Problem Diagnosis And Resolution

Terms you'll need to understand:

- √ Troubleshooting
- √ User and account management
- √ Performance tuning
- √ Network operations
- √ Physical plant
- √ Security policies
- √ Auditing
- √ Disaster planning and recovery
- √ Capacity planning
- √ Network modeling

Techniques you'll need to master:

- √ Evaluating and troubleshooting network problems
- √ Preparing for successful software and hardware upgrades and maintenance
- √ Auditing events on the network

Even in the most smoothly planned, designed, and executed system, problems will occur simply because of the complexity of a network. Just like children, a network system is conceived, born, and continues to grow and change throughout its existence. Unlike children, some even outlive their usefulness. But there are tools that allow you to observe components of the network, help you to determine what is normal, and alert you when there might be problems. There are certain preventive measures you can take to avoid common problems before they happen and there are established troubleshooting procedures to follow when difficulties do occur.

In this chapter, we discuss some approaches to proactive network management, such as the use of management utilities, network monitoring and baselining, performance management, and preemptive troubleshooting. Following will be a discussion of prevention through careful planning, which includes backup systems and methodologies, elimination of security risks, standardized components and procedures, documentation, and training. Finally, we work through some common troubleshooting tips and techniques.

Approaches To Network Management

Network management can be defined as the act or process of regularly managing or supervising a network's execution, usage, and conduct. Administration is a daily, ongoing process. An effective administrator must continually deal with and be an expert at:

- User and account management
- Performance tuning
- Network operations
- Software/hardware upgrades and maintenance
- Physical plant, including cabling, data, and telecommunications
- Security policies and auditing
- Disaster planning and recovery
- Capacity planning
- Network modeling

Network administrators need both breadth and depth of knowledge. Although you can't be an expert at *everything*, you are generally expected to

be one at all times. So Microsoft included several tools with Windows NT to assist you in managing daily operations. Knowing how to use these tools and including them in your management regimen will make your life easier and your job saner.

Introduction To Network Management Utilities

A network administrator must be able to use all the tools at his or her disposal in order to properly detect, analyze, and correct problems. It is important to know what you started with, how it's changing, how to expand it painlessly, and what to do when it fails. Gathering and analyzing data, known as baselining, will give you the foundation to measure the network's reaction to changes and stresses. Practicing preemptive troubleshooting regularly will help to prevent problems. Microsoft Windows NT includes such tools as the Performance Monitor, the Network Monitor, and the Event Viewer to assist in a smooth-running operation.

Baselining Your Network

Now that we've discussed what network management is, let's further examine baselining, an often overlooked but effective tool for general network administration and for troubleshooting problems. As we already mentioned, baselining is the practice of taking snapshots of your network and its various components at predetermined time intervals in order to establish a basis for trend comparison. Certain events are monitored and information about those events is recorded. You may then use the raw data to construct a graphical representation of the information so that it will be easier to compare and analyze trends, which simplifies your monitoring and planning tasks.

What should you baseline? Such classes as security, applications, and the system itself. The following tools are included with Windows NT operating system and can be used to assist in network monitoring.

Event Viewer

In the early days of networking, events on the server could be accurately judged by the sounds and various lights on the server. Things will never be that simple again, so Microsoft included the Event Viewer to log critical and informational events that affect the daily operation of your servers and your network environment. The Event Viewer can be an alert service for

critical events, such as loss of power, or an information service, which logs and records non-critical events, like low disk space on the volume or a failed logon attempt. The Event Viewer utility allows an administrator to view, sort, filter, and search for specific events in the log.

The Event Viewer can be used to monitor such activities as unsuccessful logon attempts, but you must enable logon auditing first. You can see a report of unsuccessful logon attempts with the Event Viewer's Security log.

Network Monitoring

Administrators monitor network performance and activities in order to detect bottlenecks (or to prevent them from happening), to improve performance based on the existing configuration, to forecast capacity requirements, and to avoid problems. One of the tools readily available and most widely used for monitoring events on the TCP/IP network is the Simple Network Management Protocol (SNMP).

In SNMP, clients load a special program, known as an agent, in memory. These agents monitor the network for "gets," "sets," and "traps." A special management program polls the agents and downloads the information from their management information base (MIB), where the information has been stored. Because various network-management services are used for different types of devices or for different network-management protocols, each service may have its own set of objects. The MIB refers to the entire set of objects that any service or protocol uses. The management program not only collects the data, but it also presents the information in the form of maps, graphs, and/or charts; it also packages the information to send to designated databases for analysis.

