Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**12**

**Performance and Recovery**

* [Module Introduction](javascript://)
* **12-1**[Collect Network Data](javascript://)
  + **12-1a**[Environmental Monitoring](javascript://)
  + **12-1b**[Traffic Monitoring Tools](javascript://)
* **12-2**[Manage Network Traffic](javascript://)
  + **12-2a**[Performance Baselines](javascript://)
  + **12-2b**[Bandwidth Management](javascript://)
  + **12-2c**[Flow Control](javascript://)
  + **12-2d**[Congestion Control](javascript://)
  + **12-2e**[QoS (Quality of Service) Assurance](javascript://)
* **12-3**[Plan Response and Recovery Strategies](javascript://)
  + **12-3a**[Incident Response](javascript://)
  + **12-3b**[Data Preservation](javascript://)
  + **12-3c**[Disaster Recovery Planning](javascript://)
  + **12-3d**[Disaster Recovery Contingencies](javascript://)
  + **12-3e**[Power Management](javascript://)
  + **12-3f**[Backup Systems](javascript://)
* **12-4**[Module Review](javascript://)
  + **12-4a**[Module Summary](javascript://)
  + **12-4b**[Key Terms](javascript://)
  + **12-4c**[Review Questions](javascript://)
  + **12-4d**[Hands-On Projects](javascript://)
  + **12-4e**[Capstone Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Introduction

### Objectives

After reading this module and completing the exercises, you should be able to:

* **1**Use appropriate tools to collect data about the network
* **2**Identify methods to optimize network performance
* **3**Identify best practices for incident response and disaster recovery

**On the Job**

Recently, the CISO (Chief Information Security Officer) of an organization determined that there was an increase in network latency, and my team was tasked to root out the culprit. All the usual suspects were tested in our attempt to isolate the problem. Malware scans on the network showed no issues. We looked for employees streaming music or video feeds, but those ideas also proved unfruitful. Finally, we turned on the IDS and used Wireshark to monitor all traffic in and out of the network.

Initially, nothing stood out. But once the daily traffic patterns were laid over our network baseline, there it was staring at us: Rogue devices on the network were consuming a higher than usual amount of bandwidth. These devices were likely employee-owned devices that had been connected to the network without permission. The MAC addresses of these high-consumption devices did not match any of the corporate-owned devices on our inventory list.

As a team we brainstormed ideas to combat the issue. Simply changing the wireless network SSID and password would not suffice, as employees would likely just reconnect their personal devices when they were given the information for their work-owned devices.

Instead, we developed a more complex strategy. First, we blocked all non-company device MAC addresses on the wireless access points. We did this easily enough by consulting the asset inventory list and inputting all corporate-owned devices on a whitelist. We then decided to enable 802.1X on the network switches to ensure only company-owned devices would be able to connect to the wired network, thereby preventing any further issues with rogue devices. We deployed 802.1X utilizing certificate-based credentials that could easily be deployed to all corporate-owned devices. This provided another layer of protection for the wireless network and also allowed us to control wired network access. Finally, we validated the solution by reexamining a network traffic file and confirmed the solution was having the intended effect. Then we just had to answer all the new trouble call tickets about the wireless network no longer working on their personal devices!

**Nicholas Pierce**

**Instructor**

**Thomas Nelson Community College**

Because networks are a vital part of keeping an organization running, you must pay careful attention to measures that keep network resources safe, available, and performing well. Throughout this course, you have learned about building scalable, reliable networks as well as selecting the most appropriate hardware, topologies, and services to operate your network. You have also learned about security measures to guard network access and resources. In this module, you will learn how to optimize networks for today’s high bandwidth needs, protect your network’s performance from faults and failures, and recover in the event your network experiences a minor outage or a more severe disaster. With proper adjustments, redundancies, and preparations, you can create and maintain a resilient network.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 12-1Collect Network Data

### Certification

* 1.5

Explain common ports and protocols, their application, and encrypted alternatives.

* 2.3

Given a scenario, configure and deploy common Ethernet switching features.

* 3.1

Given a scenario, use the appropriate statistics and sensors to ensure network availability.

* 4.3

Given a scenario, apply network hardening techniques.

* 5.3

Given a scenario, use the appropriate network software tools and commands.

Average reading time: 41 minutes

Network management is a general term that means different things to different networking professionals. At its broadest, [**network management**](javascript://) refers to the assessment, monitoring, and maintenance of all aspects of a network. It can include controlling user access to network resources, monitoring performance baselines, checking for hardware faults, ensuring optimized QoS (quality of service) for critical applications, maintaining records of network assets and software configurations, and determining what time of day is best for upgrading hardware and software.

Several disciplines fall under the heading of network management. All share the goals of enhancing efficiency and performance while preventing costly downtime or loss. Ideally, network management accomplishes these tasks by helping the administrator predict problems before they occur. For example, a trend in network usage could indicate when a switch will be overwhelmed with traffic. In response, the network administrator could increase the switch’s processing capabilities or replace the switch before users begin experiencing slow or dropped connections.

Before you can assess and make predictions about a network’s health, however, you must first understand its logical and physical structure and how it functions under typical conditions. And to do that, you must be able to collect data about the network’s state, devices, and traffic. Let’s begin this discussion with a look at how to monitor the network’s physical environment. You’ll then learn techniques for monitoring the network itself.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-1aEnvironmental Monitoring

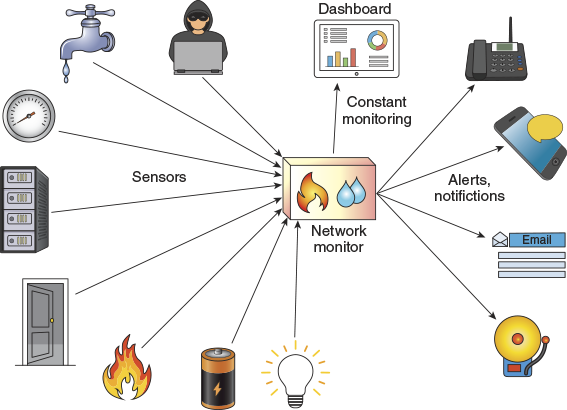
The best network security and traffic optimization in the world won’t do your network any good if the physical environment is not properly maintained. It’s essential to monitor the following environmental factors, optimizing for best performance as necessary, to ensure your network functions reliably:

* Device, rack, or room temperature
* Device, rack, or room humidity, dew point, or barometric pressure
* Flooding as sensed by liquid detectors
* Smoke or fire
* Airflow
* Vibration
* Motion as sensed by security cameras
* Room lights on or off
* Room or rack doors open or closed
* Power (main or UPS voltage, battery level, outages, power consumption)

Monitoring sensors in each data room, equipment rack, or device chassis feed information to a physical device or software installed on a server. This data is then presented in an administrative dashboard to network administrators (see [Figure 12-1](javascript://)). This dashboard might be accessed over the network or over the Internet, even on a smartphone, allowing network admins to check current environmental data, adjust alarm thresholds, analyze historical data, and respond to alerts. For example, the Room Alert Monitor by AVTECH ([avtech.com](http://avtech.com/" \t "_blank)) displays sensor data on a configurable dashboard (see [Figure 12-2](javascript://)).

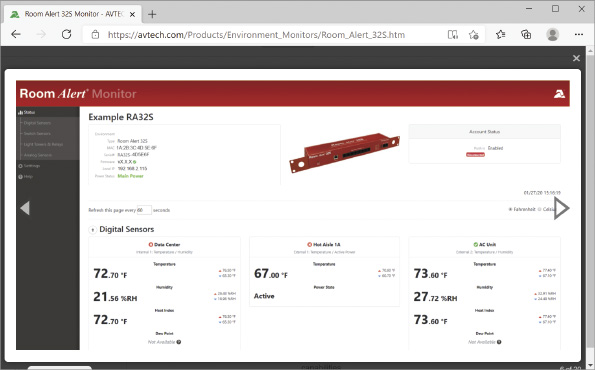
**Figure 12-1**

Sensors feed data to the network monitor, which outputs information to dashboards and alerts or notifications



**Figure 12-2**

A dashboard provides constant monitoring



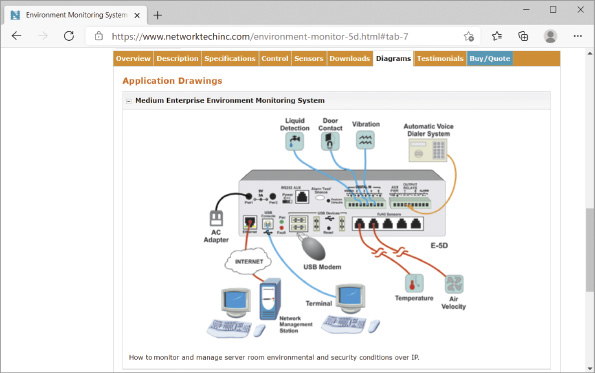
Enlarge Image

Source: AVTECH Software, Inc.

Environment monitoring hardware might have dual power connectors for redundancy, a USB console connector for configuration from an attached laptop, a web interface for configuration over the network, additional USB ports for connection to a modem or for saving logs to flash drives, and the ability to maintain wireless connections with sensors. [Figure 12-3](javascript://) shows a diagram of the various connectors on NTI’s (Network Technologies Inc.) ENVIROMUX device for medium enterprises. You can see demonstration videos at their website: [networktechinc.com/enviro-monitor.html](http://networktechinc.com/enviro-monitor.html" \t "_blank).

**Figure 12-3**

Ports provide built-in redundancy and flexibility



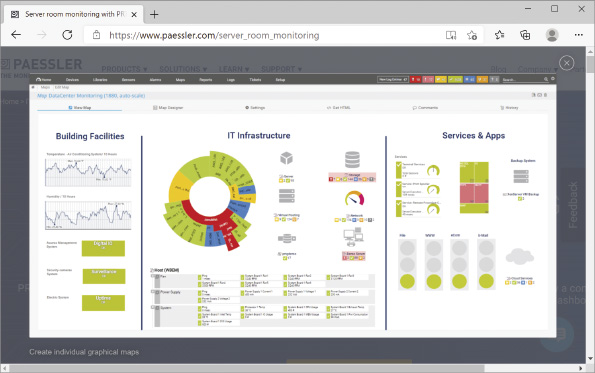
Enlarge Image

Source: Network Technologies Inc.

On the software side, products such as PRTG Network Monitor by Paessler ([paessler.com](http://paessler.com/" \t "_blank)) work with ICMP, SNMP, WMI, HTTPS, and others to collect and organize information about monitored devices and sensors. For example, your servers’ CPU temperatures and other data can be collected and monitored through the PRTG dashboard (see [Figure 12-4](javascript://)). Alerts from monitoring software can be transmitted via email, SMS (Short Message Service, which sends text messages), phone calls, push notifications, audible alerts (such as a siren or voice alert), SNMP traps (you’ll learn more about SNMP later in this section), or other options. Monitoring solutions sometimes offer the ability to remotely control some environmental factors, such as adjusting room temperature. In a project at the end of this module, you’ll install PRTG in a VM and use the network monitor to detect information about other devices on your network.

**Figure 12-4**

Custom dashboards provide insights at a glance



Enlarge Image

Source: Paessler AG

**Applying Concepts 12-1**

### Check Windows 10 Performance Statistics

Much of the data collected by environmental monitoring systems indicates health and status of individual devices on the network, such as a server’s CPU usage, demand on memory resources, available storage space, network throughput, and uptime versus downtime. You can see this kind of information for your own Windows 10 computer in Task Manager. Complete the following steps:

1. 1

Press **Ctrl + Alt + Del** and then click **Task Manager**. Click the **Performance** tab.

1. 2

Notice the numbers are changing constantly as you use your computer. Perhaps you’re playing some music in the background, or you have a social media site open that is frequently updating. Take a snapshot of each screen as needed to answer the following questions about your computer:

* 1. What is your CPU’s Utilization and Up time? How many processes are currently running on your CPU?
  2. How much memory is available on your computer? How much of your available memory is in use?
  3. How many storage drives are connected to your computer? What is your primary drive’s Read speed and Write speed?
  4. How many network connections does your computer list? What is the maximum possible throughput for the primary network connection?

1. 3

Click **Open Resource Monitor**. Which resources are monitored here?

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-1bTraffic Monitoring Tools

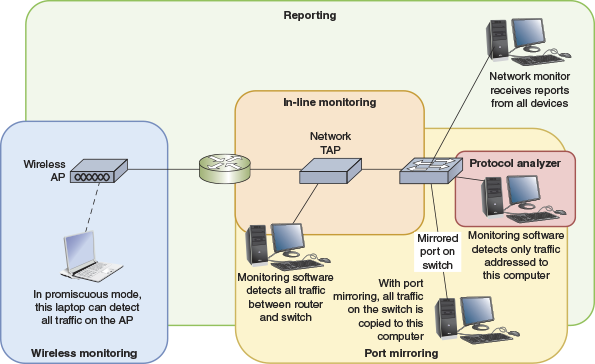
As you confirm the network’s physical environment and its various devices are operating within expected parameters, you’ll also need to monitor the traffic flowing between devices. Some traffic monitoring tools will provide real-time analysis of data with alerts when conditions meet certain thresholds, while other tools are designed to log data for retroactive analysis only as needed. These historical [**traffic logs**](javascript://) are primarily used to investigate network performance issues. The challenge with both real-time network monitoring and traffic logging is gaining access to the traffic itself. Consider the following explanation of how network monitors work.

A network monitor is a tool that continually monitors network traffic and might receive data from monitored devices that are configured to report their statistics. A similar tool, a protocol analyzer, can monitor traffic at a specific interface between a server or client and the network. In practice, these two terms—network monitor and protocol analyzer—are often used interchangeably. However, they differ significantly when it comes to the kinds of data you can expect to gather with each tool. Think about the difference between monitoring the traffic that a single device encounters on its connection to the network, versus monitoring devices and traffic patterns throughout the network. For example, Spiceworks is a type of network monitoring software because it can be configured to monitor multiple devices on a network at one time. Wireshark is a type of protocol analyzer because it monitors traffic on the interface between a single device and the network.

Wireshark or other monitoring applications running on a single computer connected to a switch don’t see all the traffic on a network—they only see the traffic the switch sends to them, which includes broadcast traffic and traffic specifically addressed to the one computer (see the computer in the red box on the right in [Figure 12-5](javascript://)). To track more of the network traffic, you can use one of these other methods, which are also illustrated in [Figure 12-5](javascript://):

**Figure 12-5**

Methods to monitor network traffic

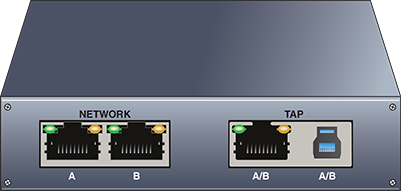


Enlarge Image

* **Wireless monitoring**—Run monitoring software on a computer connected wirelessly to the network (see the computer on the left in [Figure 12-5](javascript://)). For the computer to “see” all traffic, its network adapter must support promiscuous mode. In promiscuous mode, a device driver directs the NIC to pass all wireless frames to the operating system and on to the monitoring software, not just those broadcasted or intended for the host. Usually, promiscuous mode is enabled in the monitoring application. Occasionally you’ll need to enable the feature through the OS. (For Windows, use the NIC’s properties box from Device Manager.)
* **Port mirroring**—Configure a switch to use port mirroring, which ensures that all traffic sent to any port on the switch is also sent to a device connected to the mirrored port, such as the computer in the bottom right of [Figure 12-5](javascript://). Recall you learned about port mirroring (also called SPAN) when you studied NIDS. In a project at the end of this module, you’ll configure SPAN on a switch in Packet Tracer. Then you’ll monitor traffic through a device connected to the monitored port.
* **In-line monitoring**—Install a device, called a network TAP (test access point) or packet sniffer, in line with network traffic, as shown in the center of [Figure 12-5](javascript://). As you can see in [Figure 12-6](javascript://), a TAP usually has a variety of ports:
  + Two ports send and receive all traffic, usually between a switch and a router.
  + One or two other ports (Ethernet or USB) mirror the traffic, sending it to a computer running monitoring software in promiscuous mode, such as Wireshark.
  + A port on the back is used for device configuration.

**Figure 12-6**

Network TAPs are available for both copper and fiber network troubleshooting



* **Reporting**—Many devices can be configured to report their traffic and other statistics to a network monitor, such as the computer in the top right corner of [Figure 12-5](javascript://). These techniques rely on protocols such as syslog and SNMP, which you’ll read about shortly.

Some NOSs come with built-in network monitoring tools. In addition, you can purchase or download free network monitoring tools developed by other software companies. Hundreds of such programs exist. After you have worked with one network monitoring tool, such as Spiceworks, you’ll find that other products work in much the same way. Most even use very similar graphical interfaces. All network monitoring tools can perform at least the following functions:

* Set the NIC to run in promiscuous mode so it will pass all traffic it receives to the monitoring software.
* Continuously monitor network traffic on a segment.
* Capture network data transmitted on a segment.
* Capture frames sent to or from a specific node.
* Reproduce network conditions by transmitting a selected amount and type of data.
* Generate statistics about network activity (for example, what percentage of the total frames transmitted on a segment are broadcast frames).

Some network monitoring tools can also perform the following functions:

* Discover all network nodes on a segment.
* Establish a baseline, including performance, utilization rate, and so on.
* Track utilization of network resources (such as bandwidth and storage) and device resources (such as CPU or memory usage), and present this information in the form of graphs, tables, or charts.
* Store traffic data and generate reports.
* Trigger alarms when traffic conditions meet specific thresholds (for example, if usage exceeds 60 percent of capacity).
* Identify usage anomalies, such as top talkers (hosts that send an inordinate amount of data) or top listeners (hosts that receive an inordinate amount of data).

How can capturing data help you solve networking problems? Imagine that traffic on a segment of the network you administer suddenly grinds to a halt one morning at about 8:00 a.m. You no sooner step in the door than everyone from the help desk calls to tell you how slowly the network is running. Nothing has changed on the network since last night when it ran normally, so you can think of no obvious reasons for problems.

At the workstation where you have previously installed a network monitoring tool, you capture all data transmissions for approximately five minutes. You then sort the frames in the network monitoring software, arranging the nodes in order based on the volume of traffic each has generated. You might find that one workstation appears at the top of the list with an excessively high number of bad transmissions. Or you might discover that a server has been compromised by a hacker and is generating a flood of data over the network. Or possibly your current sampling size doesn’t yet reveal any problems, and you run a second, longer capture. Once you know the source of the problem, you know where to look for a resolution, as you read about in the On the Job story at the beginning of this module.

