

"I got even with all the bad management I had by being a good manager."

—VICTORIA PRINCIPAL



In this chapter, you will learn how to

- Describe how configuration management documentation enables you to manage and upgrade a network efficiently
- Conduct network monitoring to identify performance and connectivity issues
- Explain how to optimize network performance

Managing a network well on-the-fly can challenge even very advanced network techs, so it won't come as any surprise to you that most techs use an array of techniques and tools to make it all . . . well . . . manageable. This chapter looks first at documentation for networks, including how the network is put together and how you go about making changes that don't disrupt the network. We'll then turn to tools and techniques for monitoring performance and connectivity. The chapter concludes with a section on optimizing network performance.

■ Network Configuration Management

The more complicated a network becomes, the more vulnerable it becomes in terms of security, efficiency, duplication or unnecessary redundancy, and unnecessary cost. Chapter 17 covered many of the security issues, but left a rather major component for coverage here, configuration management.

Configuration management is a set of documents, policies, and procedures designed to help you maintain and update your network in a logical, orderly fashion so that you may lessen the risks of these vulnerabilities. Your network should standardize on types of NICs, cabling, network operating systems, and network applications to make certain that when upgrades need to happen, they do so with the utmost efficiency.

If you want to upgrade your users from Windows XP to Windows Vista, for example, you don't want to create a huge security risk for your network, nor waste a lot of money, time, and effort by realizing *after the fact* that an important application wasn't compatible with the new OS. That's not the way to do it in the real world!

Configuration Management Documentation

The **configuration management documentation** enables you to see very quickly everything about your network. Good documentation helps you to troubleshoot your network efficiently. You can also determine as efficiently as possible both how to upgrade components of that network and what effects such an upgrade might have. Configuration management documentation covers everything, from the wires used to how the people using the network should be trained. You can think about the configuration management documentation in five broad categories:

- Wiring diagrams
- Network diagrams
- Baselines
- Policies, procedures, and configurations
- Regulations

Wiring Schematics or Diagrams

The **wiring diagram** or **wiring schematic** identifies how the wires in a network connect to various switches and such, plus what standards are used for those wires, such as CAT 5e, CAT 6, 568A, 568B, or various fiber standards. It usually consists of multiple pages, starting with a very detailed overview of every cable run, telecommunications closet, and network outlet, as well as other details such as cross-connects and demarcs (Figure 18.1).

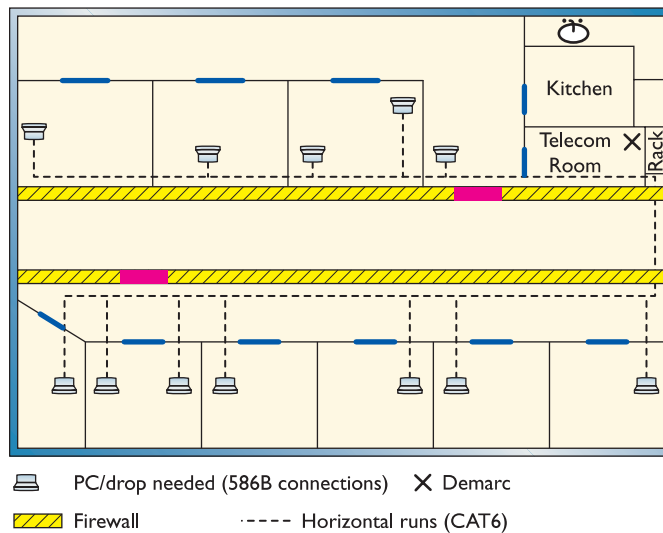


The CompTIA Network+ exam uses the term “wiring schematic” to mean how the wires connect and also which technology standard should be used for this wiring. The industry does not typically use the term, preferring instead “wiring diagram,” “network layout,” or “cabling standard.”

A wiring schematic is more closely associated with electronics engineering, like what to refer to when re-creating the wiring harness on your 1968 Chevy Camaro Super Sport restoration project. Nevertheless, look for questions on the exam on cabling diagrams and wiring standards for which “wiring schematics” is the correct answer.



It’s a sad but true statement that a large number of smaller networks lack wiring schematics. If you’re in charge of a network and you don’t have schematics, you’ll probably draw one up yourself.



• **Figure 18.1** Wiring diagram overview

The overview is then detailed with diagrams of individual structured cabling connections, mainly cross-connects and patch panels, giving a clear view of the endpoints of each cable. These detailed diagrams will usually include the actual designations for each cable run (Figure 18.2).

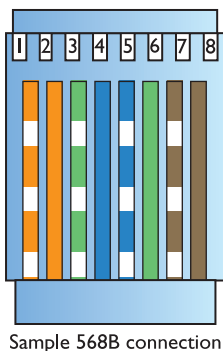
It’s part of the cabling puller’s job to generate the wiring diagram. Depending on the office building, it’s very common for telephone runs to show up in the same diagram—although every situation is different. Most wiring diagrams stay with the folks in charge of the building (CompTIA uses the term “building services” to describe those people). A network administrator should at the very least have access to these diagrams and at best have a copy to mark up as he or she plans new runs or other changes to the physical network.

Physical and Logical Network Diagrams

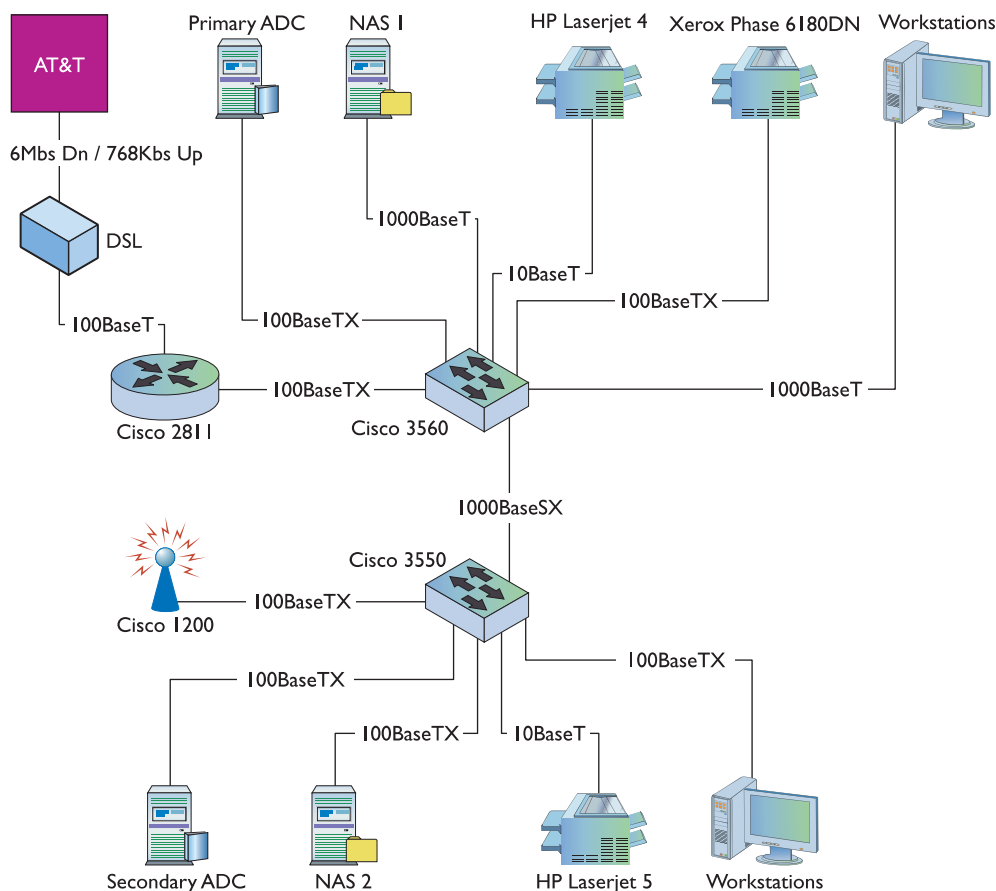
Most of the time network administrators don’t need the detail provided by wiring diagrams to deal with the day-to-day issues of network management. In general the problems you run into are more in the vein of “What kind of connection is between these two things” as opposed to “What kind of wiring connects these two things.” For that we turn to a physical network diagram. A **physical network diagram** is similar to a wiring diagram in that you see the physical runs, but in this case you define the type of connection: Gigabit Ethernet, T1, and so on. A physical network diagram includes every router, switch, server, CSU/DSU, cable modem, wireless access point, and so on, including the make and model and firmware upgrade. Figure 18.3 shows a typical physical network diagram.

It’s the network administrator’s job to create the physical network diagram. Lucky for you, there are two critical tools to make your job easier. First are standardized icons. As you look at Figure 18.3, you notice the icons are somewhat cryptic. That’s because many years ago Cisco developed this shorthand to represent any type of networking device you might imagine.

All connections must be EIA/TIA 568B. Sample below.



• **Figure 18.2** Wiring diagram detail



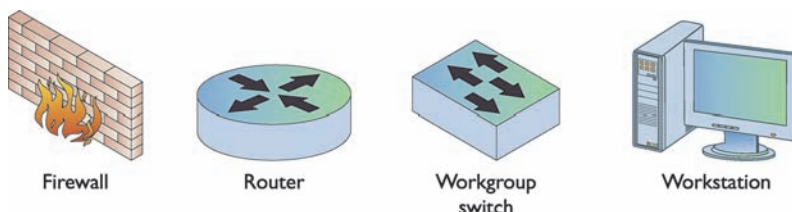
• **Figure 18.3** Physical network diagram

Cisco usually calls these “network topology icons” and they are the accepted standard to use whenever you’re drawing a network. Figure 18.4 shows some examples of the more common topology icons.