A community is a cluster of hosts to which the computer or device running the SNMP agent belongs. SNMP security allows the administrator to specify the communities and hosts a computer will accept requests from, and to specify whether to send an authentication trap when an unauthorized community or host requests information. Should the agent receive a request for information from an unidentified source, it will send a trap to the designated trap destination that indicates the failed authentication.

In an SNMP environment, the agent is the program loaded on a client machine or a networked device to monitor network traffic and to report events to the management program console.

Performance Management

Microsoft defines performance as time per transaction, where a transaction is a request or an action a user or a system wants to perform. We may envision performance as pure, raw power and speed; if you notice the response, it's too slow! System bottlenecks, such as inadequate bandwidth, slow NICs, slow server buses, or poor hard disk subsystems, may affect performance. Too much happening at once—too many processes for the CPU, too much data for the buffers, or too many transactions for both—may also influence performance. Excessive paging, disk thrashing, high utilization percentages, and sluggish server response will result. Performance tuning is the fine art of identifying these bottlenecks, correcting them in a non-intrusive manner, and moving on to identify the next bottleneck.

Performance Monitor charts historical as well as realtime performance data to identify both trends over time and bottlenecks in the system. It also monitors the effects of system or configuration changes, and determines system capacity limits. Four views are available in the Windows NT Performance Monitor:

- Chart Realtime as well as historical; might be useful to analyze why an application is performing poorly, to discover intermittent problems, or to inform you where to increase capacity.
- Alert Tracks up to 1,000 alerts; notifies you when a counter is outside the range of permitted values; selected by the administrator.
- Log Historical only; instrumental in capacity planning.
- Report Realtime view of performance of selected counters in a columnar format.

You can monitor numerous items. Each object that you can monitor contains subcategories, called counters. Performance Monitor actually reports on the counters, instead of the objects directly, in all views except Log view. Here are the objects that can be measured with Performance Monitor:

- Cache
- Logical disk
- Memory
- Objects
- Physical disk

- Process
- Processor
- System
- Thread
- Network-related objects
- Printers

Through performance monitoring, the network administrator can identify bottlenecks and gauge the results of network changes.

Preemptive Troubleshooting Through Preventative Maintenance

Normally, we would include in our annual budget money for auto, house, and life insurance. We think nothing of having our vehicles and household items regularly serviced and maintained. We may visit our family physician annually for general checkups. Likewise, we should budget time and money to regularly maintain and check up on our network systems. There are many simple but effective ways to proactively manage your assets.

A network file server is not a PC on steroids, but many of the same preventative maintenance principles may apply. Although Windows NT is generally self-tuning, that only goes so far. Regular, documented activities such as virus checking/detection and cleaning, disk defragmentation, disk checking (CHKDSK), and deletion of temporary files help preserve disk space that is necessary for performance and general health. The AT command can be very helpful in automating a lot of these routine checkups. You can use the tools supplied with the NOS, or there are many third-party products available. Some may be useful in keeping tabs on disk quotas—limiting runaway processes or disk hogs and providing accountability. You should, however, make sure that any add-on products are certified to be compatible with your NOS and hardware.

Be aware that corrupted or virus-infected files are usually backed up in their corrupted state, so check those restore processes as part of your routine maintenance procedures. Add to your baseline measurements by checking for such things as free disk space, number of user and group accounts, and backup times. We were able to pinpoint a WAN problem many times

just by noticing the backup time had increased dramatically. Recording disk-space usage and user accounts will help you plan for growth. It is wise to keep a log book to record these activities and their outcomes by date. By keeping things neat, orderly, and accounted for, you may prevent many common problems.

Prevention Through Planning

You have established the need for a network, perhaps through an organized process as a consultant for a client firm, through joint development efforts with a team of your fellow employees, or just because of circumstances outside your control. As part of the planning process, you then proceed to identify the benefits and set priorities for those outcomes that are viable. As you do this, you must take into account the human factors involved in a network installation, because these can affect the system just as much as hardware or software.

When you are in the pre-planning stage, you should consider the health of the entire network: Don't forget to include provisions for training, documentation, and transitioning. Consider such issues as your company's history (how the organization responds to change), projected growth, operating policies (how difficult it will be to acquire what you need), working environment, office systems and procedures (who will provide frontline and backup support), and the people who will be using the final product (what kinds of training will you require).

