Text Part Number: 78-5527-01

Catalyst 5000 Series Network Analysis Module Configuration Note

Product Number: WS-X5380(=), WS-X5381(=)

This configuration note contains instructions on how to install and configure the Catalyst 5000 series Network Analysis Module.

For a complete description of commands used to configure and maintain Catalyst 5000 series switches, refer to the *Catalyst 5000 Series Software Configuration Guide* and the *Catalyst 5000 Series Command Reference* publication. For complete switch hardware configuration and maintenance procedures, refer to the *Catalyst 5000 Series Installation Guide*. For information on Catalyst 5000 series switching modules, refer to the *Catalyst 5000 Series Module Installation Guide*. These documents are available on the Cisco Connection Documentation, Enterprise Series CD, or in print.

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Document Contents

This document is divided into the following sections:

Network Analysis Module Features

The Network Analysis Module, shown in Figure 1, provides RMON and RMON2 support for Ethernet VLANs to monitor applications and analyze traffic, which extends the Remote Monitoring (RMON) support provided by the Catalyst 5000 series supervisor engine. The module acts as a network data-gathering agent and provides network traffic monitoring when used with a client equipped with network monitoring software. The Network Analysis Module supports the following RMON groups (see the “Supported RMON and RMON2 MIB Objects” section on page 13 for details):

- RMON groups defined in RFC 1757
  - Hosts (RMON group 4)
  - HostTopN (RMON group 5)
  - Matrix (RMON group 6)
  - Filter (RMON group 7)
  - Capture (RMON group 8)
- RMON2 groups defined in RFC 2021
  - ProtocolDirectory (RMON2 group 11)
  - ProtocolDistribution (RMON2 group 12)
  - AddressMap (RMON2 group 13)
  - NlHost (RMON2 group 14)
  - NlMatrix (RMON2 group 15)
  - AlHost (RMON2 group 16)
  - AlMatrix (RMON2 group 17)
  - UsrHistory (RMON2 group 18)

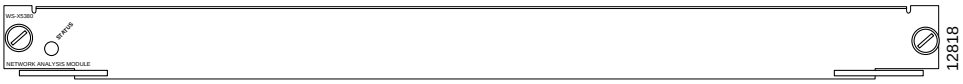
The Network Analysis Module can analyze Ethernet virtual LAN (VLAN) traffic from either or both:

- The Switched Port Analyzer (SPAN) source: one or more Ethernet ports or a Fast Ethernet port or a Fast Ethernet trunk port or an Ethernet VLAN
- NetFlow Data Export (NDE) from a NetFlow Feature Card (NFFC or NFFC II)

Note When monitoring a VLAN or a Fast Ethernet port or more than two Ethernet ports, use a Supervisor Engine III module in the system to ensure the most reliable SNMP access to the Network Analysis Module under heavy traffic conditions.

The Network Analysis Module is managed and controlled from a simple network management protocol (SNMP) management application, such as CiscoWorks2000.

Figure 1 Network Analysis Module (WS-X5380 and WS-X5381)



Status LED

Each Network Analysis Module contains a STATUS LED, shown in Figure 2, and described in Table 1.

Figure 2 Network Analysis Module (WS-X5380 and WS-X5381) LEDs

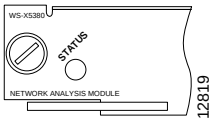


Table 1 Network Analysis Module (WS-X5380 and WS-X5381) LED Descriptions

LED	Description
STATUS	The switch performs a series of self-tests and diagnostic tests. If all the tests pass, the LED is green. If a test other than an individual port test fails, the LED is red. During system boot or if the module is disabled, the LED is orange. During self-test diagnostics, the LED is orange. If the module is disabled, the LED is orange.

Specifications

Table 2 lists the specifications for the Network Analysis Module.

Table 2 Network Analysis Module 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)
Environmental Conditions:	
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
Memory	32 MB (WS-X5380)
	128 MB (WS-X5381)

Safety Warnings

Safety warnings appear throughout this configuration note in procedures that, if performed incorrectly, might harm you. A warning symbol precedes each warning statement. This section describes the warning symbol used in this note.

