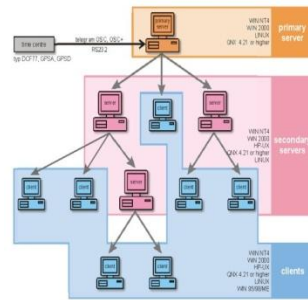


Chapter 14

Solving Network Problems



Objectives

- Describe the benefits of network management and planning
- Explain different approaches to network troubleshooting
- List the steps of the problem-solving process
- Explain the types of specialized equipment and other resources for troubleshooting
- Describe some measures to take in common troubleshooting situations



Preventing Problems with Planning and Documentation

- You solve network problems in one of two ways
 - Preventing problems through planning and management (called **preemptive troubleshooting**)
 - Repairing and controlling existing damage (called **troubleshooting**)
- Network management and troubleshooting should combine to form an overall network plan
 - Outline this plan in a comprehensive document
 - Establish policies/procedures that apply to network during planning stages; continue throughout its life



Backing Up Network Data

- Guidelines to formulate any backup plan
 - Determine what data to back up and how often
 - Develop a backup schedule that includes the type of backup to be performed, how often, and time of day
 - Identify people responsible for performing backups
 - Test your backup system regularly
 - Maintain a backup log listing what data was backed up, when the backup took place, who performed the backup, and which tapes were involved
 - Develop a plan for storing data after it has been backed up to tape



Setting Hardware and Software Standards

- To make HW and SW easier to manage, network components should follow established standards
 - When you define standards for desktop computers, establish configurations for several levels of users
 - Establish standards for networking devices (include supported manufacturers and OSs), and indicate which protocols and services should be used
 - Define standards for server configurations, document current server configurations, and establish guidelines for new server installations
 - Evaluate standards often—ideally, once per quarter



Establishing Upgrade Guidelines

- As an extension of hardware and software standards, also establish guidelines for upgrades
 - Vendors upgrade products and introduce new ones
 - If you establish guidelines in advance, you can handle upgrades more easily
 - Give your users advanced notice so that they know changes will take place
 - Disruptive upgrades shouldn't be carried out during normal working hours
 - “Pilot” new upgrades with technically astute users
 - Always formulate a **rollback plan**



Maintaining Documentation

- Documents you should include in any network plan
 - Network address list
 - Cable map
 - Contact list
 - Equipment list
 - Network history
 - Network map



Maintaining Documentation

- Documents you should include in any network plan (continued)
 - Networking hardware configuration
 - Policies and procedures
 - Server configuration
 - Software configuration
 - Software licensing
 - User administration



Performing Preemptive Troubleshooting

- Preemptive troubleshooting is costly but saves time when problems do come up, prevents equipment problems, and ensures data security
- The ISO identifies five preemptive troubleshooting network management categories
 - Accounting management
 - Configuration management
 - Fault management
 - Performance management
 - Security management



Practicing Good Customer-Relation Skills

- Build a relationship with your users so that they trust you and are more likely to give you pertinent information when there's a problem
 - Technically adept users are an excellent source of troubleshooting information
- All IT Departments should have guidelines that instruct personnel how to interact with users
 - Guidelines should include what questions to ask users, how to respond to irate users, how to respond to user questions, and how to follow general user communication etiquette guidelines



Using Network-Monitoring Utilities

- Network-monitoring utilities are long-term troubleshooting tools
 - Learn which statistics to monitor
 - Collect data over time to establish baseline
- Network-monitoring utilities gather the following types of information:
 - Events
 - System use statistics
 - System performance statistics



Using Network-Monitoring Utilities

- Information gathered can help:
 - Identify network devices that create bottlenecks
 - Provide information for forecasting growth and planning capacity requirements
 - Develop plans to improve network performance
 - Monitor events caused by SW or HW changes
 - Monitor trends in network traffic and utilization
- The Windows Performance Monitor monitors and tracks many different areas of server performance, and can monitor many events concurrently



