

Configuring the Network Analysis Module

This chapter describes how to configure the Catalyst 5000 series Network Analysis Module.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference* for your switch.

This chapter consists of these sections:

- Understanding How the Network Analysis Module Works on page 33-1
- Network Analysis Module Default Configuration on page 33-2
- Configuring the Network Analysis Module from the NMS on page 33-2
- Configuring the Network Analysis Module from the CLI on page 33-3
- Additional Network Analysis Module Commands on page 33-5

Note These sections describe the Network Analysis Module configuration that can be done from the CLI of a Catalyst 5000 series switch. See the CiscoWorks2000 documentation for procedures required on the NMS.

Understanding How the Network Analysis Module Works

For Ethernet VLANs, the Network Analysis Module extends the RMON support provided by the supervisor engine module software with the following (see the “Supported RMON and RMON2 MIB Objects” section on page 30-3 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)
- NIHost (RMON2 group 14)
- NIMatrix (RMON2 group 15)
- AIHost (RMON2 group 16)
- AIMatrix (RMON2 group 17)
- UsrHistory (RMON2 group 18)

The Network Analysis Module can analyze Ethernet VLAN traffic from either or both:

- The Switched Port Analyzer (SPAN) source port (for more information about SPAN, see Chapter 31, “Configuring SPAN”)
- NetFlow Data Export (NDE) (for more information about NDE, see Chapter 43, “Configuring NetFlow Data Export”)

Note When monitoring a VLAN, 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 an SNMP management application, such as CiscoWorks2000 (see the “Using CiscoWorks2000” section on page 29-5).

Network Analysis Module Default Configuration

Table 33-1 describes the Network Analysis Module default configuration.

Table 33-1 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

To configure the Network Analysis Module from the NMS, refer to the NMS documentation (see the “Using CiscoWorks2000” section on page 29-5). RMON domain configuration can be done only via SNMP from the NMS.

Configuring the Network Analysis Module from the CLI

These sections describe how to use the CLI to configure the Network Analysis Module:

- Using SPAN as a Traffic Source on page 33-3
- Using NetFlow Data Export as a Traffic Source on page 33-3
- Enabling the VLAN Monitor Option on page 33-4
- Enabling the VLAN Agents Option on page 33-5

Using SPAN as a Traffic Source

To use the SPAN source port as a traffic source for the Network Analysis Module, set the Network Analysis Module as the SPAN destination port.

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, set a trunk port as the SPAN source port (for more information, see the “Enabling the VLAN Monitor Option” section on page 33-4)

Using NetFlow Data Export as a Traffic Source

To 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 For information on configuring NDE, see Chapter 43, “Configuring NetFlow Data Export.”

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
Snm 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 “Specifying a NetFlow Data Export Collector” section on page 43-5. Ignore messages that the host and port are not set.

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, perform this task in privileged mode:

Task	Command
Enable VLAN Monitor.	<code>set snmp extendedrmon vlanmode enable</code>

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
Snm 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 The VLAN Agents option imposes increased load on the Network Analysis Module and might not be suitable for use on a heavily loaded switch, or when the switch is configured to analyze a high volume of network 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, perform this task 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
Snm 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)

```

Additional Network Analysis Module Commands

The Network Analysis Module also supports these commands, which are described in the *Command Reference* for your switch:

- **clear config** [*mod_num*]
Clears the modules's configuration and resets it
- **clear config extendedrmon**
Clears the module's RMON configuration from NVRAM
- **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 a “not supported” message.
