SNMP Monitoring: One Critical Component to Network Management

Although SNMP agents provide essential information for effective network monitoring and troubleshooting, SNMP alone does not provide all the information you need to stay on top of your network. For comprehensive analysis of many issues, a network analyzer with packet capture capabilities is required as well. This white paper describes how SNMP works, the advantages of SNMP monitoring, and how SNMP continues to remain a critical part of a complete network analysis solution.

Overview

SNMP (Simple Network Management Protocol) is the common language of network monitoring–it is integrated into most network infrastructure devices today, and many network management tools include the ability to pull and receive SNMP information. SNMP extends network visibility into network-attached devices by providing data collection services useful to any administrator. These devices include switches and routers as well as servers and printers. The following information is designed to give the reader a general understanding of what SNMP is, the benefits of SNMP, and the proper usage of SNMP as part of a complete network monitoring and management solution.

What is SNMP?

The Simple Network Management Protocol (SNMP) is a standard application layer protocol (defined by RFC 1157) that allows a management station (the software that collects SNMP information) to poll agents running on network devices for specific pieces of information. What the agents report is dependent on the device. For example, if the agent is running on a server, it might report the server's processor utilization and memory usage. If the agent is running on a router, it could report statistics such as interface utilization, priority queue levels, congestion notifications, environmental factors (i.e. fans are running, heat is acceptable), and interface status.

All SNMP-compliant devices include a specific text file called a Management Information Base (MIB). A MIB is a collection of hierarchically organized information that defines what specific data can be collected from that particular device. SNMP is the protocol used to access the information on the device the MIB describes. MIB compilers convert these text-based MIB modules into a format usable by SNMP management stations. With this information, the SNMP management station queries the device using different commands to obtain device-specific information.

There are three principal commands that an SNMP management station uses to obtain information from an SNMP agent:

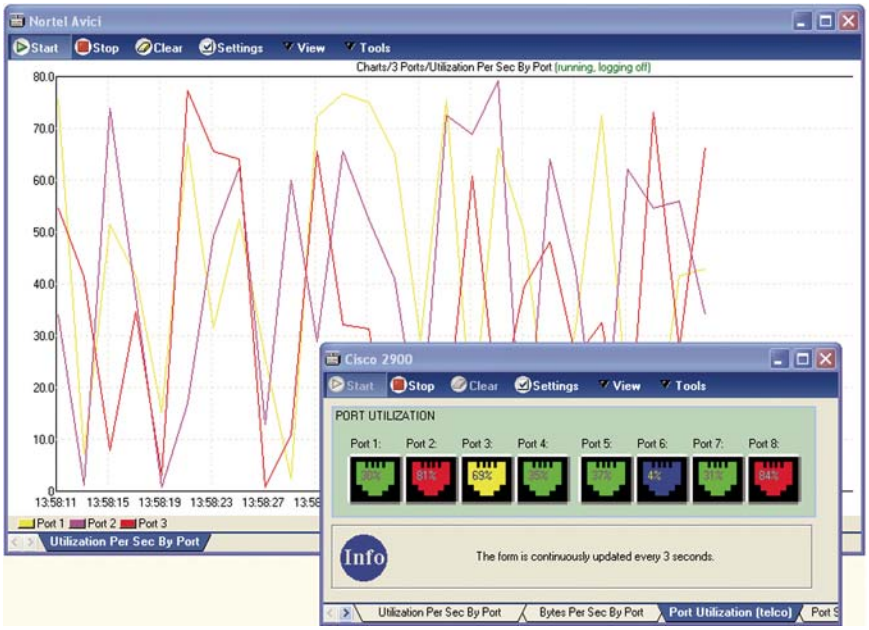
1. The get command collects statistics on SNMP devices.
2. The set command changes the values of variables stored within the device.
3. The trap command reports on unusual events that occur on the SNMP device.

The SNMP management console reviews and analyzes the different variables maintained by that device to report on device uptime, bandwidth utilization, and other network details.

Why use SNMP?

SNMP delivers management information in a common, non-proprietary manner, making it easy for an administrator to manage devices from different vendors using the same tools and interface. Its power is in the fact that it is a standard: one SNMP-compliant management station can communicate with agents from multiple vendors, and do so simultaneously. Illustration 1 shows a sample SNMP management station screen displaying key network statistics.

Another advantage of SNMP is in the type of data that can be acquired. For example, when using a protocol analyzer to monitor network traffic from a switch's SPAN or mirror port, physical layer errors are invisible. This is because switches do not forward error packets to either the original destination port or to the analysis port. However, the switch maintains a count of the discarded error frames and this counter can be retrieved via an SNMP query.

