Objectives

4.2 Identify types of configuration management documentation
- Wiring schematics
- Physical and logical network diagrams
- Baselines
- Policies, procedures, and configurations
- Regulations

4.3 Given a scenario, evaluate the network based on configuration management documentation
- Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures, and configurations to network devices and infrastructure
- Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed

4.4 Conduct network monitoring to identify performance and connectivity issues using the following:
- Network monitoring utilities (for example, packet sniffers, connectivity software, load testing, throughput testers)
- System logs, history logs, event logs

5.2 Explain the purpose of network scanners
- Packet sniffers
- Intrusion detection software
- Intrusion prevention software
- Port scanners

5.3 Given a scenario, utilize the appropriate hardware tools
- Cable testers
- Protocol analyzer
Introduction

This chapter focuses on two important parts of the role of a network administrator—documentation and wiring. Documentation, although not glamorous, is an essential part of the job. This chapter looks at several aspects of network documentation.

Administrators have several daily tasks, and new ones are cropping up all the time. In this environment, tasks such as documentation sometimes fall to the background. This is when it is important to understand why administrators need to spend their valuable time sitting down writing and reviewing documentation. Having a well-documented network offers a number of advantages:

- **Troubleshooting**: When something goes wrong on the network, including the wiring, up-to-date documentation is an important reference to guide the troubleshooting effort. The documentation saves you money and time in isolating potential problems.
Training new administrators: In many network environments, new administrators are hired, and old ones leave. In this scenario, documentation is critical. New administrators do not have the time to try and figure out where cabling is run, what cabling is used, potential trouble spots, and more. Up-to-date information helps new administrators quickly see the network layout.

Contractors and consultants: Consultants and contractors occasionally may need to visit the network. This may be done to make future recommendations for the network or to add wiring or other components. In such cases, up-to-date documentation is needed. If it were missing, it would be much more difficult for these people to do their jobs, and more time and money probably would be required.

Recognizing the importance of documentation is one thing; knowing what to document and when to document it is another. This chapter looks at types of management documentation and how network administrators use documentation.

Documentation Management

Quality network documentation does not happen by accident; rather, it requires careful planning. When creating network documentation, you must keep in mind who you are creating the documentation for and that it is a communication tool. Documentation is used to take technical information and present it in a manner that someone new to the network can understand. When planning network documentation, it is important to decide what you need to document.

NOTE

Write it down Imagine that you have just taken over a network as administrator. What information would you like to see? This is often a clear gauge of what to include in your network documentation.

All networks differ, and so does the documentation required for each network. However, certain elements are always included in quality documentation:

Network topology: Networks can be complicated, so if someone new is looking over the network, it is important to document the entire topology. This includes both the wired and wireless topologies used on the network. Network topology documentation typically consists of a diagram or diagrams labeling all critical components used to create the network. These diagrams include such components as routers, switches, hubs, gateways, and firewalls.
Wiring layout: Network wiring can be very confusing. Much of it is hidden in walls and ceilings, making it hard to know where the wiring is and what kind is used on the network. This makes it critical to keep documentation on network wiring up to date.

Server configuration: A single network typically uses multiple servers spread over a large geographic area. Documentation must include schematic drawings of where servers are located on the network and the services each provides. This includes server function, server IP address, operating system (OS), software information, and more. Basically, you need to document all the information you will need to manage or administer the servers.

Network equipment: The hardware used on a network is configured in a particular way—with protocols, security settings, permissions, and more. Trying to remember these would be a difficult task. Having up-to-date documentation would make it easier to recover from a failure.

Key applications: Documentation also includes information on all the key applications used on the network, such as up-to-date information on their updates, vendors, install dates, and more.

Detailed account of network services: Network services are a key ingredient in all networks. Services such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Remote Access Service (RAS), and more are an important part of documentation. You should describe in detail which server maintains these services, the backup servers for these services, maintenance schedules, how they are structured, and more.

Network procedures: Finally, documentation should include information on network policy and procedures. This includes many elements, ranging from who can and cannot access the server room, to network firewalls, protocols, passwords, physical security, and so on.
**Wiring Schematics**

Network wiring schematics are an important part of network documentation, particularly for midsize to large networks, where the cabling is certainly complex. For such networks, it becomes increasingly difficult to visualize network cabling and even harder to explain it to someone else. A number of software tools exist to help administrators clearly document network wiring in detail.

Several types of wiring schematics exist. They can be general, as shown in Figure 10.1, or they can be supplemented with the details found in Table 10.1, as shown in Figure 10.2.

![Figure 10.1: A general wiring schematic.](image)
FIGURE 10.2 A wiring schematic that has a corresponding detail table.
Table 10.1  Wiring Schematic Details

<table>
<thead>
<tr>
<th>Cable</th>
<th>Description</th>
<th>Vendor</th>
<th>Installation Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cat5E 350MHz nonplenum-rated CMP cable</td>
<td>King Wiring 350-777-5656 Purchased by Mike Harwood January 2009.</td>
<td>Cable runs 50 feet from the MDF to IDF. Cable placed through ceiling and through a mechanical room. Cable was installed 01/15/2009, upgrading a nonplenum Cat5 cable.</td>
</tr>
<tr>
<td>2</td>
<td>Cat5E 350MHz nonplenum cable</td>
<td>King Wiring 350-777-5656 Purchased by Mike Harwood February 2008.</td>
<td>Horizontal cable runs 45 feet to 55 feet from IDF to wall jack. Cable 5E replaced Cat5 cable February 2008. Section of cable run through ceiling and over fluorescent lights.</td>
</tr>
<tr>
<td>3</td>
<td>Category 5E UTP cable</td>
<td>King Wiring 350-777-5656 Purchased by Mike Harwood June 2007.</td>
<td>All patch cable connectors were attached in house. Patch cable connecting printer runs 45 feet due to printer placement.</td>
</tr>
<tr>
<td>4</td>
<td>8.3-micron core/125-micron cladding single mode</td>
<td>King Wiring 350-777-5656 Purchased by Mike Harwood June 2007.</td>
<td>Connecting fiber cable runs 2 kilometers between the primary and secondary buildings.</td>
</tr>
</tbody>
</table>

Figures 10.1 and 10.2 provide a simplified look at network wiring schematics. Imagine how complicated these diagrams would look on a network with one, two, or even six thousand computers. Quality network documentation software makes this easier; however, the task of network wiring can be a large one for administrators. Administrators need to ensure that someone can pick up the wiring documentation diagrams and have a good idea of the network wiring.

