REPORT ON SNMP

Submitted by:

Abdul Hakeem (770401-T159)
Adnan Ahmed Khan (780523-T011)
Adnan Altaf (850923 –T075)

1- Introduction:

This report is about the SNMP protocol, its functionality and different versions. This report also depicts some important features and importance of the SNMP in the network environment. With the increase of internet use and traffic on the networks, it was very necessary to develop such methods to capture and monitor the traffic to find the errors and troubleshoot the networking problems. SNMP is a very useful tool to handle all such issues and help the administrator to resolve them.

Contents:

2- SNMP

Simple Network Management Protocol is used to monitor the network traffic. This protocol was developed in 1988 and it is basically derived from SGMP (Simple Gateway Network Protocol). It works on the Application Layer and it is the part of TCP/IP protocol suites. SNMP not only used to monitor traffic but it also captures the errors on the network and notifies the administrator to solve it. By knowing the problems on the net, administrator can improve the performance of the network and make strategies to growth the network for future needs. There are two versions of SNMP: SNMP v1, SNMP v2 and SNMP v3, about which we will talk later. Although they have many common characteristics but due to updates version 2 and 3 are more advanced than version 1 and provide some extra features.

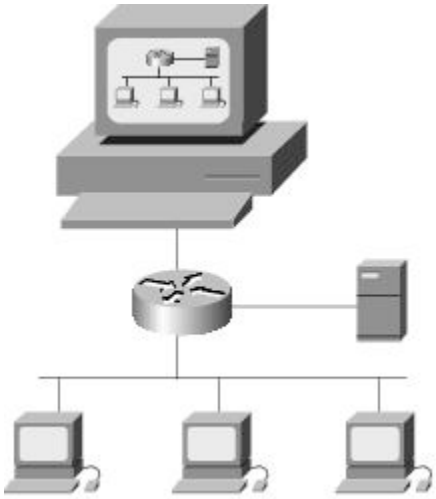

Figure 1[1] SNMP Facilitates the Exchange of Network Information Between Devices

2.1- Components of SNMP

SNMP consists of three components; Devices to be managed, Manager and Agent. It is sometimes called the Manager /Agent model. The Manager provides the interface between human network manager and the management system, while the Agent provides the interface between the manager and the physical devices being managed [2].

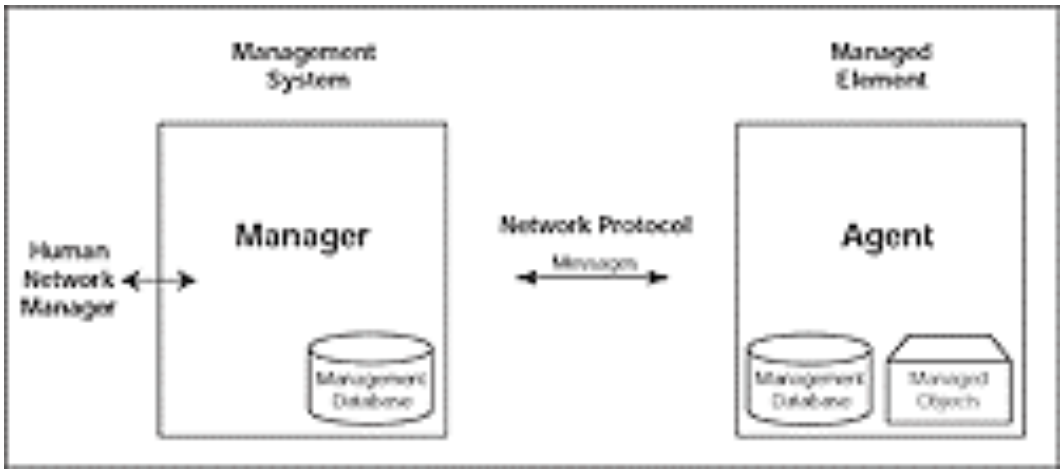

Figure 2 [3] Manager / Agent model

There may be many kinds of devices on the network to be managed like computers, printers, hubs, switches, routers etc. Agent is resides on these devices and collect information, provide these information to the manager to take necessary and corrective actions by the administrator. There are special software installed on Manager to control the devices and all the traffic of network. The manager also provides the processing resources and memory to handle network management.

