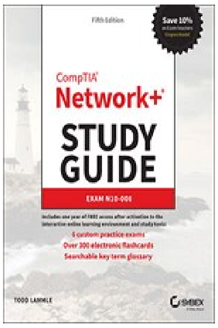


CompTIA Network+ Study Guide: Exam N10-008, 5th Edition

by Todd Lammle

Chapter 13: Using Statistics and Sensors to Ensure Network Availability

The following Comptia Network+ Exam Objectives are Covered in This Chapter

- **3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.**
    - Performance metrics/sensors
        - Device/chassis
            - Temperature
            - Central processing unit (CPU) usage
            - Memory
        - Network metrics
            - Bandwidth
            - Latency
            - Jitter
    - SNMP
        - Traps
        - Object identifiers (OIDs)
        - Management information bases (MIBs)
    - Network device logs
        - Log reviews
            - Traffic logs
            - Audit logs
            - Syslog
        - Logging levels/severity levels
    - Interface statistics/status
        - Link state (up/down)
        - Speed/duplex
        - Send/receive traffic
        - Cyclic redundancy checks (CRCs)
        - Protocol packet and byte counts
    - Interface errors or alerts
        - CRC errors
        - Giants
        - Runts
        - Encapsulation errors

  - Environmental factors and sensors
    - Temperature
    - Humidity
    - Electrical
    - Flooding
  - Baselines
  - NetFlow data
  - Uptime/downtime

All organizations detest downtime. It costs money and it damages their reputation. So they spend millions trying to solve the issue. One of the keys to stopping downtime is to be listening to what the devices may be telling you about their current state of health. Doing so forms a sort of early warning system that alerts you before a system goes down so there is time to address it. In this chapter you'll learn what sort of data you should be monitoring and some of the ways to do so.

Note To find Todd Lammle CompTIA videos and practice questions, please see `www.lammle.com`.

Performance Metrics/Sensors

Let's imagine you were just brought from the 1800s to the present in a time machine, and on your first trip in a car, you examine the dashboard. Speed, temperature, tire inflation, tachometer, what does all that stuff mean? It would be meaningless to you and useless for monitoring the state of the car's health. Likewise, you cannot monitor the health of a device or a network unless you understand the metrics. In these opening sections, you will learn what these are and how to use them.

Device/Chassis

There are certain basic items to monitor when dealing with physical computing devices, regardless of whether it's a computer, router, or switch. While not the only things to monitor, these items would be on the dashboard (if they had dashboards).

Temperature

Heat and computers do not mix well. Many computer systems require both temperature and humidity control for reliable service. The larger servers, communications equipment, and drive arrays generate considerable amounts of heat; this is especially true of mainframes and older minicomputers. An environmental system for this type of equipment is a significant expense beyond the actual computer system costs. Fortunately, newer systems operate in a wider temperature range. Most new systems are designed to operate in an office environment.

Overheating is also a big cause of reboots. When CPUs get overheated, a cycle of reboots can ensue. Make sure the fan is working on the heat sink and the system fan is also working. If required, vacuum the dust from around the vents.

Under normal conditions, the PC cools itself by pulling in air. That air is used to dissipate the heat created by the processor (and absorbed by the heat sink). When airflow is restricted by clogged ports, a bad fan, and so forth, heat can build up inside the unit and cause problems. Chip creep—the loosening of components—is one of the more common by—products of overheating and cooling cycles inside the system.

Since the air is being pulled into the machine, excessive heat can originate from outside the PC as well because of a hot working environment. The heat can be pulled in and cause the same problems. Take care to keep the ambient air within normal ranges (approximately 60°F to 90°F) and at a constant temperature.

Replacing slot covers is vital. Computers are designed to circulate air with slot covers in place or cards plugged into the ports. Leaving slots on the back of the computer open alters the air circulation and causes more dust to be pulled into the system.

Finally, make sure the fan is working; if it stops, that is a major cause of overheating.

Central Processing Unit (CPU) Usage

When monitoring the CPU, the specific counters you use depend on the server role. Consult the vendor's documentation for information on those counters and what they mean to the performance of the service or application. The following counters are commonly monitored:

- Processor\% Processor Time—The percentage of time the CPU spends executing a non-idle thread. This should not be over 85 percent on a sustained basis.
- Processor\% User Time—The percentage of time the CPU spends in user mode, which means it is doing work for an application. If this value is higher than the baseline you captured during normal operation, the service or application is dominating the CPU.
- Processor\% Interrupt Time—The percentage of time the CPU receives and services hardware interrupts during specific sample intervals. If this is over 15 percent, there could be a hardware issue.
- System\Processor Queue Length—The number of threads (which are smaller pieces of an overall operation) in the processor queue. If this value is over two times the number of CPUs, the server is not keeping up with the workload.

Memory

Different system roles place different demands on the memory, so there may be specific counters of interest you can learn by consulting the documentation provided by the vendor of the specific service. Some of the most common counters monitored by server administrators are listed here:

- Memory\% Committed Bytes in Use—The amount of virtual memory in use. If this is over 80 percent, you need more memory.
- Memory\Available Mbytes—The amount of physical memory, in megabytes, currently available. If this is less than 5 percent you need more memory.
- Memory\Free System Page Table Entries—The number of entries in the page table not currently in use by the system. If the number is less than 5000, there may well be a memory leak.
- Memory\Pool Non-Paged Bytes—The size, in bytes, of the non-paged pool, which contains objects that cannot be paged to the disk. If the value is greater than 175 MB, you may have a memory leak (an application is not releasing its allocated memory when it is done).
- Memory\Pool Paged Bytes—The size, in bytes, of the paged pool, which contains objects that *can* be paged to disk. (If this value is greater than 250 MB, there may be a memory leak.)
- Memory\Pages per Second—The rate at which pages are written to and read from the disk during paging. If the value is greater than 1000, as a result of excessive paging, there may be a memory leak.

Network Metrics

The health of a network’s operation can also be monitored so you can maintain its performance at peak efficiency. Just as you can avoid a problem issue with a workstation or server, so you can react to network conditions before they cause an issue by monitoring these items.

Bandwidth

In a perfect world, there would be unlimited bandwidth, but in reality, you're more likely to find Bigfoot. So, it's helpful to have some great strategies up your sleeve.

If you look at what computers are used for today, there's a huge difference between the files we transfer now versus those transferred even three to five years ago. Now we do things like watch movies online without them stalling, and we can send huge email attachments. Video teleconferencing is almost more common than Starbucks locations. The point is that the files we transfer today are really large compared to what we sent back and forth just a few years ago. And although bandwidth has increased to allow us to do what we do, there are still limitations that cause network performance to suffer miserably.

The following are metrics to follow for bandwidth on a system:

- Network Interface\Bytes Total/Sec—The percentage of bandwidth the NIC is capable of that is currently being used. If this value is more than 70 percent of the bandwidth of the interface, the interface is saturated or not keeping up.

- Network Interface\Output Queue Length—The number of packets in the output queue. If this value is over 2, the NIC is not keeping up with the workload.

Latency

Latency is the delay typically incurred in the processing of network data. A low-latency network connection is one that generally experiences short delay times, while a high-latency connection generally suffers from long delays. Many security solutions may negatively affect latency. For example, routers take a certain amount of time to process and forward any communication. Configuring additional rules on a router generally increases latency, thereby resulting in longer delays. An organization may decide not to deploy certain security solutions because of the negative effects they will have on network latency.

Auditing is a great example of a security solution that affects latency and performance.

When auditing is configured, it records certain actions as they occur. The recording of these actions may affect the latency and performance.

Measuring latency is typically done using a metric called round-trip time (RTT). This metric is calculated using a ping, a command-line tool that bounces a user request off a server and calculates how long it takes to return to the user device.

Jitter

Jitter occurs when the data flow in a connection is not consistent; that is, it increases and decreases in no discernable pattern. Jitter results from network congestion, timing drift, and route changes. Jitter is especially problematic in real-time communications like IP telephony and videoconferencing.

SNMP

Simple Network Management Protocol (SNMP), which uses ports 161 and 162, collects and manipulates valuable network information. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. When all is well, SNMP receives something called a baseline—a report delimiting the operational traits of a healthy network. This protocol can also stand as a watchdog over the network, quickly notifying managers of any sudden turn of events. The network watchdogs are called agents, and when aberrations occur, agents send an alert called a trap to the management station. In addition, SNMP can help simplify the process of setting up a network as well as the administration of your entire network.

SNMP has three versions, with version 1 being rarely, if ever, implemented today. Here's a summary of these three versions:

- SNMPv1—Supports plaintext authentication with community strings and uses only UDP.
- SNMPv2c—Supports plaintext authentication with MD5 or SHA with no encryption but provides GET BULK, which is a way to gather many types of information at once and minimize the number of GET requests. It offers a more detailed error message reporting method, but it's not more secure than v1. It uses UDP even though it can be configured to use TCP.
- SNMPv3—Supports strong authentication with MD5 or SHA, providing confidentiality (encryption) and data integrity of messages via DES or DES-256 encryption between agents and managers. GET BULK is a supported feature of SNMPv3, and this version also uses TCP. (Note: MD5 and DES are no longer considered secure.)

Traps

SNMP provides a message format for agents on a variety of devices to communicate with network management stations (NMSs)—for example, Cisco Prime or HP OpenView. These agents send messages to the NMS station, which then either reads or writes information in the database, stored on the NMS, that's called a management information base (MIB).

The NMS periodically queries or polls the SNMP agent on a device to gather and analyze statistics via GET messages. These messages can be sent to a console or alert you via email or SMS. The command `snmpwalk` uses the SNMP GET NEXT request to query a network for a tree of information.

End devices running SNMP agents will send an SNMP trap to the NMS if a problem occurs. This is demonstrated in Figure 13.1.

