Module 6

This is a single, concatenated file, suitable for printing or saving as a PDF for offline viewing. Please note that some animations or images may not work.

Module 6 Study Guide and Deliverables

Readings:	• Online lecture material plus the following chapters from the textbook: ◦ Chapter 12 - Network Management
Assignments:	• Concepts Assignment 6 and Lab 6 due **Wednesday, October 18 at 6:00 AM ET**
Assessments:	• Quiz 6 due **Wednesday, October 18 at 6:00 AM ET**
Course Evaluation:	Course Evaluation opens on Tuesday, October 10, at 10:00 AM ET and closes on Tuesday, October 17, at 11:59 PM ET. Please complete the course evaluation. Your feedback is important to MET, as it helps us make improvements to the program and the course for future students.
Live Classroom:	• **Saturday, October 14 from 11:00 AM–1:00 PM ET**

Network Management

Network Management

Introduction

A network is of no use to a business if it can't be managed. New users must be registered, equipment failures detected and repaired, network congestion avoided, service levels maintained, growth and changes planned for,

etc. In this chapter, we will consider the problem of network management, its organization, and the business forces that influence it.

Objectives

- Understand the fundamentals of network management
- Understand that management is about monitoring and repairing, not controlling
- Understand the SNMP, its capabilities, and its limitations

The Basics of Network Management

While network management is critically important to a network, it is the area in which the least advancement has been made. Let us consider what network management is all about, and then we will consider why it has lagged so much. First, it is about just what its name suggests: management, not control.

Network management can be summarized as "monitor and repair, not control." Events and conditions change in a network far too fast to put a human in the loop. The actions of a human operator can often make matters worse. So, it is very much a case of *managing* rather than controlling.

In a presentation to a well-known cellular manufacturer some years ago, I made the above claim, and several of the senior engineers insisted, "No!" *They* controlled *their* networks! A young engineer in the back of the room who had supported a nation-wide network in Europe for a few years spoke up and said that I might have a point. He proceeded to tell the story of an incident when engineers noticed that the number of switch crashes had dropped off precipitously for about six weeks and then come back to normal levels. They were quite puzzled. They hadn't made any configuration changes, installed any new software, or done anything that could account for the drop-off. Finally, someone realized that it coincided with the six weeks that the operators had been on strike. The operators had been trying to control the network. Human reaction times were too slow, and the operators ended up working at cross-purposes with what the network was doing.

Test Yourself 6.1

Network management consists of monitoring the operation of a network and repairing its defects rather than controlling the network.

True

This is correct.

False

This is incorrect.

This is true. Network management can be summarized as “monitor and repair, not control.”

Test Yourself 6.2

All events and conditions that occur in a network can be controlled by a network engineer, provided that he or she has advanced skills in networking technologies.

True

This is incorrect.

False

This is correct.

This is false. Networks are usually characterized by events and conditions that change too fast for the network engineer to react.

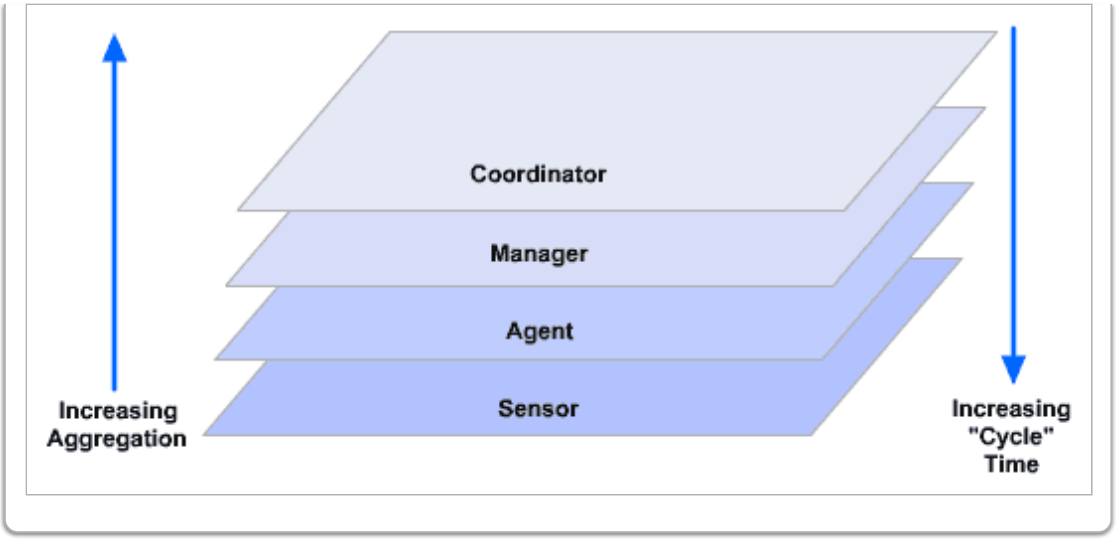
Four Levels of Network Management

Network management can be viewed as occurring at the following four levels, starting with the lowest:

Sensor Level—Within the elements of the network, the equipment is keeping track of various parameters. This data is collected, and parameters may be modified to change the device's configuration. This is where events will happen the fastest.

Agent Level—Within each device is a management agent, which collects sensor information and aggregates it for use by the management system. The agent also moderates the setting of parameters within the device and sends unsolicited events indicating important information. Interactions happen less frequently at this level than at the sensor level.

Network-Management Levels



Manager Level—The manager level integrates the information collected at the agent level, organizes it, and presents it to operators so that they can observe network operations. This level is responsible for the hour-by-hour, day-in, day-out operation of the network. The primary functions of the manager can be organized into event management, configuration management, performance monitoring, trouble ticketing, operational response, and fault management, which is largely separate.

