Payoff

By standardizing the management information base (MIB) for Ethernet and Token Ring LANs, a network administrator can use the management platform obtained from one vendor with RMON probes obtained from other vendors. Remote network monitoring (RMON) provides interoperability between network management products so that network administrators receive continuous feedback on activity on distant networks, which can be invaluable for troubleshooting.

Introduction

By standardizing the Management Information Base for Ethernet and Token Ring local area networks (LANs), the management platform obtained from one vendor can be used with remote network monitoring (RMON) probes obtained from other vendors. Thus, Remote MONitoring provides interoperability between network management products that monitor activity on distant networks, which may be extremely valuable in alleviating network problems.

This article reviews the Simple Network Management Protocol, on which RMON is based, and describes the use of Ethernet and Token Ring RMON probes. Screens captured from a personal computer executing a management program illustrate how RMON provides information concerning activity on a remote network.

Simple Network Management Protocol

The Simple Network Management Protocol was originally developed as a mechanism for managing Ethernet gateways in the Internet. The simple network management protocol (SNMP) architecture is based on three components: an agent, a manager, and a Management Information Base.

The agent is a software program or read-only memory (ROM) firmware code that operates in a managed network device, such as a computer, bridge, or router. The manager represents another software program; however, this program operates on a computer that becomes the network management station. The manager interoperates with agents through the use of simple network management protocol (SNMP) commands. The third component of simple network management protocol (SNMP) is the management information base (MIB). The management information base (MIB) denotes a data base of standardized elements that is queried by simple network management protocol (SNMP) agents and provided to the manager.

Exhibit 1 illustrates the relationship of the three basic components of simple network management protocol (SNMP) on a bus-based Ethernet LAN. The manager operating on a network management station queries an agent operating on a managed device. The agent, in turn, depending on the manager's command, can query its data base, returning requested information to the manager.
Basic Components of SNMP

SNMP Commands

SNMP specifies five commands that are referred to as verbs and protocol data units: GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap.

The GetRequest command is issued by the manager to retrieve a single value from the agent. By comparison, the GetNextRequest is used by the manager to examine an agent's Management Information Base, one element at a time. The agent replies to both the GetRequest and GetNextRequest commands through the use of the GetResponse command.

The SetRequest command is used to modify or reset one or more configuration parameters of a managed device. Because of the lack of security in the first version of Simple Network Management Protocol, many vendors did not include recognition of the SetRequest command in their agents. Under simple network management protocol (SNMP) version 2, which included security to prevent unauthorized managers from using the SetRequest command, that command is now commonly supported by agents.

The Trap command represents an unsolicited command. A Trap command is transmitted from an agent to a manager to alert the manager to a predefined condition, such as a circuit failure.

RMON Probes

As previously mentioned, simple network management protocol (SNMP) was originally developed as a mechanism for managing Transmission Control Protocol/Internet Protocol (TCP/IP) and Ethernet gateways. A logical extension of simple network management protocol (SNMP) was to permit the monitoring of remote networks. This was accomplished by the development of Remote MONitoring probes based on request for comment (RFC) 1271 and 1513 for Ethernet and Token Ring networks, respectively. The term “probe” represents a host computer operating RMON software or a hardware device that is operating ROM code that supports RMON.

As an extension to simple network management protocol (SNMP), an simple network management protocol (SNMP) manager can be used to interact with RMON probes. In fact, even the RMON Management Information Base can be considered extensions of the originally defined Ethernet and Token Ring LAN management information base (MIB).

Ethernet and Token Ring RMON MIBs

The Ethernet Remote MONitoring Management Information Base consists of managed objects arranged in nine groups, each representing a basic unit of conformance. If a RMON device implements a group, it must implement all objects in the group. The following sections briefly describe each group; the statistics and alarm groups are discussed at greater length later in the article.

Statistics.
This group contains statistics measured by the remote probe for each monitored interface on the network management tool.

History.
This group contains periodic samples that are stored for later retrieval.
Alarm.  
This group periodically retrieves statistical samples from variables in the probe and compares them to predefined thresholds, generating an event if the threshold is exceeded.

Host.  
This group contains statistics associated with each host discovered on the network.

