Centralized Management

Remote Monitoring (RMON)

Ethernet Switch

ZyNOS 3.7

Support Notes

Version 3.70

August 2006

ZyXEL

Unleash Networking Power

Overview of RMON

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet the particular networking needs.

RMON was originally developed to address the problem of managing LAN segments and remote sites from a central location. The RMON specification, which is an extension of the SNMP MIB, is a standard monitoring specification. Within an RMON network monitoring, data is defined by a set of statistics and functions and exchanged between various different monitors and console systems. Resultant data is used to monitor network utilization for network planning and performance-tuning, as well as assisting in diagnosing a network fault.

RMON solutions are comprised of two components: a probe (or an agent or a monitor), and a client, usually a management station. Agents store network information within their RMON MIB and normally have a form of an embedded software on a network hardware such as routers and switches. However, they can also be some programs running on a PC. Agents can only see the traffic that flows through them so they must be placed on each LAN segment or WAN link that is to be monitored. Clients, or management stations, communicate with the RMON agent or probe, using SNMP to obtain and correlate RMON data.

There is a number of variations to the RMON MIB. For example, the Token Ring RMON MIB provides objects specific for managing Token Ring networks. The SMON MIB extends RMON by providing RMON analysis for switched networks.

RMON Groups

RMON delivers information in nine RMON groups of monitoring elements,

each providing specific sets of data to meet common network-monitoring requirements. Each group is optional so that the vendors do not need to support all the groups within the Management Information Base (MIB). Some RMON groups require support of other RMON groups to function properly. Table 1 summarizes the nine monitoring groups specified in the RFC 1757 Ethernet RMON MIB.

Table 1: RMON Monitoring Groups

RMON 1 MIB Group	Function	Elements
Statistics	Contains statistics measured by the probe for each monitored interface on the device.	Packets dropped, packets sent, bytes sent (octets), broadcast packets, multicast packets, CRC errors, runts, giants, fragments, jabbers, collisions, and counters for packets ranging from 64 to 128, 128 to 256, 256 to 512, 512 to 1024, and 1024 to 1518 bytes.
History	Records periodic statistical samples from a network and stores for retrieval.	Sample period, number of samples, items sampled.
Alarm	Periodically takes statistical samples and compares them with set thresholds for events generation.	Includes the alarm table and requires the implementation of the event group. Alarm type, interval, starting threshold, stop threshold.
Host	Contains statistics associated with each host discovered on the network.	Host address, packets, and bytes received and transmitted, as well as broadcast, multicast, and error packets.
HostTopN	Prepares tables that describe the top hosts.	Statistics, host(s), sample start and stop periods, rate base, and duration.

Matrix	Stores and retrieves statistics for conversations between sets of two addresses.	Source and destination address pairs and packets, bytes, and errors for each pair.
Filters	Enables packets to be matched by a filter equation for capturing or events.	Bit-filter type (mask or not mask), filter expression (bit level), conditional expression (and, or not) to other filters.
Packet Capture	Enables packets to be captured after they flow through a channel.	Size of buffer for captured packets, full status (alarm), and number of captured packets.
Events	Controls the generation and notification of events from this device.	Event type, description, last time event sent

Groups of RMON MIB

The objects are arranged into the following groups:

Statistics (iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).rmon(16).statistics(1))

History (1.3.6.1.2.1.16.2)

Alarm (1.3.6.1.2.1.16.3)

Hosts (1.3.6.1.2.1.16.4)

HostTopN (1.3.6.1.2.1.16.5)

Matrix (1.3.6.1.2.1.16.6)