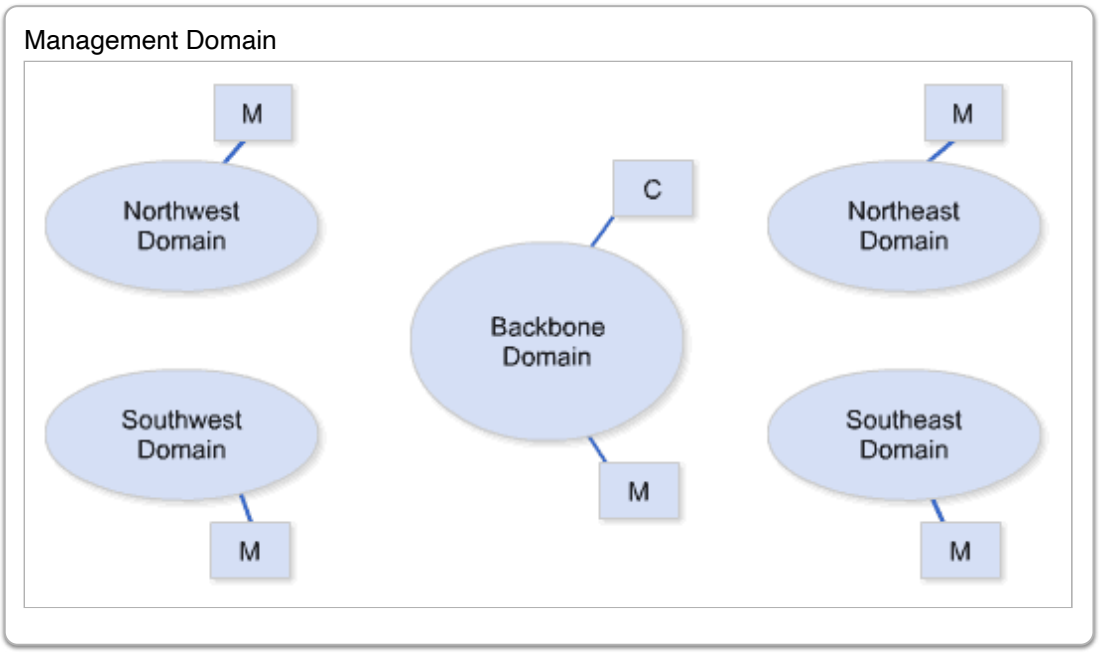
Admin and Planning Coordinator Level—The top level consists of various long-term management and planning functions, as well as administrative functions, such as accounting management and inventory management. This level is responsible for the month-by-month management of the network.

As you move up through the levels, the aggregation of data increases, and the rate of change, or "cycle time," decreases. This means that we want to locate more computation-intensive functions at higher levels. Referring back to Chapter 1, this structure is carefully keyed to managing uncertainty. Fast-changing events are managed by flow control and routing protocols at the lowest levels, close to where the events are happening. At higher levels, the aggregation of information insulates us from this fast-changing information to give us information that we can build on to manage the network.

One would not be wrong to see an analogy between this structure and that of a nervous system. The sensors are the peripheral nervous system. The agents are the ganglia, spinal cord, or hypothalamus; the manager is the cerebrum; and the admin and planning coordinator is the cerebellum. Routing corresponds to the autonomic nervous system. This is the architecture we first arrived at in 1984.

As one may guess, implicit in this description is a concept of a management domain: the set of all network elements managed by a given manager. One can easily imagine a large corporate or provider network having multiple management domains for different parts of the country, different countries, different large installations, etc. This has been a somewhat controversial concept. Some vendors have talked about hierarchies of managers. One must be careful. While we may arrange networks into hierarchies of backbone, region, campus, etc., if one thinks carefully about the problem, one realizes that the managers for these subnets are all peers. They collaborate to manage their subnets and the network as a whole. Considering these that management systems are manned, one would not want a higher-level manager managing through a lower-level system. There is a need

for a function at the admin and planning level that looks for cross-domain trends, or failures in one domain that may impact other domains, and then coordinates a response. But this is as much hierarchy as is required. One must be very careful that the actions taken to rectify any cross-domain conditions do not work counter to what the managers of domains are doing. There may be a hierarchy in the management of personnel, but not that of the network.



Test Yourself 6.3

The sensor level, which is the lowest level of network management, is concerned with the collection of data by network devices that use that data to modify their configurations.

True

This is correct.

False

This is incorrect.

This is true. Network management begins at the sensor level, which is the lowest of all four levels of network management; this is where the network equipment collects data and keeps track of various parameters with the goal of modifying device configurations.

Test Yourself 6.4

The agent level of network management collects sensor data and aggregates it for later use by the manager level of network management.

True

This is correct.

False

This is incorrect.

This is true. The agent level collects sensor data and aggregates it for use by the manager level.

Test Yourself 6.5

The manager level of network management is responsible for long-term, month-by-month management and planning functions.

True

This is incorrect.

False

This is correct.

This is false. The manager level is responsible for operating the network hour-by-hour, day-in, day-out, by integrating the information collected at the agent level, organizing it, and presenting it to the operators so that they can observe the network operations.

Test Yourself 6.6

The sensor level needs the most computation-intensive functions of all four levels of network management because it handles the greatest amount of data.

True

This is incorrect.

False

This is correct.

This is false. The aggregation of data increases as one moves up through the network-management levels, which means that the levels above the sensor level require more computation-intensive functions.

Test Yourself 6.7

Even though a network can be arranged into a hierarchy of network domains, the managers of different domains should be regarded as peers who collaborate to manage their respective domains and the network as a whole.

True

This is correct.

False

This is incorrect.

This is true. The managers of different domains of a network should be regarded as peers whose goal is to collaborate to manage their respective domains and the network as a whole.