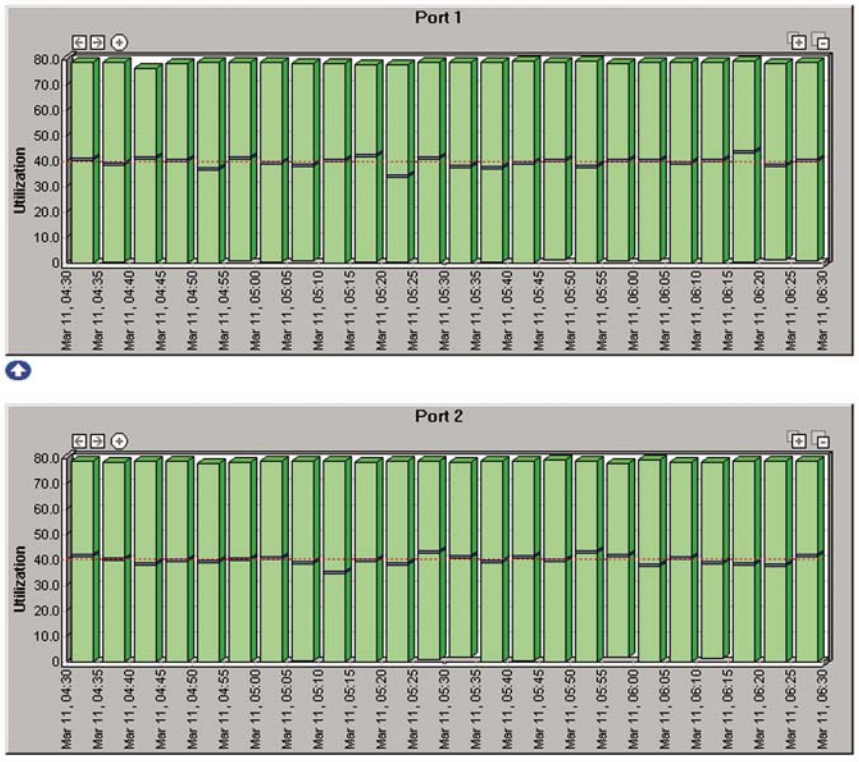


Sample SNMP management station showing utilization on an SNMP device

Where should you use SNMP?

SNMP can be used in any environment where constant monitoring of key devices is required. Many SNMP management stations offer long-term reporting capabilities, allowing an administrator to watch network trends develop over time and to take appropriate action before problems can seriously affect users. Illustration 2 shows a sample report illustrating maximum, minimum and average router utilization.

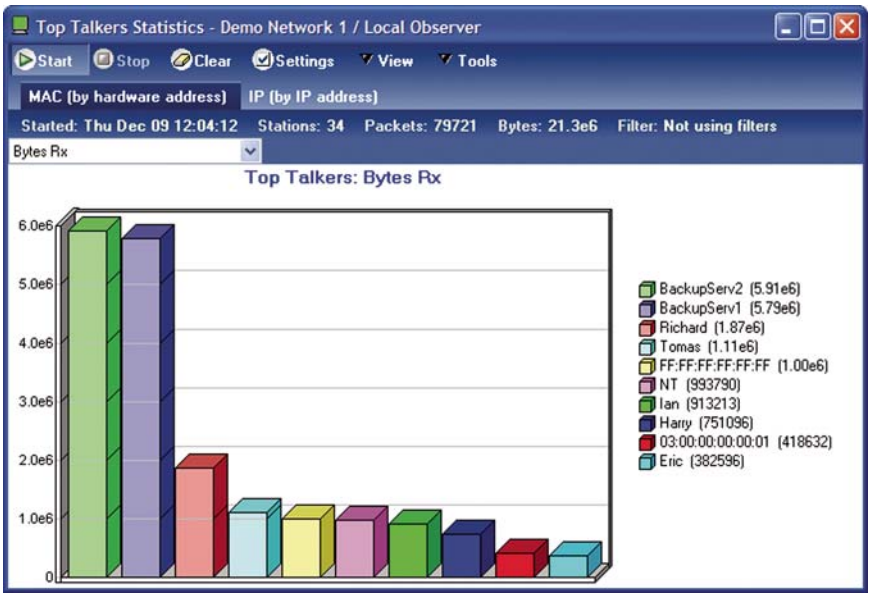
Triggered notifications are also available from many SNMP management stations. Notifications allow the administrator to receive an e-mail or page if certain user-defined thresholds have been exceeded, such as maximum port utilization.



Sample SNMP Report showing Router Utilization

What is missing from SNMP?