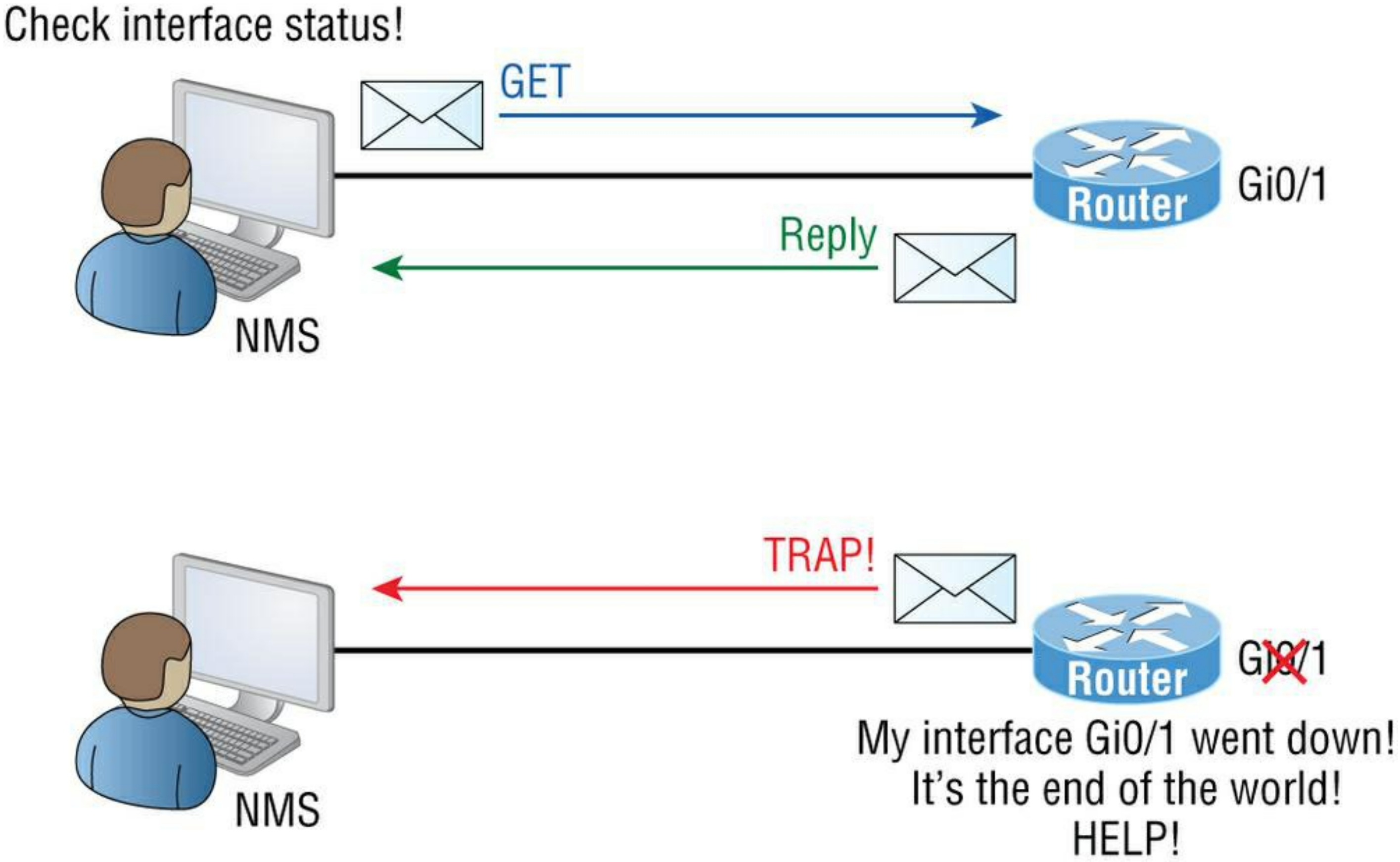


Figure 13.1: SNMP GET and TRAP messages

In addition to polling to obtain statistics, SNMP can be used for analyzing information and compiling the results in a report or even a graph. Thresholds can be used to trigger a notification process when exceeded. Graphing tools are used to monitor the CPU statistics of devices like a core router. The CPU should be monitored continuously, and the NMS can graph the statistics. Notification will be sent when any threshold you have set has been exceeded.

Object Identifiers (OIDs)

Object identifiers (OIDs) are an identifier mechanism standardized by the International Telecommunications Union (ITU) and ISO/IEC for naming any object, concept, or "thing" with a globally unambiguous persistent name.

Each physical component can possess a number of OIDs to describe the current state of a system. In Simple Network Management Protocol (SNMP), each node in a management information base (MIB) is identified by an OID.

Management Information Bases (MIBs)

OIDs are organized into a hierarchical structure called management information bases (MIBs). A managed object (sometimes called a MIB object or object) is one of any number of specific characteristics of a managed device. Managed objects are made up of one or more object instances, which are essentially variables. An OID uniquely identifies a managed object in the MIB hierarchy.

Network Device Logs

While SMTP should be in your toolbox when monitoring the network, there is also a wealth of information to be found in the logs on the network devices. You will now learn about the main log types and methods to manage the volume of data that exists in these logs. Baseline configurations are covered in detail in Chapter 14.

Log Reviews

High-quality documentation should include a baseline for network performance because you and your client need to know what "normal" looks like in order to detect problems before they develop into disasters. Don't forget to verify that the network conforms to all internal and external regulations and that you've developed and itemized solid management procedures and security policies for future network administrators to refer to and follow.

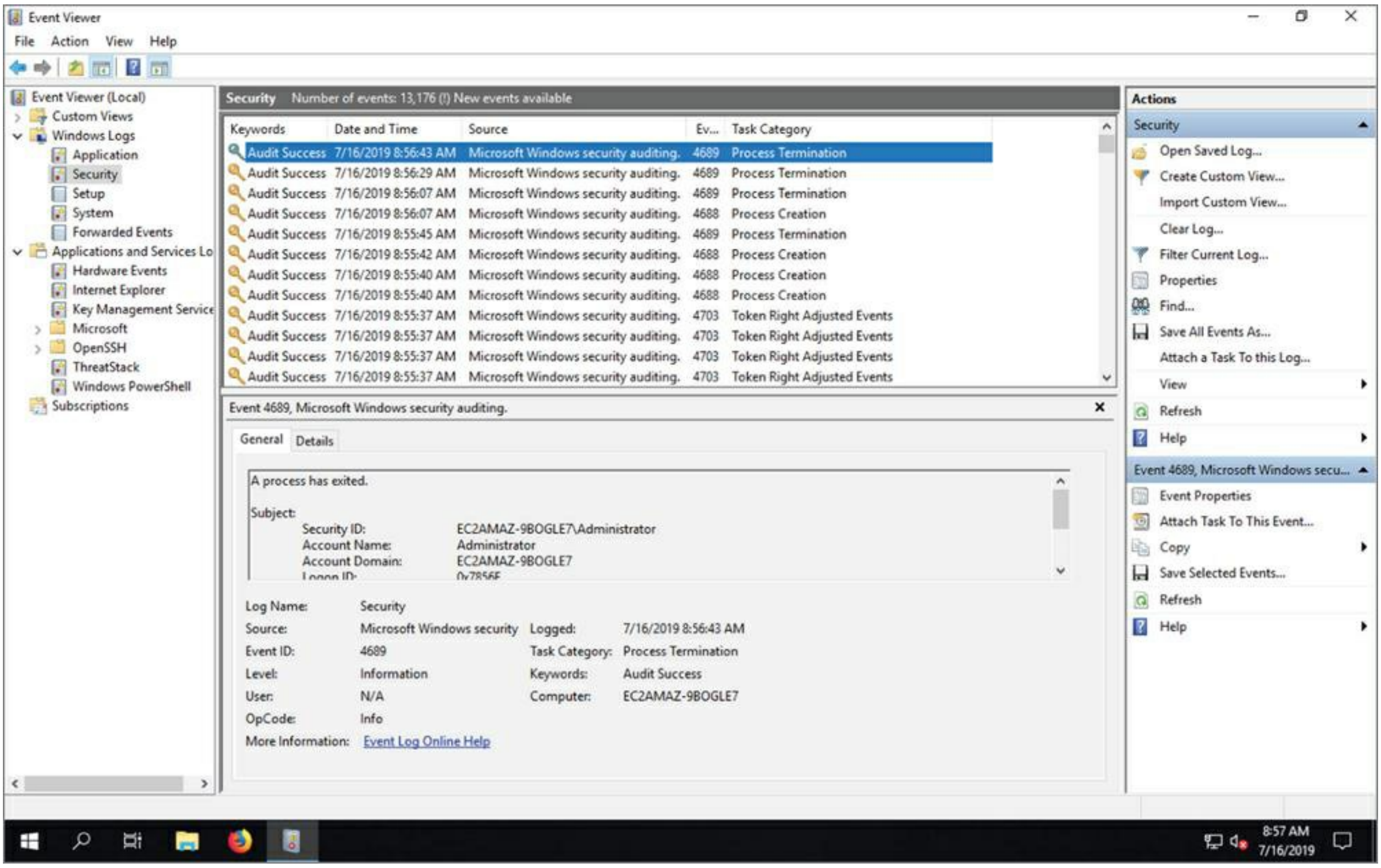
Traffic Logs

Some of your infrastructure devices will have logs that record the network traffic that has traversed the device. Examples include firewalls and intrusion detection and prevention devices. Those devices were covered in Chapter 5.

Many organizations choose to direct the traffic logs from these devices to a syslog server or to security information and event management (SIEM) systems (both covered later in this section).

Audit Logs

Audit logs record the activities of the users. Windows Server 2019 (and most other Windows operating systems) comes with a tool called Event Viewer that provides you with several logs containing vital information about events happening on your computer. Other server operating systems have similar logs, and many connectivity devices like routers and switches also have graphical logs that gather statistics on what's happening to them. These logs can go by various names, such as history logs, general logs, or server logs. Figure 13.2 shows an Event Viewer security log display from a Windows Server 2019 machine.



Security Number of events: 13,176 (!) New events available

Keywords	Date and Time	Source	Ev...	Task Category
Audit Success	7/16/2019 8:56:43 AM	Microsoft Windows security auditing.	4689	Process Termination
Audit Success	7/16/2019 8:56:29 AM	Microsoft Windows security auditing.	4689	Process Termination
Audit Success	7/16/2019 8:56:07 AM	Microsoft Windows security auditing.	4689	Process Termination
Audit Success	7/16/2019 8:56:07 AM	Microsoft Windows security auditing.	4688	Process Creation
Audit Success	7/16/2019 8:55:45 AM	Microsoft Windows security auditing.	4689	Process Termination
Audit Success	7/16/2019 8:55:42 AM	Microsoft Windows security auditing.	4688	Process Creation
Audit Success	7/16/2019 8:55:40 AM	Microsoft Windows security auditing.	4688	Process Creation
Audit Success	7/16/2019 8:55:40 AM	Microsoft Windows security auditing.	4688	Process Creation
Audit Success	7/16/2019 8:55:37 AM	Microsoft Windows security auditing.	4703	Token Right Adjusted Events
Audit Success	7/16/2019 8:55:37 AM	Microsoft Windows security auditing.	4703	Token Right Adjusted Events
Audit Success	7/16/2019 8:55:37 AM	Microsoft Windows security auditing.	4703	Token Right Adjusted Events
Audit Success	7/16/2019 8:55:37 AM	Microsoft Windows security auditing.	4703	Token Right Adjusted Events

Event 4689, Microsoft Windows security auditing.