Warning 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. To see translations of the warnings that appear in this publication, refer to the appendix “Translated Safety Warnings” in the *Catalyst 5000 Series Installation Guide*.

Installing the Network Analysis Module

All Catalyst 5000 series switches support hot swapping, which lets you install, remove, replace, and rearrange modules without turning off the system power. When the system detects that a module has been installed or removed, it automatically runs diagnostic and discovery routines, acknowledges the presence or absence of the module, and resumes system operation with no operator intervention.

Warning Only trained and qualified personnel should install or replace this equipment.

Tools Required

You need a flat-blade screwdriver to remove any filler (blank) switching modules and to tighten the captive installation screws that secure the modules in their slots. Whenever you handle switching modules, you should use a wrist strap or other grounding device to prevent ESD damage.

Removing Modules

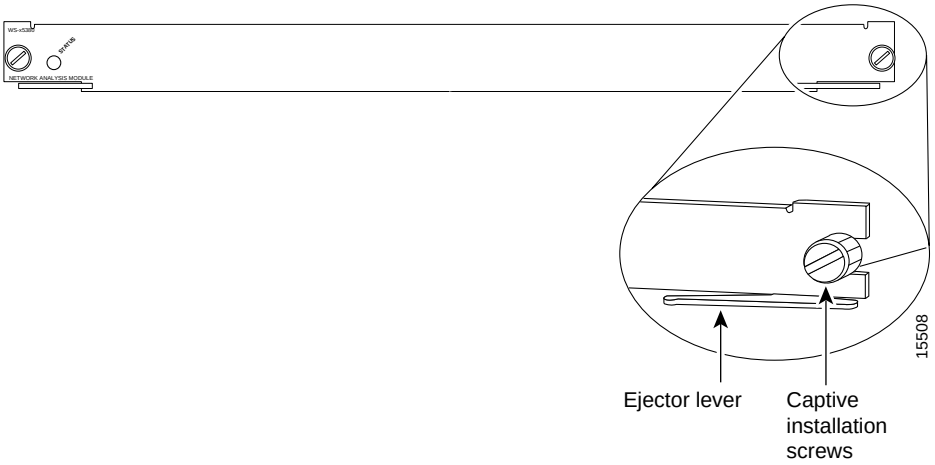
To remove a module from a Catalyst 5000 series switch, perform these steps:

Caution To prevent ESD damage, handle switching modules by the carrier edges only.

Step 1 If you do not plan to reinstall the switching module immediately after removing it, disconnect any network interface cables attached to the switching module ports.

Step 2 Use a flat-blade screwdriver to loosen the captive installation screws, shown in Figure 3.

Figure 3 Ejector Levers and Captive Installation Screws



Step 3 Place your thumbs on the left and right ejector levers and simultaneously push the levers outward to release the module from the backplane connector. Figure 3 shows a close-up of the right ejector lever.

Step 4 Grasp the module handle with one hand and place your other hand under the carrier to support and guide it out of the slot. Avoid touching the module.

Step 5 Carefully pull the switching module straight out of the slot, keeping your other hand under the carrier to guide it. Keep the switching module oriented horizontally.

Step 6 Place the switching module on an antistatic mat or antistatic foam or immediately install it in another slot.

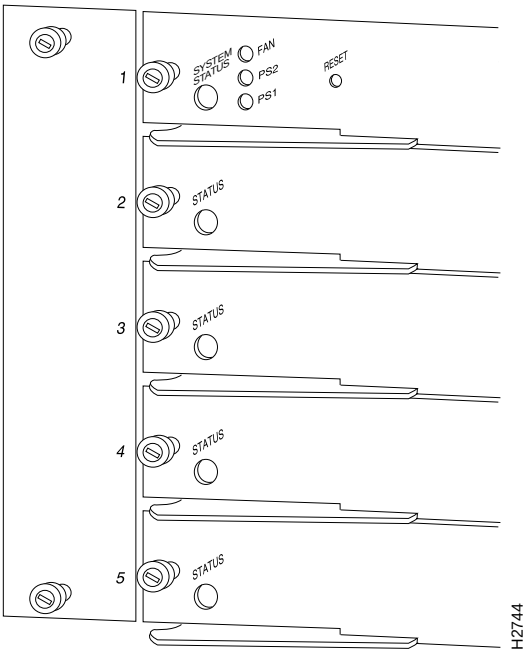
Step 7 If the slot is to remain empty, install a module filler plate (part number 800-00292-01) to keep dust out of the chassis and to maintain proper airflow through the module compartment.

