cover.



Step 4 Insert AIP-SSM through the slot opening.



Step 5 Attach the screws to secure AIP-SSM to the chassis.

Step 6 Power on ASA by pushing the power switch at the back of the chassis.

Step 7 Check the indicators.

If AIP-SSM is properly installed, the POWER indicator is solid green and the STATUS indicator is flashing green. You can also verify that AIP-SSM is online using the **show module** command. For the procedure, see Verifying the Status of AIP-SSM, page 7-4.

Step 8 Initialize AIP-SSM.

For the procedure, see Initializing the Sensor, page 10-2.

Step 9 Install the most recent Cisco IPS software.

For the procedure, see Obtaining Cisco IPS Software, page 11-1.

Step 10 Configure AIP-SSM to receive IPS traffic.

For the procedure, refer to Sending Traffic to AIP-SSM.

For More Information

- For the procedure for using HTTPS to log in to IDM and ASDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

Verifying the Status of AIP-SSM

You can use the **show module 1** command to verify that AIP-SSM is up and running.

To verify the status of AIP-SSM, follow these steps:

Step 1 Log in to ASA.

Step 2 Verify the status of AIP-SSM:

```
asa# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         P2B000005D0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 000b.fcf8.0144 to 000b.fcf8.0144  0.2          1.0(9)0      5.0(0.27)S129.0

Mod Status
--- ------------------
  1 Up
asa#
```

If the status reads `Up`, AIP-SSM has been properly installed.

The following values are valid for the Status field:

- `Initializing`—AIP-SSM is being detected and the control communication is being initialized by the system.
- `Up`—AIP-SSM has completed initialization by the system.
- `Unresponsive`—The system encountered an error communicating with AIP-SSM.
- `Reloading`—AIP-SSM is reloading.
- `Shutting Down`—AIP-SSM is shutting down.

- `Down`—AIP-SSM is shut down.
- `Recover`—AIP-SSM is attempting to download a recovery image.

Removing AIP-SSM

To remove AIP-SSM, follow these steps:

Step 1 Shut down AIP-SSM:

```
asa# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm]
```

Step 2 Press **Enter** to confirm.

Step 3 Verify if AIP-SSM is down by checking the indicators.

Step 4 Power off ASA.

Step 5 Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.

For more information, see Working in an ESD Environment, page 1-25.

Step 6 Remove the two screws at the left back end of the chassis, and remove the slot cover.

Step 7 Remove AIP-SSM and set it aside.

Step 8 If you need to replace the existing AIP-SSM, insert the new AIP-SSM through the slot opening.

Note Do not replace AIP-SSM with a different model. The ASA will not recognize it.

Step 9 Attach the screws to secure AIP-SSM to the chassis.

Step 10 Power on ASA.

Step 11 Reset AIP-SSM:

```
asa# hw-module module 1 reset
Reset module in slot 1? [confirm]
```

Step 12 Press **Enter** to confirm.

Step 13 Check the indicators to see if AIP-SSM is properly installed.

If AIP-SSM is properly installed, the POWER indicator is solid green and the STATUS indicator is flashing green. Or you can verify installation using the **show module** command. For the procedure, see Verifying the Status of AIP-SSM, page 7-4.

CHAPTER 8

Installing IDSM-2

This chapter lists the software and hardware requirements of IDSM-2, and describes how to remove and install it.

This chapter contains the following sections:

Specifications

Table 8-1 lists the specifications for IDSM-2.

Table 8-1 IDSM-2 Specifications

Specification	Description
Dimensions (H x W x D)	1.18 x 15.51 x 16.34 in. (30 x 394 x 415 mm)
Weight	Minimum: 3 lb (1.36 kg) Maximum: 5 lb (2.27 kg)
Operating temperature	+32° to +104°F (+0° to +40°C)
Nonoperating temperature	–40° to +167°F (–40° to +75°C)
Humidity	10% to 90%, noncondensing

Software and Hardware Requirements

The following are the IDSM-2 software and hardware requirements:

- Catalyst software release 7.5(1) or later with Supervisor Engine 1A with MSFC2
- Catalyst software release 7.5(1) or later with Supervisor Engine 2 with MSFC2 or PFC2
- Cisco IOS software release 12.2(14)SY with Supervisor Engine 2 with MSFC2
- Cisco IOS software release 12.1(19)E or later with Supervisor Engine 2 with MSFC2
- Cisco IOS software release 12.1(19)E1 or later with Supervisor Engine 1A with MSFC2
- Cisco IOS software release 12.2(14)SX1 with Supervisor Engine 720
- Cisco IDS software release 4.0 or later
- Any Catalyst 6500 series switch chassis or 7600 router

Minimum Supported IDSM-2 Configurations

Note The following matrix is not intended to recommend any particular version, but rather lists the earliest supported versions.

Table 8-2 lists the minimum supported configurations for IDSM-2.

Table 8-2 Minimum Catalyst 6500 Software Version for IDSM-2 Feature Support

Catalyst/IDSM-2 Feature	Catalyst Software				Cisco IOS Software			
	Sup1	Sup2	Sup32	Sup720	Sup1	Sup2	Sup32	Sup720
SPAN	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
VACL capture[1]	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
ECLB with VACL capture[2]	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF1	12.2(18)SXE1
Inline interface pairs	8.4(1)	8.4(1)	8.4(1)	8.4(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXE1
ECLB with inline interface pairs	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
Inline VLAN pairs	8.4(1)	8.4(1)	8.4(1)	8.4(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
ECLB with inline VLAN pairs	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4

1. Requires PFC2/3 or MSFC2/3.
2. Requires PFC2/3 or MSFC2/3.

Using the TCP Reset Interface

The IDSM-2 has a TCP reset interface—port 1. The IDSM-2 has a specific TCP reset interface because it cannot send TCP resets on its sensing ports.

If you have reset problems with IDSM-2, try the following:

- If the sensing ports are access ports (a single VLAN), you need to configure the reset port to be in the same VLAN.
- If the sensing ports are dot1q trunk ports (multi-VLAN), the sensing ports and reset port all must have the same native VLAN, and the reset port must trunk all the VLANs being trunked by both the sensing ports.

Front Panel Features

IDSM-2 (Figure 8-1) has a status indicator and a Shutdown button.

Figure 8-1 IDSM-2 Front Panel

Table 8-3 describes the IDSM-2 states as indicated by the status indicator.

Table 8-3 Status Indicator

Color	Description
Green	All diagnostics tests pass—IDSM-2 is operational.
Red	A diagnostics test other than an individual port test failed.
Amber	IDSM-2 is running through its boot and self-test diagnostics sequence, or IDSM-2 is disabled, or IDSM-2 is in the shutdown state.
Off	IDSM-2 power is off.

To prevent corruption of IDSM-2, you must use the **shutdown** command to shut it down properly. For instructions on properly shutting down IDSM-2, see Step 1 of Removing IDSM-2, page 8-10. If IDSM-2 does not respond, firmly press the Shutdown button on the faceplate and wait for the Status indicator to turn amber. The shutdown procedure may take several minutes.

Caution Do not remove IDSM-2 from the switch until the module shuts down completely. Removing the module without going through a shutdown procedure can corrupt the application partition on the module and result in data loss.

Installation and Removal Instructions

All Catalyst 6500 series switches support hot swapping, which lets you install, remove, replace, and rearrange modules without turning off the system power to the switch. When the system detects that a module has been installed or removed, it runs diagnostic and discovery routines, acknowledges the presence or absence of the module, and resumes system operation with no operator intervention.

Caution You must first shut down IDSM-2 before removing it from a Catalyst 6500 series switch. For the procedure for removing an IDSM-2 from a Catalyst 6500 series switch, see Removing IDSM-2, page 8-10.

This section contains the following topics:

Required Tools

Note You must have at least one supervisor engine running in the Catalyst 6500 series switch with IDSM-2. For more information, refer to the *Catalyst 6500 Series Switch Installation Guide*.

You need the following tools to install IDSM-2 in the Catalyst 6500 series switches:

- Flat-blade screwdriver
- Wrist strap or other grounding device
- Antistatic mat or antistatic foam

  Whenever you handle IDSM-2, always use a wrist strap or other grounding device to prevent serious damage from ESD. For more information, see Site and Safety Guidelines, page 1-23.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Slot Assignments

Note The Catalyst 6509-NEB switch has vertical slots numbered 1 to 9 from right to left. Install IDSM-2 with the component side facing to the right.

The Catalyst 6006 and 6506 switch chassis each have six slots. The Catalyst 6009 and 6509 switch chassis each have nine slots. The Catalyst 6513 switch chassis has 13 slots. You can installing IDSM-2 in the following ways:

- You can install IDSM-2 in any slot that is not used by the supervisor engine.
- You can install up to eight IDSM-2s in a single chassis.

Caution Install module filler plates (blank module carriers) in the empty slots to maintain consistent airflow through the switch chassis.

Note IDSM-2 works with any supervisor engine using SPAN, but the copy capture feature with security VACLs requires that the supervisor engine has the PFC or the MSFC option.

Installing IDSM-2

To install IDSM-2 in the Catalyst 6500 series switch, follow these steps:

Step 1 Make sure that you take necessary ESD precautions.

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not touch the backplane with your hand or any metal tool, or you could shock yourself.**

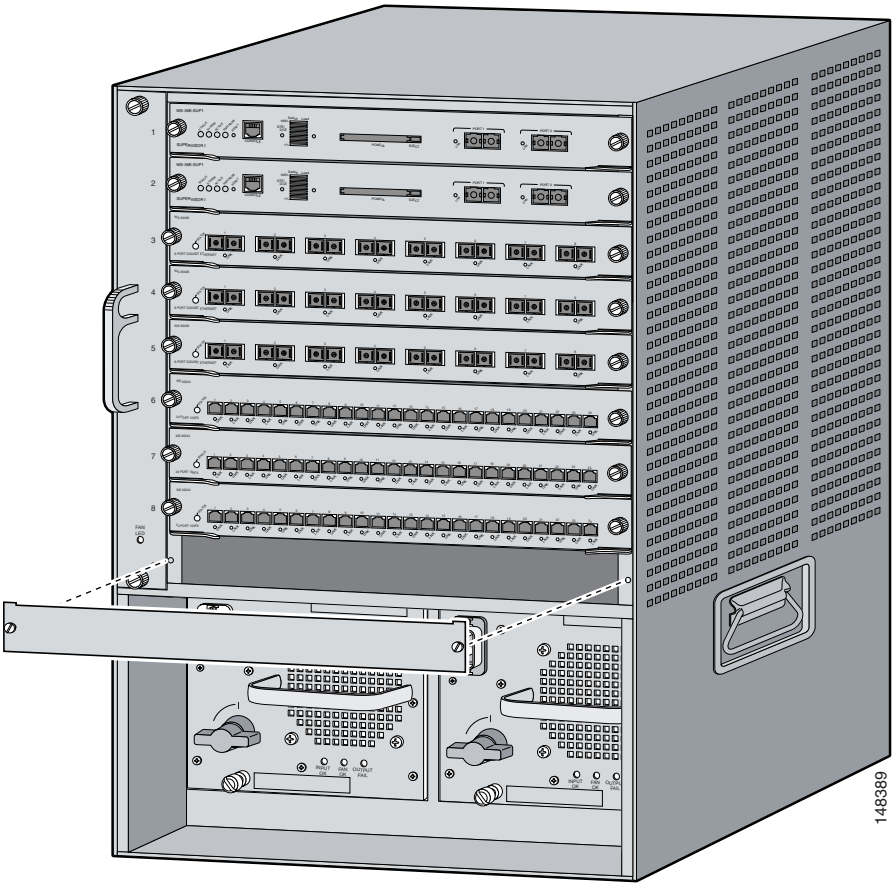
For more information, see Site and Safety Guidelines, page 1-23.

Step 2 Choose a slot for IDSM-2.

Note You can install IDSM-2 in any slot that is not reserved for a supervisor engine or other module. Refer to your switch documentation for information about which slots are reserved for the supervisor engine or other modules.

Step 3 Remove the installation screws (use a screwdriver, if necessary) that secure the filler plate to the desired slot.

Step 4 Remove the filler plate by prying it out carefully.

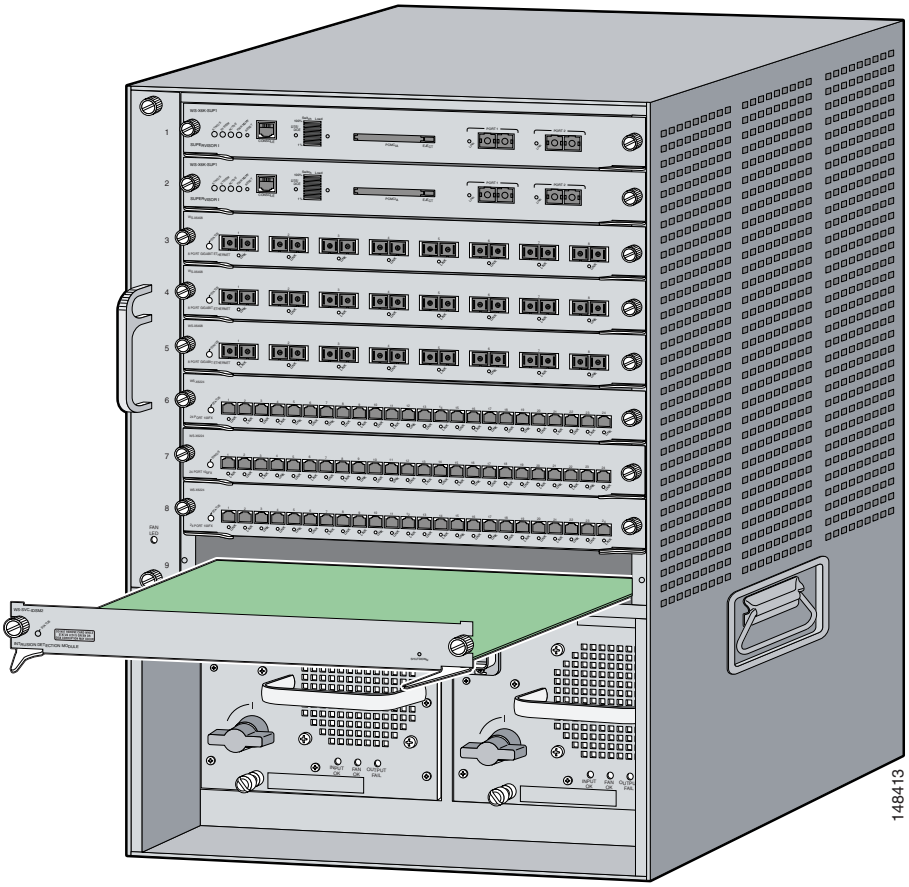


Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Statement 1029**

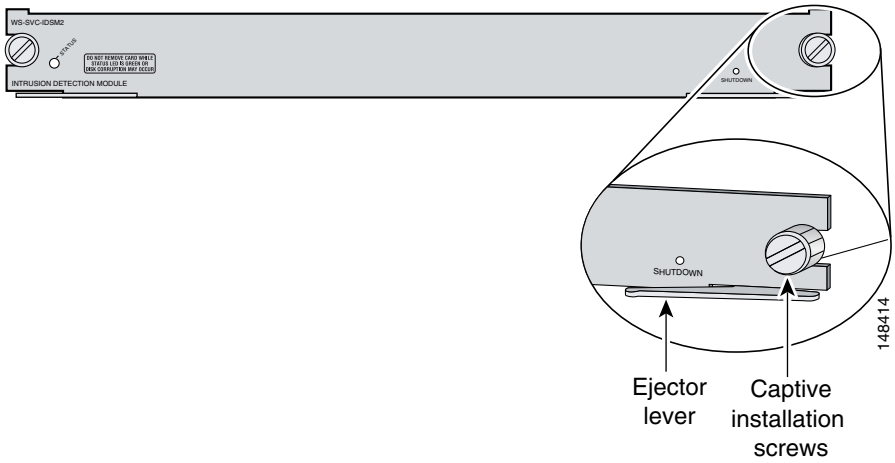
Step 5 Hold the IDSM-2 with one hand, and place your other hand under the IDSM-2 carrier to support it.