At the same time, finding the source of the problem requires using the correct tool. A network monitor’s data will allow for [**traffic analysis**](javascript://), which examines the flow of network traffic for patterns and exceptions to those patterns. For example, traffic analysis will identify locations of network bottlenecks, such as an outdated device that should be replaced or a network service that needs more resources. A protocol analyzer, however, will dig into the details of specific packets and perform [**packet analysis**](javascript://) functions, which identify protocols, errors, and misconfigurations. Both approaches can yield insightful information; however, focusing on the most relevant approach will help you locate the source of the problem more quickly.

A network monitor or protocol analyzer can use traffic analysis and packet analysis techniques to identify specific types of data errors and other transmission problems, such as the following:

* **Runts**—Packets that are smaller than the medium’s minimum packet size. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.
* **Giants**—Packets that exceed the medium’s maximum packet size. For example, an Ethernet packet larger than 1518 bytes (or 1522 bytes for VLAN packets) is normally considered a giant.
* **Jabber**—A device that handles electrical signals improperly, usually affecting the rest of the network. A network monitor will detect a jabber as a device that is always retransmitting, effectively bringing the network to a halt. A jabber usually results from a bad NIC. Occasionally, it can be caused by outside electrical interference.
* **Ghosts**—Frames that are not actually data frames, but aberrations caused by a device misinterpreting stray voltage on the wire. Unlike true data frames, ghosts have an invalid pattern at the beginning of the frame pattern.
* **Packet loss**—Packets lost due to an unknown protocol, unrecognized port, network noise, or some other anomaly. Lost packets never arrive at their destination.
* **Discarded packets**—Packets that arrive at their destination beyond their usable time frame and are then discarded, or dropped, by the receiving device. Issues that might cause this include buffer overflow, latency, bottlenecks, or other forms of network congestion. A discarded packet is often referred to as a discard.
* **Interface resets**—Repeated resets of the connection, resulting in lower-quality utilization; typically caused by an interface misconfiguration.

**Applying Concepts 12-2**

### Identify a Process Hogging Network Resources

Suppose you notice a sudden decrease in network performance and suspect malware is hogging network resources. Follow these steps to identify a legitimate process or malware on a Windows machine that is affecting network performance:

1. 1

Every process is assigned a PID (process identifier). To display the PID associated with each network connection, open an elevated PowerShell or Command Prompt window and enter the command **netstat –o**.

1. 2

You can identify the names of the processes for each PID by looking in Task Manager (press **Ctrl + Alt + Del** and then click **Task Manager**). Click **More details**. On the Processes tab, if the PID column is not showing, right-click a column heading and check **PID**.

1. 3

Alternatively, you can have the netstat utility resolve process names. Enter the command **netstat -b**, which will take longer to run. If you don’t recognize a process name, do a quick Google search to learn about it.

1. 4

You might need to forcefully stop an out-of-control process. In most cases, you could do this with the Windows Services console (services.msc). To stop a process that refuses to stop by normal means, you can instead use the **taskkill** command with the **/f** parameter and the process’s PID. For example, if the PID is 2212, enter the command:

**taskkill /f /pid:2212**

If that doesn’t work, you might first need to take ownership of the process program file. To do this, enter the command **takeown /f <filename>** using the filename listed for the process when you ran the **netstat -b** command.

Faults and conditions that exceed certain thresholds can trigger [**alerts**](javascript://), which are messages that indicate some threshold has been met, and those alerts might generate notifications to IT personnel. Depending on the software used, these notifications might be transmitted either by email or text message, also called SMS, or they can automatically prompt support ticket generation. Alerts can also be recorded by system and event logs. Many devices, such as routers, switches, servers, and workstations, include embedded event logging tools of various types and will store logs within their own systems. Other tools collect log entries from devices across the network. Let’s look at both possibilities.

### Event Viewer in Windows

Virtually every condition recognized by an operating system can be recorded. Records of such activities are kept in a [**log**](javascript://). For example, each time your computer requests an IP address from the DHCP server and doesn’t receive a response, this event is logged. Likewise, a log entry can be added each time a firewall denies a host’s attempt to connect to another host on the network that the firewall defends.

Different operating systems log different kinds of events by default, which is called an event log. In addition, network administrators can customize logs by defining conditions under which new entries are created. For example, an engineer might want to know when the relative humidity in a data center exceeds 60 percent. If a device can monitor this information and communicate it in real time to a computer, the results can be written to a log. On Windows-based computers, the event log can be easily viewed with the [**Event Viewer**](javascript://) application, as you will see in the following activity.

**Applying Concepts 12-3**

### Explore Event Viewer in Windows

In this activity, you will use the Event Viewer application to explore the event log on a computer running Windows 10. Ideally, the computer will have been used for a while, so the event log contains several entries. It need not be connected to a network. However, you must be logged on to the computer as a user with administrator privileges. Complete the following steps:

1. 1

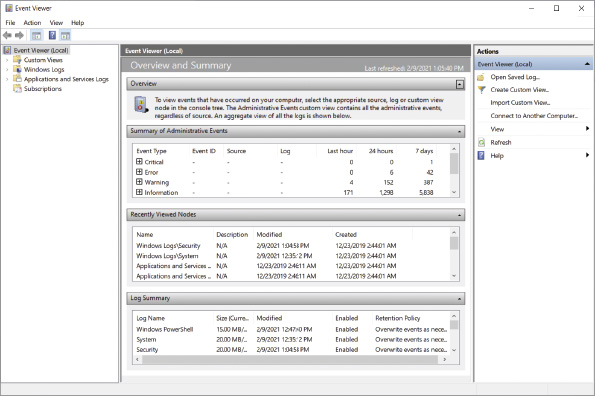
Right-click **Start** and click **Event Viewer**.

1. 2

The Event Viewer window opens, with three panes as shown in [Figure 12-7](javascript://). The center pane lists a summary of administrative events. Event Viewer’s default screen lists entries for all types of logs kept by the Windows operating system. Notice that events are classified into several types, which might include Critical, Error, Warning, Information, Audit Success and, in some cases, Audit Failure. The number of events that have been logged in each category is listed to the right of the classification entry. How many Critical and Error events has your workstation logged in the last 24 hours? In the last seven days?

**Figure 12-7**

Event Viewer logs errors and other activities in Windows



Enlarge Image

1. 3

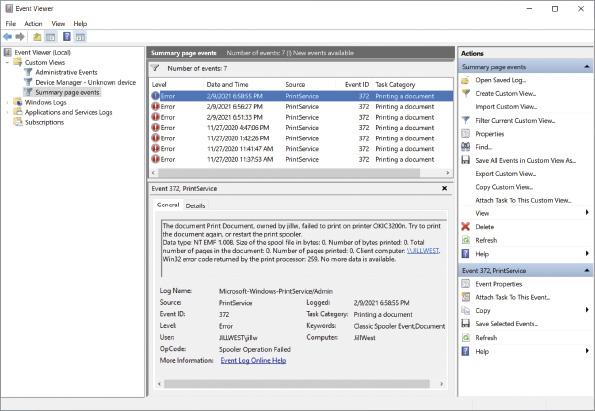
If your workstation has logged any critical or error events in the past seven days, click the plus sign next to the event type. A list of events appears. (If you do not have any entries in the Critical or Error categories, click the plus sign next to the event type Warning instead.)

1. 4

Notice that each event log entry is identified by an Event ID, its source, and the type of log on which it’s recorded. Scroll through the entries to find one that looks interesting—if possible, one that has occurred more than once in the past seven days. Double-click that entry to read more about it. The Summary page events pane appears in the center of the Event Viewer display (see [Figure 12-8](javascript://)).

**Figure 12-8**

This event shows a problem with a network printer



Enlarge Image

1. 5

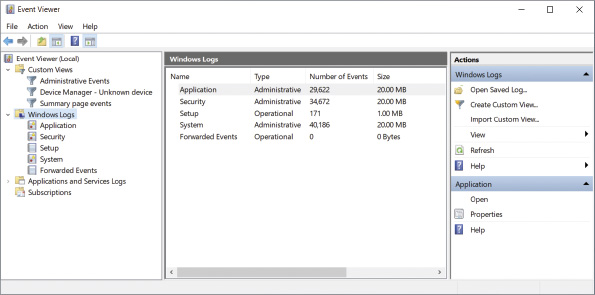
Notice when these errors were recorded. On the General tab in the lower portion of the middle pane, read a detailed description of the error you chose to view. If you were a network manager, would you choose to be alerted whenever this error occurred on a workstation or server? Why or why not?

1. 6

Now click **Windows Logs** in the left pane of Event Viewer to see the different types of logs about Windows events. The Windows Logs listing appears in the center pane, as shown in [Figure 12-9](javascript://).

**Figure 12-9**

Windows Logs listing in Event Viewer



Enlarge Image

1. 7

Which of the five logs has recorded the highest number of events? How large is that log file?

1. 8

Suppose you want to limit the size of the system log. Right-click the **System** log and click **Properties**.

1. 9

The Log Properties - System (Type: Administrative) dialog box opens. Next to the Maximum log size (KB) text box, enter **16000** to limit the log file size to 16 MB.

1. 10

Click **OK** to save your change. If you receive a message that indicates your current log’s size exceeds the maximum limit you just entered, click **OK** to accept the recommended practice of enforcing the maximum after the log is cleared.

In a project at the end of this module, you’ll learn how to work with the data collected in Windows event logs.

### Syslog Messages

Event logs and additional information are routinely recorded by many other types of devices. These logs can be centrally collected via the syslog utility. Syslog is a standard for generating, storing, and processing messages about events on many networked systems. It describes methods for detecting and reporting events and specifies the format and contents of messages. The syslog standard addresses three primary components, as described next and illustrated in [Figure 12-10](javascript://):

**Figure 12-10**

Three components of the syslog standard



* **Event message format**—Event messages must be organized and formatted in a specific manner with certain types of information included, although flexibility to this format is built in to allow syslog’s use in a wide variety of environments and scenarios.
* **Event message transmission**—Event messages are transported across the network on port 514. Syslog messages secured by TLS are transported instead over port 6514.
* **Event message handling**—The syslog utility on all monitored devices and on the syslog server follow protocols for creating, handling, analyzing, and storing event messages.

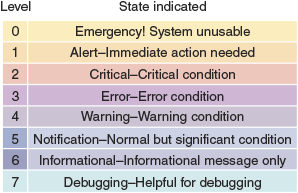
The syslog standard also defines two roles for devices participating in logging events:

* **Generator**—The device that is monitored by a syslog-compatible application and that issues event information
* **Collector**—The server that gathers event messages from generators

You likely don’t want to collect every possible event message, as that would generate massive amounts of data to be stored and analyzed. Unless this is necessary for compliance purposes, you’ll probably want to limit the types of messages generated, transmitted, and stored. For this purpose, syslog assigns a [**severity level**](javascript://), also called a [**logging level**](javascript://) or priority value, to each event. For example, “0” indicates an emergency situation, whereas “7” points to specific information that might help in debugging a problem, as shown in [Figure 12-11](javascript://). You configure a filter on the device so that it sends all events from a specific level and above to the syslog server. Further, you can filter syslog messages by the facility, or machine process, which created the event, such as the kernel (facility “0”), users (facility “1”), or security and authorization (facility “4”).

**Figure 12-11**

Syslog severity levels



The filters and other syslog configurations you implement on each device must be carefully considered in situations where you need to conform to regulatory compliance requirements. In some cases, you must be able to track every movement of every user. By referring to information stored in your logs, you should be able to answer the question, “Who did what activity when and in what way?” When tracking this level of information, the collective data is called an [**audit log**](javascript://), or audit trail. The data in these logs is consistent and thorough enough to retroactively prove compliance and also to defensibly prove user actions (that is, your network logs document user action in a way that is presentable in a court of law). This data is often used in forensics investigations to determine how a particular problem occurred, especially if criminal investigations are involved. Make sure you know exactly what types of actions and other events you must log on your network to meet relevant compliance standards.

**Note 12-1**

Computers running Linux and UNIX record syslog data in a [**system log**](javascript://), found in the /var/log directory. Configure the types of events to log and what priority to assign each event in the /etc/syslog.conf file (on some systems, this is the /etc/rsyslog.conf file).

Bear in mind that the syslog utility doesn’t alert you to any problems, but it does keep a history of messages issued by the system. It’s up to you to monitor the system log for issues, review the logs regularly for missed problems, or filter log data to monitor packet flow when troubleshooting a problem or checking for patterns that might indicate developing problems. Most UNIX and Linux desktop operating systems provide a GUI application for easily reviewing and filtering the information in system logs. Other applications are available for sifting through syslog data and generating alerts. In a project at the end of this module, you’ll view and sort through data in a system log.

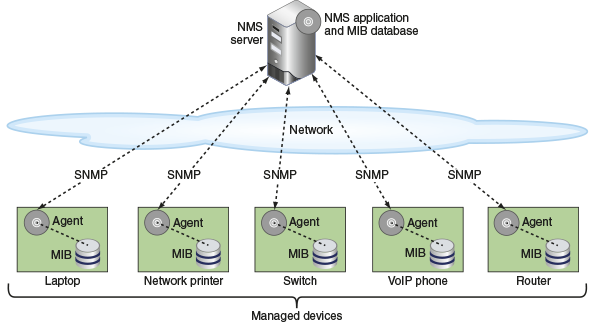
Using the information collected in event logs and system logs for security and fault management requires thoughtful data filtering and sorting. After all, you can’t assume that all of the information in these logs points to a problem, even if it is marked with a warning. For example, you might have typed your password incorrectly while trying to log on to your computer, thus generating a log entry. Keep in mind, however, that sometimes seemingly innocuous information turns out to be exactly the data you need to diagnose a problem.

### SNMP Communications

You’ve just learned about logs that are created on individual devices and then collected at a central location on a syslog server. In contrast, organizations often use enterprise-wide network management systems to perform real-time monitoring functions across an entire network. Hundreds of such tools exist. All rely on a similar architecture (see [Figure 12-12](javascript://)), in which the following entities work together:

**Figure 12-12**

Network management architecture



Enlarge Image

* **[NMS (network management system) server](javascript://)**—At least one network management console, which may be a server or workstation, depending on the size of the network, collects data from multiple managed devices at regular intervals in a process called polling.
* **Managed device**—Any network node monitored by the NMS is a managed device. Each managed device may contain several managed objects. This can be any characteristic of the device that is monitored, including components such as a processor, memory, hard disk, or NIC, or intangibles such as performance or utilization. Each managed object is assigned an [**OID (object identifier)**](javascript://), which is standardized across all NMSs.
* **Network management agent**—Each managed device runs a network management agent, which is a software routine that collects information about the device’s operation and provides it to the NMS. For example, on a server, an agent can measure how many users are connected to the server or what percentage of the processor’s resources are used at any given time. So as not to affect the performance of a device while collecting information, agents demand minimal processing resources.
* [**MIB (Management Information Base)**](javascript://)—The list of objects managed by the NMS, as well as the descriptions of these objects, are kept in the MIB (Management Information Base). The MIB also contains data about an object’s performance in a database format that can be mined and analyzed. The MIB is designed in a top-down, hierarchical tree structure that supports faster and more efficient analysis.

Agents communicate information about managed devices via any one of several application layer protocols. On modern networks, most agents use SNMP (Simple Network Management Protocol). Recall that SNMP is part of the TCP/IP suite of protocols and typically runs over UDP ports 161 and 162 (though it can be configured to run over TCP ports 10161 and 10162). Port 161 is used to send information from the manager to the installed agents, while port 162 is used for agents to send messages to the manager. One characteristic that sets SNMP apart from syslog is that SNMP can be used to reconfigure managed devices. Additionally, SNMP is used more for real-time network monitoring rather than retroactive analysis.

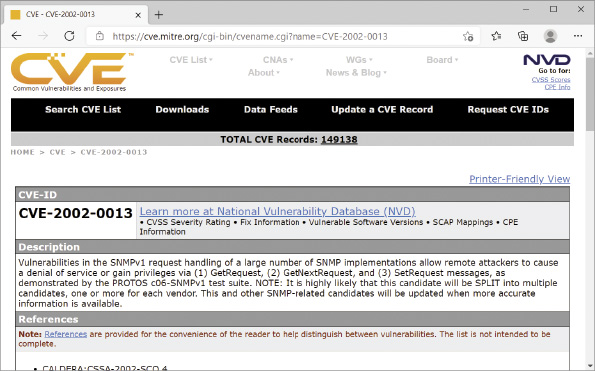
Three versions of SNMP include the following:

* **SNMPv1 (Simple Network Management Protocol version 1)**—This is the original version, released in 1988. Because of its limited features, it is rarely used on modern networks.
* **SNMPv2 (Simple Network Management Protocol version 2)**—This version improved on SNMPv1 with increased performance and slightly better security, among other features.
* **SNMPv3 (Simple Network Management Protocol version 3)**—This version is similar to SNMPv2 and adds authentication, validation, and encryption for messages exchanged between managed devices and the network management console.

Most, but not all, network management applications support multiple versions of SNMP. SNMPv3 is the most secure version of the protocol. However, some administrators have hesitated to upgrade to SNMPv3 because it requires more complex configuration. Therefore, SNMPv2 is still widely used, despite the many SNMP vulnerabilities listed in the CVE (Common Vulnerabilities and Exposures), one of which is displayed in [Figure 12-13](javascript://). When using older versions of SNMP, it’s important to incorporate additional security measures, such as the following:

**Figure 12-13**

One of many SNMP vulnerabilities listed in the CVE



Enlarge Image

Source: The MITRE Corporation

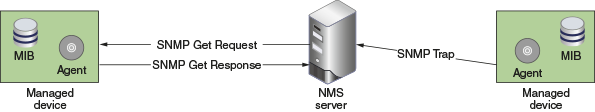
* Disable SNMP on devices where it’s not needed.
* Limit approved sources of SNMP messages.
* Require read-only mode so devices can’t be reconfigured using SNMP messages.
* Configure strong passwords, called community strings, on SNMP managed devices.
* Use different community strings on different types of devices so, for example, a compromised UPS (which incorporates less secure protections) doesn’t result in a compromised router using the same community string.