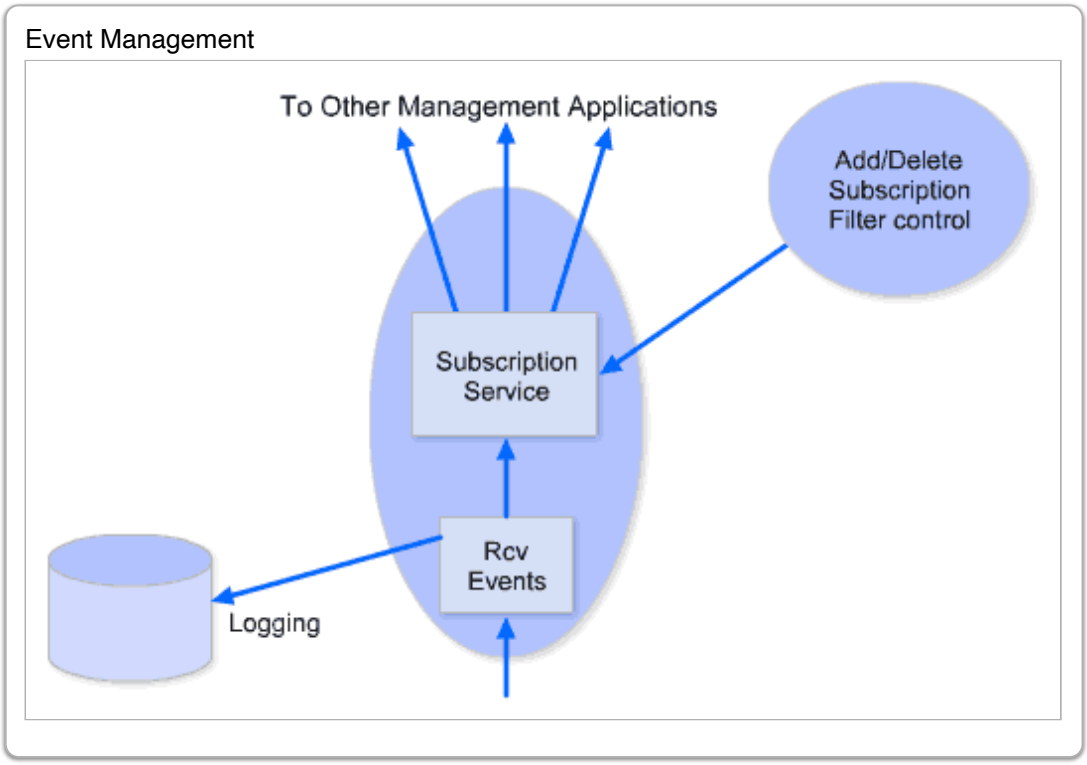
Management Systems

Should elements of a network only communicate with one management system? More or less. Only one management system should be able to modify parameters and configurations—i.e., only one should have write access. On the other hand, it is often useful to allow management systems to have direct read access to at least some of the device's parameters on the other side of the domain boundary. If the management system should then need to modify parameters on such a device (which is likely to be connecting to equipment in this manager's domain), then it should either request the device's management system to make the change or have the element moved to its domain.

Also, managers may act as backup for other managers in the event that they fail or are partitioned from part of their domain, or alternate managers may take over responsibility for a domain during off hours. Measures can be taken for managers to continually update their backups, so that a manager can quickly assume responsibility if a failure takes out part of the normal management system. (Note: This would also include a network partition—that is, a failure such that the network was partitioned into multiple, noncommunicating subnets. During a network partition, a device on one side of the partition would assume that all of the devices on the other side of the partition had crashed. Only once the partition had been repaired would the device be able to establish whether or not that was the case.)

The heart of any manager is event management. This is the one piece that everyone seems to build. Its purpose is to collect the unsolicited events coming in from the devices in the network and then to filter, correlate, and log them and pass them off to other manager applications that have subscribed to them. The event stream is basically how the manager listens to the network. Some management systems refer to these as alarms. It is important to distinguish events (uninterpreted data) from alarms (interpretations). It is also important not to make this distinction too early. For example, an event may be deemed unimportant at the agent level and not forwarded; but if the same event were forwarded to the manager and correlated with other events, it might indicate a major problem. On the other hand, forwarding everything can create a considerable load on the network. This is one of the trade-offs that must be handled carefully. Events from different devices may all indicate the same cause, or they may indicate a condition that the manager has already seen. Filtering and

correlation do the interpreting and presents alarms of varying degrees to the operators. But filtering and distinguishing whether events have the same cause can be very subtle matters.



A Real-World Example

Some years ago, on a summer weekend, there was a line of thunderstorms moving across Iowa and Illinois—not an uncommon occurrence. As the storms moved east, the network operators for AT&T were watching central offices experience power failures and come back up as they switched to batteries or the power came back on. So, the operators weren't too concerned when they saw the massive Hinsdale facility, a major hub for transcontinental and Chicago-area phone service, register a power failure. When it didn't come back up as expected, they became concerned. It was an unmanned facility on weekends, so it took some time for a local technician to be dispatched to the facility. When the tech opened the door, he found the place almost fully engulfed in a fire that had nothing to do with the thunderstorms. The station was so overwhelmed by the fire, in fact, that the tech had to drive to a gas station some distance away to find a phone to call the fire department. Phone service between the FAA's Aurora approach control and O'Hare Airport and many other critical connections were knocked out, as was much of the phone service in the western suburbs of Chicago. The operators had filtered alarms that they shouldn't have. (Also, the Hinsdale facility was woefully lacking in sensors to detect the fire, especially for such a critical resource.) The devastation was so extensive that there was a shortage of equipment in the system for most of a year while deployments were delayed so that Hinsdale could be rebuilt.

Test Yourself 6.8

A network may be characterized by multiple management systems, of which only one should be able to modify device parameters and configurations.

True

This is correct.

False

This is incorrect.

This is true. Only one management system should be able to modify device parameters and configurations, but it is often useful to allow additional management systems to have direct read access to at least some of the device parameters and configurations.

Test Yourself 6.9

A manager who manages a certain domain of a network should never allow managers responsible for other domains to act as his or her backup if that domain experiences network issues.

True

This is incorrect.

False

This is correct.

This is false. A manager who manages one domain may act as a backup for a manager who manages another domain in case the latter domain experiences network issues.

Test Yourself 6.10

The purpose of event management is to collect unsolicited events coming in from network devices and then to filter, correlate, and log them and finally pass them off to other manager applications that have subscribed to them.

True

This is correct.

False

This is incorrect.

This is true. The purpose of event management is to collect unsolicited events coming in from network devices and then to filter, correlate, and log them and finally pass them off to other manager applications that have subscribed to them.

Test Yourself 6.11

The filtering of events in a network should be performed carefully because sometimes an event that is deemed unimportant may indicate a major problem in the network.

True

This is correct.

False

This is incorrect.

This is true. An event that is deemed unimportant may indicate a major problem in the network, so the filtering of events in a network should be performed carefully.

Configuration Management

Configuration management (CM) is a function that is rarely done. Later, we will discuss why. While there is a great deal of detail to CM, it is a relatively straightforward task. Its purpose is to aid in the creation of new configurations and in their deployment. Deploying a new configuration is not just a matter of sending it out to all of the network elements and telling them to do it. The order in which configurations are deployed can be quite important. For example, if you are deploying a new configuration that is incompatible with some parts of the existing configuration, it is important to start making changes as far from the manager as possible and work your way back toward the manager, so that the manager can maintain contact with the unchanged parts of the network.