Caution Do not touch the printed circuit boards or connector pins on the IDSM-2.

Step 6 Place IDSM-2 in the slot by aligning the notch on the sides of the IDSM-2 carrier with the groove in the slot.



Step 7 Keeping IDSM-2 at a 90-degree orientation to the backplane, carefully push it into the slot until the notches on both ejector levers engage the chassis sides.



Step 8 Using the thumb and forefinger of each hand, simultaneously pivot in both ejector levers to fully seat IDSM-2 in the backplane connector.

Caution Always use the ejector levers when installing or removing IDSM-2. A module that is partially seated in the backplane causes the system to halt and subsequently crash.

Note If you perform a hot swap, the console displays the message `Module x has been inserted`. This message does not appear, however, if you are connected to the Catalyst 6500 series switch through a Telnet session.

Step 9 Use a screwdriver to tighten the installation screws on the left and right ends of IDSM-2.

Step 10 Verify that you have correctly installed IDSM-2 and can bring it online. For the procedure, see Verifying Installation, page 8-8.

Step 11 Initialize IDSM-2.

For the procedure, see Initializing the Sensor, page 10-2.

Step 12 Configure the switch for command and control access to IDSM-2.

For the procedure, refer to Configuring the Catalyst 6500 Series Switch for Command and Control Access to IDSM-2.

Step 13 Upgrade IDSM-2 to the most recent Cisco IDS software.

For the procedure, see Obtaining Cisco IPS Software, page 11-1.

Step 14 Set up IDSM-2 to capture IPS traffic in promiscuous mode or inline mode.

For the procedure, refer to Configuring IDSM-2.

You are now ready to configure IDSM-2 for intrusion prevention.

For More Information

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

Verifying Installation

Verify that the switch acknowledges IDSM-2 and has brought it online.

To verify the installation, follow these steps:

Step 1 Log in to the console.

Step 2 For Catalyst software:

```
console> (enable) show module
Mod Slot Ports Module-Type                Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
```

```
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
2   2    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
3   3    48    10/100/1000BaseT Ethernet WS-X6548-GE-TX      no  ok
4   4    16    1000BaseX Ethernet        WS-X6516A-GBIC      no  ok
6   6    8     Intrusion Detection Mod   WS-SVC-IDSM2        yes ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
1                        SAD041308AN
15                       SAD04120BRB
2                        SAD03475400
3                        SAD073906RC
4                        SAL0751QYN0
6                        SAD062004LV

Mod MAC-Address(es)                         Hw     Fw          Sw
--- -------------------------------------- ------ ---------- -----------------
1   00-d0-c0-cc-0e-d2 to 00-d0-c0-cc-0e-d3 3.1    5.3.1      8.4(1)
    00-d0-c0-cc-0e-d0 to 00-d0-c0-cc-0e-d1
    00-30-71-34-10-00 to 00-30-71-34-13-ff
15  00-30-7b-91-77-b0 to 00-30-7b-91-77-ef 1.4    12.1(23)E2 12.1(23)E2
2   00-30-96-2b-c7-2c to 00-30-96-2b-c7-5b 1.1    4.2(0.24)V 8.4(1)
3   00-0d-29-f6-01-98 to 00-0d-29-f6-01-c7 5.0    7.2(1)     8.4(1)
4   00-0e-83-af-15-48 to 00-0e-83-af-15-57 1.0    7.2(1)     8.4(1)
6   00-e0-b0-ff-3b-80 to 00-e0-b0-ff-3b-87 0.102  7.2(0.67)  5.0(0.30)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw Sub-Sw
--- ----------------------- ------------------- ----------- ------ ------
1   L3 Switching Engine     WS-F6K-PFC          SAD041303G6 1.1
6   IDS 2 accelerator board WS-SVC-IDSUPG       .           2.0
console> (enable)
```

Step 3 For Cisco IOS software:

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ------------------------------------- ------------------ -----------
  1   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD0401012S
  2   48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL04483QBL
  3   48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAD073906GH
  6   16  SFM-capable 16 port 1000mb GBIC        WS-X6516A-GBIC     SAL0740MMYJ
  7    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAD08320L2T
  9    1  1 port 10-Gigabit Ethernet Module      WS-X6502-10GE      SAD071903BT
 10    3  Anomaly Detector Module                WS-SVC-ADM-1-K9    SAD084104JR
 11    8  Intrusion Detection System             WS-SVC-IDSM2       SAD05380608
 13    8  Intrusion Detection System             WS-SVC-IDSM-2      SAD072405D8

Mod MAC addresses                        Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  1  00d0.d328.e2ac to 00d0.d328.e2db   1.1   4.2(0.24)VAI 8.5(0.46)ROC Ok
  2  0003.6c14.e1d0 to 0003.6c14.e1ff   1.4   5.4(2)       8.5(0.46)ROC Ok
  3  000d.29f6.7a80 to 000d.29f6.7aaf   5.0   7.2(1)       8.5(0.46)ROC Ok
  6  000d.ed23.1658 to 000d.ed23.1667   1.0   7.2(1)       8.5(0.46)ROC Ok
  7  0011.21a1.1398 to 0011.21a1.139b   4.0   8.1(3)       12.2(PIKESPE Ok
  9  000d.29c1.41bc to 000d.29c1.41bc   1.3   Unknown      Unknown      PwrDown
 10  000b.fcf8.2ca8 to 000b.fcf8.2caf   0.101 7.2(1)       4.0(0.25)    Ok
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102 7.2(0.67)    5.0(1)       Ok
 13  0003.feab.c850 to 0003.feab.c857   4.0   7.2(1)       5.0(1)       Ok

Mod Sub-Module                  Model              Serial        Hw     Status
--- -------------------------- ------------------ ------------ ------- -------
  7 Policy Feature Card 3       WS-F6K-PFC3BXL     SAD083305A1   1.3    Ok
  7 MSFC3 Daughterboard         WS-SUP720          SAD083206JX   2.1    Ok
 11 IDS 2 accelerator board     WS-SVC-IDSUPG      .             2.0    Ok
```

```
 13 IDS 2 accelerator board     WS-SVC-IDSUPG      0347331976    2.0    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  2 Pass
  3 Pass
  6 Pass
  7 Pass
  9 Unknown
 10 Not Applicable
 11 Pass
 13 Pass
Router#
```

Note It is normal for the status to read `other` when IDSM-2 is first installed. After IDSM-2 completes the diagnostics routines and comes online, the status reads `ok`. Allow up to 5 minutes for IDSM-2 to come online.

For information on enabling a full memory test after verifying IDSM-2 installation, see Enabling Full Memory Tests, page 8-12.

Removing IDSM-2

This procedure describes how to remove IDSM-2 from the Catalyst 6500 series switch.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment. Statement 1030**

Caution Before removing IDSM-2, be sure to perform the shutdown procedure. If IDSM-2 is not shut down correctly, you could corrupt the software.

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not touch the backplane with your hand or any metal tool, or you could shock yourself.**

To remove IDSM-2, follow these steps:

Step 1 Shut down IDSM-2 by one of these methods:

- Log in to the IDSM-2 CLI and enter **reset powerdown**.

  Note The **reset powerdown** command performs a shut down but does not remove power from IDSM-2. To remove power from IDSM-2, use the **set module power down** *module_number* command.

- Log in to the switch CLI and enter one of the following commands:
  - For Catalyst software:

    set module shutdown *module_number*

  - For Cisco IOS software:

    hw-module module *module_number* **shutdown**

- Shut down IDSM-2 through IDM.
- Press the Shutdown button.

Note Shutdown may take several minutes.

Caution If IDSM-2 is removed from the switch chassis without first being shut down, or the chassis loses power, you may need to reset IDSM-2 more than once. If the module fails to respond after three reset attempts, boot the maintenance partition, and perform the instructions for restoring the application partition.

Step 2 Verify that IDSM-2 shuts down. Do not remove IDSM-2 until the status indicator is amber or off.

Step 3 Use a screwdriver to loosen the installation screws at the left and right sides of IDSM-2.

Step 4 Grasp the left and right ejector levers and simultaneously pull the left lever to the left and the right lever to the right to release IDSM-2 from the backplane connector.

Step 5 As you pull IDSM-2 out of the slot, place one hand under the carrier to support it.

Caution Do not touch the printed circuit boards or connector pins.

Step 6 Carefully pull IDSM-2 straight out of the slot, keeping your other hand under the carrier to guide it.

Note Keep IDSM-2 at a 90-degree orientation to the backplane (horizontal to the floor).

Step 7 Place IDSM-2 on an antistatic mat or antistatic foam.

Step 8 If the slot is to remain empty, install a filler plate (part number 800-00292-01) to keep dust out of the chassis and to maintain proper airflow through the module compartment.

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Statement 1029**

For More Information

- For more information on ESD-controlled environments, see Site and Safety Guidelines, page 1-23.
- For the procedure for restoring the application partition, refer to Installing the IDSM-2 System Image.
- For the procedure for resetting IDSM-2, see Resetting IDSM-2, page 8-13.
- For the procedure for powering IDSM-2 up and down, see Powering IDSM-2 Up and Down, page 8-15.

Enabling Full Memory Tests

When IDSM-2 initially boots, by default it runs a partial memory test. You can enable a full memory test in Catalyst software and Cisco IOS software.

This section describes how to enable memory tests, and contains the following topics:

Catalyst Software

Use the **set boot device** *boot_sequence module_number* **mem-test-full** command to enable a full memory test. The full memory test takes about 12 minutes.

To enable a full memory test, follow these steps:

Step 1 Log in to the console.

Step 2 Enter privileged mode:

```
console> enable
```

Step 3 Enable the full memory test:

```
console> (enable) set boot dev cf:1 3 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
console> (enable) set boot dev hdd:1 3 mem-test-full
Device BOOT variable = hdd:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
console> (enable)
```

The **set boot device** command can either contain **cf:1** or **hdd:1**.

Step 4 Reset IDSM-2.

For the procedure, see Resetting IDSM-2, page 8-13.

The full memory test runs.

Note A full memory test takes more time to complete than a partial memory test.

Cisco IOS Software

Use the **hw-module module** *module_number* **reset mem-test-full** command to enable a full memory test. The full memory test takes about 12 minutes.

To enable a full memory test, follow these steps:

Step 1 Log in to the console.

Step 2 Enable the full memory test:

```
Router# hw-module module 9 reset mem-test-full
    Device BOOT variable for reset = <empty>
    Warning: Device list is not verified.

    Proceed with reload of module?[confirm]
    % reset issued for module 9
Router#
```

Step 3 Reset IDSM-2.

For the procedure, see Resetting IDSM-2, page 8-13.

The full memory test runs.

Note A full memory test takes more time to complete than a partial memory test.

Resetting IDSM-2

If for some reason you cannot communicate with IDSM-2 through SSH, Telnet, or the switch **session** command, you must reset IDSM-2 from the switch console. The reset process requires several minutes.

This section describes how to reset IDMS-2, and contains the following topics:

Catalyst Software

To reset IDSM-2 from the CLI, follow these steps:

Step 1 Log in to the console.

Step 2 Enter privileged mode:

```
console> enable
```

Step 3 Reset IDSM-2 to the application partition or the maintenance partition:

```
console> (enable) reset module_number [hdd:1 | cf:1]
```

Note If you do not specify either the application partition (hdd:1 the default) or the maintenance partition (cf:1), IDSM-2 uses the boot device variable.

Example:

```
console> (enable) reset 3
2003 Feb 01 00:18:23 %SYS-5-MOD_RESET: Module 3 reset from console//
Resetting module 3... This may take several minutes.
2003 Feb 01 00:20:03 %SYS-5-MOD_OK: Module 3 is online.
console> (enable)
```

Caution If IDSM-2 is removed from the switch chassis without first being shut down, or the chassis loses power, you may need to reset IDSM-2 more than once. If IDSM-2 fails to respond after three reset attempts, boot the maintenance partition, and perform the instructions for restoring the application partition. For the procedure, refer to Installing the IDSM-2 System Image.

Cisco IOS Software

Use the **hw-module module** *slot_number* **reset** [**hdd:1** | **cf:1**] command in EXEC mode to reset IDSM-2. The reset process takes several minutes. IDSM-2 boots into the boot partition you specify. If you do not specify the boot string, the default boot string is used.

To reset IDSM-2 from the CLI, follow these steps:

Step 1 Log in to the console.

Step 2 Reset IDSM-2:

```
Router# hw-module module module-number reset [hdd:1 | cf:1]
```

Note If you do not specify either the application partition (**hdd:1** the default) or the maintenance partition (**cf:1**), IDSM-2 uses the boot device variable.

Example:

```
Router# hw-module module 8 reset
```

```
Device BOOT variable for reset =
Warning: Device list is not verified.
Proceed with reload of module? [confirm]
% reset issued for module 8
Router#
```

Powering IDSM-2 Up and Down

You can remove and restore power to IDSM-2 through the switch CLI. This section describes how to power IDSM-2 up and down through the switch CLI, and contains the following sections:

- Catalyst Software, page 8-15
- Cisco IOS Software, page 8-15

Catalyst Software

Once you power off IDSM-2, you must power it up through the switch CLI.

Note The IDSM-2 CLI **reset powerdown** command performs a shut down, but does not remove power from IDSM-2.

To power IDSM-2 up and down from the switch CLI, follow these steps:

Step 1 Log in to the console.

Step 2 Enter privileged mode:

console> **enable**

Step 3 Power up IDSM-2:

console> (enable) **set module power up** *module_number*

Step 4 Power down IDSM-2:

console> (enable) **set module power down** *module_number*

Cisco IOS Software

Once you power off IDSM-2, you must power it up through the switch CLI.

Note The IDSM-2 CLI **reset powerdown** command performs a shut down, but does not remove power from IDSM-2.

To power IDSM-2 up and down from the switch CLI, follow these steps:

Step 1 Log in to the console.

Step 2 Enter configure terminal mode:

