Net Management Chapter 3

Network administrator/Manager

The extensive use of the Internet, intranets, and the move to a webcentric world has redefined the way companies depend on computers. The Internet is a 24/7 operation, and poor operations can no longer be tolerated. Paper purchase orders can be processed daily in batches. On the other hand, there is an expectation that the web-based system that does the process will be available all the time, from anywhere. Nightly maintenance windows have become an unheard-of luxury.

Duties of a network administrator

After the analysis and design phases of network development are completed and the computer network is in place and operating, it is the network administrator's responsibility to keep it running smoothly. (Some companies are starting to call this position a network engineer, although network engineers tend to perform more network design while network administrators may perform more network upkeep. Keeping a network running involves making repairs on failed components, installing new applications and updating the existing ones, keeping the system's existing users up to date, and looking for new ways to improve the overall system and service level. It is not an easy job. With the complexity of today's networks and businesses' reliance on their applications, network administrators are very much valuable, visible, and always on the move.

Due to the fact that many network administrators are dealing with both computers and people, they need the skills necessary to work with both. A checklist of skills for the network administrator would consist of a wide platform of technology skills, including, but not limited to, knowledge of local area networks, wide area networks, voice telecommunications systems, data transmission systems, video transmission, basic hardware concepts, and basic software skills. A network administrator should also have interpersonal skills, including the ability to talk to users in order to service problems and explore new applications. Along with interpersonal skills, a network administrator also needs training skills, which involve the ability to train users or other network support personnel.

To make effective use of limited resources, a network administrator should also possess a number of common management skills. For instance, the network administrator should have budget management skills, which include knowing how to prepare a budget to justify continuing funds or to request additional funds. In addition to those skills, a network administrator needs basic statistical skills, which implies that he or she must know how to collect and use system statistics to justify the performance of existing systems or to validate the addition of new ones. Time management skills are also a necessity. These include the ability to manage not only one's own time, but also that of projects and any information technology workers who may be working for the administrator.

Just as valuable as time management skills are project management skills, which centre on the ability to keep a project on schedule and to use project-estimating tools, project-scheduling tools, and other methods for continuous project assessment. Finally, a network administrator should possess policy creation and enforcement skills, which consist of the ability to create policies concerning the use of the computer systems, access to facilities, password protection, access to

applications, access to databases, distribution of hardware and software, replacement of hardware and software, and the handling of service requests.

Training and certifications specifically for network administrators

In order to learn new skills and demonstrate proficiency within a particular area, the network administrator can obtain certification. It is possible to become certified on a particular type of network operating system, such as Windows Server, or on a particular brand of network equipment, such as Cisco routers. The following is a list of some of the more popular certification programs:

- Microsoft Certified Systems Engineer (MCSE) — This certificate addresses the design, installation, and support of the Windows network operating system.
- Cisco Certified Network Associate (CCNA) — This certificate covers the topics of installing, configuring, operating, and troubleshooting enterprise-level router and switched networks.
- IBM Certified Systems Expert (CSE) and Certified Administrator (CA) — These certificates demonstrate the ability to successfully plan for, install, and support IBM's networking products.

The position of network administrator is demanding, challenging, and constantly changing. Being a successful network administrator requires a wide range of technical, management, and interpersonal skills. A good network administrator is constantly learning new skills and trying to keep abreast of rapidly evolving technology. A computer network system could not survive without the network administrator. The network administrator has to keep in mind, however, that the system would also not survive without users.

Let us now take a look at an additional tool that network administrators can use for supporting or improving a system: statistics

Generating Usable Statistics

Computer networks are in a constant state of change. New users and applications are added, while former users and unwanted applications are deleted. The age of a network (and its underlying technology) is often based on Internet-years, which many experts equate to approximately 90 calendar days. Since technology changes so quickly and networks are constantly being called upon to support new and computationally intensive applications, a network administrator is constantly working on improving the data transfer speed and throughput of network applications.