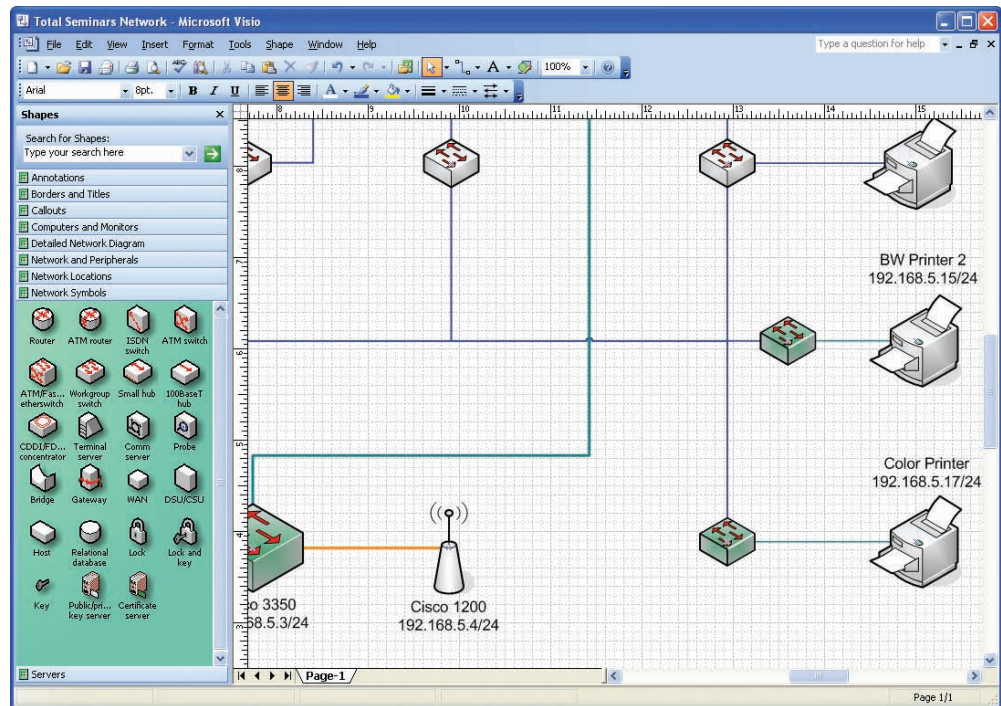
Your second tool is one of the many drawing programs that support network topology icons. You can use a presentation tool like Microsoft PowerPoint, but Microsoft Visio is the most famous tool for drawing any type of network diagram. Visio adds a number of extras that make putting together any type of diagram a snap. Figure 18.5 shows how I made Figures 18.3 and 18.6: with Visio!

The last paper document you’ll find very handy is the logical network diagram. A **logical network diagram** describes the broadcast domains and individual IP addresses for all the devices in your network with static IP addresses. These are at first glance similar to physical network diagrams but in some cases they show the individual computers (if there are not too many) and almost never show connections

New network devices show up all the time, so there’s no single place to see every network topology icon available. However, Cisco keeps a fairly complete list at www.cisco.com/web/about/ac50/ac47/2.html.



• **Figure 18.4** Sample network topology icons

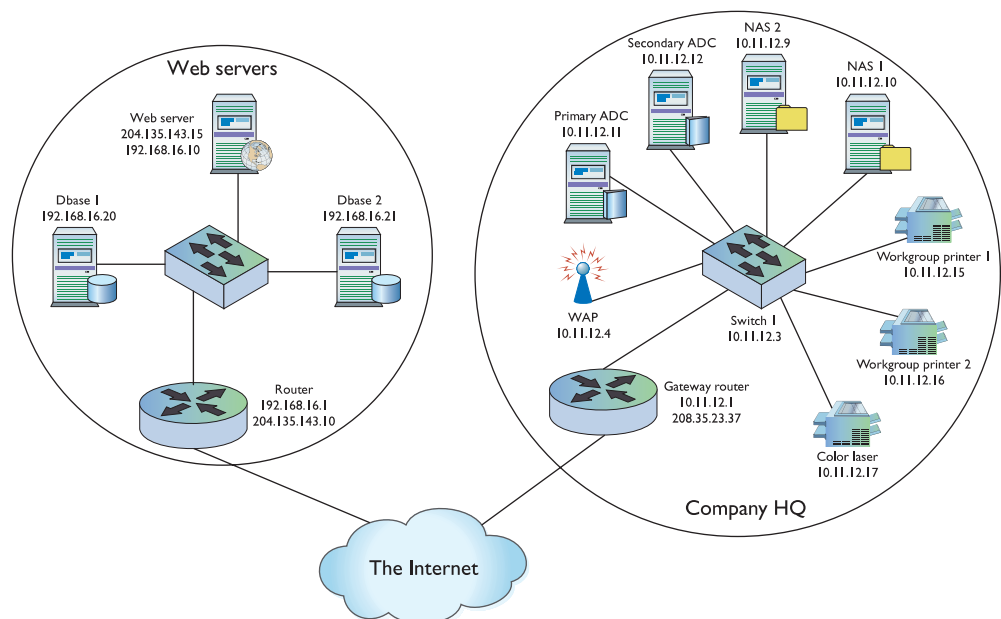


• **Figure 18.5** Visio in action



Make updating your network documentation the last step of any changes you make to the network.

to individual computers. Instead, they represent broadcast domains with circles and Internet connections with clouds. Logical network diagrams usually only show a few critical physical switches or routers and only if those devices affect the logical network (gateway routers, VLAN switches). Figure 18.6 show a typical logical network diagram.



• **Figure 18.6** Logical network diagram

Baselines

The best way to know when a problem is brewing is to know how things perform when all's well with the system. Part of any proper configuration management documentation is a **baseline**: a log of performance indicators such as CPU usage, network utilization, and other values to give you a picture of your network and servers when they are working correctly. A major change in these values can point to problems on a server or the network as a whole.

All operating systems come with some form of baseline tools. A common tool used to create a baseline on Windows systems is the Performance Monitor utility that comes with all versions of Windows. You'll see Performance Monitor at work later in this chapter.

Policies, Procedures, and Configurations

Network security, cost, time, employee and management frustration—all of these things matter when managing a complex network. As part of any good documentation, therefore, you'll find policies about what people can and cannot do with network hardware and software. You'll see procedures outlined for what to do when upgrading components or adding new user accounts. You'll also get down-to-the-user-interface-level information about how software and hardware should be configured.

Much of this stuff should be familiar from a CompTIA A+ certification level. For example, what's a great way to keep a Windows PC from becoming vulnerable to a new piece of malware floating around the Internet? C'mon, one guess! Keep it patched and up to date with Windows Update, right? Exactly.

Properly created configuration management documentation will inform network folks what to do with user training. Who gets it? What departments? What level of access for new employees versus seasoned and trusted veterans?

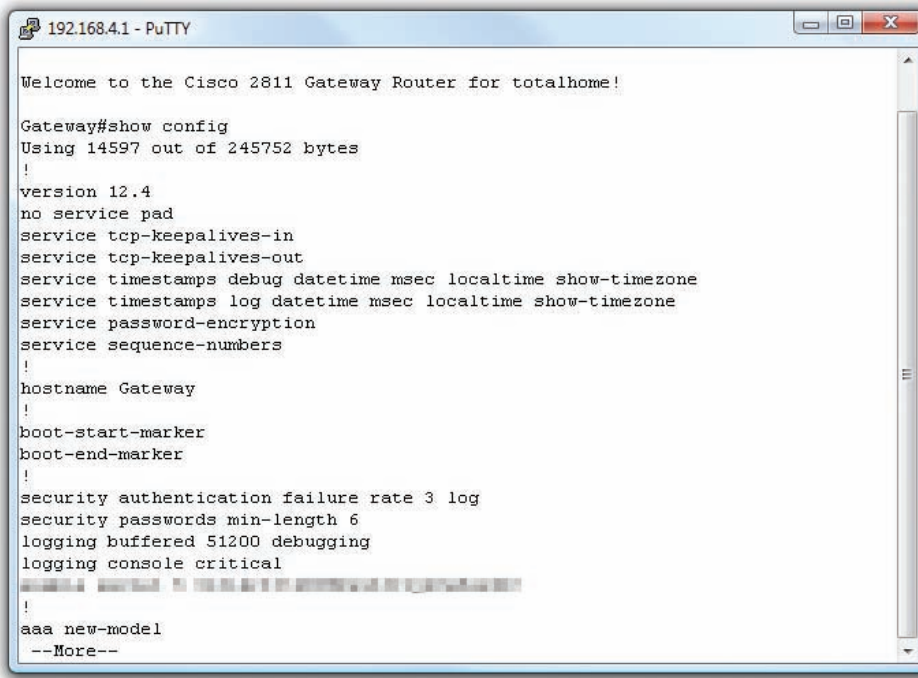
Many of the policies and procedures help protect your network from harm. In CompTIA terms, they mitigate security risks like those outlined in gory detail in Chapter 17!

Two policies affect most users: acceptable use and security. After explaining these policies, I'll also give you an example of configuration.

Acceptable Use Policy Acceptable use policies define exactly what you can and cannot do with your computers and network. Some classic areas defined by an **acceptable use policy** include personal computer use and adding personal software.