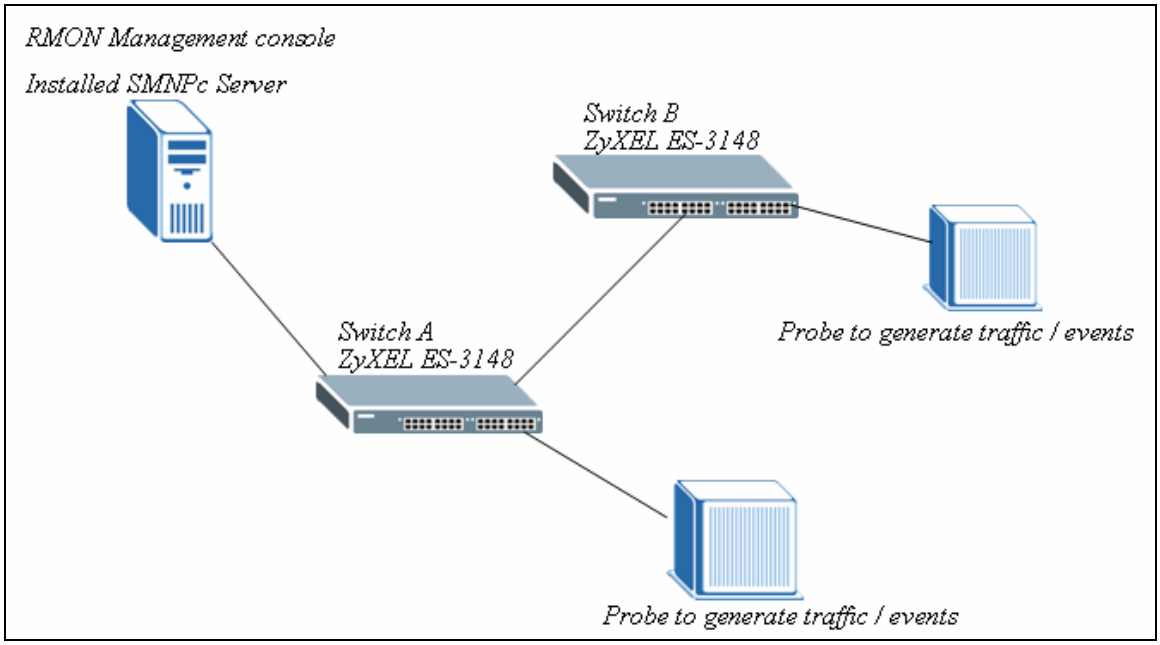
Filter (1.3.6.1.2.1.16.7)

Capture (1.3.6.1.2.1.16.8)

Event (1.3.6.1.2.1.16.9)

All groups in this MIB are optional. (MIB-II is **mandatory**)

Scenario (ES-3100 Series supports RMON 1.2.3.9)



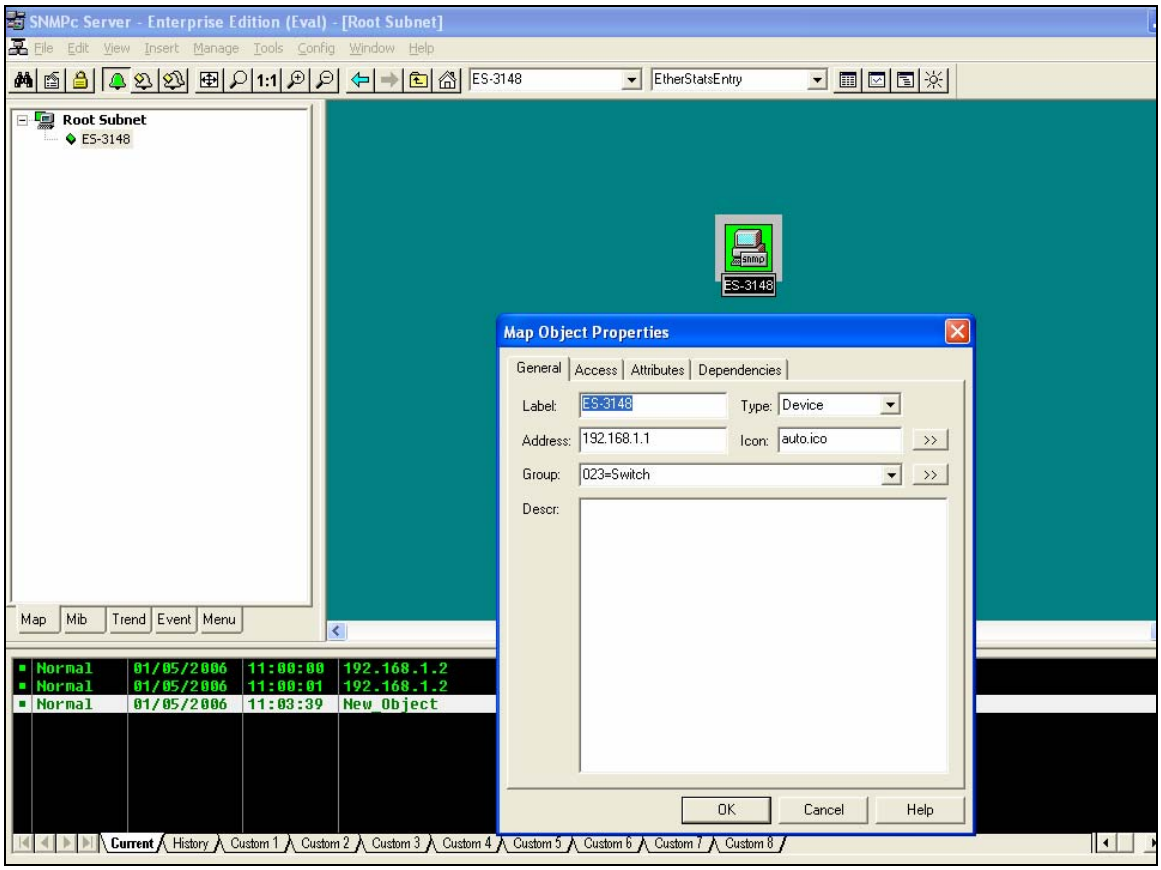
In this illustration, SNMPc Enterprise Edition Version 5.1.6c is installed on the PC, and this PC is defined as “RMON management console”. This PC can ping both ZyXEL ES-3148 (or any ZyXEL Management Switch which supports RMON) devices (both Switch A & Switch B). Also, there are some probes / networking devices to generate the traffic to the ZyXEL Switches in order to verify the RMON result. Since the work flow and the technology of RMON on the two switches are the same, only one of the Switch will be demonstrated.