2.2- Messages of SNMP

SNMP is very simple and easy to use. It has five basic messages to control the network traffic. These messages are communicated between Manager and Agent. These messages are GET, GET-NEXT, SET, GET-RESPONSE and TRAP[4].

First three messages are issued by the Manager but the last two are managed by the Agent. These messages are sent or received by UDP protocol which is very easy to build and run. GET and GET-NEXT messages inquire information about some variables from agent. These variables may be free memory, computer name, running process or any kind of default route. GET-RESPONSE is issued by the Agent which gives the confirmation of requests received from manager. If the Manager wishes to change some values on the devices, a SET message is sent along with the required change which is also replied by GET-RESPONSE. The TRAP message is kind of alarm and issued by the Agent when something happens unusual.

3-MIB (Management Information Base)

It is basically a logical database which has information about the configuration, status and other statistics about the device. Any action on the network is considered as the new variable in the MIB and this database holds all the information about that action. It stores the name of that variables, attributes and operations that can be performed on that variable. This information is then provided to the Manager by SNMP to take necessary

steps. We can say that MIB serves as a data dictionary which is used to assemble and interpret SNMP messages.
These variables are organized in hierarchies or trees with nameless roots. An Object Identifier (OID) is allocated to each variable which uniquely identifies it in the hierarchy. There are different levels of hierarchy which are assigned by different organizations. Top levels are assigned by some Standardized organizations like ISO and lower levels are assigned by associated organizations. MIB uses the notations and names defined by the ASN.1 (Abstract Syntax Notation One).