Creating a Network Baseline

- A baseline is helpful for identifying daily network utilization patterns, possible bottlenecks, heavy use patterns, and protocol traffic patterns
- Using Performance Monitor and a baseline, you can often avoid potential network problems
 - Baseline can indicate whether a network needs partitioning, more file servers, or the increased speed of upgraded NICs and networking equipment
- Establish baseline over a period when no problems are evident on the network
- Baselines must be taken periodically



Monitoring with Simple Network Management Protocol

- TCP/IP's SNMP is an industry-standard protocol that most networking HW manufacturers support
- **Software agents** are loaded on each network device that SNMP manages
 - Agents monitor network traffic and device status, and store information in **MIB**
 - Management station communicates with agents and collects data stored in MIBs
 - Combines information and generates statistics
 - You can set thresholds for generating alert messages



Using Remote Monitoring for Advanced Monitoring

- **RMON** is an advanced networking monitoring protocol that extends the capabilities of SNMP
 - Two versions: RMON1 and RMON2
 - RMON1 is designed to capture data and collect statistics at the Data Link and Physical layers
 - RMON2 can collect and analyze traffic at the Network layer and higher layers
 - SNMP defines a single MIB type to collect network data, but RMON1 defines nine additional MIB types
 - RMON-capable devices contain SW agents (probes) that collect data and communicate with management station using SNMP



Approaches to Network Troubleshooting

- Different problems require different approaches
 - Sometimes it makes sense to just try a solution and see whether it works
 - Sometimes you can use a similar system as a working model, or you might have to buckle down and research the problem thoroughly
- In this section, you learn about different methods and circumstances in which some methods work and others do not



Trial and Error

- Can be used under the following conditions:
 - The system is newly configured (no data can be lost)
 - The system is not attached to a live network
 - You can easily undo changes
 - Other approaches would take considerably more time than a few trial-and-error attempts
 - There are few possible causes of the problem (helps you make a good educated guess at the solution)
 - No documentation and other resources are available to draw on to arrive at a solution more scientifically



Trial and Error

- If you determine that trial and error is the right approach for your problem, you should follow some guidelines:
 - Make one change at a time before testing the results
 - Avoid making changes that might affect the operation of a live network
 - Document the original settings of HW and SW before making changes
 - Avoid making a change that can destroy user data unless a known good backup exists
 - If possible, avoid making changes you can't undo



Solve by Example

- Solving by example: process of comparing something that doesn't work with something that does, and then making modifications to the nonfunctioning item until it performs like model
 - Easy and fast way to solve a problem; requires no special knowledge or problem-solving skills
 - General rules to follow
 - Use only when the working sample has a similar environment as the problem machine
 - Don't make configuration changes that cause conflicts
 - Don't make changes that could destroy data that cannot be restored



The Replacement Method

- Favorite among PC technicians
- Follow these rules:
 1. Narrow list of potentially defective parts down to one or two possibilities
 2. Make sure you have the correct part replacement
 3. Replace only one part at a time
 4. If your first replacement doesn't fix the problem, reinstall original part before replacing another part



