CHAPTER

15

Network Management

I believe in having each device secured and monitoring each device, rather than just monitoring holistically on the network, and then responding in short enough time for damage control.

— Kevin Mitnick[1]

Network management is a very broad term. It is not a single aspect unto itself but encompasses the entire network operations arena, from the mundane to the cutting edge of network technological advances. It is all-inclusive, from ordering pencils for the network operations staff to buying the latest and greatest piece of networking hardware. In other words, it deals with everything required for the daily operation of the network. It includes the ability to ensure that the network runs smoothly and that the base of network users is content. Remember, there is a direct correlation between the number of calls into the network operations help desk and how well the network is designed, deployed, and maintained. In a perfectly managed network, the help desk telephones simply collect dust. Of course, this is more fantasy than reality, but the idea is to keep the call volume down as much as possible.

The opening quote for this chapter highlights that size of the network does have a bearing on its management. A small office may have a single person who manages everything about the network, so perhaps he or she can have an opportunity to use a holistic approach to network management. However, very large corporate networks have a whole hierarchy of staff, possibly including even a vice president of IT who oversees the entire network operations. The number of network node devices also affects how many

[1]Kevin Mitnick is the author of the book *The Art of Deception*, a convicted computer cracker, and currently a computer security consultant.

POP QUIZ

Think about a network you are familiar with. It may be any network — home, work, school, organization, etc. How would you rate their user to support staff ratio? Give reasons why.

support staff are required to maintain the network. Large corporations with networks spread over geographically distant locales may require staffing that appears redundant at times. However, such staffing is required because of the sheer size of the networks and the need to mobilize support staff in the shortest amount of time possible. This comes with a cost, so there needs to be a balance between what is ideal and what is practical. Contingency planning can aid in developing required response times and in turn set staffing levels. A totally holistic approach for a very large network is not practical, but cost is always a factor. Each organization has to place a value on its network. Value has to be seen, not implied, and the network staff needs to be aware that many times they are viewed as overhead. A well-managed network can save a company money by minimizing lost productivity; it can also be a driving force in increasing revenues due to speed and availability of resources to increase productivity. Network management is not just a mere casual consideration, it's essential, as it may very well be the foundation on which the modern organization is built.

15.1 Operation

A network operation is the day-to-day operation of network resources. In most instances, the components that make up the network fabric[2] are powered on 24 hours a day, every day of the year, and hopefully are running error-free. Depending on the type of organization, the network it supports will determine whether support staff positions must also be manned on a 24/7 schedule. In an environment where network users (employees) only work a portion of the day, there may not be a need to maintain support staff throughout the 24/7 time period. In these instances, scheduling for support staff should encompass those hours when network users are present. Support staff should be scheduled to arrive before the start of the business day to ensure the network is functional before the network user base starts their workday. Staff members are required to handle end-user calls and respond to these calls if further assistance is required. The main activity of the day-to-day network operation is manning the help desk. Figure 15-1 illustrates a possible network operations help desk implementation.

[2]*Network fabric* refers to cabling and network node devices that forward network traffic, such as routers, switches, and hubs. It does not include endpoints such as PCs and servers not involved in network operation. Servers that provide a network service, such as DNS servers, DHCP servers, print servers, etc., are considered to be part of the overall network fabric.

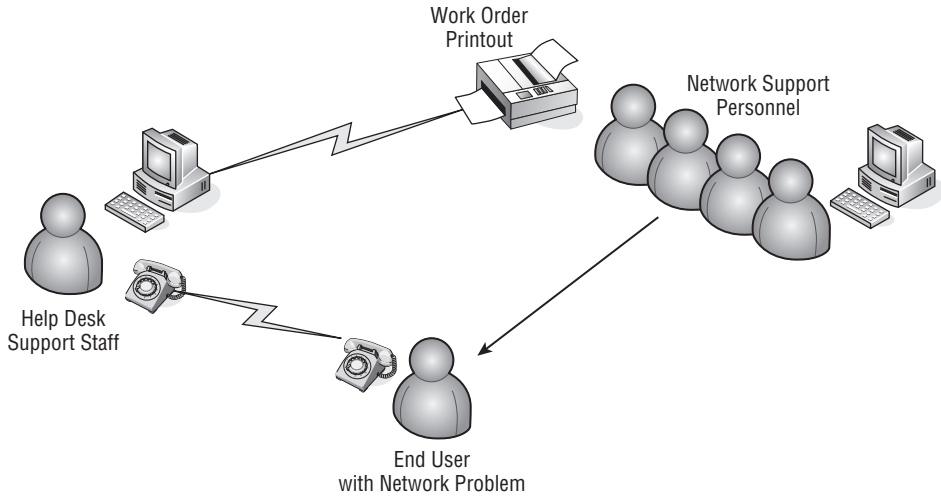


Figure 15-1 A network operations help desk implementation

A successful help desk implementation requires that someone is available to answer the telephone. In small operations, where there is only one person running the whole department, there is still a need to answer the call, no matter where that person may be located. There are a couple of ways this can be done. The first is to have the help desk telephone number be a mobile telephone that is carried at all times. An alternative would be to have a fixed land-line telephone in the network operations area which is the help desk number but is forwarded to a mobile telephone if the phone is not picked up in a certain number of rings. We can already sense the question arising about why bother to have a land-line telephone at all if there is still a mobile telephone in the mix? The answer is that every organization, no matter how small, has aspirations of growing, and with it the network would also need to grow. It would be possible to have the person who is currently heading up the network area eventually add another staff person, even if only on a part-time basis. Then one person can remain in the network operations area while the other is reachable when he or she is out and about in the facility by calling the mobile telephone number. Another possible scenario is that the daytime person is tied to the mobile telephone on a 24-hour basis, with other staff added to maintain and monitor the network during overnight hours. The daytime person should be reachable on an on-call basis.

Larger organizations may have one or more people whose prime responsibility is to answer the help desk telephone calls. This may be a network support person or an operator able to open a service-request ticket for the networking trained staff.

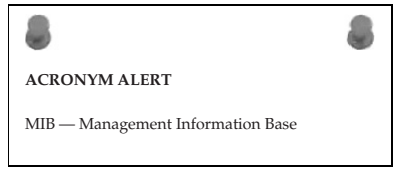
ACRONYM ALERT

VAR — Value-added reseller

In a very large, fast-paced networking organization, the person answering the help desk telephone has the responsibility to triage the call to find out the problem's severity, how the user is affected, the expected response time, and how many other workers in the same area may have been affected. Once all the pertinent information is collected, along with the necessary contact information, a trouble ticket is generated and dispatched to the appropriate network support group for further action.

15.1.1 Help Desk Software

When a call is received, there needs to be some sort of record. Even for a small, low-cost operation, there needs to be at least a spiral-bound notebook designated as the call log. The minimum information includes the date, time, caller, nature of the issue, and whether the issue has been resolved. A step up from the notebook is a spreadsheet that records the same information and perhaps a few more columns for other pertinent information.