Security Policy An organization's **security policy** defines procedures employees should perform to protect the network's security. Security policies cover a wide gamut. They define password complexity, explain to users how to deal with social engineering, and clarify how to deal with virus attacks. Security policies almost always define action plans to deal with serious events that might threaten your network.

Configuration **Configurations** are the results of the procedures. It's important to document configurations for critical systems. Imagine if a carefully configured gateway router were to suddenly lose all of its settings and no one had made a backup? Every configurable device in today's networking



```
192.168.4.1 - PuTTY

Welcome to the Cisco 2811 Gateway Router for totalhome!

Gateway#show config
Using 14597 out of 245752 bytes
!
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname Gateway
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 51200 debugging
logging console critical
!
aaa new-model
--More--
```

• **Figure 18.7** Section of SHOW CONFIG

world comes with some tool to document its configuration. Figure 18.7 shows a part of one of the most famous of all configurations, the infamous SHOW CONFIG command built into almost every device made by Cisco.

Regulations

Very few people profess to liking regulations, the rules that govern behavior in the workplace. Nevertheless, **regulations** help keep networks and people safe and productive. Every decent configuration management documentation talks about the regulations, such as what to do when you have a safety violation or some sort of potentially bad accident.

Change Management Documentation

Although CompTIA seems to separate the detailed overview of the network from how to upgrade it, most networking professionals use the term **change management documentation** to describe the single body of knowledge. An example will make this clear. Let's say you want to change your network by adding a demilitarized zone (DMZ), because you want to add a server that is easily accessible to people outside the network.

The change management documentation will show you network diagrams, so you can verify where to place the DMZ and what other machines will be potentially affected by the change. Plus, it will give you the detailed information on what to do to get approval from supervisors, get through the budgeting office, and so on.

Change management documentation details the procedures and policies to update the documentation so that after each change in the network, your master documents are accurate. This is an extremely important piece of information! Failure to update the correct document will eventually result in you looking really bad when an otherwise minor troubleshoot turns into a nightmare.



Cross Check

DMZ

You read about DMZs in Chapter 17, "Protecting Your Network," so check your memory now. What sorts of servers might be in a DMZ? How does creating a DMZ help protect your internal, private network?

■ Monitoring Performance and Connectivity

Networking technicians need to know how to use the tools that are available to monitor network performance and connectivity. A network administrator will set up the tools you use, but a tech needs to know how to use those tools to create baselines, monitoring utilities, and logs of various sorts. The tools vary from operating system to operating system, but let's look at the two most commonly in use: Performance Monitor and Event Viewer, both Windows utilities.

Administrators use **Performance Monitor** (also called PerfMon) to view the behavior of hardware and other resources on Windows machines, either locally or remotely. Performance Monitor can monitor both real-time and historical data about the performance of your systems. Figure 18.8 shows the default Performance Monitor in Windows XP.

Once you access Performance Monitor, you need to configure it to display data. To do that accurately, you set objects, counters, and views.

An **object**, in Performance Monitor terms, is a system component that you want to monitor, such as the processor or the memory. Each object has different measurable features, called **counters**. Counters, in other words, are the aspects of an object that you want to track. As you decide which object(s) to monitor, you can also select specific counters for each object. Performance Monitor can organize and display selected counter information using a variety of **views**, each of which provides different way of presenting information. In addition to showing you real-time information about the system, Performance Monitor can also log so you can store data about your system for later review. This is the view you use to create a baseline.

To create a new log in Windows XP, expand the **Performance Logs and Alerts** tree in the left pane and click **Counter Logs**. Click **Action | New Log Settings** and give the new log a name such as Domain Controller. To add objects to the new log, click the **Add Objects** button in the middle of the dialog box. In the Add Objects dialog box, first select the computer you want to monitor. You can choose either the local machine (the default) or a remote machine. To monitor a remote machine, type the Universal Naming Convention (UNC) name of the computer in question. To monitor a machine named HOUBDC1, for example, you would type **\\HOUBDC1** in the **Select counter objects from computer** field (Figure 18.9).

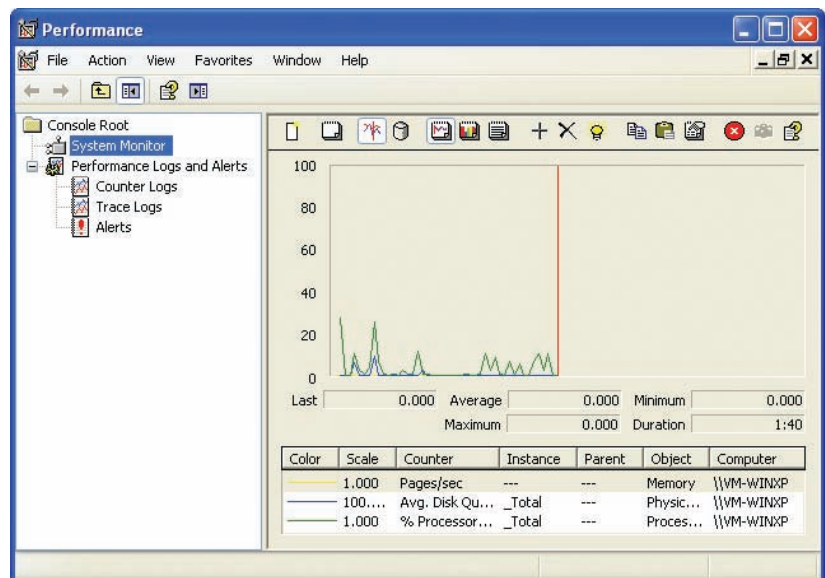
You must now select the object to monitor. Select one or more objects to monitor from the **Performance objects** list. Note that the Log view is



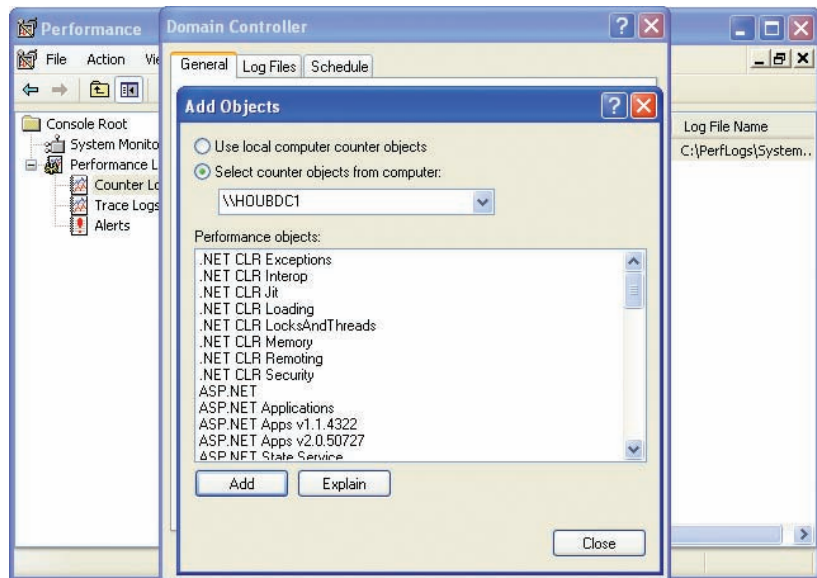
Windows Vista calls the tool *Reliability and Performance Monitor*. It functions similarly to the Windows XP tool, though the screens differ a little. Vista calls the log files "Data Collector Sets," though a log file by any other name . . . is still a log file.



CompTIA Network+ is not going to test you on using Performance Monitor or any other single baselining tool. Just make sure you use something to understand what a baseline does for you.



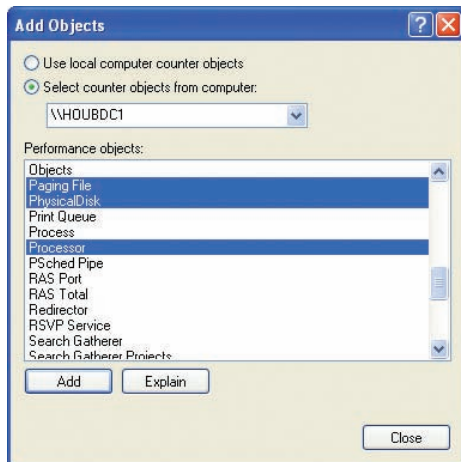
• **Figure 18.8** Performance Monitor in action



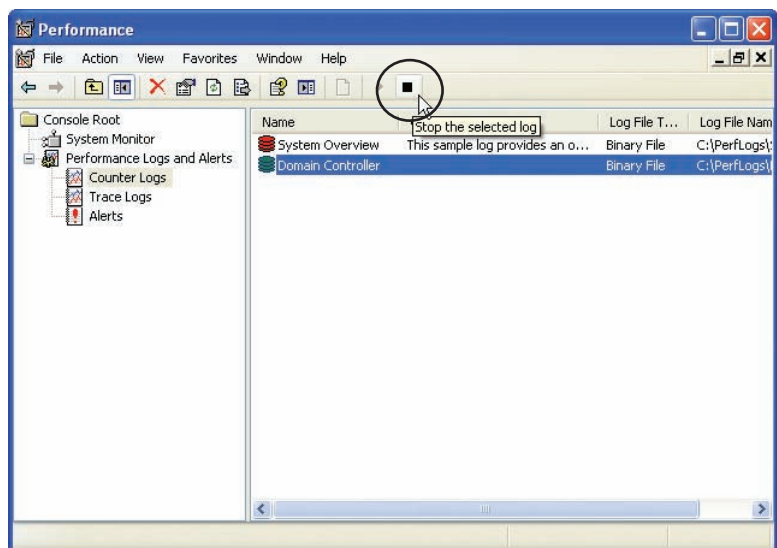
• **Figure 18.9** Monitoring a remote computer

somewhat different from the other views, in that you only add *objects* to the view, not the specific counters for the objects, as shown in the Add Objects dialog box in Figure 18.10.