There are a few, key SNMP messages used to communicate between the NMS and managed devices. As you can see in the following list, most of these conversations are initiated by the NMS:

* **Get Request**—The NMS sends a request for data to the agent on a managed device. See the left side of [Figure 12-14](javascript://).
* **Get Response**—The agent sends a response with the requested information.
* **Get Next**—The NMS might then request the next row of data in the MIB database.
* **Walk**—With this one command, the NMS can issue the equivalent of a sequence of SNMP Get Next messages to walk through sequential rows in the MIB database on a monitored device.
* [**Trap**](javascript://)—An agent can be programmed to detect certain abnormal conditions that prompt the generation of Trap messages, where the agent sends the NMS unsolicited data once the specified conditions on the managed device are met (see the right side of [Figure 12-14](javascript://)). For example, on a Cisco server, you could use the command **snmp trap link-status** to instruct the agent to send an alert if or when an interface fails. The trap can later be disabled with the command **no snmp trap link-status**. Trap messages can alert network administrators of unresponsive services or devices, power supply issues, high temperatures, and tripped circuit breakers, which allows technicians to identify and address problems quickly—hopefully before users start to notice the problem. For example, a report of a tripped circuit breaker eliminates the need for further investigation into why a specific device isn’t responsive. Or an unresponsive service, such as DHCP, could be restarted remotely.

**Figure 12-14**

Most SNMP conversations are initiated by the NMS server, except when a managed device sends an SNMP Trap message

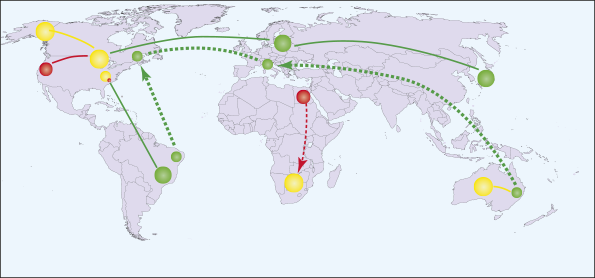


Enlarge Image

After data is collected, the network management application can present an administrator with several options to view and analyze the data. For example, a common way to analyze data is by a line graph. Another popular method is a map that shows fully functional links or devices in green, partially (or less than optimally) functioning links or devices in yellow, and failed links or devices in red. An example of the type of map generated by a network performance monitor is shown in [Figure 12-15](javascript://).

**Figure 12-15**

Map showing network status



Enlarge Image

Because of their flexibility, sophisticated network management applications are also challenging to configure and fine-tune. You must be careful to collect only useful data and not an excessive amount of routine information. For example, on a network with dozens of routers, collecting SNMP-generated messages that essentially say “I’m still here” every five seconds would result in massive amounts of insignificant data. A glut of information makes it difficult to ascertain when a router in fact requires attention. Instead, when configuring a network management application to poll a router, you might choose to generate an SNMP-based message only when the router’s processor is operating at 75 percent of its capacity or to measure only the amount of traffic passing through a NIC every five minutes.

### NetFlow

SNMP provides real-time monitoring of network activities and device states with an emphasis on device health, performance, and configuration. But what if you want to get a comprehensive view of network traffic across all devices? [**NetFlow**](javascript://) is a proprietary traffic monitoring protocol from Cisco that tracks all IP traffic crossing any interface where NetFlow is enabled. From that information, NetFlow creates flow records that show relationships among various traffic types. While SNMP focuses on individual devices, NetFlow focuses on the way network bandwidth is being utilized by identifying how communications from all devices are related to each other.

When NetFlow is enabled on a network device, each unique conversation is collected in a NetFlow cache as a flow record. Additional messages in the same conversation are aggregated into that one flow record. When complete, the flow record is then sent, or exported, to a centralized NetFlow collector for analysis. A [**NetFlow analyzer**](javascript://), or NetFlow collector, collates flow records from throughout the network to provide insights into traffic patterns, such as why congestion is happening, what changes are occurring, and how those changes are affecting other traffic. A NetFlow analyzer can be hardware-based or software-based, which is more common.

A significant challenge with NetFlow is determining the optimal balance between tracking all traffic and tracking enough traffic to sufficiently observe network behavior. While NetFlow can provide in-depth access to traffic information, all the data must be transferred from the NetFlow exporter (the router, switch, or other device monitoring its traffic) to the NetFlow analyzer. NetFlow is capable of tracking nearly 100% of messages crossing an interface. However, transferring this volume of flow records to the analyzer will, on its own, negatively impact network performance. The trick is to sample enough traffic to get an accurate picture and catch problems early while not transferring any more flow records than necessary across the network for analysis. Still, NetFlow requires shallower examination of messages on the network and, therefore, fewer resources than other options that capture entire packets. This allows NetFlow to analyze very high volumes of traffic that would overwhelm more traditional approaches.

**Note 12-2**

A similar technology, sFlow, is compatible with many platforms and relies on a dedicated hardware chip to avoid placing additional demand on a network device’s CPU and memory. While NetFlow is limited to capturing IP traffic, sFlow can sample traffic from all layers 2 through 7.

**Remember This…**

* Implement appropriate environmental monitoring.
* Use port mirroring to capture network traffic.
* Compare SNMP and syslog.
* Explain how SNMP works and how to secure it.
* Compare various types of logs.

**Self-Check**

1. Which of the following would an environmental monitoring system not track?

Answer

* 1. Liquid detection
  2. User authentication
  3. Data room lights
  4. UPS voltage

1. Which log type would most likely be used first to investigate the cause of high numbers of dropped packets?

Answer

* 1. Traffic log
  2. System log
  3. Jitter log
  4. Audit log

1. Which of the following is not defined by syslog?

Answer

* 1. Message transmission
  2. Message format
  3. Message handling
  4. Message security

1. Which of the following would be assigned an OID?

Answer

* 1. An NMS server
  2. A switch’s interface
  3. A web server
  4. A UDP port

**You’re Ready**

You’re now ready to complete [Project 12-1: Work with Data in Event Viewer](javascript://), or you can wait until you’ve finished reading this module.

**You’re Ready**

You’re now ready to complete [Project 12-2: Configure SPAN and Syslog in Packet Tracer](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 12-2Manage Network Traffic

### Certification

* 2.2

Compare and contrast routing technologies and bandwidth management concepts.

* 2.3

Given a scenario, configure and deploy common Ethernet switching features.

* 3.1

Given a scenario, use the appropriate statistics and sensors to ensure network availability.

* 5.3

Given a scenario, use the appropriate network software tools and commands.

* 5.5

Given a scenario, troubleshoot general networking issues.

Average reading time: 26 minutes

After you’ve begun collecting data on your network’s traffic patterns, you’re ready to monitor your network’s status on an ongoing basis and make changes to best meet the needs of your network’s users. This process includes two major factors:

* **Performance management**—Monitoring how well links and devices are keeping up with the demands placed on them
* **Fault management**—Detecting and signaling of device, link, or component faults

To accomplish both fault and performance management, network administrators respond to errors as needed and tweak device and network configurations to optimize performance. To do this effectively, however, you first need to know your starting point, as you’ll see next.

Go to pg.

[**help**](javascript://)

Application Opened

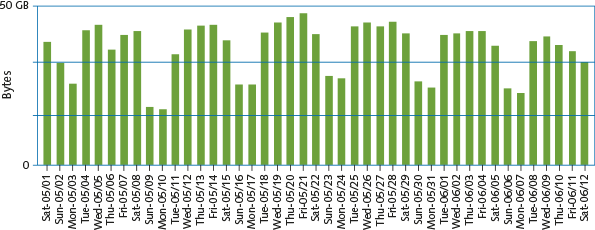
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-2aPerformance Baselines

When it comes to monitoring network performance, data creation is the easy part. The challenge is to identify and efficiently analyze useful and relevant data. To know when there’s a problem on the network, you must first know what is normal for that network. A [**baseline**](javascript://) is a report of the network’s normal state of operation and might include a range of acceptable measurements. Network performance baselines are obtained by analyzing network traffic information and might include information on the utilization rate for your network backbone, number of users logged on per day or per hour, number of protocols that run on your network, statistics about errors (such as runts, jabbers, or giants), frequency with which networked applications are used, or information regarding which users take up the most bandwidth. The graph in [Figure 12-16](javascript://) shows a sample baseline for daily network traffic over a six-week period.

**Figure 12-16**

Baseline of daily network traffic



Enlarge Image

Baseline measurements serve as a basis of comparison for future performance increases or decreases caused by network changes or events with past network performance. As you saw in the On the Job story at the beginning of this module, a network baseline can provide valuable insights when trying to diagnose a problem or pinpoint an intrusion, over usage, or misconfiguration. Obtaining baseline measurements is the only way to know for certain whether a pattern of usage has changed (and requires attention) or whether a network upgrade made a difference. Each network requires its own approach and a reliable schedule for documenting and reviewing baselines to identify unexpected variations. The elements you measure and monitor depend on which functions are most critical to your network and its users.

For instance, suppose that your network currently serves 500 users, and your backbone traffic exceeds 50 percent capacity at 10:00 a.m. and 2:00 p.m. each business day. That pattern constitutes your baseline. Now suppose that your company decides to add 200 users who perform the same types of functions on the network. This is a 40 percent in users. Therefore, you can estimate that your backbone’s capacity should increase by approximately 40 percent to maintain your current service levels.

The more data you gather while establishing your network’s baseline, the more accurate your prediction will be. Network traffic patterns can vary considerably over time and must account for two major factors:

* Normal variations throughout the day, week, month, and different seasons. For example, a large retail company will have significantly busier traffic patterns during holiday seasons, and this is completely normal for that network.
* Changes to the network that might be unpredictable in the resulting impact. For instance, the preceding example assumed that all new users would share the same network usage habits as the current users. In fact, however, the new users might generate a lot more (or a lot less) network traffic.

How do you gather baseline data on your network? Several software applications can perform the baselining for you. These applications range from freeware available on the Internet to expensive, customizable hardware and software combination products. Before choosing a network-baselining tool, determine how you will use it. If you manage a small network that provides only one critical application, an inexpensive tool may suffice. For example, you could use the simple CLI-based tool **[iPerf](javascript://)** to establish throughput between network hosts, or you could use one of the throughput testing tools you’ve used in some of your projects in this course, such as TotuSoft’s LAN Speed Test or TamoSoft’s Throughput Test app. In a project at the end of this module, you’ll see how iPerf can test throughput between nearly any two devices on your network. Exploring and documenting this data helps establish a baseline you could reference if (or when) you experience traffic problems in the future.

If you work on a WAN with several critical links, however, investigate purchasing a more comprehensive package. The baseline measurement tool should be capable of collecting the statistics needed. For example, only a sophisticated tool can measure traffic generated by each node on a network, filter traffic according to types of protocols and errors, and simultaneously measure statistics from several network segments.

Once you’ve gathered this data, analyze the data for typical rates of utilization and failure. Some of the more common network performance KPIs (key performance indicators) include the following:

* **Device availability and performance**—This includes such metrics as CPU and memory usage, temperature, and network connection speed.
* **Interface statistics**—Feedback collated from all network interfaces can provide insights into what’s changing on the network and what might be going wrong. For example, a device that regularly shows a low uptime might be repeatedly power cycling.
* **Utilization**—This metric refers to the actual throughput used as a percentage of available bandwidth. No network should be required to operate at maximum capacity. Identify patterns of utilization and ensure that available bandwidth accounts for utilization spikes.
* **Error rate**—Bits can be damaged in transit due to EMI or other interference. The calculated percentage of how often this occurs is the error rate.
* **Packet drops**—Packets that are damaged beyond use, arrive after their expiration, or are not allowed through an interface are dropped. Packet drops result in delayed network communications while devices wait for responses or resend transmissions. Knowing what’s normal for your network will help you identify problems when packet drop rates vary.
* **Jitter**—All packets experience some latency. When successive packets experience varying amounts of latency, resulting in their arriving out of order, the user experience is degraded. This is called jitter, a problem that can be addressed through traffic management techniques, which you’ll read about next.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-2bBandwidth Management

As you know, a network’s bandwidth is its potential to handle network traffic. This is not just a single number, but a conglomeration of numbers from every link and interface on the network. As you’ve learned throughout this course, different devices can handle different volumes of traffic, and your overall bandwidth management techniques must take this reality into account. As a subset of performance management, [**bandwidth management**](javascript://) refers to a collection of strategies to optimize the volume of traffic a network can support. These techniques might include any of the following technologies:

* [**Flow control**](javascript://)—Configure interfaces and protocols to balance permitted traffic volume with a device’s capability of handling that traffic.
* [**Congestion control**](javascript://)—Adjust the way network devices respond to indications of network performance issues caused by traffic congestion so they don’t make the problem worse.
* **QoS (quality of service)**—Prioritize some traffic over other traffic so the most important traffic gets through even during times of congestion.

Let’s explore each of these technologies in more detail.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

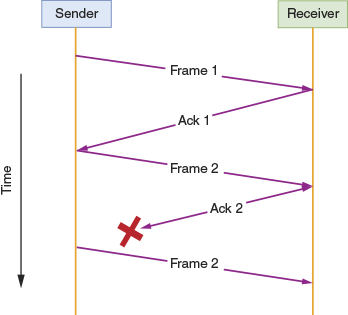
## 12-2cFlow Control

Flow control is a bandwidth management technique configured on a local connection between two devices. The purpose is to ensure the receiver is not overwhelmed with the rate of data transmission. Flow control can be managed either at the data link layer or at the network and transport layers. When managed at the higher layers, rate-based flow control limits the amount of data that can be transmitted but does not provide feedback to the sender when that rate is exceeded. Instead, traffic is lost. In contrast, feedback-based flow control at the data link layer gives the sender some kind of indication when the transmission rate is exceeding the receiver’s ability to handle the incoming traffic. Common approaches are the stop-and-wait method and two versions of the sliding window method. Consider the following scenarios:

* **Stop-and-wait method**—A sender transmits a frame and then waits for an acknowledgment before transmitting the next frame. See [Figure 12-17](javascript://). If an acknowledgment is not received, the sender retransmits the unacknowledged frame. This way, whether the frame is lost in transit or the acknowledgment is lost, the frame is still resent. At no time is the receiver required to handle more than one incoming frame, and each frame must be acknowledged before sending another frame. This approach is simple and provides high accuracy. However, it’s also very slow because only one frame can be sent at a time.

**Figure 12-17**

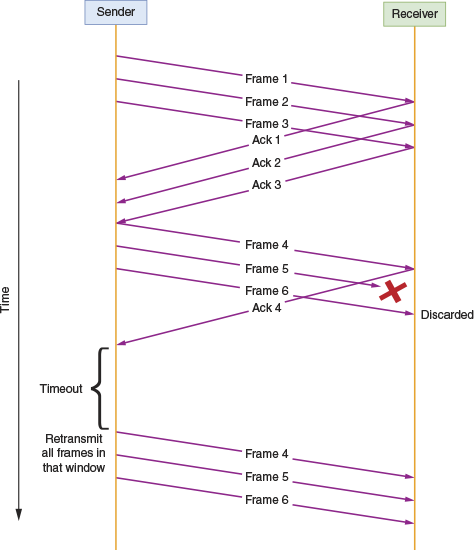
Stop-and-wait method



* **Go-back-n sliding window method**—A sender can transmit multiple frames at one time while considering the maximum number of frames the receiver can handle at any time. For example, suppose a receiver can handle up to three incoming frames at any given time, as shown in [Figure 12-18](javascript://). The sender transmits three frames and waits for three acknowledgments. If all three acknowledgments are received, the sender transmits another three frames. If an acknowledgment is missing, the sender retransmits all three frames, even if only one frame was lost.

**Figure 12-18**

Go-back-n sliding window method

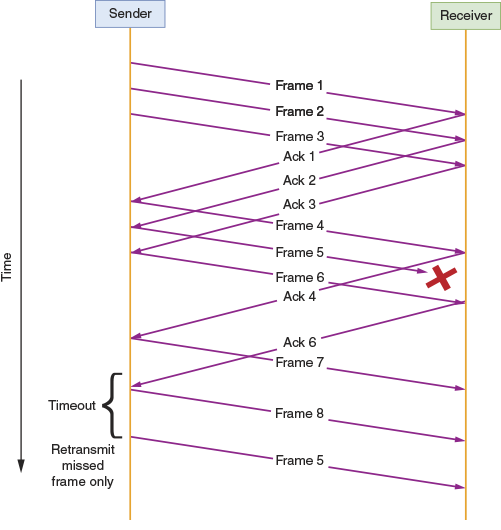


Enlarge Image

* **Selective repeat sliding window method**—In this scenario, as shown in [Figure 12-19](javascript://), only the unacknowledged frame is retransmitted. The sender continues sending additional frames as long as space is available in the window for new frames. This is a more efficient approach because later frames don’t have to wait on as many earlier frames to be acknowledged. However, it’s also more complex because the receiver must be able to receive frames out of order and reorganize them, even if a much earlier frame experiences a relatively lengthy delay.

**Figure 12-19**

Selective repeat sliding window method



Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-2dCongestion Control

Notice that flow control manages the number of frames transmitted end-to-end between a single sender and a single receiver. Congestion control, however, manages the volume of traffic throughout the network. Think about the perspective of a switch or router when evaluating network traffic performance: Are too many devices trying to send messages at the same time? Is one host sending so much data that it’s hogging network resources? These kinds of problems can overwhelm the network as a whole. When the network starts experiencing congestion, messages are corrupted or dropped, and connected devices start resending frames to make up for the loss. This response, then, generates even more traffic, making the congestion even worse.

Congestion control techniques are designed to prevent this congestion before it occurs (called open-loop congestion control) and also to remedy congestion after it starts (called closed-loop congestion control). Open-loop techniques include the following policies:

* **Retransmission policy**—Retransmission timers help reduce increasing congestion caused by devices attempting to resend lost packets too quickly or too often.
* **Window policy**—Senders might be required to use the selective repeat sliding window method to reduce the number of frames that must be resent when errors occur.
* **Acknowledgment policy**—Receivers can be required to send a single ACK message for multiple received frames, thereby reducing acknowledgment traffic on the network.
* **Discarding policy**—Less sensitive frames are discarded so important traffic can survive the congestion.
* **Admission policy**—Routers and switches can temporarily reject new traffic that will contribute to or create congestion rather than admitting that new traffic onto the network.

The closed-loop response to existing congestion includes the following techniques:

* **Implicit signaling**—A sending device detects congestion on the network after experiencing several missed acknowledgment messages.
* **Explicit signaling**—A congested networking device alters existing data packets to indicate to either the sender (this is called backward signaling) or the receiver (this is called forward signaling) that the network is congested.
* **Choke packet**—A router experiencing congestion creates and sends a choke packet to the traffic source, informing it of the congestion so the sender can reduce its rate of transmission.
* **Backpressure**—A node downstream from sender to receiver stops accepting traffic, which transfers the pressure of the congestion upstream toward the source. This technique is limited to specific types of congestion scenarios.