**EXAM ALERT**

Reading schematics and determining where wiring runs is an important part of the administrator’s role. Expect to see a schematic on your Network+ exam.
Troubleshooting Using Wiring Schematics

Some network administrators do not take the time to maintain quality documentation. This will haunt them when it comes time to troubleshoot some random network problems. Without any network wiring schematics, the task will be frustrating and time-consuming. The information shown in Figure 10.2 might be simplified, but it is possible using that documentation to evaluate the network wiring and make recommendations. In the hypothetical information provided in Figure 10.2 and Table 10.1, several potential problems with the network wiring exist. Any administrator could walk in and review the network documentation and isolate the potential problems. Now it's your turn. Can you find some problems in those schematics?

Need a hint? Cable 1 runs through the ceiling and a mechanical room and is not plenum-rated. This could cause interference for a regular UTP cable. Cable 2 has sections running through the ceiling and over fluorescent lights. In this case the cable needs to be shielded somehow. Perhaps STP (shielded twisted pair) needs to be used. Finally, Cable 3 might be a problem. The cable connectors were attached in house, meaning that some of the cables may not be made as well as cable purchased with connectors attached. There may be intermittent problems that can be traced to a poorly made cable.

EXAM ALERT

When looking at a wiring schematic, pay close attention to where the cable is run and the type of cable being used. If a correct cable is not used, there could be a problem.

NOTE

Network wiring schematics are a work in progress. Although changes to wiring do not happen daily, they do occur when the network expands or old cabling is replaced. It is important to remember that when changes occur to the network, the schematics and their corresponding references have to be updated to reflect the changes. Out-of-date schematics can be frustrating to work with.

Physical and Logical Network Diagrams

In addition to the wiring schematics, documentation should include diagrams of the physical and logical network design. Recall from Chapter 1, “Introduction to Networking,” that network topologies can be defined on a physical or logical level. The physical topology refers to how a network is physically constructed—how it looks. The logical topology refers to how a network looks to the devices that use it—how it functions.
Network infrastructure documentation isn’t reviewed daily; however, this documentation is essential for someone unfamiliar with the network to manage or troubleshoot the network. When it comes to documenting the network, you need to document all aspects of the infrastructure. This includes the physical hardware, physical structure, protocols, and software used.

**EXAM ALERT**

Physical or logical For the Network+ exam you should be able to identify a physical and logical diagram. You need to know the types of information that should be included in each diagram.

The physical documentation of the network should include the following elements:

- **Cabling information**: A visual description of all the physical communication links, including all cabling, cable grades, cable lengths, WAN cabling, and more.
- **Servers**: The physical network diagram includes the server names and IP addresses, types of servers, and domain membership.
- **Network devices**: The physical diagram includes the location of the devices on the network. This includes the printers, hubs, switches, routers, gateways, and more.
- **Wide area network**: The physical network also includes the location and devices of the WAN network and components.
- **User information**: The diagram might include some user information, including the number of local and remote users.

As you can see, many elements can be included in the physical network diagram. Figure 10.3 shows a physical segment of a network.

Networks are dynamic, and changes can happen regularly, which is why the physical network diagrams have to be updated as well. Networks have different policies and procedures on how often updates should occur. A rule of thumb is that the diagram should be updated whenever significant changes to the network occur, such as the addition of a bridge, a change in protocols, or the addition of a new server. These changes impact how the network operates, and the documentation should reflect the changes.
Document change  There are no hard and fast rules about when to change or update network documentation. However, most administrators will want to update whenever functional changes to the network occur.

The logical network refers to the direction in which data flows on the network within the physical topology. The logical diagram is not intended to focus on the network hardware but rather on how data flows through that hardware. In practice, the physical and logical topologies can be the same. In the case of the bus physical topology, data travels along the length of the cable from one computer to the next. So the diagram for the physical and logical bus would be the same.

This is not always the case. For example, a topology can be in the physical shape of a star, but data is passed in a logical ring. The function of data travel is performed inside a switch in a ring formation. So the physical diagram appears to be a star, but the logical diagram shows data flowing in a ring formation from one computer to the next. Simply put, it is difficult to tell from looking at a physical diagram how data is flowing on the network.

In today’s network environments, the star topology is a common network implementation. Ethernet uses a physical star topology but a logical bus topology. In the center of the physical Ethernet star topology is a switch. It is what happens inside the switch that defines the logical bus topology. The switch passes data between ports as if they were on an Ethernet bus segment.
In addition to data flow, logical diagrams may include additional elements, such as the network domain architecture, server roles, protocols used, and more. Figure 10.4 shows how a logical topology may look in the form of network documentation.

![Logical Topology Diagram](image)

**NOTE**

Logical topology The logical topology of a network identifies the logical paths that data signals travel over the network.

**Baselines**

Baselines play an integral part in network documentation because they let you monitor the network's overall performance. In simple terms, a **baseline** is a measure of performance that indicates how hard the network is working and where network resources are being spent. The purpose of a baseline is to provide a basis of comparison. For example, you can compare the network’s performance results taken in March to results taken in June or from one year to the next. More commonly, you would compare the baseline information at a time when the network is having a problem to information recorded when the network was operating with greater efficiency. Such comparisons help you determine if, in fact, there has been a problem with the network, how significant that problem is, and even where the problem lies.
To be of any use, baselining is not a one-time task; rather, baselines should be taken periodically to be able to provide an accurate comparison. You should take an initial baseline after the network is set up and operational, and then again when major changes are made to the network. Even if no changes are made to the network, periodic baselining can prove useful as a means to determine if the network is still operating correctly.

All network operating systems (NOSs), including Windows, Mac OS, UNIX, and Linux, have built-in support for network monitoring. In addition, many third-party software packages are available for detailed network monitoring. These system-monitoring tools provided in a NOS give you the means to take performance baselines, either of the entire network or for an individual segment within the network. Because of the different functions of these two baselines, they are called a system baseline and a component baseline.

To create a network baseline, network monitors provide a graphical display of network statistics. Network administrators can choose a variety of network measurements to track. They can use these statistics to perform routine troubleshooting tasks, such as locating a malfunctioning network card, downed server, or denial-of-service attack.

Collecting network statistics is a process called capturing. Administrators can capture statistics on all elements of the network. For baseline purposes, one of the most common statistics to monitor is bandwidth usage. By reviewing bandwidth statistics, administrators can see where the bulk of network bandwidth is being used. Then they can adapt the network for bandwidth use. If too much bandwidth is being used by a particular application, administrators can actively control its bandwidth usage. Without comparing baselines, however, it is difficult to see what is normal network bandwidth usage and what is unusual.

**EXAM ALERT**

Baselines For the Network+ exam, remember that baselines need to be taken periodically and under the same conditions to be effective. They are used to compare current performance with past performance to help determine if the network is functioning properly or if troubleshooting is required.
Policies, Procedures, Configurations, and Regulations

Well-functioning networks are characterized by documented policies, procedures, configurations, and regulations. Because they are unique to every network, policies, procedures, configurations, and regulations should be clearly documented.

