International Journal of Power Control Signal and Computation(IJPCSC)
Vol3. No1. Jan-Mar 2012 ISSN: 0976-268X
www.ijcns.com

Network Monitoring Using SNMP Protocol

Sivakumar S.R. #1, Mangaiyarkarasi.R *2
PG Scholar #
Assistant Professor *
Department of Computer Science & Engineering #*
srshiva71@yahoo.com #, mangai.svr@gmail.com *

Abstract

SNMP (Simple Network Management Protocol) monitor is used to manage agents in a network by collecting network-related parameters. The development of Network Monitor is capable of extracting valid parameters from an SNMP agent. These parameters predefined in management information base (MIB). It is makes an interactive environment between the SNMP manager and SNMP Agent to make monitoring between manager and agent. The manager is a tool for extracting the values of the managed objects and the agent is a user who needs the details. To manage large system and networks, which continue to grow in scale and diversity, a rich set of automated network managing tools and applications are need. In response to the ever demanding needs, Simple Network Management Protocol (SNMP) that was a standard for TCP/IP protocol. One another process that constantly monitors the status of various MIB variables is SNMP polling. If this function is on, the program polls the values of the variables currently displayed on the screen at the specified interval. To enable SNMP polling, it should specify the period using the special drop-down list on the toolbar (from 1 second to 10 minutes). SNMP polling is used to send SNMP requests, defined in various MIBs, to devices on the network that use SNMP. The user can create own polling processes by creating one or more text based versatile programs.

1. INTRODUCTION

. SNMP was deriving from its ancestor SGMP (Simple Gateway Management Protocol) and it planned to exchange by a solution based on the Common Management Information Service/Protocol (CMIS/CMIP) architecture. This long-term solution, however, never received the general acceptance of SNMP.

SNMP based on the manager/agent model consisting of an SNMP manager, an SNMP agent and a database of management information, managed SNMP devices and the network protocol. The SNMP manager provides the interface between the human network manager and the management system. The SNMP agent provides the interface between the manager and the physical device(s) being managed.

The SNMP manager and agent use an SNMP Management Information Base (MIB) and a relatively small set of commands to exchange information. The SNMP MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A long numeric tag or object identifier (OID) used to distinguish each variable uniquely in the MIB and in SNMP messages.

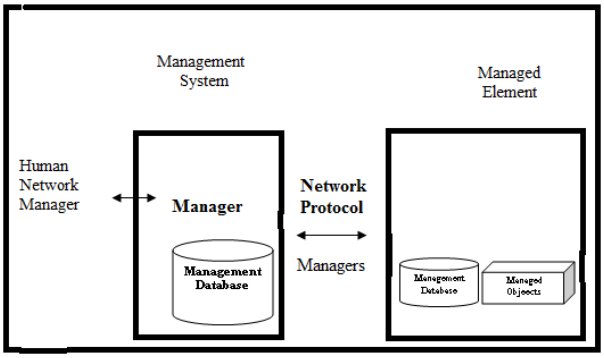

Figure 1. SNMP Architecture

A. SNMP protocol

SNMP uses five basic messages (GET, GET-NEXT, GET-RESPONSE, SET, and TRAP) to communicate between the manager and the agent. The GET and GET-NEXT messages allow the manager to request information for a specific variable.

The agent, upon receiving a GET or GET-NEXT message, will issue a GET-RESPONSE message to the manager with either the information requested or an error indication as to why the request cannot be processed. A SET message allows the manager to request a change made to the value of a specific variable. The SNMP agent will then respond with a GET-RESPONSE message indicating the change has made or an error indication as to why the change cannot make. The SNMP TRAP message allows the agent to spontaneously informed, that the SNMP manager of an "important" event.

Each SNMP element manages specific objects with each object having specific characteristics. Each object / characteristic has a unique object identifier (OID) consisting of numbers separated by decimal points (i.e., 1.3.6.1.4.1.2682.1). These object identifiers naturally form a tree as shown below. The MIB associates each OID with a readable label and various other parameters related to the object. The MIB then serves as a data dictionary or code book that is used to assemble and interpret SNMP messages.

SNMP is referred to as "Simple Network Management Protocol" because the agent requires minimal software. Most of the processing power and the data storage reside on the management systems, while a complementary subset of those functions resides in the managed system.

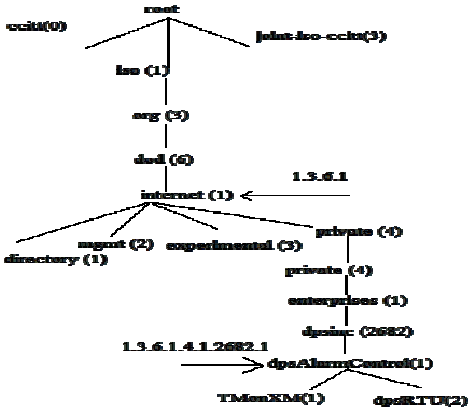

Figure.2 The branch of MIB OID tree

SNMP operates in the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port-to-port 161 in the agent. The agent response will sent back to the source port on the manager. The manager receives notifications (Traps and Inform Requests) on port 162. The agent may generate notifications from any available port. When used with Transport Layer Security or Datagram

IP header	UDP header	version	community	PDU-type	request-id	error-status	error-index	variable bindings

Figure.3 SNMP PDU Construction

Transport Layer Security requests received on port 10161 and traps sent to port 10162. SNMPv1 specifies five-core protocol data units (PDUs). Two other PDUs, GetBulkRequest and InformRequest added in SNMPv2 and carried over to SNMPv3.