While congestion control manages the entrance of traffic onto the network, other methods allow for more nuanced control of what happens to the traffic once it’s on the network. That’s where QoS comes in, as you’ll read about next.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-2eQoS (Quality of Service) Assurance

You don’t want to hear breaks in an online phone conversation or see a buffering message when you watch a movie over the Internet. For that reason, voice and video transmissions are considered [**delay-sensitive**](javascript://). On the other hand, occasional loss of data (skipping video frames, for example) can be tolerated; for that reason, voice and video transmissions are considered [**loss-tolerant**](javascript://). Typical web surfing might not present much of a challenge for network bandwidth. However, streaming movies, voice or video calls, and online gaming can all place heavy demands on available bandwidth.

To manage these demands, network administrators must efficiently manage a network’s QoS (quality of service) configurations, which is a group of techniques for adjusting the priority a network assigns to various types of transmissions. To do this, network administrators need to be aware of the applications used on a network, including the application protocols they use and the amount of bandwidth they require. For example, variable delays of VoIP packets result in choppy voice quality. A network that handles a lot of VoIP traffic would need to prioritize that traffic to avoid problems with jitter.

From the perspective of a person watching a movie online, optimized QoS translates into an uninterrupted, accurate, and faithful reproduction of audio or visual input. For someone competing in online games, high priority on gaming traffic gives quick and accurate responsiveness to game play in addition to a high-quality audio and visual experience. Network engineers have devised several techniques to address the QoS-related challenges inherent in delivering high-bandwidth network services. The following sections describe some of these techniques.

### Traffic Shaping

When a network must handle high volumes of network traffic, users benefit from a bandwidth management and optimization technique known as traffic shaping. [**Traffic shaping**](javascript://), also called packet shaping, involves manipulating certain characteristics of packets, data streams, or connections to manage the type and amount of traffic traversing a network or interface at any moment. Its goals are to ensure timely delivery of the most important traffic while optimizing performance for all users. Traffic shaping can involve any of the following:

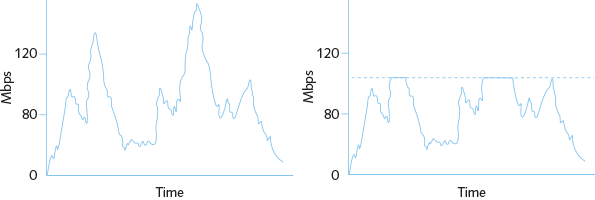
* Delaying less-important traffic, which is called [**buffering**](javascript://)
* Increasing the priority of more-important traffic
* Limiting the volume of traffic flowing into or out of an interface during a specified time period
* Limiting the momentary throughput rate for an interface

The last two techniques belong to a category of traffic shaping known as [**traffic policing**](javascript://) and results in dropped traffic rather than buffered, or delayed, traffic. For example, an ISP might impose a maximum on the capacity it will grant a certain customer. This prevents the customer from tying up more than a certain amount of the WAN’s overall capacity. Traffic policing helps the service provider predict how much capacity it must purchase from its network provider. It also holds down costs because the ISP doesn’t have to plan for every client using all available throughput at all times (an unlikely scenario).

An ISP that imposes traffic policing might allow customers to choose their preferred maximum daily traffic volume or momentary throughput and pay commensurate fees. A more sophisticated instance of traffic policing is dynamic and considers the network’s current traffic patterns. For example, the service provider might allow certain customers to exceed their maximums when few other customers are using the network. [Figure 12-20](javascript://) illustrates how traffic volume might appear on an interface without limits compared with an interface subject to traffic policing.

**Figure 12-20**

Traffic volume before and after applying limits



Enlarge Image

A controversial example of traffic shaping came to light in 2007. Comcast, one of the largest Internet service providers in the United States, was found to be clandestinely discriminating against certain types of traffic. For users uploading files to P2P (peer-to-peer) networks such as BitTorrent, Comcast was interjecting TCP segments with the RST (reset) field set. These segments were spoofed to appear as if they originated from the accepting site, and they cut the connection as the user attempted to upload files. Soon customers figured out the pattern and used monitoring software such as Wireshark to reveal the forged TCP RST segments. They complained to authorities that Comcast had violated their user agreement. The FCC investigated, upheld the customers’ claims, and ordered Comcast to stop this practice. Comcast then chose a different method of traffic shaping. It assigned a lower priority to data from customers who generated a high volume of traffic at times when the network was at risk of congestion.

In the past several years, many ISPs have used traffic throttling to slow down high-bandwidth users. This isn’t necessarily a bad thing, so long as all interested parties are aware of what’s going on. In fact, some ISPs use traffic shaping to temporarily increase a busy user’s bandwidth without negatively affecting other users’ network activities. To learn more about these practices, search on phrases such as “comcast traffic shaping,” “ISP throttling,” “net neutrality,” and “bandwidth throttling test,” which will give you links you can use to test your own Internet connection.

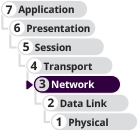
Several types of traffic prioritization exist where more important traffic is treated preferentially. Software running on a router, multilayer switch, gateway, server, or even a client workstation can act as a traffic shaper by prioritizing traffic according to any of the following characteristics:

* Protocol
* IP address
* User group
* DiffServ (Differentiated Services) flag in an IP packet
* VLAN tag in a data link layer frame
* Service or application

Depending on the traffic prioritization software, different types of traffic might be assigned priority classes, such as high, normal, low, or slow; alternatively, it can be rated on a prioritization scale from 0 (lowest priority) to 7 (highest priority). For example, traffic generated by time-sensitive VoIP applications might be assigned high priority, while online gaming might be assigned low priority (or vice versa, depending on your preferences). Traffic prioritization is needed most when the network is busiest. It ensures that during peak usage times, the most important data gets through quickly, while less-important data waits. When network usage is low, however, prioritization might have no noticeable effects.

Some types of network traffic contribute more significantly to the overall volume of traffic than other types do. When a network is expected to simultaneously support voice, video, and data communications, performance is always a major concern. Let’s see what other options are available for addressing these concerns.

### DiffServ (Differentiated Services)

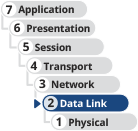


[**DiffServ (Differentiated Services)**](javascript://) is a simple technique that addresses QoS issues by prioritizing traffic at layer 3. DiffServ considers all types of network traffic, not just the time-sensitive services such as voice and video. That way, it can assign voice streams a high priority and at the same time assign unessential data streams (for example, employees surfing the Internet on their lunch hour) a low priority. This technique offers more protection for time-sensitive, prioritized services. To prioritize traffic, DiffServ places information in the DiffServ field of an IPv4 packet. The first 6 bits of this 8-bit field are called [**DSCP (Differentiated Services Code Point)**](javascript://). (For a review of the fields in an IP packet, refer to [Module 4](javascript://).) In IPv6 packets, DiffServ uses a similar field known as the Traffic Class field. This information in both IPv4 and IPv6 packets indicates to network routers how the data stream should be forwarded. DiffServ defines two types of forwarding:

* **EF (Expedited Forwarding)**—A data stream is assigned a minimum departure rate from a given node. This technique circumvents delays that slow normal data from reaching its destination on time and in sequence.
* **AF (Assured Forwarding)**—Different levels of router resources can be assigned to data streams. AF prioritizes data handling but provides no guarantee that on a busy network, messages will arrive on time and in sequence.

This description of DiffServ’s prioritization mechanisms is oversimplified, but helps you understand some of the many nuanced configurations available for managing network traffic. Because of its simplicity and relatively low overhead, DiffServ is well suited to large, heavily trafficked networks.

### CoS (Class of Service)



CoS (Class of Service) is sometimes used synonymously with QoS, but there is an important distinction. The term QoS refers to techniques that are performed at various OSI layers via several protocols. By contrast, the term **[CoS (Class of Service)](javascript://)** is one method of implementing QoS that refers only to techniques performed at layer 2 on Ethernet frames.

CoS is most often used to more efficiently route Ethernet traffic between VLANs. Frames that have been tagged (addressed to a specific VLAN) contain a 3-bit field in the frame header called the PCP (Priority Code Point). CoS works by setting these bits to one of eight levels ranging from 0 to 7, which indicates to the switch the level of priority the message should be given if the port is receiving more traffic than it can forward at any one time. Waiting messages are cached until the port can get to them, or discarded, depending on the class assignment for that frame.

A network’s connectivity devices and clients must support the same set of protocols to achieve their QoS benefits. However, networks can—and often do—combine multiple QoS techniques.

**Remember This…**

* Analyze network and device performance metrics in comparison to performance baselines.
* Compare bandwidth management techniques, including flow control, congestion control, and QoS.
* Explain the various methods of flow control.
* Use iPerf to test throughput between two network devices.

**Self-Check**

1. Which bandwidth management technique limits traffic specifically between a single sender and a single receiver?

Answer

* 1. Congestion control
  2. Traffic shaping
  3. Quality of Service
  4. Flow control

1. Which flow control method resends a lost frame along with all frames sent with it?

Answer

* 1. Selective repeat sliding window
  2. Stop-and-wait
  3. Go-back-n sliding window
  4. Backpressure

1. Which of the following statements is true? Choose two.

Answer

* 1. When streaming a movie, the transmission is sensitive to loss and tolerant of delays.
  2. When sending an email, the transmission is sensitive to delays and tolerant of loss.
  3. When streaming a movie, the transmission is sensitive to delays and tolerant of loss.
  4. When sending an email, the transmission is sensitive to loss and tolerant of delays.

**You’re Ready**

You’re now ready to complete [Project 12-3: Test Network Throughput with iPerf](javascript://), or you can wait until you’ve finished reading this module.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 12-3Plan Response and Recovery Strategies

### Certification

* 3.2

Explain the purpose of organizational documents and policies.

* 3.3

Explain high availability and disaster recovery concepts and summarize which is the best solution.

Average reading time: 50 minutes

Despite every precaution, disasters and security breaches do happen. Training and preparation can make all the difference in your company’s ability to respond and adapt to these situations. This section discusses a spectrum of possible disasters and breaches. As you read about them, think about how you might anticipate your network’s and users’ needs in various scenarios. First, let’s start with some basic terms:

* [**Incident**](javascript://)—Any event, large or small, that has adverse effects on a network’s availability or resources. This could be a security breach, such as a hacker gaining access to a user’s account, an infection, such as a worm or virus, or an environmental issue, such as a fire or flood.
* [**Disaster**](javascript://)—An extreme type of incident, involving a network outage that affects more than a single system or limited group of users.

Each of these possibilities requires advance preparation by a team of people and should have plans and procedures in place to reduce the amount of confusion, chaos, and mistakes in handling the event once it occurs. Let’s first explore the more general incident response policies and then look at disaster recovery techniques.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-3aIncident Response

An [**incident response plan**](javascript://) specifically defines the characteristics of an event that qualifies as a formal incident and the steps that should be followed as a result. Qualifying incidents take into account the full spectrum of possible events, which might include a break-in, fire, weather-related emergency, hacking attack, discovery of illegal content or activity on an employee’s computer, malware outbreak, or a full-scale, environmental disaster that shuts down businesses throughout the city or state. The policy is written with the intent of keeping people safe; protecting sensitive data; ensuring network availability and integrity; and collecting data to determine what went wrong, who is responsible, and what actions should be taken in the future to prevent similar damage. An incident response is a six-stage process, which actually begins before the incident occurs, as described next:

1. Step 1

Preparation: The response team brainstorms possible incidents and plans procedures for handling them. This includes installing backup systems and compiling all the information required to restore the network, such as passwords, configurations, vendor lists and their SLAs, locations of backup data storage, emergency contact information, and relevant privacy laws.

1. Step 2

Detection and identification: Because security and environmental alarm systems can detect incidents of all kinds, staff not directly involved with incident response planning are educated about what qualifies as an incident and what to do if they notice a potential problem. Any system or staff alerts are routed to assigned personnel to determine whether the event requires escalation—that is, if it should be recognized as something other than a normal problem faced by IT technicians. Each company will have its own criteria for which incidents require escalation, as well as its own chain of command for notification purposes. Make sure you’re familiar with your company’s requirements.

1. Step 3

Containment: The team works to limit the damage. Affected systems or areas are isolated, and response staff are called in as required by the situation.

1. Step 4

Remediation: The team finds what caused the problem and begins to resolve it so no further damage occurs.

1. Step 5

Recovery: Operations return to normal as affected systems are repaired and put back in operation.

1. Step 6

Review: The team determines what can be learned from the incident and uses this information to make adjustments in preparation for and perhaps prevention of future threats.

The response plan should identify the members of a response team, all of whom should clearly understand the security policy, risks to the network, and security measures that have already been implemented. The responsibilities assigned to each team member should be clearly spelled out, and the team should regularly rehearse their roles by participating in security threat drills. Suggested team roles include the following:

* **Dispatcher**—The person on call who first notices or is alerted to the problem. The dispatcher notifies the lead technical support specialist and then the manager. The dispatcher also creates a record for the incident, detailing the time it began, its symptoms, and any other pertinent information about the situation. The dispatcher remains available to answer calls from clients or employees or to assist the manager.
* **Technical support specialist**—The team member(s) who focuses on only one thing: solving the problem as quickly as possible. After the situation has been resolved, the technical support specialist describes in detail what happened and helps the manager find ways to avoid such an incident in the future. Depending on the size of the organization and the severity of the incident, this role may be filled by more than one person.
* **Manager**—The team member who coordinates the resources necessary to solve the problem. If in-house technicians cannot handle the incident, the manager finds outside assistance. The manager also ensures that the security policy is followed and that everyone within the organization is aware of the situation. As the response ensues, the manager continues to monitor events and communicate with the public relations specialist.
* **Public relations specialist**—If necessary, this team member learns about the situation and the response and then acts as official spokesperson for the organization to the public or other interested parties.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-3bData Preservation

During some incidents, data will need to be collected in such a way that it can be presented in a court of law for the purpose of prosecuting an instigator of illegal activity. Some of the forensic data available for analysis can be damaged or destroyed if improperly handled. Ideally, one or more first responders would take charge in these cases. [**First responders**](javascript://) are the people with training and/or certifications that prepare them to handle evidence in such a way as to preserve its admissibility in court. However, it’s critical that every IT technician in a company know how to safeguard sensitive information, logged data, and other legal evidence until the first responder or incident response team can take over the collection of evidence, as described next:

1. **Secure the area**—To prevent contamination of evidence, each device involved must be isolated. This means it should be disconnected from the network (remove the Ethernet cable or disable the Wi-Fi antenna) and secured to ensure that no one else has contact with it until the response team arrives. Ideally, you should leave the device running without closing any applications or files. Different OSs require different shutdown procedures to preserve forensic data, so the shutdown process should be left to incident response experts. However, if a destructive program is running that might be destroying evidence, the fastest and safest solution is to unplug the power cord from the back of the machine (not just from the wall). Treat the entire work area as a crime scene. In some cases, such as with a physical break-in, an entire room or possibly multiple rooms must be secured to protect the evidence.
2. **Document the scene**—Creating a defensible audit trail is one of the highest priorities in the forensics process. An [**audit trail**](javascript://) is a system of documentation that makes it possible for a third party to inspect evidence later and understand the flow of events. A defensible audit trail is an audit trail that can be justified and defended in a court of law according to specific standards. Document everything you or your team does, noting the time and the reason for each action. For example, if you unplugged the machine because a virus was wiping the hard drive, document the time and describe the symptoms you observed that led you to unplug the machine. Also make a list of everyone found in the area and their access to the computer in question. Make sure no one else enters the area until the response team arrives and don’t leave the area unattended even for a few moments.
3. **Monitor evidence and data collection**—Record all items collected for evidence. Take care to preserve all evidence in its original state. Do not attempt to access any files on a computer or server being collected for evidence, as this action alters a file’s metadata and could render it inadmissible in court.
4. **Protect the chain of custody**—All collected data must be carefully processed and tracked so it does not leave official hands at any point in the forensics process. Typically, documentation used to track [**chain of custody**](javascript://) describes exactly what the evidence is, when it was collected, who collected it, its condition, and how it was secured. If at any point in the process you have custody of evidence, be sure to sign off on a chain of custody document and obtain a signature from the next person in line when you hand over custody of the evidence.
5. **Monitor transport of data and equipment**—Generally, the incident response team is responsible for transporting all evidence to the forensics lab or other authority. Every item should be carefully documented so the exact same configuration can be replicated in the lab. The response team might even have the capability to do a hot seizure and removal, which means they can use specialized devices to transfer a computer from one power source to another without shutting down the computer. This can be especially critical if it’s possible the computer or its data will become inaccessible after power is turned off—perhaps because a password is unknown or data is currently in memory.
6. **Create a report**—Be prepared to report on all activities that you observed or participated in during the incident response. It’s best to take notes along the way and to write your report in full as soon as possible after the event while it’s still fresh on your mind. All this information will likely be included in the final forensics report, so it’s important to be thorough and accurate.

**Note 12-3**

eDiscovery (electronic discovery) can reveal a great deal of information contained on a computer’s hard drives and storage media. For example, it can reveal calendars, email, and databases. The information revealed by eDiscovery is known as ESI (electronically stored information), or active data. In contrast, computer forensics is a deeper, more thorough investigation than eDiscovery—essentially a computer autopsy designed to discover hidden data. Examples of hidden data include deleted files or file fragments and who has accessed that data and when. This hidden information is called ambient data.

Next, let’s look at some specifics on handling extreme incidents and recovering from these disasters.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-3cDisaster Recovery Planning

When bad things happen, businesses need a plan to ensure [**business continuity**](javascript://), which is the ability of the company to continue doing business with the least amount of interruption possible. At a high level, a [**BCP (business continuity plan)**](javascript://) defines the resources and protocols the business will use to continue providing service to its customers with little or no disruption during a disaster. Considering all possible disasters that could put a company’s ability to continue doing business at risk might seem so theoretical as to be impossible to plan for. But if the worst does happen, a plan is essential. Research shows that half of businesses don’t survive a major disaster (see [Figure 12-21](javascript://)), and many more fail within the first year following a major disaster. By establishing contingency plans ahead of time, a business significantly improves its odds of survival in the face of a natural disaster such as fire, flood, earthquake, hurricane, or tornado, or another catastrophic event such as workplace violence, cyberattack, or industrial sabotage.

**Figure 12-21**

A disaster such as a fire can ruin a business



wk1003mike/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

A BCP takes a big-picture approach to preparations, such as identifying critical operations that require significant backups and ensuring core communications channels are available under a variety of possible circumstances. A BCP also includes ways to prevent disasters from affecting the company at all, ways to limit the damage if or when those disasters occur, and processes for restoring operations and limiting downtime.