```
router# configure terminal
```

Step 3 Power up IDSM-2:

```
router(config)# power enable module module_number
```

Step 4 Power down IDSM-2:

```
router(config)# no power enable module module_number
```

CHAPTER 9

Installing NM-CIDS

This chapter lists the software and hardware requirements of NM-CIDS, and describes how to install and remove it.

Note In Cisco IOS documentation, NM-CIDS is referred to as the Cisco IDS network module.

Note NM-CIDS does not support inline (IPS) mode. It can only be configured for promiscuous (IDS) mode.

Caution Although NM-CIDS has a compact flash slot, a compact flash device is not used. Removing the compact flash cover and installing a compact flash device is not supported. NM-CIDS does not operate with a compact flash device installed.

This chapter contains the following sections:

Specifications

Table 9-1 lists the specifications for NM-CIDS.

Table 9-1 NM-CIDS Specifications

Specification	Description
Dimensions (H x W x D)	1.55 x 7.10 x 7.2 in. (3.9 x 18.0 x 19.3 cm)
Weight	1.5 lb (0.7 kg) (maximum)
Operating temperature	+32° to +104°F (+0° to +40°C)

Table 9-1 NM-CIDS Specifications (continued)

Specification	Description
Nonoperating temperature	–40° to +185°F (–40° to +85°C)
Humidity	5% to 95% noncondensing
Operating altitude	0 to 10,000 ft (0 to 3,000 m)

Software and Hardware Requirements

NM-CIDS has the following software and hardware requirements.

NM-CIDS supports the following software:

- Cisco IOS software 12.2(15)ZJ or later
- Cisco IOS software 12.3(4)T or later
- Cisco IDS software 4.1 or later

Caution Do not confuse Cisco IOS IDS (a software-based intrusion-detection application that runs in the Cisco IOS) with the IDS that runs on NM-CIDS. NM-CIDS runs Cisco IPS 5.1. Because performance can be reduced and duplicate alarms can be generated, we recommend that you do not run Cisco IOS IDS and Cisco IPS 51 simultaneously.

NM-CIDS supports the following feature sets:

- IOS IP/FW/IDS
- IOS IP/FW/IDS PLUS IPSEC 56
- IOS IP/FW/IDS PLUS IPSEC 3DES
- IOS IP/IPX/AT/DEC/FW/IDS PLUS
- IOS ENTERPRISE/FW/IDS PLUS IPSEC 56
- IOS ENTERPRISE/FW/IDS PLUS IPSEC 3DES
- IOS Advanced Security
- IOS Advanced IP
- IOS Advanced Enterprise

Table 9-2 lists supported and unsupported platforms for NM-CIDS.

Table 9-2 Supported and Unsupported Platforms

Router	NM-CIDS
Cisco 2600 series	No
Cisco 2600XM series	Yes
Cisco 2691	Yes
Cisco 3620	No
Cisco 3631	No
Cisco 3640, Cisco 3640A	No

Table 9-2 Supported and Unsupported Platforms (continued)

Router	NM-CIDS
Cisco 3660	Yes
Cisco 3725	Yes
Cisco 3745	Yes

Note The supported Cisco series routers only support one NM-CIDS per chassis.

Table 9-3 lists the hardware specifications for NM-CIDS.

Table 9-3 Hardware Requirements

Feature	Description
Processor	500 Mhz Intel Mobile Pentium III
Default SDRAM	512 MB
Maximum DSRAM	512 MB
Internal disk storage	NM-CIDS 20-GB IDE

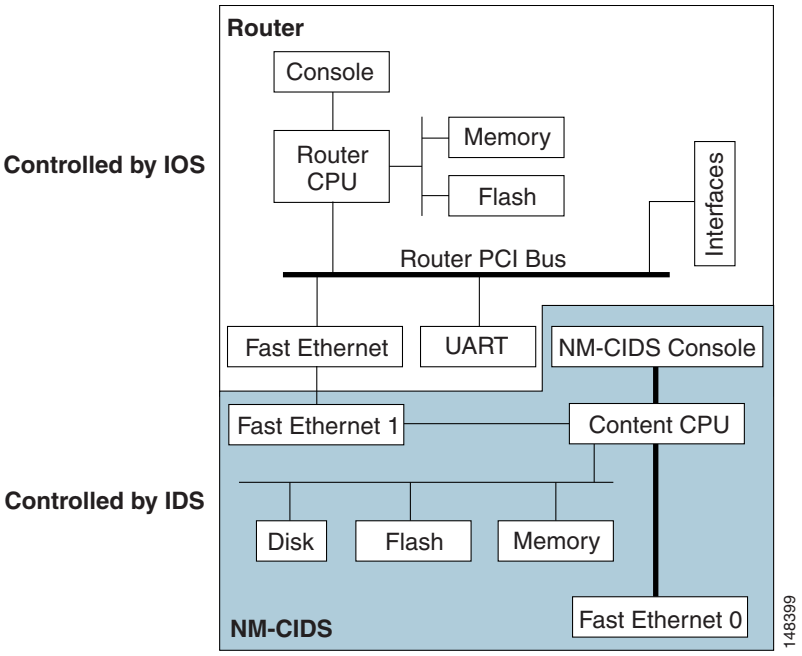
Hardware Architecture

NM-CIDS has the following hardware architecture:

- Back-to-back Ethernet, which provides interface-level connectivity to the router.
- 100-Mbps full-duplex interface between the router and the module.
- Back-to-back UART, which provides console access from router side.
- Console access to the module from the router.
- External FE interface, which provides a command and control interface.

Figure 9-1 shows the hardware architecture of NM-CIDS.

Figure 9-1 NM-CIDS Hardware Architecture



Front Panel Features

Figure 9-2 shows the front panel features of the NM-CIDS.

Figure 9-2 Front Panel Features

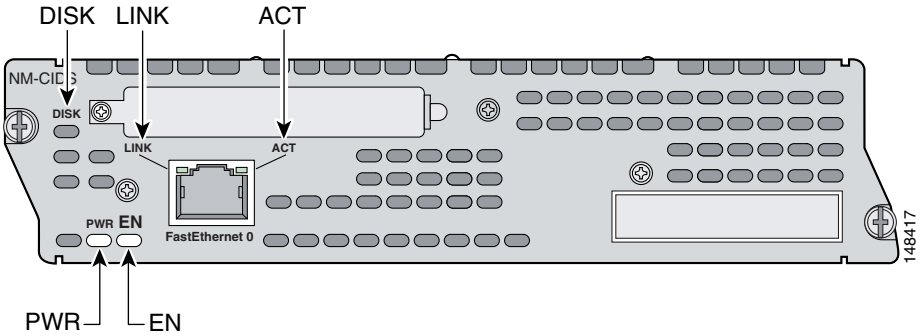


Table 9-4 describes the NM-CIDS states as indicated by the status indicators.

Table 9-4 Status Indicators

Indicator	Description
ACT	Activity on the fast ethernet connection.
DISK	Activity on the IDS hard-disk drive.
EN	NM-CIDS has passed self-test and is available to the router.
LINK	Fast Ethernet connection is available to NM-CIDS.
PWR	Power is available to NM-CIDS.

Interfaces

The router-side fast ethernet interface is known as "interface IDS-Sensor." This interface name appears in the **show interface** and **show controller** commands. You must assign the IP address to the interface to get console access to IDS.

Caution We recommend that you assign a loopback address on the monitoring interface, otherwise if the IP address is advertised through routing updates, the monitoring interface can become vulnerable to attacks.

For the procedure for assigning the IP address to gain access to the console and for setting up a loopback address, refer to Configuring IDS-Interfaces on the Router.

Installation and Removal Instructions

You must install NM-CIDS offline in Cisco 2650XM, 2651XM, and 2961 series routers.

Caution To avoid damaging NM-CIDS, you must turn OFF electrical power and disconnect network cables before you insert NM-CIDS into a chassis slot or remove NM-CIDS from a chassis slot.

Cisco 3660 and Cisco 3700 series routers lets you replace network modules without switching off the router or affecting the operation of other interfaces. OIR provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

Note Cisco 2600, 3600, and 3700 series routers support only one NM-CIDS per chassis.

Caution Unlike other network modules, NM-CIDS uses a hard-disk drive. Online removal of hard-disk drives without proper shutdown can result in file system corruption and might render the hard-disk drive unusable. The operating system on NM-CIDS must be shut down in an orderly fashion before it is removed.

This section contains the following topics:

Required Tools

You need the following tools and equipment to install NM-CIDS in a Cisco modular router chassis slot:

- #1 Phillips screwdriver or small flat-blade screwdriver
- ESD-preventive wrist strap
- Tape for DC circuit breaker handle

Installing NM-CIDS

This section describes how to install NM-CIDS off line and using OIR support, and contains the following topics:

Installing NM-CIDS Offline

You can install NM-CIDS in the chassis either before or after mounting the router, whichever is more convenient.

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.**

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

Caution ESD can damage equipment and impair electrical circuitry. Always follow ESD prevention procedures when removing and replacing cards. For more information, see Site and Safety Guidelines, page 1-23.

To install NM-CIDS, follow these steps:

Step 1 Turn OFF electrical power to the router.

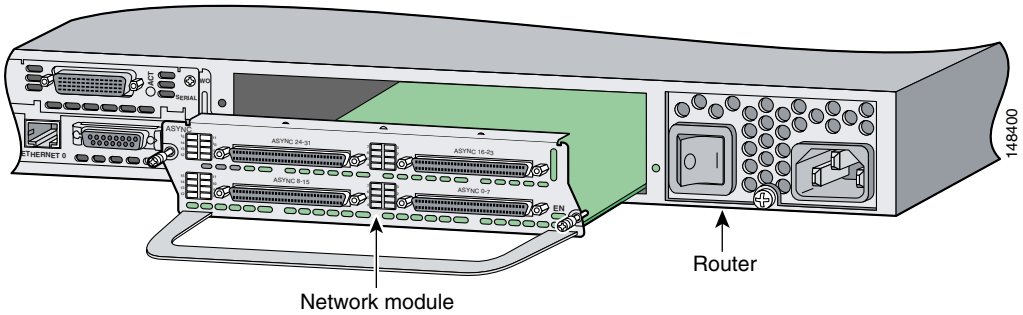
To channel ESD voltages to ground, do not unplug the power cable.

Step 2 Remove all network interface cables, including telephone cables, from the back panel.

Step 3 Using either a #1 Phillips screwdriver or a small flat-blade screwdriver, remove the blank filler panel from the chassis slot where you plan to install NM-CIDS.

Save the blank panel for future use.

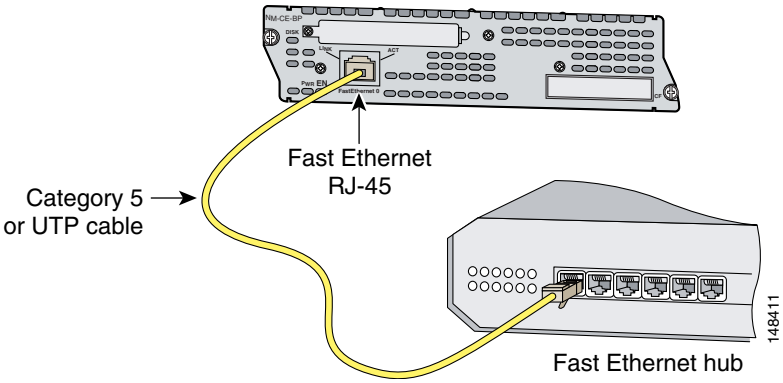
Step 4 Align NM-CIDS with the guides in the chassis and slide it gently into the slot.



Step 5 Push NM-CIDS into place until you feel its edge connector mate securely with the connector on the motherboard.

Step 6 Fasten the captive mounting screws of NM-CIDS into the holes in the chassis, using a Phillips or flat-blade screwdriver.

Step 7 If the router was previously running, reinstall the network interface cables and turn ON power to the router.



The following warning applies to routers that use a DC power supply:

Warning **After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.**

Step 8 Connect the command and control port to a hub or switch.

Step 9 Check that NM-CIDS indicators light up, and that the Active/Ready indicators on the front panel also light up.

Step 10 Initialize NM-CIDS.

For the procedure, see Initializing the Sensor, page 10-2.

Step 11 Upgrade NM-CIDS to the most recent Cisco software.

For the procedure, see Obtaining Cisco IPS Software, page 11-1.

You are now ready to configure intrusion detection on NM-CIDS.

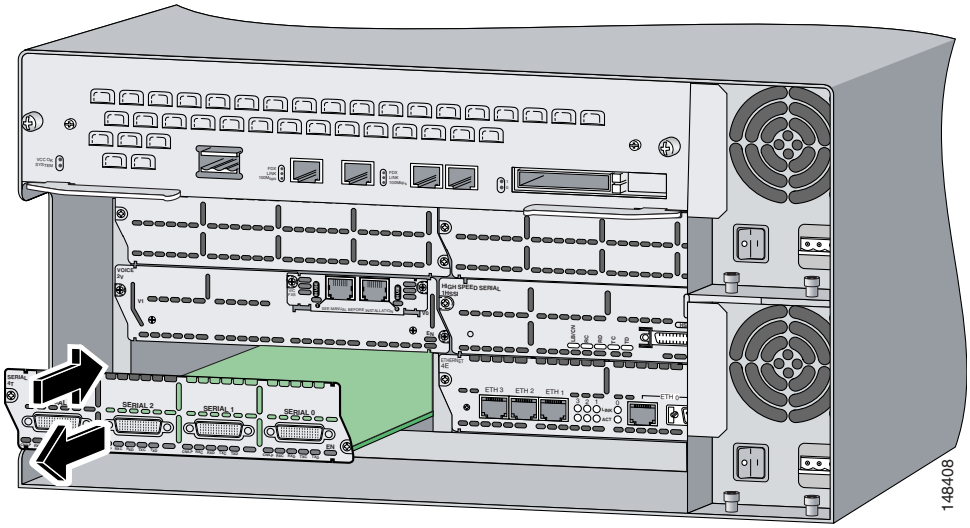
For More Information

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For the procedures for configuring intrusion detection on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

Installing NM-CIDS Using OIR Support

To install NM-CIDS using OIR support, follow these steps:

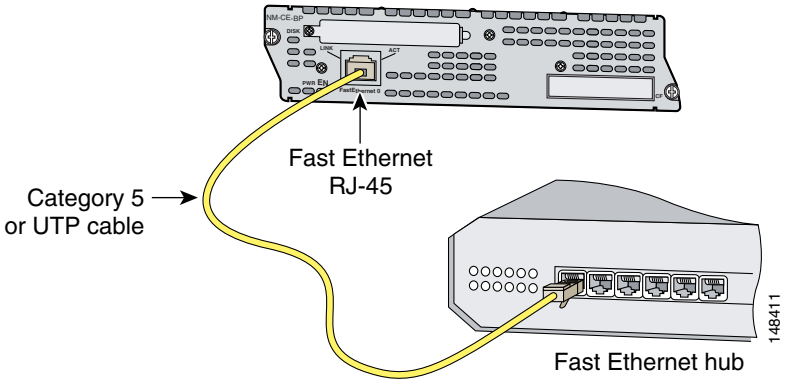
Step 1 Align NM-CIDS with the guides in the chassis slot and slide it gently into the slot.



Step 2 Push NM-CIDS into place until you feel its edge connector mate securely with the connector on the backplane.

Step 3 Tighten the two captive screws on the faceplate.

Step 4 Connect the command and control port to a hub or switch.



Step 5 Verify that NM-CIDS indicators light up, and that the Active/Ready indicators on the front panel also light up.

Step 6 Initialize NM-CIDS.

For the procedure, see Initializing the Sensor, page 10-2.

Step 7 Upgrade NM-CIDS to the most recent Cisco IPS software.

For the procedure, see Obtaining Cisco IPS Software, page 11-1.

You are now ready to configure intrusion detection on NM-CIDS.

Removing NM-CIDS

This section describes how to remove NM-CIDS offline or using OIR support and contains the following topics:

- Removing NM-CIDS Offline, page 9-9
- Removing NM-CIDS Using OIR Support, page 9-10

Removing NM-CIDS Offline

You must turn off all power to the router before removing NM-CIDS.

To remove NM-CIDS from the router chassis, follow these steps:

Step 1 Prepare NM-CIDS to be powered off:

```
router# service-module IDS-Sensor slot_number/0 shutdown
Trying 10.10.10.1, 2129 ... Open
```

Wait for the shutdown message before continuing with Step 2:

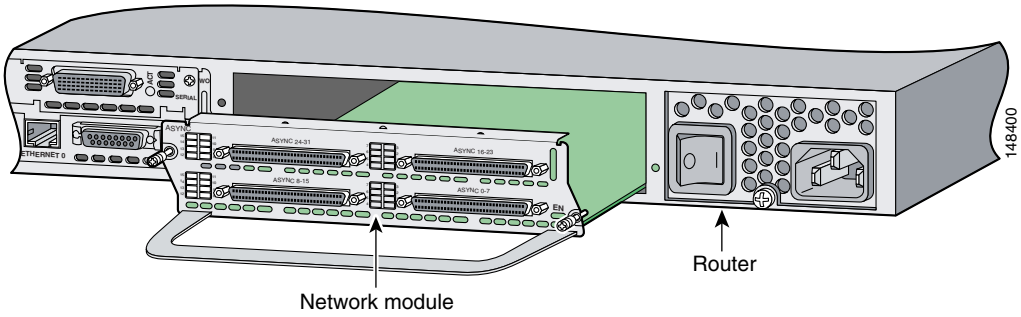
```
%SERVICEMODULE-5-SHUTDOWN2:Service module IDS-Sensor1/0 shutdown complete
```

Step 2 Turn OFF electrical power to the router.

To channel ESD voltages to ground, do not unplug the power cable.

Step 3 Unplug the command and control network interface cable from NM-CIDS.

Step 4 Loosen the two captive screws holding NM-CIDS in the chassis slot.



Step 5 Slide NM-CIDS out of the slot.

Note Either install a replacement NM-CIDS (for the procedure, see Installing NM-CIDS Offline, page 9-6) or install a blank panel (for the procedure, see Blank Network Module Panels, page 9-11).

Removing NM-CIDS Using OIR Support

Caution Cisco 3660 and Cisco 3700 series routers support OIR with similar modules only. If you remove an NM-CIDS, install another NM-CIDS in its place.

To remove NM-CIDS with OIR support, follow these steps:

Step 1 Prepare NM-CIDS to be powered off:

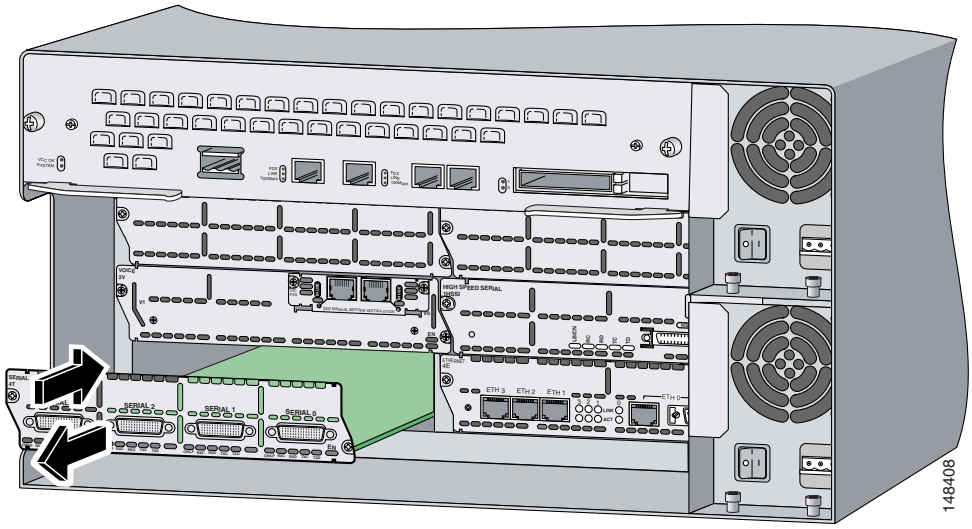
```
router# service-module IDS-Sensor slot_number/0 shutdown
Trying 10.10.10.1, 2129 ... Open
```

Wait for the shutdown message before continuing with Step 2:

```
%SERVICEMODULE-5-SHUTDOWN2:Service module IDS-Sensor1/0 shutdown complete
```

Step 2 Unplug the command and control network interface cable from NM-CIDS.

Step 3 Loosen the two captive screws holding NM-CIDS in the chassis slot.



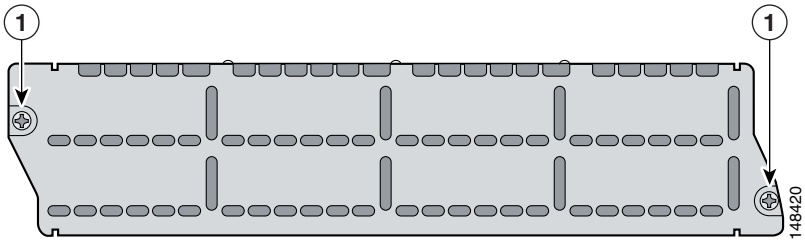
Step 4 Slide NM-CIDS out of the slot.

Note Either install a replacement NM-CIDS (for the procedure, see Installing NM-CIDS Using OIR Support, page 9-8), or install a blank panel (for the procedure, see Blank Network Module Panels, page 9-11).

Blank Network Module Panels

If the router is not fully configured with network modules, make sure that blank panels fill the unoccupied chassis slots to provide proper airflow as shown in Figure 9-3.

Figure 9-3 Blank Network Module Panel



CHAPTER 10

Initializing the Sensor

This chapter explains how to initialize the sensor using the **setup** command. It contains the following sections:

Overview

After you have installed the sensor on your network, you must use the **setup** command to initialize it. With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, Telnet server, web server port, access control lists, time settings, and assign and enable interfaces. After you have initialized the sensor, you can communicate with it over the network. You are then ready to configure intrusion prevention.

System Configuration Dialog

When you enter the **setup** command, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process.

The values shown in brackets next to each prompt are the current values.

You must go through the entire System Configuration Dialog until you come to the option that you want to change. To accept default settings for items that you do not want to change, press **Enter**.

To return to the EXEC prompt without making changes and without going through the entire System Configuration Dialog, press **Ctrl-C**.

The System Configuration Dialog also provides help text for each prompt. To access the help text, press the question mark (?) key at a prompt.

When you complete your changes, the System Configuration Dialog shows you the configuration that you created during the setup session. It also asks you if you want to use this configuration. If you enter **`yes`**, the configuration is saved. If you enter **`no`**, the configuration is not saved and the process begins again. There is no default for this prompt; you must enter either **`yes`** or **`no`**.

You can configure daylight savings time either in recurring mode or date mode. If you select recurring mode, the start and end days are based on week, day, month, and time. If you select date mode, the start and end days are based on month, day, year, and time. Selecting Disable turns off daylight savings time.

You can edit the default virtual sensor, vs0, through the System Configuration Dialog. You can assign promiscuous and/or inline-pairs to the virtual sensor. This also enables the assigned interfaces. After setup is complete, the virtual sensor is configured to monitor traffic.

Note You only need to set the date and time in the System Configuration Dialog if the system is an appliance and is NOT using NTP.

Initializing the Sensor

To initialize the sensor, follow these steps:

Step 1 Log in to the sensor using an account with administrator privileges:

- Log in to the appliance by using a serial connection or with a monitor and keyboard.

  Note You cannot use a monitor and keyboard with IDS-4215, IPS-4240, or IPS-4255.

- Session to IDSM-2:
  - For Catalyst software:

    ```
    cat6k> enable
    cat6k> (enable) session module_number
    ```

  - For Cisco IOS software:

    ```
    switch# session slot slot_number processor 1
    ```

- Session to NM-CIDS:

  ```
  router# service-module IDS-Sensor slot_number/port_number session
  ```

- Session to AIP-SSM:

  ```
  asa# session 1
  ```

Note The default username and password are both **cisco**.

Step 2 The first time you log in to the sensor you are prompted to change the default password.

Passwords must be at least eight characters long and be strong, that is, not be a dictionary word.

Caution If you forget your password, you may have to reimage your sensor unless there is another user with Administrator privileges. The other Administrator can log in and assign a new password to the user who forgot the password. Or, if you have created the service account for support purposes, you can have TAC create a password.

After you change the password, the `sensor#` prompt appears.

Step 3 Enter the **setup** command.

The System Configuration Dialog is displayed.

Note The System Configuration Dialog is an interactive dialog. The default settings are displayed.

```
    --- System Configuration Dialog ---


At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit


Current time: Wed May 5 10:25:35 2004
```

Step 4 Press the spacebar to get to the following question:

```
Continue with configuration dialog?[yes]:
```

Press the spacebar to show one page at a time. Press **Enter** to show one line at a time.

Step 5 Enter **yes** to continue.

Step 6 Specify the hostname.

The hostname is a case-sensitive character string up to 64 characters. Numbers, "_" and "-" are valid, but spaces are not acceptable. The default is sensor.

Step 7 Specify the IP interface.

The IP interface is in the form of IP Address/Netmask,Gateway: X.X.X.X/nn,Y.Y.Y.Y, where X.X.X.X specifies the sensor IP address as a 32-bit address written as 4 octets separated by periods where X = 0-255, nn specifies the number of bits in the netmask, and Y.Y.Y.Y specifies the default gateway as a 32-bit address written as 4 octets separated by periods where Y = 0-255.

Step 8 Specify the Telnet server status.

You can disable or enable Telnet services. The default is disabled.

Step 9 Specify the web server port.

The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note If you change the web server port, you must specify the port in the URL address of your browser when you connect to the IDM in the format `https://`*sensor_ip_ address*`:port` (for example, `https://10.1.9.201:1040`).

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 10 Enter **yes** to modify the network access list.

a. If you want to delete an entry, enter the number of the entry and press **Enter**, or press **Enter** to get to the Permit line.

b. Enter the IP address and netmask of the network you want to add to the access list.

The IP network interface is in the form of IP Address/Netmask: X.X.X.X/nn, where X.X.X.X specifies the network IP address as a 32-bit address written as 4 octets separated by periods where X = 0-255, nn specifies the number of bits in the netmask for that network.

For example, 10.0.0.0/8 permits all IP addresses on the 10.0.0.0 network (10.0.0.0-10.255.255.255) and 10.1.1.0/24 permits only the IP addresses on the 10.1.1.0 subnet (10.1.1.0-10.1.1.255).

If you want to permit access to a single IP address than the entire network, use a 32-bit netmask. For example, 10.1.1.1/32 permits just the 10.1.1.1 address.

c. Repeat Step b until you have added all networks that you want to add to the access list.

d. Press **Enter** at a blank permit line to proceed to the next step.

Step 11 Enter **yes** to modify the system clock settings.

a. Enter **yes** if you want to use NTP.

You will need the NTP server IP address, the NTP key ID, and the NTP key value. If you do not have those at this time, you can configure NTP later.

b. Enter **yes** to modify summertime settings.

Note Summertime is also known as DST. If your location does not use Summertime, go to Step n.

c. Choose recurring, date, or disable to specify how you want to configure summertime settings.

The default is recurring.

d. If you chose recurring, specify the month you want to start summertime settings.

   Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december.

   The default is april.

e. Specify the week you want to start summertime settings.

   Valid entries are first, second, third, fourth, fifth, and last.

   The default is first.

f. Specify the day you want to start summertime settings.

   Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday.

   The default is sunday.

g. Specify the time you want to start summertime settings.

   The default is 02:00:00.

Note The default recurring summertime parameters are correct for time zones in the United States. The default values specify a start time of 2 a.m. on the first Sunday in April, and a stop time of 2 a.m. on the fourth Sunday in October. The default summertime offset is 60 minutes.

h. Specify the month you want summertime settings to end.

   Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december.

   The default is october.

i. Specify the week you want the summertime settings to end.

   Valid entries are first, second, third, fourth, fifth, and last.

   The default is last.

j. Specify the day you want the summertime settings to end.

   Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday.

   The default is sunday.

k. Specify the time you want summertime settings to end.

l. Specify the DST zone.

   The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+:,_/-]+$.

m. Specify the summertime offset.

   Specify the summertime offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian).

   The default is 0.

n. Enter `yes` to modify the system time zone.

o. Specify the standard time zone name.

   The zone name is a character string up to 24 characters long.

p. Specify the standard time offset.

The default is 0.

Specify the standard time zone offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian).

Step 12 Enter **yes** to modify the virtual sensor configuration (vs0).

The current interface configuration appears:

```
Current interface configuration
  Command control: GigabitEthernet0/1
  Unused:
    GigabitEthernet2/1
    GigabitEthernet2/0
  Promiscuous:
    GigabitEthernet0/0
  Inline:
    None
  Inline VLAN Pair:
    None
```

Step 13 Enter **yes** to add a promiscuous or monitoring interface.

Step 14 Enter the interface you want to add, for example, **GigabitEthernet0/1**.

Step 15 Enter **yes** to add inline interface pairs (appears only if your platform supports inline interface pairs).

a. Enter the inline interface pair name.

b. Enter the inline interface pair description.

The default is `Created via setup by user <yourusername>`.

c. Enter the name of the first interface in the inline pair, **interface1**.

d. Enter the name of the second interface in the inline pair, **interface2**.

e. Repeat Steps a through d to add another inline interface pair, or press **Enter** for the next option.

Step 16 Enter **yes** to add inline VLAN pairs (appears only if your platform supports inline VLAN pairs).

A list of interfaces available for inline VLAN pairs appears:

```
Available Interfaces:
 [1] GigabitEthernet0/0
 [2] GigabitEthernet2/0
 [3] GigabitEthernet2/1
```

Step 17 Enter the number of the interface you want to subdivide into inline VLAN pairs.

The current inline VLAN pair configuration for that interface appears:

```
Inline Vlan Pairs for GigabitEthernet0/0
  None
```

a. Enter the subinterface number to add.

b. Enter the inline VLAN pair description.

c. Enter the first VLAN number (vlan1).

d. Enter the second VLAN number (vlan2).

e. Repeat Steps a through d to add another inline VLAN pair on this interface or press **Enter** for the next option.

Step 18 Enter **yes** to subdivide another interface. Enter **no** or press **Enter** to complete the addition of the inline VLAN pairs.

Your configuration appears with the following options:

```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 19 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 20 Enter **yes** to modify the system date and time.