General Details

```
A process has exited.

Subject:
        Security ID:        EC2AMAZ-9BOGLE7\Administrator
        Account Name:       Administrator
        Account Domain:     EC2AMAZ-9BOGLE7
        Logon ID:           0x7856F
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	7/16/2019 8:56:43 AM
Event ID:	4689	Task Category:	Process Termination
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	EC2AMAZ-9BOGLE7
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 13.2: Event Viewer security log

On Windows servers and client systems, a minimum of three separate logs hold different types of information:

- Application log: Contains events triggered by applications or programs determined by their programmers. Example applications include LiveUpdate, the Microsoft Office suite, and SQL and Exchange servers.
- Security log: Contains security events like valid or invalid logon attempts and potential security problems.
- System log: Contains events generated by Windows system components, including drivers and services that started or failed to start.

The basic "Big Three" can give us lots of juicy information about who's logging on, who's accessing the computer, and which services are running properly (or not). If you want to find out whether your Dynamic Host Configuration Protocol (DHCP) server started up its DHCP service properly, just check out its system log.

Syslog

Reading system messages from a switch's or router's internal buffer is the most popular and efficient method of seeing what's going on with your network at a particular time. But the best way is to log messages to a syslog server, which stores messages from you and can even time-stamp and sequence them for you, and it's easy to set up and configure! Figure 13.3 shows a syslog server and client in action.

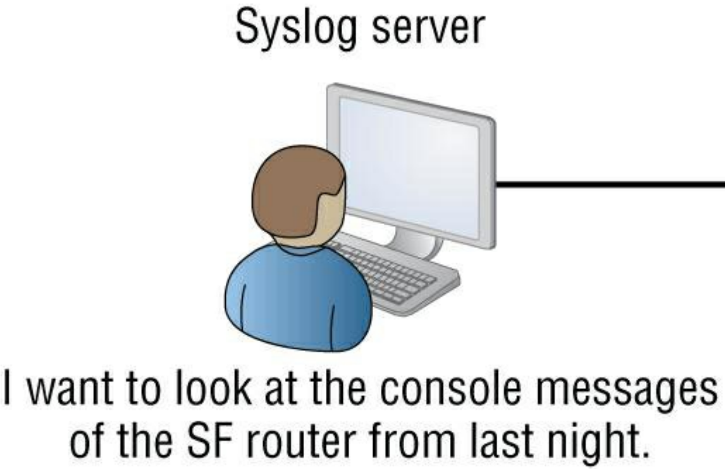

Syslog server
SF
I want to look at the console messages of the SF router from last night.

Figure 13.3: Syslog server and client

Syslog allows you to display, sort, and even search messages, all of which makes it a really great troubleshooting tool. The search feature is especially powerful because you can use keywords and even severity levels. Plus, the server can email administrators based on the severity level of the message.

Network devices can be configured to generate a syslog message and forward it to various destinations. These four examples are popular ways to gather messages from Cisco devices:

- Logging buffer (on by default)
- Console line (on by default)
- Terminal lines (using the terminal monitor command)
- Syslog server

All system messages and debug output generated by the IOS go out only through the console port by default and are also logged in buffers in RAM. And you also know that routers aren't exactly shy about sending messages! To send message to the VTY lines, use the `terminal monitor` command.

So, by default, we'd see something like this on our console line:

```
*Oct 21 17:33:50.565:%LINK-5-CHANGED:Interface FastEthernet0/0, changed state to administratively down
```

```
*Oct 21 17:33:51.565:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet0/0, changed state to down
```

And the router would send a general version of the message to the syslog server that would be formatted something like this:

```
Seq no:timestamp: %facility-severity- MNEMONIC:description
```

The system message format can be broken down in this way:

- **seq no**: This stamp logs messages with a sequence number, but not by default. If you want this output, you've got to configure it.
- **Timestamp**: Date and time of the message or event.
- **Facility**: The facility to which the message refers.
- **Severity**: A single-digit code from 0 to 7 that indicates the severity of the message.
- **MNEMONIC**: Text string that uniquely describes the message.

- **Description**: Text string containing detailed information about the event being reported.

SIEM

Security information and event management (SIEM) is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. You can get this as a software solution or a hardware appliance, and some businesses sell managed services using SIEM. Any one of these solutions provides log security data and can generate reports for compliance purposes.

The acronyms SEM, SIM, and SIEM are used interchangeably; however, SEM is typically used to describe the management that deals with real-time monitoring and correlation of events, notifications, and console views.

The term SIM is used to describe long-term storage, analysis, and reporting of log data.

Recently, vSIEM (voice security information and event management) was introduced to provide voice data visibility.

SIEM can collect useful data about the following items:

- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance
- Retention
- Forensic analysis

Notifications

SIEM systems not only assess the aggregated logs in real time, they generate alerts or notifications when an issue is discovered. This allows for continuous monitoring of the environment in a way not possible with other log centralization approaches such as syslog.

Logging Levels/Severity Levels

In most cases you need to know what to filter so you get the information you really need and nothing else. For example, with syslog you can filter by the security level. Severity levels, from the most severe level to the least severe, are explained in Table 13.1. Informational is the default and will result in all messages being sent to the buffers and console.

Table 13.1: Severity levels

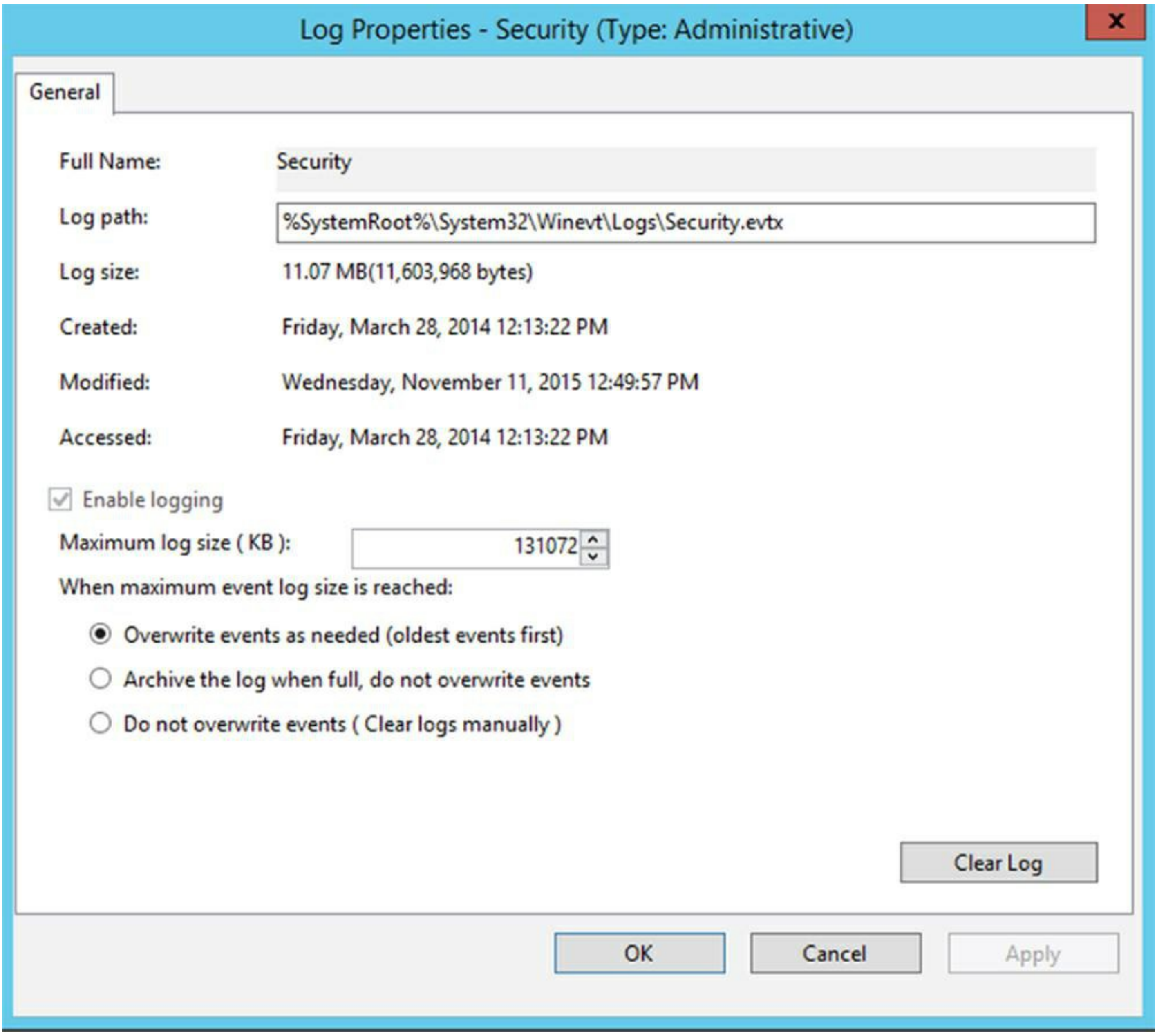
Severity Level	**Explanation**
Emergency (severity 0)	System is unusable.
Alert (severity 1)	Immediate action is needed.
Critical (severity 2)	Critical condition.
Error (severity 3)	Error condition.
Warning (severity 4)	Warning condition.
Notification (severity 5) Information (severity 6)	Normal but significant condition. Normal information message.
Debugging (severity 7)	Debugging message.

Understand that only emergency-level messages will be displayed if you've configured severity level 0. But if, for example, you opt for level 4 instead, levels 0 through 4 will be displayed, giving you emergency, alert, critical, error, and warning messages too. Level 7 is the highest-level security option and displays everything, but be warned that going with it could have a serious impact on the performance of your device. So always use debugging commands carefully with an eye on the messages you really need to meet your specific business requirements!

Servers also create useful logs that you may or may not be using. Even if you are using the logs (and you should!), you shouldn't allow them to slowly eat up all of the space. You can control the behavior of log files in Windows in several ways:

- You can limit the amount of space used for each log.
- You can determine the behavior when the log is full.
- You can choose to save a log for later viewing.

To set the maximum size for a log file, access the properties of the log in Event Viewer. In the Maximum Log Size option, use the spinner control to set the value you want and click OK as shown in Figure 13.4.



Log Properties - Security (Type: Administrative)

General

Full Name: Security

Log path: %SystemRoot%\System32\Winevt\Logs\Security.evtx

Log size: 11.07 MB(11,603,968 bytes)

Created: Friday, March 28, 2014 12:13:22 PM

Modified: Wednesday, November 11, 2015 12:49:57 PM

Accessed: Friday, March 28, 2014 12:13:22 PM

☑ Enable logging

Maximum log size (KB): 131072

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

Figure 13.4: Event log properties

This can also be done at the command line using the following command, inserting the name of the log file and the maximum size in bytes:

```
wevtutil sl <LogName> /ms:<MaxSizeInBytes>
```

To determine what happens when the log is full, access the same dialog box shown in Figure 13.4 and select one of the three options:

- Overwrite events as needed (oldest events first)
- Archive the log when full, do not overwrite events
- Do not overwrite events (Clear logs manually)

This can also be done at the command line using the following command:

```
wevtutil sl <LogName> /r:{true | false} /ab:{true | false}
```

The `r` parameter specifies whether to retain the log, and the `ab` parameter specifies whether to automatically back up the log.

Therefore, use the following combinations to achieve the desired result:

- Overwrite events as needed: `r = false, ab = false`
- Archive the log when full, do not overwrite events: `r = true, ab = true`
- Do not overwrite events. (Clear logs manually): `r = true, ab = false`

Interface Statistics/Status

You've got to be able to analyze interface statistics to find problems there if they exist, so let's pick out the important factors relevant to meeting that challenge effectively now.

Link State (Up/Down)

Typically, the most important metric on an interface is its link state. Is it up (functional) or down? While some tools can only tell you the link status, other devices and tools can tell you what the issue is. For example, Cisco routers and switches can tell you the link state along with an indication of the issue. On network interface cards (NICs), link lights can also tell the state of the connection. When the light is green, the connection is good, and when it's amber, there is an issue. Also, it will blink rapidly when data is traversing the NIC.

The first thing to check when there is a trouble ticket or our network management tools alert us of a link error is the link status. This is the first line in the output as shown. This would be the same on serial links as it is on Ethernet links.