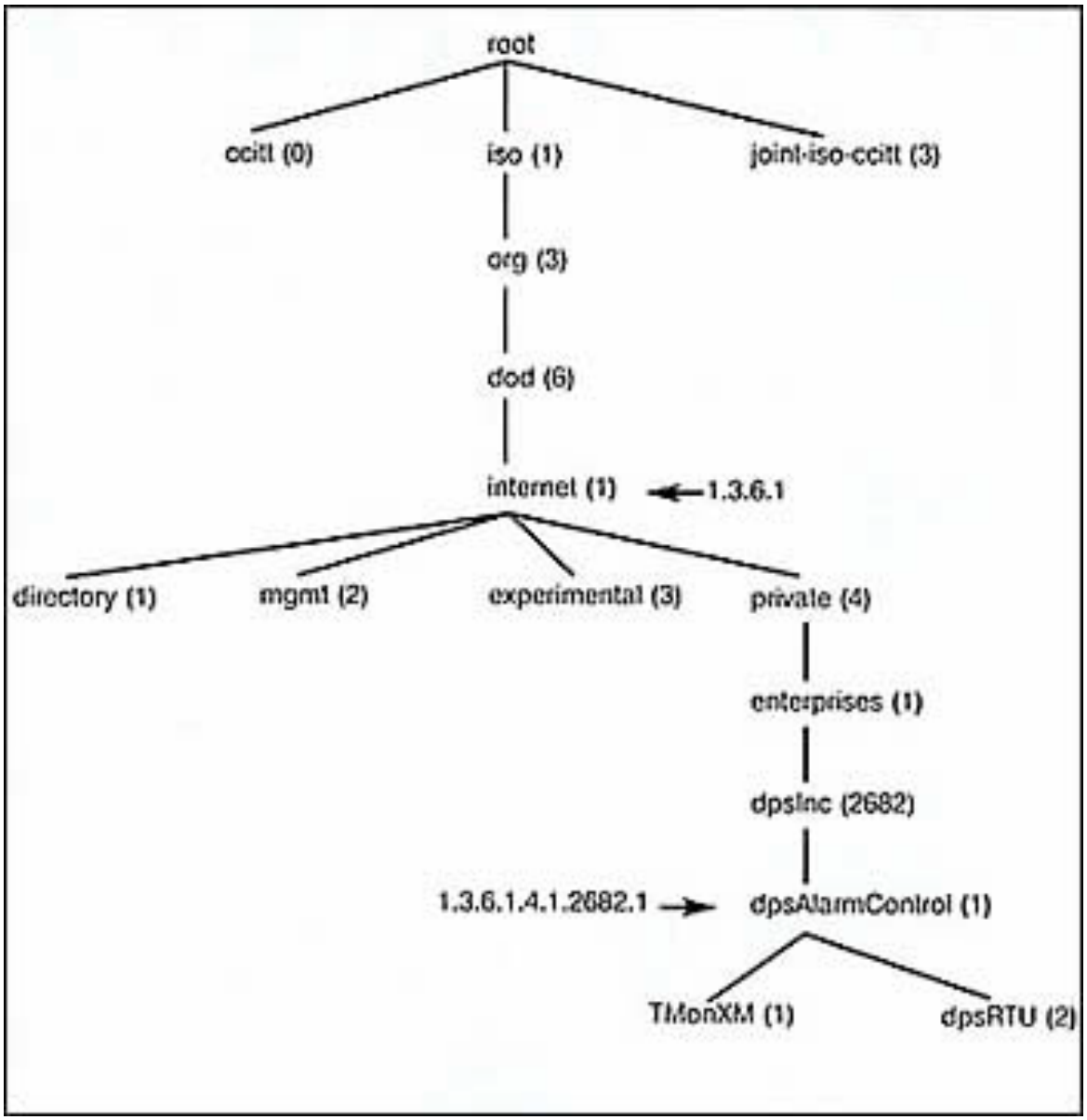

Fig.3 [5] Example of MIB Hierarchy

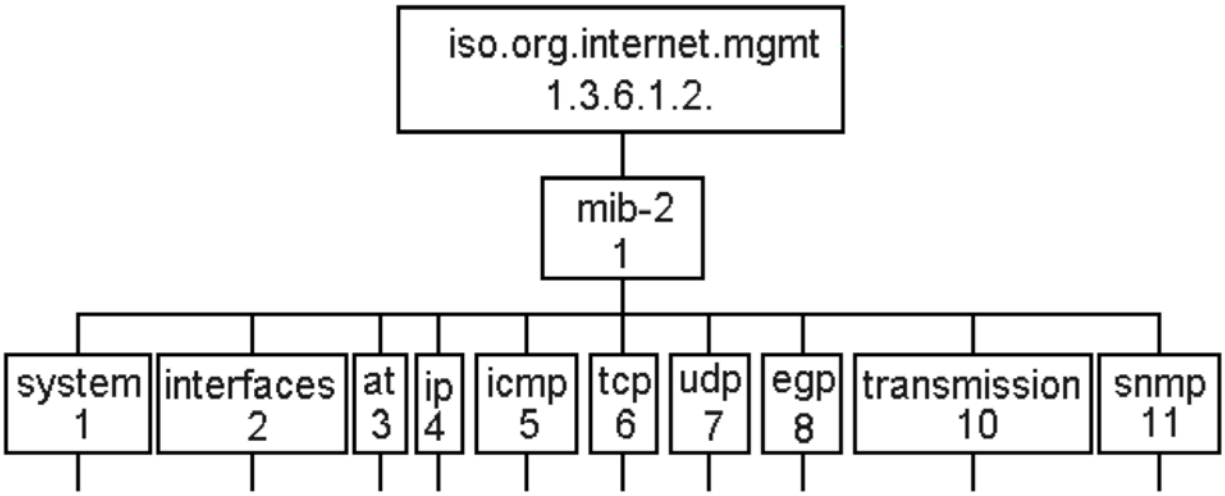

Fig. 4 [6] The MIB node and its object identifiers (OID).

4- Versions of SNMP

There are two versions of SNMP being used now a day. We will briefly discuss about these versions.

4.1- SNMP Version 1

This was the first implementation of SNMP. It is a simple request/ response in which Manager send some request and the Managed Devices give response back. It is briefly described in RFC 1157. It is widely used and is considered as the de facto network protocol in the internet community.

The message in this version contains two parts: Message Header and PDU. The message header contains the version no. and community name, while the PDU contains one of the SNMP messages.

