1 Networking Basics and Terminology

CERTIFICATION OBJECTIVES

When preparing for your Security+ certification exam, you will need a lot of knowledge of networking, networking devices, and protocols. This chapter reviews the basics of networking and ensures that you not only are familiar with the functions of devices such as switches and routers, but also understand the basics of the protocols that exist in the TCP/IP protocol suite.

This chapter is not designed to be a complete networking discussion, which would take an entire book. Although not required, it is recommended that you have a Network+ certification background before taking the Security+ certification exam.

CERTIFICATION OBJECTIVE 1.01

Understanding Network Devices and Cabling

Let's review the fundamentals of network environments by reviewing the concepts of networking devices and cabling. You may not get direct questions on these topics on the Security+ exam, but you are expected to understand the security implications of using the different devices and cable types.

Looking at Network Devices

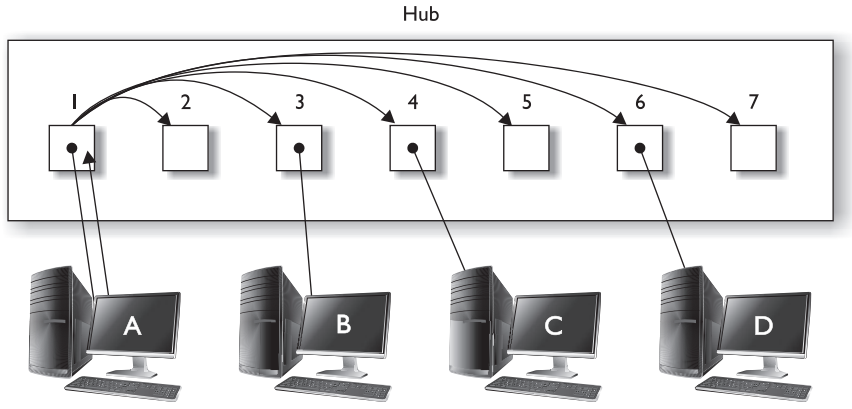
To perform any job function as a security professional, you need to be familiar with a number of different networking devices. For example, you may be requested to perform a security audit within an organization, which involves identifying the devices used in the company and making recommendations on more secure devices to use.

Hub

The network hub is an older networking device used to connect all the systems together in a network environment. The hub is a layer-1 device that simply receives a signal from one system and then sends the signal to all other ports on the hub. For example, looking at Figure 1-1, you can see that when Computer A sends data to Computer C, the data is received on port 1 of the hub and then sent to all other ports.

FIGURE 1-1

Looking at how a hub works



The drawback to the hub is that it uses up bandwidth by sending the data to every port on the hub. Why do that if the data has to be sent only to Computer C? The other drawback to a network hub is that it is a security issue if all systems on the network receive the data—although they ignore the data because it is not for them. Computers B and D would be able to view all traffic on the network because those stations receive a copy of the traffic as well. This is a huge security concern and is one reason you should not be using hubs on the network.

Switch

A network switch is similar to a network hub in that it is used to connect all systems together in a network environment, but the difference is that a switch is a layer-2 device that filters traffic by the layer-2 address. Remember from the Network+ exam that the layer-2 address is the MAC address, or hardware address, that is assigned to the network card by the manufacturer.

If you look at the earlier example of Computer A sending data to Computer C with a switch being used instead, you will notice that the switch receives the data from Computer A, but then filters the traffic by sending the data only to the port that the destination system resides on, in this case port 4 (see Figure 1-2).

The switch is able to filter the traffic because it stores the MAC addresses of each system connected to the switch, and what port that system is connected to, in the MAC address table. The MAC address table is a table stored in memory on the switch and is responsible for tracking what ports each system is connected to (see Figure 1-3).

FIGURE 1-2

Looking at how a switch filters traffic

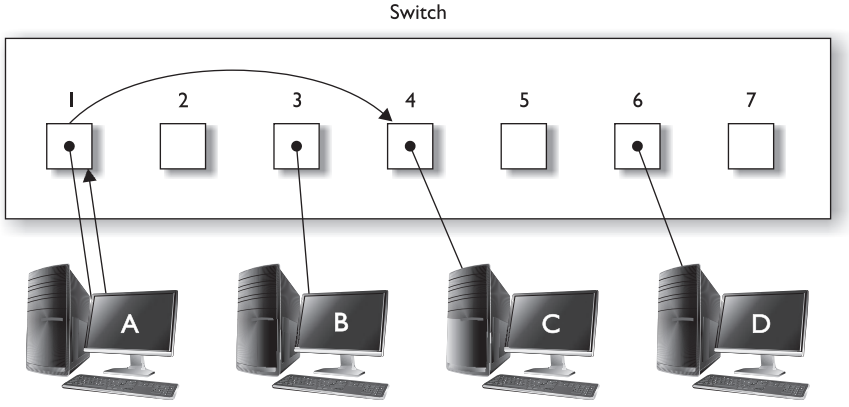
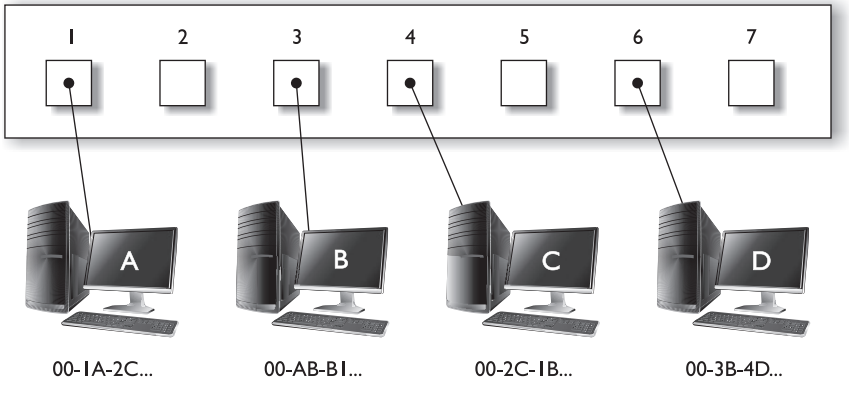