```
Router#sh int fa0/0
FastEthernet0/0 is up, line protocol is up
```

The first `up` listed is carrier detect. If this shows `down`, then you have a physical layer problem locally and you need to get to that port immediately and check the cable and port. The second statistic, which is `protocol is up` in this example, is keepalives from the remote end. If you see `up/down`, then you know your local end is good but you're not getting a digital signal from the remote end.

The utilities known as ipconfig (in Windows) and ifconfig (in Unix/Linux/macOS) will display the current configuration of TCP/IP on a given workstation—including the current IP address, DNS configuration, Windows Internet Naming Service (WINS) configuration, and default gateway. In Chapter 23 you will learn more about using these tools.

Speed/Duplex

As you will learn in Chapter 11, in full-duplex communication, both devices can send and receive communication at the same time.

This means that the effective throughput is doubled and communication is much more efficient. Full-duplex is typical in most of today's switched networks.

You also learned that two interfaces on the end of a common link should be set to both the same duplex and the same speed to function correctly. Later in this chapter you will learn how to interpret the output of an interface to determine when a speed mismatch is indicated and when duplex mismatch is the issue.

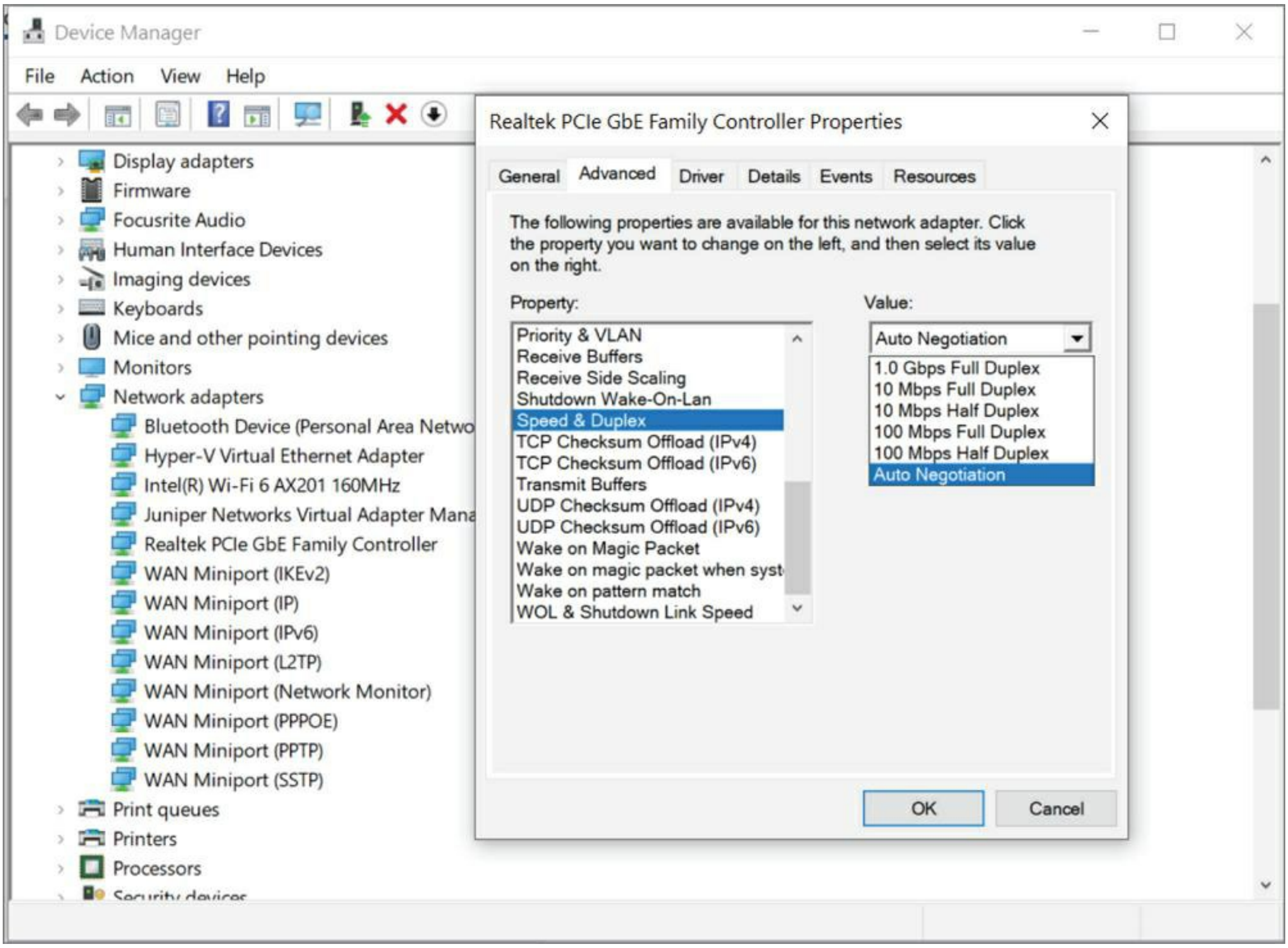
To determine the status on a router or switch, execute the following command:

```
R2#show run
Building configuration...
Current configuration : 1036 bytes
<output omitted>
```

```
version 12.4
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 10.2.2.2 255.255.255.0
duplex auto
speed auto
```

In this case both interfaces are set for auto-detect.

To verify speed and duplex settings on a Windows device use Device Manager as shown on the Advanced tab of the interface properties (Figure 13.5).



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

Priority & VLAN
Receive Buffers
Receive Side Scaling
Shutdown Wake-On-Lan
Speed & Duplex
TCP Checksum Offload (IPv4)
TCP Checksum Offload (IPv6)
Transmit Buffers
UDP Checksum Offload (IPv4)
UDP Checksum Offload (IPv6)
Wake on Magic Packet
Wake on magic packet when syst
Wake on pattern match
WOL & Shutdown Link Speed

Value:

Auto Negotiation

1.0 Gbps Full Duplex
10 Mbps Full Duplex
10 Mbps Half Duplex
100 Mbps Full Duplex
100 Mbps Half Duplex
Auto Negotiation

Figure 13.5: Speed and duplex

Send/Receive Traffic

Sometimes you need to check how well traffic is flowing into and out of a device, without regard to the type. The `show run` command will show this as well. In this case, the interface is down so there is no traffic flowing in either direction.

```
Router#sh int s0/0
Serial0/0 is up, line protocol is down
Hardware is PowerQUICC Serial
<output omitted>
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
```

To check the latest input and output statistics on a Windows interface, use the `netsh` command as shown below.

```
netsh interface ipv4>show ipstats
MIB-II IP Statistics
------------------------------------------------------
Forwarding is:                 Disabled
Default TTL:                        128
In Receives:                    5696170
In Header Errors:                   0
In Address Errors:                81691
Datagrams Forwarded:                0
In Unknown Protocol:                0
In Discarded:                      2972
In Delivered:                   2898662
Out Requests:                   1907432
Routing Discards:                   0
Out Discards:                      1965
Out No Routes:                      6
Reassembly Timeout:                 60
Reassembly Required:                0
Reassembled Ok:                     0
Reassembly Failures:                0
Fragments Ok:                       0
Fragments Failed:                   0
Fragments Created:                  0
netsh interface ipv4>
```

Cyclic Redundancy Checks (CRCs)

As you learned in Chapter 11, the function of Ethernet stations is to pass data frames between each other using a group of bits known as a MAC frame format. This provides error detection from a cyclic redundancy check (CRC). But remember—this is error detection, not error correction. Just know that when CRC errors occur, something has corrupted the received packet.

Protocol Packet and Byte Counts

It is also possible to determine the number of packets received from protocols and the number of bytes received. This is also contained in a section of the output of the `show run` command as shown here:

```
FastEthernet0/0 is up, line protocol is up
[output cut]
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1325 packets input, 157823 bytes
Received 1157 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
2294 packets output, 244630 bytes, 0 underruns
0 output errors, 0 collisions, 3 interface resets
347 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
4 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Interface Errors or Alerts

Let's take a look at an example to clarify how to use this information for interface monitoring to scrutinize errors, utilization, discards, packet drops, interface resets, and duplex issues:

```
Router#sh int fa0/0
FastEthernet0/0 is up, line protocol is up
[output cut]
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
WAN Troubleshooting 625
Last input 00:00:05, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
1325 packets input, 157823 bytes
Received 1157 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
2294 packets output, 244630 bytes, 0 underruns
0 output errors, 0 collisions, 3 interface resets
347 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
4 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

If you have a duplex mismatch, a telling sign is that the late collision counter will increment.

- **Input Queue Drops**: If the input queue drops counter increments, this tells you that more traffic is being delivered to the router than it can process. If this value is consistently high, try to determine exactly when these counters are increasing and how the events relate to CPU usage. Know that you'll see the ignored and throttle counters increment as well.
- **Output Queue Drops**: This counter indicates that packets were dropped due to interface congestion, leading to lost data and queuing delays. When this occurs, applications like VoIP will experience performance issues. If you observe this constantly incrementing, consider QoS as the culprit.
- **Input Errors**: Input errors often indicate high-level errors such as CRCs. This can point to cabling problems, hardware issues, or duplex mismatches.
- **Output Errors**: This issue equals the total number of frames that the port tried to transmit when an issue such as a collision occurred.

CRC Errors

CRC errors mean that packets have been damaged. This can be caused by a faulty port on the device or a bad Ethernet cable. Changing the cable or swapping the port is a relatively easy fix. Occasionally, they are generated on layer 2 by a duplex mismatch. It can also be the result of collisions or a station transmitting bad data.

Giants and Runts

Giants are packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant. They also have an incorrect frame check sequence (FCS). What causes this? In many cases, this is the result of a bad NIC.

Because collisions are a normal aspect of half-duplex communications, runt (packets that are discarded because they do not meet minimum packet size requirements) and giant frames are common by-products of those operations. A malfunctioning NIC can also place frames on the network that are either too short or longer than the maximum allowed length. CRC errors can result from using the wrong type of cable or from electrical interference. Using a cable that is too long can result in late collisions rather than runts and giants.

Encapsulation Errors

As you have learned in Chapter 2, encapsulation is the process of adding headers and trailers to data. When a host transmits data to another device over a network, the data is encapsulated, with protocol information at each layer of the OSI reference model. Each layer uses protocol data units (PDUs) to communicate and exchange information from the source to the destination.

A failed encapsulation error message indicates that the router has a layer 3 packet to forward and is lacking some element of the layer 2 header that it needs to be able to forward the packet toward the next hop. You may see this in the logs of a router as shown here:

```
Dec 26 18:18:38.081 PST: IP: s=0.0.0.0 (FastEthernet0/0), d=255.255.255.255, len 328, rcvd 2

Dec 26 18:18:38.081 PST: UDP src=68, dst=67

Dec 26 18:18:38.085 PST: IP: s=10.209.2.254 (local), d=10.69.96.30 (FastEthernet0/0), len 328, sending