Caution Always install the module filler plate in empty module slots to maintain the proper flow of cooling air across the modules.

Installing Modules

All Catalyst 5000 series modules are installed in horizontal slots that are numbered from top to bottom. Figure 4 shows an example of how slots are numbered on the chassis; in this case using the Catalyst 5000 switch. The slot numbering for all Catalyst 5000 series switches is similar to that shown in Figure 4.

Figure 4 Module Slot Numbers



The Network Analysis Module can be installed in slots 2 through 5 in the Catalyst 5000 and Catalyst 5505 switches, slots 2 through 9 of the Catalyst 5509 switch, and slots 2 through 12 of the Catalyst 5500 switch.

Note You can install the Network Analysis Module in slot 2 of the Catalyst 5002 switch, but with the supervisor engine module occupying slot 1 of the two-slot chassis, you cannot install any other switching modules.

To install a module in a Catalyst 5000 series switch, perform these steps:

Caution To prevent ESD damage, handle modules by the carrier edges only.

Step 1 Make sure you take the necessary precautions to prevent ESD damage.

Step 2 Choose a slot for the new module. If possible, place modules between empty slots.

Note Empty slots have module filler plates installed.

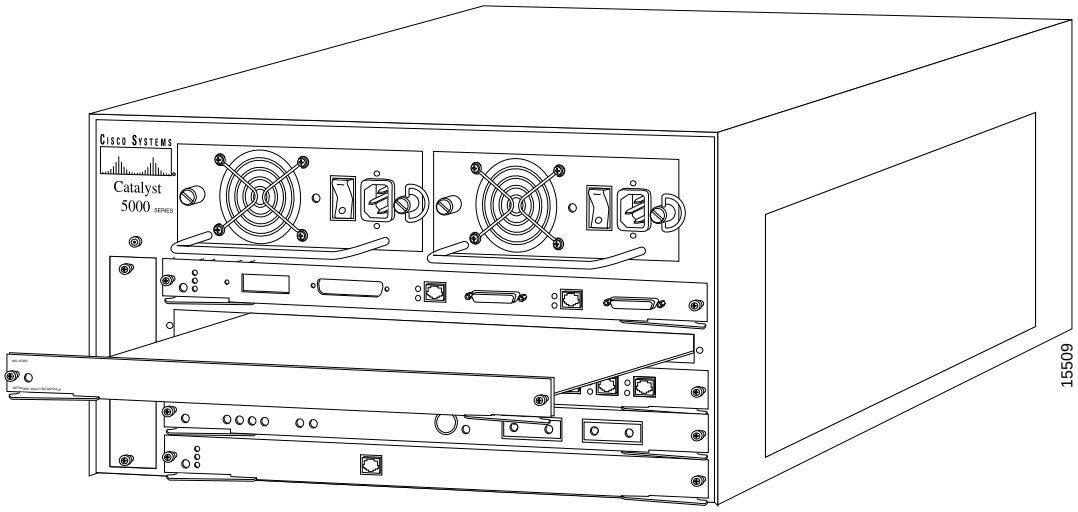
Step 3 Use a flat-blade screwdriver to loosen the captive installation screws securing the module filler plate (or the existing module) from the desired slot.

Step 4 Remove the module filler plate (or the existing module).

Step 5 Hold the module handle with one hand and place your other hand under the carrier to support the module and guide it into the slot. Avoid touching the printed circuit boards or connector pins.