The collection of this data is not only used in determining open and closed issues but as a collection of the network's operational history. Recurring issues need to be analyzed to find the root cause and to determine the actions that can be taken to eliminate them. Of course, some software is always better than others. Each has its advantages and disadvantages as far as how it fits into a particular network operations environment. If there is already a help desk or network operations program in use, this may be a situation of living with what you've got. This is especially true if the program has been in use for a long time and is serviceable in that network environment. However, if you are employed in a network environment that has not committed to any particular help desk or network operations program, you can investigate some to integrate into your network support area.

All help desk programs can open a trouble ticket and follow that ticket through to its resolution. The difference in many is in the database area and their capability to search on issues or generate reports to indicate trends or problem areas. Some programs are fairly inexpensive and a good start. However, it is best to investigate the capability for moving stored network-related information in the event there is a need to migrate to a more sophisticated program in the future. You want to be able to migrate the data to the new software system to provide continuity in the network operations area. Avoid programs that use a compressed, proprietary format and do not provide tools to export the data in a readable and sortable format.

Some programs are single-user applications that are loaded on a local PC. This is fine in a one-person department where future growth may not exist. Attempt to find a program that would easily migrate to a multiuser environment. Client/server applications have client and server components; however, they may require a per-seat license for each user using the client application. Normally, these types of licenses are based on simultaneous connections, so you may not need a license for every staff member who needs access to the program. Make sure there is a firm understanding of the license terms prior to committing to the purchase of the program.

The last consideration is the program's user interface. Is it fairly intuitive, requiring little to no training? The idea is to have a help desk program that increases the productivity of the network support staff, not tie them down with the business of just running the help desk program. If a program requires leafing through thick manuals for explanation of various functions, it is perhaps best to look in another direction.

POP QUIZ

List the minimum information that is needed to generate a trouble ticket or work order for network support.

15.1.2 Network Operations Staff

In a small, one-person network operations shop, the person needs to wear many hats. Perhaps the person is fairly knowledgeable about all facets of the network environment, but if the network is sophisticated, certain components may need to be supported via support contracts with either the original equipment manufacturer or some other third party with expertise in that particular piece of hardware or software. In larger installations, there may be an entire staff dedicated to different network aspects.

The tasks performed by help desk personnel may be more of a clerical function in a large, high call volume network environment. It would be the responsibility of these staff members to capture as much relevant information as possible and then pass the ticket to a network specialist. In some environments, the call volume may be such that the person answering the telephone at the help desk is expected to perform some minor troubleshooting prior to handing off the ticket for further work by a network specialist. In a shop with a handful of network support staff, the person taking the support call may be expected to manage the issue until it is resolved. There will be times when all the staff is working on issues and no one is available to answer the phone. Calls should be routed to an answering service that relays the messages as soon as a staff member returns to the network operations area.

In large organizations that need to have dedicated expertise in certain areas, the staff can be divided as follows:

- **PC support** — Staff members dedicated to desktop applications and hardware issues related to the computer and the network node it is directly connected to.
- **Server support** — Staff members dedicated to various server-based applications, such as e-mail, authentication servers, domain servers, etc. A server administrator may be dedicated to a single server application.
- **Network support** — Staff members dedicated to the network fabric consisting of network forwarding devices, such as routers, switches, hubs, and related cabling.
- **Telecommunications support** — This function may be broken out into a voice group and a data group. However, with the convergence of voice and data networks, this function can overlap into the network, server, and PC support areas with the use of IP voice-based devices and applications. Data telecommunications staff mostly work with the high-speed network data carriers and the devices locally located to provide a network path to the outside world.
- **User base support** — Staff members dedicated to training users, creating user manuals, and creating and maintaining user accounts, including passwords and network access privileges.

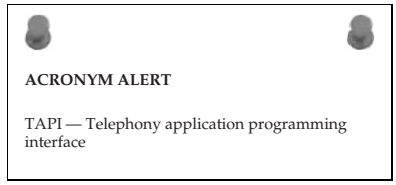
This is a granular description of possible support functions for those organizations that have the ability to divide these functions into separate areas. There are many instances where these functions may overlap or where one support person from one group can help in supplying support to a different group.

15.1.3 Network Monitoring

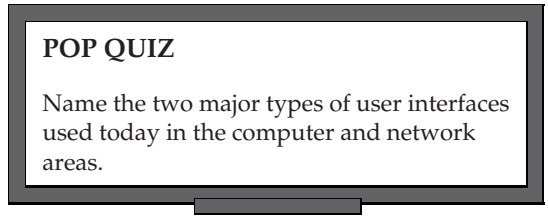
Monitoring network performance for larger networks is an automated process. There are monitoring stations that monitor not only the health of network devices but also can track traffic patterns through the network. In these types of network environments, network support personnel is dedicated to evaluating the information that is displayed and determining if there is a need for some sort of service on the network. This kind of monitoring is interactive and is normally used in a 24/7 network operations environment to ensure that the network is functioning at optimum performance throughout the day. The networks where this

type of monitoring can be found are those that deal with thousands of devices spread not only around a single site but perhaps several sites whose networks are being monitored from a central location.

This type of network monitoring may be too costly for a smaller network installation. However, monitoring can be done on a less grand scale using Simple Network Management Protocol (SNMP). There are low-cost SNMP programs that can be set up on a workstation where the network devices can be polled. These programs poll the devices and query the management information base (MIB).[3] An MIB is a database containing the network objects that provide information on the major elements of the device and its interfaces. The program can simply query and display the retrieved information or in more feature-rich programs, retain the information captured over a fixed interval and display it in a historical graph. So the feature-to-cost ratio would be a deciding factor when selecting a program using SNMP to monitor your network.



Even without SNMP, many devices retain information that can be used to monitor their health. This information can be read using a console connection[4] or Telnet to a management address on the device to retrieve the information. These methods utilize the command-line interface (CLI)[5] of the device to retrieve the requested information. Whereas SNMP for the most part has many standardized MIBs, CLIs can vary from manufacturer to manufacturer, as well as from device to device from the same manufacturer, so there is no standard query. Keeping CLI reference manuals for all the different devices within the network is essential.



Monitoring is a preemptive activity. It is used to provide early warning of network problem areas. It most definitely is capable of reporting network

[3]MIB is a collection of object identifiers (OID) to collect information regarding the operation of a network device. There are standard MIB OID values, which every network device supports, and then there are the proprietary MIB OID values, which are designed to query components of a nonstandard device. The MIB database is loaded on an SMNP workstation so it can use the appropriate OID to retrieve the desired information from the network device.

[4]Console connection usually refers to an RS232 serial connection that allows the establishment of a terminal session. This connection can be used to issue commands for either configuring the device or retrieving the requested information. These commands may be of a proprietary nature, depending upon the device. In these cases, the manufacturer's operational manual should be consulted.