Contingency planning involves identifying the costs of a failure and the likelihood that any one component will fail. It may be easy to identify the cost of replacing or repairing a lost server, gateway, hub, router, or their individual components. It is much more difficult, however, to measure the cost of downtime in terms of lost sales, competitiveness, customer goodwill, employee productivity and confidence, perishables, and contractual obligations.

When planning, keep in mind that you need to minimize a single point of failure in any system. That is, try to limit the components whose failure will result in the loss of the computer or the network. The components most likely to cause network downtime are failed servers, faulty or inadequate power systems, lack of climate control, faulty wiring, insufficient cabling, failed intermediate devices, lost telecommunications, and buggy software. For each of these components, consider fault tolerance, redundancy, additional vendor support, and quick repair or replacement.

Standardization

Standardization is another technique of smart network administration. By limiting the number of components in a system, you will also limit the complexity. NICs, gateways, routers, hubs, servers, access devices, and so on, all carry a certain amount of excess baggage, in the form of documentation, staff technical training, software drivers and firmware, and spares and replacement parts.

Another technique is to centralize as many of the events associated with network connectivity as you can, including centrally accessible logon scripts, profiles, and policies. Using WINS and DNS servers for browsing services or centrally located HOSTS and LMHOSTS files reduces the amount of administrative overhead substantially. Another helpful tool that is not widely deployed in heterogeneous shops is Dynamic Host Configuration Protocol (DHCP) services. Not only can DHCP control the assignment of IP addresses, but it also lends some administrative control through the use of DHCP options, configured using the DHCP Manager, and makes the movement of TCP/IP clients much easier.

Finally, even though it may cost a little more up front, there is something to be said about purchasing industry-standard components and devices. Not only will doing so reduce administrative and technical burdens, but you will have a greater chance of choosing items from the Microsoft Hardware Compatibility List. This is extremely important in the real world. You may have purchased the highest level of support agreement that exists, but if you call for technical support on products that aren't on that list, you will be refused in some way or another.

Backing Up

The first line of defense against a network disaster is a reliable, current backup. Backups are also useful for archiving seldom-used data that must be saved for legal or historical purposes, allowing the administrator to recover that disk space for other uses. Clearly and completely document your backup system, policies, and procedures. Depending on the nature of your organization, backups may be included in an audit or needed in case of an extreme emergency. It's also wise to keep a secondary backup system offsite in "hot standby" mode, ensuring the restoration of data in a catastrophe.

Even in the most fault-tolerant environment, you still need backups to protect your data from the following:

- User errors
- Sabotage and virus infections
- Software malfunctions
- Catastrophes
- Disk corruption

Data recovery will be easier and less time-consuming if your backup operations are based on good planning, reliable, high-quality hardware, and consistent, easy-to-use software. You must make sure the system you choose will both back up the type of data you have in the available amount of time and restore it reliably.

Your primary defense against data loss is the implementation of an effective, efficient backup system with an appropriate schedule and methodology. Use fault-tolerant systems, such as RAID 1 or RAID 5, in addition to—not at the exclusion of—data backups.

In Chapter 9, you learned about the different backup strategies. Now let's consider various backup approaches. The two extremes you need to consider when planning an appropriate backup strategy are the small, simple network with less than 10 computers and one with high-powered servers that store huge amounts of data that need to be available on a twenty-four-hour-a-day, seven-day-a-week basis. Here are some guidelines for the small networks:

- Test your backup capability frequently and record the results. Adjust your procedures as needed.
- Store tapes in a safe environment—offsite—and have trusted individuals maintain them.
- Ensure the backup media will hold the amount of data to be backed up.
- Ensure the backup system will cooperate with the computer in which it's installed.
- Standardize all of your backup systems with the same media, hardware, and software.
- Verify that the media works in all the backup devices.
- Test your restoration capability frequently and record the results. Make adjustments as necessary.

- Implement a standard labeling scheme for the tapes and logs, which includes, at minimum, date, type of backup, amount of data backed up, and server backed up.
- Make sure all details of the backup are documented in a log, and send a copy of the log offsite at regular intervals.
- Rotate your media in a scheme that supports your organizational goals and objectives.
- Back up critical data and important servers, such as domain controllers and mission-critical application servers, on a daily basis.
- Test your backup and restoration capability frequently and record the results. (We cannot stress this enough!)