Note This option is not available on modules or when NTP has been configured. The modules get their time from the router or switch in which they are installed, or from the configured NTP server.

a. Enter the local date (yyyy-mm-dd).

b. Enter the local time (hh:mm:ss).

Step 21 Reboot the sensor:

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 22 Enter **yes** to continue the reboot.

Step 23 Display the self-signed X.509 certificate (needed by TLS):

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 24 Write down the certificate fingerprints.

You need the fingerprints to check the authenticity of the certificate when using HTTPS to connect to this appliance with a web browser.

Step 25 Apply the most recent service pack and signature update.

The Readme explains how to apply the most recent software update.

You are now ready to configure your sensor for intrusion prevention.

For More Information

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For information on how to obtain the most recent software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedures for reimaging sensors, refer to Upgrading, Downgrading, and Installing System Images.
- For the procedure for creating the Service account, refer to Creating the Service Account.
- For the procedure for configuring NTP, refer to Configuring the Sensor to Use an NTP Time Source.

- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

Verifying Initialization

After you have run the **setup** command, you should verify that your sensor has been initialized correctly.

To verify that you initialized your sensor, follow these steps:

Step 1 Log in to the sensor.

Step 2 View your configuration:

```
sensor# show configuration
generating current config:
! ------------------------------
! Version 5.1(1)
! Current configuration last modified Wed Jun 29 19:18:14 2005
! ------------------------------
display-serial
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 0
physical-interface GigabitEthernet2/1
exit
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.149.27/25,10.89.149.126
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
access-list 171.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
```

```
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
bypass-mode auto
interface-notifications
missed-percentage-threshold 19
notification-interval 36
idle-interface-delay 33
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity high
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 2004 0
alert-severity low
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3201 1
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3301 0
status
enabled true
exit
exit
signatures 3401 0
status
enabled true
retired false
exit
engine string-tcp
event-action produce-alert|request-block-host
exit
alert-frequency
summary-mode fire-all
exit
exit
```

```
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
trusted-certificates 10.89.149.227:443 certificate MIICJDCCAY0CCPy71vhtAwyNMA0GC
SqGSIb3DQEBBQUAMFcxCzAJBgNVBAYTAlVTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwE
AYDVQQLEwlTU00tSVBTMTAxFjAUBgNVBAMTDTEwLjg5LjE0OS4yMjcwHhcNMDUwNjE0MDUwODA3WhcNM
DcwNjE1MDUwODA3WjBXMQswCQYDVQQGEwJVUzEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESM
BAGA1UECxMJU1NNLUlQUzEwMRYwFAYDVQQDEw0xMC44OS4xNDkuMjI3MIGfMA0GCSqGSIb3DQEBAQUAA
4GNADCBiQKBgQCoOobDuZOEPudw63Rlt8K1YsymzR/D9Rlcnad/U0gjAQGfcUh3sG3TXPQewon1fH0+A
nBw8Jxv/ovSB1HJ3ujh5k7BrrB2QMv73ESsBDdxLY6SoX/yYANMf4zPcPCAORJ6DMQHFj44A+3tMZWsC
yaod23S1oYOxx7v5puPDYn3IQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAHfPM7jawvdfXkYyazqvy3ZOK
kHVwHji12vBLo+biULJG95hbTFlqO+ba3R6nPD3tepgx5zTdOr2onnlFHWD95Ii+PKdUxj7vfDBG8atn
obsEBJ1lAQDiogskdCs4ax1tB4SbEU5y1tktKgcwWEdJpbbNJhzpoRsRICfM3HlOEwN
exit
! ------------------------------
service web-server
exit
sensor#
```

Note You can also use the **more current-config** command to view your configuration.

Step 3 Display the self-signed X.509 certificate (needed by TLS):

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 4 Write down the certificate fingerprints.

You need these to check the authenticity of the certificate when connecting to this sensor with a web browser.

For More Information

For the procedure for logging in to the various sensors, refer to Logging In to the Sensor.

CHAPTER 11

Obtaining Software

This chapter provides information on obtaining Cisco IPS software for the sensor. It contains the following sections:

Caution The BIOS on Cisco IDS/IPS sensors is specific to Cisco IDS/IPS sensors and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on Cisco IDS/IPS sensors voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Cisco IPS Software, page 11-1.

Obtaining Cisco IPS Software

You can find major and minor updates, service packs, signature and signature engine updates, system and recovery files, firmware upgrades, and readmes on the Download Software site on Cisco.com.

Note You must be logged in to Cisco.com to download software.

Signature updates are posted to Cisco.com approximately every week, more often if needed. Service packs are posted to Cisco.com as needed. Major and minor updates are also posted periodically. Check Cisco.com regularly for the latest IPS software.

Note You must have an active IPS maintenance contract and a Cisco.com password to download software. You must have a license to apply signature updates.

To download software on Cisco.com, follow these steps:

Step 1 Log in to Cisco.com.

Step 2 From the Support drop-down menu, choose **Download Software**.

Step 3 Under Select a Software Product Category, choose **Security Software**.

Step 4 Choose **Intrusion Prevention System (IPS)**.

Step 5 Enter your username and password.

Step 6 In the Download Software window, choose **IPS Appliances > Cisco Intrusion Prevention System** and then click the version you want to download.

Note You must have an IPS subscription service license to download software.

Step 7 Click the type of software file you need.

The available files appear in a list in the right side of the window. You can sort by file name, file size, memory, and release date. And you can access the Release Notes and other product documentation.

Step 8 Click the file you want to download.

The file details appear.

Step 9 Verify that it is the correct file, and click **Download**.

Step 10 Click **Agree** to accept the software download rules.

The first time you download a file from Cisco.com, you must fill in the Encryption Software Export Distribution Authorization form before you can download the software.

- Fill out the form and click **Submit**.

  The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.

- Read the policy and click **I Accept**.

  The Encryption Software Export/Distribution Form appears.

If you previously filled out the Encryption Software Export Distribution Authorization form, and read and accepted the Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy, these forms are not displayed again.

The File Download dialog box appears.

Step 11 Open the file or save it to your computer.

Step 12 Follow the instructions in the Readme to install the update.

Note Major and minor updates, service packs, recovery files, signature and signature engine updates are the same for all sensors. System image files are unique per platform.

For More Information

- For the procedure for obtaining a license key, see Obtaining a License Key From Cisco.com, page 11-8.
- For an explanation of the IPS file versioning scheme, see IPS Software Versioning, page 11-3.
- For the procedures for reimaging your sensor, refer to Upgrading, Downgrading, and Installing System Images.

IPS Software Versioning

When you download IPS software images from Cisco.com, you should understand the versioning scheme so that you know which files are base files, which are cumulative, and which are incremental.

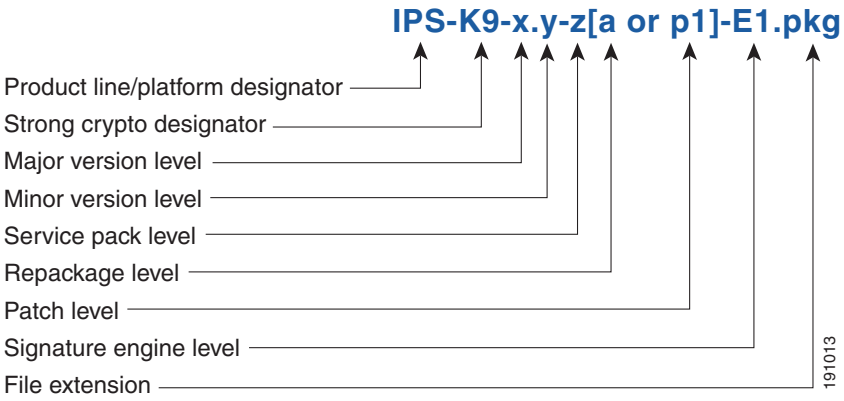
Note You can determine which software version is installed on your sensor by using the **show version** command.

This section describes the various IPS software files, gives software release examples, and contains the following topics:

Major and Minor Updates, Service Packs, and Patch Releases

Figure 11-1 illustrates what each part of the IPS software file represents for major and minor updates, service packs, and patch releases.

Figure 11-1 IPS Software File Name for Major and Minor Updates, Service Packs, and Patch Releases



Major Update

Contains new functionality or an architectural change in the product. For example, the IPS 5.0 base version includes everything (except deprecated features) since the previous major release (the minor update features, service pack fixes, and signature updates) plus any new changes. Major update 5.0(1) requires 4.*x*. With each major update there are corresponding system and recovery packages.

Note The 5.0(1) major update is only used to upgrade 4.*x* sensors to 5.0(1). If you are reinstalling 5.0(1) on a sensor that already has 5.0(1) installed, use the system image or recovery procedures rather than the major update.

Minor Update

Incremental to the major version. Minor updates are also base versions for service packs. The first minor update for 5.0 is 5.1(1). Minor updates are released for minor enhancements to the product. Minor updates contain all previous minor features (except deprecated features), service pack fixes, signature updates since the last major version, and the new minor features being released. You can install the minor updates on the previous major or minor version (and often even on earlier versions). The minimum supported version needed to upgrade to the newest minor version is listed in the Readme that accompanies the minor update. With each minor update there are corresponding system and recovery packages.

Service Packs

Cumulative following a base version release (minor or major). Service packs are used for the release of defect fixes with no new enhancements. Service packs contain all service pack fixes since the last base version (minor or major) and the new defect fixes being released. Service packs require the minor version. The minimum supported version needed to upgrade to the newest service pack is listed in the Readme that accompanies the service pack. Service packs also include the latest engine update. For example, if service pack 6.0(3) is released, and E3 is the latest engine level, the service pack is released as 6.0(3)E3.

Patch Release

Used to address defects that are identified in the upgrade binaries after a software release. Rather than waiting until the next major or minor update, or service pack to address these defects, a patch can be posted. Patches include all prior patch releases within the associated service pack level. The patches roll into the next official major or minor update, or service pack.

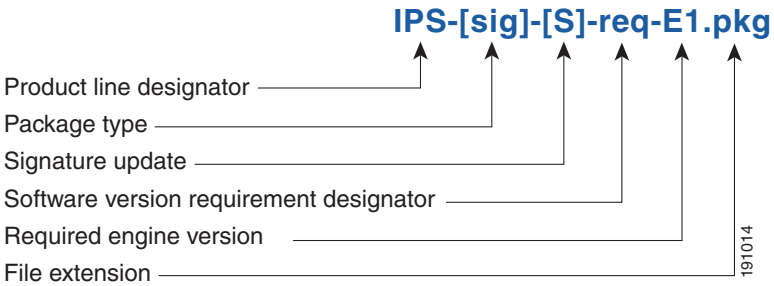
Before you can install a patch release, the most recent major or minor update, or service pack must be installed. For example, patch release 5.0(1p1) requires 5.0(1).

Note Upgrading to a newer patch does not require you to uninstall the old patch. For example, you can upgrade from patch 5.0(1p1) to 5.0(1p2) without first uninstalling 5.0(1p1).

Signature/Virus Updates and Signature Engine Updates

Figure 11-2 illustrates what each part of the IPS software file represents for signature/virus updates.

Figure 11-2 IPS Software File Name for Signature/Virus Updates,



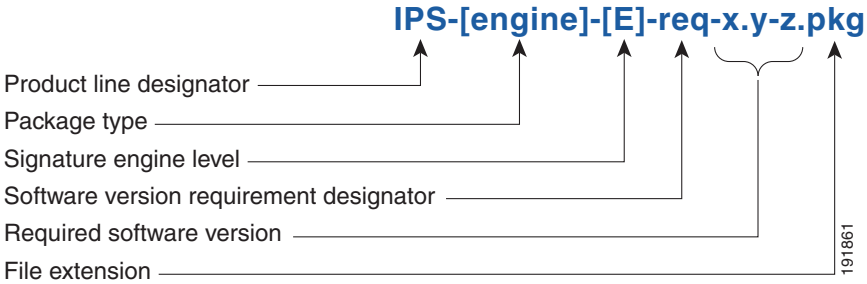
Signature/Virus Updates

Executable file containing a set of rules designed to recognize malicious network activities. Signature updates are released independently from other software updates. Each time a major or minor update is released, you can install signature updates on the new version and the next oldest version for a period of at least six months. Signature updates are dependent on a required signature engine version. Because of this, a *req* designator lists the signature engine required to support a particular signature update.

A virus component for the signature updates is packaged with the signature update. Virus updates are generated by Trend Microsystems for use by the Cisco Intrusion Containment System (Cisco ICS). Once created for use by Cisco ICS, they are later be incorporated into standard Cisco signature updates.

Figure 11-3 illustrates what each part of the IPS software file represents for signature engine updates.

Figure 11-3 IPS Software File Name for Signature Engine Updates



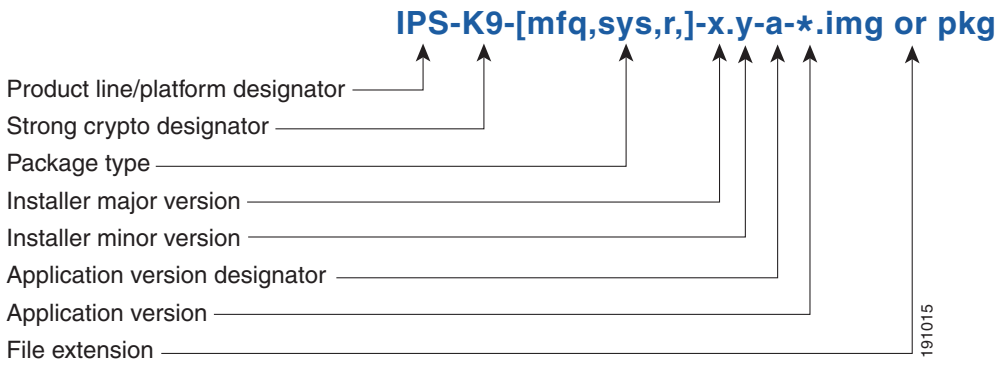
Signature Engine Updates

Executable files containing binary code to support new signature updates. Signature engine files require a specific service pack, which is also identified by the *req* designator.