FIGURE 1-3

Looking at the MAC address table on a switch

MAC address table

MAC	Port
00-1A-2C...	1
00-AB-B1...	3
00-2C-1B...	4
00-3B-4D...	6



Besides filtering traffic by sending the data only to the port that the destination system resides on, most network switches provide the following benefits:

- **Filtering** As mentioned, a switch filters traffic, which prevents others from capturing and viewing potentially confidential information.
- **Port mirroring** Port mirroring, also known as port monitoring, is a feature of some switches that allows the administrator to copy traffic from other ports to a single destination port (known as a monitoring port). Because the switch filters traffic by default, the administrator cannot monitor network traffic. The switch vendors had to come up with a way to copy all the traffic to a single port so the administrator could connect their monitoring system to that port. The following commands are used to configure port 12 (known as an *interface*) on the switch to monitor traffic sent or received on ports 1 to 5:

```
HAL-SW1(config)#interface fastethernet 0/12
HAL-SW1(config-if)#port monitor fastethernet 0/1
HAL-SW1(config-if)#port monitor fastethernet 0/2
HAL-SW1(config-if)#port monitor fastethernet 0/3
HAL-SW1(config-if)#port monitor fastethernet 0/4
HAL-SW1(config-if)#port monitor fastethernet 0/5
```

- **Port security** Port security is a feature of a network switch that lets you configure a port for a specific MAC address. This allows you to control which systems can connect to the switch because the switch can temporarily disable the port until the correct system is plugged into the switch. The following commands are used to configure port 6 on the Halifax switch to accept only connections from a particular MAC address. In this example, the MAC address is *aaaa.bbbb.cccc*, which you would replace with an actual MAC address:

```
HAL-SW1(config)#interface f0/6
HAL-SW1(config-if)#switchport mode access
HAL-SW1(config-if)#switchport port-security
HAL-SW1(config-if)#switchport port-security mac-address aaaa.bbbb.cccc
HAL-SW1(config-if)#switchport port-security maximum 1
HAL-SW1(config-if)#switchport port-security violation shutdown
```

- **Disable ports** It is a security best practice that if you have ports on the switch that are not being used, you should disable them so that they cannot be used. The following commands are used to disable ports 7 through 12 on a Cisco switch with the **shutdown** command:

```
HAL-SW1(config)#interface range f0/7—12
HAL-SW1(config-if-range)#shutdown
```

exam Watch

The Security+ certification exam does not expect you to know the commands to configure port security or to disable a port on a Cisco switch, but it does expect you to understand features of the switch that offer security.

Collision Domains Another important feature of a switch is known as collision domains. A collision domain is a group of networked systems that share the same network segment and therefore can have their data collide with one another. For example, in a network hub, if one system sends data, any other system connected to the hub could send data at the same time, resulting in data collision. This is because the hub creates a "shared" network segment that all systems have access to. With a switch, each port on the switch creates a collision domain that is its own network segment. Because no other system is on the network segment, there won't be data collisions.

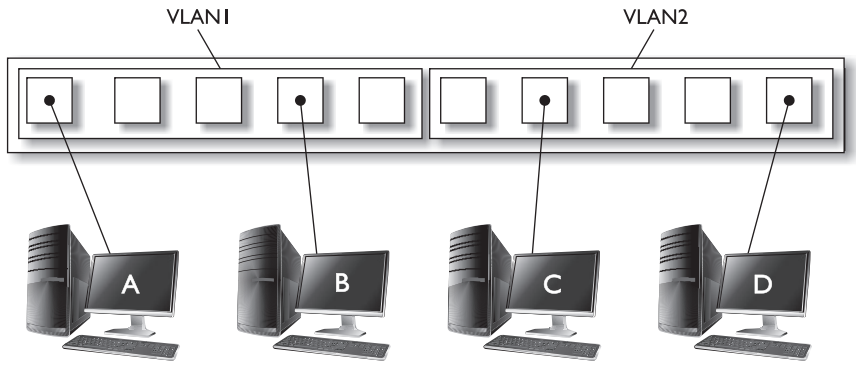
exam Watch

For the exam, remember that a switch offers great security because it filters traffic by sending the traffic only to the port that the destination system resides on. You should also be able to describe features such as port security, port mirroring, and the need to disable unused ports.

VLANs Most switches today support a feature known as Virtual LANs (VLANs). The purpose of a VLAN is to create multiple networks within the one network switch. One way to do this is by placing ports on the switch into groupings known as VLANs. When a system is connected to a port on the switch, it becomes a member of the VLAN that the port is associated with. The important point is that when a system is a member of one VLAN, it cannot communicate with systems in another VLAN. It's as if each VLAN has its own switch with no connection to another switch. Figure 1-4 displays a switch configured in two VLANs. In this example, Computer A can communicate only with Computer B because they are the only systems in VLAN1. Computer A and Computer B cannot communicate with Computer C and Computer D because communication across VLANs is not allowed without a router.

FIGURE 1-4

Looking at VLANs on a switch



The following code shows how to configure VLANs on a Cisco 2950 switch. This example shows two VLANs—PrivateLAN and WebServers:

```
HAL-SW1>enable
HAL-SW1#config term
HAL-SW1(config)#vlan 2
HAL-SW1(config-vlan)# name PrivateLAN
HAL-SW1(config-vlan)# exit
HAL-SW1(config)#vlan 3
HAL-SW1(config-vlan)# name WebServers
HAL-SW1(config-vlan)# exit
```

Once the VLANs have been created, you then place different ports in particular VLANs. For example, the following commands place ports 18 to 24 in the WebServers VLAN:

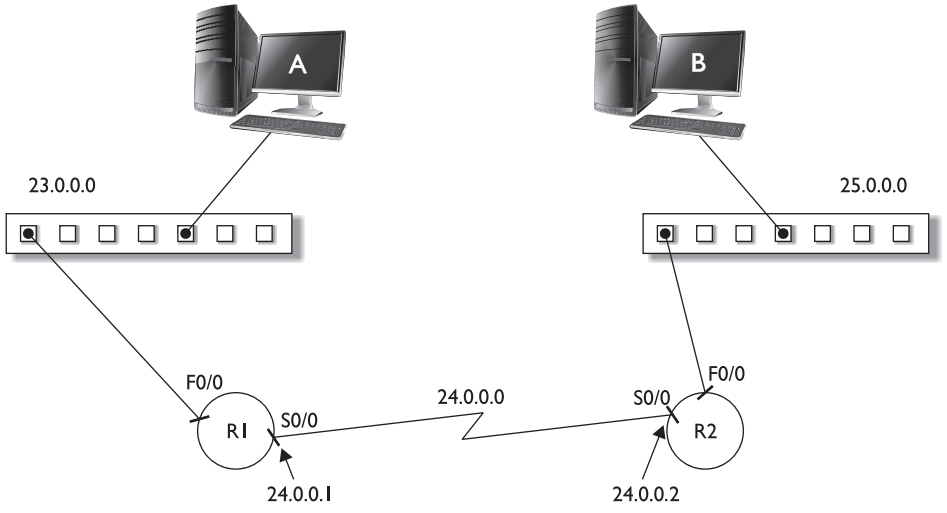
```
HAL-SW1(config-if-range)#interface range f0/18 – 24
HAL-SW1(config-if-range)#switchport access vlan 3
```

Router

A router is a layer-3 device of the OSI (open systems interconnection) model that is responsible for routing, or sending, data from one network to another network. The router uses a routing table that resides in its memory to determine the networks that the router knows how to send data to. Figure 1-5 displays a network topology and the routing table on a router. Notice in the figure that in order for router R1 to send data to the 25.0.0.0 network, it must send the data to the 24.0.0.2 address, as indicated by the routing table.

FIGURE 1-5

Routers use routing tables to deliver data.



Routing table

Network	Path
23.0.0.0	F0/0
24.0.0.0	S0/0
25.0.0.0	24.0.0.2

exam Watch

For the exam, remember that VLANs are a way to create communication boundaries on the network. By default, systems in one VLAN cannot communicate with systems in another VLAN.

The following code listing displays the routing table on a Cisco router by using the **show ip route** command. Notice in the listing that there are three routes; routes to the 23.0.0.0 and 24.0.0.0 network are known because the router is connected to those networks (notice the C on the left). Also, a static route (code *S* on the left) that the administrator added has been configured to pass data to the 24.0.0.2 system to reach the 25.0.0.0 network:

```
HAL-R1#show ip route
Codes: C—connected, S—static, I—IGRP, R—RIP, ...
 (Additional codes omitted for briefness)
```

```
Gateway of last resort is not set
S   25.0.0.0 [1/0] via 24.0.0.2
C   24.0.0.0/8 is directly connected, Serial0/0/0
C   23.0.0.0/8 is directly connected, FastEthernet0/1
```

Routers are great network devices because they define the boundary of the network by creating what is called a broadcast domain. A *broadcast domain* is a group of systems that can receive one another's broadcast messages. A broadcast message is a message that is destined for all systems—and the router is strategically placed on the network to keep those broadcast messages within your network because broadcast traffic does not pass through the router.

Load Balancer

A *load balancer* is a device that is designed to split the load between components such as servers or routers. Load balancing is the concept of trying to improve performance. Instead of having a single server or device handle all the work, you have multiple servers or devices that the workload is divided between. This increases overall performance because you have more systems working at the same time to handle all the incoming requests.

Firewalls and Proxy Servers

You will learn more about firewalls and proxy servers in Chapter 8, but here I wanted to give a quick description of the purpose of a firewall and a proxy server to introduce them as network devices.

exam Watch

For the Security+ exam, remember that a proxy server makes the request for the Internet resource on behalf of the user, and commonly the company will filter and log what web sites users have visited.

A firewall is a network device that controls what traffic is allowed to enter or leave the network. The firewall filters traffic based on rules you place on the firewall indicating what traffic is allowed or not allowed to enter or leave the network. You typically start with a deny-all rule that states all traffic is denied, unless you specify otherwise by building a rule for a specific type of traffic.

A proxy server is a type of firewall, but it is typically associated with being able to control outbound communication by limiting what web sites an employee can visit. Proxy servers are a little different from firewalls in the sense that the employee will typically first authenticate to the proxy server (via a username and password), and based on that username, the proxy administrator will decide whether the employee is allowed to use the Internet and what web sites they can visit. Proxy servers also

perform a high level of logging so that the administrator can see what sites are visited each day.

Understanding Network Cabling

Cabling is the transmission medium for data sent between hosts on the LAN. Systems on the LAN can be connected together using a variety of cable types such as unshielded twisted-pair, coax, or fiber. Each cable type has its own advantages and disadvantages, which you will examine in this section.

The three primary types of cable media that can be used to connect systems to a network are coaxial cable, twisted-pair cable, and fiber-optic cable. Transmission rates supported on each of these physical media are measured in millions of bits per second, or megabits per second (Mbps).

Coaxial Cable

Coaxial, or coax, cable looks like the cable used to bring the cable TV signal to a television. One strand (a solid-core copper wire) runs down the middle of the cable. Around that strand is a layer of insulation, and covering that insulation is braided wire and metal foil, which shields against electromagnetic interference. A final layer of insulation covers the braided wire. Because of the layers of insulation, coaxial cable is more resistant to outside interference than other cabling such as unshielded twisted-pair (UTP) cable. Figure 1-6 shows a coaxial cable with the copper core and the layers of insulation.