HostTopN.  
This group is used to prepare reports for a list ordered by the top N statistics for a host.

Matrix.  
This group stores statistics about conversations between two network addresses.

Filter.  
This group enables packets to be matched based on a predefined filter equation. Matched packets may be used to generate events or they can be captured.

Packet Capture.  
This group enables packets to be captured based on predefined filters.

Event.  
This group controls the generation and notification of events.

The Statistics and Alarm Groups

For many network management applications, the statistics and alarm groups are especially important. The statistics group contains statistics measured by the Remote MONitoring probe in real time for each monitored interface on the probe. Thus, viewing the statistics group provides the network manager or administrator with information concerning the utilization level of a monitored network, the type of activity being performed, and similar information that may indicate the cause of a network problem.

Through the use of the alarm group, statistical samples from variables in the RMON probe are compared to previously configured thresholds. Thus, users obtain a proactive network management capability through the use of the alarm group because they can configure thresholds below the level where serious degradation occurs. This results in the generation of alarms that can then be used as a signal to carefully monitor network activity, such as information generated by the statistics group. Thus, many times the network manager will focus primarily on the statistics and alarm groups, using the information obtained from the other groups only periodically.

Statistics Group Counters

Because of the importance of the statistics group, the counters for Ethernet and Token Ring for that group are listed. Although Ethernet has one statistics group, Token Ring has two such groups.

The first Token Ring statistics group consists of a series of counters that track Media Access Control packets. The second Token Ring statistics group consists of a series of counters that track all frames that flow on the network with the exception of MAC frames, which are tracked by the general statistics group. Because this statistics group tracks all non-MAC frames, it is referred to as a promiscuous statistics group. Under Regional Financial Center 1271, the implementation of the promiscuous statistics group is optional.
Exhibit 2 lists the Ethernet RMON statistics group counters, Token Ring MAC, and Token Ring promiscuous statistics group counters. For each type of network, the RMON statistics group tracks error conditions applicable to each type of LAN. In addition, the Ethernet statistics group and the Token Ring promiscuous statistics group also track the distribution of frame lengths.

## RMON Statistics Groups for Ethernet and Token Ring

<table>
<thead>
<tr>
<th>Ethernet RMON Statistics Group</th>
<th>Token Ring MAC Statistics Group</th>
<th>Token Ring Promiscuous Statistics Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropped events</td>
<td>Dropped events</td>
<td>Dropped events</td>
</tr>
<tr>
<td>Octets</td>
<td>MAC Packet Octets</td>
<td>Data Octets</td>
</tr>
<tr>
<td>Packets</td>
<td>MAC Packets</td>
<td>Data Packets</td>
</tr>
<tr>
<td>Broadcast Packets</td>
<td>Ring Purge Events</td>
<td>Data Broadcast Packets</td>
</tr>
<tr>
<td>Multicast Packets</td>
<td>Ring Purge Packets</td>
<td>Data Multicast Packets</td>
</tr>
<tr>
<td>CRC Alignment Errors</td>
<td>Beacon Events</td>
<td>Data Packets 18 to 63 Octets</td>
</tr>
<tr>
<td>Undersize Packets</td>
<td>Beacon Time</td>
<td>Data Packets 64 to 127 Octets</td>
</tr>
<tr>
<td>Oversize Packets</td>
<td>Beacon Packets</td>
<td>Data Packets 128 to 255 Octets</td>
</tr>
<tr>
<td>Fragments</td>
<td>Claim Token Events</td>
<td>Data Packets 256 to 511 Octets</td>
</tr>
<tr>
<td>Collisions</td>
<td>NAUN Changes</td>
<td>Data Packets 256 to 511 Octets</td>
</tr>
<tr>
<td>Packets&lt;=64 Octets</td>
<td>Line Errors</td>
<td>Data Packets 1024 to 2047 Octets</td>
</tr>
<tr>
<td>Packets 65 to 127 Octets</td>
<td>Internal Errors</td>
<td>Data Packets 2048 to 4095 Octets</td>
</tr>
<tr>
<td>Packets 128 to 255 Octets</td>
<td>Burst Errors</td>
<td>Data Packets 4096 to 8191 Octets</td>
</tr>
<tr>
<td>Packets 256 to 511 Octets</td>
<td>AC Errors</td>
<td>Data Packets 8192 to 18000 Octets</td>
</tr>
<tr>
<td>Packets 512 to 1023 Octets</td>
<td>Abort Errors</td>
<td>Data Packets&gt;18000 Octets</td>
</tr>
<tr>
<td>Packets 1024 to 1513 Octets</td>
<td>Lost Frame Errors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Congestion Errors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Frame Copied Errors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Token Errors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Soft Error Report Frames</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ring Poll Events</td>
<td></td>
</tr>
</tbody>
</table>