After you select the objects for Performance Monitor to track and log, click the **Add** button and then the **Close** button. Click **OK** to close the Add Objects dialog box. Select your new log—in this case labeled Domain Controller. By default, logging will begin immediately upon closing the Domain Controller dialog box. With the newly created log selected, you can easily start and stop logging by clicking the play and pause buttons, as shown in Figure 18.11.



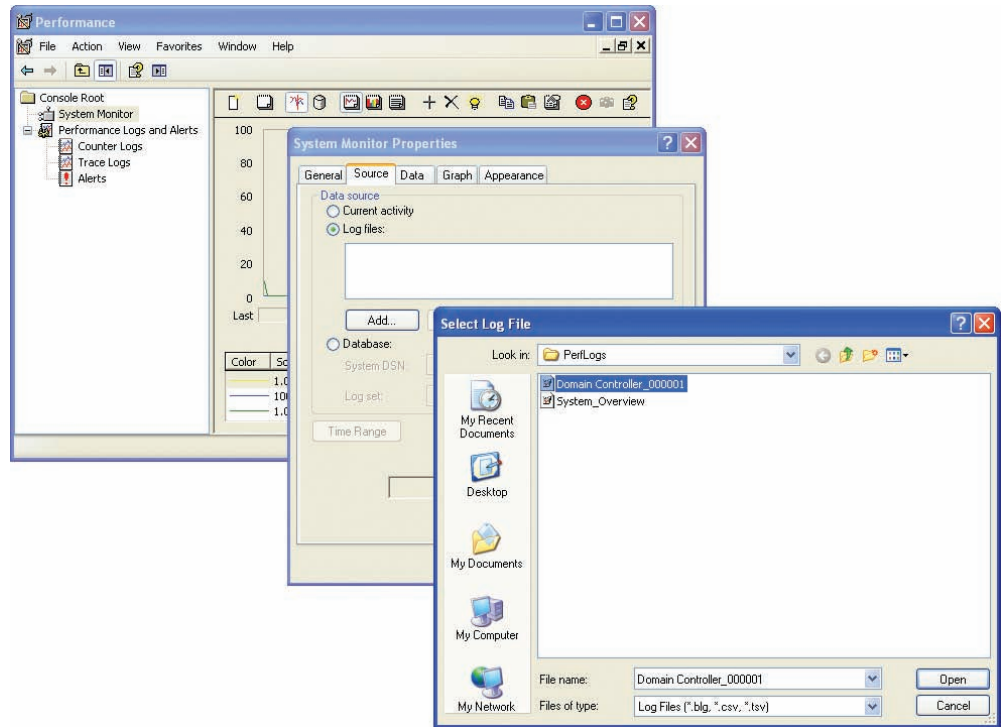
• **Figure 18.10** Selecting performance objects



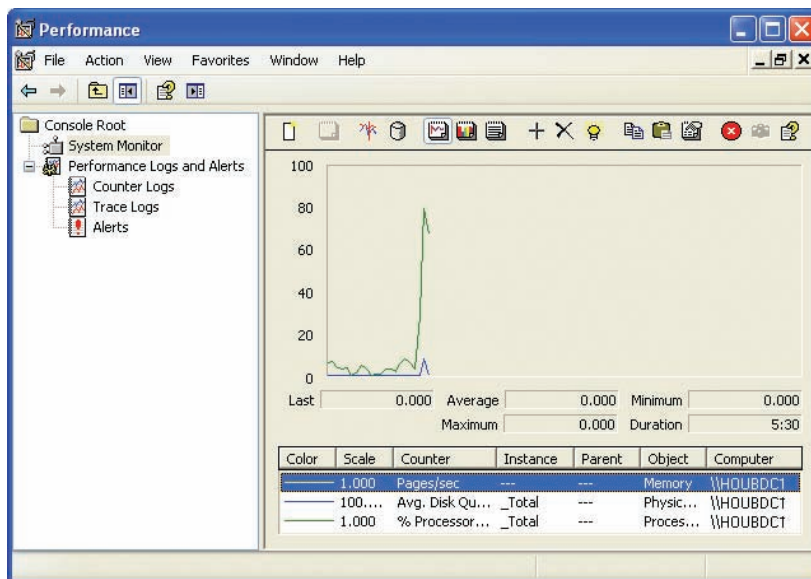
• **Figure 18.11** Logging data

After you have configured the log settings and captured data for a minute or so, you can then view the results in System Monitor. Click the **System Monitor** item in the console tree on the left. In System Monitor, click the **View Log Data** button and then select the **Log files** radio button on the Source tab of the System Monitor Properties dialog box. From there you can click the **Add** button and select the log file created earlier (Figure 18.12).

When you choose to obtain data from a saved log, you go back to that frozen moment in time and add counters to the other views for the objects you chose to save in the log. In our log options, for example, we chose to store data for the paging file, physical disk, and processor objects. After you've loaded a particular log file, you can view a static chart for that moment in time (Figure 18.13).



• **Figure 18.12** Selecting a log file



• **Figure 18.13** Replaying a log file



Try This!

Using Reliability and Performance Monitor in Windows

Vista and Windows 7

The CompTIA Network+ exam won't test you on how to use Performance Monitor in Windows 2000/XP or Reliability and Performance Monitor in Windows Vista and Windows 7, but this stuff is fun. So try this!

If you have a Vista or 7 box handy, open the Control Panel and run Reliability and Performance Monitor. How does it resemble Performance Monitor in Windows XP, as the chapter has described? How does it differ? Go through the steps to create a custom log file—or Data Collector Set—so you get a sense of how to do it.

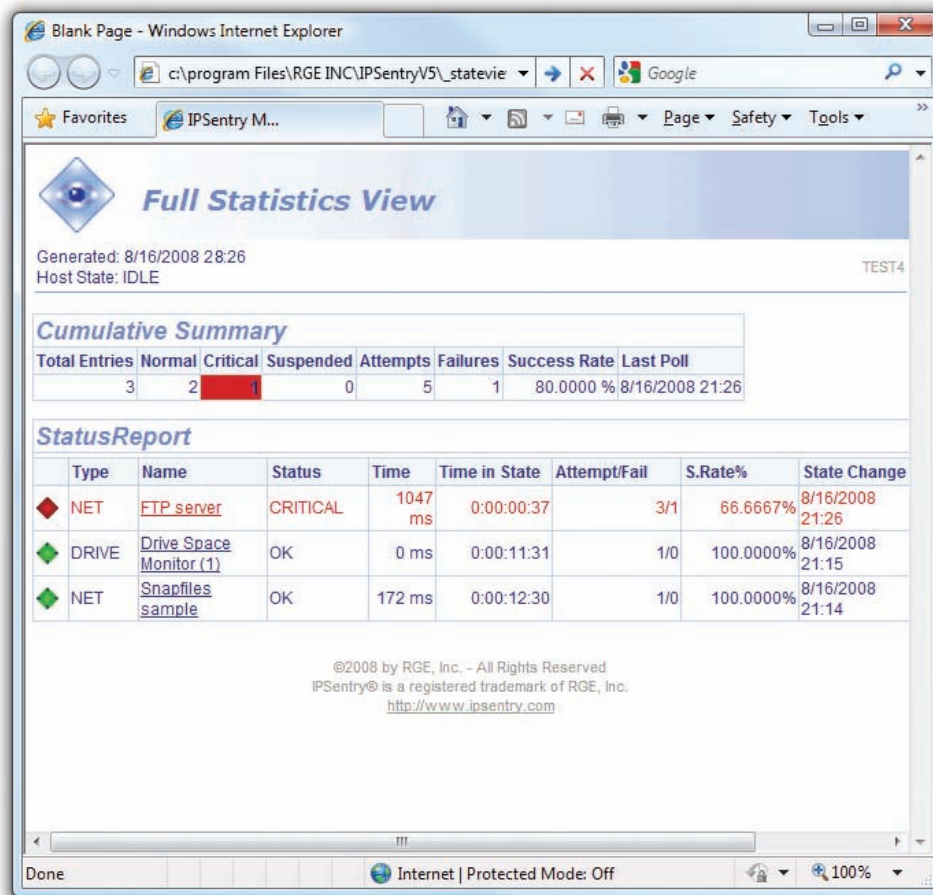
The Performance Monitor utility described here is specific to Windows 2000 and XP systems, but you should create baselines for whatever types of systems you have, and they should cover all aspects of your network. Be certain to create multiple baselines, to show the systems both at rest and in use, using the baselining tools at your disposal.