Step 6 Place the module in the slot. Align the notch on the sides of the module carrier with the groove in the slot, as shown in Figure 5 for the Catalyst 5000 switch. Use the same procedure for all Catalyst 5000 series switches.

Figure 5 Module Installation



Step 7 Maintain the module at a 90-degree orientation to the backplane and carefully slide the module into the slot until the module faceplate contacts the ejector levers.

Step 8 Use the thumb and forefinger of each hand and simultaneously push in the left and the right levers to seat the module in the backplane connector.

Caution Always use the ejector levers when installing or removing modules. A module that is partially seated in the backplane will cause the system to halt and subsequently crash.

Step 9 Use a flat-blade screwdriver to tighten the captive installation screws on the left and right ends of the module.

Step 10 Check the status of the interfaces as follows:

- If this installation is a replacement module, use the **show module** command to verify that the system has acknowledged the new module and brought it up.
- If the module is new, complete the procedures in the following section.

Configuring the Network Analysis Module

Table 3 describes the Network Analysis Module default configuration.

Table 3 Network Analysis Module Default Configuration

Feature	Default Setting
SPAN (supervisor engine feature)	Disabled
NetFlow Data Export (NFFC/NFFC II feature)	Disabled
Extended RMON	Enabled
Extended RMON Netflow (NetFlow Monitor option)	Disabled
Extended RMON Vlanmode (VLAN Monitor option)	Disabled
Extended RMON Vlanagent (VLAN Agent option)	Disabled

Configuring the Network Analysis Module from the NMS

An SNMP management application, such as CiscoWorks2000, together with the computer it runs on, is called a network management system (NMS). To configure the Network Analysis Module from an NMS, refer to the NMS documentation. RMON domain configuration can be done only through SNMP from the NMS.

Configuring the Network Analysis Module from the CLI

The following sections describe how to use the command line interface (CLI) to configure the Network Analysis Module. For additional information on the CLI, refer to the *Catalyst 5000 Series Command Reference* publication.

Enabling Traffic Sources

The Network Analysis Module can analyze Ethernet virtual LAN (VLAN) traffic from either or both:

- The Switched Port Analyzer (SPAN) source: one or more Ethernet ports or a Fast Ethernet port or a Fast Ethernet trunk port or an Ethernet VLAN
- NetFlow Data Export (NDE) from a NetFlow Feature Card (NFFC or NFFC II) installed on the Supervisor Engine III module

Enable one or both of the Ethernet VLAN network traffic sources. Enable at least one source of Ethernet VLAN network traffic.

Using SPAN as a Traffic Source

If desired, use the SPAN feature as a traffic source for the Network Analysis Module:

— Set the Network Analysis Module as the SPAN destination port (see the *Catalyst 5000 Series Software Configuration Guide* for procedures).

— The Network Analysis Module can analyze Ethernet VLAN traffic from Ethernet or Fast Ethernet SPAN source ports, or you can specify an Ethernet VLAN as the SPAN source.

— To use the Network Analysis Module VLAN Monitor option (see the “Enabling the VLAN Monitor Option” section on page 10), set a trunk port as the SPAN source port.

Using NetFlow Data Export as a Traffic Source

If desired, use NDE as a traffic source for the Network Analysis Module. Enable the NetFlow Monitor option to allow the Network Analysis Module to receive the NDE stream from an NFFC or NFCC II installed in the switch. The resultant statistics are presented on reserved ifIndex.3000.

Note If you are using software release 5.4(2) and later, the password is not required. Skip steps 2 through 4 in the following procedure if your system is running Release 5.4(2) and later.

To enable the NetFlow Monitor option:

Step 1 Purchase a NetFlow Monitor option license from your Cisco sales representative, which will have a registration key and URL on it.

Step 2 Get the Media Access Control (MAC) address of your Network Analysis Module. Enter this command:

```
Console> show module mod_num
```

This example shows how to display the MAC address:

```
Console> show module 4
Mod Module-Name         Ports Module-Type           Model    Serial-Num Status
--- ------------------- ----- --------------------- --------- --------- -------
4                       1     Network Analysis/RMON WS-X5380  008175475 ok

Mod MAC-Address(es)                         Hw     Fw         Sw
--- --------------------------------------- ------ ---------- -----------------
4   00-e0-14-10-18-00                       0.100  4.1.1      4.3(1)
```

Note The MAC address in the example is 00-e0-14-10-18-00.