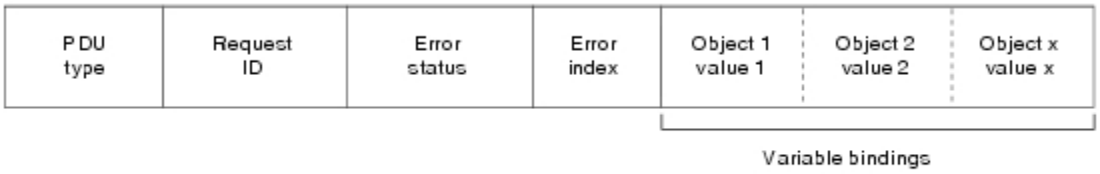

Fig. 5 [7] PDU Format

- ∞ *PDU Type*: It shows the type of message being sent.
- ∞ *Request ID*: It associates the request ID with response.
- ∞ *Error Status*: It indicates the number of errors and their types.
- ∞ *Error Index*: It associates an error with a particular error index.
- ∞ *Variable binding*: Each variable binding associates a particular object instance with its current value.

4.2- SNMP Version 2

It is the improvements of version 1 with some changes and extra feature added. This version provides better administration of network, authentication and privacy. The following are some of the changes made in the version 2:

- ∞ *Data Type Changes*: Bit String data type was added to replace the integers.
- ∞ *Setting Values*: It added the feature that protect the updates and set values.
- ∞ *Authentication and Security*: These features are enhanced in the second version.

4.3- SNMP Version 3

This version was approved by Internet Engineering Steering Group (IESG) as a full internet standard in March, 2002. SNMP version 3 has added security and remote configuration capabilities to the previous version of SNMP. It provides the security to SNMP protocol by adding authentication and encryption. It use advanced mechanism that is the sign of great security level. The architecture of this version introduces two new things.

USM: - User-based Security Model. It used for message security.
VACM: - View-based Access Control Model. It used for access control.

This architecture is very useful to support the concurrent use of security, access control and message processing models.

5- Why SNMP is Important

SNMP is very important for enterprise/large ISP Network Let's suppose that you have a network of 100 machines running various operating systems. Several machines are file servers, Internet server, Web Server and you provide high speed Internet connectivity to the Banking organizations to run their online transaction. In addition, there are various switches and routers that help keep the actual network going. A T1 circuit or Fiber optic link connects the bank to the global Internet Service provider, and there is a private connection to the online transaction Server and web sever of the bank.

What happens when one of the web servers crashes? If it happens in the middle of the workweek, it is likely that the people using it will notice and the appropriate Network Engineer will be called to fix it. But what if it happens after everyone has gone home, including the Engineer

What if the private connection to the online transaction, server verification system goes down at 10 p.m. on Friday and isn't restored until Monday morning? If the problem was faulty Network media or hardware and could have been fixed by replacing a Network media/router, thousands of online transaction and service in web site could have been lost for no reason. Likewise, if the T1 circuit to the Internet goes down, it could adversely affect the online services generated by individuals accessing your web site and using services.

These are obviously serious problems -- problems that can conceivably affect the survival of your business. This is where SNMP comes in. Instead of waiting for someone to notice that something is wrong and locate the person responsible for fixing the problem (which may not happen until Monday morning, if the problem occurs over the weekend), SNMP allows you to monitor your network constantly, even when you're not there. For example, it will notice if the number of bad packets coming through one of your router's interfaces is gradually increasing, suggesting that the router is about to fail. You can arrange to be notified automatically when failure seems imminent, so you can fix the network media before it actually breaks. You can also arrange to be notified if the credit card processor appears to get hung you may even be able to fix it from home. And if nothing goes wrong, you can return to the office on Monday morning knowing there won't be any surprises.

There might not be quite as much glory in fixing problems before they occur, but you and your management will rest more easily. We can't tell you how to translate that into a higher salary sometimes it's better to be the guy who rushes in and fixes things in the middle of a crisis, rather than the guy who makes sure the crisis never occurs. But SNMP does enable you to keep logs that prove your network is running reliably and show when you took action to avert an impending crisis.

References

[1] http://www.cisco.com/en/US/docs/internetworking/technology/handbook/SNMP.html
[2] http://www.dpstele.com/layers/l2/snmp_l2_tut_part1.php
[3] http://www.dpstele.com/layers/l2/snmp_l2_tut_part1.php
[4] http://www.dpstele.com/layers/l2/snmp_l2_tut_part1.php
[5] http://www.dpstele.com/layers/l2/snmp_l2_tut_part2.php
[6] http://www.et.put.poznan.pl/snmp/intro/indexint.html
[7] http://www.cisco.com/en/US/docs/internetworking/technology/handbook/SNMP.html