Circumstances are more difficult for larger networks, where the health and availability of the server are critical to the functions of the organizations. For large amounts of data, it is often difficult to back up in the allotted amount of time. If the server must be running and available 24 hours a day, you must choose backup software that can back up open or locked files. These types of software make a backup of the file's image, because you cannot really back up an open or locked file. Other creative solutions we've seen include:

- Disconnecting all users prior to backup and keeping them out until the backup has completed. In Windows NT Server, you can automate this task using the AT command.
- Pausing the Server service, which logically removes the server from the network.
- Ensuring all files are unlocked or closed, which usually requires cooperation of the application and/or programming team.
- Replicating the data to a duplicate server or extra volume that has no connected users, and backing up that machine. When choosing this method, make sure permissions and file attributes are replicated along with the data.

Security

It's important to plan to minimize the effects of human error or deliberate acts of sabotage, with the former being the most common. This usually involves a lot of common sense and a little diligence. Servers, as well as critical devices and peripherals, should be kept in an adequately cooled,

sufficiently powered environment that limits access. If anyone can walk up to your server, he or she can walk off with it or find a way to fool with it. Ensure that only trained, trusted individuals have access to those critical resources, either locally or remotely. This includes password protecting any server or device that can be remotely administered.

Other common-sense considerations include password-protected screen savers on servers, locked enclosures, diligent virus checking, and virus-detecting software that stays resident on users' desktops but doesn't interfere with the computer's operations.

One item that is often overlooked is a regular audit of security enforcement. Special software programs accomplish this, or a resourceful network administrator can make use of the tools at hand. As we have already mentioned, Windows NT includes such tools as the Event Viewer to assist in security auditing.

Finally, include security measures in your network plan. Determine what levels of restrictions allow your users to do their jobs without interference and undue burden but still maintain the security and integrity of your data. A complete network operating system allows the network administrator to determine and manage what the users can and cannot do. In Windows NT, this is accomplished through the use of user- and share-level security as well as through user profiles. Auditing makes sure that these levels of security are not compromised as changes occur in the network.

Upgrades

Information technology changes daily, promises the networking environment we all want, and renders a lot of what's installed obsolete. We upgrade to:

- Keep up with changing technology.
- Keep up with changing user needs.
- Incorporate new technologies to meet changing user needs.
- Prepare for growth and change.

Here are a few guidelines for when you are preparing to upgrade software or hardware, particularly on a critical server or device:

- Make sure your documentation is current and complete.
- Make sure you have two reliable, full backups of data, as well as system configurations.

- Be sure to keep a separate backup of critical files like Registries, boot partitions, and system files.
- Have Emergency Repair Disks current, tested, and handy.
- Test the upgrade as many times as possible before deploying it in a production environment.

Documentation

No one will ever know your network as well as you, especially the intricate ins, outs, and exceptions that lace every installation. Cover your assets! Document *everything*. Create a log book for every server and backup system, your users, network, cabling systems, vendor services, pertinent telephone numbers, scheduled maintenance, MIS policies and procedures, troubleshooting tips, escalation procedures, and WAN diagrams—and maintain detailed information about your software. This is your second line of defense in the disaster planning and recovery process and your first reference source when troubleshooting problems.

There is a wide variety of vendor-supplied and third-party documentation products available for every NOS and every system's individual needs, but you can usually achieve the most effective documentation through a combination of effective tools and due diligence on the part of the MIS staff. The documentation process should begin with the conception phase and become a routine part of system administration. As part of the documentation process, include such information as where the documentation is stored, who has access, how often it should be updated, and what is included in the documentation process itself.

Training

If your users can't utilize your network effectively, it is useless to them. If you and your staff lack the proper skill sets and knowledge to effectively monitor, maintain, and manage the network, the project is doomed to failure. Your organization must realize that the investment in training is an investment in success. It's as important as the network design and must become an integral part of planning and implementation.

Train the administrators and backup operators first, because their functions are critical to the inception of the networking system. You can accomplish this in many ways, but perhaps the most effective is a round of formal

classes, where personnel are trained at each phase of development, then allowed to cement their new knowledge with experience before taking on the next phase. This training should begin in the planning stage and continue throughout the lifetime of the network.

There are usually many available training options. Formal, instructor-led classes are offered in most metropolitan areas and network vendors are usually happy to assist their clients with training opportunities whenever possible. Vendors and user groups are good sources of practical, hands-on training as well as general knowledge, in-depth tips and techniques, and sharing of experiences. Time and time again, whenever we hear an especially knowledgeable speaker give a productive training session, the first question from the attendees will be about the source of the instructor's practical knowledge. Most will usually cite direct experience first, then credit a user community second.