To support changes to a network, a network administrator needs funding. The management, regrettably, is not always receptive to investing more funds in technology. Most often, the management needs to be persuaded that services are suffering or response time is not what it needs to be. Statistics on computer network systems can be a very useful tool for demonstrating the need to invest in technology. If properly generated, statistics can be used to support the request for a new system or modifications to an existing system.

Four statistics, or measures, that are useful in evaluating networks are mean time between failures, mean time to repair, availability, and reliability.

Mean time between failures (MTBF) is the average time a device or system will operate before it will fail. This value is sometimes generated by the manufacturer of the equipment and passed along to the purchaser. But very often this value is not available, and the owner of the equipment has to

generate an MTBF value from the equipment's past performance. Even though every device is different, the longer the mean time between failures, the better.

Mean time to repair (MTTR) is the average time necessary to repair a failure within the computer network. This time includes the time necessary to isolate the failure. It also includes the time required to either swap the defective component with a working component or repair a component—either on-site or by removing the component and sending it to a repair centre. Thus, the mean time to repair includes the time needed to bring the system back up to normal operation.

The value of mean time to repair depends on each installation and, within an installation, on each type of component. For example, a network server with hot-swappable devices should have a shorter mean time to repair than a device that has to be shut off, opened, repaired, and then rebooted.

The third statistic, **availability**, is the probability that a particular component or system will be available during a fixed time period. A component or network with a high availability (near 1.0) is almost always operational. Software that generates statistics often calculates the value for availability based on mean time to repair and mean time between failure values. Components with a small MTTR and a large MTBF will produce availability values very near to 1.0. For simplicity, however, we will calculate availability by simply subtracting the downtime from the total available time and then dividing by the total available time:

Availability% = (Total available time – Downtime)/ Total available time

Suppose we want to calculate the availability of a printer for one month (24 hours per day for 30 days, or 720 hours), knowing that the printer will be down (inoperable) for 2 hours during that period.

Availability% = (720 – 2)/ 720 = 0.997

Since the availability is near 1.0, there is a very high probability that the printer will be available during that one-month period.

To calculate the availability of a system of components, you should calculate the availability of each component and find the product of all availabilities. For example, if a network has three devices with availabilities of 0.992, 0.894, and 0.999, the availability of the network is the product of $0.992 \times 0.894 \times 0.999$, or 0.886. Companies usually like to see availability values in the "nines," with the more nines the better. For example, 0.9999 is better than 0.999.

The fourth statistic, **reliability**, calculates the probability that a component or system will be operational for the duration of a transaction of time *t*.

A reliability of exactly 1.0 means the network or device is reliable 100 percent of the time. What if the reliability of a second device was calculated and found to be 0.995? Although this value also appears to be near 1.0, there is a difference between the two reliabilities: 0.00489. Therefore, many network administrators strive to maintain system availability and reliability values of 0.9999 to 0.99999.

Network Diagnostic Tools

In order to support a computer network and all of its workstations, nodes, wiring, applications, and protocols, network administrators and their support staff require an armoury of diagnostic tools. This armoury of possible diagnostic tools continues to grow, with more powerful and helpful tools becoming available every day. Diagnostic tools can be grouped into two categories:

- Tools that test and debug the network hardware,
- And tools that analyze the data transmitted over the network.

Ultimately, the command centre and the help desk have to be considered. Even though not precisely tools in the traditional sense, the command centre and the help desk are valuable additions to a network support staff's arsenal. We will start by looking at the tools that test the network hardware first.

Tools that test and debug network hardware

Tools that test and debug network hardware range from very simple devices to more elaborate, complex devices. Three common testing devices are electrical testers (the simplest), cable testers, and local area network testers (the most sophisticated).

Electrical testers measure AC and DC volts, resistance, and continuity. An electrical tester will prove if there is voltage on a line, and if so, how much voltage. If two bare wires are touching each other, they will create a short, and the electrical tester will show zero resistance. The continuity tester is a handy device that shows whether two wires are grounded to each other. Electrical and continuity testers are used to determine if the wires themselves are experiencing simple electrical problems.