Since RMON is an extension of the SNMP, SNMP must be enabled first on the ZyXEL Switch. By default SNMP is enabled, and the Community (Get,Set,Trap) is set to “public”, and Trap Destination to 0.0.0.0; It is not mandatory to change the default value in order for SNMP & RMON to work. Therefore, modification is not necessary in this case.

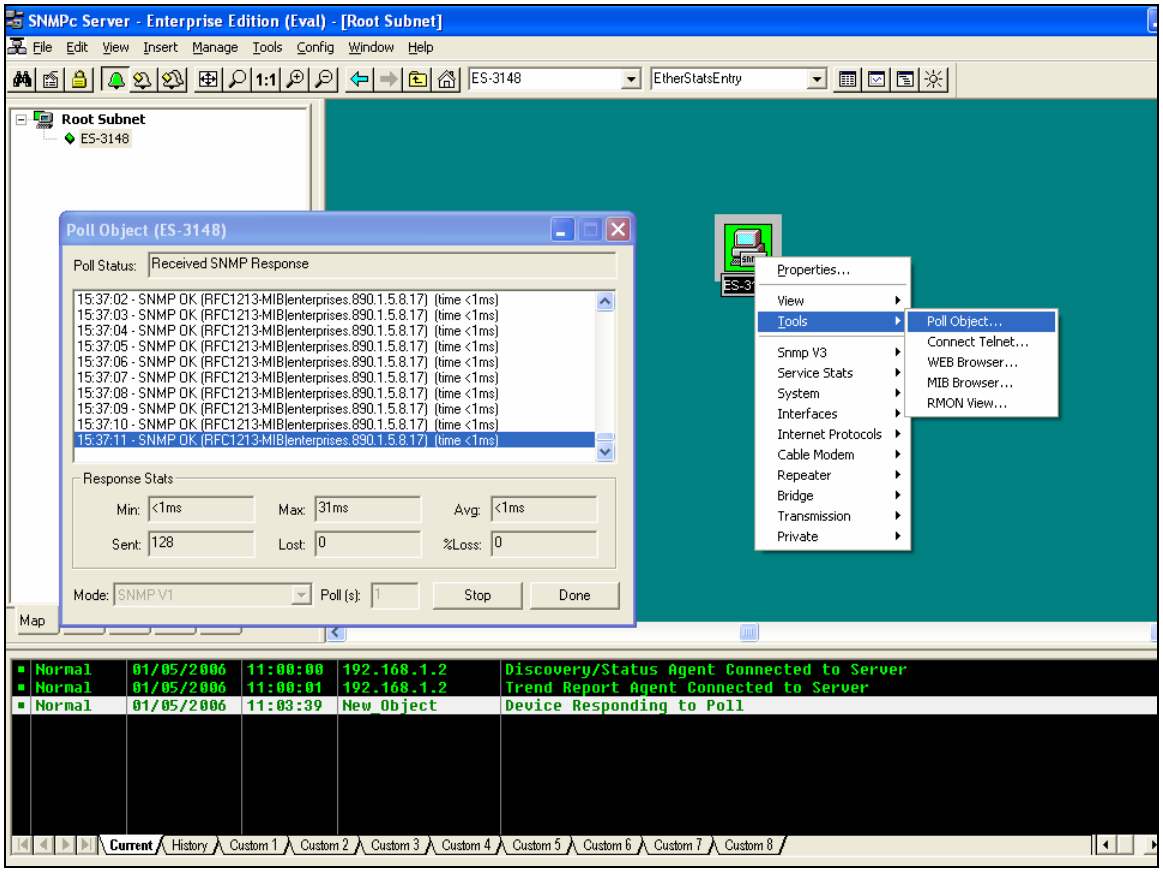
In this scenario, we are going to monitor the Broadcast Packets by using the RMON MIB. The following will show the steps to monitor the Broadcast Packets by using SNMPc Enterprise Edition Version 5.1.6c.