Step 3 Access the URL specified on the NetFlow Monitor option license.

Step 4 Enter the registration key and the MAC address of the Network Analysis Module to generate the password for your Network Analyzer Module.

Step 5 Enter this command in privileged mode to enable the NetFlow Monitor option:

```
Console> set snmp extendedrmon netflow enable password
```

This example shows how to enable the NetFlow Monitor option and how to verify that it is enabled:

```
Console> (enable) set snmp extendedrmon netflow enable password
Snmp extended RMON netflow enabled
Console> (enable) show snmp
RMON:                          Disabled
Extended RMON:                 Enabled
Extended RMON Netflow:         Enabled
Extended RMON Vlanmode:        Disabled
Extended RMON Vlanagent:       Disabled

<...output truncated...>

Console> (enable)
```

Step 6 Enter this command in privileged mode to enable NDE:

```
Console> set mls nde enable
```

Note With a Network Analysis Module installed, you do not need to specify an external data collector with a **set mls nde** *collector_ip* [*udp_port_number*] command as described in the "Configuring Multilayer Switching" chapter of the *Catalyst 5000 Series Software Configuration Guide*.

Enabling the VLAN Monitor Option

When the SPAN source is a trunk port and the VLAN Monitor option is enabled, the Network Analysis Module aggregates statistics by VLAN, rather than by source MAC address.

To enable the VLAN Monitor option, enter this command in privileged mode:

Task	Command
Enable VLAN Monitor.	**set snmp extendedrmon vlanmode enable**

This example shows how to enable the VLAN Monitor option and how to verify that it is enabled:

```
Console> (enable) set snmp extendedrmon vlanmode enable
Snmp extended RMON vlanmode enabled
Console> (enable) show snmp
RMON:                          Disabled
Extended RMON:                 Enabled
Extended RMON Netflow:         Disabled
Extended RMON Vlanmode:        Enabled
Extended RMON Vlanagent:       Disabled

<...output truncated...>

Console> (enable)
```

Enabling the VLAN Agents Option

Note Enabling the VLAN Agents option increases the load on the Network Analysis Module: each packet is counted twice, once as port traffic and once as VLAN traffic.

When the VLAN Agents option is enabled, the Network Analysis Module aggregates statistics by VLAN as well as by port.

To enable the VLAN Agents option, enter this command in privileged mode:

Task	Command
Enable VLAN Agents.	**set snmp extendedrmon vlanagent enable**

This example shows how to enable the VLAN Agents option and how to verify that it is enabled:

```
Console> (enable) set snmp extendedrmon vlanagent enable
Snmp extended RMON vlanagent enabled
Console> (enable) show snmp
RMON:                          Disabled
Extended RMON:                 Enabled
Extended RMON Netflow:         Disabled
Extended RMON Vlanmode:        Disabled
Extended RMON Vlanagent:       Enabled

<...output truncated...>

Console> (enable)
```

Other Network Analysis Module Commands

The Network Analysis Module also supports these commands, which are described in the *Catalyst 5000 Series Command Reference* publication:

- **clear config** [*mod_num*]
  Clears the module's configuration and resets it
- **clear counter** [*mod_num*]
  Clears the module's MAC and port counters
- **clear log** [*mod_num*]
  Deletes all entries in the module's error log
- **set module** commands (all other **set module** commands return an error message):
  - **set module** {**enable** | **disable**} *mod_num*
    Enables or disables the module
  - **set module name** *mod_num*
    Sets the name of the module
- **set port name** *mod_num*/**1**
  Sets the name of the module's port (all other **set port** commands return an error message)
- **show log** *mod_num*
  Displays the module's error logs
- **show module** [*mod_num*]
  With a Network Analysis Module installed, displays "Network Analysis/RMON" under "Module-Type"
- **show mac** [*mod_num*[/**1**]]
  Shows MAC counters
- **show port** commands (all other **show port** commands return an error message)
  - **show port** [*mod_num*[/**1**]]
    Shows port status and counters
  - **show port capabilities** [*mod_num*[/**1**]]
    Shows module information
  - **show port ifindex** [*mod_num*[/**1**]]
    Shows the module's SNMP ifindex