On-site training may seem prohibitively expensive, but it may prove to be the most productive in the near term. This can be an option when time and resources are the constraining factors and usually offers a good return on the investment. Independent training companies and even large organizations like Microsoft are increasingly offering on-site as well as self-paced training.

Finally, look to the Web. Even prestigious universities are offering MIS degrees via the Internet, and training opportunities are boundless and cost effective, both in terms of time and money.

Although lack of time may be an obstacle to effective training, the most common barrier may be the corporation itself. It may be afraid to send MIS staff to training for fear of losing its investment as soon as the individual is certified, or the company may cite lost time and lack of adequate backup resources as reasons for not training end-users. It should be stressed that rewarding, long-term gain will definitely compensate for minor, short-term losses.

Troubleshooting Networks

The following sections detail some specifics on how to troubleshoot your network. Common areas to consider when troubleshooting include: how to go about troubleshooting (methodology), as well as special tools and resources that can be used for troubleshooting purposes.

Methodology

Network troubleshooting shares a lot of the same principles as the scientific method: A five-step, structured approach will usually lead to problem resolution. First, set the problem's priority by determining its impact. In most situations, you will be fighting many fires at once. Second, collect as much information as possible about the obvious as well as the not so obvious. Question users, employ all the available tools, and turn to special resources for help. Next, develop a list of all possible causes and conduct tests to isolate them. Finally, identify the solution by the process of elimination.

In general, to troubleshoot a problem, it is best to begin with a series of standard questions. Your first question should always be: "Did it ever work correctly?" Next ask: " When did it last perform satisfactorily?" And finally, "What has changed since then?" (This is where diligent documentation efforts will pay off in platinum.) Other useful questions include: "what works?"; "what doesn't work?"; "how are these items related?"; and "whom and what has this problem affected?"

If you don't have time to stop, gather information, and study a problem, then you have no choice but to rely on well-documented, well-practiced procedures for problem elimination. Just like a well-trained paramedic, your MIS staff should rehearse a series of escalation procedures often enough that their reactions to crisis situations become automatic. In these cases, emergency responses may not allow for scholarly contemplation until the system is functional and the crisis is resolved. It is best to plan early from the start for these types of situations.

Special Tools

It may be necessary to bring in special hardware or software when troubleshooting problems or determining performance bottlenecks. The following tools are very effective:

- Protocol analyzer Captures data packets on a network segment and provides detailed data about them, analyzes and simulates trends, and distinguishes protocols. Also known as a network analyzer.
- Cable tester Detects cable breaks, shorts, faults, and distance limitations.
- Time-domain reflectometer (TDR) or an optical TDR A super cable tester, can also provide the location of the break, short, or fault, as well as lack of proper termination.

- Power monitor Can log fluctuations in electrical power.
- Oscilloscope Electronic measurement device that determines the amount of signal voltage (amperage) per unit of time for display on a monitor. Can detect shorts, cable bends or crimps, opens, or loss of signal power.
- A Volt/Ohm meter and/or Digital Volt Meter (DVM) Can be used to detect resistance in cables, terminators, and barrel connectors. Cables and barrel connectors should provide zero (or very little) resistance. Terminators for 10Base2 and 10Base5 networks should provide 50 Ohms of resistance. Components that display incorrect resistance should be replaced.

You must know the capabilities of each of these devices. In particular, the protocol (network) analyzer has the capability to capture and decode packets, perform trend analysis and simulation, and distinguish protocols. Most network monitors and cable-testing devices work at the Physical layer of the OSI model.

Support Resources

Access to online services, such as CompuServe and MSN, and to the Internet is essential for research and troubleshooting as well as for sources of the most current software and firmware updates. These services also offer the best in-road to technical support departments through email and public list servers. Vendors and technical consultants are usually very happy to participate in these types of communications because it allows them time to reply without pressure, and provides maximum exposure to their skills.

Subscriptions to most major industry periodicals are free for the qualified individuals who renew annually. Other types of subscriptions, such as to knowledge bases like TechNet, Cisco Support Solutions CD, or Novell Support Connections, should be maintained for all operating systems and hardware installed at your site. Subscriptions to third-party technical-reference services have saved many weekends for the short-handed network administrator. The absolute best, daily reference source and tool kit for Microsoft networks and operating systems will be the *Resource Kits*, which provide lots of detailed information, tools, and valuable insight; they are a lot of value for a small investment.