[5]Command-line interface (CLI) refers to a line-by-line command set that is a proprietary set of commands designed by the manufacturer to allow the device to be configured or respond to information queries relating to its configuration or operation.

outages as well as network device failures, but its real value is pointing out areas of the network that may need modification to handle increased demand or traffic patterns that can be rerouted for a more even distribution of network bandwidth.

15.2 Administration

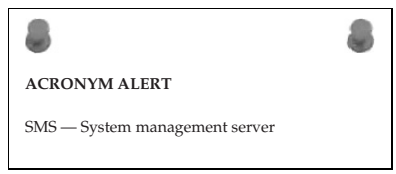
The main thrust of network administration is evaluating and allocating network resources and other administrative needs in support of the organization's network. What are the resources? First, it is people — understanding the staffing needs required to maintain a network, scheduling staff members efficiently to carry out the mission of ensuring network maintainability and availability with a minimal amount of downtime. Second, it is relationships with vendors and suppliers, not only for material goods but as resources for their knowledge expertise of the products they market. Third, it is the creation of processes and policies for the smooth operation of the network management group.

15.2.1 Network Management Staff Members

The main topic of discussion in this section is for those network management organizations that have been tasked with the care of a large organization's network. There are natural divisions of labor as far as expertise, with a support hierarchy to coordinate activities to ensure a high level of service to their user base with minimal impact on those users whose productivity is directly related to the availability of network resources.

For smaller network operations with only a handful of staff in support of network resources, this section may seem like overkill. However, networks tend to grow as organizations grow, so this information may be usable as a roadmap to aid in planning that growth. Figure 15-2 illustrates an organizational chart for a hypothetical large network management organization.

In very large companies, it is recognized that the network management organization is an integral part of the organization and that it requires an executive-level employee with the title of VP or director to lead the network management organization. The smaller the company, the fewer staff are required. It may be run by a higher-level manager acting as the focal point for the whole department.



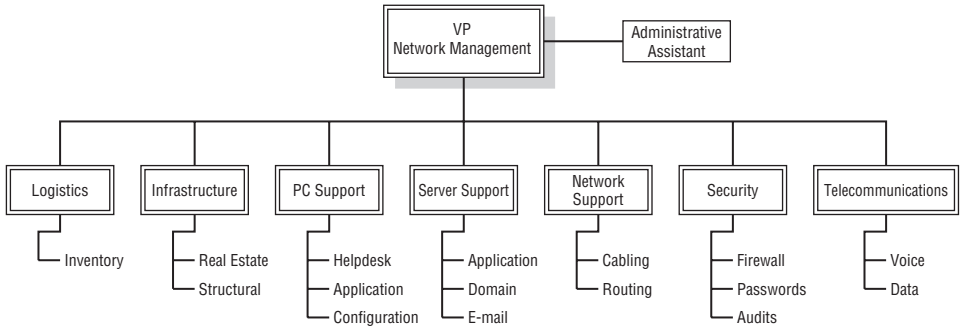


Figure 15-2 A network management organizational chart

15.2.1.1 Executive Level

Only a very large organization would have a vice president of network management. The reason for it would be the number of staff positions that are reporting to this position. If a network management organization has a multilevel hierarchy, such as division or group managers with a support structure under them, someone needs to drive the coordination between the various groups. There also may be large purchases for major expansion or upgrades that require contract negotiations. On that level, an executive position is warranted.

This position or office may require additional staff, such as an administrative assistant to coordinate and schedule events. Attached to the position may be an accounting function and a contracts function for managing budgets, accounting for expenditures, and negotiating contracts for equipment and services. The executive position would be able to authorize those expenditures and contracts, and to set staffing levels.

This position is the focal point for all things related to network resources. It is the position that oversees all activities and is responsible for preparing reports to the other members of the executive office. The position requires a skilled management person more than a technocrat. However, he or she must be knowledgeable enough to understand some of the aspects involved with the overall network infrastructure. More technical management is left to the department heads and managers. They are the ones who oversee the day-to-day activity within their respective departments.

15.2.1.2 Department Heads/Managers

Department head (or manager) positions should be filled by people who are technically competent in the area they have been placed in charge of. They

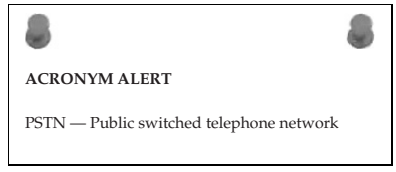
should have good managerial skills as well as people skills. In a smaller organization, this may be a hands-on position where the department head/manager/supervisor performs some network-related responsibilities as well as oversees the overall operation of the department. The differing functional areas are broken out for easier identification of their roles and activity level within the organization. In a smaller organization, a department head may wear many hats and cover more than one functional area at the same time.

15.2.1.2.1 Telecommunications Department

This department may have both voice and data responsibilities. It coordinates communication activities not only with internal users, but potentially with remote users as well. The type of telephone service that is in use, POTS[6] or VoIP, will determine how much separation there actually is between the voice and data groups.

The telecommunications department is responsible for interfacing with the long line companies that connect the organization to the outside world. The department also monitors the bandwidth needs of the organization and negotiates contracts and rates with telecommunications providers. Final approval of contracts occurs at the executive level, but the details of the services and support that are to be provided is usually worked out by those that are intimately involved in the daily operations of the telecommunications department.

On the voice side, there is usually a telephone switch that needs to be administered and maintained. The telecommunications department is responsible for the entire circuit, from the switch to the handset of the user base, including assigning telephone numbers to employees and generating reports about telephone usage and billing.



15.2.1.2.2 Security Department

The security department conducts a broad range of activities that deal with all aspects of network security. It deals with the physical and the abstract. On the physical side, it is tasked with locking down the network to prevent any malicious intent. It is responsible for monitoring the network's security with

[6]POTS (plain old telephone service) is the standard convention of analog signals traveling over old low-grade telephone wires. These may be found in older installations where the convergence of the voice and data networks has not yet taken place.

periodic security audits. The department also looks for any vulnerabilities that may exist but have not yet been exploited.

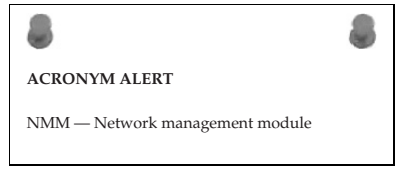
Members of the security department are responsible for developing policies for network usage and for enforcing those policies with monitoring. They are also are in charge of the various firewalls in the network. The group is in control of the traffic that enters and leaves the network. This is accomplished by placing the appropriate policies on the firewall devices to restrict undesirable traffic and permit traffic that is necessary for the performance of the organization's business.

User authentication, including the servers involved, is under the auspices of the group, although parts of this responsibility may be shared with other groups. Ultimately, however, this group is the highest authority on user password control. The group administers the policies that set user permission levels on the network and monitors network usage to ensure it falls within the organization's policies.