Many network-operations departments find that the conditions in the operation of their businesses that warrant changes in management policy occur at different, but often regular, times. For example, changes may need to be made during the day or at night, at the end of the month, or for special events, such as the Super Bowl, Mother's Day, or, if you are in Hong Kong, Race Day. Alternate configurations can be stored as trees. Then, deploying a configuration is merely a matter of traversing the tree according to an ordering imposed on the nodes of the tree.

Test Yourself 6.12

The purpose of configuration management is to aid in the creation of new configurations and in their deployment.

True

This is correct.

False

This is incorrect.

This is true. The purpose of configuration management is to aid in the creation of new configurations and in their deployment.

Test Yourself 6.13

The deployment of several new configurations in a network can be always performed in an arbitrary order.

True

This is incorrect.

False

This is correct.

This is false. The order in which configurations are deployed is important (e.g., in case a new configuration is incompatible with some parts of an existing configuration).

Performance Management

Performance management should be mostly a monitoring function. Any modifications to improve performance must be carefully made by effecting changes to the automatic processes in the network. Direct intervention can lead to the same results as in our story of the striking operators. Performance management is not concerned with responding to congestion and other performance problems occurring in a network. Those problems will be handled, in due course, by the automatic feedback processes of congestion control and routing. Performance management is concerned with changes in traffic patterns that may require adjustments in the policies for automatic processes. Again, we are managing uncertainty.

Test Yourself 6.14

Performance management is concerned with changes in the traffic patterns in a network that, in turn, may require adjustments in the *policies* that govern the network's automatic processes.

True

This is correct.

False

This is incorrect.

This is true. Performance management is concerned with changes in the traffic patterns in a network that, in turn, may require adjustments in the *policies* that govern the network's automatic processes.

Test Yourself 6.15

Network congestion and other performance problems that may occur in a network are most adequately handled through performance management.

True

This is incorrect.

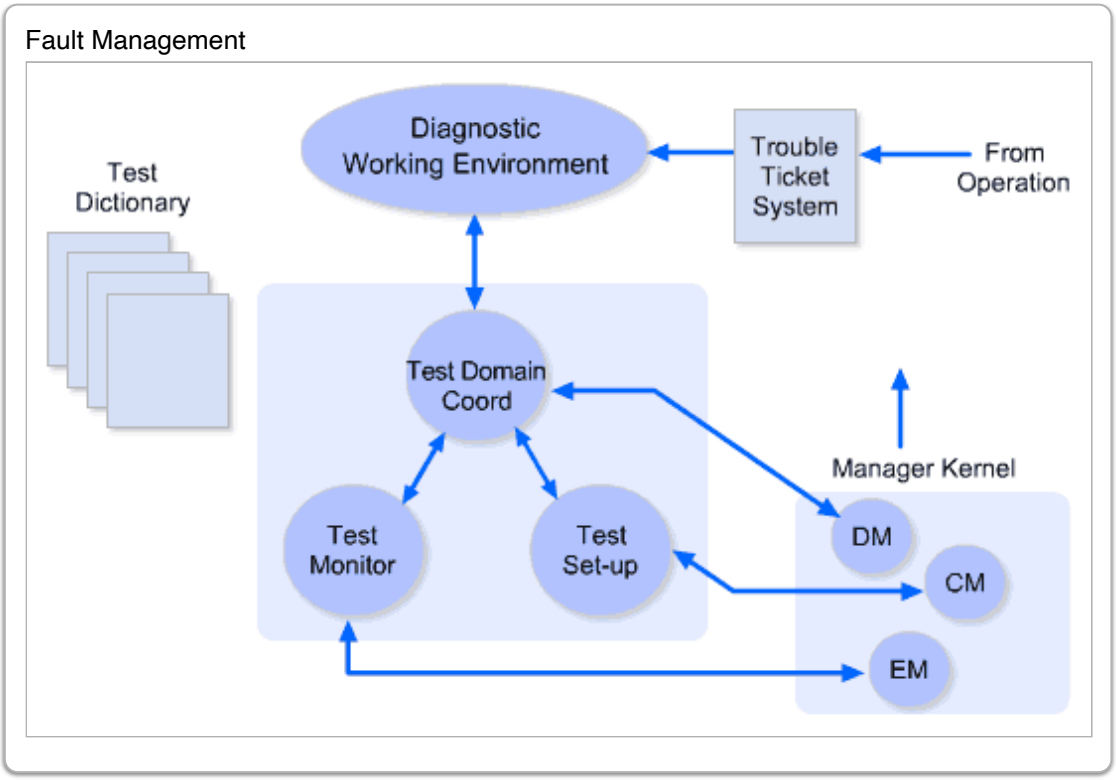
False

This is correct.

This is false. The goal of performance management is not to handle network congestion and other performance problems that may occur in a network; these network problems are handled, in due course, by automatic feedback processes (e.g., congestion control and routing).

Fault Management

We noted above that fault management is largely separate. There are two parts to fault management: operational response and fault management. We know that, in a packet-switched network like the internet, if a line or router goes down, the network will automatically route around the failure. It is only with a circuit-switched technology like MPLS that an equipment failure may require human intervention, but even this is quickly disappearing. When a failure occurs, it may well be outside the parameters that the network can deal with. It is then necessary for the operators to jury-rig a fix. A trouble ticket is created that documents the jury-rigging actions of the operators. Or, it may simply be a case in which the operators notice abnormal behavior in the network and create a trouble ticket to document the conditions, so that someone may investigate it in more detail. The operators do not try to resolve the problem. Their responsibility is to monitor the network and provide a first-level response to problems in order to maintain the stability and service level of the network to the greatest degree possible.



Most management systems use a trouble-ticket system to track and schedule problem resolution. The trouble ticket is handed off to a fault manager to diagnosis and repair. The trouble-ticket system is the job-shop scheduler for fault management.

Fault management is then charged with delving into the failure (or problem) in detail, which will probably require a number of tests to determine what repairs are necessary, and then making these repairs. With network equipment, it is often possible to do a large amount of this testing, analysis, and even the repair remotely. To run tests on a device, the tester must have access to the device. A careful consideration of this process will lead one to realize that fault management is a management system whose management domain is the equipment being tested and any other elements used in the test. The device to be tested is simply assigned to a fault management domain for the duration of the testing. Note that this does not necessarily require the device to be taken offline. It may be very important to the tester to perform the test *in vivo,* as it were.