Step by Step with the OSI Model

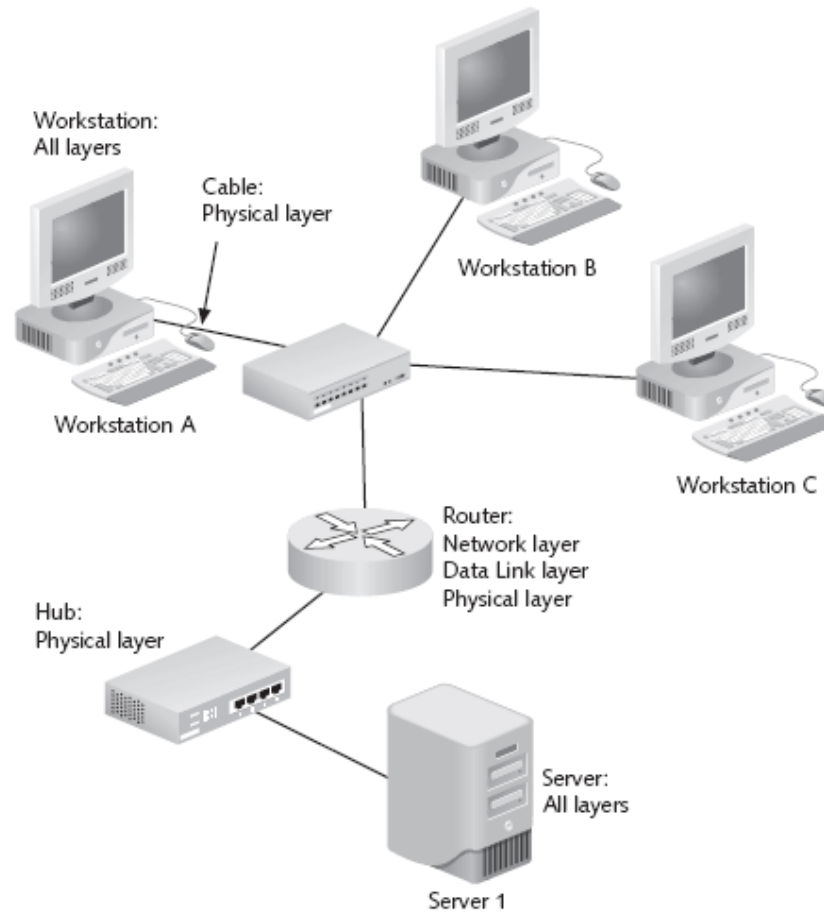


Figure 14-1 Troubleshooting with the OSI model



The Problem-Solving Process

- General framework for approaching problems
 1. Determine the problem definition and scope
 2. Gather information
 3. Consider possible causes
 4. Devise a solution
 5. Implement the solution
 6. Test the solution
 7. Document the solution
 8. Devise preventive measures



The Problem-Solving Process

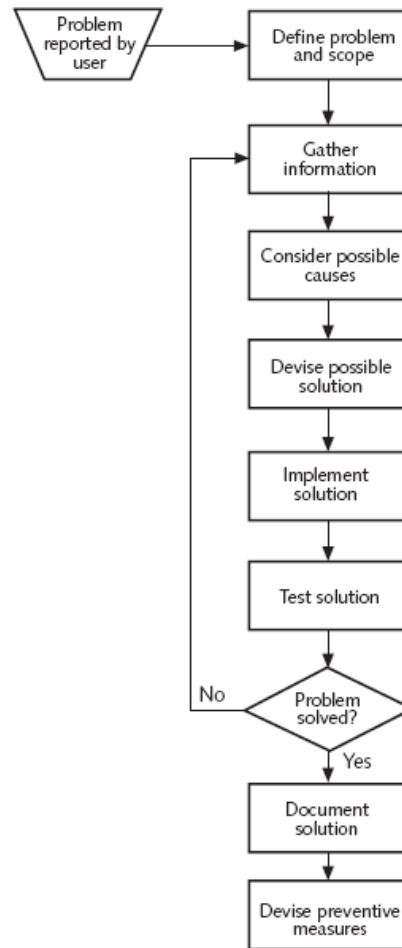


Figure 14-2 The problem-solving process



Step 1: Determine the Problem Definition and Scope

- Although this part of the troubleshooting process is more art than technical skill, there are some questions you can ask to start you on your way
 - Is anyone else near you having the same problem?
 - What about other areas of the building?
 - Is the problem occurring with all applications or just one?
 - If you move to a different computer, does the problem occur there as well?
- The goal of your questions is to determine a problem definition and scope



Step 2: Gather Information

- Use your user interview skills
 - Most of the initial information you get about a problem comes from users
 - Knowing what questions to ask and how to ask them is extremely important
 - Did it ever work?
 - When did it stop working?
 - Has anything changed?
 - Never ignore the obvious
 - Define how it's supposed to work



Step 3: Consider Possible Causes

- From symptoms and other information gathered, consider what could be the cause of the problem
- Experience is invaluable in this step
- As you proceed through this step, you'll probably gather more information
- Goal is to create a checklist of possible things that could have gone wrong to cause the problem



Step 4: Devise a Solution

- Before devising a solution consider the following:
 - Is the identified cause of the problem truly the cause, or is it just another symptom of the true cause?
 - Is there a way to adequately test proposed solution?
 - What results should the proposed solution produce?
 - What are the ramifications of the proposed solution for the rest of the network?
 - Do you need additional help to answer some of these questions?