Policies

By definition, policies refer to an organization’s documented rules about what is to be done, or not done, and why. Policies dictate who can and cannot access particular network resources, server rooms, backup tapes, and more.

Although networks might have different policies depending on their needs, some common policies include the following:

- **Network usage policy**: Who can use network resources such as PCs, printers, scanners, and remote connections. In addition to who can use these resources, the usage policy dictates what can be done with these resources after they are accessed. No outside systems will be networked without permission from the network administrator.

- **Internet usage policy**: This policy specifies the rules for Internet use on the job. Typically, usage should be focused on business-related tasks. Incidental personal use is allowed during specified times.

- **Email usage policy**: Email must follow the same code of conduct as expected in any other form of written or face-to-face communication. All emails are company property and can be accessed by the company. Personal emails should be deleted immediately.

- **Personal software policy**: No outside software should be installed on network computer systems. All software installations must be approved by the network administrator. No software can be copied or removed from a site.

- **User account policy**: All users are responsible for keeping their password and account information secret. All staff are required to log off and sometimes lock their systems after they are finished using them. Attempting to log on to the network with another user account is considered a serious violation.

- **Ownership policy**: The company owns all data, including users’ email, voice mail, and Internet usage logs, and the company reserves the right to inspect these at any time. Some companies even go so far as controlling how much personal data can be stored on a workstation.
This list is just a snapshot of the policies that guide the behavior for administrators and network users. Network policies should be clearly documented and available to network users. Often, these policies are reviewed with new staff members or new administrators. As they are updated, they are rereleased to network users. Policies are reviewed and updated regularly.

**EXAM ALERT**

Policy making On the Network+ exam, you may be asked about network policies. Network policies dictate network rules and provide guidelines for network conduct. Policies are updated and reviewed often and are changed to reflect changes to the network and perhaps changes in business requirements.

**Procedures**

Network procedures differ from policies in that they describe how tasks are to be performed. For example, each network administrator has backup procedures specifying the time of day backups are done, how often they are done, and where they are stored. A network is full of a number of procedures for practical reasons and, perhaps more importantly, for security reasons.

Administrators must be aware of several procedures when on the job. The number and exact type of procedures depends on the network. The network’s overall goal is to ensure uniformity and ensure that network tasks follow a framework. Without this procedural framework, different administrators might approach tasks differently, which could lead to confusion on the network.

Network procedures might include the following:

- **Backup procedures**: Backup procedures specify when they are to be performed, how often a backup occurs, who does the backup, what data is to be backed up, and where and how it will be stored. Network administrators should carefully follow backup procedures.

- **Procedures for adding new users**: When new users are added to a network, administrators typically have to follow certain guidelines to ensure that the users have access to what they need, but no more. This is called the principle of least privilege.

- **Security procedures**: Some of the more critical procedures involve security. Security procedures are numerous but may include specifying what the administrator must do in the event of security breaches, security monitoring, security reporting, and updating the OS and applications for potential security holes.
Network monitoring procedures: The network needs to be constantly monitored. This includes tracking such things as bandwidth usage, remote access, user logons, and more.

Software procedures: All software needs to be monitored and updated periodically. Documented procedures dictate when, how often, why, and for whom these updates are done.

Procedures for reporting violations: Users do not always follow outlined network policies. This is why documented procedures should exist to handle the violations properly. This might include a verbal warning upon the first offense, followed by written reports and account lockouts thereafter.

Remote-access procedures: Many workers access the network remotely. This remote access is granted and maintained using a series of defined procedures. These procedures might dictate when remote users can access the network, how long they can access it, and what they can access.

These represent just a few of the procedures that administrators must follow on the job. It is important that all of these procedures are well-documented, accessible, reviewed, and updated as needed in order to be effective.

Configuration Documentation

One other critical form of documentation is configuration documentation. Many administrators feel they could never forget the configuration of a router, server, or switch, but it happens more often than not. Although it's often a thankless, time-consuming task, documenting the network hardware and software configurations is critical for continued network functionality.

Two primary types of network configuration documentation are required—software documentation and hardware documentation. Both include all configuration information so that should a computer or other hardware fail, both the hardware and software can be replaced and reconfigured as quickly as possible.

The documentation is important because often the administrator who configured the software or hardware is unavailable, and someone else has to re-create the configuration using nothing but the documentation. To be effective in this case, the documentation has to be as current as possible. Older configuration information might not help.
Regulations

The terms regulation and policy are often used interchangeably; however, there is a difference. As mentioned, policies are written by an organization for its employees. Regulations are actual legal restrictions with legal consequences. These regulations are set not by the organizations, but by applicable laws in the area. Improper use of networks and the Internet can certainly lead to legal violations and consequences. The following is an example of network regulation from an online company:

“Transmission, distribution, uploading, posting or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, material kept in violation of state laws or industry regulations such as social security numbers or credit card numbers, and material that is obscene, defamatory, libelous, unlawful, harassing, abusive, threatening, harmful, vulgar, constitutes an illegal threat, violates export control laws, hate propaganda, fraudulent material or fraudulent activity, invasive of privacy or publicity rights, profane, indecent or otherwise objectionable material of any kind or nature. You may not transmit, distribute, or store material that contains a virus, ‘Trojan Horse,’ adware or spyware, corrupted data, or any software or information to promote or utilize software or any of Network Solutions services to deliver unsolicited e-mail. You further agree not to transmit any material that encourages conduct that could constitute a criminal offense, gives rise to civil liability or otherwise violates any applicable local, state, national or international law or regulation.”

EXAM ALERT
Regulations are the law For the exam and for real-life networking, remember that regulations often are enforceable by law.

NOTE
Change is constant Organizing and completing the initial set of network documentation is a huge task, but it really is just the beginning. Administrators must constantly update all documentation to keep it from becoming obsolete. Documentation is perhaps one of the less glamorous aspects of the administrator’s role, but it’s one of the most important.
Monitoring Network Performance

When networks were smaller and few stretched beyond the confines of a single location, network management was a simple task. In today's complex, multisite, hybrid networks, however, the task of maintaining and monitoring network devices and servers has become a complicated but essential part of the network administrator's role. Nowadays, the role of network administrator often stretches beyond the physical boundary of the server room and reaches every node and component on the network. Whether an organization has 10 computers on a single segment or a multisite network with several thousand devices attached, the network administrator has to be able to monitor all network devices, protocols, and usage—preferably from a central location.

Given the sheer number and diversity of possible devices, software, and systems on any network, it is clear why network management is such an important consideration. Despite the fact that a robust network management strategy can improve administrator productivity and reduce downtime, many companies choose to neglect network management because of the time involved in setting up the system or because of the associated costs. If these companies understood the potential savings, they would realize that neglecting network management provides false economies.

