CHAPTER IV

ADVANTAGES & VERSIONS OF NETWORK MANAGEMENT
4.1. Applying the Concepts of Network Management

Being able to apply the concepts of network management is as important as learning how to use SNMP. This section of the chapter provides insights into some of the issues surrounding network management.

4.1.1. Business Case Requirements

The endeavor of network management involves solving a business problem through an implementation of some sort. A business case is developed to understand the impact of implementing some sort of task or function. It looks at how, for example, network administrators do their day-to-day jobs. The basic idea is to reduce costs and increase effectiveness. If the implementation doesn't save a company any money while providing more effective services, there is almost no need to implement a given solution.

4.1.2. Levels of Activity

Before applying management to a specific service or device, you must understand the four possible levels of activity and decide what is appropriate for that service or device:

Inactive: No monitoring is being done, and, if you did receive an alarm in this area, you would ignore it.

Reactive: No monitoring is being done; you react to a problem if it occurs.

Interactive: You monitor components but must interactively troubleshoot them to eliminate side-effect alarms and isolate a root cause.
Proactive: You monitor components, and the system provides a root-cause alarm for the problem at hand and initiates predefined automatic restoral processes where possible to minimize downtime.

4.1.3. Reporting of Trend Analysis

The ability to monitor a service or system proactively begins with trend analysis and reporting. In general, the goal of trend analysis is to identify when systems, services, or networks are beginning to reach their maximum capacity, with enough lead time to do something about it before it becomes a real problem for end users. For example, you may discover a need to add more memory to your database server or upgrade to a newer version of some application server software that adds a performance boost. Doing so before it becomes a real problem can help your users avoid frustration and possibly keep you employed.

4.1.4. Response Time Reporting

If you are responsible for managing any sort of server (HTTP, SMTP, etc.), you know how frustrating it can be when users come knocking on your door to say that the web server is slow or that surfing the Internet is slow. Response time reporting measures how various aspects of your network (including systems) are performing with respect to responsiveness.

4.1.5. Alarm Correlation

Alarm correlation deals with narrowing down many alerts and events into a single alert or several events that depict the real problem. Another name for this is root-cause analysis. The idea is simple, but it tends to be difficult in practice. For
example, when a web server on your network goes down, and you are managing all devices between you and the server (including the switch the server is on and the router), you may get any number of alerts including ones for the server being down, the switch being down, or the router being down, depending on where the real failure is.

4.1.6. Trouble Resolution

The key to trouble resolution knows that what you are looking at is valuable and can help you resolve the problem. As such, alarms and alerts should aid an operator in resolving the problem. For example, when your router goes down, a cryptic message like "router down" is not helpful. If possible, alerts and alarms should provide the operator with enough detail so that she can effectively troubleshoot and resolve the problem.

4.2 Advantages:

As the name goes, the protocol is quite simple because it is easy to understand and the agent requires only minimal software. It is this simplicity that serves as a key reason for its widespread acceptance, besides being the chief Internet standard for network management. Implementing SNMP management in a networked device is far more straightforward than most other approaches to network management.

Some of the benefits you derive on using SNMP are as follows.

_Standardized protocol_: SNMP is the standard network management protocol for TCP/IP networks. Internet Protocols are open, nonproprietary standards developed through voluntary efforts by the Internet community, so is the SNMP that is actively
maintained and all future enhancements to SNMP are based on existing protocol standards.

*Universal acceptance:* All major vendors support SNMP. All SNMP-managed devices use the same type of management interface to support a common set of network management information.

*Portability:* SNMP is independent of operating system and programming language. The functional design of SNMP is also portable and it defines a core set of operations that must function identically in all devices that support SNMP.

*Lightweight:* SNMP facilitates the addition of management capability to a device without impacting the operation of the device or its performance. SNMP management may be added to a network device with very little increase in workload and demand on system resources.

*Extendibility:* SNMP is a core set of operations that remain the same on all managed devices. SNMP has the capability of supporting any type of information on any type of device that may be part of any type of computer network.

*Widely deployed:* SNMP is one of the most popular protocols in the protocol suite that every vendor is aware of. This popularity serves as one dominant factor for its wide deployment by the vendors.

### 4.3. SNMP Versions:

There are Three versions of SNMP, there are key differences between the three versions of them. While SNMPv1 worked well there were some serious shortcomings with it. Notably there was little to no security with it. All messages were
sent in plain text across the wire, and could be read by any one with a packet sniffer installed on the network. This is not a good a good thing for obvious reasons. So along came SNMPv2, which attempted to correct some of the failings of its predecessor. SNMPv2 contained changes to MIB definitions, also the PDU saw changes, and lastly improved security. The improved security came in the form of data integrity. Lastly there was some form of protection to reply attacks due to the use of authentication procedures.

Just in case SNMPv2 was not confusing enough, you should know that, in reality, there is actually four variants of it. They are as follows; SNMPv2c which is a community based, SNMPv2* or also known as "star" for meta I assume, SNMPv2u that was user based, and the original SNMPv2. The complexity introduced with SNMPv2 is one of the main reasons that it was not widely adopted by the community at large. Complexity does not make for usability.

With continuing security issues in SNMPv1 and v2, plus the complexity issues of SNMPv2 it was decided a new version needed to address these shortcomings. This resulted in SNMPv3, which took into account its predecessors shortcomings. Far better security came in the form of authentication via hashing, timestamps, and message confidentiality due the use of encryption. This version also less complex than the SNMPv2 variants, and far superior in terms of security than version one. In spite of this, as mentioned above, many networks still use SNMPv1, with all shortcomings.