1. Methodology of Scenario Verification

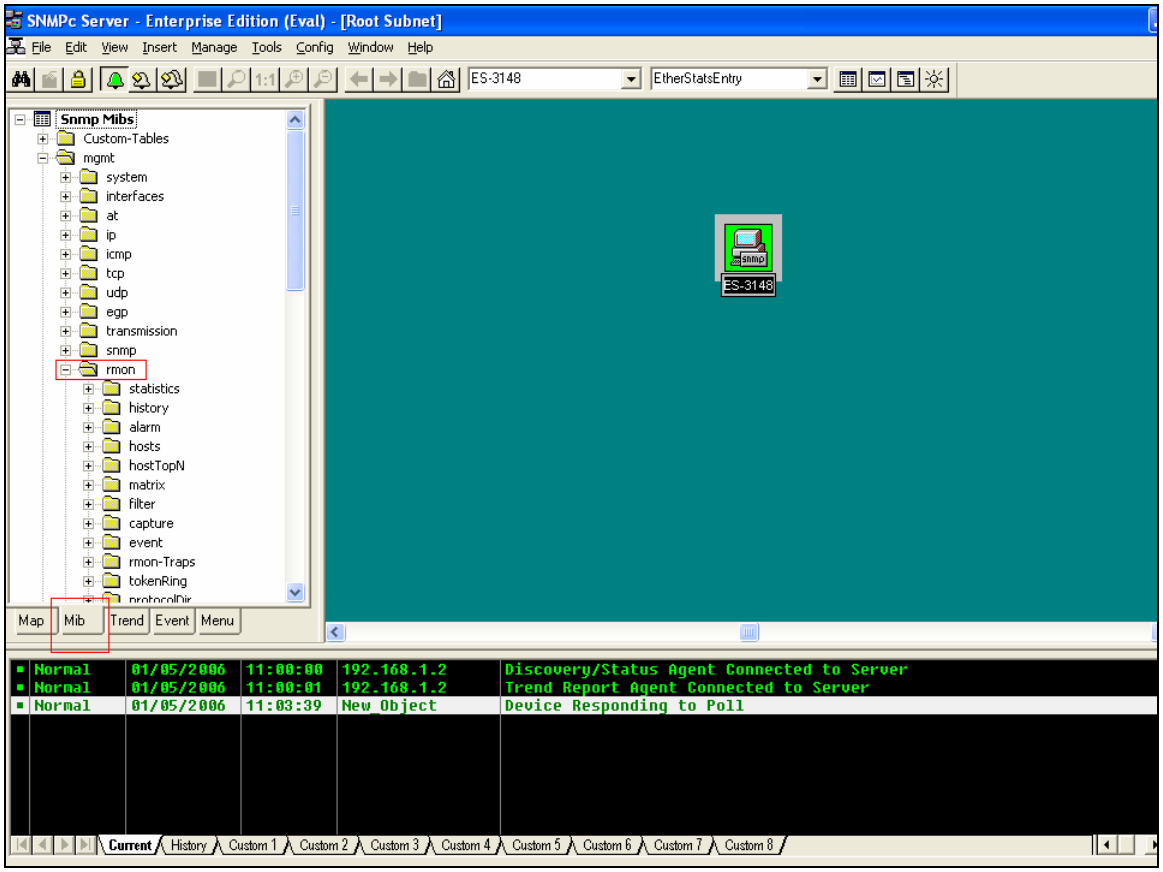
1. Open your SNMPc program first, then pick the ZyXEL-3148 Switch (initially it is named “root”) and give it the correct IP information to get the SNMP information. You can also rename it to whatever you want.