The two types of coax cabling are thinnet and thicknet. The two differ in thickness and maximum cable distance that the signal can travel. Let's take a look:

- **Thinnet** This refers to RG-58 cabling, which is a flexible coaxial cable about ¼-inch thick. Thinnet is used for short-distance communication and is flexible enough to facilitate maneuvering between workstations. Thinnet connects directly to a workstation's network adapter card by using a British naval connector (BNC) and uses the network adapter card's internal

FIGURE 1-6

A coaxial cable

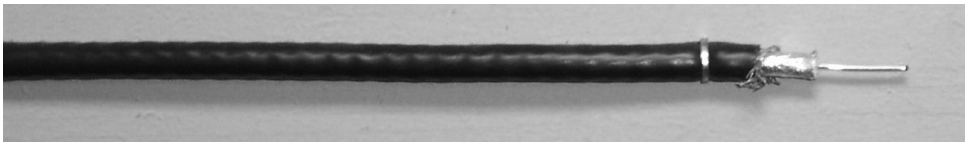
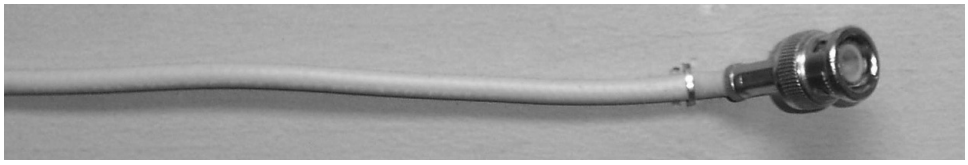


FIGURE 1-7

Thinnet coaxial cable with a BNC connector



transceiver. The maximum length of thinnet is 185 meters. Figure 1-7 displays thinnet coaxial cabling and the BNC connector on the end.

- **Thicknet** This coaxial cable, also known as RG-8, gets its name by being a thicker cable than thinnet. Thicknet cable is about ½-inch thick and can support data transfer over longer distances than thinnet. Thicknet has a maximum cable length of 500 meters and usually is used as a backbone to connect several smaller thinnet-based networks. Due to its ½-inch thickness, this cable is harder to work with than thinnet cable. A transceiver often is connected directly to the thicknet cable by using a connector known as a vampire tap. Connection from the transceiver to the network adapter card is made using a drop cable to connect to the adapter unit interface (AUI) port connector. Table 1-1 summarizes the characteristics of thicknet and thinnet.

Twisted-Pair Cable

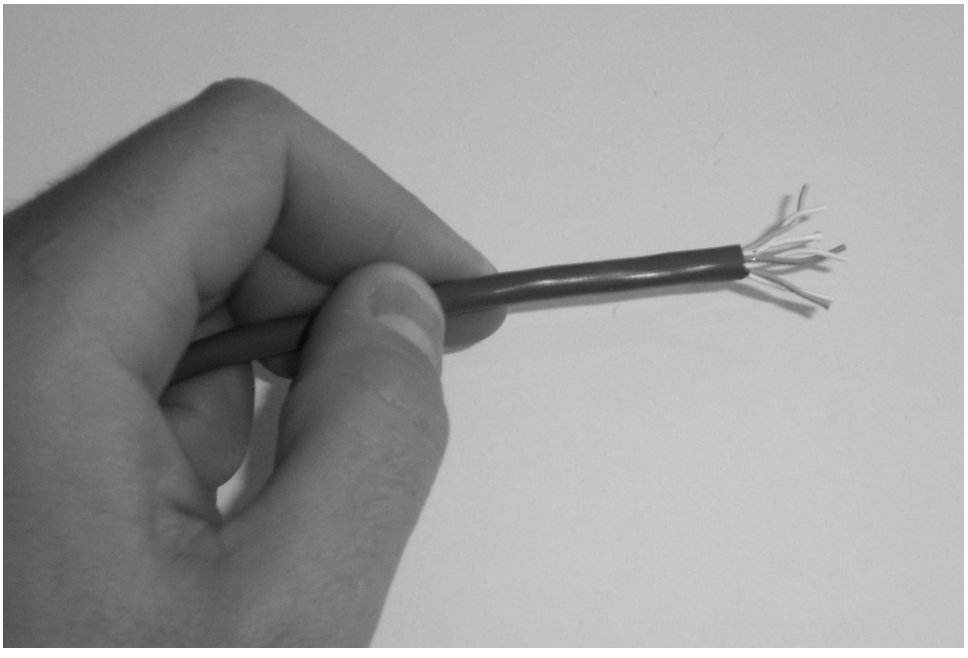
Coaxial cable is not as popular today as it was years ago. Today, twisted-pair cabling dominates the popularity contest. Twisted-pair cabling gets its name from having four pairs of wires that are twisted to help reduce crosstalk or interference from outside electrical devices. Crosstalk is interference from adjacent wires. Figure 1-8 shows a twisted-pair cable. Just as there are two forms of coaxial cable, there are two forms of twisted-pair cabling—unshielded twisted-pair (UTP) and shielded twisted-pair (STP).

TABLE 1-1 Thinnet Versus Thicknet Cabling

Coax Type	Cable Grade	Thickness	Maximum Distance	Transfer Rate	Connector Used to Connect NIC to Cable Type
Thinnet	RG-58	0.25 in	185 m	10 Mbps	BNC
Thicknet	RG-8	0.5 in	500 m	10 Mbps	AUI

FIGURE 1-8

Unshielded twisted-pair (UTP) cable



Unshielded Twisted-Pair (UTP) Cable UTP cables are familiar to you if you have worked with telephone cable. The typical twisted-pair cable for network use contains four pairs of wires. Each member of the pair of wires contained in the cable is twisted around the other. The twists in the wires help shield against electromagnetic interference. The maximum distance of UTP is 100 meters.