Network management and network monitoring are essentially methods to control, configure, and monitor devices on a network. Imagine a scenario in which you are a network administrator working out of your main office in Spokane, Washington, and you have satellite offices in New York, Dallas, Vancouver, and London. Network management allows you to access systems in the remote locations or have the systems notify you when something goes awry. In essence, network management is about being able to see beyond your current boundaries and being able to act on what you see.

Network management is not one thing. Rather, it's a collection of tools, systems, and protocols that, when used together, let you perform tasks such as reconfiguring a network card in the next room or installing an application in the next state.

Common Reasons to Monitor Networks

The capabilities demanded from network management vary somewhat among organizations, but essentially, several key types of information and functionality are required, such as fault detection and performance monitoring. Some of the types of information and functions that network management tools can provide include the following:
Fault detection: One of the most important aspects of network management is knowing if anything is not working or is not working correctly. Network management tools can detect and report on a variety of faults on the network. Given the number of possible devices that constitute a typical network, determining faults without these tools could be an impossible task. Additionally, network management tools might be able to not only detect the faulty device, but also shut it down. This means that if a network card is malfunctioning, you can disable it remotely. When a network spans a large area, fault detection becomes even more invaluable, because it allows you to be alerted to network faults and to manage them, thereby reducing downtime.

Performance monitoring: Another feature of network management is the ability to monitor network performance. Performance monitoring is an essential consideration that gives you some crucial information. Specifically, performance monitoring can provide network usage statistics and user usage trends. This type of information is essential when you’re planning network capacity and growth. Monitoring performance also helps you determine if there are any performance-related concerns, such as whether the network can adequately support the current user base.

Security monitoring: Any good server administrator has a touch of paranoia built into his or her personality. A network management system lets you monitor who is on the network, what they are doing, and how long they have been doing it. More importantly, in an environment where corporate networks are increasingly exposed to outside sources, the capability to identify and react to potential security threats is a priority. Reading log files to learn of an attack is a poor second to knowing that an attack is in progress and being able to react accordingly.

Maintenance and configuration: Want to reconfigure or shut down the server that is located in Australia? Reconfigure a local router? Change the settings on a client system? Remote management and configuration are key parts of the network management strategy, enabling you to manage huge multisite locations centrally.

Many tools are available to help monitor the network and ensure that it is functioning properly. Some tools, such as a packet sniffer, can be used to monitor traffic by administrators and those who want to obtain data that doesn’t belong to them. The following sections look at several monitoring tools.
Packet Sniffers

Packet sniffers are commonly used on networks. They are either a hardware device or software that basically eavesdrops on transmissions that are traveling throughout the network. The packet sniffer quietly captures data and saves it to be reviewed later. Packet sniffers can also be used on the Internet to capture data traveling between computers. Internet packets often have very long distances to travel, going through various servers, routers, and gateways. Anywhere along this path, packet sniffers can quietly sit and collect data. Given the capability of packet sniffers to sit and silently collect data packets, it’s easy to see how they could be exploited.

You should use two key defenses against packet sniffers to protect your network:

- Use a switched network, which most today are. In a switched network, data is sent from one computer system and is directed from the switch only to intended targeted destinations. In an older network using traditional hubs, the hub does not switch the traffic to isolated users but to all users connected to the hub’s ports. This shotgun approach to network transmission makes it easier to place a packet sniffer on the network to obtain data.

- Ensure that all sensitive data is encrypted as it travels. Ordinarily, encryption is used when data is sent over a public network such as the Internet, but it may also be necessary to encrypt sensitive data on a LAN. Encryption can be implemented in a number of ways. For example, connections to web servers can be protected using the Secure Socket Layer (SSL) protocol and HTTPS. Communications to mail servers can also be encrypted using SSL. For public networks, the IPSec protocol can provide end-to-end encryption services.

NOTE

More encryption Chapter 9, “Network Security,” provides more information on encryption protocols.

Throughput Testing

In the networking world, throughput refers to the rate of data delivery over a communication channel. In this case, throughput testers test the rate of data delivery over a network. Throughput is measured in bits per second (bps). Testing throughput is important for administrators to make them aware of
exactly what the network is doing. With throughput testing, you can tell if a high-speed network is functioning close to its expected throughput.

A throughput tester is designed to quickly gather information about network functionality—specifically, the average overall network throughput. Many software-based throughput testers are available online—some for free and some for a fee. Figure 10.5 shows a software-based throughput tester.

As you can see, throughput testers do not have to be complicated to be effective. A throughput tester tells you how long it takes to send data to a destination point and receive an acknowledgment that the data was received. To use the tester, enter the beginning point, and then the destination point. The tester sends a predetermined number of data packets to the destination and then reports on the throughput level. The results typically are displayed in kilobits per second (Kbps) or megabits per second (Mbps). Table 10.2 shows the various data rate units.
Administrators can periodically conduct throughput tests and keep them on file to create a picture of network performance. If you suspected a problem with the network functioning, you can run a test to compare with past performance to see exactly what is happening.

One thing worth mentioning is the difference between *throughput* and *bandwidth*. These terms are often used interchangeably, but they have different meanings. When we talk about measuring *throughput*, we are measuring the amount of data flow under real-world conditions—measuring with possible EMI influences, heavy traffic loads, improper wiring, and even network collisions. Take all this into account, take a measurement, and you have the network throughput. *Bandwidth*, on the other hand, refers to the maximum amount of information that can be sent through a particular medium under ideal conditions.

**EXAM ALERT**

*Know the difference* For the Network+ exam, be sure you know the difference between throughput and bandwidth.

---

**Table 10.2 Data Rate Units**

<table>
<thead>
<tr>
<th>Data Transfer</th>
<th>Abbreviation</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kilobits per second</td>
<td>Kbps or Kbit/s</td>
<td>1,000 bits per second</td>
</tr>
<tr>
<td>Megabits per second</td>
<td>Mbps or Mbit/s</td>
<td>1,000,000 bits per second</td>
</tr>
<tr>
<td>Gigabits per second</td>
<td>Gbps or Gbit/s</td>
<td>1,000,000,000 bits per second</td>
</tr>
<tr>
<td>Kilobytes per second</td>
<td>KBps</td>
<td>1,000 bytes per second, or 8 kilobits per second</td>
</tr>
<tr>
<td>Megabytes per second</td>
<td>MBps</td>
<td>1,000,000 bytes per second, or 8 megabits per second</td>
</tr>
<tr>
<td>Gigabytes per second</td>
<td>GBps</td>
<td>1,000,000,000 bytes per second, or 8 gigabits per second</td>
</tr>
</tbody>
</table>

---

**Port Scanners**

Port scanners are software-based security utilities designed to search a network host for open ports on a TCP/IP-based network. As a refresher, in a TCP/IP-based network, a system can be accessed through one of 65,536 available port numbers. Each network service is associated with a particular port. Table 10.3 shows some common protocols and their associated ports.
Table 10.3 Some of the Most Common TCP/IP Suite Protocols and Their Port Assignments