Step 4: Devise a Solution

- Before you implement the solution, you must be prepared for the possibility that it could make things worse than the existing problem
- Depending on the scope of the problem and solution, you might need to do the following:
 - Save all network device configuration files
 - Document and back up workstation configurations
 - Document wiring closet configurations, including device locations and patch cable connections
 - Conduct a final baseline to compare new and old results if a rollback becomes necessary



Step 5: Implement the Solution

- If you have done a good job with the first steps, the implementation step should go fairly smoothly
 - In step 5, you:
 - Create intermediate testing opportunities
 - Design the implementation so that you can stop and test it at critical points
 - Inform users of your intentions
 - Give your users time to schedule network downtime
 - Put the plan into action
 - Take notes about every change you make



Step 6: Test the Solution

- It's 3:00 a.m. and you're finished with the upgrade. Time to go home, right?
 - Wrong. It's time to test your implementation as a whole
- Testing should attempt to emulate a real-world situation as closely as possible
- If you're testing a major network upgrade, you have probably already tested end-to-end connectivity
 - Now you need to put some stress on the network



Step 7: Document the Solution

- After solving the problem, you must take the notes made during the implementation and testing steps and turn them into a cohesive document
 - This step is as important as any previous step
- Documentation should include everything pertinent to the problem, such as the problem definition, the solution, the implementation, and the testing
 - Including this information in your overall network plan may be advisable



Step 8: Devise Preventive Measures

- After you have solved a problem and documented it, you should do everything you can to prevent that problem or similar problems from recurring
- Devising preventive measures is proactive rather than reactive network management
- If you let the problem come to you, it's always far more serious than if you had nipped it in the bud before it caused serious productivity issues



Making Use of Problem Solving Tools

- This section covers tools available for troubleshooting, monitoring, and documenting your network
- Each tool has its place; experience will tell you what's appropriate for different situations



Experience

- Make the most of your experience
 - Keep a journal of your experiences
- If it happened once, it will happen again
 - Due to standardized HW and SW, obscure looking problems will likely show up again
- Use your colleague's experience
 - You may put them on an e-mail distribution list
- Use experience from manufacturer's tech support
 - Best time to call technical support is when you have a specific error number or message that you can report to the manufacturer



The World Wide Web

- Useful Web resources
 - Manufacturers' knowledge bases or **FAQs**
 - When you're researching a problem, you should be as specific as possible
 - Drivers and updates in manufacturers' sites
 - Read the installation guide or Readme.txt file before installing OS updates
 - Online support services and newsgroups
 - e.g., Experts Exchange (www.experts-exchange.com)
 - Online periodicals
 - e.g., LAN Magazine, eWeek, Network Computing, etc.



Network Documentation

- Good network documentation can mean the difference between a five-minute fix and hours, or even days, of troubleshooting
- Document everything that's important to installing, maintaining, and troubleshooting the network
- Your documentation should read like a user's manual for network administrators