### Foundation Manager: An Example of Remote Network Management

In a Simple Network Management Protocol environment, the Foundation Manager program (developed by ProTools, Inc., a subsidiary of Network General Corp.) is a network management platform with a built-in Simple Network Management Protocol manager. The network management platform interacts with the SNMP manager to retrieve data from remote probes and then uses its built-in display capability to present the retrieved information in a format that facilitates the understanding and comparison of multiple Remote MONitoring agent variables.

Foundation Manager can monitor both Ethernet and Token Ring networks, either singularly for a local network or simultaneously for multiple networks. Although Network
General markets a probe for use with its Foundation Manager, any vendor's RMON probe can be used as long as it is compliant with Regional Financial Center 1271 or 1513.

Remote Ethernet Monitoring

Under the main window menu is the program's ribbon bar, which contains a series of icons in two sections, separated by a pull-down menu in the center. The icons in the ribbon bar provide quick access to various program options, such as starting or stopping monitoring by an agent, viewing outstanding alarms, and configuring simple network management protocol (SNMP) communications settings.

Under the ribbon bar is the solution bar, represented by a series of larger icons. Those icons represent functions associated with the pull-down menu labeled Remote Ethernet Monitoring, which is displayed in the ribbon bar.

Foundation Manager permits the monitoring of one local network to which the computer running the software is directly connected as well as the monitoring of multiple remote networks. In addition, this network management platform can perform functions beyond those standardized by RMON, such as packet decoding. Through the selection of a pull-down ribbon bar entry, users can initiate the basic operation of the management platform.

The Icon Panel

Users can construct paths of predefined functions to analyze a network by moving icons into the main portion of the window that is the program's path area. For example, the icon at the top left column in the icon panel is the acquire icon. By moving that icon into the path area, users can acquire frames from the network. Then, by clicking on a predefined icon in the path area, users can display a specific RMON group of information. As an alternative, users can directly select a solution bar icon to rapidly display different types of network statistics.

Exhibit 3 illustrates the resulting display obtained from selecting the second and third icons from the left in the program's solution bar. The second icon, which appears as a bar chart labeled Net, produces the display of network activity that is shown in the top portion of the program's main window area in Exhibit 3. The labels of each bar correspond to Ethernet RMON statistics group counters. The display method of those counters is not standardized, so management platform developers can select any method they desire.

Network Statistics Displayed in Bar Chart and a Line Graph of Network Utilization and Broadcast Packets per Second

Displaying Network Information in a Line Graph.

If selected, the third icon in the solution bar displays Ethernet use and broadcast packets per-second in a line graph format. The result of the selection of this line graph icon in the solution bar is displayed in the lower half of the Foundation Manager's main window area shown in Exhibit 3. Although the percentage of network use is not included in the Ethernet statistics group, it can be easily calculated, because the maximum number of frames or packets that can flow on an Ethernet LAN is known and by counting packets actually transmitted, the management platform can then compute the utilization of the network. Similarly, although there is no broadcast-per-second counter in the Ethernet statistics
group, there is a broadcast counter. By dividing the value of that counter by one-second
time intervals, a management platform can track and display broadcast packets per second.

**Displaying Network Information in a Bar Graph.**

Through the selection of the fourth and fifth icons in the solution bar, users can display
another line graph of information and a bar graph showing the distribution of packets by
size as well as packet errors. Exhibit 4 shows the line chart display of four variables on a
per-second basis (shown in the top portion of the main window area) and the display of
packet-size distribution in a bar chart format in the lower portion of the main window area.
The line graph in Exhibit 4 provides a visual display of bytes, fragments, frames, and
cyclical redundancy checking (CRC) and alignment errors on a per-second basis as well as
digital display of a running total. Thus, users can view this display for an indication of the
transmission activity on the remote network as well as the state of two error conditions—
fragments and CRC/alignment errors.