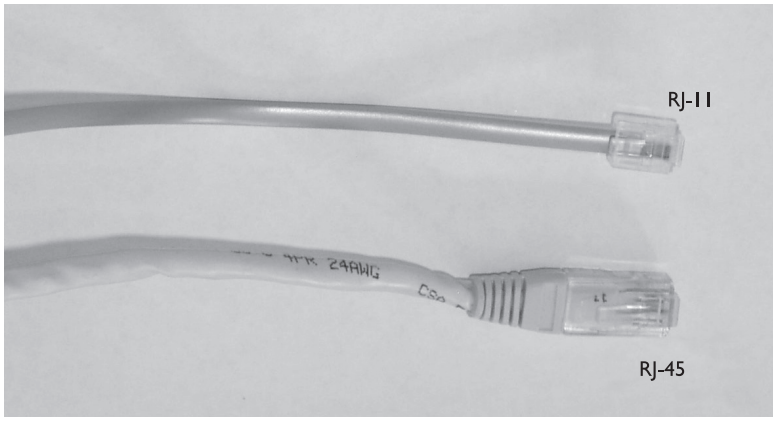
UTP cable uses small plastic connectors designated as registered jack 45, most often referred to as RJ-45. RJ-45 is similar to the phone connectors, except that instead of four wires, as found in the home system, the network RJ-45 connector contains eight contacts, one for each wire in a UTP cable.

It can be easy to confuse the RJ-45 connector with the RJ-11 connector. The RJ-11 connector is a telephone connector and is shown in Figure 1-9 (the cable on the top). An RJ-11 connector has four contacts; hence, there are four wires found in the telephone cable. With RJ-45 and RJ-11, you will need a special crimping tool when creating the cables to make contact between the pins in the connector and the wires inside the cable.

UTP cable is easier to install than coaxial because you can pull it around corners more easily due to its flexibility and small size. Twisted-pair cable is more susceptible

FIGURE 1-9

An RJ-11 connector (top) and an RJ-45 connector (bottom)



to interference than coaxial, however, and should not be used in environments containing large electrical devices.

UTP cabling has different flavors known as grades or categories. Each category of UTP cabling was designed for a specific type of communication or transfer rate. Table 1-2 summarizes the different UTP categories—the most popular today being CAT 5e, which can reach transfer rates of over 1,000 Mbps, or 1 gigabit per second (Gbps).

When working on a network that uses UTP cabling, you will come across different types of cable for different purposes. For example, sometimes you will use a straight-through cable or a crossover cable.

Straight-Through Cables CAT 5 UTP cabling usually uses only four wires when sending and receiving information on the network. The four wires of the eight

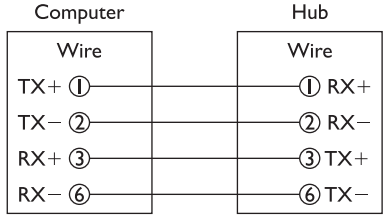
TABLE 1-2

Different UTP Category Cabling

UTP Category	Purpose	Transfer Rate
Category 1	Voice only	
Category 2	Data	4 Mbps
Category 3	Data	10 Mbps
Category 4	Data	16 Mbps
Category 5	Data	100 Mbps
Category 5e	Data	1 Gbps (1,000 Mbps)
Category 6	Data	10 Gbps

FIGURE 1-10

Pinout diagram for a straight-through cable



that are used are wires 1, 2, 3, and 6. Figure 1-10 shows the meaning of the pins on a computer and the pins on a hub (or switch), which is what you typically will be connecting the computers to. When you configure the wire for the same pin at either end of the cable, this is known as a straight-through cable.

You will notice in the figure that wires 1 and 2 are used to transmit data (TX) from the computer, while wires 3 and 6 are used to receive information (RX) on the computer. You will also notice that the transmit pin on the computer is connected to the receive pin (RX) on the hub via wires 1 and 2. This is important because you want to make sure that data sent from the computer is received at the network hub. You also want to make sure that data sent from the hub is received at the computer, so you will notice that the transmit pins (TX) on the hub are connected to the receive pins (RX) on the computer through wires 3 and 6. This will allow the computer to receive information from the hub.

The last thing to note about Figure 1-10 is that pin 1 on the computer is connected to pin 1 on the hub by the same wire, thus the term *straight-through*. You will notice that all pins are matched straight through to the other side in Figure 1-10.

Crossover Cables At some point, you may need to connect two computer systems directly together without the use of a switch (or hub) from network card to network card. Or you may find you need to connect one switch to another switch. In any scenario where you are connecting similar devices together, you would be unable to use a straight-through cable because the transmit pin on one end would be connected to the transmit pin on the other end, as shown in Figure 1-11. How could a

FIGURE 1-11

Using a straight-through cable to connect two computers will not work.

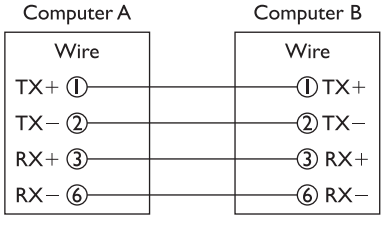
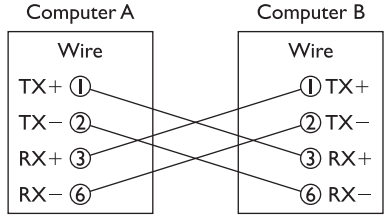


FIGURE 1-12

Pinout diagram of a crossover cable



computer pick up the data not sent to the receive pins? Since this will not work, you will need to change the wiring of the cable to what is known as a crossover cable.

To connect two systems directly together without the use of a switch, you will need to create a crossover cable by switching wires 1 and 2 with wires 3 and 6 at one end of the cable, as shown in Figure 1-12. You will notice that the transmit pins on Computer A are connected to the receive pins on Computer B, thus allowing Computer A to send data to Computer B. The same applies for Computer B to send to Computer A—pins 1 and 2 on Computer B are wired to pins 3 and 6 on Computer A so that Computer A can receive data from Computer B.

on the job

Most network administrators will use certain color cables (such as yellow) to represent crossover cables and use a different color cable to represent straight-through cables to prevent confusing the two types of cabling.

Shielded Twisted-Pair (STP) Cable STP cable is very similar to UTP cabling, but it differs from UTP in that it uses a layer of insulation within the protective jacket, which helps maintain the quality of the signal. Figure 1-13 shows the size of STP cabling as compared with UTP.