15.2.1.2.3 Network Support Group

The network support group is responsible for the distribution of network services over the network fabric. This includes the cabling, wireless access, or whatever network media is being used and the devices placed within the network to facilitate network traffic flow. The group interacts with other network groups to help resolve network-related issues, varying from the network access in the telecommunications group to the PC support group bringing the network to the desktop computer.

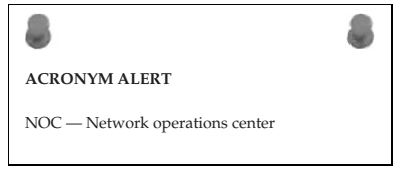
The group is in control of the bandwidth distribution across the network, as well as routing policies that control the flow of network traffic. They are responsible for configuring and maintaining all the devices that perform the distribution and routing functions, as well as media that is used. Some large network installations do enough cabling to justify having staff whose sole function is to distribute cable throughout the facility. Smaller organizations subcontract out the cabling function on an as-needed basis. Usually, small runs not requiring a major effort can be carried out directly by the network support staff members. Every network administrator at one time or another has strung a fair amount of CAT 5 cabling.



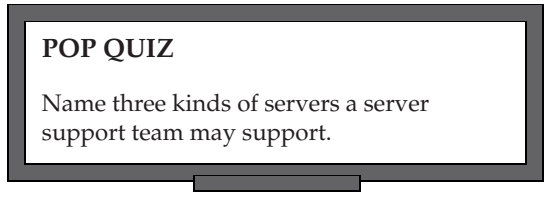
15.2.1.2.4 Server Support Team

As its name implies, the server support team is responsible for maintaining all servers. These may be specific application servers, such as e-mail, print services, database, etc. The goal is for the servers to function with a minimal amount of downtime. Members of the server support team perform preventive measures, such as running daily backups on all servers that are being strategically used in the conducting of the organization's business.

Access to the servers is normally restricted, even to other members of the network operations group. The reason for this is that the information an organization has and controls is an integral component of its business. The server support group may work closely with the security group, but it has a major say in any decisions involving the operation of the servers.



If there are network domain servers under the control of the server support group, the group needs to interface with the security, PC support, and network support groups to ensure that users are assigned within the proper domain, subdomains, and groups, and that users can reach all the resources their particular membership allows. The server support group coordinates with the security group to add or remove users as they move into and out of the organization.



15.2.1.2.5 PC Support

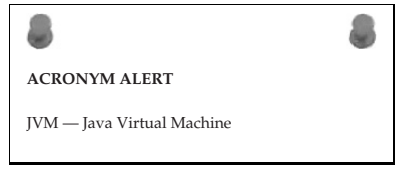
The network operations help desk is often the first place a network user calls when experiencing a computer issue, whether network-related or not. For this reason, it may fall within the realm of the PC support staff. In reality, it can be a number manned by a call coordinator function without any particular network technology knowledge other than to determine if the issue is related to software, hardware, or network access. The call can then be directed to a staff member within that particular group for further diagnosis and remedy.

If the help desk is to resolve problems, it needs to be manned by technically competent staff members and requires additional staff, as the possibility of receiving multiple calls simultaneously is a constant reality. It is a balance that needs to be attained and perhaps it can be met with staff members with duties other than help desk–related tasks who can jump in and assist during peak call periods. There is no hard and fast rule of how many user seats per help desk member is ideal. It is not a one-size-fits-all situation.

It benefits the PC support group to have an educated user base, so there may be training personnel assigned to the group whose responsibility is to prepare user-based documentation to facilitate the users in the use of network resources and perhaps other applications. Depending on the organization and the applications used to run the business, there may be multiple application specialists who not only conduct training but who can also troubleshoot issues related to specific applications.

Needless to say, PC support is involved in computer hardware as much it is with application programs. Larger organizations use ''corporate builds.'' These are the base programs that need to be loaded on each computer within the organization. Since a large organization has many users with computers, the ideal situation would be to develop a standard that is a combination of hardware and software given to each user. There are application programs that allow the creation of an image file that contains the base operating system and any other standard applications given to each user, including antivirus, e-mail, and productivity programs such as word-processing, spreadsheet, and database applications. Use of the image file allows for the rapid deployment of standard production PCs. Users requiring additional programs to carry out their functions within the organization would have them loaded on an as-needed basis.

In the area of computer hardware, some organizations depend on support directly from the computer manufacturer. Some go as far as leasing computers from vendors so that they do not own them outright. Usually at the end of the lease, the equipment is returned and the computer is replaced with a more current version. The organization often specifies the software suite image or develops an image and supplies it to the vendor to load on the computers before they are shipped to the organization.



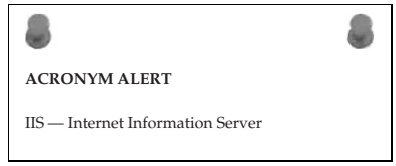
Members of the PC support group are directly involved in negotiating the technical details of all major computer purchases, but large contracts require final approval at the executive level.

15.2.1.2.6 Infrastructure Group

Users often think of the network as a massive cloud that information flows over. However, the cloud is more solid than its usual representation. In reality, network infrastructure does occupy real estate space. It occupies space not only in closets and offices but also in many different areas throughout the facility it serves. The network operations group may not have real estate staff members as part of its staff. However, there is a need for this function within the group. The staff member performing this function works with facility administrators and real estate management to ensure that the network has the required space and is secured properly.

Planning is required anytime there is a network expansion or change that requires the involvement of other areas of the facility not under the direct control of the network operations group. Network operation staff members need to interface with the people who determine real estate usage. The network staff should map out the space requirements and any other special needs, such as cableway access to support cabling needed within the area.

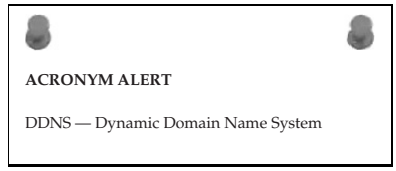
An infrastructure group as part of the network operations group may only be a reality within very large organizations. However, it is a necessity, and if it's not a group of its own, then one of the functional department heads should assume the role. In all likelihood, it will fall within the network support group.



15.2.1.2.7 Logistics Group

The logistics group is responsible for overseeing all the devices deployed in the network, as well as any spare equipment. It is the department responsible for logging the new stock as well as the units that have been returned to the manufacturer for repair (RMA).[7] Various accounting processes are used to keep track of all major components. It is easier if a bar coding process is in place. When a new component is received, its description, serial number, barcode, and date are entered into an inventory database. The date is essential if there is ever a question of warranty. If a company is large enough, it makes sense to have a single department control the flow of materials into and out of the network's facility. If an organization is not large enough, or the volume of goods entering and leaving the network's facility is low, a separate department to handle this activity or function may not be required.

Control of inventory is essential. The PC support group should maintain its own inventory of computer-related materials, as should the server support and network support groups. If the volume is high, a centralized service that performs this function for those groups may be warranted. If planned correctly, there can be a savings involved, as well as the elimination of redundant activity.



