
The Concept of Network Management

SNMP is really about network management. Network management is a discipline of its own, but before learning about the details of SNMP in Chapter 2, it's helpful to have an overview of network management itself.

What is network management? Network management is a general concept that employs the use of various tools, techniques, and systems to aid human beings in managing various devices, systems, or networks. Let's take SNMP out of the picture right now and look at a model for network management called *FCAPS*, or Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Management. These conceptual areas were created by the International Organization for Standardization (ISO) to aid in the understanding of the major functions of network management systems. Let's briefly look at each of these now.

Fault Management

The goal of fault management is to detect, log, and notify users of systems or networks of problems. In many environments, downtime of any kind is not acceptable.

Fault management dictates that these steps for fault resolution be followed:

1. Isolate the problem by using tools to determine symptoms.
2. Resolve the problem.
3. Record the process that was used to detect and resolve the problem.

While step 3 is important, it is often not used. Neglecting step 3 has the unwanted effect of causing new engineers to follow steps 1 and 2 in the dark when they could have consulted a database of troubleshooting tips.

Configuration Management

The goal of configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

Any system may have a number of interesting and pertinent configuration parameters that engineers may be interested in capturing, including:

- Version of operating system, firmware, etc.
- Number of network interfaces and speeds, etc.
- Number of hard disks
- Number of CPUs
- Amount of RAM

This information generally is stored in a database of some kind. As configuration parameters change for systems, this database is updated. An added benefit to having this data store is that it can aid in problem resolution.

Accounting Management

The goal of accounting management is to ensure that computing and network resources are used fairly by all groups or individuals who access them. Through this form of regulation, network problems can be minimized since resources are divided based on capacities.

Performance Management

The goal of performance management is to measure and report on various aspects of network or system performance.

Let's look at the steps involved in performance management:

1. Performance data is gathered.
2. Baseline levels are established based on analysis of the data gathered.
3. Performance thresholds are established. When these thresholds are exceeded, it is indicative of a problem that requires attention.

One example of performance management is service monitoring. For example, an Internet service provider (ISP) may be interested in monitoring its email service response time. This includes sending emails via SMTP and getting email via POP3. See Chapter 11 for examples of how to do this.

Security Management

The goal of security management is twofold. First, we wish to control access to some resource, such as a network and its hosts. Second, we wish to help detect and prevent

attacks that can compromise networks and hosts. Attacks against networks and hosts can lead to denial of service and, even worse, allow hackers to gain access to vital systems that contain accounting, payroll, and source code data.

Security management encompasses not only network security systems but also physical security. Physical security includes card access and video surveillance systems. The goal here is to ensure that only authorized individuals have physical access to vulnerable systems.

Today, network security management is accomplished through the use of various tools and systems designed specifically for this purpose. These include:

- Firewalls
- Intrusion Detection Systems (IDSs)
- Intrusion Prevention Systems (IPSs)
- Antivirus systems
- Policy management and enforcement systems

Most if not all of today's network security systems can integrate with network management systems via SNMP.