Test Yourself 6.16

The goal of the operational response, as part of fault management, is always to *resolve* the problems that occur in a network.

True

This is incorrect.

False

This is correct.

This is false. Operational response is a first-level *response* to the problems that occur in a network, to maintain the stability and service level of the network to the greatest degree possible; it does not try to resolve the problems.

Test Yourself 6.17

Most management systems use a trouble-ticket system to track the problems that occur in a network and schedule their resolution.

True

This is correct.

False

This is incorrect.

This is true. Most management systems use a trouble-ticket system to track and schedule problem resolution.

Test Yourself 6.18

Once a network problem occurs and a trouble ticket is handed to fault management for resolution, the engineers responsible for fault management first run tests on the problematic device to determine what repairs may be necessary. They then make the required repairs.

True

This is correct.

False

This is incorrect.

This is true. Fault management consists of delving into the failure (or problem) in detail, which may require a number of tests on the problematic device itself to determine what repairs may be necessary, and then proceeding with the identified repairs.

Management Protocols

Sensors feed information to agents within the same system. Agents in network devices feed information to management systems. For this process, we need a management protocol. Starting in the mid-1980s,

considerable work was devoted to developing management protocols. Clearly, they had to be relatively efficient, and they could not use many resources. The devices in which the agents resided were relatively resource constrained. The earliest standard management protocol was the IEEE 802.1 protocol. This was a simple, connectionless protocol operating over LLC or the MAC protocol. The operations consisted of a simple set and get and an unsolicited event. This work was introduced into OSI and led to the development of the object-oriented Common Management Information Protocol (CMIP), starting in 1985. In the IETF, work began a bit later. There were two proposed protocols: an innovative, object-oriented protocol called HEMS (High-Level Entity Management System), which was extensible based on a postscript-like model, and the much "simpler" SNMP (Simple Network Management Protocol), which was not object oriented. In the end, SNMP was chosen. All of these except the early IEEE 802 protocol used ASN.1 (Abstract Syntax Notation One) for encoding. ASN.1 was a rich and complex data structure–definition language that could describe just about any data structure a device might have.

SNMP

SNMP follows the guidelines of most other network-management protocols in that it consists of a simple set/get model along with an asynchronous trap. Early SNMP used User Datagram Protocol (UDP) for all commands and responses.

Almost immediately after SNMP's introduction, certain router vendors objected that, while SNMP was fine for monitoring, it was too insecure for doing configuration. On the face of it, this was true; there was essentially no security in the first version of SNMP. The use of UDP made security difficult because, without a connection to relate requests and responses, each message had to be secured by itself. However, the current practice for modifying configurations on routers was (and is) to open a Telnet connection and send a password in the clear. Nearly every PC comes with a Telnet program. At least SNMP was encoded in the obscure ASN.1, for which almost no PC had an interpreter. So, in fact, SNMP was more secure than the current practice, although not in a formal sense. But customers and the IETF bought the vendor's argument. And the IETF embarked on what turned out to be a decade-long effort to put better security into SNMP. But long before that came to pass, the world relegated SNMP to monitoring.

Why would a router vendor not want a common management protocol? Any network provider will tell you that they limit the number of vendors they buy routers from to one or two, because the training costs are simply too high to have more. A common network-management protocol for managing all aspects of routers would remove this barrier. The management interface to network equipment is a major source of account control for equipment vendors.

In the late '90s, when the IETF was considering a common command language for management, the same vendor insisted that whatever was proposed should be simple enough to operate on a router. When asked why

on earth such a requirement was necessary, the vendor responded that it was so field engineers could access the routers. Was the vendor was still issuing field engineers dumb terminals instead of PCs? Any PC could run a basic management system. Hardly. Account control is everything.

There are other problems with SNMP, as well. The choice of UDP was based on dogma, not practicalities. (SNMP was proposed at the height of the "the internet is connectionless, everything should be connectionless" lunacy; this is something that none of the internet's original designers believed.) The limited nature of the trap also required that devices be polled. Anyone in the early days of the 'net who had proposed polling would have been dubbed a backward-thinking mainframe person. Polling doesn't scale, as has been discovered with SNMP. For a network of any size, it becomes impossible to poll often enough to be responsive, and polling generates a lot of useless traffic. The only reason one would choose polling for an application is if, most of the times when a device was polled, it had data to send. This was generally true of old terminal systems. However, in network management, for the conditions to be appropriate for polling, one must assume that devices fail most of the time! (If devices fail infrequently, then polling amounts to wasted overhead, and an event generated when the exceptional failure occurs is preferable.)

With the use of UDP, the amount of information that could be retrieved with a get command had to fit in one UDP packet. This meant that, to retrieve the contents of a table, multiple gets had to be sent. However, the table could be changing while this was being done. So, it was essentially impossible to get a consistent view of something like a routing table. This led to the GetBulk operation in SNMPv2, which was still limited and still not object oriented; in addition, the command was cumbersome to use. The command/response flow should have used TCP, and the unsolicited trap should have used UDP. Also, the lack of create/delete commands made configuration difficult. Various workarounds for this were proposed, but they were all cumbersome.

The development of SNMPv2 and SNMPv3 was not the nice, continuous stride toward progress that one might have hoped for. SNMPv2 was announced to the world when its four authors (later known as the "Gang of Four") produced an entire set of new documentation and submitted it to the IETF without any consultation with the people working on SNMPv1. (Being a subset of the authors of v1, they felt they could do as they pleased.) Furthermore, they rather roughly squelched any attempts to modify the original set of documents. Bitter disputes broke out. Flame wars raged (there were hundreds of messages a day on the SNMP list). Sides were chosen. Two or three different SNMPv2 security approaches were worked on. People (including the original authors) were no longer speaking to each other. There was great confusion in the market, and SNMP basically languished. (Note that this fit in with the desires of the vendors, who could simply sit back and watch.)

A point on political dynamics: Given the bottom-up nature of standards committees, any effort by a small group or the chair to dictate direction is virtually guaranteed to fail. The further it is pushed, generally, the more spectacular the blowup. In fact, the outcome of SNMPv2 was predicted by some at the time it was announced. That said, it is possible to engineer the adoption of a proposal, but it must be carefully done. Several techniques have proved effective depending on the circumstances.