15.3 Maintenance

Maintenance is a network operations–wide activity. Each area should carry out its prescribed plan of what is considered maintenance. However, the primary activities are as discussed below.

[7]RMA (returned materials authorization) is a process used by all manufacturers for the return of materials, whether in warranty or not, for repair or replacement of the failed component.

- **Preventive measures** — This activity can be as simple as performing household-type activities such as making sure that ventilation vents on equipment are free and clear. If there are filters involved, they should be changed at the manufacturer's recommended interval. An occasional survey of all equipment within the network should be taken to ensure that no obstructions block vents or fan intakes. General housekeeping should be performed to eliminate any clutter that may have gathered around equipment. The serviceability of electronic equipment is directly proportional to how well it is kept to its normal operational range. If devices become stressed due to excessive heat, they will eventually fail. Good housekeeping practices can boost the reliability of the network while eliminating unnecessary costs.
- A major preventive measure that often is forgotten is the saving of configuration files related to a piece of equipment. This needs to be done on the initial configuration and any time the unit has been reconfigured. Having the ability to reload a configuration if it is ever lost can save many hours of trying to reconstruct all the configuration information and applied policies by hand. Unfortunately, there are cases when there are no configurations to be had, either in electronic storage or on paper. These are the times the network needs to be reinvented — a most painful task that could cause the loss of network resources not only for hours but for days.
- **Corrective measures** — For the most part, corrective measures deal with a direct failure in the network's operation. They involve troubleshooting, locating the cause of the problem, and eliminating the problem with a correction of some type. It could be as simple as finding a lose connector or as complicated as replacing a major network component. It may also involve finding a workaround to allow network users to continue working, thus eliminating lost productivity due to a network failure. If a workaround can be found, a maintenance window can be arranged for the full repair of the network issue.
- Some network problems occur when a device has lost its configuration. There are many reasons why this happens, such as power surge, etc. However, the impact of the downtime can be reduced with the availability of a configuration backup file. The file can be used to restore the configuration, and in case of an equipment failure the configuration can be quickly moved to a spare unit restoring network operation.
- Corrective measures need not wait for a network problem to occur. It can entail other activities such as taking care of cabling that is exposed in a manner that it may become damaged. It may require a maintenance window to allow for the corrective measure to be taken.

- **Revision-control measures** — Most equipment in the network area has firmware or software programs embedded within it. Like all software, there are revisions that occur due to bug fixes or added features. Manufacturers release updates to software from time to time, but may or may not issue bulletins. It is up to the user base that is utilizing that equipment within their network to keep abreast of any changes that may have taken place. Many times the software is free, and some companies sell maintenance agreements for continued software support after the warranty period has been exceeded. It is best to keep an ongoing relationship with your equipment vendor to ensure that you are made aware of any bug fixes or new features that have been added to the software. Bug fixes are necessary patches, whereas added features are more of a selective choice. If a feature is not needed and your software is running fine in its current configuration, you may be able to save the effort required to upgrade your network device.

15.4 Provisioning

Many people believe that provisioning happens only once, at the initial installation of the network. However, networks tend to change and grow. As a result, they may require some reprovisioning within their life cycle. This may be adding more bandwidth in certain network segments to facilitate an increase of network traffic, or segmenting networks to isolate elements in order to increase security or improve performance. It could be reprovisioning of a switch to add more VLAN circuits to isolate certain network resources. A VLAN may have experienced network performance issues and upon investigation the network support staff might determine that breaking up the VLAN into multiple segments would increase performance without the need for any additional hardware or bandwidth.

POP QUIZ

Performing nightly backups on all network servers is called what type of measure?

Provisioning of network resources mainly falls upon the network support group. They are in control of the network fabric over which the network flows. However, it is the responsibility of all the network operations groups to identify areas where provisioning may be needed.

Both the initial provisioning and the reprovisioning need to be documented. If there are configuration changes made on a unit, it needs to be backed up and the old configuration file archived. A rule to remember is to never discard the previous running configuration file after making some configuration changes. If in doubt whether a backup of the current running configuration file exists, play it safe and perform a backup before installing any changes on a network

device. This will allow for a quick reversal if the new changes do not work or cause other issues. Even if it appears that the new changes are working as planned, it does no harm to archive the previous running configuration file. However, make sure the file name is duly marked that it was the previous running configuration.

ACRONYM ALERT

PKCS — Public Key Cryptography Standard

15.5 Tools

The tools that can be used in the network operations area are many and varied, ranging from generic programs designed to monitor a wide range of network devices to small utility programs that diagnose a specific issue. They may be proprietary and provided by the manufacturer of a device to configure and maintain that device. Some of these tools are graphical (GUI) or others use a command-line interface (CLI). GUIs can be either proprietary or web-based, requiring a web browser for configuration and reporting. Figure 15-3 illustrates a web-based configuration/monitoring tool for a network device.

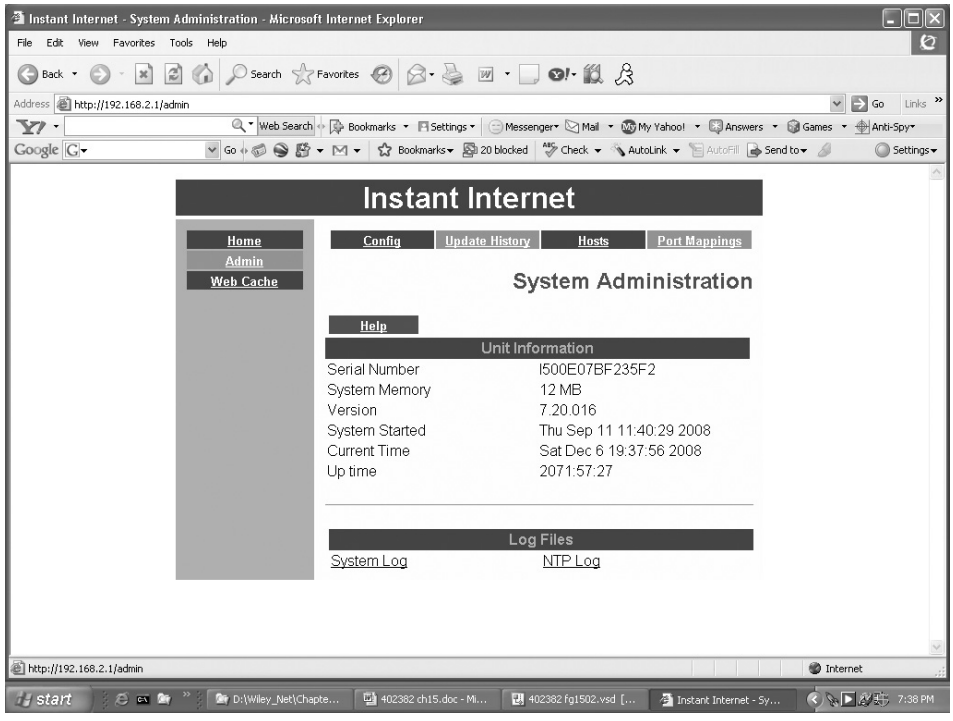


Figure 15-3 A web-based configuration/monitoring tool

The same device also has a proprietary configuration tool, which is also graphical in nature. This user interface is illustrated in Figure 15-4.