Fiber-Optic Cable

The third type of cabling to discuss is fiber-optic cabling. Fiber-optic cabling is unlike coax and twisted-pair because both of those types of cabling use a copper wire that carries the electrical signal. Fiber-optic cables use optical fibers that carry digital data signals in the form of modulated pulses of light. An optical fiber consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding. There are two fibers per cable—one to transmit and one to receive. The core also can be an optical-quality clear plastic, and the cladding can be made up of gel that reflects signals back into the fiber to reduce signal loss. Figure 1-14 shows fibers in a fiber-optic cable.

FIGURE 1-13

UTP cabling versus STP cabling

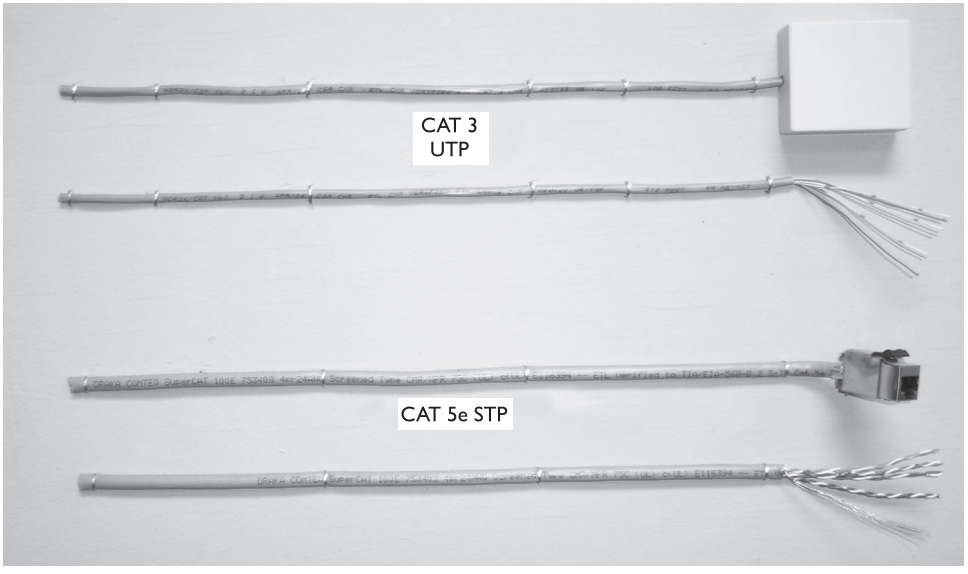
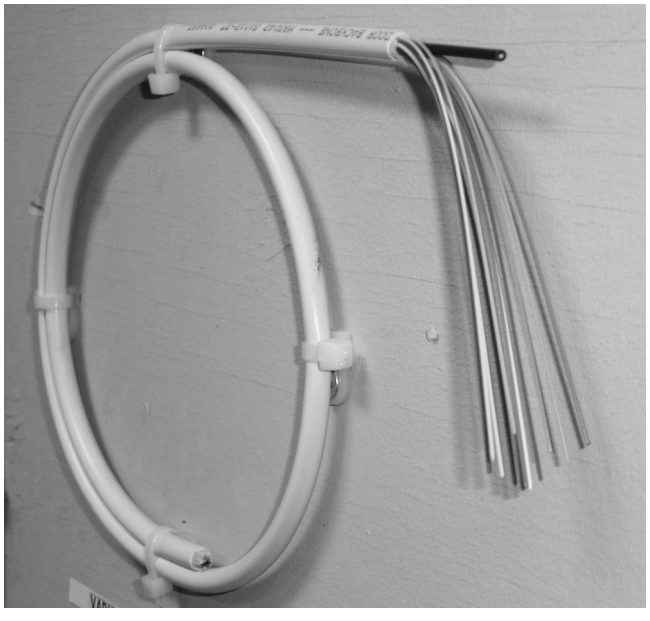


FIGURE 1-14

A fiber-optic cable



The two types of fiber-optic cables are single-mode fiber (SMF) and multimode fiber (MMF):

- **Single-mode fiber** Uses a single ray of light, known as a mode, to carry the transmission over long distances
- **Multimode fiber** Uses multiple rays of light (modes) simultaneously, with each ray of light running at a different reflection angle to carry the transmission over short distances

exam Watch

Remember for the exam that fiber-optic is a more secure cable type to use because it does not carry an electrical signal, but instead carries data as pulses of light.

Fiber-optic cable supports up to 1,000 stations and can carry the signal up to and beyond 2 kilometers. Fiber-optic cables are also highly secure from outside interference such as radio transmitters, arc welders, fluorescent lights, and other sources of electrical noise. On the other hand, fiber-optic cable is by far the most expensive of these cabling methods, and a small network is unlikely to need these features.

Fiber-optic cables can use many types of connectors, but the Security+ exam is concerned only with the two major connector types: the straight-tip (ST) connector and the subscriber (SC) connector. The ST connector is based on the BNC-style connector but has a fiber-optic cable instead of a copper cable. The SC connector is square and somewhat similar to an RJ-45 connector. Figure 1-15 shows the ST

