- SNMP and Logging -

**SNMP**

Simple Network Management Protocol (SNMP) allows for centralized administration of all network resources. SNMP relies on the use of traps, or criteria for logging specific informational or critical events. Cisco developed Remote Monitoring (RMON) to utilize SNMP on routers and switches.

RMON alarms identify a specific occurrence on a device. RMON events can then be configured to perform an action once the alarm is tripped.

**Configuring RMON Alarms and Events**

To configure an RMON alarm:

```
Router(config)# rmon alarm 1 ifEntry.20.1 30 delta rising-threshold 100 1
falling-threshold 0 owner AARON
```

To configure an RMON event once the ALARM is triggered:

```
Router(config)# rmon event 1 log trap SNMPCOMMUNITY description
ERROR owner AARON
```

To configure the SNMP specific information:

```
Router(config)# snmp-server community SNMPCOMMUNITY RO
Router(config)# snmp-server host 150.50.4.10 SNMPCOMMUNITY

Router(config)# snmp-server enable traps
Router(config)# snmp-server trap-source e0
Router(config)# snmp-server packetsize 1450
Router(config)# snmp-server location Detroit, Michigan
Router(config)# snmp-server contact Aaron Balchunas

Router(config)# snmp-server enable traps isdn layer2
Router(config)# snmp-server enable traps frame-relay
```

To force RMON to capture every packet coming inbound on an interface:

```
Router(config)# interface e0
Router(config-if)# rmon promiscuous
```

To adjust the RMON queue size:

```
Router(config)# rmon queuesize 256
```
Configuring a SYSLOG Server

To direct all logging and debugging information to a centralized syslog server:

```plaintext
Router(config)# logging 150.50.1.1
Router(config)# logging buffered
```

Syslog servers use **UDP port 514**. When using a logging server, it is important to configure the router to include time and date stamps with the logs:

```plaintext
Router(config)# service timestamps log datetime localtime msec show-timezone
Router(config)# service timestamps debug datetime localtime msec show-timezone
```

To identify what messages to actually log:

```plaintext
Router(config)# logging trap 5
```

The default value is 7, which logs informational and everything else.

Other logging commands include:

```plaintext
Router(config)# logging facility LOCAL6
Router(config)# logging source-interface e0
```

Troubleshooting RMON, SNMP, and Logging

Important show commands would include:

```plaintext
Router# show snmp
Router# show rmon events
Router# show logging
```
Interface “Accounting”

Accounting can be configured on an interface to track several items:

- The number of packets sent or received on an interface.
- The number of packets of a certain IP precedence sent or received on an interface.
- The number of access-list violations on an interface.

To configure accounting:

```sh
Router(config)# interface e0/0
Router(config-if)# ip accounting output-packets
Router(config-if)# ip accounting precedence input
Router(config-if)# ip accounting precedence output
Router(config-if)# ip accounting access-violations
```

To view the accounting statistics:

```sh
Router# show ip accounting
```