  - **show port status** [*mod_num*[/**1**]]
    Shows port status information
  - **show port trap** [*mod_num*[/**1**]]
    Shows port trap as disabled (cannot be enabled for the network Analysis Module)

- **show snmp**
  - With no Network Analysis Module installed, the command displays “Extended RMON: Extended RMON module is not present.”
  - The command displays “Extended RMON: Enabled” when a Network Analysis Module is installed.
  - With SPAN enabled and the Network Analysis Module as the SPAN destination, the command displays these additional lines when a Network Analysis Module is installed:

```
...
     RMON-Mcast           RMON-Bcast           RMON-Ucast       RMON-DropEvent
------------------- -------------------- -------------------- -----------------
0                   0                    0                    0
```

- **show span**

  With SPAN enabled and the Network Analysis Module as the SPAN destination, the command displays these additional lines when a Network Analysis Module is installed:

```
...
     RMON-Mcast           RMON-Bcast           RMON-Ucast       RMON-DropEvent
------------------- -------------------- -------------------- -----------------
0                   0                    0                    0
```

- **show test** [*mod_num*]
- **download** [*mod_num*]

Note Entering a download command for a Network Analysis Module does not disconnect a Telnet session; ignore the message that says the command may disconnect your Telnet session.

- **reset** [*mod_num*]

Note Any command not listed returns an error message.

Supported RMON and RMON2 MIB Objects

Table 4 lists the RMON and RMON2 MIB objects supported by the supervisor engine module and the Network Analysis Module.

Table 4 Supervisor Engine Module and Network Analysis Module RMON Support

Module	Object Identifier (OID) and Description	Source
Supervisor Engine	...mib-2(1).rmon(16).statistics(1).etherStatsTable(1) ...mib-2(1).rmon(16).statistics(1).tokenRingMLStatsTable(2) ...mib-2(1).rmon(16).statistics(1).tokenRingPStatsTable(3)	RFC 1757 (RMON-MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)
	Counters for packets, octets, broadcasts, errors, etc.	
Supervisor Engine	...mib-2(1).rmon(16).history(2).historyControlTable(1) ...mib-2(1).rmon(16).history(2).etherHistoryTable(2) ...mib-2(1).rmon(16).history(2).tokenRingMLHistoryTable(3) ...mib-2(1).rmon(16).history(2).tokenRingPHistoryTable(4)	RFC 1757 (RMON-MIB) RFC 1757 (RMON-MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)
	Periodically samples and saves statistics group counters for later retrieval.	
Supervisor Engine	...mib-2(1).rmon(16).alarm(3)	RFC 1757 (RMON-MIB)
	A threshold that can be set on critical RMON variables for network management.	
Network Analysis	...mib-2(1).rmon(16).hosts(4)	RFC 1757 (RMON-MIB)
	Maintains statistics on each host device on the segment or port.	
Network Analysis	...mib-2(1).rmon(16).hostTopN(5)	RFC 1757 (RMON-MIB)
	A user-defined subset report of the Hosts group, sorted by a statistical counter.	
Network Analysis	...mib-2(1).rmon(16).matrix(6)	RFC 1757 (RMON-MIB)
	Maintains conversation statistics between hosts on network.	
Network Analysis	...mib-2(1).rmon(16).filter(7)	RFC 1757 (RMON-MIB)
	A filter engine that generates a packet stream from frames that match a specified pattern.	
Network Analysis	...mib-2(1).rmon(16).capture(8)	RFC 1757 (RMON-MIB)
	Manages buffers for packets captured by the Filter group for uploading to the management console.	
Supervisor Engine	...mib-2(1).rmon(16).event(9)	RFC 1757 (RMON-MIB)
	Generates SNMP traps when an Alarms group threshold is exceeded and logs the events.	
Supervisor Engine	...mib-2(1).rmon(16).tokenRing(10).ringStationControlTable(1) ...mib-2(1).rmon(16).tokenRing(10).ringStationTable(2) ...mib-2(1).rmon(16).tokenRing(10).ringStationOrderTable(3) ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigControlTable(4) ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigTable(5) ...mib-2(1).rmon(16).tokenRing(10).sourceRoutingStatsTable(6)	RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB) RFC 1513 (TOKEN-RING-RMON MIB)
	Aggregates detailed Token-Ring statistics.	
Network Analysis	...mib-2(1).rmon(16).protocolDir(11)	RFC 2021 (RMON2-MIB)
	A table of protocols for which the Network Analysis Module monitors and maintains statistics.	
Network Analysis	...mib-2(1).rmon(16).protocolDist(12)	RFC 2021 (RMON2-MIB)
	A table of statistics for each protocol in protocolDir(11).	
Network Analysis	...mib-2(1).rmon(16).addressMap(13)	RFC 2021 (RMON2-MIB)
	List of MAC-to-network-layer address bindings.	