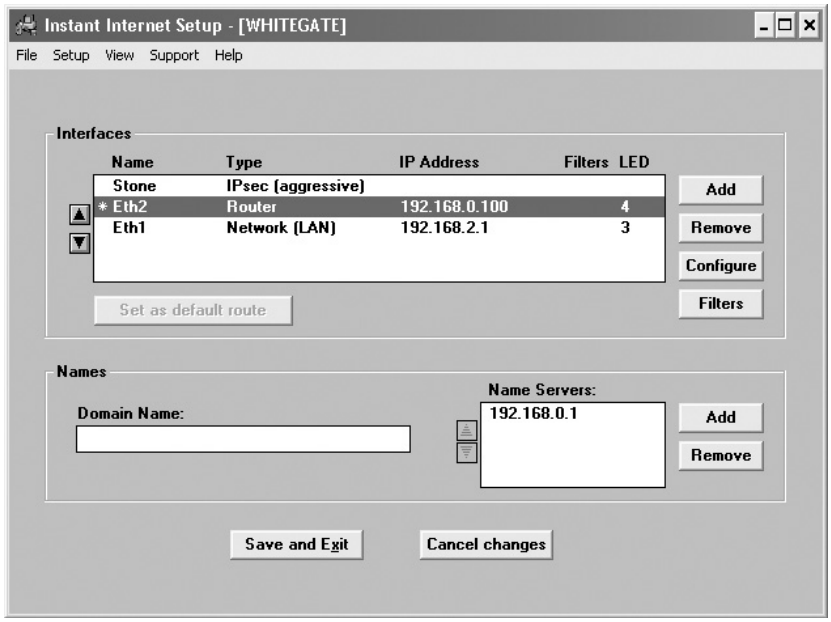
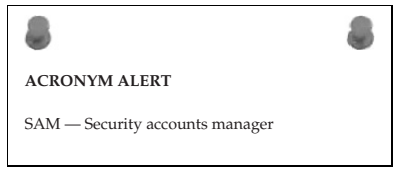


Figure 15-4 A proprietary configuration/monitoring tool

For this particular piece of equipment, the proprietary tool is easier to use than the web-based tool. The implementation depends on how the manufacturer envisions the tool is to be used.

Most equipment manufacturers provide a CLI to configure, provision, and monitor their device. Access to this interface is usually through a console terminal connection or a Telnet session using a TCP/IP connection to one of the Ethernet ports on the device. Figure 15-5 illustrates a typical Telnet session.

Figure 15-5 A typical Telnet session



Utilities that come with network devices are handy to have and usually a lot easier to use while configuring units, but as far as monitoring one device at a time on a network, they can be formidable at best. SNMP was devised to allow the monitoring of many network devices from many different manufacturers, but it can be used to make configuration changes on the devices as well.

15.5.1 Simple Network Management Protocol

Most of today's network devices are considered to be ''managed'' devices. Many devices can be managed thanks to the development of SNMP. Devices such as computers, servers, IP telephones, printers, hubs, bridges, routers, wireless access points, remote access devices, and many more all have an imbedded SNMP agent that allows them to be considered ''network managed.'' The SNMP agent is software that answers queries from a network management station (NMS). Each device has a standard MIB and if needed, additional proprietary MIB entries. An MIB is a collection of managed variables within the device that is identified by its object identifier (OID). There are objects for many elements in a device. Each element has its own unique OID. The OID is used to retrieve information on the object or to set an object variable to configure the unit. Figure 15-6 illustrates a network-managed device with an embedded SNMP agent.

A network support staff person is monitoring the network. In normal polling fashion, the device's operational information can be retrieved on an ongoing basis to monitor the overall performance of the network. Network-managed devices can have SNMP traps set for various alert conditions. If a trap setting is reached, the device waits to be polled but sends a trap message to the network management station notifying it of the alert condition on the device. Figure 15-7 illustrates the output from an MIB polling program.

In this figure, the interfaces on the unit are listed with their attributes, which include IP address with subnet mask, MAC address, MTU size, speed, and a description. Notice that all ports are reported, even an AUX console port (a serial RS232 port). Its administrative state is up, but its operational state is down, as there is no connection to that console port. All the Ethernet ports are showing up and operational.

Additional operational information can be obtained from the device, such as the routing table displayed in Figure 15-8.

This figure shows the internal routing table of the device. These are direct routes, which means they were programmed into the device. If a routing protocol were involved, such as RIP or OSPF, those routes obtained from the protocol running on the device would be indicated in the protocol (proto) column.