FIGURE 1-15

Fiber-optic ST and SC connector types

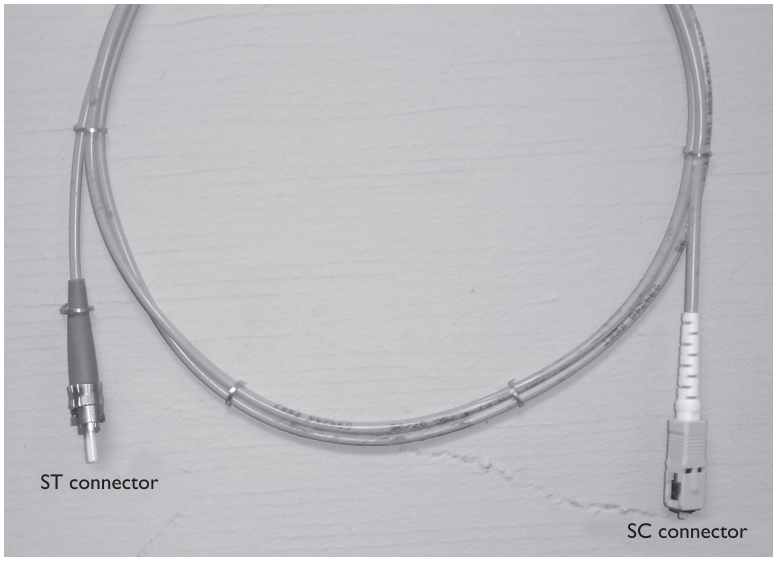


TABLE 1-3

Summary of Cable Types

Cable	Max Distance	Transfer Rate	Connector Used
Thinnet	185 m	10 Mbps	BNC
Thicknet	500 m	10 Mbps	AUI
CAT 3 (UTP)	100 m	10 Mbps	RJ-45
CAT 5 (UTP)	100 m	100 Mbps	RJ-45
CAT 5e	100 m	1 Gbps	RJ-45
CAT 6	100 m	10 Gbps	RJ-45
Fiber-optic	2 km	1+ Gbps	SC, ST

(the connector on the left side) and the SC (the connector on the right side) connector types.

Regardless of the connector type, the fiber-optic cable functions at the same speed, which is typically 1,000 Mbps and faster. The only thing that you need to worry about is that the connector matches the device to which it is being connected, since the two connector types are not interchangeable.

When preparing for the Security+ exam, it is sometimes helpful to have a table listing the differences between the cable types. Table 1-3 summarizes the different cable types—be sure to review it for the Security+ exam.

EXERCISE 1-1

Reviewing Networking Components

In this exercise, you will put your knowledge of networking cables and devices to use by matching the terms to the appropriate scenario.

Device	Scenario
____ Switch	A. Sending bogus MAC address information to the switch to cause the switch to fail-open
____ Load balancer	B. A communication boundary
____ UTP	C. A layer-3 device that sends data from one network to another
____ Port security	D. A layer-2 device that filters traffic based on MAC address
____ VLAN	E. A device that is used to split the workload between multiple servers
____ Router	F. A cable type that carries pulses of light
____ MAC flooding	G. A type of cable that has copper wires divided into pairs
____ Fiber-optic	H. Controlling which MAC addresses can connect to the switch

CERTIFICATION OBJECTIVE 1.02

Understanding TCP/IP

Now that you understand some of the different types of networking devices that are used on networks and the cable types being used, let's switch directions by talking about the TCP/IP protocol. As a security professional, it is critical that you not only are familiar with the TCP/IP protocol, but also understand how communication occurs on a TCP/IP network. Let's get started with a quick review of the protocol basics.

Reviewing IP Addressing

TCP/IP requires a little bit of knowledge to configure the systems properly. When you configure TCP/IP, you are required to know the settings for the IP address, subnet mask, and default gateway. Let's start with the IP address.

IP Address The IP address is a 32-bit value that uniquely identifies the system on the network (or the Internet). An IP address looks similar in appearance to 192.168.1.15. The four decimal values in an IP address are separated by decimal points. Each value is made up of 8 bits (1's and 0's), so with four decimal values, 8 bits × 4 = the 32-bit address.

Since each of the decimal values is made up of 8 bits (for example, the *192*), we refer to each of the decimal values as an octet. Four octets are in an IP address. It is very important to understand that the four octets in an IP address are divided into two parts—a *network ID* and a *host ID*. The subnet mask determines the number of bits that make up the network ID and the number of bits that make up the host ID. Let's see how this works.

Subnet Mask When looking at a subnet mask, if there is a 255 in an octet, then the corresponding octet in the IP address is part of the network ID. For example, if I had an IP address of 192.168.1.15 and a subnet mask of 255.255.255.0, the first three octets would make up the network ID, and the last octet would be the host ID. The network ID assigns a unique address to the network itself, while the host ID uniquely identifies the system on the network. Table 1-4 summarizes this example.

You can see in Table 1-4 that the network ID (shown with an *N*) is 192.168.1, and the host ID is the last octet with a value of 15. This means that this system is on the 192.168.1 network, and any other system on the same network will have the same network ID.

TABLE 1-4

Identifying the Network ID and Host ID Portions of an IP Address

	Octet 1	Octet 2	Octet 3	Octet 4
IP address	192	168	1	15
Subnet mask	255	255	255	0
Address portion	N	N	N	H

To use a different example, if you had a subnet mask of 255.0.0.0, it would mean that the first octet of the IP address is used as the network ID portion, while the last three octets are the host ID portion of the IP address.

So what is the purpose of the subnet mask? Or better yet, why do we have a subnet mask that breaks the IP address into a network ID and a host ID? Because when a system such as 192.168.1.15 with a subnet mask of 255.255.255.0 sends a piece of data to 192.198.45.10, the sending system first needs to determine whether the target computer exists on the same network. It does this by comparing the network IDs (Table 1-5); if the network IDs are the same, then both systems exist on the same network, and one system can send to the other without the use of a router. If the systems exist on different networks, the data will need to be passed to the router so the router can send the data to the other network.

Default Gateway When your system wants to send data to another system on the network, it looks at its own network ID and compares that with the destination system's IP address. If they have the same network ID, the data is sent directly from your system to the destination system. If the two systems are on different networks, your system must pass the data to the router so that the router can send the data to the destination system's router.

How does your system know which router to use? The answer is "the default gateway." The default gateway is the IP address of the router that can send data from your network.

TABLE 1-5

Identifying Two Systems on Different Networks Using the Subnet Masks

	Octet 1	Octet 2	Octet 3	Octet 4
IP address #1	192	168	1	15
Subnet mask	255	255	255	0
IP address #2	192	198	45	10

To communicate on the Internet, your system will need to be configured with an IP address, a subnet mask, and a default gateway. If you need to communicate only with other systems on your network, you will need only an IP address and a subnet mask.

Address Classes

Every IP address belongs to a distinct address class. The Internet community defined these classes to accommodate networks of various sizes. The class to which the IP address belongs initially determines the network ID and host ID portions of the address, along with the number of hosts that are supported on that network. The different class addresses are named class A, class B, class C, class D, and class E. This section details each class of addresses.