Outsourcing may be a viable option for your company. This affords many organizations access to resources on an "as-needed" basis, without the

burden of training and maintaining full-time, highly skilled staff. Outsourcing options can range from remote monitoring services and server administration to electronic software distribution and asset management. These organizations price their services to be competitive and they survive on volume, which translates into a wealth of experience and effective tools for the end-user, as well as a personnel resource that knows and is in tune with your particular environment and corporate culture. A trusted value-added reseller (VAR) or maintenance provider can usually be called upon for consulting services on a time-and-materials basis for special projects, freeing you for project management, research, or the skills that only you can provide the organization.

Troubleshooting Hardware Problems

You've learned some general troubleshooting techniques that should apply in most situations. Now let's turn our attention to some more specific categories of troubleshooting. The largest percentage of network makeup is hardware, so we can start with this category. Hard disks, NICs, hardware configurations, and startup problems fall into this category.

For network-related problems, it is usually best to start with preemptive planning. Ask the following questions in the design and implementation phase as well as when confronted with problems:

- Is the current or proposed hardware on the network operating system vendor's compatibility list?
- Are all pertinent drivers current? What access to drivers is available?
- Does the machine have enough of the appropriate memory?
- Is there enough free hard disk space to support storage needs?
- Is the CPU powerful enough?
- Are the buses compatible?
- What IRQs are available?

For current situations, check cabling: You can trace 95 percent of all network-related problems to cabling faults. Check for loose, lost, broken, or compromised cables and connections; proper cable lengths, resistance, and termination; and most importantly in elusive situations, electrical or magnetic interference.

Isolate the hardware and simplify its configuration as much as possible. For a quick determination of whether the problem is hardware or cabling, attach the PC directly to a port on the hub with an adapter cable known to be good. To determine hardware conflicts, remove all unnecessary cards from the PC and reinstall them one at a time until the problem occurs again. You can try to segment the network in order to troubleshoot one section at a time.

Troubleshooting Software Connection Problems

You should have cleared up or prevented 99 percent of your problems with proper planning, preventative maintenance, user training, painstaking documentation, and wizardry monitoring. Software-related problems are the final obstacle to a properly operating network system:

- Protocol mismatches
- Application conflicts or misconfiguration problems
- Accounting, security, and rights issues
- Client server/problems

Sometimes, the server you are trying to connect to isn't up. More often, however, the client simply isn't connecting to the network or isn't communicating with it properly. The client must be running at least one of the server's protocols: NetBEUI, TCP/IP, or NWLink. When Novell's NetWare is included in the network soup, the most common troubleshooting tip involves using the proper frame types. In a NetWare environment, the two devices attempting to communicate must be using the same frame type. The default frame type is 802.2. You can set this using the Advanced tab on the NWLink protocol's Properties sheet.

In TCP/IP networks, misspelling the computer's NetBIOS name is another common problem. In some cases, the FQDN may have been misspelled or the IP address mistyped in the DNS entry or HOSTS file. It may be that the WINS server is down and there is no LMHOSTS file accessible to you.

Finally, most problems are user-oriented: Did the user enter the correct password? Is the account locked? Does that user have an account on that server? Does that user have rights to access those files or that application?

The most effective way to configure the binding order of multiple transport protocols on a computer is to place the most frequently used protocol at the top of the binding order.

Handling Network Performance Problems

We've determined that bottlenecks somewhere in the system cause most performance problems, so performance tuning will involve continually finding the source of traffic congestion, relieving it, and moving on to the next problem. A lot like untangling the knots in a very long rope, relieving bottlenecks in one part of the system may cause others to occur elsewhere.

Again, start with the basic troubleshooting process of elimination. Ask yourself:

- Have I (or others) changed anything?
- Did this occur all at once or gradually?
- What new application or device has been added?
- At what rate have new users and machines been added to the network?
- Do my servers have enough disk space and RAM to do their jobs?
- Is the CPU operating at full capacity?

Performance tuning in a TCP/IP network may involve adjusting the send or receive window size or the network packet size. Reducing the receive or send window size may cause performance to degrade due to increased acknowledgments on the network. Reducing the receive window size is usually the safest route. Increasing the network packet size can reduce the number of reads and writes in a given time period and improve overall performance.

Practice Questions

Question 1

Your server has slowed down considerably over the last month and you suspect additional RAM may be needed due to a SQL installation that occurred at about the same time. What instrument would you use to confirm your suspicions?

- ❍ a. Network Monitor
- ❍ b. Performance Monitor
- ❍ c. TDR
- ❍ d. Cable tester

Answer b is correct. You would need Performance Monitor to determine whether or not the server had adequate RAM. The number of the page faults per second counter would be high in this case, which indicates the application can't find the requested data or code page in memory. Although you would use the Network Monitor to analyze traffic to and from the server, it would not indicate the need for more RAM. Therefore, answer a is incorrect. Answers c and d are incorrect because you use these devices to test the cabling.