SNMPv2 was finally published with several options and a confused user community. After a period, a new consensus developed around a fresh start at SNMP security, and SNMPv3 was produced, which included a mapping to TCP. All of this took the better part of a decade. But this was perfectly fine with the equipment

vendors. They had nice, stable management interfaces that kept their customers trained on their equipment… buying it.

Test Yourself 6.19

The use of UDP as the underlying transport-layer protocol for the first version of SNMP made SNMP's security challenging because, with the absence of a connection necessary to relate requests and responses, each SNMP message had to be secured by itself.

True

This is correct.

False

This is incorrect.

This is true. The first version of SNMP used UDP as the transport-layer protocol. This made SNMP's security challenging because, without a connection to relate requests and responses, each SNMP message had to be secured by itself.

Test Yourself 6.20

Network providers benefit from having a common network-management protocol because it decreases the training costs that would otherwise be spent to acquire knowledge of how to use and manage network equipment from different vendors.

True

This is correct.

False

This is incorrect.

This is true. It is in the interest of network providers to have a common network-management protocol because it decreases the costs of training people to use and manage network equipment from different vendors.

Test Yourself 6.21

One of the disadvantages of the first version of SNMP was the difficulty of obtaining consistent device information (e.g., routing table) while issuing multiple gets to retrieve the complete contents of that device information.

True

This is correct.

False

This is incorrect.

This is true. One of the disadvantages of the first version of SNMP was the difficulty of obtaining consistent device information (e.g., routing table) while issuing multiple gets to retrieve the complete contents of that device information.

Test Yourself 6.22

The development of SNMPv2 was slow because of political disputes that sparked among groups of authors who developed SNMPv1, rather than the difficulty of resolving SNMP's technical challenges.

True

This is correct.

False

This is incorrect.

This is true. The development of SNMPv2 was slow because of political disputes, which in turn caused confusion in the market and made the development of SNMP languish.

Test Yourself 6.23

Equipment vendors lost significant revenue because it took a very long time for standardization bodies to design and adopt SNMP's security.

True

This is incorrect.

False

This is correct.

This is false. Equipment vendors actually benefited from the prolonged time to push the standardization of SNMP's security forward, because this situation kept their customers locked into using their equipment—probably the only equipment the customers were trained to use and manage.

Beyond SNMP

It turned out that SNMP wasn't so simple after all. As we discussed before, there were two other management protocols being proposed at the time: HEMS in the IETF and CMIP in OSI. Both were object oriented (SNMP is not object oriented). HEMS was based on a novel pushdown automata model patterned after postscript, which held out the promise of being extensible. It turned out that implementations of both HEMS and CMIP are smaller than SNMP implementations.

But there is a more difficult problem. The set/get model can almost be too simple; it's a bit like having a Turing machine rather than a computer. Each step requires sending and receiving a command, and each step can be rather small. The object-oriented protocols made it relatively easy to retrieve related information in one command, a bit like sending a query. But doing something for set is much more difficult. This remains an unsolved problem. One would like to send sequences of set commands, but this quickly leads to adding some rudimentary control structure, and it doesn't take much before one has a full-blown scripting language. While there is a solution, it is one that anyone might be somewhat reticent to utilize: a full script-language interpreter on every type of device that might be deployed in a network. A middle ground is hard to find.

In addition to the confusion over protocols, there is the proliferation of MIBs. For the protocol to have something to act on or information to retrieve, a management information base (MIB) for the device must be defined. This generally has a tree-like structure that reflects the component structure of the device. Standards committees, including the IETF, were slow to impose commonality among MIBs for devices at the same layer or using the same protocol, or even across the architecture as a whole. This has led to literally hundreds of MIBs. But without much commonality among them, network management is pushed toward being more like device management. This has not helped in the development of integrated network management. (A reasonable degree of commonality among MIBs is possible and has been built and deployed at least once.)

Twenty-five years ago, network management was primarily a matter of manipulating unorganized lists of parameters. Not much has changed. The promise of integrated management systems was squandered in an ill-conceived push to just get something out there. While what is required is not hard, it is messy and takes time. And no one has been willing to take the time or deal with the messy aspects. Usually, an event monitor and a fancy GUI with a network map that has separate windows for each vendor's specific command interface is called an "integrated" network-management system. The confusion over protocols and the proliferation of MIBs has led network management to become a hodgepodge of tools, many of them homegrown, from different management or equipment vendors. Most networks' management is based more on experience than science and, consequently, is an impediment to the growth and evolution of the network.

Test Yourself 6.24

The HEMS and CMIP management protocols are object-oriented protocols, unlike SNMP, which is not.

True

This is correct.

False

This is incorrect.

This is true. Unlike SNMP, HEMS and CMIP are object-oriented management protocols.

Test Yourself 6.25

Implementing the set command in the set/get model is as difficult as implementing the get command.

True

This is incorrect.

False

This is correct.

This is false. Implementing the set command in the set/get model is more difficult than implementing the get command.

Test Yourself 6.26

The management information base (MIB) of a device is a tree-like structure that defines the component structure of the device.

True

This is correct.

False

This is incorrect.

This is true. A MIB of a device is a tree-like structure that defines the component structure of the device.

Test Yourself 6.27

The reason for the existence of so many management information bases (MIBs) is that standard committees were slow to impose commonality among MIBs for devices at the same layer or using the same protocol.

True

This is correct.

False

This is incorrect.

This is true. MIBs have proliferated because standard committees were slow to define common attributes among MIBs for devices at the same layer or using the same protocol.

Test Yourself 6.28

Network engineers and managers have at their disposal a wide choice of network-management protocols and management information bases (MIBs), a situation that helps them achieve an integrated network-management system.

True

This is incorrect.

False

This is correct.

This is false. The existence of various network-management protocols and MIBs actually hinders efforts to achieve an integrated network management system.

More Network Management

Here's another interesting point about network management. Over the years, there have been occasions to look at the management problems of large, automated networks other than those of computers and communication equipment. Both surprisingly and not surprisingly, one finds that the fundamental structures are very similar, whether communications networks, electric grids, pipelines, or others are involved. The primary difference is in how fast events can occur. The details of the object models are different, but most other aspects are similar. So, it is very likely that the same system can be used for all of them, even many of the same MIBs.