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port Assignment</th>
<th>TCP/UDP Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>20</td>
<td>TCP</td>
</tr>
<tr>
<td>FTP</td>
<td>21</td>
<td>TCP</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td>TCP</td>
</tr>
<tr>
<td>Telnet</td>
<td>23</td>
<td>TCP</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>TCP</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>UDP</td>
</tr>
<tr>
<td>DHCP</td>
<td>67</td>
<td>UDP</td>
</tr>
<tr>
<td>TFTP</td>
<td>69</td>
<td>UDP</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
<td>TCP</td>
</tr>
<tr>
<td>NNTP</td>
<td>119</td>
<td>TCP</td>
</tr>
<tr>
<td>NTP</td>
<td>123</td>
<td>TCP</td>
</tr>
<tr>
<td>IMAP4</td>
<td>143</td>
<td>TCP</td>
</tr>
<tr>
<td>SNMP</td>
<td>161</td>
<td>UDP</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**EXAM ALERT**

Be prepared to identify the port number used by a particular network service for the Network+ exam.

These are just a few available ports and the ports we would expect to be open and available. But what about all the others? Many of the thousands of ports are closed by default; however, many others, depending on the OS, are open by default. These are the ports that can cause trouble. Like packet sniffers, port scanners can be used by both administrators and hackers. Hackers use port scanners to try to find an open port that they can use to access a system. Port scanners are easily obtained on the Internet either for free or for a modest cost. After it is installed, the scanner probes a computer system running TCP/IP, looking for a UDP or TCP port that is open and listening.

When a port scanner is used, several port states may be reported:

- **Open/Listening**: The host sent a reply indicating that a service is listening on the port. There was a response from the port.
Closed or Denied or Not Listening: No process is listening on that port. Access to this port will likely be denied.

Filtered or Blocked: There was no reply from the host, meaning that the port is not listening or the port is secured and filtered.

Because others can potentially review the status of our ports, it is important that administrators know which ports are open and potentially vulnerable. As mentioned, many tools and utilities are available for this. The quickest way to get an overview of the ports being used by the system and their status is to issue the `netstat -a` command from the command line. The following is a sample of the output from the `netstat -a` command and active connections for a computer system:

```
Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:135            mike-PC:0              LISTENING
TCP    0.0.0.0:10114          mike-PC:0              LISTENING
TCP    0.0.0.0:10115          mike-PC:0              LISTENING
TCP    0.0.0.0:20523          mike-PC:0              LISTENING
TCP    0.0.0.0:20943          mike-PC:0              LISTENING
TCP    0.0.0.0:49152          mike-PC:0              LISTENING
TCP    0.0.0.0:49153          mike-PC:0              LISTENING
TCP    0.0.0.0:49154          mike-PC:0              LISTENING
TCP    0.0.0.0:49155          mike-PC:0              LISTENING
TCP    0.0.0.0:49156          mike-PC:0              LISTENING
TCP    0.0.0.0:49157          mike-PC:0              LISTENING
TCP    127.0.0.1:5354         mike-PC:0              LISTENING
TCP    127.0.0.1:27015        mike-PC:49187          ESTABLISHED
TCP    127.0.0.1:49187        mike-PC:27015          ESTABLISHED
TCP    192.168.0.100:49190    206.18.166.15:http     CLOSED
TCP    192.168.1.66:139       mike-PC:0              LISTENING
TCP    [::]:135               mike-PC:0              LISTENING
TCP    [::]:445               mike-PC:0              LISTENING
TCP    [::]:2069              mike-PC:0              LISTENING
TCP    [::]:5957              mike-PC:0              LISTENING
TCP    [::]:10115             mike-PC:0              LISTENING
TCP    [::]:20523             mike-PC:0              LISTENING
```

NOTE
For your protection Sometimes, an ISP takes the initiative and blocks specific traffic entering its network before the traffic reaches the ISP’s customers, or after the traffic leaves the customers and before it exits the network. This is done to protect customers from well-known attacks.
TCP [::]:49152  mike-PC:0 LISTENING
TCP [::]:49153  mike-PC:0 LISTENING
TCP [::]:49154  mike-PC:0 LISTENING
TCP [::]:49155  mike-PC:0 LISTENING
TCP [::]:49156  mike-PC:0 LISTENING
TCP [::]:49157  mike-PC:0 LISTENING
UDP 0.0.0.0:123 *:*    
UDP 0.0.0.0:500 *:*    
UDP 0.0.0.0:3702 *:*    
UDP 0.0.0.0:3702 *:*    

As you can see from the output, the system has many listening ports. Not all of these suggest that a risk exists, but the output does let you know that there are many listening ports and that they might be vulnerable. To test for actual vulnerability, you use a port scanner. For example, you can use a free online scanner to probe the system. Many free online scanning services are available. Although a network administrator might use these free online tools out of curiosity, for real security testing, you should use a quality scanner.

**NOTE**
Scan yourself To find out more about port scanners and to conduct an online scan of your computer system, go to www.grc.com and use the ShieldsUP! utility.

**EXAM ALERT**
Administrators use the detailed information revealed from a port scan to ensure network security. Port scans identify closed, open, and listening ports. However, port scanners also can be used by people who want to compromise security by finding open and unguarded ports.

**Network Performance, Load, and Stress Testing**

When it comes to testing the network, administrators often perform three distinct types of tests:

- Performance tests
- Load tests
- Stress tests
Monitoring Network Performance

These test names are sometimes used interchangeably. Although there is some overlap, they are actually different types of network tests, each with different goals.

**Performance Tests**
A performance test is, as the name suggests, all about measuring the network's current performance level. The goal is to take ongoing performance tests and evaluate and compare them, looking for potential bottlenecks. For performance tests to be effective, they need to be taken under the same type of network load each time, or the comparison is invalid. For example, a performance test taken at 3 a.m. will be different from one taken at 3 p.m.

**EXAM ALERT**
Performance testing. The goal of performance testing is to establish baselines for the comparison of network functioning. The results of a performance test are meaningless unless you can compare them to previously documented performance levels.

**Load Tests**
Load testing has some overlap with performance testing. Sometimes called volume or endurance testing, load tests involve artificially placing the network under a larger workload. For example, the network traffic might be increased throughout the entire network. After this is done, performance tests can be done on the network with the increased load. Load testing is sometimes done to see if bugs exist in the network that are not currently visible but that may become a problem as the network grows. For example, the mail server might work fine with current requirements. However, if the number of users in the network grew by 10%, you would want to determine if the increased load would cause problems with the mail server. Load tests are all about finding a potential problem before it happens.