Don't limit your thinking to operating system tools when you think about baselining. There are a

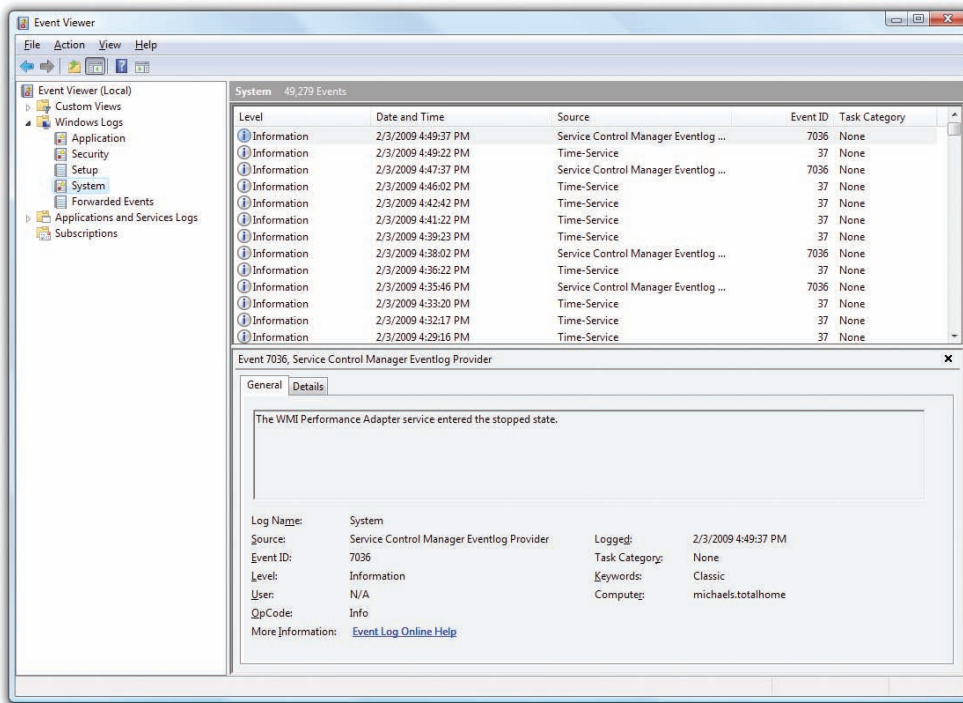
number of third-party network monitoring tools available that not only generate baselines on almost any criteria you wish but that will also stay online and monitor the network to let you know if any parameters have been exceeded. These network monitors are expensive, but if you want real-time monitoring they are a great option. Since network monitors are always on-

line and always checking for certain items, they also often act as network intrusion detection system (IDS) devices at the same time. Figure 18.14 shows one example, IPSentry by RGE, Inc.

Logs by themselves are a powerful tool because every operating system generates a number of logs outside of the ones you create. Generally you can break up logs into three different types: system, application, and security. In Windows you can see all of these logs in Event Viewer (Figure 18.15). Linux systems tend to have lots of logs, but most versions have a folder called /VAR/LOG where all of your logs (usually) reside. Mac OS X has roughly the same logs as Linux, but has a nice GUI viewer called Console. Whatever the OS, do know



• Figure 18.14 IPSentry at work



• **Figure 18.15** Event Viewer in Windows Vista

that the CompTIA Network+ exam takes a Windows bias and assumes there are always at least three logs, Application, Security, and System.

- **Application logs**, as the name implies, deal with events that take place with applications. If an application starts, stops, fails to start, or does anything else an application wishes to report, it shows up here.
- **Security logs** are the place to look for anything that might affect security. The most important counters to look for under Security are successful and failed logons and logoffs.
- **System logs** cover a wide range of issues that deal with the entire system. Anything that has to do with system services, device drivers, or configuration changes tend to show up here.



Even though the CompTIA Network+ exam lightly touches upon logs and makes some serious simplifications, know that every operating system has a log file for just about any event you might want to know about. Even the default logs are highly customizable, giving you the ability to choose what types of events you want monitored or not monitored.

■ Network Performance Optimization

It's a tough, ugly world when you're a network administrator. You get very little praise when the network runs well and all the blame when the network isn't running in the fashion the users expect. The situation in which you'll get the most complaints from users is when the network isn't running as fast as they're used to experiencing. We work hard to keep users from contacting us, and the best way to keep them at bay is to make sure the network runs at optimal performance at all times.

Okay, maybe fear of users yelling at you isn't the best rationale. On a more professional basis, we need our networks to deliver their resources as quickly as possible. A Web site that keeps users waiting for long loads or a file server that drags along, leaving users staring at status bars, is contrary to efficiency. It's our duty as network administrators to do everything we can to optimize network performance.

Luckily there are hundreds if not thousands of strategies and technologies designed to optimize network performance. The CompTIA Network+ exam objectives define a short but well-considered list of topics that this section will address. Some of these you've seen in earlier chapters, so I'll not belabor them here, but merely mention and point you to those chapters. Others are topics new to the book. To make learning easier, I've broken them into three distinct groups: caching, controlling data throughput, and keeping resources available.

Caching

Caching is the process of storing data that someone asks for in the hope that someone else will ask for it again. Generally, odds are incredibly good that anytime anyone asks for anything on the Internet, either they or other folks on your LAN will ask for the same thing again—and that's why caching works so well in so many different ways. Caching reduces network workload by eliminating the processes required to reacquire data. Caching reduces network traffic and server workloads.

The challenge to caching is identifying all the diverse places one can cache. Different caching methods and devices have already been discussed in the book. Refer back to Chapter 10, "Network Naming," for DNS caching and Chapter 12, "Advanced Networking Devices," for proxy servers for two examples. To put it simply: when you can cache, do it!

Controlling Data Throughput

Despite the derision aimed at the remarks made by a certain U.S. senator a few years ago to the effect that the Internet is made out of "a series of pipes," there's actually a strong argument for the idea of pipes when discussing the amount of data per second any given Internet connection may need. Unless your budget allows you to buy a "big pipe" connection to the Internet, every network suffers from a limited amount of bandwidth that's rarely truly sufficient for everything your users need. Even if you're lucky enough to have good bandwidth today, ongoing network growth guarantees you'll eventually run into network slowdowns as demand grows.

There's no magic point at which a network goes from working well to working slowly. Most people are used to having to wait a bit for a Web page or a file transfer. Certain applications, called *latency-sensitive* applications, do not perform well when they lack adequate bandwidth. Some latency-sensitive applications require high bandwidth. Streaming video is a great example. Have you ever watched a video on YouTube that constantly stops and starts? At least YouTube enables you to pause the video so it can load more before you continue watching (Figure 18.16).



• **Figure 18.16** Pausing a video on YouTube

Try watching a video on Hulu.com (Figure 18.17) over an overly busy or slow connection. Hulu, unlike YouTube but like most other video sites, only caches a few seconds (to prevent people from stealing the video) and is all but unwatchable if there are constant stops and starts. Voice over IP (VoIP) applications are another great example. If every conversation is clipped . . . and . . . chopped . . . the beauty of VoIP falls apart.

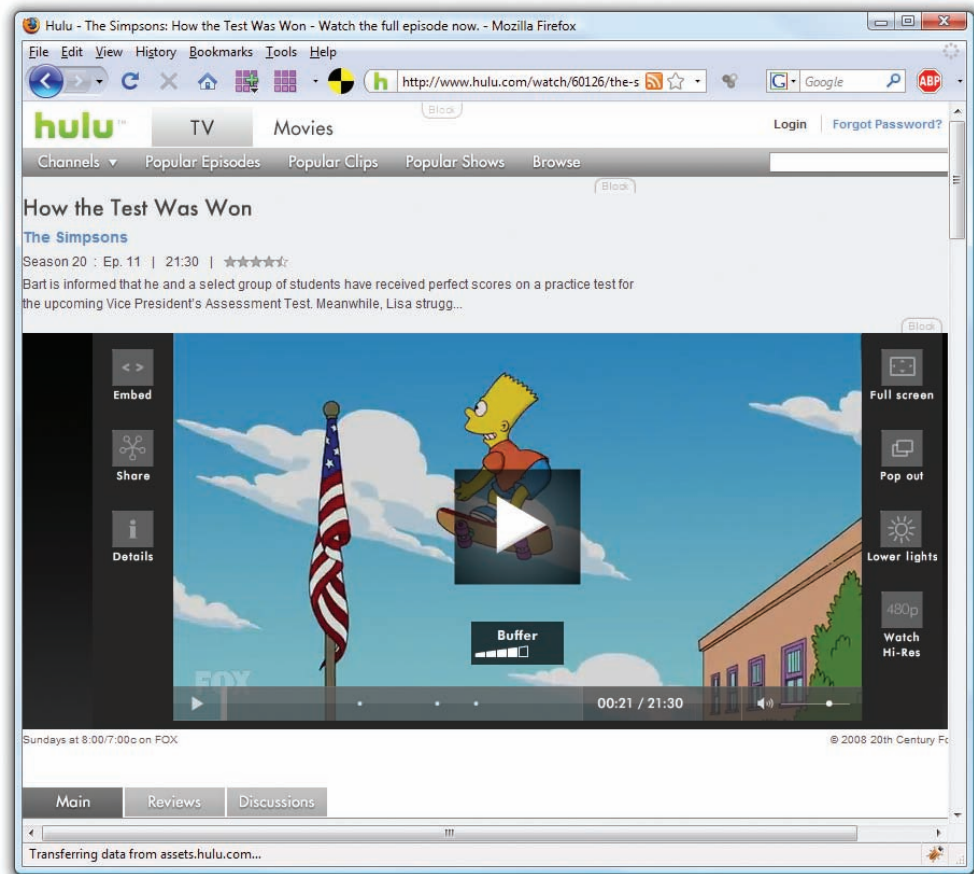
When the size of your Internet pipe is limited, you need some method to throttle bandwidth so that in high-demand times latency-sensitive applications get more bandwidth at the cost of reducing bandwidth to those applications that don't mind the wait. The CompTIA Network+ exam mentions two of the most common: quality of service (QoS) and traffic shaping, both of which you learned about in Chapter 12, "Advanced Networking Devices." Here's a quick recap and some extra details.