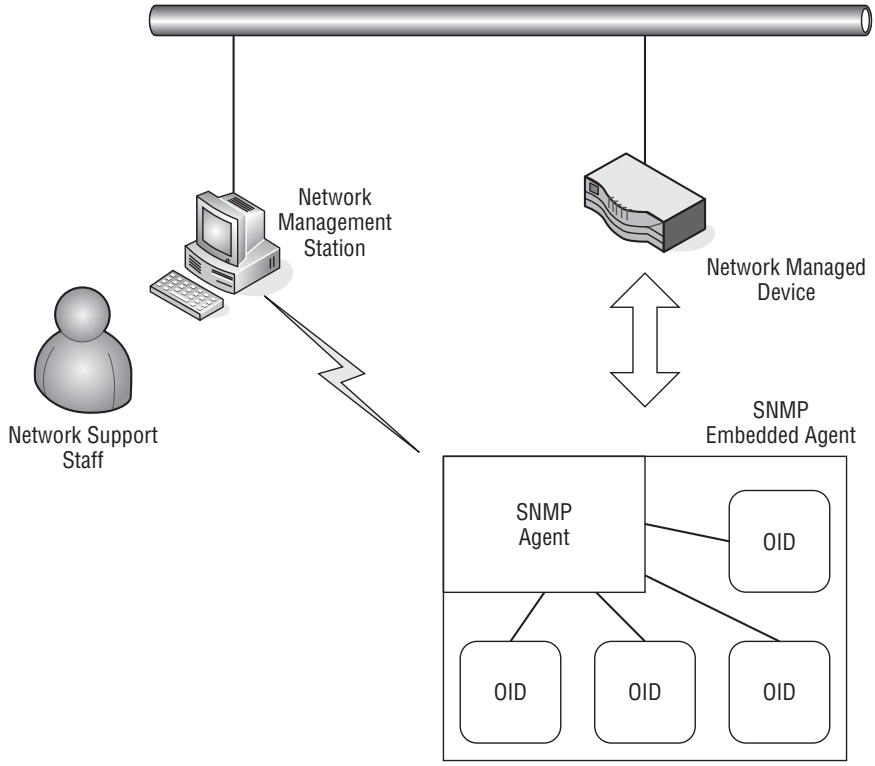


Figure 15-6 A network-managed device with an embedded SNMP agent

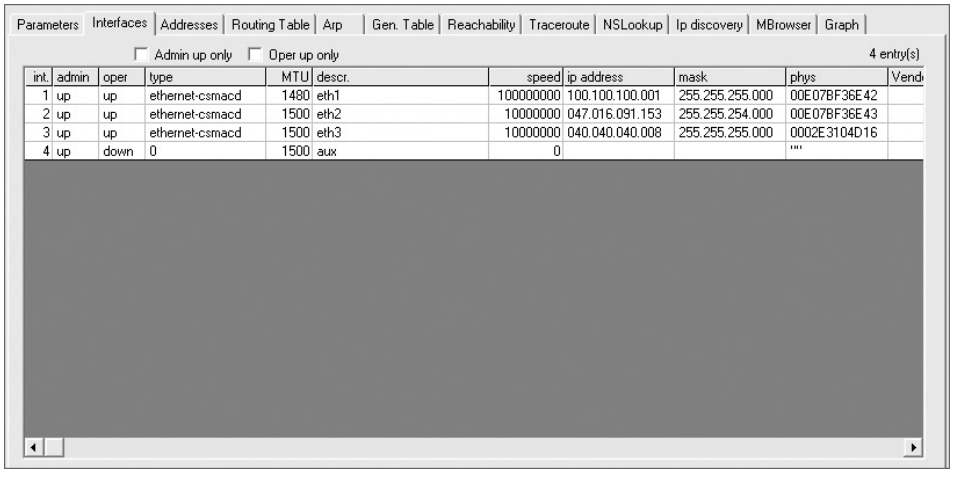
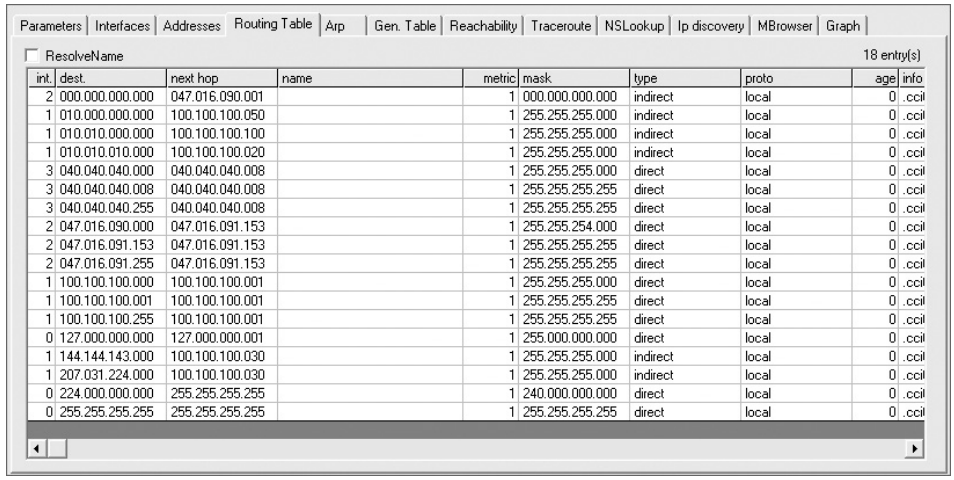


Figure 15-7 The output from an MIB polling program



int.	dest.	next hop	name	metric	mask	type	proto	age	info
2	000.000.000.000	047.016.090.001		1	000.000.000.000	indirect	local	0	.ccil
1	010.000.000.000	100.100.100.050		1	255.255.255.000	indirect	local	0	.ccil
1	010.010.000.000	100.100.100.100		1	255.255.255.000	indirect	local	0	.ccil
1	010.010.010.000	100.100.100.020		1	255.255.255.000	indirect	local	0	.ccil
3	040.040.040.000	040.040.040.008		1	255.255.255.000	direct	local	0	.ccil
3	040.040.040.008	040.040.040.008		1	255.255.255.255	direct	local	0	.ccil
3	040.040.040.255	040.040.040.008		1	255.255.255.255	direct	local	0	.ccil
2	047.016.090.000	047.016.091.153		1	255.255.254.000	direct	local	0	.ccil
2	047.016.091.153	047.016.091.153		1	255.255.255.255	direct	local	0	.ccil
2	047.016.091.255	047.016.091.153		1	255.255.255.255	direct	local	0	.ccil
1	100.100.100.000	100.100.100.001		1	255.255.255.000	direct	local	0	.ccil
1	100.100.100.001	100.100.100.001		1	255.255.255.255	direct	local	0	.ccil
1	100.100.100.255	100.100.100.001		1	255.255.255.255	direct	local	0	.ccil
0	127.000.000.000	127.000.000.001		1	255.000.000.000	direct	local	0	.ccil
1	144.144.143.000	100.100.100.030		1	255.255.255.000	indirect	local	0	.ccil
1	207.031.224.000	100.100.100.030		1	255.255.255.000	indirect	local	0	.ccil
0	224.000.000.000	255.255.255.255		1	240.000.000.000	direct	local	0	.ccil
0	255.255.255.255	255.255.255.255		1	255.255.255.255	direct	local	0	.ccil

Figure 15-8 MIB program displaying the routing table

An MIB walkthrough can illustrate the OID associated with a particular object. In Figure 15-9, the OID for interface speed has been selected.

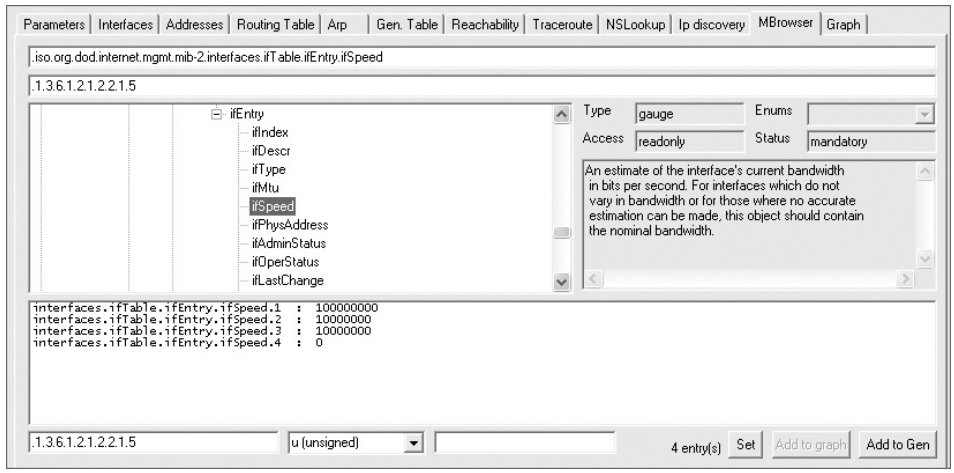


Figure 15-9 MIB program displaying interface speed

Notice that the speed of all four interfaces is shown. This differs from Figure 15-7, which showed all the information relating to each interface. To build that table, all the OID entities for each column would need to be gathered for display. However, an OID is unique, and the displayed OID is the interface speed. Notice that the OID description and MIB number are displayed and it is a read-only MIB, so a setting to another value is not allowed.