Dec 26 18:18:38.085 PST: UDP src=67, dst=67

Dec 26 18:18:38.085 PST: IP: s=10.209.2.254 (local), d=10.69.96.30 (FastEthernet0/0), len 328, encapsulation failed
Dec 26 18:18:38.085 PST: UDP src=67, dst=67
```

Environmental Factors and Sensors

All of the equipment discussed in this chapter—switches, routers, hubs, and so on—require proper environmental conditions to operate correctly. These devices have the same needs as any computing device. The environmental concerns and methods to address these concerns are covered in the following sections.

Temperature

Like any device with a CPU, infrastructure devices such as routers, switches, and specialty appliances must have a cool area to operate. When temperatures rise, servers start rebooting and appliance CPUs start overworking as well. The room(s) where these devices are located should be provided with heavy-duty HVAC systems and ample ventilation.

It may even be advisable to dedicate a suite for this purpose and put the entire system on an uninterruptable power supply (UPS) with a backup generator in the case of a loss of power.

Humidity

The air around these systems can be neither too damp nor too dry; it must be "just right." If it is too dry, static electricity will build up in the air, making the situation ripe for damaging a system. It takes very little static electricity to fry some electrical components.

If it is too damp, connections start corroding and shorts begin to occur. A humidifying system should be used to maintain the level above 50 percent. The air conditioning should keep it within acceptable levels on the upper end.

Note **Check On It**

> Recommendations change, so techs should keep up with new ASHRAE recommendations: `https://www.ashrae.org/File%20Library/Technical%20Resources/ Standards%20and%20Guidelines/Standards%20Addenda/62. 1-2016/62_1_2016_ae_20190826.pdf.`

Environmental Monitors

Environmental monitors are designed to monitor the temperature, humidity, power, and air flow in an area or in a device.

High humidity cannot be tolerated because it leads to corrosion of electrical parts followed by shorts and other failures. Low humidity sounds good on paper, but with it comes static electricity buildup in the air, which can fry computer parts if it reaches them. Both of these conditions should be monitored.

A temperature and humidity monitor can save you and your precious devices from a total meltdown. By their very nature, networks often include lots of machines placed close together in one or several location(s)—like server rooms. Clearly, these devices, all humming along at once, generate quite a bit of heat.

Just like us, electronics need to "breathe," and they're also pretty sensitive to becoming overheated, which is why you'll often need a jacket in a chilly server room. It's also why we need to set up and use temperature-monitoring devices. Twenty years ago or so, these devices didn't send alerts or give off any kind of alarms; they were just little plastic boxes that had pieces of round graph paper to graph temperature. The paper was good for a month, and for that duration, it would just spin around in a circle. As the temperature moved up or down, the pen attached to the temperature coil moved in or out, leaving a circle line around the paper. All of this allowed you to manually monitor the temperature modulation in the server room over time. Although intended to "alert" you when and if there were climate changes, it usually did so after the fact, and therefore, too late.

Today, these temperature/humidity systems can provide multiple sensors feeding data to a single control point—nice. Now we can much more accurately track the temperature in our server rooms dynamically in real time. The central control point is usually equipped with HTTPS software that can send alerts and provide alarms via a browser should your server room experience a warming event.

Temperature/humidity monitors also come in a variety of flavors. They vary in size and cost and come in hardware and/or software varieties. The kind you need varies and is based on the size of the room and the number of devices in it. You can even get one that will just monitor your PC's internal heat.

What else will indicate you have a temperature problem in your server room? When you install new servers in a rack and you have network instability and other issues across all the servers in the rack but the power resources and bandwidth have been tested, this would be a good time to check your temperature monitor and verify that the servers are staying cool enough. Another red flag when it comes to environmental issues is a problem that occurs every day at the same time. This could be the time of day when the room temperature reaches the problematic stage.

Electrical

Power is the lifeline of the data center. One of your goals is to ensure that all systems have a constant clean source of power. In the following sections, we'll look at the proper use of uninterruptable power supplies (UPSs). We'll also talk about how to plan to ensure you have sufficient capacity to serve your devices. Finally, we'll explore the use of redundant power supplies and the use of multiple circuits to enhance availability.

UPS

All systems of any importance to the continued functioning of the enterprise should be connected to a UPS. You probably already know that UPSs have a battery attached that can provide power to your devices in the event of a power outage. You may also be aware that these systems are designed to only provide short-term power to the devices, that is, a length of time sufficient to allow someone to gracefully shut down the devices. We'll now dig a bit deeper and identify some of the features of these devices. We'll also go over some best practices with regard to ensuring your UPS solution provides the protection you intended.

Runtime vs. Capacity

Two important metrics that are related but are *not* the same when assessing a UPS are its runtime and its capacity. The runtime is the amount of time the UPS can provide power at a given power level. This means you can't really evaluate this metric without knowing the amount of load you will be placing on the UPS. Documentation that comes with the UPS should reveal to you the number of minutes expected at various power levels. So if you doubled the number of similar devices attached to the UPS, you should expect the time to be cut in half (actually, it will cut more than half in reality because the batteries discharge quicker at higher loads).

Capacity, on the other hand, is the maximum amount of power the UPS can supply at any moment in time. So, if the UPS has a capacity of 650 volt amperes (VA) and you attempt to pull 800 VA from the UPS, it will probably shut itself down. So both of the values must be considered. You need to know the total amount of power the devices may require (capacity) and, based on that figure, select a UPS that can provide that for the amount of time you will need to shut all the devices down.