Quality of Service

Quality of service (QoS) is a procedure used almost exclusively on gateway devices to give certain applications priority when a connection reaches a certain amount of utilization. QoS works at Layer 2 of the OSI model and works with 802.1Q trunks to prioritize traffic. QoS applies a Class of Service (CoS) priority (0 to 7) to a certain port. As traffic from that port goes through



QoS is particularly helpful to reduce jitter on VoIP connections.



• **Figure 18.17** Hulu.com (I love this site!)



When ISPs limit traffic based on applications to customers, it is called bandwidth throttling.

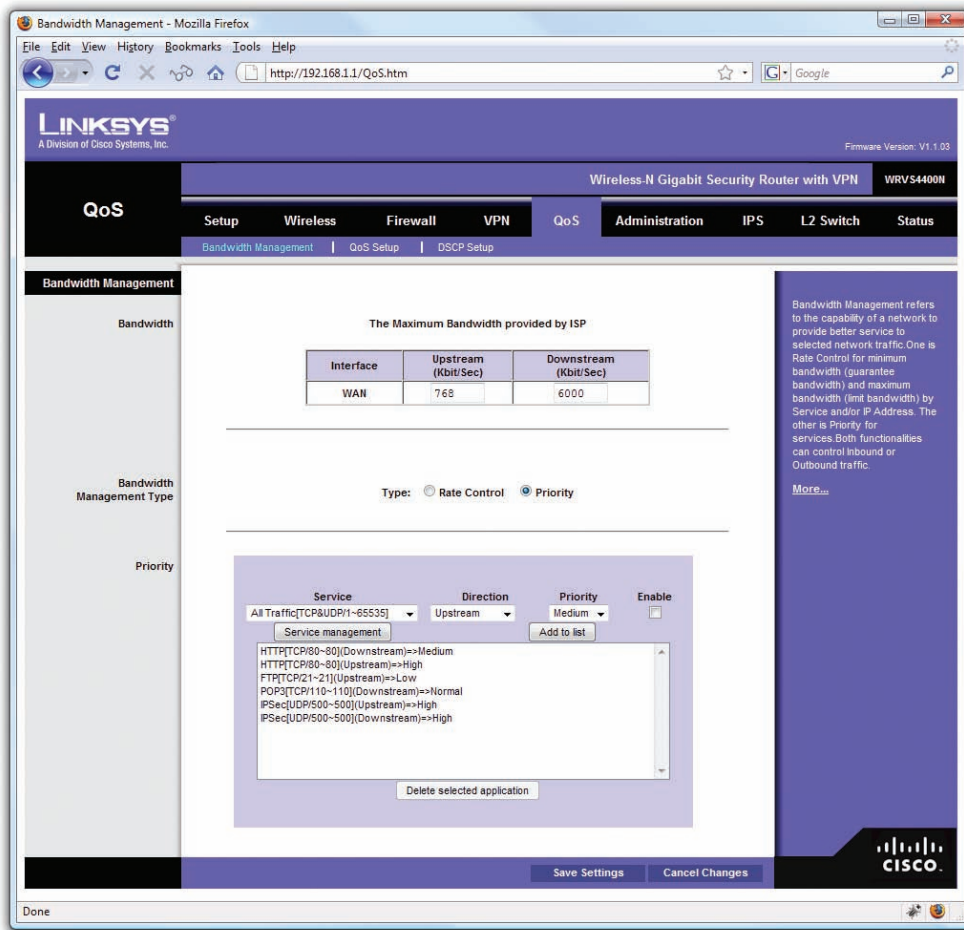
a trunk line, its priority defines how much bandwidth is allocated. The higher the priority of traffic, the more bandwidth it gets. This form of QoS is specialized when you have high-priority file server or VoIP server systems connected to your network.

Traffic Shaping

Traffic shaping (also called bandwidth shaping) prioritizes traffic at Layer 3 and Layer 7 of the OSI seven-layer model. Traffic shaping usually works at the edge routers, placing priority on traffic based usually on TCP/UDP port number. Traffic shaping works in either of two ways: by giving certain packets a priority or by directly assigning a fixed amount of bandwidth (in bits/sec) to packets from a particular application based on port number.

A typical setup of traffic shaping first requires you to tell the router the total upstream and downstream bandwidth of your connection. From there, you assign bandwidth to a particular application, as shown in Figure 18.18

QoS and traffic shaping give you a number of tools to control traffic. You can control or prioritize traffic based on port/MAC address (QoS), IP address, or application. The choice depends on the equipment you choose and the needs of your networks.



• Figure 18.18 Traffic shaping on a SOHO router

Keeping Resources Available

No throttling or QoS does you a bit of good if the resource itself isn't available due to problems with the hardware. There are two areas where hardware limitations come into play. First is some form of hardware failure. Anyone who has worked on a PC for more than a few months knows one thing: hardware fails. Second, the design of the Internet dictates that a single IP address be given to a resource. Every Web server has a single IP address; every e-mail server eventually goes back to one IP address. This creates a problem when a resource becomes popular, because no single machine could ever handle the demands of a www.yahoo.com or a www.google.com. No worries, though, because there are many techniques to make multiple physical servers look as though they're a single IP address. Collectively, these techniques make sure that a shared resource is available in a timely manner when clients request it: what we call **high availability**.

Proper network management requires **fault tolerance**: systems that can continue to provide network functions even in the face of catastrophic hardware failure. Ensuring fault tolerance begins with a plain old **data backup**,

where you make a copy of all important files and folders, but then quickly goes into redundant hardware, real-time load balancing, and more.

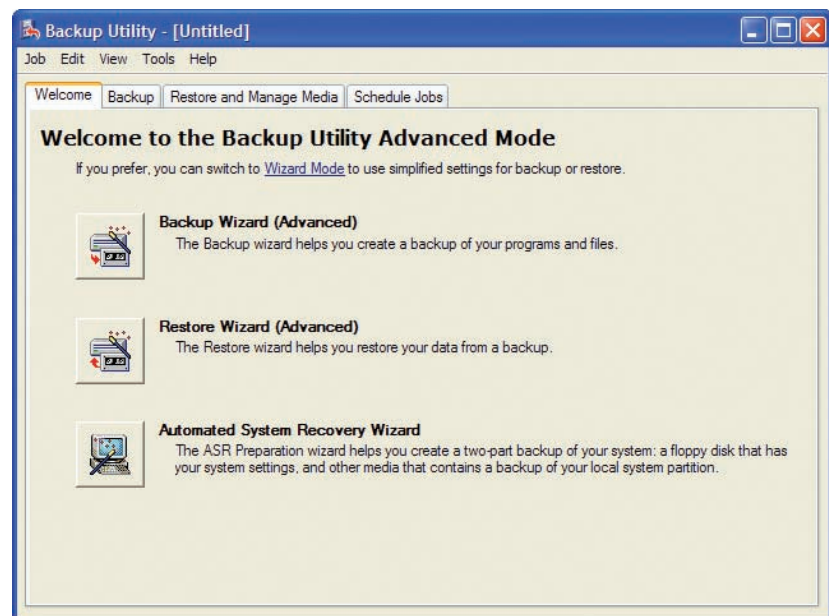
Data Backup

Without a solid data backup, you're sunk if too much hardware goes down too quickly. Proper backup routines require both software and hardware to create, preferably, removable or remote backup of all data.

Most operating systems come with some type of backup program, plus developers offer many third-party tools. Figure 18.19 shows the venerable Backup for Windows. Third-party tools include Veritas NetBackup from Symantec and CA ARCserve Backup (from the company formerly known as Computer Associates), both of which offer enterprise-level backup and recovery tools.

Most backup software looks first to tape backup devices and then to hard drive or networked storage for backup. Use of tape drives seemed to be on the wane a few years ago, but they have made a strong comeback as a storage medium. Tape is relatively inexpensive and quite reliable over a long period of time. Some of the big players in tape drives include Dell, HP, IBM, and Qualstar.

The goal of backing up data is to ensure that when a system dies, there will be an available, recent copy you can use to restore the system. You could simply back up the complete system at the end of each day—or whatever interval you feel is prudent to keep the backups fresh—but complete backups can be a tremendous waste of time and materials. Instead of backing up the entire system, take advantage of the fact that all the files won't be changed in any given period; much of the time you only need to back up what's changed since your last backup. Recognizing this, most backup software solutions have a series of options available beyond the old complete (usually called Full or Normal) backup.



• Figure 18.19 Windows Backup

The key to understanding backups other than the full backup is *attributes*, 1-bit storage areas that all files have. The most common attributes are Hidden (don't show the file in Computer or when `dir` is typed at the command line), System (it's a critical file for the system), Read-Only (can't erase it), and Archive. These attributes were first used in FAT-formatted drives in the DOS era, but they are still completely supported today by all file formats. The **archive bit** works basically like this: whenever a file is saved, the archive bit is turned on. Simply opening a file will affect the current state of the archive bit. Backup programs will usually turn off a file's archive bit when the file is backed up. In theory, if a file's archive bit is turned off, it means there's a good backup of that file on some tape. If the archive bit is turned -on, it means that the file has been changed since it was last backed up (see Figure 18-20).

Archive bits are used to perform backups that are not full backups. The following backup types are most often supported:

- A **normal backup** is a full backup. Every file selected will be backed up, and the archive bit will be turned off for every file backed up. This is the standard "back it all up" option.
- A **copy backup** is identical to a normal backup, with the important distinction being that the archive bits are *not* changed. This is used (although not often) for making extra copies of a previously completed backup.
- An **incremental backup** includes only files with the archive bit turned on. In other words, it copies only the files that have been changed since the last backup. This backup turns off the archive bits.
- A **differential backup** is identical to an incremental backup, except that it doesn't turn off the archive bits.
- A **daily backup**, also known as a daily copy backup, makes copies of all the files that have been changed that day. It does not change the archive bits.

