SNMP Software Solutions for Optimizing DNS/DHCP Server Performance and Availability

IT Managers need a way to streamline the collection and monitoring of critical performance statistics and operational data across the enterprise.

Advanced solutions like Lucent VitalQIP™ SNMP software ensures that critical network services are operating at optimal performance, reducing network downtime and associated costs while lowering network operation expenses.

This white paper addresses how to:

- Use SNMP management software to quickly obtain the statistical data required to ensure maximum availability of IP name and address services
- Automate repetitive manual tasks; reduce operations and administration staffing needs
- Leverage the capabilities of Lucent VitalQIP™ SNMP Module software in proactive network management

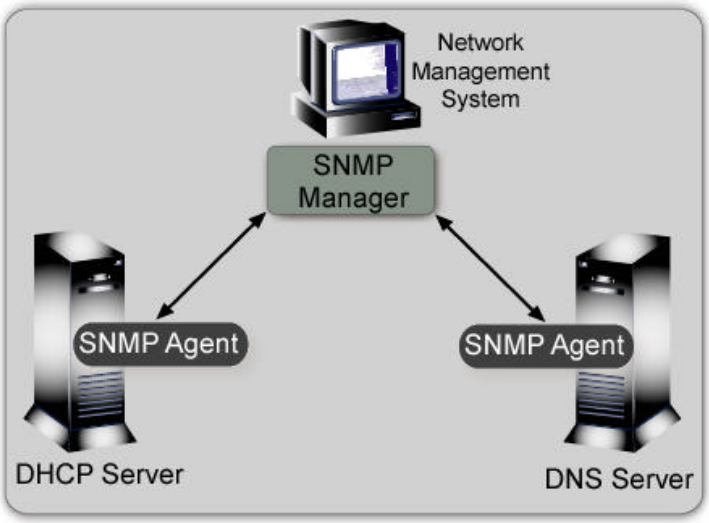
Lucent Technologies
Bell Labs Innovations



Introduction to SNMP

Developed in 1988, the Simple Network Management Protocol (SNMP) is the de facto standard for network management. The SNMP architecture consists of primarily two components -- a Manager and an Agent. The Manager is the application through which network management functions are performed. Agents are the entities that interface to the actual devices being managed. Typically, there is one or potentially a few Managers in a network and there may be hundreds or even thousands of agents.

Historically, SNMP has been used to perform management of physical network devices or elements, such as routers, hubs, and switches. The information managed on these devices usually consists of configuration parameters, performance statistics, and error conditions. These variables are organized into a database called the Management Information Base (MIB). The MIB is a hierarchical data structure, which is represented as a tree; each branch and leaf in the MIB tree is uniquely identified by an Object Identifier (OID).



SNMP ultimately defines the protocol for Managers and Agents to access and report upon data maintained in the MIB:

Agents

- Implement SNMP
- Store and retrieve management data from the MIB
- Asynchronously signal events to an SNMP Manager

Managers

- Implement SNMP
- Query Agents
- Get responses from Agents
- Set variables in Agents
- Receive asynchronous events from Agents

The importance of SNMP management for DNS and DHCP services

Early deployments of SNMP were focused on the management of hardware devices that are critical to the functioning of the network. These devices typically included routers, switches, and servers. For example, the SNMP Agent for a router generally maintains information regarding each of the interfaces configured on the router, as well as keeping statistics for number, size, etc. of packets that flow through the router. In addition, a router's SNMP Agent could report significant events, especially error conditions, to a Manager in order to alert someone about the event.

In today's networks, there are several software components that are equally as important as hardware elements in providing network connectivity. Two such software services include Dynamic Host Configuration Protocol (DHCP), which provides IP addresses and other configuration information to hosts on the network, and the Domain Name System (DNS), which resolves names to IP addresses. These services are critical to the proper operation of the network and therefore must be managed by network administrators in much the same way that hardware devices are managed.

The SNMP protocol runs over a connectionless communication transport, typically User Datagram Protocol (UDP). UDP is used because it is a fairly lightweight protocol, and hence incurs very little overhead for both the Agent and Manager implementations. This is important, because SNMP is intended to manage networks without severely impacting the performance of the monitored network elements.

However, UDP is also an unreliable network protocol, which means that sometimes certain messages may not be delivered to their intended recipients. In order to handle such situations, SNMP Agents and Managers often retry sending of SNMP packets.

Typical SNMP environments operate using version 1 or version 2c of the SNMP protocol. These versions use a Community-based Security Model (CSM). This offers a base level of security, which relies on passwords, or community strings, that are configured on the Agents and required by the Manager in order to manage the Agents. There are two levels of security, one for querying information from the Agent, and another for setting variables on the Agent. The levels are specified using a read community string and a write community string, respectively. These community strings must be specified by any Manager that wishes to perform such actions against the Agent.

SNMP version 3 introduced a more granular security paradigm, known as the User-based Security Model (USM). The USM is defined in Internet Official Protocol Standard RFC 2574. The goals of this security model are as follows:

1. Provide for verification that each received SNMP message has not been modified during its transmission through the network.

2. Provide for verification of the identity of the user on whose behalf a received SNMP message claims to have been generated.

3. Provide for detection of received SNMP messages, which request or contain management information, whose time of generation was not recent.