POP QUIZ

How is a network device element uniquely categorized within its MIB?

SNMP uses a community setting to group a number of devices to be monitored within the community. The default community setting is ''public,'' although this can be changed. The network management station is able to poll all devices in the community it is monitoring. SNMP traps will be sent to the MNS server that is a member of the community the device is a member of.

A variety of SNMP programs are available, each with varying levels of capability. Standard MIB variables can be read by many different SNMP programs, but the software that reads and sets them may be far different in capability. This is an area a network administrator really needs to comparison shop to get the functions that are desired and the best price-to-performance ratio. Some programs are more glitzy than others, showing all sorts of graphs and histograms. Although they may be attractive, you may be paying extra for information overload. Determine what is valuable for your network and develop a checklist to see which SNMP program has the desired features at the best price.

ACRONYM ALERT

NCC — Network control center

15.5.2 Packet-Capture Capability

There are times it is difficult to determine what is going on when a network is having traffic problems. Often the only way to do this is to analyze the packets that are entering and leaving a particular network device. Packet-capture devices and programs can return some statistical information when you are investigating traffic patterns or performance issues on a network segment. With the availability of open source packet-capture software, there is no reason not to have this ability, even for a network operations center with a small budget. Even if you are uncomfortable reading through a packet capture to see if you can find a problem, it is useful if you can use the packet capture under the direction of your third-party support organization. Figure 15-10 illustrates a screen of a packet-capture program.

Summary information can be retrieved, and individual packets can be selected, opened, and analyzed. The summary can give you an idea of the performance level of the network segment the packet-capture station is attached to. A packet-capture program can be a low-cost traffic analyzer that measures network traffic load on a particular segment. Statistical information can also be displayed in graphical form, as shown in Figure 15-11.

ACRONYM ALERT

PDU — Protocol data unit

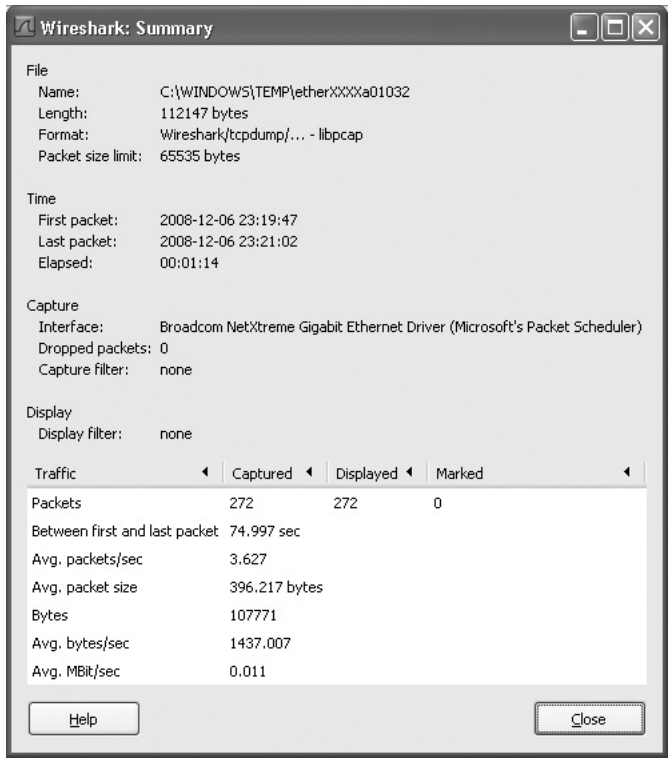


Figure 15-10 A packet-capture program's display

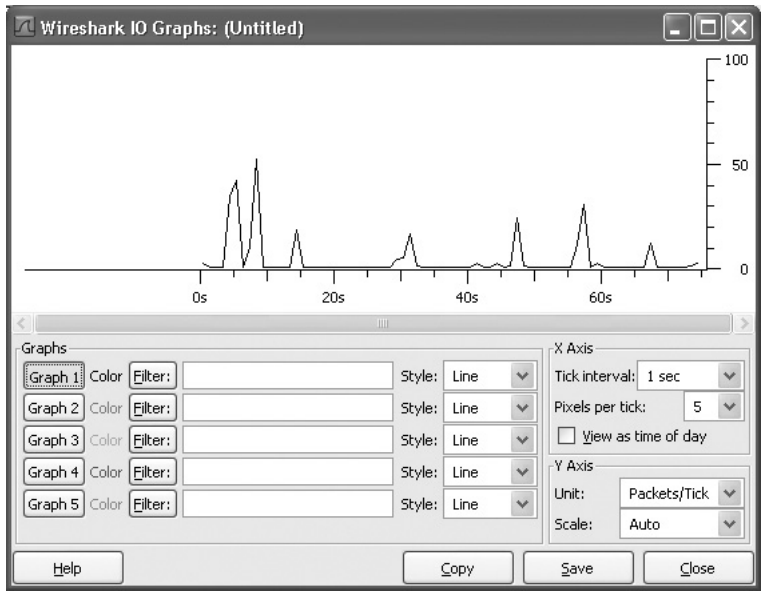


Figure 15-11 A packet-capture program's graphical display

15.6 Chapter Exercises

1. Which protocol can be used to monitor devices on a network?
2. Where would an SNMP agent be found?
3. What would cause an alert to be displayed on an NMS workstation?
4. How would packets on a network be captured and inspected?

15.7 Pop Quiz Answers

1. Think about a network you are familiar with. It may be any network home, work, school, organization, etc. How would you rate their user to support staff ratio? Give reasons why.

   A ratio of 1,000 network users to one support staff member may be considered poor, whereas a 10-to-1 ratio would be considered overkill. At home, it is one to one, because it is your network and you are both the user and support staff. There is no set textbook answer or a one-size-fits-all answer. Staffing levels are set by the dynamics of the organization and how quickly network issues must be resolved.
2. List the minimum information that is needed to generate a trouble ticket or work order for network support.

   Date, time, contact, problem description, severity
3. Name the two major types of user interfaces used today in the computer and network areas.

   GUI (graphical user interface) and CLI (command-line interface)
4. Name three kinds of servers a server support team may support.

   E-mail, print services, database
5. Performing nightly backups on all network servers is called what type of measure?

   Preventive
6. How is a network device element uniquely categorized within its MIB?

   OID (object identifier)