One part of a BCP, a focused and thorough [**disaster recovery plan**](javascript://), details the processes for restoring critical functionality and data after an outage that affects more than a single system or a limited group of users. A disaster recovery plan accounts for the worst-case scenarios, from a far-reaching hurricane to a military or terrorist attack. It should provide contingency plans for restoring or replacing computer systems, power, telephone systems, and paper-based files. The part of the plan that addresses computer systems should include the following:

* Contact names and phone numbers for emergency coordinators who will execute the disaster recovery response, as well as roles and responsibilities of other staff.
* Details on which data and servers are being backed up, how frequently backups occur, where onsite and offsite backups are kept, and (most importantly) how backed-up data can be recovered in full.
* Details on network topology, redundancy, and agreements with national service carriers, in case local or regional vendors fall prey to the same disaster.
* Regular strategies for testing the disaster recovery plan.
* A plan for managing the crisis, including frequent communications with employees and customers via regular communication modes and via alternative methods in case phone lines or other standard options are unavailable. For example, a terrorist bomb in Nashville, Tennessee, in late 2020 damaged a major cellular provider, cutting cell service throughout the region for days. A widespread natural disaster, such as several tornadoes or a large hurricane, can also knock out all normal communications channels for days or weeks.

Having a comprehensive disaster recovery plan lessens the risk of losing critical data in case of extreme situations. It also makes potential customers and your insurance providers look more favorably on your organization.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-3dDisaster Recovery Contingencies

You’ve already read about redundancy strategies where, for example, you use multiple servers to run a website or you pay for multiple ISP connections to your network. That way, if one goes down, the other can take over. The same principle applies to your entire data center in disaster recovery planning. An organization can choose from several options for recovering its network infrastructure from a disaster. The options vary by the amount of hardware, software, planning, investment, and employee involvement each requires. These options also vary according to how quickly they will restore network functionality in case a disaster occurs. As you might expect, every contingency plan at this level necessitates a site other than the building where the network’s main components normally reside. An organization can maintain its own disaster recovery sites—for example, by renting office space in a different city—or contract with a company that specializes in disaster recovery services to provide the alternate site. Disaster recovery contingencies are commonly divided into three categories, as shown in [Figure 12-22](javascript://) and described next:

**Figure 12-22**

The most expensive option also provides the fastest recovery



* [**Cold site**](javascript://)—Computers, devices, and connectivity necessary to rebuild a network exist, but they are not appropriately configured, updated, or connected. Therefore, restoring functionality from a cold site could take a long time. For example, suppose your small business network consists of a file and print server, mail server, backup server, Internet gateway, DNS/DHCP server, 25 workstations, four printers, a router, a switch, two access points, and a connection to your local ISP. At your cold site, you might store two server computers on which your company’s NOS is not installed, and that do not possess the appropriate configurations and data necessary to operate in your environment. The 25 client machines stored there might be in a similar state. In addition, you might have a router, a switch, and two access points at the cold site, but these might also require configuration to operate in your environment. Finally, the cold site would not necessarily have Internet connectivity, or at least not the same type your network uses. Supposing you followed good backup practices and stored your backup media at the cold site, you would then need to restore operating systems, applications, and data to your servers and clients; reconfigure your connectivity devices; and arrange with your ISP to have your connectivity restored to the cold site. Even for a small network, this process of rebuilding your network could take weeks.
* [**Warm site**](javascript://)—Computers, devices, and connectivity necessary to rebuild a network exist, with some pieces appropriately configured, updated, or connected. For example, a service provider that specializes in disaster recovery might maintain a duplicate of each of your servers in its data center. You might arrange to have the service provider update those duplicate servers with your backed-up data on the first of each month because updating the servers daily is much more expensive. In that case, if a disaster occurs in the middle of the month, you would still need to update your duplicate servers with your latest weekly or daily backups before they could stand in for the downed servers. Recovery using a warm site can take hours or days, compared with the weeks a cold site might require. Maintaining a warm site costs more than maintaining a cold site, but not as much as maintaining a hot site.
* [**Hot site**](javascript://)—Computers, devices, and connectivity necessary to rebuild a network are all appropriately configured, updated, and connected to match your network’s current state. For example, you might use server mirroring to maintain identical copies of your servers at two WAN locations. In a hot site contingency plan, both locations would also contain identical connectivity devices and configurations, and thus be able to stand in for the other at a moment’s notice. With a hot site, your team could drive from your usual location to your hot site, walk in the door, and immediately get back to work. As you can imagine, hot sites are expensive and potentially time consuming to maintain. For organizations that cannot tolerate downtime, however, hot sites provide the best disaster recovery option.

With increasing reliance on the cloud, companies are finding inexpensive and effective disaster recovery solutions that incorporate cloud technologies. **[DRaaS (disaster recovery as a service)](javascript://)**, also called a [**cloud site**](javascript://), provides a highly scalable, inexpensive DR option by establishing a cloud configuration that could take over many or most business processes in the event of a disaster. To increase the metaphorical temperature of your cloud site, you might have some cloud resources already configured and running. Other resources, however, can be scripted using IaC (infrastructure as code) and created only when needed after a disaster occurs. Be careful, though, to consider your cloud connectivity needs during a disaster. Some types of disasters might prevent you from accessing the cloud at all, at least for a time.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-3ePower Management

Part of managing a network’s availability involves managing the facilities and infrastructure that support the network, such as power connections and power sources during outages or fluctuations. No matter where you live, you have probably experienced a complete loss of power (a blackout) or a temporary dimming of lights (a brownout). Such fluctuations in power are frequently caused by forces of nature, such as hurricanes, tornadoes, or ice storms. They might also occur when a utility company performs maintenance or construction tasks. Power surges, even small ones, can cause serious damage to sensitive computer equipment and can be one of the most frustrating sources of network problems.

Before you learn how to manage power sources to avoid these problems, first arm yourself with an understanding of the nature of an electric circuit and some electrical components that manage electricity.

**Applying Concepts 12-4**

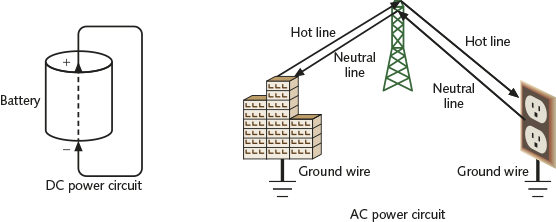
### AC and DC Power and Converters

An electric circuit provides a medium for the transfer of electrical power over a closed loop. If the loop is broken in any way, the circuit won’t conduct electricity. In a circuit, DC (direct current) flows at a steady rate in only one direction. By contrast, AC (alternating current) continually switches direction on the circuit.

A flashlight, for example, uses DC. The batteries in a flashlight have positive and negative poles, and the current always flows at a steady rate in the same direction between those poles, as shown on the left side of [Figure 12-23](javascript://). AC, however, travels in compression waves, similar to the coils of a Slinky®, alternating direction on the power line back and forth between the source and destination. Just as waves can travel across a huge body of water, power moving in an AC wave pattern can travel efficiently for long distances, as illustrated on the right side of [Figure 12-23](javascript://). Because AC power can be conducted at very high voltages, the source of the current can be located far away from the point of use, where it is transformed to lower voltages. Consider the power running a typical laptop computer. AC power comes from the power station through the wall outlet to the laptop’s power supply, which converts it to DC so the laptop can use it.

**Figure 12-23**

DC circuit and AC circuit



**Note 12-4**

For AC power to travel from the electric company to your house, three wires are required. The hot wire carries electricity from the power station to your house. The neutral wire carries unused power from your house back to the power station. A third wire, the ground wire, is used to channel the electric charge in case of a short. These three wires are illustrated and labeled in [Figure 12-23](javascript://).

You’re now ready to investigate the types of power fluctuations, or flaws, that network administrators should prepare for. Then you’ll learn about devices used to manage the power your network devices need.

### Power Flaws

Whatever the cause, power loss or less-than-optimal power cannot be tolerated by networks. The following list describes power flaws that can damage your equipment:

* **Surge**—A momentary increase in voltage due to lightning strikes, solar flares, or electrical problems. Surges might last only a few thousandths of a second, but they can degrade a computer’s power supply. Surges are common. You can guard against surges by making sure every computer device is plugged into a [**surge protector**](javascript://) (see [Figure 12-24](javascript://)), which redirects excess voltage away from the device to a ground, thereby protecting the device from harm. Without surge protectors, systems would be subjected to multiple surges each year.

**Figure 12-24**

A surge protector



Karen Roach/ [Shutterstock.com](http://shutterstock.com/" \t "_blank)

* **Noise**—Fluctuation in voltage levels caused by other devices on the network or EMI. Some noise is unavoidable on an electrical circuit, but excessive noise can cause a power supply to malfunction, immediately corrupting application or data files and gradually damaging motherboards and other computer circuits. If you’ve ever turned on fluorescent lights or a microwave oven and noticed other lights dim at the same time, you have probably introduced noise into the electrical system. Power that is free from noise is called clean power. To make sure power is clean, a circuit must pass through an electrical filter.
* **Brownout**—A momentary decrease in voltage; also known as a sag. An overtaxed electrical system can cause brownouts, which you might recognize in your home as a dimming of the lights. Such voltage decreases can cause computers or applications to fail and potentially corrupt data.
* **Blackout**—A complete power loss. A blackout could cause significant damage to your network. For example, if a server loses power while files are open and processes are running, its NOS might be damaged so extensively that the server cannot restart and the NOS must be reinstalled from scratch. A backup power source, however, can provide power long enough for the server to shut down gracefully and avoid harm.

**Note 12-5**

Increasingly, organizations are adding power redundancy—especially for critical servers—by installing dual power supplies in their servers, thereby giving each server at least one backup in case a power supply fails. Each power supply can handle the full power demands of the server if needed. Some companies are also running redundant power circuits to their data centers so if, for example, a circuit breaker trips, the servers can keep running on the other power circuit. Racks often have multiple UPSs installed as well.

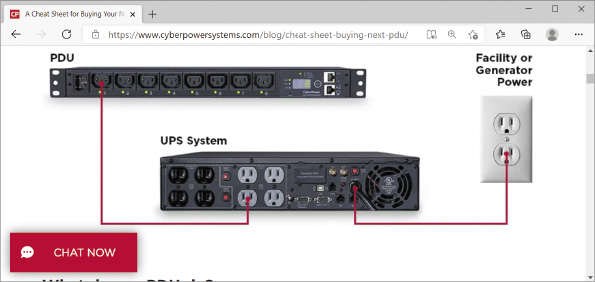
### Network Power Devices

If you track the journey of power coming into your building all the way to servers, routers, and switches on your data racks, you’ll likely encounter several types of devices along the way. Some of these devices are focused on controlling and distributing power, while other devices store or generate power. For example, as you’ve already read, a surge protector can absorb excess energy from power lines to protect sensitive network equipment from power surges.

A similar device is a [**PDU (power distribution unit)**](javascript://), which might be attached to a nearby wall, the outside of a rack, or within a rack to connect the rack’s equipment with a power source. Data rooms aren’t designed to provide enough outlets for all its devices to plug directly into the wall. Instead, a PDU acts as a power strip to bring power from outlets, a generator, or a UPS (described next) closer to the devices on the rack, as shown in [Figure 12-25](javascript://). The PDU is specifically designed to handle the high power requirements of a rack full of electronic equipment. Intelligent PDUs can even provide monitoring via SNMP and remote-control features so you can know which devices are consuming the most power, remotely power cycle a device (that is, shut off power to the device and then turn the power back on), and receive alerts or configure alarms to indicate when problems occur.

**Figure 12-25**

Install this PDU on a rack and plug into a UPS



Enlarge Image

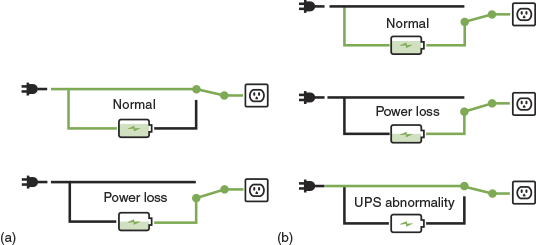
Source: Cyber Power Systems (USA), Inc.

A [**UPS (uninterruptible power supply)**](javascript://), also shown in [Figure 12-25](javascript://), is a battery-operated power source directly attached to one or more devices and to a power supply, such as a wall outlet, that provides a backup power source in the event of a power outage. A UPS can also help prevent undesired fluctuations of the wall outlet’s AC power from harming devices. A power supply issue may be long in developing, with on-again/off-again symptoms for some time before the power issue finally solidifies and reveals itself. A good UPS in each data closet or on each rack will help prevent these kinds of problems from affecting the entire network at once. Each critical workstation should also be equipped with a UPS or some other battery backup, which can help to protect the computers themselves. UPSs are classified into two general categories, as follows:

* **Standby UPS, also called an SPS (standby power supply)**—Provides continuous voltage to a device by switching virtually instantaneously to the battery when it detects a loss of power from the wall outlet. Upon restoration of power, the standby UPS switches the device back to AC power (see [Figure 12-26](javascript://)a). The problem with standby UPSs is that, in the brief amount of time it takes the UPS to discover that power from the wall outlet has faltered, a device may have already detected the power loss and shut down or restarted. Technically, a standby UPS doesn’t provide perfectly continuous power; for this reason, it is sometimes called an offline UPS. Nevertheless, standby UPSs may prove adequate even for critical network devices, such as servers, routers, and gateways. They cost significantly less than online UPSs.

**Figure 12-26**

Standby UPS vs. online UPS



* **Online UPS**—Uses the AC power from the wall outlet to continuously charge its battery while providing power to a network device through its battery, as illustrated in [Figure 12-26](javascript://)b. In other words, a server connected to an online UPS always relies on the UPS battery for its electricity. Because the server never needs to switch from the wall outlet’s power to the UPS’s battery power, there is no risk of briefly losing service. Also, because the UPS always provides the power, it can handle noise, surges, and sags before the fluctuations reach the attached device. As you can imagine, online UPSs are more expensive than standby UPSs. [Figure 12-27](javascript://) shows some online UPSs installed on a rack in a data room.

**Figure 12-27**

Online UPSs installed on a rack



UPSs vary widely in the type of power aberrations they can rectify, the length of time they can provide power, and the number of devices they can support. Of course, they also vary widely in price. UPSs intended for home and small office use are designed merely to keep your workstation running long enough for you to properly shut it down in case of a blackout. Other UPSs perform sophisticated operations such as line filtering or conditioning, power supply monitoring, and error notification. To decide which UPS is right for your network, consider these factors:

* **Amount of power needed**—The more power required by your device, the more powerful the UPS must be. Electrical power is measured in VAs (volt-amperes), also called volt-amps. A VA is the product of the voltage and current (measured in amps) of the electricity on a line. To determine approximately how many VAs your device requires, you can use the following conversion: ‍‍‍. A desktop computer, for example, may use a 200 W power supply and, therefore, requires a UPS capable of at least 280 VA to keep the CPU running in case of a blackout. A medium-sized server with a monitor and external tape drive might use 402 W, thus requiring a UPS capable of providing at least 562 VA of power. Determining your power needs can be a challenge. You must account for your existing equipment and consider how you might upgrade the supported device(s) over the next several years. Consider consulting with your equipment manufacturer to obtain recommendations on your power needs.
* **Required time to keep a device running**—The longer you anticipate needing a UPS to power your device, the more powerful your UPS must be. For example, a medium-sized server that relies on a 500 VA UPS to remain functional for 20 minutes might need a 1500 VA UPS to remain functional for 90 minutes. To determine how long your device might require power from a UPS, research the length of typical power outages in your area.
* **Line conditioning**—A UPS should offer surge suppression to protect against surges and line conditioning (a type of filtering) to guard against line noise. A UPS that provides line conditioning includes special noise filters that remove line noise. The manufacturer’s technical specifications should indicate the amount of filtration required for each UPS. Noise suppression is expressed in dB levels at a specific frequency (KHz or MHz). The higher the dB level, the greater the protection.
* **Cost**—Prices for good UPSs vary widely, depending on the unit’s size and extra features. A relatively small UPS that can power one server for 5 to 10 minutes might cost between $100 and $300. A large UPS that can power a sophisticated router for three hours might cost upwards of $5000. Still larger UPSs, which can power an entire data center for several hours, can cost hundreds of thousands of dollars. On a critical system, you should not try to cut costs by buying an off-brand, potentially unreliable, or weak UPS.

As when considering other large purchases, research several UPS manufacturers and their products before selecting a UPS. Make sure the manufacturer provides a warranty and lets you test the UPS with your equipment. Testing UPSs with your equipment is an important part of the decision-making process. Popular UPS manufacturers are APC ([apc.com](http://apc.com/" \t "_blank)), Emerson ([emerson.com](http://emerson.com/" \t "_blank)), Falcon ([falconups.com](http://falconups.com/" \t "_blank)), and Tripp Lite ([tripplite.com](http://tripplite.com/" \t "_blank)).

**Note 12-6**

After installing a new UPS, follow the manufacturer’s instructions for performing initial tests to verify the UPS’s proper functioning. Make it a practice to retest the UPS monthly or quarterly to ensure it will perform as expected in case of a sag or blackout.

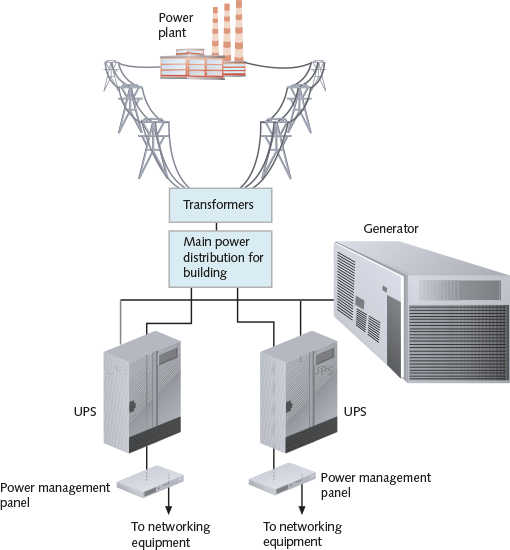
### Generators

A generator serves as a backup power source for many devices, providing power redundancy in the event of a total blackout. Generators can be powered by diesel, liquid propane gas, natural gas, or steam. Standard generators provide power that is relatively free from noise and are used in environments that demand consistently reliable service, such as an ISP’s or telecommunications carrier’s data center. In fact, in those environments, they are typically combined with large UPSs to ensure that clean power is always available. In the event of a power failure, the UPS supplies electricity until the generator starts and reaches its full capacity, typically no more than three minutes. If your organization relies on a generator for backup power, be certain to check fuel levels and quality regularly.