One good thing to know is that some UPS vendors can supply expansion packs for existing units that increase their capacity and runtime. That would be a favorable feature to insist on to allow your system to grow.

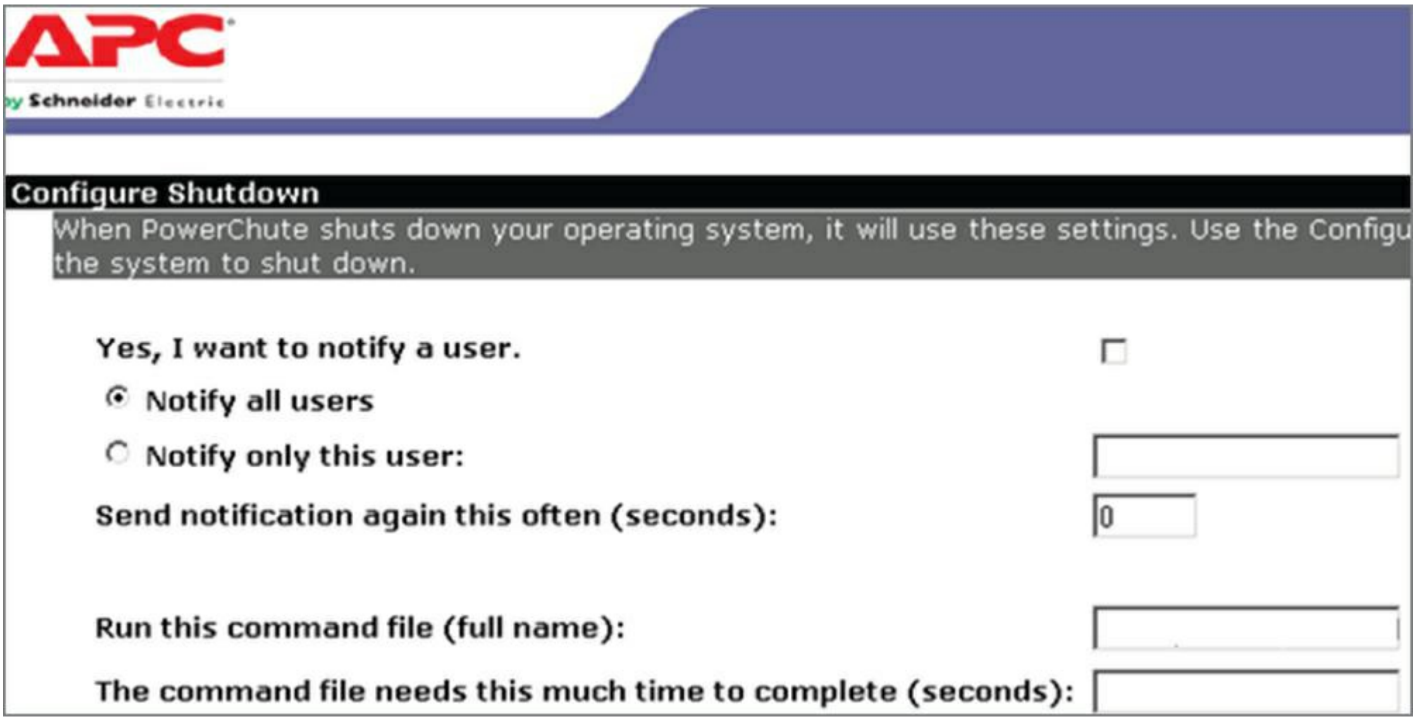
Automated Graceful Shutdown of Attached Devices

Many of today's enterprise-level UPS systems offer the ability to shut down a server to which it is attached when the power is lost. A proper shutdown is called a graceful shutdown. If all devices were thus equipped, it could reduce the amount of runtime required and eliminate the race to shut servers down.

There are several approaches that vendors have taken to this. In some cases, if you purchase a special network card for the UPS, a single UPS can provide the automatic shutdown to multiple servers. The agent on each server communicates with the network card in the UPS.

Another option is to use a dedicated UPS for each server and attach the server to the UPS using a serial or USB cable. The disadvantage of this approach is that it requires a UPS for each device and you will be faced with the cable length limitations of serial and USB cables.

In either case, using the software that comes with the UPS, you can also have scripts run prior to the shutdown, and you can configure the amount of time to wait for the shutdown so the script has time to execute, as shown in Figure 13.6. You can also set a notification of this event.



Configure Shutdown

When PowerChute shuts down your operating system, it will use these settings. Use the Configu
the system to shut down.

Yes, I want to notify a user. □

● Notify all users

○ Notify only this user:

Send notification again this often (seconds): 0

Run this command file (full name):

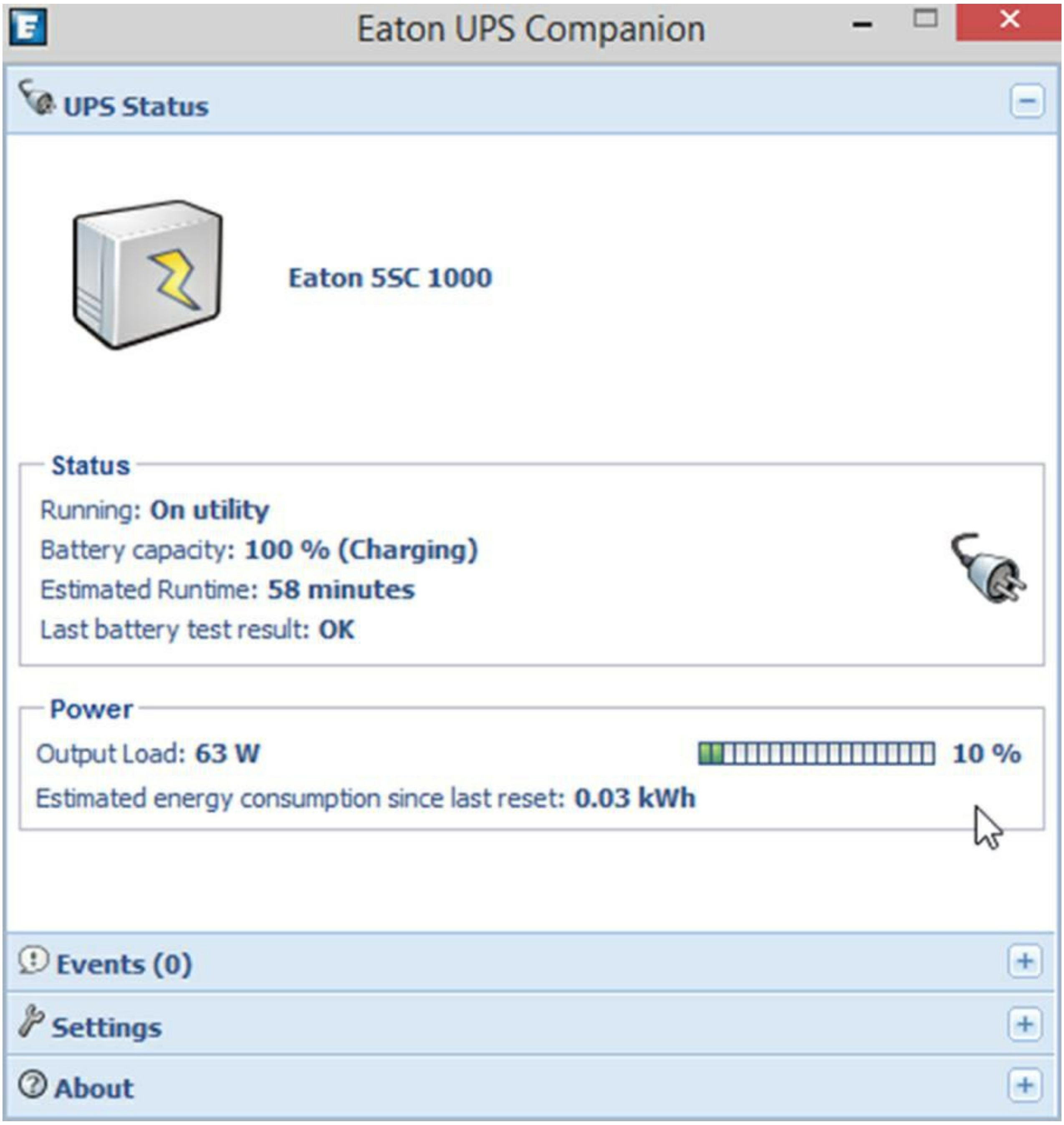
The command file needs this much time to complete (seconds):

Figure 13.6: Automatic shutdown

Periodic Testing of Batteries

Just as you would never wait until there is a loss of data to find out if the backup system is working, you should never wait until the power goes out to see the UPS does its job. Periodically, you should test the batteries to ensure they stand ready to provide the expected runtime.

While the simplest test would be to remove power and see what happens, if you have production servers connected when you do this, it could be a resume generating event (RGE). In most cases the software that came with the UPS will have the ability to report the current expected runtime based on the current state of the battery, as shown in Figure 13.7.



Eaton 5SC 1000

Status

Running: On utility

Battery capacity: 100 % (Charging)

Estimated Runtime: 58 minutes

Last battery test result: OK

Power

Output Load: 63 W 10 %

Estimated energy consumption since last reset: 0.03 kWh

Figure 13.7: Checking battery level

Even with this information, it is probably advisable to test the units from time to time with devices that you don't care about connected just to make sure the process of switching over to the battery succeeds and the correct runtime is provided.

Maximum Load

While the capacity of a UPS is rated in volts ampere (VA), that is not the same as maximum load. The capacity value assumes that all of the attached devices are pulling the maximum amount of power, which they rarely do. As a rule of thumb, if you multiply the VA times .6, you will get a rough estimate of the maximum load your UPS may undergo at any particular time. So a UPS that is rated for 650 VA cannot provide more than 390 watts. If either of these values are exceeded during operation, the UPS will fail to provide the power you need.

Bypass Procedures

Putting a UPS in bypass mode removes the UPS from between the device and the wall output conceptually, without disconnecting it. A static bypass is one in which the UPS, either by the administrator invoking the bypass manually or by an inverter failure in the UPS, switches the power path back to the main line and removes itself from the line.

A maintenance bypass is possible when the UPS is augmented with an external appliance called the bypass cabinet. This allows for enabling the bypass and then working with the UPS without concerns about the power being on (although it can be enabled while leaving the power to the UPS on). This concept is shown in Figure 13.8. Notice the two switches on the bypass cabinet that can be opened and shut to accomplish this power segregation.

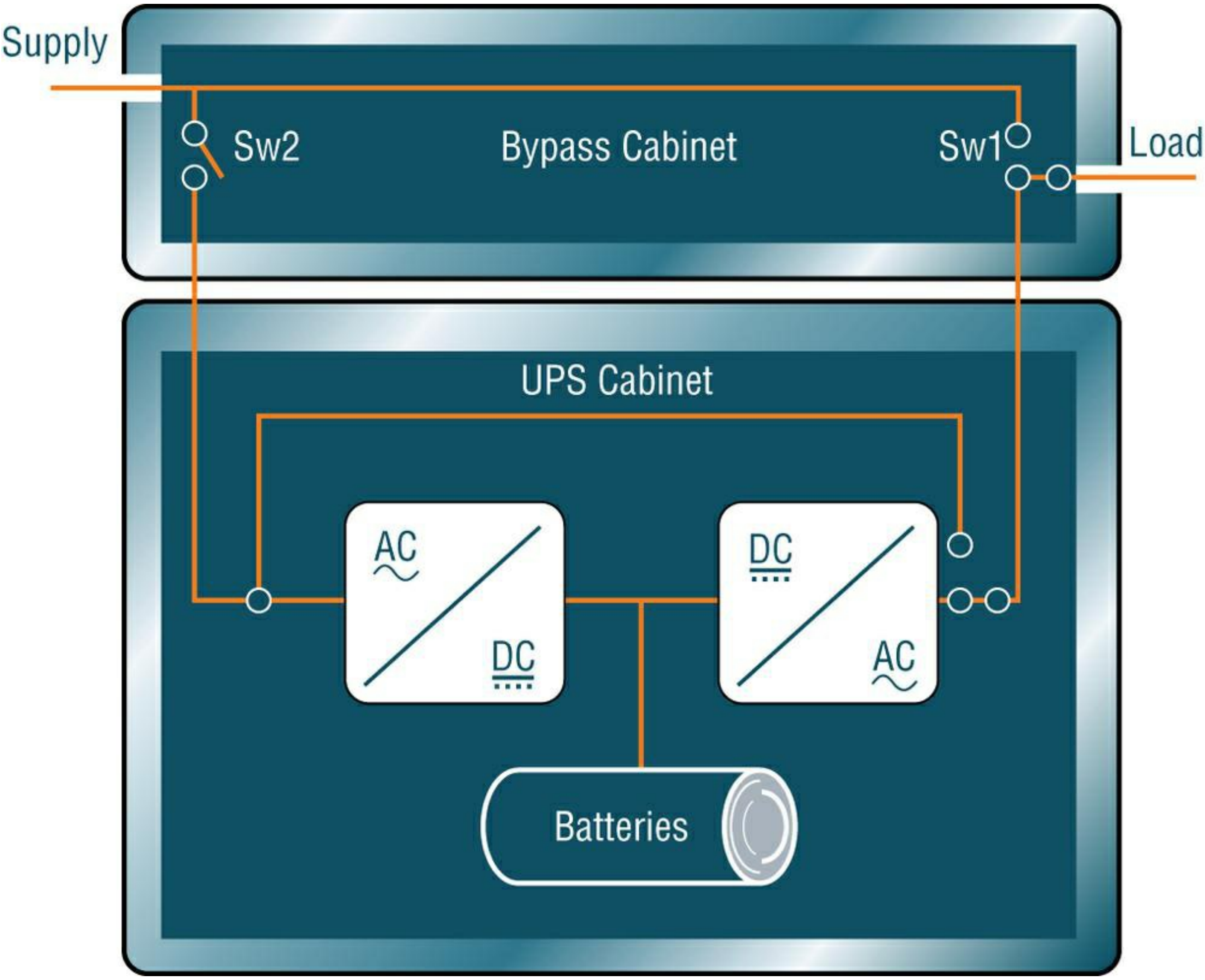


Figure 13.8: Maintenance bypass

Multiple Circuits

If you have a single power circuit and it fails, you will only be up as long as your batteries last or as long as the generator can run. Many data centers commission multiple power circuits to prevent this. A comparison of a center with a single circuit to one with two circuits is shown in Figure 13.9. In this particular case, the engineers have gone beyond circuit redundancy and also implemented main power panel, auto transfer switch, power panel, MBP, and UPS redundancy.

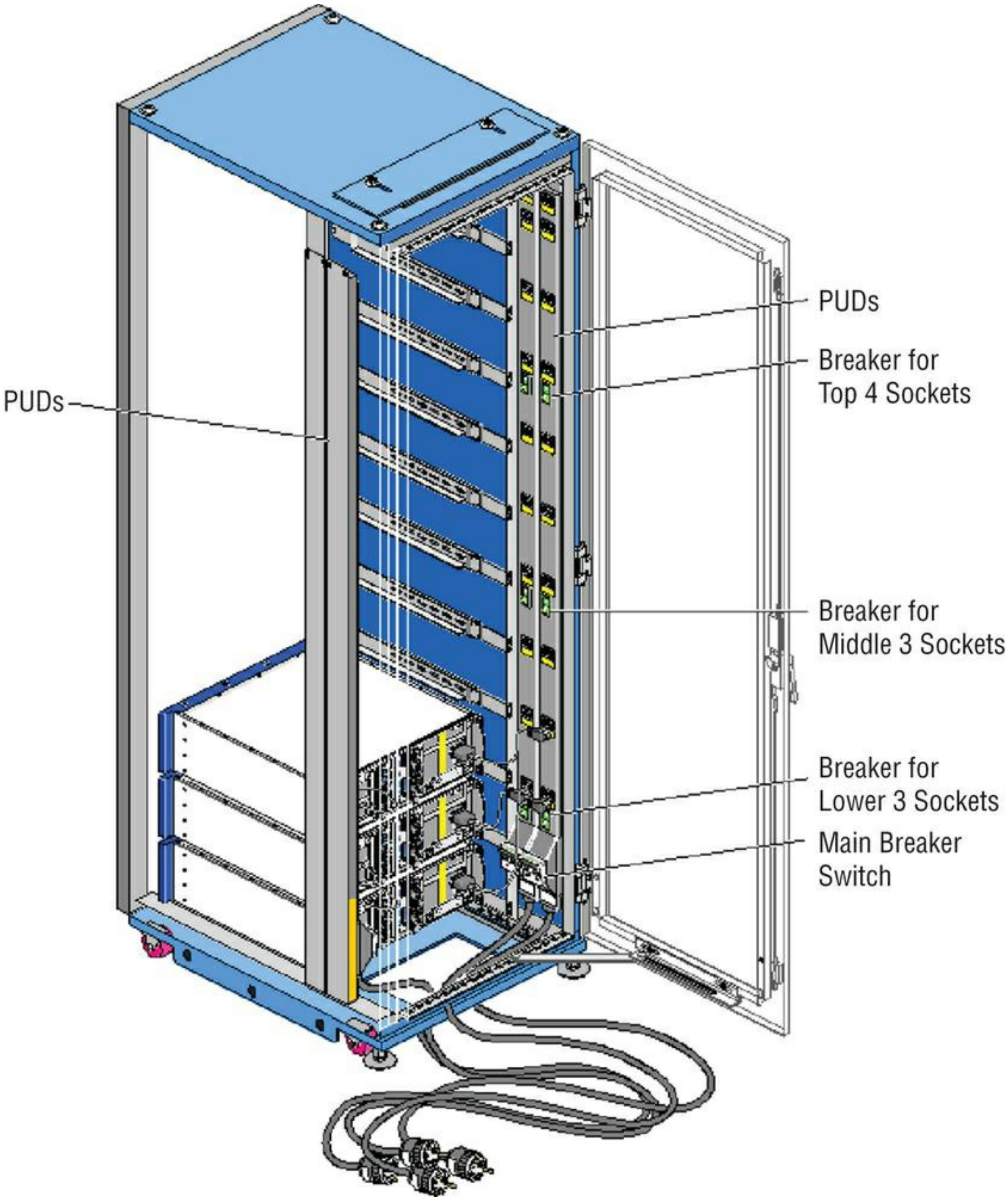

PUDs
PUDs
Breaker for Top 4 Sockets
Breaker for Middle 3 Sockets
Breaker for Lower 3 Sockets
Main Breaker Switch

Figure 13.9: Multiple circuits

Flooding

In some parts of the country, floods are a constant source of concern. For this reason, server rooms and data centers should be located on upper floors if possible. If not, raised floors should be deployed to help prevent the water from reaching the equipment, as shown in Figure 13.10.

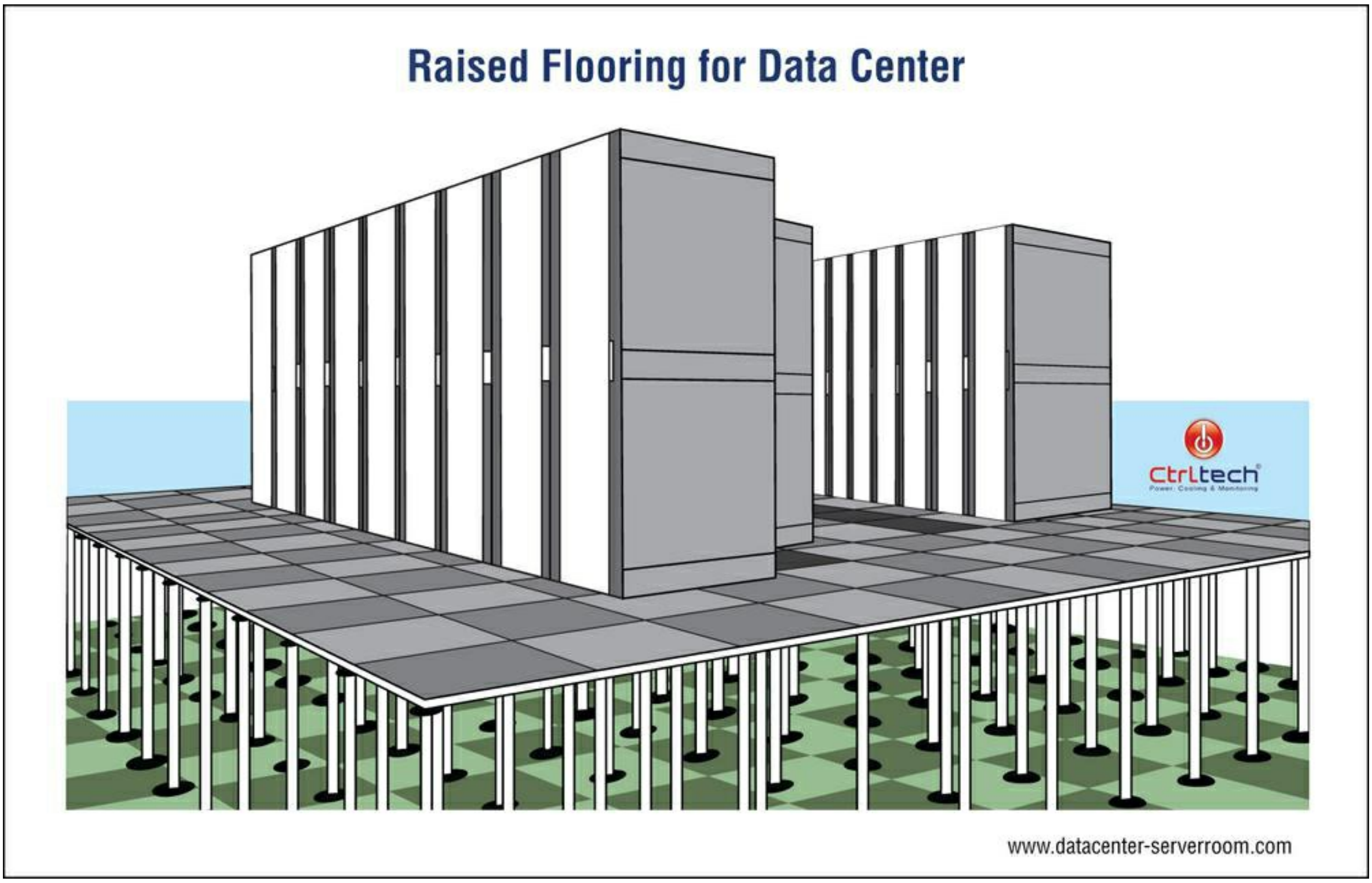

Raised Flooring for Data Center
Ctrltech
Power, Cooling & Monitoring
www.datacenter-serverroom.com

Figure 13.10: Flooding

Baselines

As you learned earlier in this chapter, a baseline can refer to the standard level of performance of a certain device or to the normal operating capacity for your whole network. Please review the coverage of baselines in the section "Network Device Logs" earlier in this chapter.

NetFlow Data

SNMP can be a powerful tool to help you manage and troubleshoot your network, but Cisco knew it would be very helpful for engineers to be able to track TCP/IP flows within the network as well.

That's why we have NetFlow as an application for collecting IP traffic information. Cisco compares NetFlow informational reports to receiving a phone bill with detailed call information to track calls, call frequency, and even calls that shouldn't have been made at all. A more current analogy would be the CIA and certain additional government "alphabet agencies" watching who has talked to whom, when, and for how long.

Cisco IOS NetFlow efficiently provides a key set of services for IP applications, including network traffic accounting for baselining, usage-based network billing for consumers of network services, network design and planning, general network security, and DoS and DDoS monitoring capabilities as well as general network monitoring.

NetFlow Overview and Flows

