



CHAPTER 9

Intrusion Detection System Module

This chapter describes the Intrusion Detection System Module (WS-X6381-IDS).

The Intrusion Detection System Module (IDSM) is part of the Cisco Secure Intrusion Detection System (Cisco Secure IDS) and is managed by the Cisco Secure Policy Manager (Cisco Secure PM). (See [Figure 9-1](#).) Cisco Secure PM provides a graphical interface for the management of security across a distributed network. The Intrusion Detection System Module performs network sensing, which involves real-time monitoring of network packets: packet capture and analysis.



Note

Specific combinations of supervisor engines and modules may not be supported in your chassis. Refer to the release notes of the software version running on your system for specific information on modules and supervisor engine combinations that are not supported.

The Intrusion Detection System Module captures network packets, and then reassembles and compares this data against a set of rules that indicates typical intrusion activity. Network traffic is copied either to the Intrusion Detection System Module based on security VLAN access control lists (VACLs) in the switch or is routed to the Intrusion Detection System Module using the switch's Switched Port Analyzer (SPAN) port feature. Both methods allow user-specified types of traffic that are based on switch ports, VLANs, or traffic type to be inspected.

The Intrusion Detection System Module searches for patterns of misuse by examining either the data portion or the header portion of network packets. Content-based attacks come from the data portion, and context-based attacks come from the header portion.

When the Intrusion Detection System Module detects an attack, it generates an alarm. Alarms are generated by the Intrusion Detection System Module through the Cisco 7600 series router backplane to the Cisco Secure PM, where they are logged or displayed on a graphical user interface. Alarm communication is handled by the Cisco Secure IDS Communication service protocol, a proprietary protocol that transmits alarms from the Intrusion Detection System Module to the Cisco Secure PM.

The front panel has a STATUS LED, a hard drive LED, a SHUTDOWN button, and a PCMCIA slot as shown in [Figure 9-1](#).

Figure 9-1 Intrusion Detection System Module (WS-X6381-IDS)

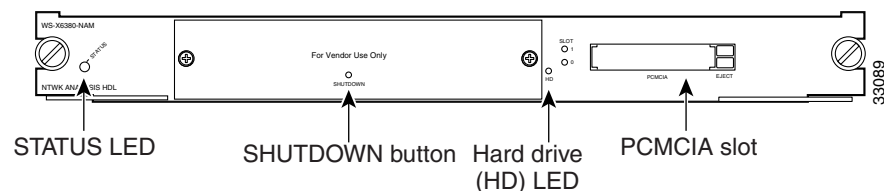


Table 9-1 describes the Intrusion Detection System Module states as indicated by the STATUS LED.

Table 9-1 Intrusion Detection System Module STATUS LED Description

Color/State	Description
Green	All diagnostics test pass. The module is operational.
Red	A diagnostic other than an individual port test failed.
Amber	The module is running through its boot and self-test diagnostics sequence.
	The IDSM is disabled.
Off	The IDSM power is off.

The SHUTDOWN button manually shuts down the Intrusion Detection System Module. To prevent corruption of the module, it is critical that you shut down the module properly. To properly shut down the switching module, session into the Intrusion Detection System Module from the Cisco 7600 series router console and enter the **shutdown** command. If the Intrusion Detection System Module fails to respond to the **shutdown** command, press the SHUTDOWN button to manually shut down the Intrusion Detection System Module.



Caution

Do not remove the Intrusion Detection System Module from the switch until after the module shuts down completely. Removing the module without going through a shutdown procedure can damage the module.

Use a small pointed object, such as a paper clip, to access the SHUTDOWN button and turn off the Intrusion Detection System Module. The shutdown procedure may take several minutes.

The HD (hard drive) activity LED indicates when the hard drive is in use.

The PCMCIA slot provides access for up to two standard PCMCIA cards and is reserved for future use.