Recovery, Manufacturing, and System Images

Figure 11-4 illustrates what each part of the IPS software file represents for recovery and system image filenames.

Figure 11-4 IPS Software File Name for Recovery and System Image Filenames



Recovery and system images contain separate versions for the installer and the underlying application. The installer version contains a major and minor version field.

Installer Major Version

The major version is incremented by one of any major changes to the image installer, for example, switching from .tar to rpm or changing kernels.

Installer Minor Version

The minor version can be incremented by any one of the following:

- Minor change to the installer, for example, a user prompt added.
- Repackages require the installer minor version to be incremented by one if the image file must be repackaged to address a defect or problem with the installer.

5.*x* Software Release Examples

Table 11-1 lists platform-independent IDS 5.*x* software release examples. Refer to the readmes that accompany the software files for detailed instructions on how to install the files. For instructions on how to access these files on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.

Table 11-1 Platform-Independent Release Examples

Release	Target Frequency	Identifier	Supported Platform	Example File Name
Signature update[1]	Weekly	sig	All	IPS-sig-S70-minreq-5.0-1.pkg
Service pack[2]	Semi-annually or as needed	sp	All	IPS-K9-sp-5.0-2.pkg
Minor version[3]	Annually	min	All	IPS-K9-min-5.1-1.pkg
Major version[4]	Annually	maj	All	IPS-K9-maj-5.0-1.pkg

Table 11-1 Platform-Independent Release Examples (continued)

Release	Target Frequency	Identifier	Supported Platform	Example File Name
Patch release[5]	As needed	patch	All	IPS-K9-patch-5.0-1pl.pkg
Recovery package [6]	Annually or as needed	r	All	IPS-K9-r-1.1-a-5.0-1.pkg

1. Signature updates include the latest cumulative IPS signatures.
2. Service packs include defect fixes.
3. Minor versions include new features and/or functionality (for example, signature engines).
4. Major versions include new functionality or new architecture.
5. Patch releases are for interim fixes.
6. The r 1.1 can be revised to r 1.2 if it is necessary to release a new recovery package that contains the same underlying application image. If there are defect fixes for the installer, for example, the underlying application version may still be 5.0(1), but the recovery partition image will be r 1.2.

Table 11-2 describes platform-dependent release examples.

Table 11-2 Platform-Dependent Release Examples

Release	Target Frequency	Identifier	Supported Platform	Example File Name
System image[1]	Annually	sys	All	IPS-4240-K9-sys-1.1-a-5.1-1.img
Maintenance partition image[2]	Annually	mp	IDSM-2 only	c6svc-mp.2-1-2.bin.gz
Recovery and upgrade CD	Annually or as needed	cd	All appliances with a CD-ROM drive	—

1. The system image includes the combined recovery and application image used to reimage an entire sensor.
2. The maintenance partition image includes the full image for the maintenance partition. The file is platform specific. If you have to recover the IDSM-2 from the maintenance partition, the application partition reflects the applicable 5.0 version after the recovery operation has been completed.

Upgrading Cisco IPS Software to 5.*x*

Note You cannot upgrade the IDSM (WS-X6381) to Cisco IDS 5.*x*. You must replace your IDSM (WS-X6381) with IDSM-2 (WS-SVC-IDSM2-K9), which supports version 5.*x*.

Pay attention to the following when upgrading to IPS 5.x:

- The minimum required version for upgrading to 5.1 is 5.0. The minimum required version for upgrading to 5.0 is 4.1(1). The upgrades from Cisco 5.0 to 5.1 and Cisco 4.1 to 5.0 are available as a downloads from Cisco.com. For the procedure for accessing Downloads on Cisco.com, see Obtaining Cisco IPS Software, page 11-1.
- After downloading the 5.1 upgrade file, refer to the accompanying Readme for the procedure for installing the 5.1 upgrade file using the **upgrade** command. Or refer to Upgrading the Sensor.

- If you configured Auto Update for your sensor, copy the 5.1 upgrade file to the directory on the server that your sensor polls for updates. Refer to Configuring Automatic Upgrades.
- If you install an upgrade on your sensor and the sensor is unusable after it reboots, you must reimage your sensor. Upgrading a sensor from any Cisco IDS version before 4.1 also requires you to use the **recover** command or the recovery/upgrade CD.

You can reimage your sensor in the following ways:

- For IDS appliances with a CD-ROM drive, use the recovery/upgrade CD.

  For the procedure, refer to Using the Recovery/Upgrade CD.
- For all sensors, use the **recover** command.

  For the procedure, refer to Recovering the Application Partition.
- For the IDS-4215, IPS-4240, IPS 4255, and IPS-4260 use the ROMMON to restore the system image.

  For the procedures, refer to Installing the IDS-4215 System Image, Installing the IPS-4240 and IPS-4255 System Image, and Installing the IPS-4260 System Image.
- For NM-CIDS, use the bootloader.

  For the procedure, refer to Installing the NM-CIDS System Image.
- For IDSM-2, reimage the application partition from the maintenance partition.

  For the procedure, refer to Installing the IDSM-2 System Image.
- For AIP-SSM, reimage from ASA using the **hw-module module 1 recover configure/boot** command.

  For the procedure, refer to Installing the AIP-SSM System Image.

Caution When you install the system image for your sensor, all accounts are removed and the default account and password are reset to cisco.

Obtaining a License Key From Cisco.com

This section describes how to obtain a license key from Cisco.com and how to install it using the CLI or IDM. It contains the following topics:

Overview

Although the sensor functions without the license key, you must have a license key to obtain signature updates. To obtain a license key, you must have the following:

- Cisco Service for IPS service contract

  Contact your reseller, Cisco service or product sales to purchase a contract. For more information, see Service Programs for IPS Products, page 11-9.

- Your IPS device serial number

  To find the IPS device serial number in IDM, click **Configuration > Licensing**, or in the CLI use the **show version** command.

- Valid Cisco.com username and password

Note You can install the first few signature updates for 5.*x* without a license. This gives you time to get your sensor licensed. If you are unable to get your sensor licensed because of confusion with your contract, you can obtain a 60-day trail license that supports signature updates that require licensing.

You can obtain a license key from the Cisco.com licensing server, which is then delivered to the sensor. Or, you can update the license key from a license key provided in a local file. Go to http://www.cisco.com/go/license and click **IPS Signature Subscription Service** to apply for a license key. For the procedure, see Obtaining and Installing the License, page 11-10.

Whenever you start IDM, a dialog box informs you of your license status—whether you have a trial, invalid, or expired license key. With no license key, an invalid license key, or an expired license key, you can continue to use IDM but you cannot download signature updates.

When you enter the CLI, you receive the following message if there is no license installed:

```
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
```

You will continue to see this message until you have installed a license.

Service Programs for IPS Products

You must have a Cisco Services for IPS service contract for any IPS product so that you can download a license key and obtain the latest IPS signature updates. If you have a direct relationship with Cisco Systems, contact your account manager or service account manager to purchase the Cisco Services for IPS service contract. If you do not have a direct relationship with Cisco Systems, you can purchase the service account from a one-tier or two-tier partner.

When you purchase the following IPS products you must also purchase a Cisco Services for IPS service contract:

- IDS-4215
- IPS-4240
- IPS-4255
- IPS-4260
- IDSM-2
- NM-CIDS

For ASA products, if you purchased one of the following ASA products that do not contain IPS, you must purchase a SMARTnet contract:

- ASA5510-K8
- ASA5510-DC-K8
- ASA5510-SEC-BUN-K9
- ASA5520-K8

- ASA5520-DC-K8
- ASA5520-BUN-K9
- ASA5540-K8
- ASA5540-DC-K8
- ASA5540-BUN-K9

Note SMARTnet provides operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

If you purchased one of the following ASA products that ships with the AIP-SSM installed or if you purchased AIP-SSM to add to your ASA product, you must purchase the Cisco Services for IPS service contract:

- ASA5510-AIP10-K9
- ASA5520-AIP10-K9
- ASA5520-AIP20-K9
- ASA5540-AIP20-K9
- ASA-SSM-AIP-10-K9
- ASA-SSM-AIP-20-K9

Note Cisco Services for IPS provides IPS signature updates, operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

For example, if you purchased an ASA-5510 and then later wanted to add IPS and purchased an ASA-SSM-AIP-10-K9, you must now purchase the Cisco Services for IPS service contract.

After you have the Cisco Services for IPS service contract, you must also have your product serial number to apply for the license key. For the procedure, see Obtaining and Installing the License, page 11-10.

Caution If you ever send your product for RMA, the serial number will change. You must then get a new license key for the new serial number.

Obtaining and Installing the License

This section describes how to obtain and install the license using IDM or the CLI. It contains the following topics:

Using IDM

Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key. For more information, see Service Programs for IPS Products, page 11-9.

To obtain and install the sensor license, follow these steps:

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

Step 2 Choose **Configuration > Licensing**.

The Licensing pane appears. Information about the current license state is displayed. If you have already installed your license, you can click **Download** to update it if needed.

Step 3 Choose the method to deliver the license:

a. Click **Cisco Connection Online** to obtain the license from Cisco.com.

IDM contacts the license server on Cisco.com and sends the server the serial number to obtain the license key. This is the default method. Go to Step 4.

b. Click **License File** to use a license file.

To use this option, you must apply for a license at www.cisco.com/go/license.

The license is sent to you in e-mail and you save it to a drive that is accessible by IDM. This option is useful if your computer does not have access to Cisco.com.

Go to Step 7.

Step 4 Click **Update License**.

The Licensing dialog box appears.

Step 5 Click **Yes** to continue.

The Status dialog box informs you that the sensor is trying to connect to Cisco.com.

An Information dialog box confirms that the license has been updated.

Step 6 Click **OK**.

Step 7 Go to www.cisco.com/go/license.

Step 8 Fill in the required fields.

Caution You must have the correct IPS device serial number because the license key only functions on the device with that number.

Your Cisco IPS Signature Subscription Service license key is sent by e-mail to the e-mail address you specified.

Step 9 Save the license file to a hard-disk drive or a network drive that is accessible by the client running IDM.

Step 10 Log in to IDM.

Step 11 Choose **Configuration > Licensing**.

Step 12 Under Update License, choose **Update From: License File**.

Step 13 In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file. he Select License File Path dialog box appears.

Step 14 Browse to the license file and click **Open**.

Step 15 Click **Update License**.

Using the CLI

Use the **copy** *source_url license_file_name* **license-key** command to copy the license file to your sensor.

The following options apply:

- *source_url*—The location of the source file to be copied. It can be a URL or keyword.
- *destination_url*—The location of the destination file to be copied. It can be a URL or a keyword.
- **license-key**—The subscription license file.
- *license_file_name*—The name of the license file you receive.

Note You cannot install an older license key over a newer license key.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

- ftp:—Source or destination URL for an FTP network server. The syntax for this prefix is:

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename
- scp:—Source or destination URL for the SCP network server. The syntax for this prefix is:

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename
- http:—Source URL for the web server. The syntax for this prefix is:

  http:[[/[username@]location]/directory]/filename
- https:—Source URL for the web server. The syntax for this prefix is:

  https:[[/[username@]location]/directory]/filename

  Note If you use FTP or SCP, you are prompted for a password.

Note If you use SCP, the remote host must be on the SSH known hosts list. For the procedure, refer to Adding Hosts to the Known Host List.

Note If you use HTTPS, the remote host must be a TLS trusted host. For the procedure, refer to Adding TLS Trusted Hosts.

To install the license key, follow these steps:

Step 1 Apply for the license key at this URL: www.cisco.com/go/license.

Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key. For more information, see Service Programs for IPS Products, page 11-9.

Step 2 Fill in the required fields.

Note You must have the correct IPS device serial number because the license key only functions on the device with that number.

Your Cisco IPS Signature Subscription Service license key is sent by e-mail to the e-mail address you specified.

Step 3 Save the license key to a system that has a web server, FTP server, or SCP server.

Step 4 Log in to the CLI using an account with administrator privileges.

Step 5 Copy the license key to the sensor:

```
sensor# copy scp://user@10.89.147.3://tftpboot/dev.lic license-key
Password: *******
```

Step 6 Verify the sensor is licensed:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R0JS
Licensed, expires: 19-Dec-2005 UTC
Sensor up-time is 2 days.
Using 706699264 out of 3974291456 bytes of available memory (17% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.5M out of 166.8M bytes of available disk space (23% usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)


MainApp          2005_Feb_18_03.00   (Release)   2008-02-18T03:13:47-0600   Running
AnalysisEngine   2005_Feb_15_03.00   (Release)   2008-02-15T12:59:35-0600   Running
CLI              2005_Feb_18_03.00   (Release)   2008-02-18T03:13:47-0600


Upgrade History:

    IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149


sensor#
```

Step 7 Copy your license key from a sensor to a server to keep a backup copy of the license:

```
sensor# copy license-key scp://user@10.89.147.3://tftpboot/dev.lic
Password: *******
sensor#
```

Cisco Security Intelligence Operations

The Cisco Security Intelligence Operations site on Cisco.com provides intelligence reports about current vulnerabilities and security threats. It also has reports on other security topics that help you protect your network and deploy your security systems to reduce organizational risk.

You should be aware of the most recent security threats so that you can most effectively secure and manage your network. Cisco Security Intelligence Operations contains the top ten intelligence reports listed by date, severity, urgency, and whether there is a new signature available to deal with the threat.

Cisco Security Intelligence Operations contains a Security News section that lists security articles of interest. There are related security tools and links.

You can access Cisco Security Intelligence Operations at this URL:

http://tools.cisco.com/security/center/home.x

Cisco Security Intelligence Operations is also a repository of information for individual signatures, including signature ID, type, structure, and description.

You can search for security alerts and signatures at this URL:

http://tools.cisco.com/security/center/search.x

Accessing IPS Documentation

You can find IPS documentation at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

Or to access IPS documentation from Cisco.com, follow these steps:

Step 1 Log in to Cisco.com.

Step 2 Click **Support**.

Step 3 Under Support at the bottom of the page, click **Documentation**.

Step 4 Choose **Products > Security > Intrusion Prevention System (IPS) > IPS Appliances > Cisco IPS 4200 Series Sensors**. The Cisco IPS 4200 Series Sensors page appears. All of the most up-to-date IPS documentation is on this page.

Note Although you will see references to other IPS documentation sites on Cisco.com, this is the site with the most complete and up-to-date IPS documentation.

Step 5 Click one of the following categories to access Cisco IPS documentation:

- **Download Software**—Takes you to the Download Software site.

Note You must be logged into Cisco.com to access the software download site.

- **Release and General Information**—Contains documentation roadmaps and release notes.
- **Reference Guides**—Contains command references and technical references.
- **Design**—Contains design guide and design tech notes.
- **Install and Upgrade**—Contains hardware installation and regulatory guides.
- **Configure**—Contains configuration guides for IPS CLI, IDM, and IME.
- **Troubleshoot and Alerts**—Contains TAC tech notes and field notices.

GLOSSARY

Numerals

3DES Triple Data Encryption Standard. A stronger version of DES, which is the default encryption method for SSH version 1.5. Used when establishing an SSH session with the sensor. It can be used when the sensor is managing a device.

A

aaa authentication, authorization, and accounting. The primary and recommended method for access control in Cisco devices.

AAA authentication, authorization, and accounting. Pronounced “triple a.”

ACE Access Control Entry. An entry in the ACL that describes what action should be taken for a specified address or protocol. The sensor adds/removes ACE to block hosts.

ACK acknowledgement. Notification sent from one network device to another to acknowledge that some event occurred (for example, the receipt of a message).

ACL Access Control List. A list of ACEs that control the flow of data through a router. There are two ACLs per router interface for inbound data and outbound data. Only one ACL per direction can be active at a time. ACLs are identified by number or by name. ACLs can be standard, enhanced, or extended. You can configure the sensor to manage ACLs.

action The sensor’s response to an event. An action only happens if the event is not filtered. Examples include TCP reset, block host, block connection, IP logging, and capturing the alert trigger packet.

active ACL The ACL created and maintained by ARC and applied to the router block interfaces.

AIC engine Application Inspection and Control engine. Provides deep analysis of web traffic. It provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It allows administrative control over applications that try to tunnel over specified ports, such as instant messaging, and tunneling applications, such as gotomypc. It can also inspect FTP traffic and control the commands being issued.

AIP-SSM Advanced Inspection and Prevention Security Services Module. The IPS plug-in module in the Cisco ASA 5500 series adaptive security appliance. See ASA.

Alarm Channel The IPS software module that processes all signature events generated by the inspectors. Its primary function is to generate alerts for each event it receives.

alert Specifically, an IPS event type; it is written to the Event Store as an evidsAlert. In general, an alert is an IPS message that indicates a network exploit in progress or a potential security problem occurrence. Also known as an alarm.

Analysis Engine The IPS software module that handles sensor configuration. It maps the interfaces and also the signature and alarm channel policy to the configured interfaces. It performs packet analysis and alert detection.

API Application Programming Interface. The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. Computer application programs run a set of standard software interrupts, calls, and data formats to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create links that an application needs to communicate with the operating system or with the network.

application Any program (process) designed to run in the Cisco IPS environment.

application instance A specific application running on a specific piece of hardware in the IPS environment. An application instance is addressable by its name and the IP address of its host computer.

ARC Attack Response Controller. Formerly known as Network Access Controller (NAC). A component of the IPS. A software module that provides block and unblock functionality where applicable.

architecture The overall structure of a computer or communication system. The architecture influences the capabilities and limitations of the system.

ARP Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.

ASA Adaptive Security Appliance. The ASA combines firewall, VPN concentrator, and intrusion prevention software functionality into one software image. You can configure ASA in single mode or multi-mode.

ASDM Adaptive Security Device Manager. A web-based application that lets you configure and manage your ASA.

atomic attack Represents exploits contained within a single packet. For example, the “ping of death” attack is a single, abnormally large ICMP packet.

Atomic engine There are two Atomic engines: Atomic IP inspects IP protocol packets and associated Layer-4 transport protocols, and Atomic ARP inspects Layer-2 ARP protocol.

attack An assault on system security that derives from an intelligent threat, that is, an intelligent act that is a deliberate attempt (especially in the sense of method or technique) to evade security services and violate the security policy of a system.

authentication Process of verifying that a user has permission to use the system, usually by means of a password key or certificate.

AuthenticationApp A component of the IPS. It verifies that users have the correct permissions to perform CLI, IDM, or RDEP actions.

B

backplane The physical connection between an interface processor or card and the data buses and the power distribution buses inside a chassis.

base version A software release that must be installed before a follow-up release such as a service pack or signature update can be installed. Major and minor version upgrades are base version releases.

benign trigger A situation in which a signature is fired correctly, but the source of the traffic is nonmalicious.

BIOS Basic Input/Output System. The program that starts the sensor and communicates between the devices in the sensor and the system.

block The ability of the sensor to direct a network device to deny entry to all packets from a specified network host or network.

block interface The interface on the network device that the sensor manages.

BO2K BackOrifice 2000. A windows back door Trojan that runs over TCP and UDP.

Bpdu Bridge Protocol Data Unit. Spanning-Tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network.

bypass mode Mode that lets packets continue to flow through the sensor even if the sensor fails. Bypass mode is only applicable to inline-paired interfaces.

C

CA certification authority. Entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. Sensors use self-signed certificates.

CA certificate Certificate for one CA issued by another CA.

certificate Digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.

cidDump A script that captures a large amount of information including the IPS processes list, log files, OS information, directory listings, package information, and configuration files.

CIDEE Cisco Intrusion Detection Event Exchange. Specifies the extensions to SDEE that are used by Cisco IPS systems. The CIDEE standard specifies all possible extensions that may be supported by Cisco IPS systems.

CIDS header The header that is attached to each packet in the IPS system. It contains packet classification, packet length, checksum results, timestamp, and the receive interface.

cipher key The secret binary data used to convert between clear text and cipher text. When the same cipher key is used for both encryption and decryption, it is called symmetric. When it is used for either encryption or decryption (but not both), it is called asymmetric.

Cisco IOS Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS allows centralized, integrated, and automated installation and management of internetworks while supporting a wide variety of protocols, media, services, and platforms.

CLI command-line interface. A shell provided with the sensor used for configuring and controlling the sensor applications.

command and control interface The interface on the sensor that communicates with the IPS manager and other network devices. This interface has an assigned IP address.

community In SNMP, a logical group of managed devices and NMSs in the same administrative domain.

composite attack Spans multiple packets in a single session. Examples include most conversation attacks such as FTP, Telnet, and most Regex-based attacks.

connection block ARC blocks traffic from a given source IP address to a given destination IP address and destination port.

console A terminal or laptop computer used to monitor and control the sensor.

console port An RJ45 or DB9 serial port on the sensor that is used to connect to a console device.

control interface When ARC opens a Telnet or SSH session with a network device, it uses one of the device's routing interfaces as the remote IP address. This is the control interface.

control transaction An IPS message containing a command addressed to a specific application instance. Example control transactions include *start*, *stop*, *getConfig*.

cookie A piece of information sent by a web server to a web browser that the browser is expected to save and send back to the web server whenever the browser makes additional requests of the web server.

D

Database Processor See DBP.

datagram Logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms cell, frame, message, packet, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

DBP Database Processor. Maintains the signature state and flow databases.

DCE data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. Modems and interface cards are examples of DCE.

DDoS Distributed Denial of Service. An attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

Deny Filters Processor See DFP.

DES Data Encryption Standard. A strong encryption method where the strength lies in a 56-bit key rather than an algorithm.

destination address Address of a network device that is receiving data.

DFP Deny Filters Processor. Handles the deny attacker functions. It maintains a list of denied source IP addresses.

DIMM Dual In-line Memory Modules.

DMZ demilitarized zone. A separate network located in the neutral zone between a private (inside) network and a public (outside) network.

DNS Domain Name System. An Internet-wide hostname to IP address mapping. DNS enables you to convert human-readable names into the IP addresses needed for network packets.

DoS Denial of Service. An attack whose goal is just to disrupt the operation of a specific system or network.

DRAM dynamic random-access memory. RAM that stores information in capacitors that must be refreshed periodically. Delays can occur because DRAMs are inaccessible to the processor when refreshing their contents. However, DRAMs are less complex and have greater capacity than SRAMs.

DTE Data Terminal Equipment. Refers to the role of a device on an RS-232C connection. A DTE writes data to the transmit line and reads data from the receive line.

E

egress Traffic leaving the network.

encryption Application of a specific algorithm to data to alter the appearance of the data making it incomprehensible to those who are not authorized to see the information.

engine A component of the sensor designed to support many signatures in a certain category. Each engine has parameters that can be used to create signatures or tune existing signatures.

enterprise network Large and diverse network connecting most major points in a company or other organization. Differs from a WAN in that it is privately owned and maintained.

escaped expression Used in regular expression. A character can be represented as its hexadecimal value, for example, \x61 equals ‘a,’ so \x61 is an escaped expression representing the character ‘a.’

ESD electrostatic discharge. Electrostatic discharge is the rapid movement of a charge from one object to another object, which produces several thousand volts of electrical charge that can cause severe damage to electronic components or entire circuit card assemblies.

event An IPS message that contains an alert, a block request, a status message, or an error message.

Event Server One of the components of the IPS.

Event Store One of the components of the IPS. A fixed-size, indexed store used to store IPS events.

evIdsAlert The XML entity written to the Event Store that represents an alert.

F

fail closed Blocks traffic on the device after a hardware failure.

fail open Lets traffic pass through the device after a hardware failure.

false negative A signature is not fired when offending traffic is detected.

false positive Normal traffic or a benign action causes a signature to fire.

Fast Ethernet Any of a number of 100-Mbps Ethernet specifications. Fast Ethernet offers a speed increase 10 times that of the 10BaseT Ethernet specification while preserving such qualities as frame format, MAC mechanisms, and MTU. Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks. Based on an extension to the IEEE 802.3 specification.

firewall Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

Flood engine Detects ICMP and UDP floods directed at hosts and networks.

flooding Traffic passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was received originally.

fragment Piece of a larger packet that has been broken down to smaller units.

fragmentation Process of breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

Fragment Reassembly Processor See FRP.

FRP Fragment Reassembly Processor. Reassembles fragmented IP datagrams. It is also responsible for normalization of IP fragments when the sensor is in inline mode.

FTP File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

FTP server File Transfer Protocol server. A server that uses the FTP protocol for transferring files between network nodes.

full duplex Capability for simultaneous data transmission between a sending station and a receiving station.

FWSM Firewall Security Module. A module that can be installed in a Catalyst 6500 series switch. It uses the **shun** command to block. You can configure the FWSM in either single mode or multi-mode.

G

Gigabit Ethernet Standard for a high-speed Ethernet, approved by the IEEE (Institute of Electrical and Electronics Engineers) 802.3z standards committee in 1996.

GMT Greenwich Mean Time. Time zone at zero degrees longitude. Now called Coordinated Universal Time (UTC).

H

H.225.0 An ITU standard that governs H.225.0 session establishment and packetization. H.225.0 actually describes several different protocols: RAS, use of Q.931, and use of RTP.

H.245 An ITU standard that governs H.245 endpoint control.

H.323 Allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods.

half duplex Capability for data transmission in only one direction at a time between a sending station and a receiving station. BSC is an example of a half-duplex protocol.

handshake Sequence of messages exchanged between two or more network devices to ensure transmission synchronization.

hardware bypass Passes traffic at the network interface, does not pass it to the IPS system.

host block ARC blocks all traffic from a given IP address.

HTTP Hypertext Transfer Protocol. The stateless request/response media transfer protocol used in the IPS architecture for remote data exchange.

HTTPS An extension to the standard HTTP protocol that provides confidentiality by encrypting the traffic from the website. By default this protocol uses TCP port 443.

I

ICMP Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

ICMP flood Denial of Service attack that sends a host more ICMP echo request (“ping”) packets than the protocol implementation can handle.

IDAPI Intrusion Detection Application Programming Interface. Provides a simple interface between IPS architecture applications. IDAPI reads and writes event data and provides a mechanism for control transactions.

IDCONF Intrusion Detection Configuration. A data format standard that defines operational messages that are used to configure intrusion detection and prevention systems.

IDIOM Intrusion Detection Interchange and Operations Messages. A data format standard that defines the event messages that are reported by intrusion detection systems and the operational messages that are used to configure and control intrusion detection systems.

IDM IPS Device Manager. A web-based application that lets you configure and manage your sensor. The web server for IDM resides on the sensor. You can access it through Netscape or Internet Explorer web browsers.

IDMEF Intrusion Detection Message Exchange Format. The IETF Intrusion Detection Working Group draft standard.

IDSM-2 Intrusion Detection System Module. A switching module that performs intrusion detection in the Catalyst 6500 series switch.

IDS MC Management Center for IDS Sensors. A web-based IDS manager that can manage configurations for up to 300 sensors.

inline mode All packets entering or leaving the network must pass through the sensor.

inline interface A pair of physical interfaces configured so that the sensor forwards all traffic received on one interface out to the other interface in the pair.

interface group Refers to the logical grouping of sensing interfaces. Multiple sensing interfaces can be assigned to a logical interface group. Signature parameters are tuned on a per-logical interface group basis.

intrusion detection system A security service that monitors and analyzes system events to find and provide real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

IP address 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

IPS Intrusion Prevention System. A system that alerts the user to the presence of an intrusion on the network through network traffic analysis techniques.

IPS data or message Describes the messages transferred over the command and control interface between IPS applications.

iplog A log of the binary packets to and from a designated address. Iplogs are created when the log Event Action is selected for a signature. Iplogs are stored in a libpcap format, which can be read by WireShark and TCPDUMP.

IP spoofing IP spoofing attack occurs when an attacker outside your network pretends to be a trusted user either by using an IP address that is within the range of IP addresses for your network or by using an authorized external IP address that you trust and to which you want to provide access to specified resources on your network. Should an attacker get access to your IPSec security parameters, that attacker can masquerade as the remote user authorized to connect to the corporate network.

IPv6 IP version 6. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

L

L2P Layer 2 Processor. Processes layer 2-related events. It also identifies malformed packets and removes them from the processing path.

LAN Local Area Network. Refers to the Layer 2 network domain local to a given host. Packets exchanged between two hosts on the same LAN do not require Layer 3 routing.

Layer 2 Processor See L2P.

Logger A component of the IPS.

logging Gathers actions that have occurred in a log file. Logging of security information is performed on two levels: logging of events (such as IPS commands, errors, and alerts), and logging of individual IP session information.