Performance tests and load tests are actually quite similar; however, the information outcomes are different. Performance tests identify the current level of network functioning for measurement and benchmarking purposes. Load tests are designed to give administrators a look into the future of their network load and to see if the current network infrastructure can handle it.

**EXAM ALERT**
Performance versus load tests. Performance tests are about network functioning today. Load tests look forward to see if performance may be hindered in the future by growth or other changes to the network.
Chapter 10: Network Management Tools and Documentation

Stress Tests
Whereas load tests do not try to break the system under intense pressure, stress tests sometimes do. They push resources to the limit. Although these tests are not done often, they are necessary and—for administrators, at least—entertaining. Stress testing has two clear goals:

- It shows you exactly what the network can handle. Knowing a network’s breaking point is useful information when you’re considering network expansion.
- It allows administrators to test their backup and recovery procedures. If a test knocks out network resources, administrators can verify that their recovery procedures work. Stress testing allows administrators to observe network hardware failure.

Stress tests assume that someday something will go wrong, and administrators will know exactly what to do when it happens.

Tracking Event Logs
In a network environment, all NOSs and most firewalls, proxy servers, and other network components have logging features. These logging features are essential for network administrators to review and monitor. Many different types of logs can be used. The following sections review some of the most common log file types.

On a Windows server system, as with the other operating systems, events and occurrences are logged to files for later review. Windows server and desktop systems such as Vista/XP and 2000 use Event Viewer to view many of the key log files. The logs in Event Viewer can be used to find information on, for example, an error on the system or a security incident. Information is recorded into key log files, although you will also see additional log files under certain conditions, such as if the system is a domain controller or is running a DHCP server application.

Event logs refer generically to all log files used to track events on a system. Event logs are crucial for finding intrusions and diagnosing current system problems. In a Windows environment, for example, three primary event logs are used—security, application, and system.

EXAM ALERT
Log review of log files. Be sure you know the types of information included in the different types of log files.
Security Logs

A system's security log contains events related to security incidents such as successful and unsuccessful logon attempts and failed resource access. Security logs can be customized, meaning that administrators can fine-tune exactly what they want to monitor. Some administrators choose to track nearly every security event on the system. Although this might be prudent, it often can create huge log files that take up too much space. Figure 10.6 shows a security log from a Windows system.

Figure 10.6 shows that some successful logons and logoffs occurred. A potential security breach would show some audit failures for logon or logoff attempts. To save space and prevent the log files from growing too big, administrators might choose to audit just failed logon attempts and not successful ones.

Each event in a security log contains additional information to make it easy to get the details on the event:

- **Date**: The exact date the security event occurred.
- **Time**: The time the event occurred.
- **User**: The name of the user account that was tracked during the event.
- **Computer**: The name of the computer used when the event occurred.
Event ID: The Event ID tells you what event has occurred. You can use this ID to obtain additional information about the particular event. For example, it is possible to take the ID number, enter it at the Microsoft support website, and gather information about the event. Without the ID, it would be difficult to find this information.

To be effective, security logs should be reviewed regularly.

Application Log
This log contains information logged by applications that run on a particular system rather than the operating system itself. Vendors of third-party applications can use the application log as a destination for error messages generated by their applications.

The application log works in much the same way as the security log. It tracks both successful events and failed events within applications. Figure 10.7 shows the details provided in an application log.

Notice in Figure 10.7 that three types of events occurred—general application information events, a warning event, and an error event. Vigilant administrators would likely want to check the event ID of both the event and warning failures to isolate the cause.
System Logs
System logs record information about components or drivers in the system, as shown in Figure 10.8. This is the place to look when you’re troubleshooting a problem with a hardware device on your system or a problem with network connectivity. For example, messages related to the client element of DHCP appear in this log. The system log is also the place to look for hardware device errors, time synchronization issues, or service startup problems.

**FIGURE 10.8** A system log.

History Logs
History logs are most often associated with the tracking of Internet surfing habits. They maintain a record of all sites that a user visits. Network administrators might review these for potential security or policy breaches, but generally these are not commonly reviewed.

Another form of history log is a compilation of events from other log files. For instance, one history log might contain all significant events over the past year from the security log on a server. History logs are critical because they provide a detailed account of alarm events that can be used to track trends and locate problem areas in the network. This information can help you revise maintenance schedules, determine equipment replacement plans, and anticipate and prevent future problems.
Chapter 10: Network Management Tools and Documentation

Log Management
While discussing these logs, it becomes clear that monitoring them can be a huge issue. That is where log management (LM) comes in. LM describes the process of managing large volumes of system-generated computer log files. LM includes the collection, retention, and disposal of all system logs. Although LM can be a huge task, it is essential to ensure the proper functioning of the network and its applications. It also helps you keep an eye on network and system security.

Configuring systems to log all sorts of events is the easy part. Trying to find the time to review the logs is an entirely different matter. To assist with this process, third-party software packages are available to help with the organization and reviewing of log files. To find this type of software, enter log management into a web browser, and you will have many options to choose from. Some have trial versions of their software that you may want to try to get a better idea of how LM works.

Networking Tools
A large part of network administration involves having the right tools for the job and knowing when and how to use them. Selecting the correct tool for a networking job sounds like an easy task, but network administrators can choose from a mind-boggling number of tools and utilities.

Given the diverse range of tools and utilities available, it is unlikely that you will encounter all the tools available—or even all those discussed in this chapter. For the Network+ exam, you are required to have general knowledge of the tools available and what they are designed to do.

Until networks become completely wireless, network administrators can expect to spend some of their time using a variety of media-related troubleshooting and installation tools. Some of these tools (such as the tone generator and locator) may be used to troubleshoot media connections, and others (such as wire crimpers and punchdown tools) are used to create network cables and connections.
The Basic Tools

Although many costly, specialized networking tools and devices are available to network administrators, the most widely used tools cost only a few dollars: the standard screwdrivers we use on almost a daily basis. As a network administrator, you can expect to take the case off a system to replace a network interface card (NIC) or perhaps remove the cover from a hub to replace a fan with amazing regularity. Advanced cable testers and specialized tools will not help you when you need a screwdriver.

Wire Crimpers, Strippers, and Snips

Wire crimpers are tools you might find yourself using regularly. Like many things, making your own cables can be fun at first, but the novelty soon wears off. Basically, a wire crimper is a tool that you use to attach media connectors to the ends of cables. For instance, you use one type of wire crimper to attach RJ-45 connectors on unshielded twisted-pair (UTP) cable. You use a different type of wire crimper to attach British Naval Connectors (BNCs) to coaxial cabling.

TIP

When making cables, always order more connectors than you need; a few mishaps will probably occur along the way.

In a sense, you can think of a wire crimper as a pair of special pliers. You insert the cable and connector separately into the crimper, making sure that the wires in the cable align with the appropriate connectors. Then, by squeezing the crimper's handles, you force metal connectors through the cable's wires, making the connection between the wire and the connector.

