

# 11 DNS Resolver and RMON

## Introduction

This chapter describes commands related to the Domain Name Server (DNS) resolver and remote network monitoring (RMON) feature in the switch.

The commands for these features are available from the Networking submenu, which is described in Chapter 22, "IP Routing."

## Configuring the DNS Resolver

### The Names Submenu

The **Names** command takes you to the Names submenu. The one command in this menu, **res**, is used to view and to configure the Domain Name Server (DNS) resolver. You can configure up to three Domain Name Servers. The switch searches all three servers until it resolves the name to an IP address or until it fails to find the name.

To display the **Names** submenu, enter the following command:

**names**

A screen similar to the following displays:

Command	Resolver Configuration Menu
<b>res</b>	View/Configure the DNS resolver
<b>Main</b>	<b>File</b>
<b>Interface</b>	<b>Summary</b>
<b>Security</b>	<b>VLAN</b>
<b>System</b>	<b>Networking</b>
	<b>Services</b>
	<b>Help</b>

To configure one or more Domain Name Servers, enter the following command:

**res**

If the resolver function has not been enabled, a screen similar to the following displays:

**DNS Resolver Configuration**

1) Resolver Enabled : No

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) :

To enable the resolver function, enter **1=y**.

A screen similar to the following then displays:

### DNS Resolver Configuration

```
1) Resolver Enabled      : Yes
2) Domain                : UNSET
3) Server Address 1     : UNSET
4) Server Address 2     : UNSET
5) Server Address 3     : UNSET
```

**Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw) :**

The prompts allow you to enter a Domain Name and up to three Domain Name Servers (identified by their IP addresses).

- To change a value, enter the number corresponding to that value, an (=), then the new value. For example, to set a Domain Name to Company.Com, enter **2=Company.Com**.
- To clear an entry, specify the value as (.) as in **2=.**
- To save all your modifications, enter **save**
- To cancel all your modifications, enter **quit**
- To view the parameters currently configured, enter **?**

# Remote Network Monitoring (RMON)

Remote Network Monitoring (RMON) allows you to set up remote monitoring within your OmniAccess 512. RMON consists of “probes” and “events.” There are two commands in the Networking menu, **probes** and **events**, which you can use to monitor, activate and inactivate probes and events. Be aware that you cannot create probes from within the switch’s User Interface; to do so requires a network application such as HP ProbeView.

## Probes and Events

A **probe** is a task that runs in the switch. By using probes instead of sending repetitive inquiries to the switch, network traffic is significantly reduced.

There are three different kinds of probes: Ethernet, History, and Alarm.

A network management station (NMS) can configure either History or Alarm probes (a maximum of 16 is allowed). The status of a probe can be one of the following:

- Creating - The probe is under creation.
- Active - The probe is active.
- Inactive - The probe is inactive.

An **event** is an action that takes place based on an alarm condition detected by a probe. The event can take the form of an SNMP trap message and/or a log entry describing the alarm.

## Ethernet Probes

An Ethernet probe monitors a selected Ethernet interface (port) and tracks Ethernet statistics. An Ethernet probe is automatically created on each Ethernet interface that is enabled. If the interface becomes disabled, that Ethernet probe is deleted.

## History Probes

A History probe keeps a running history of all the statistics it has collected. When you set up a history probe you assign a sampling interval and a total number of samples to be taken. It keeps this information in a set of rotating buffers, so that it always retains the most recent samples.

The sampling rate is configurable from 1 second to 3600 seconds (1 hour). The total number of samples is configurable, however, it is limited by system resources (memory) available. The more samples you request, the more system resources needed. You may request as many samples as you want but the system will only grant as many as it has available.

## Alarm Probes

An Alarm probe generates an alarm if the variable you are monitoring exceeds a set limit.

To set up an Alarm probe you need to select a variable (Ethernet statistic) that you want to monitor. You set an upper and lower threshold that you will allow this variable to reach. If it crosses the threshold, an event is triggered which results in the sending of an SNMP trap and/or the logging of the alarm.