LOKI Remote access, back door Trojan, ICMP tunneling software. When the computer is infected, the malicious code creates an ICMP tunnel that can be used to send small payload ICMP replies

M

MainApp The main application in the IPS. The first application to start on the sensor after the operating system has booted.

maintenance partition image A full IPS image used to reimage the maintenance partition of the IDSM-2.

major update A base version that contains major new functionality or a major architectural change in the product.

manufacturing image Full IPS system image used by manufacturing to image sensors.

master blocking sensor A remote sensor that controls one or more devices. Blocking forwarding sensors send blocking requests to the master blocking sensor and the master blocking sensor executes the blocking requests.

MD5 Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

MEG Mega Event Generator. Signature based on the Meta engine. The Meta engine takes alerts as input rather than packets.

Meta engine Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.

MIB Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MIME Multipurpose Internet Mail Extension. Standard for transmitting nontext data (or data that cannot be represented in plain ASCII code) in Internet mail, such as binary, foreign language text (such as Russian or Chinese), audio, or video data. MIME is defined in RFC 2045.

minor update A minor version that contains minor enhancements to the product line. Minor updates are incremental to the major version, and are also base versions for service packs.

module A removable card in a switch, router, or security appliance chassis. AIP SSM, IDSM-2, and NM-CIDS are IPS modules.

monitoring interface See sensing interface.

MSFC, MSFC2 Multilayer Switch Feature Card. An optional card on a Catalyst 6000 supervisor engine that performs L3 routing for the switch.

MSRPC Microsoft Remote Procedure Call.

N

NAC Network Access Controller. See ARC.

NAT Native Address Translation. A network device can present an IP address to the outside networks that is different from the actual IP address of a host.

NBD Next Business Day. The arrival of replacement hardware according to Cisco service contracts.

network device A device that controls IP traffic on a network and can block an attacking host. An example of a network device is a Cisco router or PIX Firewall.

never block address Hosts and networks you have identified that should never be blocked.

never shun address See never block address.

NIC Network Interface Card. Board that provides network communication capabilities to and from a computer system.

NM-CIDS A network module that integrates IPS functionality into the branch office router.

NMS network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

node A physical communicating element on the command and control network. For example, an appliance, an IDSM-2, or a router.

Normalizer engine Configures how the IP and TCP normalizer functions and provides configuration for signature events related to the IP and TCP normalizer.

NTP Network Timing Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

NTP server Network Timing Protocol server. A server that uses NTP. NTP is a protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

NVRAM Non-Volatile Read/Write Memory. RAM that retains its contents when a unit is powered off.

O

OIR online insertion and removal. Feature that permits you to add, replace, or remove cards without interrupting the system power, entering console commands, or causing other software or interfaces to shutdown.

P

packet Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data. The terms datagram, frame, message, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

PASC Port Spoof An attempt to open connections through a firewall to a protected FTP server to a non-FTP port. This happens when the firewall incorrectly interprets an FTP 227 (Entering Passive Mode) command by opening an unauthorized connection.

passive fingerprinting Act of determining the OS or services available on a system from passive observation of network interactions.

PAT Port Address Translation. A more restricted translation scheme than NAT in which a single IP address and different ports are used to represent the hosts of a network.

PCI Peripheral Component Interface. The most common peripheral expansion bus used on Intel-based computers.

PDU protocol data unit. OSI term for packet. See also BPDU and packet.

PEP Cisco Product Evolution Program. PEP is the UDI information that consists of the PID, the VID, and the SN of your sensor. PEP provides hardware version and serial number visibility through electronic query, product labels, and shipping items.

PER packed encoding rules. Instead of using a generic style of encoding that encodes all types in a uniform way, PER specializes the encoding based on the date type to generate much more compact representations.

PFC Policy Feature Card. An optional card on a Catalyst 6000 supervisor engine that supports VACL packet filtering.

PID Product Identifier. The orderable product identifier that is one of the three parts of the UDI. The UDI is part of the PEP policy.

ping packet internet groper. ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

PIX Firewall Private Internet Exchange Firewall. A Cisco network security device that can be programmed to block/enable addresses and ports between networks.

PKI Public Key Infrastructure. Authentication of HTTP clients using the clients' X.509 certificates.

POST Power-On Self Test. Set of hardware diagnostics that runs on a hardware device when that device is powered up.

Post-ACL Designates an ACL from which ARC should read the ACL entries, and where it places entries after all deny entries for the addresses being blocked.

Pre-ACL Designates an ACL from which ARC should read the ACL entries, and where it places entries before any deny entries for the addresses being blocked.

promiscuous mode A passive interface for monitoring packets of the network segment. The sensing interface does not have an IP address assigned to it and is therefore invisible to attackers.

Q

Q.931 ITU-T specification for signaling to establish, maintain, and clear ISDN network connections.

R

rack mounting Refers to mounting a sensor in an equipment rack.

RAM random-access memory. Volatile memory that can be read and written by a microprocessor.

RAS Registration, Admission, and Status Protocol. Protocol that is used between endpoints and the gatekeeper to perform management functions. RAS signalling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.

RDEP2 Remote Data Exchange Protocol version 2. The published specification for remote data exchange over the command and control network using HTTP and TLS.

reassembly The putting back together of an IP datagram at the destination after it has been fragmented either at the source or at an intermediate node.

recovery partition image An IPS image file that includes the full application image and installer used for recovery on sensors.

regex See regular expression.

regular expression A mechanism by which you can define how to search for a specified sequence of characters in a data stream or file. Regular expressions are a powerful and flexible notation almost like a mini-programming language that allow you to describe text. In the context of pattern matching, regular expressions allow a succinct description of any arbitrary pattern.

ROMMON Read-Only-Memory Monitor. ROMMON lets you TFTP system images onto the sensor for recovery purposes.

round-trip time See RTT.

RPC remote-procedure call. Technological foundation of client/server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.

RR Risk Rating. An RR is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.

RSM Router Switch Module. A router module that is installed in a Catalyst 5000 switch. It functions exactly like a standalone router.

RTP Real-Time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.

RTT round-trip time. A measure of the time delay imposed by a network on a host from the sending of a packet until acknowledgement of the receipt.

RU rack unit. A rack is measured in rack units. An RU is equal to 44 mm or 1.75 inches.

S

SAP Signature Analysis Processor. Dispatches packets to the inspectors that are not stream-based and that are configured for interest in the packet in process.

SCEP Simple Certificate Enrollment Protocol. The Cisco Systems PKI communication protocol that leverages existing technology by using PKCS#7 and PKCS#10. SCEP is the evolution of the enrollment protocol.

SDEE Security Device Event Exchange. A product-independent standard for communicating security device events. It is an enhancement to RDEP. It adds extensibility features that are needed for communicating events generated by various types of security devices.

SDP Slave Dispatch Processor.

SEAF signature event action filter. Subtracts actions based on the signature event's signature ID, addresses, and RR. The input to the SEAF is the signature event with actions possibly added by the SEAO.

SEAH signature event action handler. Performs the requested actions. The output from SEAH is the actions being performed and possibly an <evIdsAlert> written to the Event Store.

SEAO signature event action override. Adds actions based on the RR value. SEAO applies to all signatures that fall into the range of the configured RR threshold. Each SEAO is independent and has a separate configuration value for each action type.

SEAP Signature Event Action Processor. Processes event actions. Event actions can be associated with an event risk rating (RR) threshold that must be surpassed for the actions to take place.

Secure Shell Protocol Protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.

Security Monitor Monitoring Center for Security. Provides event collection, viewing, and reporting capability for network devices. Used with the IDS MC.

sensing interface The interface on the sensor that monitors the desired network segment. The sensing interface is in promiscuous mode; it has no IP address and is not visible on the monitored segment.

sensor The sensor is the intrusion detection engine. It analyzes network traffic searching for signs of unauthorized activity.

SensorApp A component of the IPS. Performs packet capture and analysis. SensorApp analyzes network traffic for malicious content. Packets flow through a pipeline of processors fed by a producer designed to collect packets from the network interfaces on the sensor. Sensorapp is the standalone executable that runs Analysis Engine.

Service engine Deals with specific protocols, such as DNS, FTP, H255, HTTP, IDENT, MS RPC, MS SL. NTP, RPC, SMB, SNMP, and SSH.

service pack Used for the release of bug fixes with no new enhancements. Service packs are cumulative following a base version release (minor or major).

session command Command used on routers and switches to provide either Telnet or console access to a module in the router or switch.

shun command Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection. It is used by ARC when blocking with a PIX Firewall.

Signature Analysis Processor See SAP.

signature A signature distills network information and compares it against a rule set that indicates typical intrusion activity.

signature engine A component of the sensor that supports many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters that have allowable ranges or sets of values.

signature event action filter See SEAF.

signature event action handler See SEAH.

signature event action override See SEAO.

signature event action processor See SEAP.

signature update Executable image that updates the IPS signature analysis engine (SensorApp) and the NSDB. Applying an IPS signature update is like updating virus definitions on a virus scanning program. Signature updates are released independently and have their own versioning scheme.

Slave Dispatch Processor See SDP.

SMB Server Message Block. File-system protocol used in LAN manager and similar NOSs to package data and exchange information with other systems.

SMTP Simple Mail Transfer Protocol. Internet protocol providing e-mail services.

SN Serial Number. Part of the UDI. The SN is the serial number of your Cisco product.

sniffing interface See sensing interface.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP2 SNMP Version 2. Version 2 of the network management protocol. SNMP2 supports centralized and distributed network management strategies, and includes improvements in the SMI, protocol operations, management architecture, and security.

software bypass Passes traffic through the IPS system without inspection.

source address Address of a network device that is sending data.

SP Statistics Processor. Keeps track of system statistics such as packet counts and packet arrival rates.

SPAN Switched Port Analyzer. Feature of the Catalyst 5000 switch that extends the monitoring abilities of existing network analyzers into a switched Ethernet environment. SPAN mirrors the traffic at one switched segment onto a predefined SPAN port. A network analyzer attached to the SPAN port can monitor traffic from any other Catalyst switched port.

spanning tree Loop-free subset of a network topology.

SQL Structured Query Language. International standard language for defining and accessing relational databases.

SRAM Type of RAM that retains its contents for as long as power is supplied. SRAM does not require constant refreshing, like DRAM

SRP Stream Reassembly Processor. Reorders TCP streams to ensure the arrival order of the packets at the various stream-based inspectors. It is also responsible for normalization of the TCP stream. The normalizer engine lets you enable or disable alert and deny actions.

SSH Secure Shell. A utility that uses strong authentication and secure communications to log in to another computer over a network.

SSL Secure Socket Layer. Encryption technology for the Internet used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

Stacheldraht A DDoS tool that relies on the ICMP protocol.

State engine Stateful searches of HTTP strings.

Statistics Processor See SP.

Stream Reassembly Processor See SRP.

String engine A signature engine that provides regular expression-based pattern inspection and alert functionality for multiple transport protocols, including TCP, UDP, and ICMP.

subsignature A more granular representation of a general signature. It typically further defines a broad scope signature.

surface mounting Refers to attaching rubber feet to the bottom of a sensor when it is installed on a flat surface. The rubber feet allow proper airflow around the sensor and they also absorb vibration so that the hard-disk drive is less impacted.

switch Network device that filters, forwards, and floods frames based on the destination address of each frame. The switch operates at the data link layer of the OSI model.

SYN flood Denial of Service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.

system image The full IPS application and recovery image used for reimaging an entire sensor.

T

TAC A Cisco Technical Assistance Center. There are four TACs worldwide.

TACACS+ Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

tcpdump The tcpdump utility is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can use different options for viewing summary and detail information for each packet. For more information, refer to http://www.tcpdump.org/.

TCP reset interface The interface on the IDS-4250-XL and IDSM-2 that can send TCP resets. On most sensors the TCP resets are sent out on the same sensing interface on which the packets are monitored, but on the IDS-4250-XL and IDSM-2 the sensing interfaces cannot be used for sending TCP resets. On the IDS-4250-XL the TCP reset interface is the onboard 10/100/100 TX interface, which is normally used on the IDS-4250-TX appliance when the XL card is not present. On the IDSM-2 the TCP reset interface is designated as port 1 with Catalyst software, and is not visible to the user in Cisco IOS software. The TCP reset action is only appropriate as an action selection on those signatures that are associated with a TCP-based service.

Telnet Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

terminal server A router with multiple, low speed, asynchronous ports that are connected to other serial devices. Terminal servers can be used to remotely manage network equipment, including sensors.

TFN2K Tribe Flood Network 2000. A common type of Denial of Service (DoS) attack that can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks.

TFTP Trivial File Transfer Protocol. Simplified version of FTP that lets files be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

three-way handshake Process whereby two protocol entities synchronize during connection establishment.

threshold A value, either upper- or lower-bound that defines the maximum/minimum allowable condition before an alarm is sent.

Time Processor See TP.

TLS Transport Layer Security. The protocol used over stream transports to negotiate the identity of peers and establish encrypted communications.

topology Physical arrangement of network nodes and media within an enterprise networking structure.

TP Time Processor. Processes events stored in a time-slice calendar. Its primary task is to make stale database entries expire and to calculate time-dependent statistics.

TPKT RFC 1006-defined method of demarking messages in a packet.

traceroute Program available on many systems that traces the path a packet takes to a destination. It is used mostly to debug routing problems between hosts. A traceroute protocol is also defined in RFC 1393.

traffic analysis Inference of information from observable characteristics of data flow(s), even when the data is encrypted or otherwise not directly available. Such characteristics include the identities and locations of the source(s) and destination(s), and the presence, amount, frequency, and duration of occurrence.

Traffic ICMP engine Analyzes traffic from nonstandard protocols, such as TFN2K, LOKI, and DDOS.

Transaction Server A component of the IPS.

Transaction Source A component of the IPS.

trap Message sent by an SNMP agent to an NMS, a console, or a terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

Trojan engine Analyzes traffic from nonstandard protocols, such as BO2K and TFN2K.

trunk Physical and logical connection between two switches across which network traffic travels. A backbone is composed of a number of trunks.

trusted certificate Certificate upon which a certificate user relies as being valid without the need for validation testing; especially a public-key certificate that is used to provide the first public key in a certification path.

trusted key Public key upon which a user relies; especially a public key that can be used as the first public key in a certification path.

tune Adjusting signature parameters to modify an existing signature.

U

UDI Unique Device Identifier. Provides a unique identity for every Cisco product. The UDI is composed of the PID, VID, and SN. The UDI is stored in the Cisco IPS ID PROM.

UDP User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

unblock To direct a router to remove a previously applied block.

UPS Uninterruptable Power Source.

UTC Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

V

VACL VLAN ACL. An ACL that filters all packets (both within a VLAN and between VLANs) that pass through a switch. Also known as security ACLs.

VID Version identifier. Part of the UDI.

virtual sensor A logical grouping of sensing interfaces and the configuration policy for the signature engines and alarm filters to apply to them. In other words, multiple virtual sensors running on the same appliance, each configured with different signature behavior and traffic feeds. IPS 5.x supports only one virtual sensor.

virus Hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting—that is, inserting a copy of itself into and becoming part of—another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

virus update A signature update specifically addressing viruses.

VLAN Virtual Local Area Network. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VMS CiscoWorks VPN/Security Management Solution. A suite of network security applications that combines web-based tools for configuring, monitoring, and troubleshooting enterprise VPN, firewalls, network intrusion detection systems and host-based intrusion prevention systems.

VoIP Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

VPN Virtual Private Network(ing). Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

vulnerability One or more attributes of a computer or a network that permit a subject to initiate patterns of misuse on that computer or network.

W

WAN wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.

Web Server A component of the IPS.

Wireshark Wireshark is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Wireshark has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. For more information, refer to http://www.wireshark.org.

worm A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and can consume computer resources destructively.

X

X.509 Standard that defines information contained in a certificate.

XML eXtensible Markup Language. Textual file format used for data interchange between heterogeneous hosts.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

X