4. Provide, when necessary, that the contents of each received SNMP message are protected from disclosure.

Using SNMP to ensure network connectivity

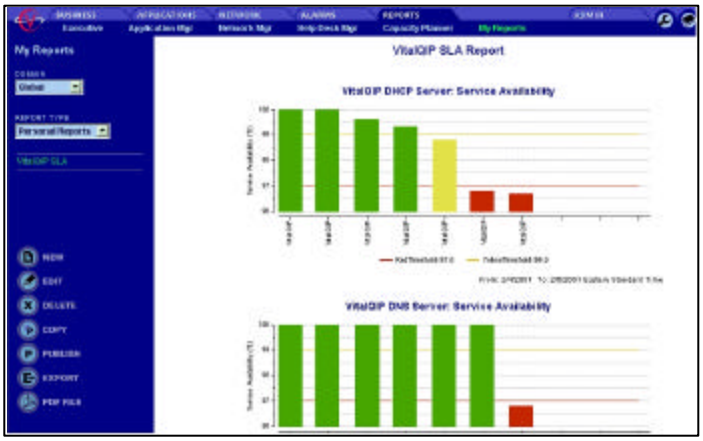
The DHCP server configuration consists mainly of IP subnets, and scopes or ranges of addresses within those subnets. The server allocates IP addresses, as needed, for hosts on the network. As business and network infrastructure needs change, often times more hosts are added to a particular subnet. If the network planning accounted for these additional hosts when the DHCP was configured, then support for these hosts will be handled automatically.

However, in many cases, the additional hosts were not planned for, and thus require configuration changes to the DHCP server in order to support them. Ideally, the network administrator could anticipate when to make the changes to the DHCP server configuration, so as to avoid any disruption, or lack of network connectivity, for new or existing hosts.

Generally, however, it is not until a network user calls a help desk to complain that the need for additional subnets or scopes is realized. By this time, there could be a flurry of users calling with network connectivity problems. This impacts the ability for the network administrator to effectively manage the necessary changes.

Using the Lucent Technologies DHCP 5.3 server and the VitalQIP™ software SNMP add-on module 2.0, network administrators can determine the need for additional subnets and/or IP scopes on a given network before addresses have been exhausted. This is accomplished by defining thresholds on address usage at the subnet level. For example, if the address usage threshold was configured at 75% of the available addresses, then the network administrator could be notified when the DHCP server had allocated that percentage of addresses. The notification is performed via an SNMP trap event, which is generated automatically upon reaching the threshold. This trap event will be directed to an SNMP management station, typically an application such as HP Openview or CA Unicenter.

In addition, combining VitalQIP™ SNMP 2.0 module with Lucent Technologies VitalNet™ network performance monitoring software, a network administrator could perform more detailed threshold monitoring as well as trend analysis. Using VitalNet™ software, each variable available from the DHCP agent plug-in can be queried over a period of time to allow analysis of all resource utilization. Specific scopes can be monitored for IP address usage, or multiple separate scopes can be combined into one view for monitoring.



VitalNet™ software monitoring a DHCP server and a DNS server for availability and compliance to a Service Level Agreement (SLA)

The Lucent VitalQIP™ SNMP Software Module

The SNMP Module v2.0 is an add-on product to the award winning VitalQIP™ IP Management platform. This module supplies additional modules, or adapters, that "plug-in" to the Lucent DHCP and DNS services. These adapters provide the functionality of an SNMP agent, allowing the servers to operate unencumbered by the presence of the adapter. The module includes MIBs specifically tailored for management of the Lucent Technologies DHCP and DNS services. The information available from the DHCP and DNS agents is defined in these MIBs, and includes the following groups:

DHCP MIB

- System – description, status
- Subnet Counters – used, unused, full subnets
- Bootp/DHCP Counters – sent and received packets by message type
- Bootp/DHCP Statistics – response times
- Server Configuration – subnets, ranges, allocation types
- Failover – partner address, type, status
- Traps – stopped, started, reload, subnet threshold, failover

DNS MIB

- System – description, status
- Counters – sent and received packets by message type
- Statistics – response times
- Configuration – recursion, round-robin
- Traps – stopped, started, reload, configuration error

Reduce Network Downtime with the VitalQIP™ SNMP Software

The SNMP 2.0 module add-on for VitalQIP™ software provides network administrators with a powerful tool for managing the Lucent DHCP and DNS servers. Important information about the utilization, performance, and error conditions of these critical services can be monitored in order to allow for proactive resolution of issues before they cause serious network service interruptions. When combined with traditional SNMP Managers, such as VitalNet™ performance monitoring system or others such as HP Openview, VitalQIP™ SNMP software can help to ensure that the network's IP infrastructure services are operating at optimal performance, reducing network downtime and associated costs and improving the bottom line of network operations.

VitalQIP™ IP Address Management and VitalSuite™ Network Performance Management Software

Each winner of many awards, VitalQIP™ software for IP address management and VitalSuite software for network performance management together offer comprehensive, fully integrated, cost effective network management solutions. Providing real-time views into everything in your network from complex e-commerce transactions to curial network resources, they allow you to continuously monitor, measure and optimize performance at every level of your IT operations.

To learn more, contact your Lucent Technologies sales representative, authorized reseller or sales agent. You can also visit our web site at http://www.lucent.com/vital or call 1-888-426-2252.

This document is for planning purposes only, and is not intended to modify or supplement any Lucent Technologies specifications or warranties relating to these products or services. The publication of information in this document does not imply freedom from patent or other protective rights of Lucent Technologies or others.

*PricewaterhouseCoopers 2000

VitalQIP™, VitalSuite™, VitalNet™, VitalEvent™ and VitalApps™ are trademarks of Lucent Technologies. All other product name and marks contained herein are the property of the respective owners.

Copyright © 2003 Lucent Technologies Inc. All rights reserved.