Understand that NetFlow is completely transparent to the users in the network, including all end stations and applications, and you don't need to run it on all your routers. Actually, you shouldn't; there's definitely overhead when using NetFlow because it requires memory for storing information in cache on the device. NetFlow enables near real-time visualization and analysis of recorded and aggregated flow data. You can specify the router, the aggregation scheme, and the time interval for when you want to view and then retrieve the relevant data and sort it into bar charts, pie charts, and so on. The components used with NetFlow include a router enabled with NetFlow and a NetFlow collector.

Service providers use NetFlow to do the following:

- Efficiently measuring who is using network service and for which purpose
- Accounting and charging back according to the resource utilizing level
- Using the measured information for more effective network planning so that resource allocation and deployment are well aligned with customer requirements
- Using the information to better structure and customize the set of available applications and services to meet user needs and customer service requirements

Moreover, there are different types of analyzers available to gather NetFlow statistics and analyze the traffic on your network by showing the following:

- Major users of the network, meaning top talkers, top listeners, top protocols, and so on
- Websites that are routinely visited, plus what's been downloaded
- Who's generating the most traffic and using excessive bandwidth
- Descriptions of bandwidth needs for an application as well as your available bandwidth

NetFlow is built around TCP/IP communication for statistical record-keeping using the concept of a flow. A flow is a unidirectional stream of packets between a source and destination host or system. With an understanding of TCP/IP, you can figure out that NetFlow is using socket information, meaning source and destination IP addresses and source and destination port numbers. But there are a few more fields that NetFlow uses. Here is a list of commonly used NetFlow flows:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol field
- Type of Service (ToS) marking
- Input logical interface

The operation of NetFlow is shown in Figure 13.11.

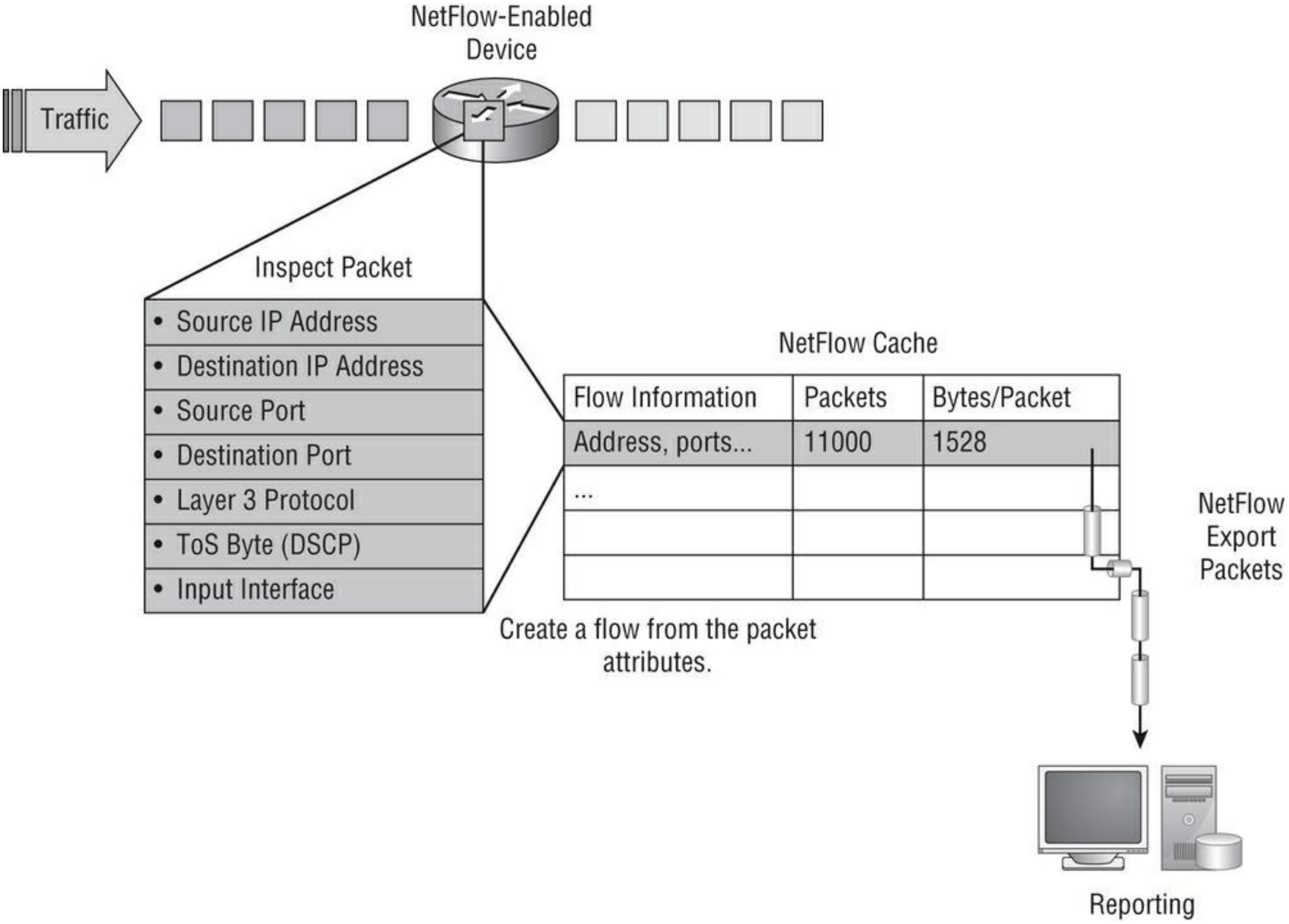


Figure 13.11: NetFlow

As mentioned, the first four listings are the sockets used between the source and destination host, which identify the application. The protocol field identifies the data the packet is carrying, and ToS in the IPv4 header describes how QoS rules are applied to the packets in the flow. If a packet has a key field that's different from another packet, it's considered to belong to another flow.

Uptime/Downtime

Uptime is the amount of time the system is up and accessible to your end users, so the more uptime you have the better. And depending on how critical the nature of your business is, you may need to provide four-nine or five-nine uptime on your network —that's a lot. Why is this a lot? Because you write out four nines as 99.99 percent, or better, you write out five nines as 99.999 percent. Now that is some serious uptime!

Summary

In this chapter you learned that one of the keys to stopping downtime is to be listening to what the devices may be telling you about their current state of health. You learned how to use performance metrics to monitor the health of a device's CPU, memory, and NIC.

You also were introduced to the use of SNMP and NetFlow to monitor both device health and network traffic from a central location, and you learned how to send log files either to a syslog server or to a SIEM system.

You learned about metrics that are used to monitor network interface performance and about settings that may impact that performance. Finally, we covered environmental factors and the sensors used to monitor these issues.

Exam Essentials

Understand how to use performance metrics. These include device metrics such as temperature, central processing unit (CPU) usage, and memory and network metrics, such as bandwidth, latency, and jitter.

Describe the operation of SNMP. Identify the role that traps, object identifiers (OIDs), and management information bases (MIBs) play in monitoring the network with SNMP.

Utilize network device logs in addressing system issues. Locate relevant information by reviewing logs such as traffic logs and audit logs. Describe the use of Syslog in centralizing these logs.

Interpret interface statistics and settings. Identify issues based on interface statistics and error messages. These include values for link state (up/down), speed/duplex, send/receive traffic, cyclic redundancy checks (CRCs), protocol packet and byte counts, CRC errors, giants, runts, and encapsulation errors. Finally, understand the importance of matching speed and duplex settings.

Identify critical environmental factors and sensors that monitor them. These factors include temperature, humidity, electrical issues, and flooding mitigation.

Written Lab

1. Complete the table by filling in the appropriate term for the description provided. You can find the answers in Appendix A.

Description	Term
The percentage of time the CPU spends executing a non-idle thread.	
The amount of physical memory in megabytes currently available.	
The percentage of bandwidth the NIC is capable of that is currently being used.	
The delay typically incurred in the processing of network data.	
Occurs when the data flow in a connection is not consistent; that is, it increases and decreases in no discernable pattern.	
Supports plaintext authentication with MD5 or SHA with no encryption but provides GET BULK.	
Sent by SNMP agents to the NMS if a problem occurs.	
Identifier mechanism standardized by the International Telecommunications Union (ITU) and ISO/IEC for naming any object, concept, or "thing" with a globally unambiguous persistent name.	
Hierarchical structure into which SNMP OIDs are organized.	
Refers to the standard level of performance of a certain device or to the normal operating capacity for your whole network.	
Centralizes and stores log messages and can even time-stamp and sequence them.	
Provides real-time analysis of security alerts generated by network hardware and applications.	
Errors that mean packets have been damaged.	

Answers

1.

Description	Term
The percentage of time the CPU spends executing a non-idle thread.	Processor\% Processor Time
The amount of physical memory in megabytes currently available.	Memory\Available Mbytes
The percentage of bandwidth the NIC is capable of that is currently being used.	Network Interface\Bytes Total/Sec
The delay typically incurred in the processing of network data.	Latency
Occurs when the data flow in a connection is not consistent; that is, it increases and decreases in no discernable pattern.	Jitter
Supports plaintext authentication with MD5 or SHA with no encryption but provides GET BULK.	SNMPv2
Sent by SNMP agents to the NMS if a problem occurs.	SNMP trap