When you crimp your own cables, you need to be sure to test them before putting them on the network. It takes only a momentary lapse to make a mistake when creating a cable, and you can waste time later trying to isolate a problem in a faulty cable.

Two other commonly used wiring tools are strippers and snips. Wire strippers come in a variety of shapes and sizes. Some are specifically designed to strip the outer sheathing from coaxial cable, and others are designed to work best with UTP cable. All strippers are designed to cleanly remove the sheathing from wire to make sure a clean contact can be made.

Many administrators do not have specialized wire strippers unless they do a lot of work with copper-based wiring. However, standard wire strippers are good things to have on hand.
Wire snips are tools designed to cleanly cut the cable. Sometimes network administrators buy cable in bulk and use wire snips to cut the cable into desired lengths. The wire strippers are then used to prepare the cable for the attachment of the connectors.

**NOTE**

**Punchdown tools**

Punchdown tools are used to attach twisted-pair network cable to connectors within a patch panel. Specifically, they connect twisted-pair wires to the insulation displacement connector (IDC). Chapter 2, “Cabling, Connectors, and Ethernet Standards,” discusses punchdown tools, IDCs, and how they are used.

**Voltage Event Recorder**

A voltage event recorder, shown in Figure 10.9, is used to monitor the quality of power used on the network or by network hardware. You plug it into a wall socket, and it finds potential power-related concerns such as power sags, spikes, surges, or other power variations. The administrator then reviews the recorder’s findings. Such power irregularities can cause problems for hardware and, in the case of serious spikes, can destroy hardware.

![Voltage Event Recorder](image)
When discussing temperature monitoring, we often refer to the temperature of the server and network equipment rooms. In general, the heat tolerance range for computer equipment is surprisingly wide. For example, consider a typical server system, which can happily operate in a range between 50°F and 93°F (10º and 33.8º Celsius). That is a spread of 43ºF (23.8ºC), plenty of room in a normal heated environment. But the problem is that if you maintain a computer room at either the upper or lower end of these levels, the equipment will run, but for how long, no one knows.

Although no specific figures relate to the recommended temperature of server rooms, the accepted optimum is around 70º to 72ºF (21º to 22ºC). At this temperature, the equipment in the room should be able to operate, and those working in the room should not get too cold. Human beings generally require a higher temperature than computer equipment, which is why placing servers in an office space with staff is not ideal.

Many people assume that the biggest problem with servers and network equipment is overheating. To some extent, this is true; servers in particular generate a great deal of heat and can overheat to the point where components fail. But this is only one heat-related issue. A more significant, and more gradual, problem is that of temperature consistency.

Heat causes components to expand, and cooling causes them to contract. Even the slightest temperature shift causes the printed circuit boards and chips to shift, and if they shift too much or too often, the chance of their becoming separated from their connections is greatly increased. This is known as chip creep. Keeping the heat at a moderate and constant level reduces the expansion and contraction of the boards and increases the components’ reliability.

**CAUTION**

*Open doors*  Never wedge open a door to an environmentally controlled room, no matter how cold you get. Not only does having an open door defeat the purpose of the controlled environment, but it also can damage air-conditioning units.

Part of how administrators keep their equipment rooms at the right temperature is by using temperature monitors. The temperature monitor sits in the equipment room and constantly documents changes in room temperature and humidity. If radical changes in temperature are detected, an alert is sent to the administrator. This can sometimes occur if someone leaves a door to the server room...
open, the air conditioning breaks, or some piece of network hardware is producing a lot of heat. Although network temperature monitors might not often be needed, just having them installed gives administrators peace of mind.

**Keeping It Cool**

Fortunately, the solution to the heat problem is relatively simple. You use an air conditioning unit. The only problem is, you can’t use just any old A/C unit. Having a late 1960s window unit may be better than nothing, but we are looking for high-quality protection.

High-quality air conditioning systems fall under the domain of industrial heating, ventilation, and air conditioning (HVAC) equipment. Server environment-specific air conditioning units are designed to maintain a constant temperature. High-quality units guarantee an accuracy of plus or minus 1ºF. Most units have an audible alarm, but some also can communicate with management systems so that the server room temperature can be monitored remotely. Although the icy blast of a server room air conditioning system may not be welcomed by those who have to work in it for an extended period of time, the discomfort is far outweighed by the benefit to the server equipment.

Calculating the correct size and type of air conditioning unit can be a tricky proposition. Air conditioning systems are rated on how many cubic feet they can cool. Using this figure, and estimating the increase in temperature caused by the hardware in the room, you will have the basic information you need to choose an A/C unit. Of course, the calculation should take into account potential future growth. In some cases, a standby A/C unit is also installed. Whether such a system is required depends on how much fault tolerance you need and are willing to pay for.

**Toner Probes**

A *toner probe* is a device that can save a network installer many hours of frustration. This device has two parts—the tone generator, or toner, and the tone locator, or probe. The toner sends the tone, and at the other end of the cable, the probe receives the toner's signal. This tool makes it easier to find the beginning and end of a cable. You might hear the tone generator and tone locator referred to as the *fox and hound*.

As you might expect, the purpose of the tone probe is to generate a signal that is transmitted on the wire you are attempting to locate. At the other end, you press the probe against individual wires. When it makes contact with the wire that has the signal on it, the locator emits an audible signal or tone.

The tone locator probe is a useful device, but it does have some drawbacks. First, it often takes two people to operate one at each end of the cable. Of
course, one person could just keep running back and forth, but if the cable is run over great distances, this can be a problem. Second, using the toner probe is time-consuming because it must be attached to each cable independently.

**NOTE**

Labeling cables. Many problems that can be discovered with a tone generator are easy to prevent by simply taking the time to properly label cables. If the cables are labeled at both ends, you will not need to use such a tool to locate them.

**EXAM ALERT**

Toners. Toner probes are specifically used to locate cables hidden in floors, ceilings, or walls and to track cables from the patch panel to their destination.

**Protocol Analyzer**

Protocol analyzers are used to do just that—analyze network protocols such as TCP, UDP, HTTP, and FTP. Protocol analyzers can be hardware- or software-based. In use, protocol analyzers help diagnose computer networking problems, alert you to unused protocols, identify unwanted or malicious network traffic, and help isolate network traffic-related problems.

Like packet sniffers, protocol analyzers capture the communication stream between systems. But unlike the sniffer, the protocol analyzer captures more than network traffic; it reads and decodes the traffic. Decoding allows the administrator to view the network communication in English. From this, administrators can get a better idea of the traffic that is flowing on the network. As soon as unwanted or damaged traffic is spotted, analyzers make it easy to isolate and repair. For example, if there is a problem with specific TCP/IP communication, such as a broadcast storm, the analyzer can find the source of the TCP/IP problem and isolate the system that is causing the storm. Protocol analyzers also provide many real-time trend statistics that help you justify to management the purchase of new hardware.