The motivation for having both the incremental and differential backups may not be clear at first glance—they seem so similar as to be basically the same. Incremental seems the better option at first. If a file is backed up, you would want to turn off the archive bit, right? Well, maybe. But there is one



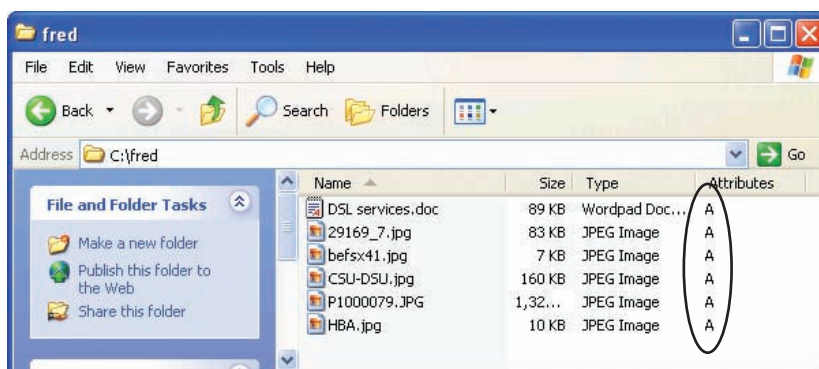
Tech Tip

Customizing Explorer in Windows XP/Vista

Windows Explorer (My Computer in Windows XP, Computer in Vista) by default does not show much about files in any view, even when you select Details from the View menu. The Details view is highly customizable, however, and can reveal a phenomenal amount and variety of information about files. To customize your view, alternate-click (right-click) the column bar (the gray bar that says Name, Size, Type, Date Modified, and so forth) to look at the default choices. You'll see everything from Attributes, Owner, Author, and Title, to file-type specific information such as Genre, Duration, and Bit Rate (for music files). If the default extra view options don't get your motor revving, selecting the More option brings up a menu offering many more view options! For the purposes of this section, click the Attribute box to display file and folder attributes.



Be sure you know the different types of backups, including which ones change the archive bits and which ones do not.



• **Figure 18.20** The archive bit on these files is on

Incremental				
MON	TUE	WED	THU	FRI
Full Backup	All Tuesday Changes	All Wednesday Changes	All Thursday Changes	All Friday Changes

Differential				
MON	TUE	WED	THU	FRI
Full Backup	All Changes Through Tuesday	All Changes Through Wednesday	All Changes Through Thursday	All Changes Through Friday

• **Figure 18.21** Incremental vs. differential

scenario where that might not be too attractive. Most backups do a big weekly normal backup, followed by daily incremental or differential backups at the end of every business day. Figure 18-21 shows the difference between incremental and differential backups.

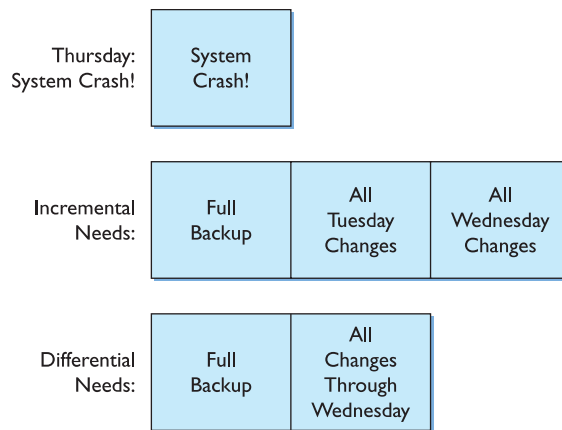
Notice that a differential backup is a cumulative backup. Because the archive bits are not set, it keeps backing up all changes since the last normal backup. This means the backup files will get progressively larger throughout the week (assuming a standard weekly normal backup). The incremental backup, by contrast, only backs up files changed since the last backup. Each incremental backup file will be relatively small and also totally different from the previous backup file.

Let's assume that the system is wiped out on a Thursday morning. How can you restore the system to a useful state?

If you're using an incremental backup, you will first have to restore the last weekly backup you ran on Monday, then the Tuesday backup, and then the Wednesday backup before the system is restored to its Thursday morning state. The longer the time between normal backups, the more incremental backups you must restore.

Using the same scenario, but assuming you're doing differential instead of incremental backups, you'll only need the weekly backup, and then the Wednesday backup to restore your system. A differential backup will always require only two backups to restore a system (see Figure 18-22). Suddenly, the differential backup looks better than the incremental! On the other hand, one big benefit of incremental over differential is backup file size. Differential backup files will be massive compared to incremental ones.

One of the typical regimens or rotations for backing up to tape or to external hard drive and rotating media is called **grandfather, father, son (GFS)**, and it works like this. Typically, you'd have a weekly and daily backup. You run a full backup once a week and typically store the tape offsite. Then you'd run a differential backup each day. The full backup is the father and the differential backups are the son. The grandfather would be the last full backup of the month that then gets stored off site. Using such a strategy enables you to restore by previous months, weeks, or days.



• **Figure 18.22** Restoring from backups

Choosing between incremental backups and differential backups is only one factor in choosing how you back up your data. You must also consider your business, your data, your backup hardware, your operating systems, and other factors to create a backup strategy.

UPS An **uninterruptible power supply (UPS)** keeps your servers afloat in the event of an electrical brownout or blackout. Without a good UPS, you simply cannot guarantee the proper level of uptime for your server. A UPS enables a computer to function for a short period of time, but for extended outages, there's only one answer: backup generators.


Backup Generators For extended blackouts, such as when Hurricane Ike took down my office (and much of the Gulf Coast) for several weeks in 2008, you need to have backup generators to guarantee any hope of uninterrupted uptime. A **backup generator** runs on some sort of fuel (often diesel or gasoline) to provide electricity.

RAID and Redundant Hardware Once you've secured the electricity for your servers, you need to make sure that individual components within the system don't take out your entire server. Most commonly, these redundant pieces of hardware include multiple hard drives, power supplies, and network connections.

As you most likely recall from studying for your CompTIA A+ exam, you can use two or more hard drives to provide fault tolerance through one of the several levels of **Redundant Array of Independent Disks (RAID)**. There are three RAID levels commonly used in networks: RAID 0, RAID 1, and RAID 5.

RAID 0 is known as striping. Requiring at least two drives, RAID 0 breaks files into chunks called stripes and spreads the stripes across each drive in the RAID 0 array. RAID 0 arrays are fast, but if one drive dies you lose everything. There's no fault tolerance with RAID 0.

RAID 1 is mirroring. Again requiring at least two drives, RAID 1 makes a copy of every stripe and places it on each drive. RAID 1 arrays have great fault tolerance, but because every file is copied twice they're slower than RAID 0 arrays.


Tech Tip

Stand By Your UPS

Uninterruptible power supplies differ a lot in how they work and in the quality of electricity they provide. The standard device we call a UPS is actually a standby power supply as it takes a few milliseconds to bring the power online. These are fine and they are much cheaper than a true UPS.



Try This!

Shopping for RAID

Many current motherboards support RAID, right out of the box, so here's a shopping trip to see what's out there. If you have a computer store handy in your neighborhood, check out its motherboards. What kind of RAID can you find? What's the price difference between a motherboard with RAID 0 and 1 versus one with RAID 5 as well? What seems to be the sweet spot for price and protection?



The CompTIA Network+ exam doesn't require you to know the different levels of RAID.



You might recall another use for a second network connection—bonding, using multiple NICs to increase your throughput. Bonding provides no fault tolerance but can be very useful if you have an overly busy server!

RAID 5 is disk striping with distributed parity. RAID 5 requires at least three drives. RAID 5 takes stripes, performs a parity calculation, and then stores the stripes and the parity across the drives in the array. If a single drive fails, the RAID array can rebuild the data. RAID 5 is fast and provides good fault tolerance.

Redundant power supplies and network connections provide

exactly what their names suggest. The spare power supply should kick on automatically if the main power supply dies for some reason. The spare network connection can do the same for either a dead NIC or a dead connection.

Cluster Servers and Load Balancing If you're not content with duplicating hardware components inside a server, you're not alone. Many network installations reproduce entire servers or use multiple servers that act as a cluster server, so that if any server goes down, the rest just pick up the slack and keep on chugging. Clustering servers requires cluster-aware operating systems, such as Windows Server for the Enterprise.

Clustered servers can also balance the load when dealing with heavy usage, as you'll recall from the discussion of busy Web servers in Chapter 12. When scaled up and done right, to the end user there's only one identity. Google.com's home page might be balanced on 20 giant servers, for example, but you merely type in www.google.com and away you go.

Chapter 18 Review

■ Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about network management.

Describe how configuration management documentation enables you to manage and upgrade a network efficiently

- The more complicated a network is, the more vulnerable it is in terms of security, efficiency, and other aspects. Configuration management helps you maintain and update your network in a logical and orderly fashion to lessen these vulnerabilities.
- Networks should be standardized on the types of NICs, cabling, network operating systems, and network applications to make upgrades to the network as efficient as possible.
- Configuration management documentation includes wiring diagrams, network diagrams, baselines, policies, procedures, configurations, and regulations.
- A wiring diagram (or wiring schematic), which usually consists of multiple pages, shows how the wires in a network connect to switches and other nodes, what types of cable are used, and how patch panels are configured, and usually includes details about each and every cable run.
- It is the cable puller's job to create the wiring schematic. In office buildings, the schematic often includes telephone wires. The schematic itself is usually kept by the people in charge of the building (building services).
- A physical network diagram is similar to a wiring schematic, but defines the type of connection such as Gigabit Ethernet, T1, and so forth. It also includes every router, switch, server, CSU/DSU, cable modem, wireless access point, and details about each.
- The network administrator should create the physical network diagram, using standardized icons and one of the many diagramming programs, such as Microsoft Visio.
- A logical network diagram shows the broadcast domains and individual IP addresses for all

devices on the network. Only critical switches and routers are shown.