To effectively manage large networks, a small number of characteristics need to hold:

1. Scalability
2. Repeatability
3. Orthogonality
4. Following from these three, commonality

If the procedures that must be performed on the network are all special cases requiring the individual manipulation of thousands, if not millions, of elements; if operations are likely to produce unforeseen interactions; if the elements to be managed must be individually configured or manipulated; if the computations needed for effective decisions can grow exponentially; then the network may be impossible to manage effectively, will require

more and more highly trained personnel, may be difficult to recover in a crisis, and may even exhibit unpredictable behavior under what appear to be "normal" conditions. If the people managing the network fail to solve or avoid these problems, then the enterprise will be required to significantly restrict the operating range of the network, or to limit itself to a small number of vendors. These factors will raise its costs of operation, block access to innovations, and potentially compromise its security (e.g., through monoculture) and its ability to react in an emergency. The more one looks at how to avoid these problems and pushes to find the root cause of what makes this hard, the more one understands that the answer lies with greater degrees of scalability, repeatability, orthogonality, and, above all, commonality.

Because network management is about managing the whole network (to state the obvious), the root cause of many of network management's problems may be found elsewhere: in the overall architecture, in the protocols of the networking layers (i.e., transport and below), and in the autonomic management systems of the network (i.e., routing and resource allocation). Management can only be as good as the limitations of what it has to manage. To a large degree, the effectiveness of network management will only come when these characteristics are extended to the protocols and devices being managed.

Test Yourself 6.29

The fundamentals of managing large, automated networks are similar irrespective of whether the networks are composed of communication equipment, electric grids, or pipelines.

True

This is correct.

False

This is incorrect.

This is true. The fundamentals of managing large, automated networks are similar irrespective of whether the networks are composed of communication equipment, electric grids, or pipelines.

Test Yourself 6.30

The root cause of many network-management problems may be related to the network’s overall architecture, the protocols used at the layers below the transport layer, and the automatic management functions, such as routing and resource allocation.

True

This is correct.

False

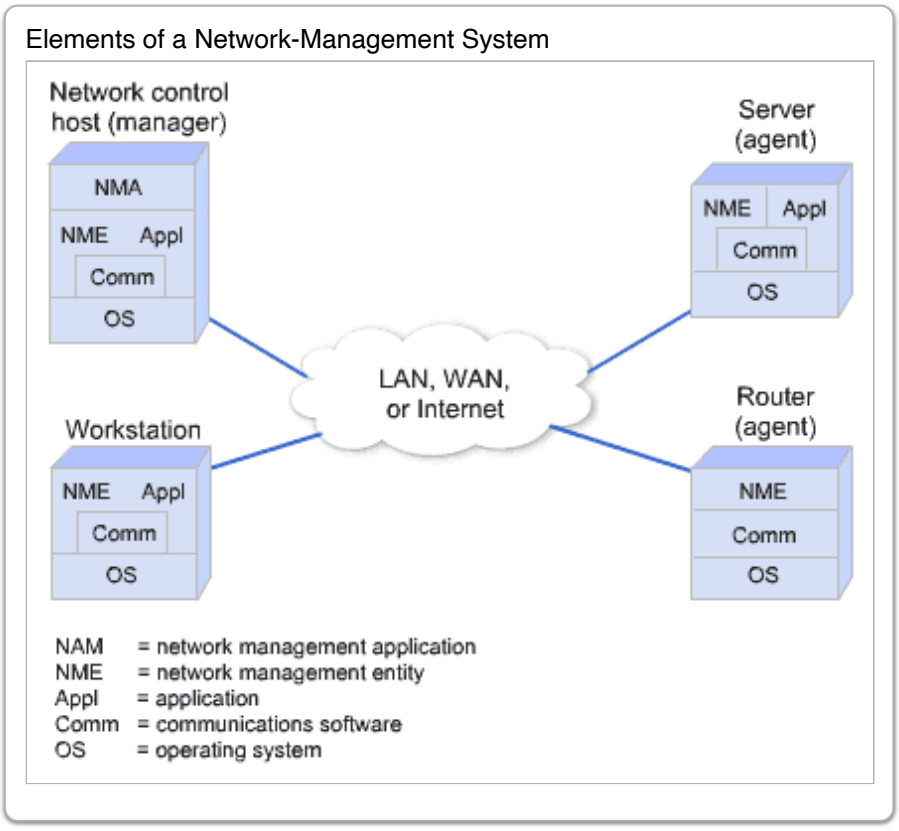
This is incorrect.

This is true. The root cause of many network-management problems may be related to the network's overall architecture, the protocols used at the layers below the transport layer, and the automatic management functions, such as routing and resource allocation.

Network-Management Systems (NMS)

A network-management system (NMS) is a combination of hardware and software used to monitor and administer a network. It's designed to view the entire network as a unified architecture, with addresses, labels, and specific attributes assigned to each network element.

Each individual element in a network contains software devoted to management tasks, called the network-management entity (NME). The NME could be a router, switch, hub, etc. The NMEs are all managed by a host called the network-management application (NMA). Each NME monitors, configures, and collects statistics on its own network element and communicates with the NMA of the network control host.



Test Yourself 6.31

A network-management system (NMS) is a combination of hardware and software used to monitor and administer a network.

True

This is correct.

False

This is incorrect.

This is true. A network-management system (NMS) is a combination of hardware and software used to monitor and administer a network.

Test Yourself 6.32

The network-management entity (NME) is a hardware component that is devoted to network-management tasks.

True

This is incorrect.

False

This is correct.

This is false. The NME is indeed responsible for network-management tasks, but it is actually software that is contained in each individual network element, not hardware.

Test Yourself 6.33

A network-management application (NMA) is a host in a network that manages network-management entities (NMEs).

True

This is correct.

False

This is incorrect.

This is true. A network-management application (NMA) is a host in a network that manages network-management entities (NMEs).