Network Topology

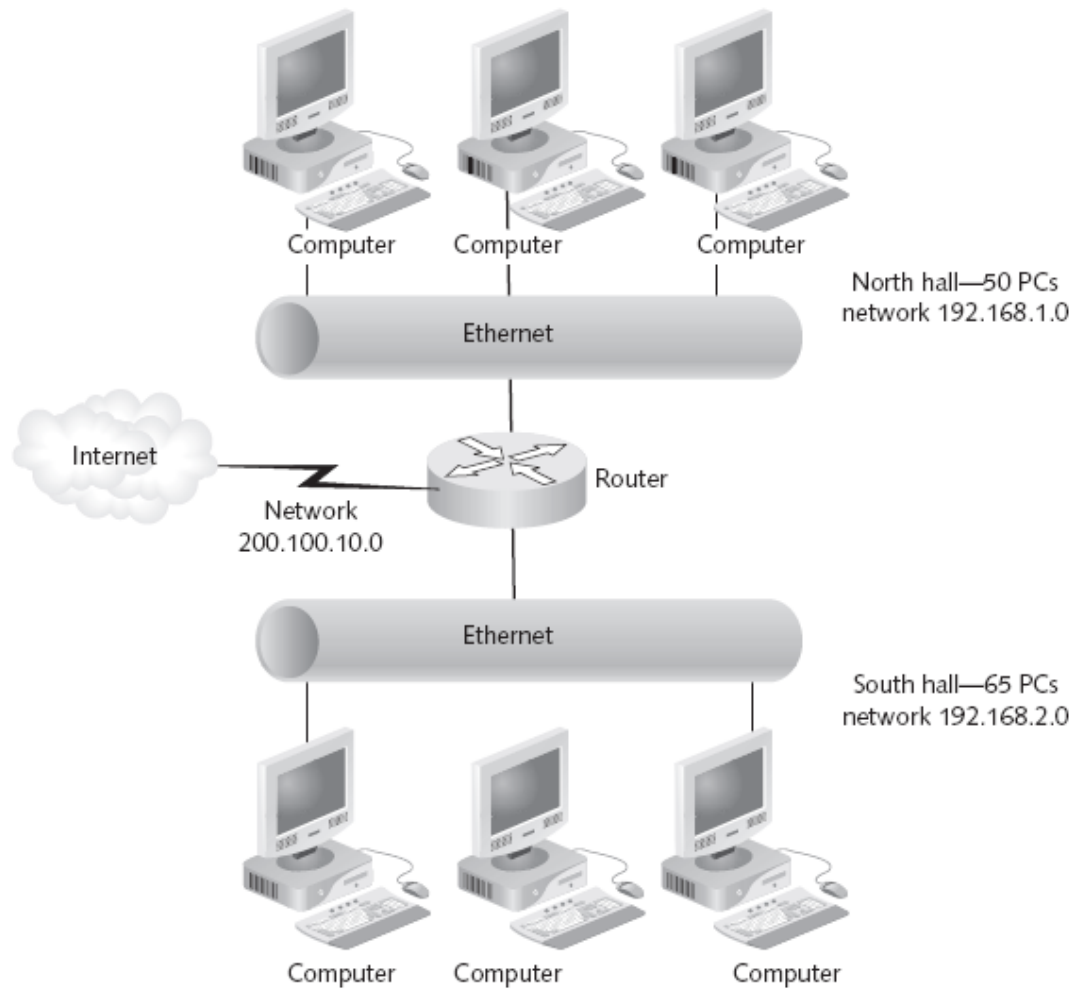


Figure 14-3 A logical network topology



Network Topology

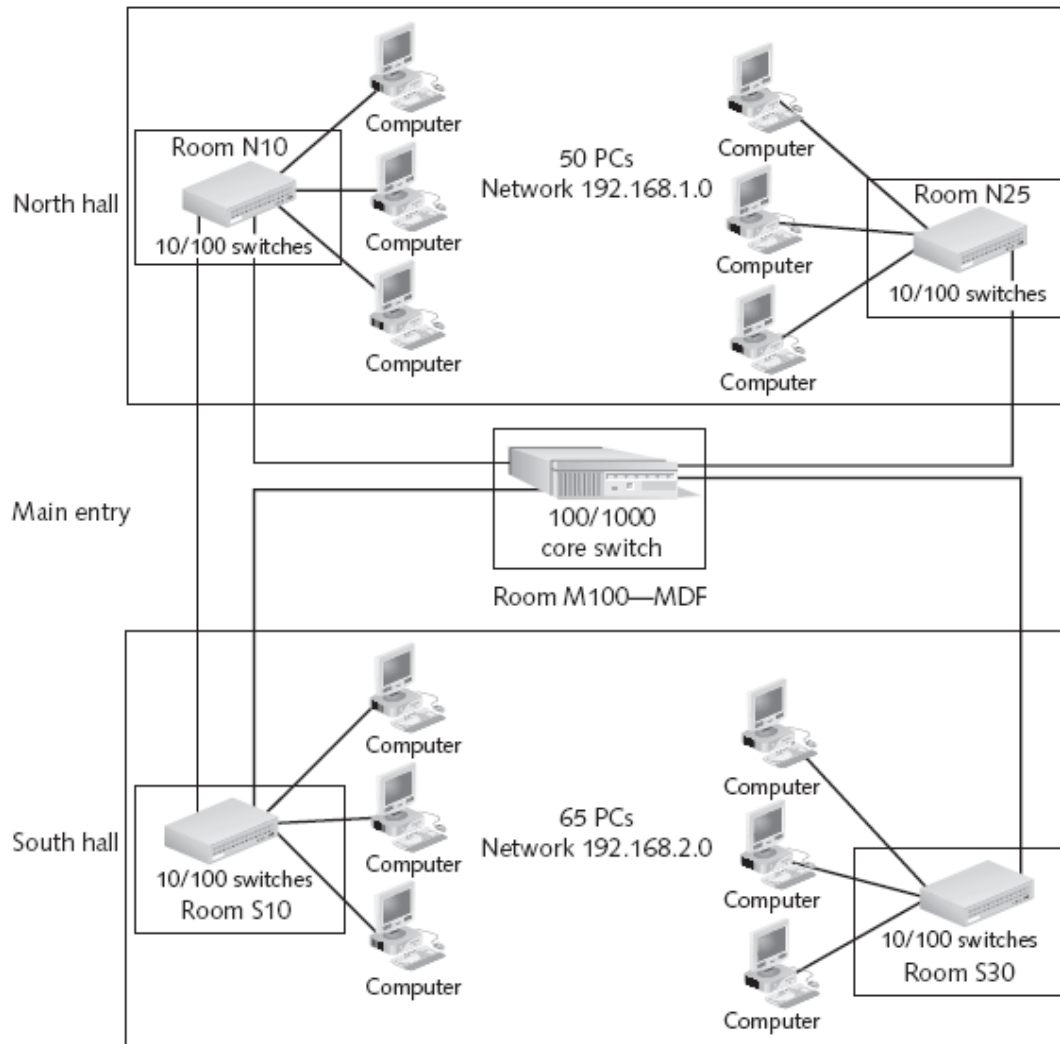


Figure 14-4 A physical network topology



Internetworking Devices

- Internetworking devices require different levels of documentation, depending on the equipment
 - Simple hubs require the least information, for example, whereas routers normally require the most
 - Besides including them in the network topology documents, you should list them in tabular form



Internetworking Devices

Table 14-1 Network equipment list: switches

Switch Model/ Serial #	Location	IP Address	MAC Address	# Ports/# Free
Cisco 2950/ 2117760	Room N10	192.168.1.240/24	00000cab3546	24/0
Cisco 2950/ 2117761	Room N25	192.168.1.241/24	00000cab3547	24/0
Bay 28115	Room S10	192.168.2.240/24	000003f25567	24/4



Additional Tools for Network Troubleshooting

- Experience, colleagues, the Web, phone support, and documentation are all fine resources for network support and troubleshooting
 - Sometimes, however, the only place you can get the information you need is from your own network
 - Many networking problems occur at lower layers of the OSI model, where they are often difficult to troubleshoot
 - Fortunately, there are tools for diagnosing these problems



Digital Voltmeter (DVM)

- A **digital voltmeter (DVM)**, also called a volt-ohm meter (VOM), is the most basic electrical measuring device
- As used in network troubleshooting, it measures a cable's resistance and determines whether a cable break occurred
- Can also be used to identify short circuits
 - A **short circuit** (or short) prevents network traffic from traversing the cable and requires repair or replacement of that cable



Time-Domain Reflectometer (TDR)

- A **TDR**, like a DVM, can be used to determine whether there's a break or short in a cable
 - Measures the time it takes for signal to return and estimates how far down the cable the fault is located
 - A high-quality TDR can determine the location of a break within a few inches
 - TDRs are available for fiber-optic as well as electrical cables
 - TDR function is standard in most advanced cable testers
 - Use a TDR to document actual lengths of all cables