[Figure 12-28](javascript://) illustrates the power infrastructure of a network (such as a data center’s) that uses both a generator and dual UPSs. Because a generator produces DC power, it must contain a component to convert the power to AC before the power can be released to the existing AC infrastructure that distributes power in a data center.

**Figure 12-28**

UPSs and a generator in a network design



Enlarge Image

Before choosing a generator, calculate your organization’s crucial electrical demands to determine the generator’s optimal size. Also estimate how long the generator might be required to power your building. Depending on the amount of power draw, a high-capacity generator can supply power for several days. Gas or diesel generators can cost between $10,000 and $3,000,000 (for the largest industrial types). For a company such as an ISP that stands to lose up to $1,000,000 per minute if its data facilities fail completely, a multimillion-dollar investment to ensure available power is a wise choice. Smaller businesses, however, might choose the more economical solution of renting an electrical generator. To find out more about options for renting or purchasing generators in your area, contact your local electrical utility.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 12-3fBackup Systems

You have probably heard or even spoken the axiom, “If you can’t do without it, back it up!” A [**backup**](javascript://) is a copy of data or program files created for archiving or safekeeping. Maintaining good backups is essential for providing fault tolerance and reliability. In deciding what to back up, you might be required by certain compliance standards to back up certain types of data for a specified period. For example, HIPAA requires that medical records be saved for at least seven years from the date of the last service to the patient. You might be able to find information about compliance standards relevant to your company in an [**audit report**](javascript://). This is a document generated after an IT audit that evaluates a business’s operations, processes, infrastructure, and policies as related to its business goals and relevant laws or other standards. The auditor will identify problems or deficiencies, applicable requirements, how weaknesses or gaps might affect the business, and recommendations to correct the problems. As you design, configure, deploy, and maintain your backup system, keep these points in mind:

1. Step 1

Decide what to back up. Besides the obvious folders used to hold user and application data, you might also want to back up user profile folders and folders that hold state and configuration files for your applications, services, routers, switches, access points, gateways, and firewalls. Recall in [Capstone Project 4-1](javascript://) you used a TFTP server to back up and restore a router using its startup-config file.

1. Step 2

Select backup methods. Consider cloud backups, where third-party vendors manage the backup hardware and software. In general, cloud backups are more expensive and reliable than other methods. Because cloud backups are not stored at your local facility, you have the added advantage that backups are protected in case your entire facility is destroyed.

For onsite backups, use only proven and reliable backup software and hardware. For your backup system, now is not the time to experiment with the latest and greatest technology.

* + Verify that backup hardware and software are compatible with your existing network hardware and software.
  + Make sure your backup software uses data error-checking techniques.
  + Verify that your backup storage media or system provides sufficient capacity, with plenty of room to spare, and can also accommodate your network’s growth.
  + Be aware of how your backup process affects the system, normal network functioning, and your users’ computing habits.
  + As you make purchasing decisions, make sure you know how much the backup methods and media cost relative to the amount of data they can store.
  + Be aware of the degree of manual intervention required to manage backups, such as exchanging backup media on a regular basis or backing up operating systems on servers that run around the clock.
  + Make wise choices for storage media, considering advantages and disadvantages of media types. For example, optical media (DVDs and Blu-ray) require more frequent human intervention to exchange disks than exchanging tapes in tape drives or exchanging removable hard drives.
  + When storing data to hard drives, recognize that the drives can be installed on computers on the local network, on a WAN, in attached storage devices, or even on a sophisticated SAN.
  + Keep your backups secure, including storing backup media offsite in the event of a major disaster such as fire or flooding.

1. Step 3

Decide what types of backup will be made regularly (see [Figure 12-29](javascript://)):

* + [**Full backup**](javascript://)—Backs up everything every time a backup is done
  + [**Incremental backup**](javascript://)—Backs up only data that has changed since the last backup
  + [**Differential backup**](javascript://)—Backs up data that has changed since the last full backup

**Figure 12-29**

Incremental and differential backups demand fewer resources



Enlarge Image

**Note 12-7**

The OS knows which files to back up for incremental and differential backups because it maintains an archive bit in the attributes for each file.

1. Step 4

Decide how often backups are needed. In general, you want to back up data after about four hours of actual data entry. Depending on user habits, this might mean you back up daily or weekly, although, by default, Windows 10 performs incremental backups hourly. Many organizations perform at least daily backups, which happen in the middle of the night when there’s less network activity.

1. Step 5

Develop a backup schedule. For example, you might perform a full backup every Thursday night and an incremental backup daily. You might take backup media offsite every Friday and overwrite backups (or destroy or rotate your backup media) every six months. You also must establish policies governing who is responsible for the backups, what information should be recorded in backup logs, and which backup logs are retained and for how long. Be sure to check relevant laws and regulations, as some types of data (such as medical or financial data) must be kept for a number of years.

1. Step 6

Regularly verify backups are being performed. From time to time, depending on how often your data changes and how critical the information is, you should attempt to recover some critical files from your backup media. Many network administrators attest that the darkest hour of their career was when they were asked to retrieve critical files from a backup and found that no backup data existed because their backup system never worked in the first place!

**Note 12-8**

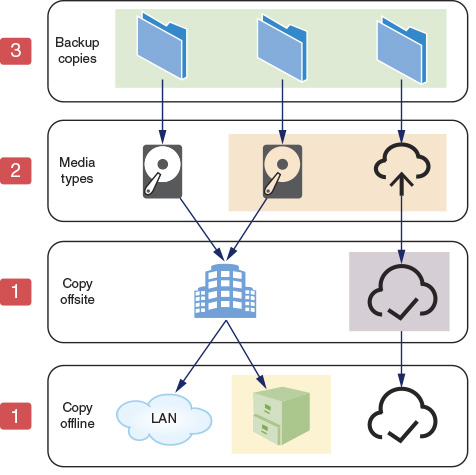
When identifying the types of data to back up, remember to include configuration files for devices such as routers, switches, access points, gateways, and firewalls.

Data backups provide a way to recover data that is lost. To do this reliably under a wide variety of adverse conditions, the [**3-2-1-1 Rule**](javascript://), as illustrated in [Figure 12-30](javascript://), defines the following backup principles:

* **3**—Keep at least three complete copies of the data.
* **2**—Save backups on at least two different media types, such as hard drive and tape drive, or tape drive and cloud storage.
* **1**—Store at least one backup copy offsite.
* **1**—For greater protection against ransomware, ensure that at least one backup copy is stored offline.

**Figure 12-30**

The 3-2-1-1 Rule for backups

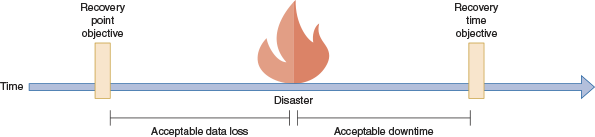


When designing contingency plans and choosing backup options, factors that will affect your decisions include the following, which are also illustrated in [Figure 12-31](javascript://):

* [**RTO (recovery time objective)**](javascript://)—The time your network can reasonably tolerate an outage. RTO shows at what point in the future full functionality will be restored (less any lost data). If you’re creating a full backup each month and differential backups each day, you can apply the full backup and one differential backup and you’re done. If, however, you’re creating an incremental backup each day, then you’ll have to apply every incremental backup since the last full backup, which will take more time. While incremental backups take up less space and take less time to create, they require more time to recover and therefore result in more recovery time needed after a loss.
* [**RPO (recovery point objective)**](javascript://)—The amount of historical data you’ll need to be able to restore from backup in response to an outage. RPO shows at what point in the past data will be recovered from. Data that was created or changed since that point will be lost because data backups were not copying data in real time. For example, relying on a full backup that’s created only once a week will result in multiple days’ worth of lost data if the disaster happens later in the week. However, if you’re also keeping incremental or differential backups each day, your RPO would lose less than a day’s worth of data.

**Figure 12-31**

RPO defines how much data loss is acceptable while RTO defines how much downtime is acceptable



Enlarge Image

**Note 12-9**

In both cases, your decisions related to RPO and RTO will likely be somewhat dictated by your company’s SLA to your customers or even to other departments within your company.

**Applying Concepts 12-5**

### Research Disaster Recovery Solutions for Small Businesses

Many companies offer DRaaS (disaster recovery as a service) solutions for all types of IT-related problems. These solutions might include basics such as offsite storage and access to virtual servers during recovery or more expensive (but more convenient) options such as customizable backup schedules and single-file recovery, which is the ability to recover a single file at a time rather than an entire drive. In this activity, you will research two different disaster recovery solutions and compare the features, cost, and reviews for each. Use complete sentences, good grammar, and correct spelling in your answers. Complete the following steps:

1. 1

Use a search engine to find companies that provide disaster recovery solutions for small businesses, and select two of these solutions. The more thorough the information provided on the company website, the easier your research will be.

1. 2

For each of your selections, find answers to at least three of the following five questions:

* + What are the key features?
  + Where would the company store your data? In other words, in what geographic areas are their servers located?
  + What kind of encryption does the company use?
  + Which standards are the services compliant with: HIPAA? PCI? SOX? GDPR?
  + Who audits the company and their disaster recovery services? What auditing process is implemented?

1. 3

Find reviews for both solutions. Summarize feedback from at least three customers about these solutions.

**Remember This…**

* Explain the purpose of an incident response plan, a business continuity plan, and a disaster recovery plan.
* Explain the purpose of a PDU, a UPS, and a generator.
* Compare cold site, warm site, hot site, and cloud site.
* Compare RTO and RPO.

**Self-Check**

1. When repairing a coworker’s computer, you find some illegal files. What should you do next?

Answer

* 1. Shut down the computer and unplug it.
  2. Take screenshots on the computer and save them in your own folder.
  3. Disconnect the computer from the network and leave it running.
  4. Delete the files.

1. Which backup site includes a running server that does not have access to the latest backups?

Answer

* 1. Warm site
  2. Cold site
  3. Hot site
  4. On site

1. Which power device prevents a critical server from losing power, even for an instant?

Answer

* 1. Surge protector
  2. Generator
  3. PDU
  4. UPS

**You’re Ready**

You’re now ready to complete [Project 12-4: Organize Your Wikidot Website](javascript://), or you can wait until you’ve finished the Review Questions for this module.

**You’re Ready**

After you finish the Hands-On Projects, you’re ready to complete the [Module 12 Capstone Projects](javascript://).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 12-4a**Module Summary**

### Collect Network Data

* At its broadest, the term network management refers to the assessment, monitoring, and maintenance of all aspects of a network. It can include controlling user access to network resources, monitoring performance baselines, checking for hardware faults, ensuring optimized QoS (quality of service) for critical applications, maintaining records of network assets and software configurations, and determining what time of day is best for upgrading hardware and software.
* Monitoring sensors in each data room, rack, or device’s chassis feed information to a physical device or software installed on a server that presents an administrative dashboard to network administrators.
* Some traffic monitoring tools will provide real-time analysis of data with alerts when conditions meet certain thresholds, while other tools are designed to log data for retroactive analysis only as needed. These historical traffic logs are primarily used to investigate network performance issues. The challenge with both real-time network monitoring and traffic logging is gaining access to the traffic itself.
* Syslog is a standard for generating, storing, and processing messages about events on many networked systems. It describes methods for detecting and reporting events and specifies the format and contents of messages.
* Organizations often use enterprise-wide network management systems to perform real-time monitoring functions across an entire network. These rely on a similar architecture with the following entities: NMS (network management system) server, managed devices, network management agent, and MIB (Management Information Base).
* NetFlow is a proprietary traffic monitoring protocol from Cisco that tracks all IP traffic crossing any interface where NetFlow is enabled. From that information, NetFlow creates flow records that show relationships among various traffic types. While SNMP focuses on individual devices, NetFlow focuses on the way network bandwidth is being utilized by identifying how communications from all devices are related to each other.

### Manage Network Traffic

* To know when there’s a problem on the network, you must first know what is normal for that network. A baseline is a report of the network’s normal state of operation and might include a range of acceptable measurements.
* As a subset of performance management, bandwidth management refers to a collection of strategies to optimize the volume of traffic a network can support. These techniques might include any of the following technologies: flow control, congestion control, and QoS (quality of service).
* Rate-based flow control limits the amount of data that can be transmitted but does not provide feedback to the sender when that rate is exceeded. Instead, traffic is lost. In contrast, feedback-based flow control at the data link layer gives the sender some kind of indication when the transmission rate is exceeding the receiver’s ability to handle the incoming traffic.
* Congestion control techniques are designed to prevent this congestion before it occurs (called open-loop congestion control) and also to remedy congestion after it starts (called closed-loop congestion control).
* Network administrators must efficiently manage a network’s QoS (quality of service) configurations, which is a group of techniques for adjusting the priority a network assigns to various types of transmissions. To do this, network administrators need to be aware of the applications used on a network, including the application protocols they use and the amount of bandwidth they require.

### Plan Response and Recovery Strategies

* An incident response plan specifically defines the characteristics of an event that qualifies as a formal incident and the steps that should be followed as a result. Incident response actually begins before the incident occurs.
* During some incidents, data will need to be collected in such a way that it can be presented in a court of law for the purpose of prosecuting an instigator of illegal activity. Some of the forensic data available for analysis can be damaged or destroyed if improperly handled. It’s critical that every IT technician in a company know how to safeguard sensitive information, logged data, and other legal evidence until the first responder or incident response team can take over the collection of evidence.
* When bad things happen, businesses need a plan to ensure business continuity, which is the ability of the company to continue doing business with the least amount of interruption possible. At a high level, a BCP (business continuity plan) defines the resources and protocols the business will use to continue providing service to its customers with little or no disruption during a disaster.
* Disaster recovery contingencies are commonly divided into these categories: cold site, warm site, hot site, and (more recently) cloud site. These options vary by the amount of hardware, software, planning, investment, and employee involvement each requires. They also vary according to how quickly they will restore network functionality in case a disaster occurs.
* Part of managing a network’s availability involves managing the facilities and infrastructure that support the network, such as power connections and power sources during outages or fluctuations. Some of the devices involved in providing power to a network are focused on controlling and distributing power, while other devices store or generate power.
* You might be able to find information about compliance standards relevant to your company in an audit report. This is a document generated after an IT audit that evaluates a business’s operations, processes, infrastructure, and policies as related to its business goals and relevant laws or other standards. The auditor will identify problems or deficiencies, applicable requirements, how weaknesses or gaps might affect the business, and recommendations to correct the problems.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 12-4b**Key Terms**

* [**3-2-1-1 Rule**](javascript://)
* [**alert**](javascript://)
* [**audit log**](javascript://)
* [**audit report**](javascript://)
* [**audit trail**](javascript://)
* [**backup**](javascript://)
* [**bandwidth management**](javascript://)
* [**baseline**](javascript://)
* [**BCP (business continuity plan)**](javascript://)
* [**buffering**](javascript://)
* [**business continuity**](javascript://)
* [**chain of custody**](javascript://)
* [**cloud site**](javascript://)
* [**cold site**](javascript://)
* [**congestion control**](javascript://)
* [**CoS (Class of Service)**](javascript://)
* [**delay-sensitive**](javascript://)
* [**differential backup**](javascript://)
* [**DiffServ (Differentiated Services)**](javascript://)
* [**disaster**](javascript://)
* [**disaster recovery plan**](javascript://)
* [**DRaaS (disaster recovery as a service)**](javascript://)
* [**DSCP (Differentiated Services Code Point)**](javascript://)
* [**Event Viewer**](javascript://)
* [**first responder**](javascript://)
* [**flow control**](javascript://)
* [**full backup**](javascript://)
* [**hot site**](javascript://)
* [**incident**](javascript://)
* [**incident response plan**](javascript://)
* [**incremental backup**](javascript://)
* [**iPerf**](javascript://)
* [**log**](javascript://)
* [**logging level**](javascript://)
* [**loss-tolerant**](javascript://)
* [**MIB (Management Information Base)**](javascript://)
* [**NetFlow**](javascript://)
* [**NetFlow analyzer**](javascript://)
* [**network management**](javascript://)
* [**NMS (network management system) server**](javascript://)
* [**OID (object identifier)**](javascript://)
* [**packet analysis**](javascript://)
* [**PDU (power distribution unit)**](javascript://)
* [**RPO (recovery point objective)**](javascript://)
* [**RTO (recovery time objective)**](javascript://)
* [**severity level**](javascript://)
* [**surge protector**](javascript://)
* [**system log**](javascript://)
* [**traffic analysis**](javascript://)
* [**traffic log**](javascript://)
* [**traffic policing**](javascript://)
* [**traffic shaping**](javascript://)
* [**trap**](javascript://)
* [**UPS (uninterruptible power supply)**](javascript://)
* [**warm site**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 12-4c**Review Questions**

1. While troubleshooting a recurring problem on your network, you want to examine the TCP messages being exchanged between a server and a client. Which tool should you use on the server?
   1. Spiceworks
   2. Wireshark
   3. iPerf
   4. NetFlow
2. One of your coworkers downloaded several, very large video files for a special project she’s working on for a new client. When you run your network monitor later this afternoon, what list will your coworker’s computer likely show up on?
   1. Top talkers
   2. Top listeners
   3. Giants
   4. Jabbers
3. What command requests the next record in an SNMP log?
   1. SNMP Get Request
   2. SNMP Get Next
   3. SNMP Trap
   4. SNMP Get Response
4. What port do SNMP agents listen on?
   1. Port 161
   2. Port 21
   3. Port 162
   4. Port 20
5. Your roommate has been hogging the bandwidth on your router lately. What feature should you configure on the router to limit the amount of bandwidth his computer can utilize at any one time?
   1. Power management
   2. Congestion control
   3. Flow control
   4. Traffic shaping
6. What field in an IPv4 packet is altered to prioritize video streaming traffic over web surfing traffic?
   1. Traffic Class
   2. Priority Code Point
   3. Time to Live
   4. DiffServ
7. Which power backup method will continually provide power to a server if the power goes out during a thunderstorm?
   1. Online UPS
   2. Generator
   3. Dual power supplies
   4. Standby UPS
8. Which type of disaster recovery site contains all the equipment you would need to get up and running again after a disaster, and yet would require several weeks to implement?
   1. Warm site
   2. Standby site
   3. Hot site
   4. Cold site
9. Which log type is used to prove who did what and when?
   1. Traffic log
   2. Audit log
   3. System log
   4. Syslog
10. Which data link layer flow control method offers the most efficient frame transmission when sending large volumes of data?
    1. Go-back-n sliding window
    2. Choke packet
    3. Selective repeat sliding window
    4. Stop-and-wait
11. When you arrive at work one morning, your inbox is full of messages complaining of a network slowdown. You collect a capture from your network monitor. What documentation can help you determine what has changed?
12. What are the primary data link layer flow control methods?
13. What’s the difference between an incident and a disaster?
14. Which QoS technique operates at layer 2 to more efficiently route Ethernet traffic between VLANs?
15. What’s the difference between a PDU and a UPS?
16. Why might you want to install two power supplies in a critical server?
17. What are the two main categories of UPSs?
18. Which congestion control techniques help to prevent network congestion?
19. What is the primary challenge in properly configuring NetFlow?
20. Which backup type, if performed daily, would offer the lowest RTO and why?