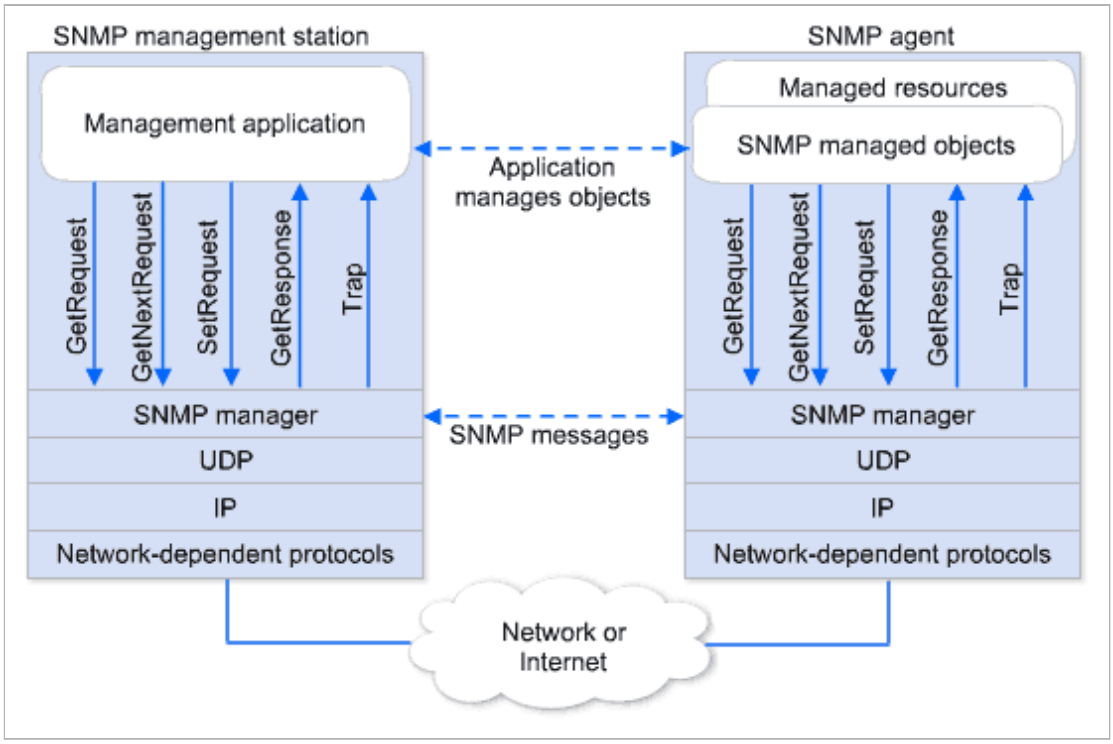
SNMP Standard

The IETF has developed a SNMP standard as a network-management system in the TCP/IP environment. SNMP relies on UDP (ports 161 and 162). It's the dominant management system, though web-based network-management systems have shown a growing market share.

SNMP major elements include the following:

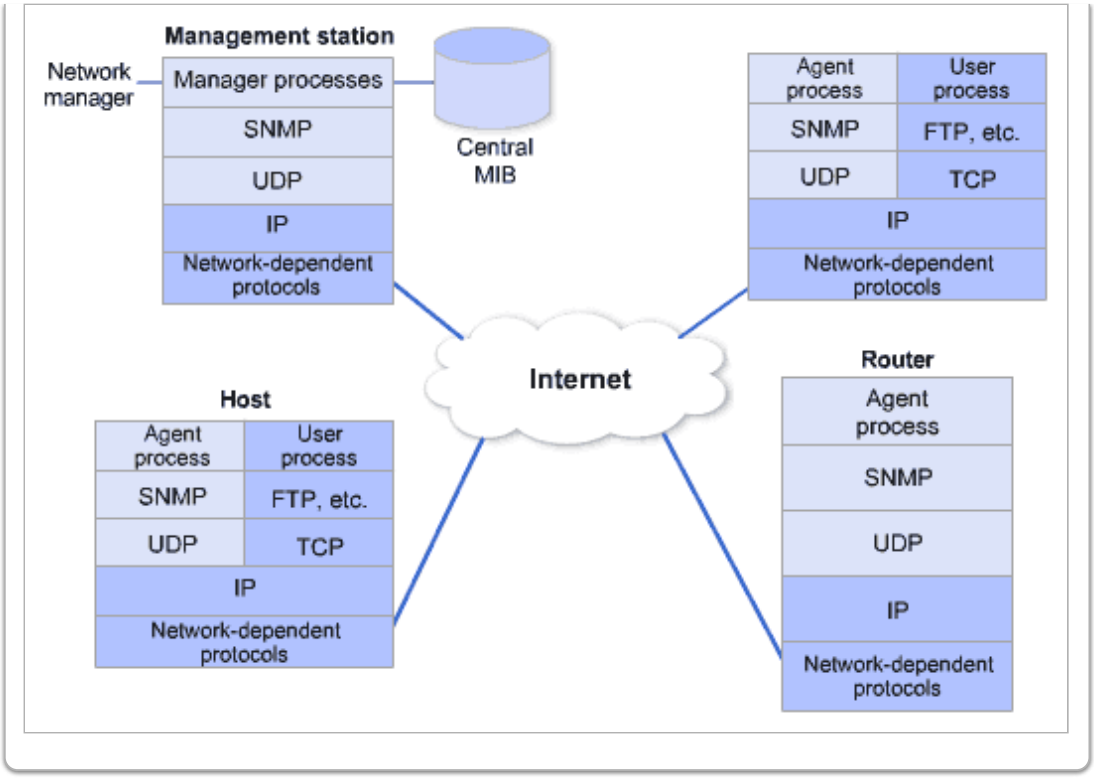
- Management station or manager (Equivalent to NMA)
- Agent (equivalent to NME)
- Management information base (MIB database)
- Network management protocol

The Role of SNMPv1



SNMPv2 was developed in 1998 to address the functional deficiencies and lack of security in SNMPv1. SNMPV2 mainly added new packet and data types. SMMPv3 was developed mainly to correct the continued lack of security in SNMPv2. It provides three main services: authentication, privacy, and control access.

SNMPv1 Configuration



Test Yourself 6.34

The four major elements of the SNMP standard are the management station, agent, management information base (MIB), and network-management protocol.

True

This is correct.

False

This is incorrect.

This is true. The SNMP standard has four major elements: the management station, agent, management information base (MIB), and network-management protocol.

Test Yourself 6.35

The management station of the SNMP standard is equivalent to a network-management entity (NME).

True

This is incorrect.

False

This is correct.

This is false. The management station of the SNMP standard is equivalent to a network management-application (NMA).

Test Yourself 6.36

Aside from addressing the functional deficiencies and lack of security in SNMPv1, the development of SNMPv2 added new packet and data types.

True

This is correct.

False

This is incorrect.

This is true. Aside from addressing the functional deficiencies and lack of security in SNMPv1, the development of SNMPv2 added new packet and data types.