Table 4 Supervisor Engine Module and Network Analysis Module RMON Support (continued)

Module	Object Identifier (OID) and Description	Source
Network Analysis	...mib-2(1).rmon(16).nlHost(14)	RFC 2021 (RMON2-MIB)
	Statistics for each network layer address.	
Network Analysis	...mib-2(1).rmon(16).nlMatrix(15)	RFC 2021 (RMON2-MIB)
	Traffic statistics for pairs of network layer addresses.	
Network Analysis	...mib-2(1).rmon(16).alHost(16)	RFC 2021 (RMON2-MIB)
	Statistics by application layer protocol for each network address.	
Network Analysis	...mib-2(1).rmon(16).alMatrix(17)	RFC 2021 (RMON2-MIB)
	Traffic statistics by application layer protocol for pairs of network layer addresses.	
Network Analysis	...mib-2(1).rmon(16).usrHistory(18)	RFC 2021 (RMON2-MIB)
	Extends history beyond RMON1 link-layer statistics to include any RMON, RMON2, MIB-I, or MIB-II statistic.	
Supervisor Engine	...mib-2(1).rmon(16).probeConfig(19)	RFC 2021 (RMON2-MIB)
	Displays a list of agent capabilities and configurations.	

Standards Compliance

The Catalyst 5000 series Network Analysis Module, when installed in a Catalyst 5000 series system, complies with the following standards.

Table 5 Standards Compliance

Specification	Description
Compliance:	CE Marking
Safety	UL[1] 1950, CSA[2]-C22.2 No. 950, EN[3] 60950, IEC[4] 950, TS[5] 001, AS/NZS[6] 3260
EMI[7]	FCC[8] Class A (47 CFR, Part 15), ICES[9]-003 Class A, EN 55022 Class A , CISPR22 Class A, AS/NZS 3548 Class A, and VCCI[10] Class A with UTP[11] cables
	EN 55022 Class B; CISPR22 Class B, AS/NZS 3590 Class B, and VCCI Class B with STP[12] cables

1 UL = Underwriters Laboratories
2 CSA = Canadian Standards Association
3 EN = Europäische Norm
4 IEC = International Electrotechnical Commission
5 TS = Technical Standard
6 AS/NZS = Australian/New Zealand Standard
7 EMI = electromagnetic interference
8 FCC = Federal Communications Commission
9 ICES = Interference-Causing Equipment Standard
10 VCCI = Voluntary Control Council for Information Technology Equipment
11 UTP = unshielded twisted-pair
12 STP = shielded twisted-pair

FCC Class A Compliance

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.

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 could void the FCC approval and negate your authority to operate this product.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

This document is to be used in conjunction with the *Catalyst 5000 Series Installation Guide* and the *Catalyst 5000 Series Software Configuration Guide*.