2. SNMP MESSAGE CONSTRUCT

A. Each SNMP message has the format:

- Version Number
- Community Name – kind of a password
- One or more SNMP PDUs – assume trivial authentication

B. Outline of SNMP protocol

- Each SNMP managed object belongs to a community
- NMS station may belong to multiple communities
- A community is defined by a community name which is an Octet String with 0 to 255 octets in length

3. FEATURES OF SNMP MONITOR

The Network Monitor provides a set of services to the network engineer. From the list given, the Manager will select the appropriate Monitoring command. The key features are:

A. MIB (Management Information Base)

This list contains all the MIB (Management Information Base) object names organized in the form of a tree structure where the leaves of the tree are the parameters to be accessed by the Monitor. SNMP agents for different types of device provide access to the objects that are specific to the type of devices. In order to enable the SNMP Monitor to operate intelligently on the data available on the device the manager needs to know the names and types of objects on the managed device

MIB modules make this possible, which is specified in the MIB files usually provide with managed devices. For Ex. (Request for comments) RFC-1213 MIB -II is a MIB module, which is typically supported by all SNMP agents on the TCP/IP enabled devices or systems. When MIB-I was developed, the number of objects was intentionally limited to about 100. In MIB-II, this limit was eliminating given the wide technological base.

The MIB file contains a description of object hierarchy on the managed device as well as name (Object id), syntax and access privileges for each variable in the MIB. One key aspect of MIB is that only the types of objects of the managed devices are specify by the MIB and not specific to the objects (object instances). When specifying an object to the SNMP agent a proper object ID, which include the instance needs to use by the manager. When not properly specified, the agent responds with "no such variable error".

B. Description Text Area:

Due to the large number of Network parameters, the user might find him-self in constant trouble in knowing the description of the selected object. The description text area avoids this situation by displaying information about the currently selected object in the MIB list.

C. M value text area:

This text area is used to display the extracted values of MIB object after specifying get_next request from the agent. This can display in a separate text box. This value can extract from the MIB table. The first number of this value is the number of the root and the next will the parent for the root.

D. Polling:

It poles for the values of the objects selected in the MIB list, after a periodic interval specified by the user. The polling can stop by using STOP button or restart it by using START button.

4. HOW SNMP WORKS

Both agents and management systems use SNMP messages to inspect and Communicate host information. SNMP messages are sent using the User Datagram Protocol (UDP). The Internet Protocol (IP) is using to route the messages between the management system and host.

The information that the management system requests is contained in a management information base (MIB). The MIB is a database that contains various types of information about a networked computer, such as the version of network software running on that computer and the available hard drive space. The following example illustrates how an SNMP agent responds to a management system request for information:

The management system (Host A), sends an SNMP datagram to the agent (Host B), using the agent's host name, IP address, or IPX address. The SNMP agent receives the datagram and verifies the community name to which the management system belongs. If it is a valid community name, the agent retrieves the data requested from the appropriate SNMP subagent. If the community name is incorrect, the agent sends an "authentication failure" trap to its trap destinations (Hosts C and D). The SNMP agent returns the datagram to the management system with the requested information.

A. Configure Remote Devices.

Configuration information can sent to each networked host from the management system. Monitor network performance. The speed can track by processing and network throughput, and collect information about the success of data transmissions.

B. Detect Network Faults or Inappropriate Access.

The configuration of trigger alarms on network devices when certain events occur. When an alarm is triggered, the device forwards an event message to the management system. Common types of alarms include a device being shut down and restarted, a link failure being detected on a router, and inappropriate access.

C. Monitor

Both overall network usage to identify user or group access, and types of usage for network devices and services. You can use this information to generate direct billing of accounts or to justify both current network costs and planned expenditures.

5. CONCLUSION

This paper aims at mounting a monitoring application for a SNMP manager and SNMP Agent in a user-interactive environment to make monitoring the network. The manager is a tool for extracting the values of the managed objects and the agent is a user who needs the details about the objects that may extracted from the MIB. After enter in to the system the user can easily find out, How to transmit and receive the frames in the local intranet. It also provides the detail information about the system for the further development. The scope could be extended from management applications to managed device, which deals with dynamic management nodes in a network. With the use of SNMP manager and agent, the user can effectively monitor the agent and control it. The user can monitor the services for possible changes in the status and the usage of ports in the hosts of the network. With more and more devices embracing Ethernet and internet protocols, the addition of SNMP protocol support adds benefits to the device. Managed devices support the SNMP protocol. Agents consist of a collection of managed objects that can queried by a manager to determine the health of the network or the status of particular devices. SNMP is not restricted to just the management of switches and routers. Any industrial device can have SNMP support and could provide much aid in industrial applications.

REFERENCES

1. Jae-Kyu Chun ,Ki-Yong Cho, Seok-Hyung Cho, Young-Woo Lee, Young-Il Kim "Network Management Based On Pc Communication Platform With Snmp And Mobile Agents" Access Network Lab., R&D Group, Korea Telecom, Korea

2. Mi-Jung Choi, Suman Pandey, Sung-Joo Lee, James W. Hong "IP Network Topology Discovery Using SNMP" Dept. of Computer Science and Engineering, POSTECH, Korea

3. Better Network Management Through SNMP - A White Paper Prepared By Liebert Corporation - Liebert Web Notice And Conditions - Copyright © 1995, 1996, 1997, 1998, 1999, Liebert Corporation.

4. Link Layer Discovery Protocol and MIB - v0.0, Paul Congdon – IEEE 802.1 3/7/2002 – St Louis Plenary

5. Enabling SNMP for IEEE 802.15.4: A Practical Architecture Cristian Mihai Vancea and Virgil Dobrota, Member, IEEE

6. SNMP Monitoring: One Critical Component to Network Management-Network Instruments White Paper-2005