While SNMP provides excellent statistics on the macro level, it does not provide the level of detail that is often required to completely resolve many network issues. For example, while SNMP may show high utilization on the router's Internet interface, it may not show what kinds of traffic are using up the bandwidth or who is responsible for the traffic. This leaves the administrator knowing what the problem is (high bandwidth consumption to the Internet), but not knowing the cause, and therefore, lacking the ability to quickly resolve the issue. Illustration 3 shows how a network analyzer's Top Talkers view with detailed analysis capabilities can assist in in-depth problem solving scenarios. By reviewing the network's Top Talkers (who is causing the traffic), the network administrator can isolate the cause of the excessive utilization and take steps to resolve the issue. This deeper level of detail is not found inside an SNMP management console. However a network analyzer with SNMP management capability can offer the full view of the fundamental network issue.



Network analyzer console showing network Top Talkers

SNMP – A Component of Total Network Management

Make no mistake-SNMP monitoring should be a part of any network management solution. But effective administration of enterprise networks requires more than SNMP management. Only a comprehensive network analyzer can deliver both in-depth analysis along with the ability to manage and view statistics from SNMP-compliant devices. When selecting a network analyzer, choose a solution that provides full network coverage for multi-vendor hardware networks including a console for SNMP devices anywhere on your LAN or WAN. Also, look for a solution that includes a network mapping program that can help you visualize the network by continually monitoring and displaying device and route statuses. In addition, the network analyzer should report information about services running on the primary devices. This information is important to an administrator of a single site, and invaluable to an administrator who is responsible for multiple sites. Often, the network mapping program is integrated with the SNMP management station, allowing the two systems to share information. This is accomplished by using the network mapping tool as a first step, SNMP as a high-level drill down, and finally a network analyzer for deeper level statistics and information.

A comprehensive network analyzer also includes a packet decoding and analysis tool. Providing the additional depth that SNMP management lacks, a network analyzer allows you to look beyond simple statistics into the actual frames being transmitted across the network. While network analyzers vary greatly in their feature sets, some of the primary functions you should look for in addition to packet capture and decode is some form of Expert analysis for advanced problem identification and resolution, long-term reporting capabilities, and triggered notifications. These features can provide ongoing insight into the day-to-day operations of the network, at a level beyond the scope of SNMP. Figure 1 is a checklist designed for any network administrator to review when choosing a comprehensive network management solution.

Conclusion

SNMP management provides valuable insight to any network administrator who requires complete visibility into the network, and it acts as a primary component of a complete management solution. However, SNMP was never intended as a comprehensive network monitoring solution. It therefore must be complimented by a complete suite of network monitoring and management tools. You should not have to choose whether you want to review network traffic or network devices. For complete visibility, choose a solution that provides both. When shopping for the right network analyzer for your network, consider a comprehensive solution for complete coverage.

Network Management Solution Checklist

Capabilities to look for when choosing a network management solution

Network Coverage
__ LAN support
__ WAN support
__ Gigabit support
__ Wireless support
__ VoIP analysis
__ VLAN analysis

Device Management
__ Ability to optimize and manage SNMP-compliant devices
__ Remote console for SNMP devices
__ RMON management
__ Support for multi-vendor hardware networks
__ Report on services running

Distributed Analysis
__ Local and remote visibility
__ Remote collection and analysis capabilities
__ Multiple remote probe access

Network Mapping
__ Continuously monitor for device and route uptime
__ Ability to build network maps

Network Statistics
__ Real-time statistics
__ Network utilization
__ Application-level statistics
__ Access point statistics

Protocol Analysis
__ Packet capture
__ Packet decode
__ Remote real-time capture and decode capability
__ Filtering capabilities
__ Data-mining options
__ Post-capture filters

Fault Analysis
__ Real-time Expert system
__ Monitor for pre-defined Expert events
__ Comprehensive list of Expert conditions
__ Ability to custom design Expert conditions

Proactive Network Management
__ Pre-defined alarms
__ User-defined or customizable alarms
__ Multiple alarm options (e-mail, page, trouble ticket, log, etc.)
__ “What-if” analysis

Trending and Reporting
__ Long-term capability
__ Ability to save data, not just reports
__ Web publishing option
__ Modeling

Corporate Headquarters Network Instruments, LLC • 8800 West Highway Seven • Fourth Floor • Minneapolis, MN 55426 • USA
toll free (800) 526-7919 • telephone (952) 932-9899 • fax (952) 932-9545 • www.networkinstruments.com
European Office Network Instruments • 7 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom
telephone +44 (0) 1959 569880 • fax +44 (0) 1959 569881 • www.networkinstruments.co.uk
France, Italy and Spain Network Instruments • 1 rue du 19 janvier • 92380 Garches • Paris • France
telephone +33 (0) 1 47 10 95 21 • fax +33 (0) 1 47 10 95 19 • www.networkinstruments.fr
Germany Network Instruments • Allacherstr. 189a • 80997 München • Germany
telephone +49 (0)89 159 842-48 • fax +49 (0)89 159 842-49 • www.networkinstruments.de