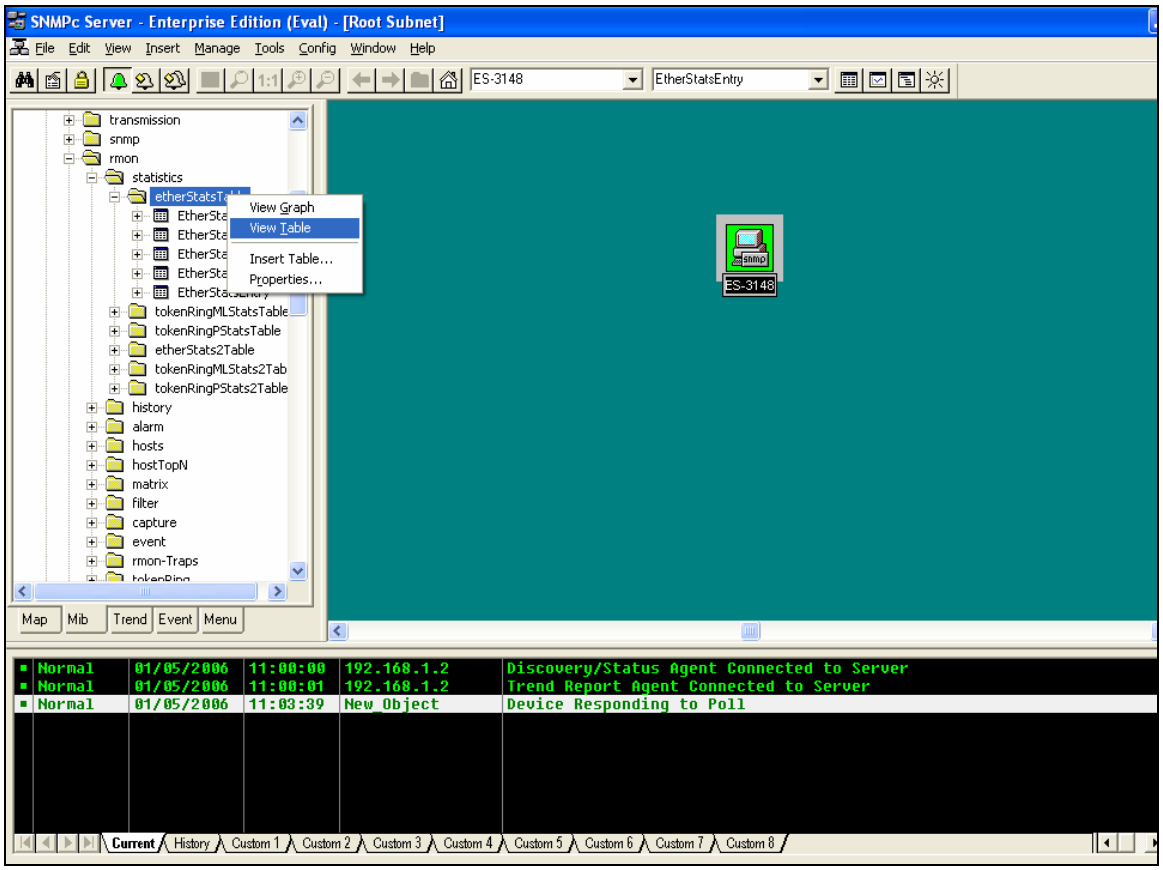
You can verify whether your configuration is correct by using the “Poll Object” option. To do that, click on the ES-3148 icon that is located in the “Tools” menu.