Identifier mechanism standardized by the International Telecommunications Union (ITU) and ISO/IEC for naming any object, concept, or "thing" with a globally unambiguous persistent name.	Object identifiers (OIDs)
Hierarchical structure into which SNMP OIDs are organized.	Management information bases (MIBs)
Refers to the standard level of performance of a certain device or to the normal operating capacity for your whole network.	Baseline
Centralizes and stores log messages and can even time-stamp and sequence them.	Syslog
Provides real-time analysis of security alerts generated by network hardware and applications.	SIEM
Errors that mean packets have been damaged.	CRC errors

Review Questions

You can find the answers to the review questions in Appendix B.

1. Which of the following represents the percentage of uptime provided when four nines of fault tolerance are present?

A. 9.999 percent

B. 99.99 percent

C. 99.999 percent

D. 90.9 percent

2. Which of the following is *not* a commonly used NetFlow identifier?

A. Source IP

B. Destination port number

C. Layer 2 protocol field

D. Input logical interface

3. Which service can identify major users of the network, meaning top talkers?

A. Syslog

B. SIEM

C. NetFlow

D. SNMP

4. Which of the following refers to the standard level of performance of a certain device or to the normal operating capacity for your whole network?

A. Baseline

B. Target

C. Normal

D. Utilization

5. Raised floors are used to address which of the following?

A. Electrical issues

B. Flooding

C. Terrorism

D. Theft

6. Which of the following removes the UPS from between the device and the wall output conceptually, without disconnecting it?

A. Inline mode

B. Offline mode

C. Bypass mode

D. Maintenance mode

E. Pie a la mode (just seeing if you're paying attention)

7. Which UPS value assumes that all of the attached devices are pulling the maximum amount of power?

A. Maximum load

B. Volts ampere

C. UPC

D. Capacity

8. Which value is the amount of time a UPS can operate based on the current battery charge?

A. Runtime

B. Remaining life

C. Lifetime

D. Live time

9. The proper shutdown of a system is called which of the following?

A. Stateful

B. Graceful

C. Stateless

D. Quick

10. Which of the following is the maximum amount of power the UPS can supply at any moment in time?

A. Maximum load

B. Volts ampere

C. UPC

D. Capacity

11. What devices have a battery attached that can provide power to the devices in the event of a power outage?

A. NFC

B. VA

C. UPS

D. Syslog server

12. Which condition leads to shorts?

A. High temperature

B. High humidity

C. Low temperature

D. Low humidity

13. Damage from static electricity can occur when which of the following is present?

A. High temperature

B. High humidity

C. Low temperature

D. Low humidity

14. Which of the following causes system reboots?

A. High temperature

B. High humidity

C. Low temperature

D. Low humidity

15. A humidifying system should be used to maintain the level above what percent?

A. 30 percent

B. 40 percent

C. 50 percent

D. 60 percent

16. Which error message indicates that the router has a layer 3 packet to forward and is lacking some element of the layer 2 header that it needs to be able to forward the packet toward the next hop?

A. CRC error

B. Encapsulación error

C. Duplex mismatch

D. Speed mismatch

17. Any Ethernet packet that is greater than 1518 bytes is which of the following?

A. Giant

B. Runt

C. Outlier

D. Exception

18. Using a cable that is too long can result in which if the following?

A. Runt

B. Giant

C. Collisions

D. CRC errors

19. Which of the following means that packets have been damaged?

A. Runt

B. Giant

C. Collisions

D. CRC errors

20. If you have a duplex mismatch, which counter will increment?

A. Late collisions

B. Babbles

C. Watchdog

D. Unknown protocol drops

Answers

1. B. Four nines means 99.99 percent of the time.
2. C. Commonly used NetFlow flows include the following identifiers: source IP address, destination IP address, source port number, destination port number, layer 3 protocol field, Type of Service (ToS) marking, and input logical interface.
3. C. NetFlow statistics can analyze the traffic on your network by showing the major users of the network, meaning top talkers, top listeners, top protocols, and so on.
4. A. In networking, a baseline can refer to the standard level of performance of a certain device or to the normal operating capacity for your whole network.
5. B. When possible, server rooms and data centers should be located on upper floors. If not, raised floors should be deployed to help prevent water from reaching the equipment.
6. C. Putting a UPS in bypass mode removes the UPS from between the device and the wall output conceptually, without disconnecting it.
7. D. The capacity value assumes that all the attached devices are pulling the maximum amount of power, which they rarely do. As a rule of thumb, if you multiply the VA times .6, you will get a rough estimate of the maximum load your UPS may undergo at any particular time.
8. A. In most cases the software that came with the UPS will have the ability to report the current expected runtime based on the current state of the battery.
9. B. Many of today's enterprise-level UPS systems offer the ability to shut down a server to which they are attached when the power is lost. A proper shutdown is called a graceful shutdown.

10. D. Capacity is the maximum amount of power the UPS can supply at any moment in time. So if it has a capacity of 650 volt amperes (VA) and you attempt to pull 800 VA from the UPS, it will probably shut itself down.
11. C. Uninterruptable power supplies (UPSs) are designed to only provide short-term power to the devices, that is, a length of time sufficient to allow someone to gracefully shut down the devices.
12. B. High humidity cannot be tolerated because it leads to corrosion of electrical parts followed by shorts and other failures.
13. D. Low humidity sounds good on paper, but with it comes static electricity buildup in the air, which can fry computer parts if it reaches them.
14. A. Overheating causes system reboots and failures.
15. C. If it is too damp, connections start corroding and shorts begin to occur. A humidifying system should be used to maintain the level above 50 percent.
16. B. A failed encapsulation error message indicates that the router has a layer 3 packet to forward and is lacking some element of the layer 2 header that it needs to be able to forward the packet toward the next hop.
17. A. Giants are packets that are discarded because they exceed the maximum packet size of the medium.
18. C. Using a cable that is too long can result in late collisions rather than runts and giants.
19. D. CRC errors mean that packets have been damaged. This can be caused by a faulty port on the device or a bad Ethernet cable.
20. A. If you have a duplex mismatch, a telling sign is that the late collision counter will increment.