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 12-4d**Hands-On Projects**

**Note 12-10**

Websites and applications change often. While the instructions given in these projects were accurate at the time of writing, you might need to adjust the steps or options according to later changes.

**Note to Instructors and Students:** A rubric is provided for evaluating student performance on these projects. Please see Appendix D.

**Project 12-1**

### Work with Data in Event Viewer

* **Estimated Time:** 20 minutes
* **Objective:** Given a scenario, use the appropriate statistics and sensors to ensure network availability. (Obj. 3.1)
* **Resources:**
  + Windows 10 computer with administrative privileges
* **Context:** In this module, you learned how to access and view event log information through the Event Viewer application in Windows 10. In this project, you will practice filtering the information contained in the log. As in the “Applying Concepts: Explore Event Viewer in Windows” project, you need a computer running Windows 10. Ideally, it should be a computer that has been used for a while, so that the event log contains several entries. It need not be connected to a network. However, you must be logged on to the computer as a user with administrator privileges. Complete the following steps:
  + 1

Open Event Viewer. In the left pane, click the **Custom Views** arrow and then click **Administrative Events.** A list of Administrative Events appears in the center pane of the Event Viewer window. This log lists Critical, Error, and Warning events.

* + 2

Suppose you want to find out whether your workstation has ever experienced trouble obtaining a DHCP-assigned IP address. In the Actions pane (the pane on the right), in the Administrative Events section, click **Find.** The Find dialog box opens.

* + 3

Type **dhcp** and then click **Find Next.**

* + 4

What is the first DHCP-related event you find? When did it occur? What was the source of this event? Read the description of the event in the General tab to learn more about it. Note: If the computer did not find a DHCP event, first make sure the topmost record is selected before beginning your search to ensure that all the records are searched. If a DHCP event is still not found, search for a different kind of event such as DNS or Service Control Manager. Otherwise, choose another event at random.

* + 5

Click **Cancel** to close the Find dialog box. Keep the event listing that you found highlighted.

* + 6

Now suppose you want to be notified each time your workstation experiences this error. In the Actions pane, click **Attach Task To This Event.** The Create Basic Task Wizard dialog box opens.

* + 7

In the Name text box, replace the default text with **DHCP\_my\_computer** or some other text appropriate for the type of event you’re saving. Click **Next** to continue.

* + 8

You’re prompted to confirm the Log, Source, and Event ID for this error. Click **Next** to continue.

* + 9

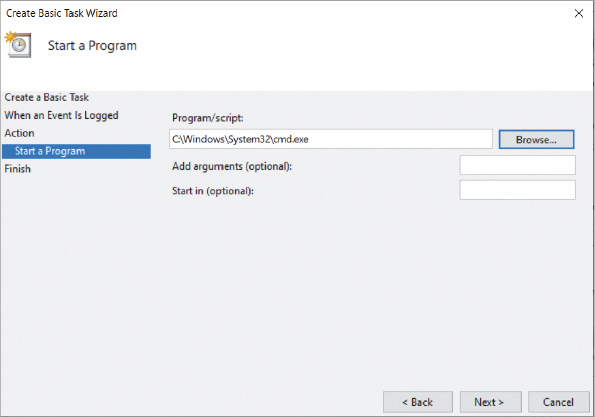
You’re prompted to indicate the type of action the operating system should take when this error occurs. **Start a program** is the only option not deprecated and should be selected by default. Click **Next** to continue.

* + 10

Now you are asked to provide information about the program you want the system to open. Click the **Browse** button and find the cmd.exe file. The default location for cmd.exe is **C:\Windows\System32\cmd.exe** as shown in [Figure 12-32](javascript://), although your location path might be different. Select the file and click **Open**. Click **Next** to continue.

**Figure 12-32**

Create an action to start Command Prompt



Enlarge Image

* + 11

A summary of your notification selections appears. **Take a screenshot** of your task configuration; submit this visual with your answers to this project’s questions. Click **Finish** to create the task and add it to the actions your operating system will perform.

* + 12

An Event Viewer dialog box opens, alerting you that the task has been created. Click **OK** to confirm.

* + 13

You can see the task you just created by opening Task Scheduler. Press **Win** + **R** and enter **taskschd.msc**.

* + 14

In the Task Scheduler window, click the down arrow next to **Task Scheduler Library** and then click **Event Viewer Tasks**. Select the task you just created and answer the following questions:

* + 1. In the lower pane, check the Security options section. Which user account will be used when the task runs?
    2. Click **Run** in the Actions pane. What happens?
    3. What command would keep this task from running without removing it from Task Scheduler?
  + 15

You can now delete this task if you want. Close all open windows.

**Project 12-2**

### Configure SPAN and Syslog in Packet Tracer

* **Estimated Time:** 45 minutes
* **Objective:** Given a scenario, use the appropriate statistics and sensors to ensure network availability. (Obj. 3.1)
* **Resources:**
  + Packet Tracer
* **Context:** In this module, you read about various ways to capture network traffic for analysis and monitoring. In this project, you’ll experiment with two of these technologies: SPAN on switches and a syslog server. Complete the following steps:
  + 1

Open Packet Tracer. In your Packet Tracer workspace, add a 2960 switch and three PCs.

* + 2

Configure static IP addresses on all three PCs within the same subnet. What IP addresses did you assign each PC?

* + 3

Connect the PCs to the first three switch ports (FastEthernet 0/1 – 0/3). Wait for all connections to come up.

* + 4

In the bottom right corner, click **Simulation**. This opens the Simulation Panel.

* + 5

By default, the simulation will display all messages from all protocols on the network once you start the simulation—you can see a list of applicable filters in the Event List Filters – Visible Events section. For this project, you only want to see ICMP messages. At the bottom of the Simulation Panel, click **Show All/None**, which clears all visible event types. Click **Edit Filters**. In the PacketTracer7 filters window, check the box on the IPv4 tab for **ICMP**. Close the PacketTracer7 filters window. Confirm ICMP is the only visible event type listed.

* + 6

When you start the simulation in the next step, you will run pings between PCs on your network, and the results will display in the PDU List Window in the bottom right corner of your Packet Tracer interface. For a more convenient arrangement, in the bottom middle pane, click **Toggle PDU List Window** to move this pane to a larger space in your Packet Tracer interface. If desired, you can also grab the top bar of the Simulation Panel to move this module around on your screen in a separate window.

* + 7

On the common tools bar, click the **Add Simple PDU (P)** button, which looks like a closed envelope. This will create a ping-based conversation between two devices. Click **PC0** as the source device and click **PC1** as the destination device.

* + 8

In the Simulation Panel, click the **Play (Alt + P)** button. As the simulation begins, a PDU leaves PC0 and arrives at the switch. Watch the traffic carefully. To which device does the switch send the first PDU? Why do you think this is?

* + 9

At the bottom of the interface, click the **Delete** button to stop the simulation for this scenario. Click **Realtime** to return to Realtime mode.

* Now you’re ready to add a sniffer to the network that will monitor all traffic on the switch. Complete the following step:
  + 10

From the End Devices group, add a **Sniffer** to the workspace. Connect the sniffer’s Ethernet0 port to the switch’s FastEthernet 0/24 port. The sniffer does not need an IP address to do its job.

* With these devices connected to your network, you’re ready to configure a SPAN monitoring session on the switch. Complete the following steps:
  + 11

On the switch’s **CLI** tab, enter the commands in [Table 12-1](javascript://).

**Table 12-1**

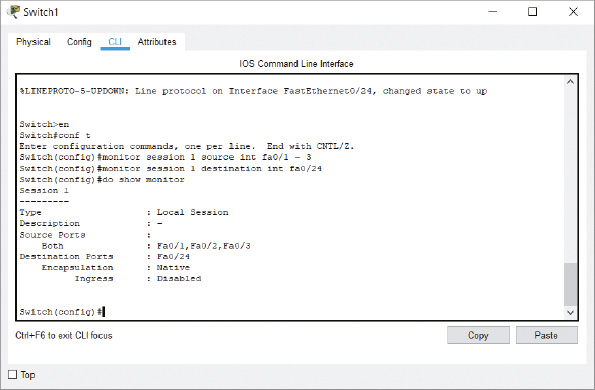
### Configure a SPAN monitoring session on a switch

| **Command** | **Purpose** |
| --- | --- |
| **enable** | Enables privileged EXEC mode |
| **configure terminal** | Enters global configuration mode |
| **monitor session 1 source int fa0/1 - 3** | Configures source interfaces for the monitoring session |
| **monitor session 1 destination int fa0/24** | Configures the destination interface for the monitoring session (there can be only one) |
| **do show monitor** | Displays the monitoring session configuration; confirm your configuration matches that shown in [Figure 12-33](javascript://) |

Enlarge Table

**Figure 12-33**

SPAN monitoring session from three interfaces to FastEthernet 0/24



Enlarge Image

Source: Cisco Systems, Inc.

* + 12

To test your monitoring session, enter Simulation Mode and send a simple PDU from PC0 to PC1 again. Watch the traffic carefully. To which device(s) does the switch send the PDU this time? Why do you think this is?

* + 13

To see the captured traffic, click the **Sniffer** and click its **GUI** tab. Apply the same filter here as the one you used for Simulation Mode in [Step 4](javascript://) and run the ping again. Click any of the captured ICMP messages. What are the source and destination IP addresses of the message you chose?

* Syslog is another way to capture network traffic; however, syslog functions differently by capturing messages processed on a monitored device. To compare SPAN and syslog functionality, complete the following steps:
  + 14

Add a 2901 router and a server to the workspace. Connect both to the switch.

* + 15

On the server’s **Services** tab, confirm the Syslog service is turned on. Configure the server with a static IP address on the same subnet as your PCs. What IP address did you give the server?

* + 16

Configure the router with a static IP address and turn on the interface connected to the switch.

* Syslog logging is enabled by default on the router, but additional information is needed to send the required logs to the server. Complete the following steps:
  + 17

To configure syslog logging on the router’s CLI, enter the commands listed in [Table 12-2](javascript://), starting in global configuration mode.

**Table 12-2**

### Configure syslog on a router

| **Command** | **Purpose** |
| --- | --- |
| **logging <server IP address>** | Tells the router where to send syslog messages |
| **logging trap debugging** | Requires all messages from the debugging level (level 7, which is the lowest severity level) and above to be logged with the server; note that Packet Tracer only supports logging at level 7 (debugging), which includes all severity levels |
| **exit** | Returns to privileged EXEC mode |
| **debug ip icmp** | Enables debugging for ICMP messages |
| **show debugging** | Displays debugging configuration; confirm ICMP packet debugging is on |
| **show logging** | Displays syslog configuration |

Enlarge Table

* + 18

Check the logging configuration on your router. Where are the router’s logs being sent? What port are these messages using?

* + 19

To test your syslog configuration, ping one of your PCs from your router. Return to your syslog server to examine captured traffic. **Take a screenshot** of the Syslog Service window showing logged traffic; submit this visual with your answers to this project’s questions. How many ICMP messages are logged?

* + 20

Syslog captured the ICMP messages for a ping between the router and a PC. Now ping between two PCs. Return to your syslog server to examine captured traffic. How many ICMP messages are logged now? Why do you think this is?

* + 21

Save this Packet Tracer file in a safe place for future reference. Make some notes on your Wikidot website about your activities in Packet Tracer for this project.

**Note to instructors:** A Packet Tracer solution file is provided for each Packet Tracer project through the Instructors site.

**Project 12-3**

### Test Network Throughput with iPerf

* **Estimated Time:** 30 minutes
* **Objective:** Given a scenario, use the appropriate network software tools and commands. (Obj. 5.3)
* **Resources:**
  + Windows computer
  + A second device, such as a computer (Windows, Linux, or macOS) or smartphone (Android or iOS)
  + Access to the same computer used to complete [Capstone Project 1-1](javascript://) or [1-2](javascript://)
  + Internet access
* **Context:** In this module, you read about iPerf, which is a CLI-based tool for testing throughput between two devices on your local network. In this project, you’ll install iPerf on two devices and then test throughput between them. Complete the following steps:
  + 1

On your primary computer, go to [iperf.fr](http://iperf.fr/" \t "_blank). Download the latest version of iperf3 for your computer and save the download in your Downloads folder. Extract the contents of the iperf download.

* + 2

Create a new folder named **iperf** in the root folder for your Windows drive. For example, if Windows is installed on your C: drive, create the folder **C:/iperf**.

* + 3

Move the iperf files from your Downloads folder to your new iperf folder. This will make it easier to find the iperf files from the CLI.

* + 4

Open a Command Prompt window. Enter the command **cd c:/iperf** to navigate to the folder you just created.

* + 5

Enter the command **iperf3.exe** to see the help files. Which command starts server mode?

* Now you’re ready to install iPerf on your secondary device. This device could be another computer (Windows, Linux, or macOS) or a smartphone (Android or Linux). Complete the following steps:
  + 6

Make sure your secondary device is on the same network as your primary device.

* + 7

If you’re using a computer, repeat [Steps 1](javascript://), [2](javascript://), [3](javascript://) and [4](javascript://) to prepare the computer.

* + 8

If you’re using a smartphone, find the free iPerf app for your phone and install it.

* You’re now ready to run iPerf between the two devices. Complete the following steps:
  + 9

Your primary device will be the iperf server. On your iperf server, enter the command **ipconfig** to display your computer’s IP address. Record this information for future use. Next, enter the command **iperf3.exe -s** so the server will start listening. In the Windows Security Alert window, click **Allow access**.

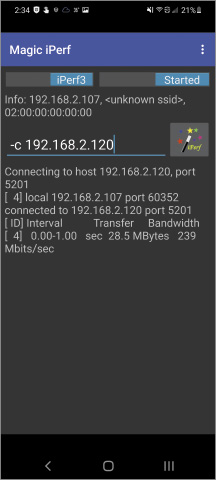
* + 10

Your secondary device will be the iperf client:

* + 1. If your secondary device is a computer, enter the command **iperf3.exe -c** ***<server’s IP address>***. For example, if the server’s IP address from [Step 9](javascript://) is 192.168.2.120, you would enter the command iperf3.exe -c 192.168.2.120.
    2. If your secondary device is a smartphone, enter the parameter **-c** ***<server’s IP address>***. For example, if the server’s IP address from [Step 9](javascript://) is 192.168.2.120, you would enter the parameter -c 192.168.2.120. At the top of the screen, toggle the **Stopped** switch to **Started** (see [Figure 12-34](javascript://)).

**Figure 12-34**

A free iPerf app on Android



Source: NextDoorDeveloper

* + 11

Watch the output on both devices for several seconds. When you’re ready, stop the test on the computer(s) by pressing **Ctrl+C**. On a smartphone, stop the test by toggling the **Started** switch to **Stopped**.

* + 12

**Take a screenshot** of the client’s output; submit this visual with your answers to this project’s questions.

* + 13

What are some of the speeds your test reported? Are these speeds what you expect on your network? What troubleshooting might you need to do to determine how to increase your network speeds?

* + 14

Start your Windows VM that you created in [Capstone Project 1-1](javascript://) or [1-2](javascript://). Repeat the steps needed to install iPerf on the VM. Then run the iperf server on your primary computer and the iperf client on your VM. How does the throughput for this connection differ from the throughput for the earlier test?

* + 15

Document this application installation in your wikidot website.

**Project 12-4**

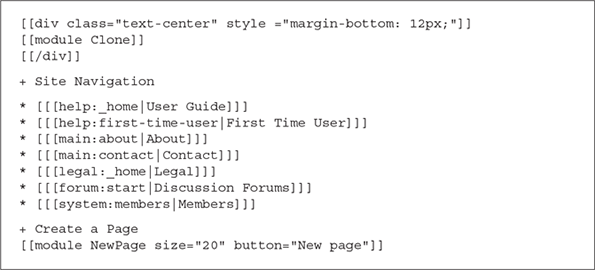
### Organize Your Wikidot Website

* **Estimated Time:** 45 minutes (+15 minutes for group work, if assigned)
* **Objective:** Explain the purpose of organization documents and policies. (Obj. 3.2)
* **Group work:** This project includes enhancements when assigned as a group project.
* **Resources:**
  + Internet access
* **Context:** Throughout this course, you’ve kept notes on various projects in your Wikidot website. To finish up these projects, let’s do some final cleanup and organization so these notes will continue to be useful and easily accessible for you as you move into your other IT classes and your career. You might decide to continue adding notes, pages, and categories, or create new wikis as needed. Using good organization and adding thorough notes could make your wiki a valuable exhibit when applying for your first job in IT. Complete the following steps:
  + 1

First, adjust the side navigation menu. On the All Pages page (click the gear icon and click **List All Pages**), click **Side Navigation** and then click **Edit**. You should see the text shown in [Figure 12-35](javascript://). Throughout this project, you can ignore any red, squiggly lines in the text unless they indicate a place where you’ve misspelled a word. Be sure to use correct spelling and good grammar in your wiki’s content text.

**Figure 12-35**

Side navigation bar coding



Enlarge Image

Source: Wikidot Inc.

* + 2

Change the User Guide link to point to the list of all pages instead. On the User Guide line (the first line under “+ Site Navigation”), edit it to read as follows:

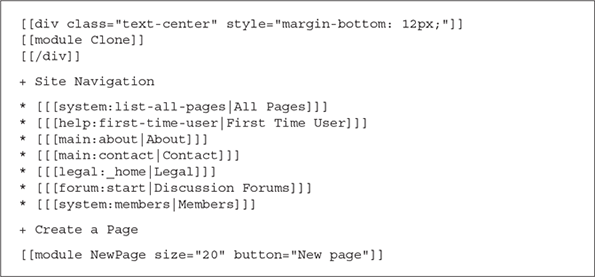
The user guide link is pointed to the list of all pages. The code is as follows. Left bracket, left bracket, left bracket, system, colon, list hyphen all hyphen pages, pipe, All Pages, right bracket, right bracket, right bracket.