- A baseline is a log of performance indicators, such as CPU usage, network utilization, and other values that describe how the network functions when things are working normally. The Performance Monitor utility that comes with Windows is helpful for creating baselines on individual Windows systems.
- Procedure and policy documentation should state what people can and cannot do with network hardware and software. Acceptable use policies and security policies are two such policies.
- Configuration settings of routers, switches, and other network devices should be documented in case they lose their settings or have to be replaced. Documenting the configuration helps to ensure that policies and procedures can still be enforced after devices have been replaced or reprogrammed.
- Regulations govern behavior in the workplace, such as what to do when a particular event occurs. Regulations should be part of your configuration management documentation.
- Change management documentation details the procedures and policies to update other documentation. For example, if a change was made to the network, the change management documentation would describe which other documents had to be updated to keep track of the change.

Conduct network monitoring to identify performance and connectivity issues

- Baselines create a benchmark or standard measurement of when everything is working correctly on your network. Consider this to be a snapshot of your systems. On a Windows computer, Performance Monitor (PerfMon) watches itself or other Windows machines, either locally or remotely.
- Every operating system creates a variety of logs automatically. These can typically be categorized as System, Application, and Security logs. In Windows, use Event Viewer to view these logs.

In Linux, most of these logs reside in the /VAR/LOG directory. On a Mac, use the GUI log viewer called Console.

- The Application log tracks events that take place with individual applications, such as starts, stops, start failures, crashes, and so forth.
- The Security log tracks anything that affects security, such as successful and failed logons and logoffs.
- The System log covers issues dealing with the overall system, such as system services, device drivers, or configuration changes.

Explain how to optimize network performance

- Quality of service is a procedure used almost exclusively on gateway devices to give certain applications priority when a connection reaches a certain amount of utilization.
- Traffic shaping (or bandwidth shaping) prioritizes traffic at Layers 3 and 7 of the OSI model. Usually in effect at the edge routers, certain packets are given priority or a fixed amount of bandwidth is allocated to packets from a particular application based on port number.
- High availability describes a situation in which a resource is available when a client requests it. QoS, bandwidth shaping, and fault tolerance help to increase the potential for high availability.
- A system that is fault tolerant can continue to function even in the face of catastrophic hardware failure. Fault tolerance can be accomplished through data backups, redundant hardware, and real-time load balancing.
- Proper backup routines require both software and hardware, including backup software such as Windows Backup, Veritas NetBackup, or CA ARCserve Backup and appropriate hardware on which to store the data backups. Backup hardware can include hard drives or tape drives.
- In a full backup, every file selected will be backed up, and the archive bit will be turned off for every file backed up. This is the standard “back it all up” option.
- A copy backup is identical to a normal backup, with the important distinction being that the archive bits are not changed. This is used (although not often) for making extra copies of a previously completed backup.
- An incremental backup includes only files with the archive bit turned on. In other words, it copies only the files that have been changed since the last backup. This backup turns off the archive bits.
- A differential backup is identical to an incremental backup, except that it doesn’t turn off the archive bits.
- Full backups get everything but require the most space and take the longest. Incremental backups are quick and use very little space; differential backups take longer than incremental backups and use more space, but they potentially offer a much quicker restore time.
- A UPS keeps delivering power to your devices for a short period of time in the event of a power outage. For extended periods of power outages, you need a backup generator.
- Servers using RAID can continue to function and serve data even if a hard drive crashes. RAID 1 and RAID 5 both offer fault tolerance.
- Clustering servers allows multiple servers to appear as a single server. This offers fault tolerance in the event one server goes down. Creating and managing clustered servers requires special operating systems, such as Windows Server for the Enterprise.
- Clustered servers can also implement load balancing to spread out client requests equally among all the clustered servers. This helps to ensure that no single machine is overloaded.

■ Key Terms

acceptable use policy (489)

Application log (495)

archive bit (501)

backup generator (503)

baseline (489)

change management documentation (490)

configuration management (485)

configuration management documentation (485)

configurations (489)

copy backup (501)

counter (491)

daily backup (501)

data backup (499)
differential backup (501)
fault tolerance (499)
grandfather, father, son (GFS) (502)
high availability (499)
incremental backup (501)
logical network diagram (487)
normal backup (501)
object (491)
Performance Monitor (PerfMon) (491)
physical network diagram (486)

quality of service (QoS) (497)
Redundant Array of Independent Disks (RAID) (503)
regulations (490)
Security log (495)
security policy (489)
System log (495)
traffic shaping (498)
uninterruptible power supply (UPS) (503)
view (491)
wiring diagram (485)
wiring schematic (485)

■ Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all the terms will be used.

1. The best Windows software tool to use when trying to establish baselines is _____.
2. A(n) _____ shows all the wiring in a building, often including the telephone system, and is kept by the people in charge of the building.
3. The _____ tracks successful and failed logons and logoffs.
4. When network resources are always ready whenever a client requests them, they are said to have _____.
5. A(n) _____ provides long-term power in the event of an extended blackout.
6. A(n) _____ shows the broadcast domains and individual IP addresses for all the devices in your network.
7. A(n) _____ shows cabling runs and the type of connection in addition to showing every router, switch, and server and their makes, models, and firmware versions.
8. A(n) _____ provides short-term power in the event of a brownout.
9. A(n) _____ copies only the files that have been changed since the last backup. This backup turns off the archive bits.
10. A(n) _____ defines exactly what you can and cannot do with your computers and network.

■ Multiple-Choice Quiz

1. What should be created to establish normal operating conditions on your network?
 - A. Backups
 - B. Baselines
 - C. Remote access
 - D. Troubleshooting
2. Where could you find a list of problems that occurred on a system?
 - A. Wiring schematic
 - B. Event Viewer
 - C. Performance Monitor
 - D. RAID
3. Where should backup tapes be kept?
 - A. In the server room
 - B. On a shelf in the storeroom
 - C. In a locked cabinet away from the server room
 - D. In the boss's car trunk
4. Your boss asks you for a diagram showing every server on the network. What do you provide to her?
 - A. Logical network diagram
 - B. Physical network diagram
 - C. Wiring schematic
 - D. Baseline

5. You are hired as a consultant to troubleshoot a network. Your client reports the network has recently slowed significantly. What should you ask to see first?
 - A. Baseline
 - B. Security policy
 - C. Application logs
 - D. PerfMon counters
6. When using Performance Monitor, what do you call the actual component you want to monitor?
 - A. Counter
 - B. Histogram
 - C. Object
 - D. View
7. You are using Performance Monitor to monitor the CPU. You need to define what aspects of the CPU to monitor, such as the percentage in use and the percentage free. What must you configure?
 - A. Counter
 - B. Histogram
 - C. Object
 - D. View
8. Which types of logs are automatically created? (Select three.)
 - A. Application
 - B. Login
 - C. Security
 - D. System
9. What technology ensures data is still immediately available in the event of a hard drive crash?
 - A. Backup generator
 - B. UPS
 - C. GFS
 - D. RAID
10. Where can you find the log files on most Linux installations?
 - A. /VAR/LOG
 - B. /CONFIG/LOG
 - C. /ADMIN/LOGS
 - D. /LOGFILES
11. How can you connect to another computer named SERVER2 using the Universal Naming Convention?
 - A. http://SERVER2
 - B. //SERVER2
 - C. \\SERVER2
 - D. SERVER2/
12. Which program can be used to create baselines?
 - A. Event Viewer
 - B. Performance Monitor
 - C. Microsoft Visio
 - D. Veritas NetBackup
13. Which backup type always requires only two backups to restore a system?
 - A. Copy backup.
 - B. Differential backup
 - C. Full backup
 - D. Incremental backup
14. What is defined in a security policy? (Select two.)
 - A. What users can and cannot do with their computers
 - B. How complex user passwords should be
 - C. How to deal with social engineering hacking attempts
 - D. How users should install their own software
15. What can help to maintain high availability? (Select three.)
 - A. QoS
 - B. RAID
 - C. VoIP
 - D. UPS

■ Essay Quiz

1. Some students in class are discussing when tape backups should be performed. One student says daily, during nonpeak hours, while another student suggests weekly. A third student says both students are correct. The trio suddenly looks at you for your definitive answer. Write down what you would say.
2. How can you view log files on Windows, Linux, and Macintosh OS X computers?
3. An intern has come to you confused and stressed because he has been asked to review the configuration management documentation. Ease the poor guy's mind and explain the difference between a wiring schematic, physical network diagram, logical network diagram, policy, procedure, configuration, regulation, acceptable use policy, and security policy.

Lab Projects

• Lab Project 18.1

Create a step-by-step guide for using Performance Monitor to create a baseline. Swap guides with a classmate and see if you can follow each other's

steps. If either of you has problems, go back and fix your steps to make them clearer.

• Lab Project 18.2

Use the Internet to find Network+ practice questions. Try to locate as many troubleshooting scenario questions in the time allowed. Share your findings with classmates who have done the same.

The more practice questions you cover as a group, the better prepared you will be to handle real questions on the Network+ exam.