There are two ways an Alarm probe monitors variables. One is by absolute value. For example, if you set an upper limit of 100, an alarm will be generated if the variable exceeds 100. The other is a delta value where you can set the amount of change allowable; for example, you could set the delta range to 10. If the current sample differs from the previous sample by more than 10, an alarm will be generated.

The Alarm probe attempts to prevent a flood of alarms from being generated by fluctuating values. It does so by continuously comparing the upper and lower limits. What this means is that the first time either an upper or lower limit is exceeded, an alarm will be generated. However, if the variable moves back inside the limit, then out again, another alarm will not be generated unless the opposite limit is exceeded. For example, consider a situation where an upper limit of 75 and a lower limit of 25 is set. The variable goes to 76. An alarm is generated. If it drops to 74 then goes back up to 76, no alarm will be generated. Only when the variable drops below 25 will another alarm be generated. If it goes back up to 76 then another alarm will be generated, etc. This procedure prevents a flood of alarms from being generated if the value fluctuates between 74 and 76.

## Monitoring Probes

The **probes** command is used to monitor, activate, and inactivate existing probes (remember, you cannot create probes in the switch's UI). You can do three things with the command:

1. View all the current probes.
2. View a specific probe.
3. Activate or inactivate a History or Alarm Probe. (You can only do this with the "admin" login.)

The **probes** command has three optional parameters. The format is:

**probes [active | inactive] [n]**

where:

**active** - activates an existing probe

**inactive** - inactivates an existing probe

**n** - is the entry number of the probe to view

If you enter the **probes** command without parameters, it displays all the current probes.

### RMON Probe Summary

Entry	Slot/Port	Flavor	Status	Time	System Resources
1	2/ 1	Ethernet	Active	0 hrs 39 mins	312 bytes
2	2/ 1	History	Active	0 hrs 4 mins	3656 bytes
3	2/ 1	Alarm	Active	0 hrs 0 mins	1336 bytes

### Entry

The entry number in the list of probes (1-16).

### Slot/Port

The slot port number (interface) that this probe is monitoring.

### Flavor

Ethernet, History, or Alarm.

### Status

Creating, Active, or Inactive.

**Time**

Time since the last change in status.

**System Resources**

Amount of memory that has been allocated to this probe.

To see the detail for each of the probes enter the **probes** command followed by the entry number as shown below.

/Networking % probes 1

**RMON Probe Summary**

Entry	Slot/Port	Flavor	Status	Time	System Resources
1	2/ 1	Ethernet	Active	0 hrs 39 mins	312 bytes

Probe's Owner: OmniAccess 512 Ethernet probe on slot 2 port 1

/Networking % probes 2

**RMON Probe Summary**

Entry	Slot/Port	Flavor	Status	Time	System Resources
2	2/ 1	History	Active	0 hrs 4 mins	3656 bytes

Probe's Owner: andy

History Control Buckets Requested	=	60
History Control Buckets Granted	=	60
History Control Interval	=	60 seconds
History Sample Index	=	6

/Networking % probes 3

**RMON Probe Summary**

Entry	Slot/Port	Flavor	Status	Time	System Resources
3	2/ 1	Alarm	Active	0 hrs 0 mins	1336 bytes

Probe's Owner: andy

Alarm Rising Threshold	=	3000
Alarm Falling Threshold	=	3000
Alarm Rising Event Index	=	1
Alarm Falling Event Index	=	3
Alarm Interval	=	30 seconds
Alarm Sample Type	=	delta value
Alarm Startup Alarm	=	rising or falling alarm
Alarm Variable	=	ethernet octets received

**Monitoring Events**

The **events** command has one optional parameter. The format is:

**events [clear]**

where:

**clear** - clears the event log. (You can only do this with the "admin" login.)

**RMON Logged Events Summary**

Entry	Time	Description
1	0 hrs 26 mins	Rising threshold alarm for etherStatsOctets on slot 2 port 1
2	0 hrs 27 mins	Rising threshold alarm for etherStatsOctets on slot 2 port 1