Protocol analyzers can be used for two key reasons:

- **Identify protocol patterns.** By creating a historical baseline of analysis, administrators can spot trends in protocol errors. That way, when a protocol error occurs, it can be researched in the documentation to see if that error has occurred before and what was done to fix it.
Chapter 10: Network Management Tools and Documentation

- **Decoding information**: Capturing and decoding network traffic allows administrators to see what exactly is going on with the network at a protocol level. This helps find protocol errors as well as potential intruders.

**EXAM ALERT**

Statistics Protocol analyzers allow administrators to examine the bandwidth that a particular protocol is using.

**Media/Cable Testers**

A media tester, also called a cable tester, defines a range of tools designed to test whether a cable is working properly. Any tool that facilitates the testing of a cable can be deemed a cable tester. However, a specific tool called a media tester allows administrators to test a segment of cable, looking for shorts, improperly attached connectors, or other cable faults. All media testers have a way of telling you whether the cable is working correctly and where the problem in the cable might be.

**TDR and OTDR**

A time domain reflectometer (TDR) is a device used to send a signal through a particular medium to check the cable's continuity. Good-quality TDRs can locate many types of cabling faults, such as a severed sheath, damaged conductors, faulty crimps, shorts, loose connectors, and more. Although network administrators will not need to use a tool such as this every day, it could significantly help in the troubleshooting process. TDRs help ensure that data sent across the network is not interrupted by poor cabling that may cause faults in data delivery.

**EXAM ALERT**

TDRs TDRs work at the physical layer of the OSI model, sending a signal through a length of cable, looking for cable faults.

Because the majority of network cabling is copper-based, most tools designed to test cabling are designed for copper-based cabling. However, when you test fiber-optic cable, you need an optical tester.
An optical cable tester performs the same basic function as a wire media tester, but on optical media. The most common problem with an optical cable is a break in the cable that prevents the signal from reaching the other end. Due to the extended distances that can be covered with fiber-optic cables, degradation is rarely an issue in a fiber-optic LAN environment.

Ascertaining whether a signal reaches the other end of a fiber-optic cable is relatively easy, but when you determine that there is a break, the problem becomes locating the break. That's when you need a tool called an optical time domain reflectometer (OTDR). By using an OTDR, you can locate how far along in the cable the break occurs. The connection on the other end of the cable might be the source of the problem, or perhaps there is a break halfway along the cable. Either way, an OTDR can pinpoint the problem.

Unless you work extensively with fiber-optic cable, you're unlikely to have an OTDR or even a fiber-optic cable tester in your toolbox. Specialized cabling contractors will have them, though, so knowing they exist is important.

Multimeter

One of the simplest cable-testing devices is a multimeter. By using the continuity setting, you can test for shorts in a length of coaxial cable. Or, if you know the correct cable pinouts and have needlepoint probes, you can test twisted-pair cable.

A basic multimeter combines several electrical meters into a single unit that can measure voltage, current, and resistance. Advanced models can also measure temperature.

A multimeter has a display, terminals, probes, and a dial to select various measurement ranges. A digital multimeter has a numeric digital display, and an analog has a dial display. Inside a multimeter, the terminals are connected to different resistors, depending on the range selected.

Network multimeters can do much more than test electrical current:

- **Ping specific network devices**: A multimeter can ping and test response times of key networking equipment, such as routers, DNS servers, DHCP servers, and more.
- **Verify network cabling**: It is possible to use a network multimeter to isolate cable shorts, split pairs, and other faults.
- **Locate and identify cable**: Quality network multimeters allow administrators to locate cables at patch panels and wall jacks using digital tones.
> **Documentation ability**: Multimeter results can be downloaded to a PC for inspection. Most network multimeters provide a means such as USB ports to link to a PC.

**Network Qualification Tester**

One more tool worth mentioning is the network qualification tester. This tool gives administrators a quick glance at the network's bandwidth and whether its current configuration can grow to support VoIP or Gigabit Ethernet, for example.

If a network is running slowly, the network qualification tester can tell you why the network is struggling. For example, it can identify crosstalk within a cable and how it is impacting network performance. Most quality network qualification testers can test twisted-pair and coaxial cable with other models available for fiber-optic cable.

**EXAM ALERT**

**Qualification testing** Network qualification testers allow administrators to identify the current speeds the network cabling can support and to isolate cabling from network problems.

**Butt Set**

A butt set is most often associated with telephony, but it can be used on some data networks as well. A butt set allows the administrator or technician to butt into a communication line and use it. In the case of a phone line, a technician can use the line normally—that is, make a call, answer a call, or listen in to a call.

The butt set for telephony looks somewhat like a regular phone handset with wires attached. The wires from the handset connect to the phone wire, and that's it. The technician can test and access the phone line. This device can be used to test network telephony but has limited use on actual network cable. Some network butt sets allow the access of data on the cable, but many other tools can do the same thing with better results.

**Wireless Detection**

Wireless media require their own types of tools. One such tool is a Wi-Fi detector. The intent of such a device is to reveal Wi-Fi hot spots and detect wireless network access with LED visual feedback. Such devices can be configured to
scan specific frequencies. When working with 802.11b/g/n networks, you will most certainly require scanning for 2.4GHz RF signals.

Such devices can be used in the troubleshooting process to see where and how powerful RF signals are. Given the increase in wireless technologies, RF detectors are sure to increase in popularity.

**Review and Test Yourself**

The following sections provide you with the opportunity to review what you've learned in this chapter and to test yourself.

**The Facts**

For the exam, don't forget these key concepts:

- Both logical and physical network diagrams provide an overview of the network layout and function.
- Keeping and reviewing baselines is an important part of the administrator's role.
- Administrators must ensure that proper documentation is kept. Log files such as security, event, and application logs must be reviewed periodically.
- In a network environment, it is important to distinguish between policies, procedures, and regulations.
- Packet sniffers can be used by both administrators and hackers to capture network data.
- Port scanners detect open and often unsecured ports.
- Performance, load, and stress tests are all important network tests but serve different functions.
- Administrators can use a number of cable-related tools. Many wiring tools are software- and hardware-based.
Key Terms

- Baseline
- Butt set
- Cable stripper
- Event log
- History log
- IP address
- Load testing
- Media tester
- Multimeter
- OTDR
- Packet sniffer
- Physical and logical network diagrams
- Policies and procedures
- Port scanner
- Protocol analyzer
- Punchdown tool
- Regulations
- System log
- TDR
- Temperature monitor
- Throughput tester
- Toner probe
- Twisted pair
- Voltage event recorder
- Wire crimpers
- Wireless
- Wiring schematic