* + 3

When you’re finished, the edited text should match the first item in the Site Navigation list in [Figure 12-36](javascript://). Save your changes and test the new link under Site Navigation on the right.

**Figure 12-36**

Edited side navigation bar



Enlarge Image

Source: Wikidot Inc.

* Each time you named a page with one part before the colon and another part after the colon, such as Applications:Wireshark, you added that page to a category. The first name, such as Applications, is the name of the category. The second name, such as Wireshark, is the name of the page. Complete the next step to display all available categories:
  + 4

To see a list of all categories in your wiki, click the gear icon and then click **Site Manager**, **Appearance & Behaviour**, and **Navigation elements**. Click the drop-down arrow next to Choose the category.

* Here, you can see the available categories, including the ones you’ve created. The trick now is to find a way to list pages according to each category. To do this, you’ll first need to create a Categories page. Complete the following steps:
  + 5

Go back to your wiki and create a new page called **system:All Categories**.

* + 6

Add the text **[[module Categories]]** to your page and save it.

* + 7

Go back to the All Pages list. The All Categories page is listed as “system:All Categories.” To change page name to “All Categories” instead, click the **system:All Categories** page, click **Edit**, and change the title to **All Categories**. The name of the page still includes its category (system), but now the title of the page is simply “All Categories.”

* This module automatically creates a list of all the categories and all the pages within each category. If any page is listed in the wrong module, you can’t edit the page’s title to change its category. When you edit the page, you’re editing the title of that page, not its name, which is what defines the page’s category. Instead, use the following step to edit the page’s category:
  + 8

If a page is listed in the wrong category, go to the page and click **+** **Options** and then click **Rename**. Change the page’s category, which is the name before the colon, and click **Rename/move**. Repeat for any other miscategorized pages.

* Now let’s edit the top navigation bar so it shows one or more categories as an option, and each page within that category as an option. Complete the following steps:
  + 9

Click the gear icon and click **Edit Top Bar**.

* + 10

Click the **Edit** button on this page. You should see text similar to [Figure 12-37](javascript://).

**Figure 12-37**

Top navigation bar coding



Enlarge Image

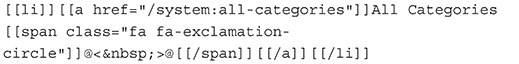
Source: Wikidot Inc.

* Currently, the only link in the top navigation bar that gives a drop-down menu is the Help Docs link. In the next few steps, you’ll remove some of the links in the top navigation bar and add a drop-down link for each category. Complete the following steps:
  + 11

Delete the **Layout** and **Membership** lines in this text (lines 3 and 4).

* + 12

On the next line, change the text **User Guide** to **All Categories**. Change its location to **system:all-categories**. The line should now read as follows:



* + 13

On the dropdown-toggle line, change the text **Help Docs** to the name of one of your categories, such as **Applications**.

* For this step, you’ll create dropdown items for the dropdown link you just created. It might help to have two browser windows open—one showing the All Pages list for a reference and the other showing the top navigation menu editing page. Add extra lines if needed. Complete the next step:
  + 14

For each sub-item, add the name and location of a page within that category. For example, the Wireshark page would be listed under Applications like this:

For each sub-item, the name and location of a page within that category is added. The code for the Wireshark page is listed under Applications as follows. Line 1. Left bracket, left bracket, l i, right bracket, right bracket, left bracket, left bracket, a. Line 2: h ref, equals, left double quotation mark, forward slash, applications, colon, Wireshark, right double quotation mark, right bracket, right bracket, Wireshark left bracket, left bracket, forward slash, a, right bracket, right bracket, left bracket, left bracket, forward slash, l i, right bracket, right bracket.

The Nmap line will look like this:

For each sub-item, the name and location of a page within that category is added. The code for the N map line is as follows. Line 1. Left bracket, left bracket, l i, right bracket, right bracket, left bracket, left bracket, a, h ref, equals, left double quotation mark, forward slash, applications, colon, n map, right double quotation mark, right bracket, right bracket, N map left bracket, left bracket, forward slash, a, right bracket, right bracket, left bracket, left bracket, forward slash, l i, right bracket, right bracket.

* Notice the small icons next to each item on the top navigation menu, such as an “i” in a circle, an exclamation mark in a circle, and a question mark in a circle. To change some of these icons, complete the following steps:
  + 15

On the Applications line (the line that includes the dropdown-toggle text), change the text that reads "fa fa-question-circle" so it says **"fa fa-info-circle"**.

* + 16

On the About line (line 2), change the text that reads "fa fa-info-circle" so it says **"fa fa-question-circle"**.

* + 17

When you’ve made all these changes, review the navigation menu again and correct any typos or missed links. When you’re ready, click **Save**. The new Top Navigation bar shows in the page’s content area and at the top of the page.

* + 18

Test each link to make sure it works correctly, and troubleshoot any problematic links. To make changes, go back to the **Top Navigation** page and click **Edit**. The edited text should look something like [Figure 12-38](javascript://). Make sure the page addresses are typed exactly right.

**Figure 12-38**

The edited top navigation bar



Enlarge Image

Source: Wikidot Inc.

* + 19

Add more categories and pages links, as desired, until you’ve listed all your categories and pages that you created for projects in this text.

* + 20

On the top navigation bar, add a link to the All Pages page, with an information circle next to it. This link will make the All Pages page accessible directly from the Home page. What line of code must you add to the top navigation bar’s code to accomplish this?

* + 21

Edit the Home page text and the About page text to reflect what you’ve accomplished during this course and to describe the information available in your wiki. Make any other changes you would like to the navigation menus, categories, or pages. You might add screenshots or photos to some of the pages, add more detailed notes, or create new categories for other projects you’ve completed. If desired, research other editing options, themes, codes, and modules so this wiki reflects your interests and learning progress.

* + 22

**For group assignments:** Invite a team member to check out your wiki and test your links. Correct any problems they find. In exchange, review your teammate’s wiki and report any errors you find. Exchange notes and ideas for ways to improve your wikis.

* + 23

When you’re ready, **take a screenshot** of your wiki showing the top navigation and side navigation panes; submit this visual with your answers to this project’s questions. Providing a link to your wiki when applying for an IT job could make a strong, positive first impression on a potential employer!

Go to pg.

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Module Review

## 12-4e**Capstone Projects**

**Note 12-11**

Websites and applications change often. While the instructions given in these projects were accurate at the time of writing, you might need to adjust the steps or options according to later changes.

**Note to Instructors and Students:** A rubric is provided for evaluating student performance on these projects. Please see Appendix D.

**Capstone Project 12-1**

### Use Syslog in Ubuntu Desktop

* **Estimated Time:** 45 minutes
* **Objective:** Explain common ports and protocols, their application, and encrypted alternatives. (Obj. 1.5)
* **Resources:**
  + Access to the same computer used to complete [Capstone Project 2-1](javascript://)
* **Context:** In this project, you will view and manipulate log file entries on a computer running the Linux operating system. Because Linux versions vary in the type of GUI application that allows you to open the system log, this exercise uses the CLI instead. For this exercise, you need a computer with a Linux operating system installed, such as the Ubuntu Desktop VM that you created in [Module 2](javascript://), [Capstone Project 2-1](javascript://). It need not be connected to a network, but for best results, it should be a computer that has been used in the past and not a fresh install. You must be logged on to the Linux computer as a user with administrator privileges. Complete the following steps:
  + 1

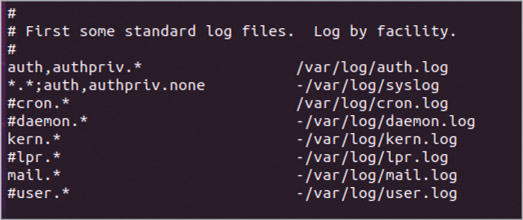
Start your Ubuntu Desktop VM and open Terminal.

* + 2

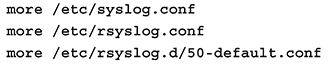
The syslog file contains information similar to that shown in [Figure 12-39](javascript://). The first step in viewing your Linux computer’s system log is to find out where the file is located. Try each of these commands until you find the syslog file that contains information similar to that in [Figure 12-39](javascript://):

**Figure 12-39**

Log files and their locations



Source: Canonical Group Limited



* + 3

The first part of the syslog file appears. In this part of the file, you should see a list of log types and their locations, similar to the listing shown in [Figure 12-39](javascript://). (If you don’t see the listing in this part of the file, press the **Enter** or **Spacebar** key until you do see it.)

* + 4

Write down the location and filename of the file that logs all events, as indicated by \*.\* in the first column. (For example, it might be /var/log/syslog or /var/adm/messages.)

* + 5

Press the **Spacebar** enough times to view the entire log configuration file and return to the shell prompt.

* + 6

Now that you know the name and location of your system log, you can view its messages. At the shell prompt, enter one of the following commands, depending on your log file’s location:

* + - If your log file is at /var/log/syslog, enter **tail /var/log/syslog**
    - If your log file is at /var/adm/messages, enter **tail /var/adm/messages**
  + 7

The last 10 lines of your log file appear (assuming it is at least 10 lines long). What types of messages are recorded? When did the events occur?

* + 8

Next find out all the types of log files your computer saves. Enter one of the following to change your working directory to the same directory where log files are kept:

* + - If your log file is in the /var/log directory, enter **cd /var/log**
    - If your log file is in the /var/adm directory, enter **cd /var/adm**
  + 9

To view a listing of the directory’s contents, enter **ls –la**. List two types of log files that appear in this directory.

* + 10

Suppose you want to find every message in the system log file that pertains to DHCP addressing. At the shell prompt, enter one of the following:

* + - If your log file is named syslog, enter **grep DHCP syslog**
    - If your log file is named messages, enter **grep DHCP messages**

A list of messages containing the term DHCP appears, if there are any.

* + 11

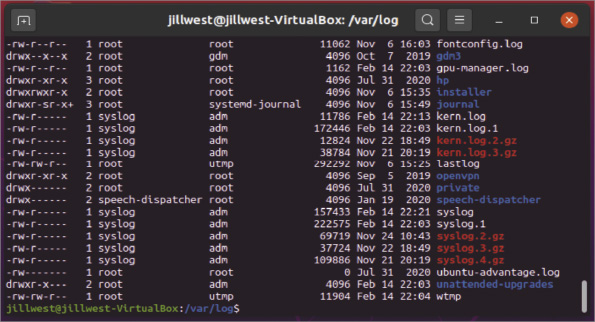
Re-enter your command from [Step 6](javascript://) and then run a new search using a text string that appears in your results. What command did you use? **Take a screenshot** of your results showing successful location of the text string; submit this visual with your answers to this project’s questions.

* + 12

If your operating system is configured to start a new log file each day or each time the computer is restarted, your log file might be brief. Repeat [Step 9](javascript://) and this time, look for other versions of the syslog or messages file in your working directory. For example, Ubuntu Linux will save older system messages in a file called syslog.1, syslog.2, and so on (see [Figure 12-40](javascript://)). If you find a larger, older log file, repeat [Step 10](javascript://) using this log file’s name. How do the results differ?

**Figure 12-40**

Several older syslog files are listed



Enlarge Image

Source: Canonical Group Limited

* + 13

Close the Terminal session window and power off your Ubuntu VM. Make some notes on your Wikidot website about your activities for this project.

**Capstone Project 12-2**

### Manage Log Files in Ubuntu Server

* **Estimated Time:** 30 minutes
* **Objective:** Given a scenario, use the appropriate statistics and sensors to ensure network availability. (Obj. 3.1)
* **Resources:**
  + Access to the same computer used to complete [Capstone Project 3-1](javascript://)
* **Context:** Oftentimes it seems that working with Linux operating systems is like driving a stick shift while working with Windows is like driving an automatic. For example, to configure an installed program in Ubuntu, you must edit a text file.

Ubuntu creates various logs to track just about any event, and these logs are also stored as text files. By default, most are stored in the /var/log directory. For example, Ubuntu stores early initialization information for cloud instances (such as hostname and SSH keys) in a text file that, by default, is /var/log/cloud-init.log. (You can change the default path and filename by editing the /etc/cloud-init.conf file.) Using the installation of Ubuntu Server in a VM you created in [Capstone Project 3-1](javascript://), follow along to learn how to manage log files in Ubuntu:

* + 1

Start Ubuntu Server and log on with your username and password. Refer to your LastPass vault if you don’t remember that information.

* + 2

Enter the commands shown in [Table 12-3](javascript://) to work with Ubuntu log files.

**Table 12-3**

### Manage Ubuntu log files

| **Command** | **Explanation** |
| --- | --- |
| **cd /var/log** | Goes to the directory that contains log files. |
| **ls –l | less** | Lists all files and subdirectories, and details about each item, one page at a time. Look for log files that have gotten excessively large. If a technician doesn’t monitor and control log files, they may get large enough to take up all available hard drive space and bring a system down. Press the **spacebar** to move to the next page and **q** to return to the prompt. |
| **ls –l cloud-init.log** | Lists details about cloud-init.log. Notice the file is owned by syslog. Also notice the file size. If it is 0, look for another large log file and view information about that one instead. |
| **less cloud-init.log** | Views and pages through the contents of the file. Note that if you want to view a file owned by root, you must use the **sudo** command in front of the less command. What are some common entries in this log? |
| **q** | Quits the less pager. |
| **grep “ownership” cloud-init.log** | Uses the **grep** command to narrow down a search in a text file for a particular string of text. Remember you must use the **sudo** command if you’re trying to access a file owned by root. The **grep** command is particularly useful for large text files when you’re searching for a particular username, event, or command. How many results did you get? If you didn’t get any results, use a word that showed up frequently when you viewed the contents of the file. |
| **grep “OWNERSHIP” cloud-init.log** | Searches for the same text string except using all capital letters in the string. How many results do you see? |
| **grep –i “OWNERSHIP” cloud-init.log** | Ignores case when searching. **Take a screenshot** of the output; submit this visual with your answers to this project’s questions. |

Enlarge Table

* + 3

It’s helpful to learn about other log files in the /var/log directory. Search the [help.ubuntu.com](http://help.ubuntu.com/" \t "_blank) website or do a general Google search on three log files you find in the directory (enter **ls –l** again if you need to see the list again). Write a one-sentence description of the type of information kept in each file and why a technician might find this information helpful.

* + 4

Power off your Ubuntu Server VM and make some notes on your Wikidot website about your activities for this project.

**Capstone Project 12-3**

### Use PRTG to Monitor Network Devices

* **Estimated Time:** 60 minutes
* **Objective:** Given a scenario, use the appropriate statistics and sensors to ensure network availability. (Obj. 3.1)
* **Resources:**
  + Access to the same computer used to complete [Capstone Project 1-1](javascript://) or [1-2](javascript://)
  + Internet access
* **Context:** Throughout this module, you’ve learned about tools to monitor network devices, including SNMP. In this project, you’ll install a network monitor called PRTG (Paessler Router Traffic Grapher) on a VM and see what information you can gather about your network with no further configuration. You’ll then enable SNMP on your Windows 10 host and see what additional information becomes available to you in the PRTG network monitor.

### Caution

Scanning a network you don’t own or don’t have permission to scan is illegal. Do not use PRTG on public Wi-Fi networks at all. Also don’t use PRTG on any network you don’t own unless you have written permission from the owner to do so.

Complete the following steps:

* + 1

Ensure your Windows 10 VM that you created in [Capstone Project 1-1](javascript://) or [1-2](javascript://) is configured with the bridged network mode. In Hyper-V, the VM should be connected to a vSwitch using the External network type. In VirtualBox, the VM should use the Bridged Adapter option. Start your Windows 10 VM.

* + 2

In the VM, go to [paessler.com](http://paessler.com/" \t "_blank). Download and install **PRTG**. You’ll need to enter an email address—you can choose any of your email addresses for this purpose.

* + 3

After installation, if PRTG doesn’t open automatically, open it from your new desktop shortcut. The user interface will open in a browser. The default login name and password are **prtgadmin**.

* + 4

You can skip the introduction and close all other information windows on the website. If you were setting this application up for use in a production network, what is the first task you would need to do to ensure its security?

* + 5

PRTG Auto-discovery automatically begins populating the monitoring system with devices on the network. Before you perform any other configurations, which devices were discovered automatically?

* + 6

In the top left corner, click the **Home** button. How many sensors are currently configured? How many trial days do you have left? How many sensors do you have available? Note that at the end of your trial, your PRTG will automatically revert to the free version, which supports only a few sensors, unless you pay for the full version.

* + 7

Click the menu icon and click **Devices** to return to the earlier screen. Click the **2 days** tab to see metrics being mapped on charts. These charts give visual output of monitored sensors and can be customized. Return to the **Overview** tab.

You can manually add devices and their various sensors. To add your physical host computer, which is a Windows 10 computer, you must first enable SNMP. Complete the following steps on your physical host computer:

* + 8

Open Settings and click **Apps**. Click **Optional features**. Click **Add a feature**. Select **Simple Network Management Protocol (SNMP)** and click **Install**. Click the back arrow to observe the installation progress.

* + 9

After installation is complete, close Settings. In the Windows search box, type **services** and click the **Services** app. Find **SNMP Service** in the list and double-click it. Make the following changes:

* + 1. Click the **Agent** tab and select all checkboxes in the Service group.
    2. Click the **Security** tab, click **Add**, and make sure **READ ONLY** is selected. Add a Community Name, such as **public**. Click **Add**.
    3. Under Accept SNMP packets from these hosts, click **Add**. Type your VM’s IP address and click **Add**. Click **OK** and then close the **Services** window.

You’re now ready to add your physical Windows machine as a monitored device in PRTG. Complete the following steps:

* + 10

Back in your VM’s PRTG user interface, under Windows > Clients, click **Add Device**.

* + 11

Give the device a name, such as **Windows10\_host**. Add the physical host’s IPv4 address. Choose a device icon, such as the Windows logo, and then click **OK**. The device is added to your list.

* + 12

Click **Run Auto-Discovery**. This process will take a few minutes. When the process is complete, **take a screenshot** of the sensors discovered for the Windows10\_host machine; submit this visual with your answers to this project’s questions.

* + 13

Which of these sensors are familiar to you? Which sensors are new to you?

* + 14

If you decide to use PRTG long-term, you might want to install it instead on a physical computer with ample hardware resources to process incoming data. What other devices on your network would you like to monitor using PRTG?

* + 15

If you decide not to continue using PRTG, be sure to disable SNMP on your host computer. Document the application installation in your wikidot website.

Go to pg.

[**help**](javascript://)

Application Opened