**Viewing Four Variables in a Line Graph and Packet-Length
Distribution in a Bar Graph**

In the lower portion of Exhibit 4, the bar chart displays the distribution of packets by their
size as well as four types of packet-size or packet-length error conditions. By examining
the distribution of packets by length, users can determine, without packet decoding, the
general type of activity occurring on the monitored network. Relatively short packets are
used to transport interactive query traffic, and relatively long packets are used for file
transfer operations.

**Remote Token Ring Monitoring**

The use of Foundation Manager to monitor a remote Token Ring network produces a
display similar to that obtained from the program with an Ethernet RMON probe. The key
difference between monitoring an Ethernet and a Token Ring network involves the display
of statistical group counters that differ between RMON probes.

Selecting icons labeled Net and Size from the Foundation Manager Screen and the
alarm icon from the program's solution displays three windows in the program's main
window area. The upper left window shows network usage information in a bar chart
format. This window provides an overview of network activity on the monitored Token
Ring network including network use and various data rates, including a soft error rate.

The window labeled Alarm displays current alarm activity as well as the thresholds
currently set to generate alarms. As indicated in the window, a ring usage exceeding 50% in
30 seconds or more than 10 ring purges in 30 seconds are currently defined alarm
generation criteria. The RMON alarm group contains other alarm criteria in addition to the
two just mentioned. Through Foundation Manager or another management platform, users
can set the thresholds for various alarms. Then, the occurrence of a threshold can be used
to generate a visual and audio alert as well as log the alarm to a logfile.

Selection of the bar chart icon labeled Size in the solution bar results in the display
of a bar chart. Similar to the Ethernet bar chart, this bar chart denotes the distribution of
packets by length on the monitored remote Token Ring networks, providing users with an
indirect mechanism to note the type of LAN activity on the network.
Conclusion

The exhibits in this article showing the display of counters maintained by Ethernet and Token Ring Remote MONitoring probes indicate how RMON can provide the network manager and administrator with valuable information. Through the use of a network management platform and one or more remote probes, users can monitor the vital signs of remote networks. In addition, by setting appropriate alarm threshold values, users can be alerted to deteriorating conditions. This allows time to reconfigure a network or perform another type of network modification to alleviate problems before the end user notices poor network performance. Because of this, network administrators should consider RMON a proactive network management tool that can be extremely valuable for isolating, reducing, and eliminating remote network problems.

Author Biographies

Gilbert Held

Gilbert Held is director of 4-Degree Consulting, a Macon GA-based high-tech consulting group. He is an internationally recognized author and lecturer, having written more than 40 books and 300 technical articles. He earned a BSEE from Pennsylvania Military College, an MSEE from New York University, and MBA and MSTM degrees from The American University. He has been selected to represent the US at technical conferences in Moscow and Jerusalem and has received numerous awards for excellence in technical writing.
### Statistics - Staffing - Ethernet

<table>
<thead>
<tr>
<th>File</th>
<th>Edit</th>
<th>Add</th>
<th>Options</th>
<th>Special</th>
</tr>
</thead>
<tbody>
<tr>
<td>500000</td>
<td>3000</td>
<td>50</td>
<td>50</td>
<td>10</td>
</tr>
<tr>
<td>705748</td>
<td>2634</td>
<td>58</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ethernet Bytes /sec</td>
<td>Ethernet Frames /sec</td>
<td>Ethernet %Usage</td>
<td>Ethernet Brdcst /sec</td>
<td>Collsn Fraqs /sec</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/ Align Errors</td>
<td>Total Drop Events</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Display remote Ethernet segment statistics in a bar chart**

- Increments are 60 seconds
- 14:25:05 Jun 06 - 15:29:32 Jun 06
- Ethernet%Usage / 58 50 Broadcast/sec / 0 50
Show Ethernet frame size distribution on the remote segment