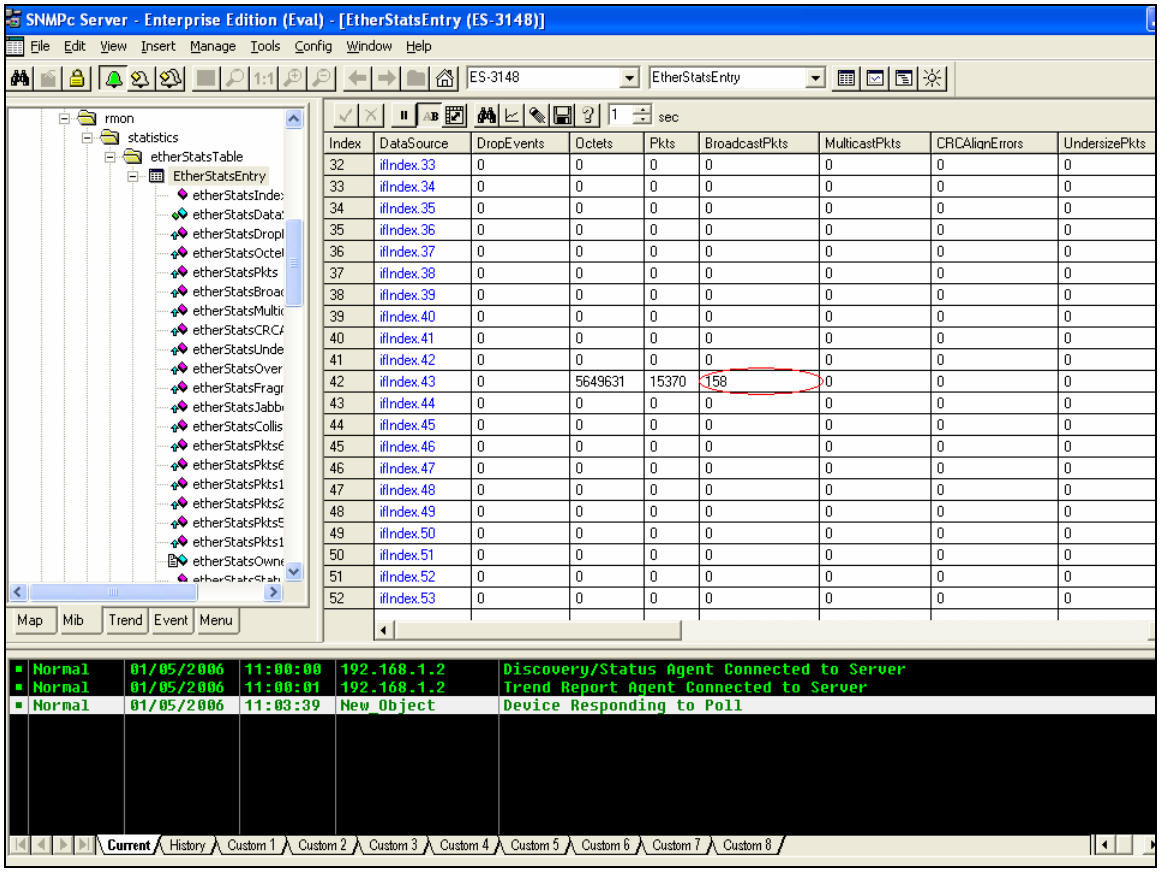
2. Second, click on the “Mib” tab and expand the SNMP Mibs’ tree. You will find that there is an “rmon” group. Again you can expand its sub-tree.



3. Right click the “etherStatsTable” and choose “View Table”



4. Find the interface or port that you are looking for. If you look at the corresponding field, you will find the value that you want to monitor. In this case, we are looking for the Broadcast Packets.



Try to generate some broadcast traffic from the probe or your network device. You should see the BroadcastPkts value increasing.

5. In conclusion, if the Switch supports RMON, then you can get the values from the Switch in the RMON Group(s), otherwise, it will return 0 that will always stay 0. Without the support of RMON, it is impossible to monitor the elements in the RMON MIB Group