Basic Cable Testers

- **Basic cable testers** cost less than \$100
- Typically test only the correct termination of a twisted-pair cable or continuity of a coaxial cable
- Excellent tools for checking patch cables and testing for correct termination of a cable at the patch panel and jack
 - Can only verify that the cable wires are terminated in correct order or that there are no breaks in the cable
 - Can't check a cable for attenuation, noise, or other possible performance problems in your cable run



Advanced Cable Testers

- Advanced cable testers not only measure where a break is located in a cable, but can also gather other information, including a cable's impedance, resistance, and attenuation characteristics
- Function at both the Physical and Data Link layers of the OSI model
 - Can measure message frame counts, collisions, congestion errors, and beaconing information or broadcast storms
 - They combine the characteristics of a DVM, a TDR, and a protocol analyzer



Oscilloscopes

- **Oscilloscopes** are advanced pieces of electronic equipment that measure signal voltage over time
- When used with a TDR, an oscilloscope can help identify shorts, sharp bends, or crimps in a cable, cable breaks, and attenuation problems



Network Monitors

- **Network monitors** are software packages that can track all or part of the network traffic
 - By examining the packets sent across the network, they can track information such as packet type, errors, and traffic
 - Can collect this data and generate reports/graphs
 - E.g., Windows Server 2000/2003 Network Monitor, WildPacket's EtherPeek, Network Instruments Analyst/Probe, and Information Systems Manager Inc.'s PerfMan



Protocol Analyzers

- A protocol analyzer evaluates the network's overall health by monitoring all traffic
 - Also captures traffic and decodes received packets
 - Some combine HW and SW in a self-contained unit
 - May include built-in TDR to help determine the network's status
 - e.g., Network General Sniffer, Ethereal, WildPacket EtherPeek, Fluke Network Protocol Inspector
- Experienced network administrators rely on protocol analyzers to establish baselines for network performance and to troubleshoot their networks



Common Troubleshooting Situations

- This section outlines some common network problems and possible solutions



Cabling and Related Components

- Majority of networking problems occur at the Physical layer
- First, determine whether the problem lies with the cable or the computer
 - Make sure you use the same type of UTP cable throughout the network
 - Check cable lengths to make sure you don't exceed the maximum length limitation
 - If you suspect a faulty or misconfigured NIC, check the back of the card
 - If the NIC seems functional and you're using TCP/IP, use Ping to check connectivity to other computers



Power Fluctuations

- Power fluctuations in a building can adversely affect computers
- Verify that servers are up and functioning
 - Remind users that it takes a few minutes for servers to come back online after a power outage
- You may eliminate effects of power fluctuations by connecting devices to UPSs
- Some packages perform shutdowns automatically, eliminating the need for human intervention when power failures or severe power fluctuations occur



Upgrades

- When you perform network upgrades, remember three important points
 - Ignoring upgrades to new software releases and new HW can lead to a situation in which a complete network overhaul is necessary because many upgrades build on top of others
 - Keep current and do one upgrade at a time
 - Test any upgrade before deploying it on your production network
 - Don't forget to tell users about upgrades



Poor Network Performance

- When performance problems appear, answering these questions should help pinpoint the causes
 - What has changed since the last time the network functioned normally?
 - Has new equipment been added to the network?
 - Have new applications been added to computers?
 - Is someone playing electronic games in the network?
 - Are there new users on the network? How many?
 - Could any other new equipment, such as a generator, cause interference near the network?



Summary

- A key part of network management is planning and documentation, which includes setting backup schedules and guidelines, security guidelines, HW and SW standards, and upgrade guidelines
 - Also maintain complete set of network documentation
 - Network map, cable map, equipment list, server configuration, SW configuration, address list, user administration, SW licensing, contact list, network HW configuration, network history, and comprehensive list of policies and procedures
- Preemptive troubleshooting and customer-relation skills are critical in managing a network
- Many programs are available for network monitoring



Summary

- Many approaches to troubleshooting a problem
 - Problem-solving process involves eight steps, some of which must be repeated if a solution is hard to devise
- Many tools and resources are available to help you troubleshoot your network
- Network documentation helps with troubleshooting and facilitates upgrades and expansion
- Change is the most common cause of network problems