Question 2

The XYZ Graphical Design firm just built a new, state-of-the-art facility to house its growing business. It has been using a combination of NetWare and Windows NT Servers on its network and all servers are on a 100 Mbps backbone. The rest of the company is using a 10 Mbps Ethernet. Things were just fine until the company changed janitorial services, and now the network is experiencing intermittent problems. What is the appropriate troubleshooting tool for this situation? [Check all correct answers]

- ❑ a. Advanced cable tester
- ❑ b. Protocol analyzer
- ❑ c. Sniffer
- ❑ d. TDR
- ❑ e. All of the above

The correct answer is e, all of the above, because these types of problems are generally related to a crimped cable somewhere in the system. In reality, the TDR would be the best tool, as it can actually pinpoint the location of the fault. A protocol analyzer would be able to determine the source of excessive collisions or beaconing. The sniffer is a third-party vendor protocol analyzer.

Question 3

Consider the following situation:

You work for a medical clinic that supports patients around the clock. You are installing a twisted-pair Ethernet in a new wing of the building. Some concern has been expressed about security due to recent events in the news, and the CFO suspects someone may be trying to intrude into the network. You check the Event Viewer's Security log daily but find no reports of unsuccessful logon attempts. What could be wrong?

- ❍ a. There are no unsuccessful logon attempts.
- ❍ b. Auditing was not enabled for that server.
- ❍ c. You have insufficient rights to view the Security log.
- ❍ d. The Security log doesn't record incidents of unsuccessful logon attempts.

The correct answer is b. In order for security auditing to be recorded in the Security log, auditing must be enabled on the server. Answer a is incorrect, because it's extremely rare to have a perfect set of users who never forget passwords. An unsuccessful logon attempt would be recorded in this case. If you are able to view the Security log on a daily basis, then you obviously have sufficient rights; therefore, answer c is incorrect. Answer d is incorrect because the Security log does record those events for which auditing has been enabled. Time stamps and computer names from which the unsuccessful attempt was made would help you track possible security breaches.

Question 4

A sliding window specifies how many packets should be received before an acknowledgment (ACK) is returned on a TCP/IP network. To improve network performance, how would you change the relationship of the send to receive packets?

- ❍ a. The send packet should be larger than the receive packet.
- ❍ b. The receive packet should be larger than the send packet.
- ❍ c. The send packet should be the same size as the receive packet.
- ❍ d. Packet size has no relationship to performance.

The correct answer is a. The send window's size indicates how many packets the sending computer can send before requesting an ACK; the receive window's size indicates how many packets can be received before sending an ACK. To be certain the sender is not idle while waiting for an acknowledgment, the send packet should be larger than the receive packet.

Question 5

You are the administrator for a small insurance office with a 27-node LAN. You currently have installed in your office a single 10BaseT Ethernet segment that runs a Windows NT application server and a Novell NetWare 3.12 file-and-print server, to which all networked devices are attached. You purchase four machines to add to the existing segment. After they are all installed and configured, one of the four machines cannot locate the file server. What is the most likely cause?

- ❍ a. You have exceeded the number of machines allowed on the segment.
- ❍ b. A router will be needed because of protocol mismatches between NetWare and Windows NT.
- ❍ c. The frame binding is incorrect.
- ❍ d. The frame type on the client PC is incorrect.

The correct answer is d. For two computers to communicate via NWLink, they must be using the same frame type. The frame type is the format used for header content and data information. Only one computer is affected, so it makes more sense to reconfigure that machine rather than the server and all the rest. The number of devices allowed on 10BaseT is 1,024, so answer a is wrong. There is no such thing as a protocol mismatch between NetWare and Windows NT, or a frame binding. Therefore, answers b and c are also incorrect.

Question 6

You are trying to connect to a Windows NT Server on your subnet and are receiving the error message that the file cannot be found. It worked yesterday. You check to make sure the WINS server is up and find out that the other users on your subnet can contact that server. You can PING the server's IP address. What is the most likely cause of the problem?

- ❍ a. An SMTP gateway is down.
- ❍ b. There is no LMHOSTS file.
- ❍ c. You've typed the name incorrectly.
- ❍ d. Your router is not configured as a BOOTP agent.