Cable testers are slightly more complex devices. They can verify connectivity and test for line faults, such as open circuits, short circuits, reversed circuits, and crossed circuits. Certain kinds of handheld cable testers can also test fibre-optic lines, Asynchronous Transfer Mode networks, and T-1 circuits. For instance, if a connector hidden in some wiring closet contains two wires that are switched, a cable tester will detect the problem and point to the source of the problem.

One of the most elaborate devices is the local area network tester. These testers can operate on Ethernet whether they have switches or not. Some local area network testers have a display that graphically shows a network segment and all of the devices attached to it. When plugged into an available network jack, these testers can troubleshoot the network and suggest possible corrections. A common problem solved by these devices is the identification and location of a network interface card (NIC) that is transmitting continuously but not sending valid data. The tester will pinpoint the precise NIC by indicating the 48-bit NIC address. A network administrator can then basically look up the particular NIC address in the system documentation and map it to a unique machine in a unique office.

Network sniffers

The second category of diagnostic tools covers tools that analyze data transmitted over the network. These tools include protocol analyzers and devices or software that emulate protocols and applications. One of the most common of these tools is the traffic analyzer or protocol analyzer. A

protocol analyzer, or **sniffer**, monitors a network 24 hours a day, seven days a week, and captures and records all transmitted packets. Each packet's protocol is analyzed, and statistics are generated that show which devices are talking to each other and which applications are being used. This information can then be used to update the network so that it operates more effectively. For instance, if a protocol analyzer indicates that a particular application is being used a great deal and is placing a strain on network resources, a network administrator can consider alternatives such as replacing the application with a more efficient one or redistributing the application to the locations where it is used the most.

A very popular sniffer that can be used on UNIX and Windows networks is Wireshark (formerly called Ethereal). Wireshark allows you to examine the data collected from a live network or from a capture file on disk. You can interactively browse the captured data and view either detailed information for each packet or summary information for the entire network. What is perhaps even more interesting about Wireshark is that it's free.

Even a company with the latest tools and techniques may have trouble properly supporting its users. Another "tool" that is necessary is the control centre and help desk. With a control centre and help desk, the network support team can present a friendly "face" to the user, someone the user can turn to in times of trouble

Managing operations

To support network administrators and information technologists in doing their jobs, businesses have control centres for their computing services. The control centre is the heart of all network operations. It contains, in one easily accessible place, all the network documentation, including network resource manuals, training manuals, baseline studies, all equipment documentation, user manuals, vendor names and telephone numbers, procedure manuals, and forms necessary to request services or equipment. The control centre can also contain a training centre to help users and other information technologists. In addition, the control centre contains all hardware and software necessary to control and monitor the network and its operations.

One of the more important elements of a control centre is the help desk. A help desk answers all telephone calls and walk-in questions with respect to computer services within the company. Whether it is called upon to address hardware problems, answer questions about running a particular software package, or introduce the company's users to new computing services, the help desk is the gateway between the user and computing and network services. Fortunately, good help desk software packages are available that the operations staff supporting computing services can use to track and identify problem areas within the system.

A well-designed control centre and help desk can make a huge impact on the users within a business. When users know there is a friendly, available person they can turn to for any computing problems, there is much less computer system/computer user friction.

Now that we have looked at the physical tools that can help a network administrator support a company's networks, it is also crucial to examine/make mention of some of the software tools that can ease the burden of network administration. The most widely used tool is the Simple Network Management Protocol (SNMP) which we have already seen.

Updating the System Software and Applications

Wouldn't it be nice if a network administrator's job was finished once the OS and applications were loaded? Regrettably, as time goes by, people identify new bugs and new security holes, all of which need to be fixed. Also, people find interesting new applications that need to be deployed. All these tasks are **software updates**. Someone has to take care of them, and that someone is you. Don't worry, though; you don't have to spend all your time doing updates. As with installation, updates can be can be automated, saving time and effort.

Every vendor has a different name for its system for automating software updates: Solaris, AutoPatch; Microsoft Windows, SMS; and various people have written layers on top of Red Hat Linux's RPMs, SGI IRIX's RoboInst, and HP-UX's Software Distributor (SD-UX).