The most likely cause is answer c, human error. Answer a is incorrect because the SMTP gateway is used to link dissimilar email systems. Answer b is incorrect because the WINS server is operating correctly, so the LMHOSTS file is not needed. As the server is on your subnet, there is no need for a router, making answer d incorrect as well.

Question 7

You are installing a NIC in a new laptop and have connected it to the network. It cannot see the file server, and your floppy drive has stopped working. What is the mostly like cause of the problem?

- ❍ a. Protocol mismatch
- ❍ b. Faulty cabling
- ❍ c. IRQ mismatch
- ❍ d. NICs will not work in a laptop

The correct answer is c. Although your first response might be b, because cabling causes the greatest majority of network connectivity problems, the more likely cause is answer c. It is most likely that the NIC was preset to the same IRQ as the floppy drive. There are very sophisticated NICs for laptops; they usually fit in a PCMCIA slot.

Question 8

The auditing firm of Dewie, Cheatam & Howe has hired you to determine the cause of a problem on its network. Upon arriving, you question the client about the problem and discover it is related to performance degradation. What device would you use to determine if the problem is excessive broadcast traffic?

- ❍ a. Bridge
- ❍ b. Router
- ❍ c. Gateway
- ❍ d. Protocol analyzer

The correct answer is d. The protocol analyzer will be able to pinpoint the source of the broadcast storms. A router would be used to filter out broadcast traffic, so answer b would not be correct. A bridge would be used to segment network traffic but couldn't be used to filter broadcasts. A gateway would be used to connect dissimilar systems.

Question 9

Because its new operations in Las Vegas have been so successful, Dewie, Cheatam & Howe has decided to upgrade its network with a new accounting package. What should its first course of action be? [Check all correct answers]

- ❑ a. Document the current network.
- ❑ b. Come up with a deployment plan.
- ❑ c. Back up the servers.
- ❑ d. Create Emergency Repair Disks.

All answers are correct. The first action should be to produce a concise, detailed plan for deployment that takes into account user training, fault tolerance, and disaster recovery. Therefore, answer b is correct. But as part of the disaster recovery plan, items a, c, and d would also need to be carried out.

Question 10

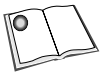
Which of the following statements is true about Simple Network Management Protocol (SNMP) agents?

- ❍ a. They isolate and resolve problems with broadcast storms.
- ❍ b. They monitor traffic and report the source of broadcast storms.
- ❍ c. They monitor, log, and audit ICMP messages.
- ❍ d. They monitor network traffic and behavior in key network components.

The correct answer is d. The SNMP agents loaded on the client devices would monitor network traffic and behavior for the key object and record them in the MIB. A management console would then poll the MIB for its information. A protocol analyzer would be used to isolate broadcast storms, and a router or similar device could be used to resolve problems due to broadcast storms, making answers a and b incorrect. ICMP is a maintenance protocol used to build route tables, assist in problem determination (PING and TRACERT), and adjust flow control to prevent router or link saturation, so answer c is incorrect.

Need To Know More?

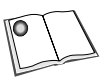
Chellis, James, Charles Perkins, and Matthew Strebe: *MCSE: Networking Essentials Study Guide, 2nd Edition*. Sybex Network Press, San Francisco, CA, 1998. ISBN 0-7821-2220-5. Chapter 12, "The Basics of Network Troubleshooting," contains many useful pointers as to how to successfully troubleshoot a network.



Microsoft Press: *Networking Essentials, 2nd Edition*. Redmond, WA, 1997. ISBN 1-57231-527-X. Unit 8, "Solving Network Problems," and Appendix C, "Network Troubleshooter," contain excellent coverage of the various topics contained within this chapter. There are also "Troubleshooter" exercises throughout the book's chapters that reinforce the chapter's topic.

Microsoft Press: *Windows NT Server Networking Guide*. Redmond, WA, 1996. ISBN 1-57231-344-7. Chapter 2, "Network Security and Planning," contains helpful information about security policies.

Microsoft Press: *Windows NT Server Resource Guide*. Redmond, WA, 1996. ISBN 1-57231-344-7. Part III, Chapter 8, is devoted to general troubleshooting and each individual chapter has a troubleshooting section particular to the chapter's topic. The Microsoft *Resource Kits* are designed with the network administrator in mind and are an excellent reference for test taking as well as daily use.



Search the TechNet CD (or its online version through www.microsoft.com) using the keywords "Performance Monitor," "Network Monitor," "advanced administration," "troubleshooting," and related terms. The Windows NT *Concepts and Planning Manual* also includes useful information on networking concepts.