Class A Addresses A class A address has a default subnet mask of 255.0.0.0, which means that the first octet is the network ID and the last three octets belong to the host ID portion of the address. Each octet can contain 256 possible values (0–255), so a class A address supports 16,777,216 hosts on the network (256 × 256 × 256). Actually, there are only 16,777,214 valid addresses to use on systems because two addresses are reserved on each IP network: the addresses with all host bits set to 0's (the network ID) and with all host bits set to 1's (the broadcast address). So with a class A address, you will not be able to assign n.0.0.0 or n.255.255.255 (where n is your network ID) to any hosts on the network.

You can always identify a class A address because the value of the first octet falls between 1 and 126. An address that starts with 127 is a class A address as well, but you are not allowed to use any address that starts with 127 because it is reserved for the loopback address (more on the loopback address later in this chapter). For example, the IP address of 12.56.87.34 is a class A address because the first octet is 12, which falls within the range of 1 to 126.

Class B Addresses Class B addresses have a default subnet mask of 255.255.0.0, which means that the first two octets are the network ID and the last two octets are the host ID portion of the address. This means that we can have 65,536 hosts (256 × 256) on the network. Oh, but wait! Don't forget to take off the two reserved addresses, so that gives us 65,534 addresses that can be assigned to hosts on the network.

Due to the number of hosts that are supported on a class B address, you usually find that a medium-sized company has a class B address. You can identify a class B address because the first octet starts with a number that falls between 128 and 191.

Class C Addresses Class C addresses have a subnet mask of 255.255.255.0, which means that the first three octets are the network ID and the last octet is the host ID. Having only one octet as the host ID means that a class C address can support only 254 hosts (256 – 2) on the network.

You can identify a class C address because it has a value for the first octet that ranges between 192 and 223. For example, an IP address of 202.45.8.6 is a class C address because 202 falls between 192 and 223. We also know that this system has a subnet mask of 255.255.255.0 because it is a class C address.

Class D Addresses Class D addresses are used for special types of applications on the network known as multicasting applications. *Multicasting applications* send data to a number of systems at the same time by sending data to the multicast address, and anyone who has registered with that address will receive the data. A multicast address is what class D addresses are used for, so you will not be assigning them specifically to hosts on the network for normal network communication.

Class D addresses have a value in the first octet that ranges from 224 to 239. With that many ranges, class D has the potential for 268,435,456 unique multicast groups that users can subscribe to from a multicast application.

INSIDE THE EXAM

Remember Address Classes?

Although the Network+ certification exam tests you on IP addressing and configuration concepts, you still need to know the concept of address classes to answer related questions on the Security+ certification exam. The following paragraphs review the key information about address classes.

Class A addresses have an IP address in which the first octet is between 1 and 126. Class A addresses also have a default subnet mask of 255.0.0.0. Also note that this subnet mask can be displayed as a /8 at the end of the address—for example, 12.0.0.10/8 means that the first eight bits make up the subnet mask.

Class B addresses have an IP address in which the value of the first octet is between 128 and 191. Class B addresses have a default subnet mask of 255.255.0.0 or can be displayed as /16 at the end of the address.

Class C addresses have an IP address in which the value of the first octet is between 192 and 223. In addition, class C addresses have a default subnet mask of 255.255.255.0, which can be displayed as /24 at the end of the address.

Class E Addresses The funny thing about class E addresses is that they were designed only for experimental purposes, so you will never see a class E address on a network. Class E addresses have a first octet with a value that falls in the range of 240 to 247.

Now that you are familiar with the different class addresses, take a look at Table 1-6, which summarizes the address classes. Be sure to know them for the exam.

Special Addresses

You have learned that you are not allowed to have a host assigned an IP address that has a value of 127 in the first octet. This is because the class A address range of 127 has been reserved for the loopback address.

The *loopback address* is used to refer to the local system, also known as the localhost. If you want to verify that the TCP/IP software has initialized on the local system even though you may not have an IP address, you may ping the loopback address, which is typically referred to as 127.0.0.1.

A *private address* is an address that can be assigned to a system but cannot be used for any kind of Internet connectivity. The private addresses are nonroutable addresses, so any system using them will be unable to function off the network. The following are the three address ranges that are the private address ranges:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Being unable to route data across the Internet when using these addresses will not pose a problem, because realistically, you will have these private addresses sitting behind a network address translation (NAT) server that will translate the private address to a public address that can be routed on the Internet.

Windows clients support a feature known as *automatic private IP addressing (APIPA)*, which is a feature that provides that when a client cannot contact a DHCP server, Windows clients configure themselves automatically with a

TABLE 1-6 Reviewing Address Classes

	First Octet Value	Subnet Mask	# of Hosts per Network
Class A	1–127	255.0.0.0	16,777,214
Class B	128–191	255.255.0.0	65,534
Class C	192–223	255.255.255.0	254

169.254.*x*.*y* address. If something is wrong with the DHCP server and all the systems on the network cannot obtain an address from the DHCP server, the clients will all assign themselves an address within the 169.254 address range and then be able to communicate with one another.

APIPA does not assign a default gateway, so you will be unable to access resources on a remote network and the Internet—but you can still communicate with systems on your network. When troubleshooting to find out why a machine cannot communicate on the network, watch for systems that have the 169.254.*x*.*y* address range because it means they could not find a DHCP server.

Illegal Addresses

Not only should you be familiar with the private address ranges in TCP/IP, but you should also be able to identify illegal addresses. An illegal address is an address that is not allowed to be assigned to a host on the network such as a system or router. From a certification exam point of view, you need to be able to identify these illegal addresses. The following are considered illegal addresses:

- **Any address starting with 127** An IP address that starts with 127 is reserved for the loopback address and cannot be assigned to a system. An example of this type of illegal address is 127.50.10.23.
- **All host bits set to 0** You are not allowed to assign a system an IP address that has all of the bits in the host ID portion set to 0 because this is the network ID. An example of this type of illegal address is 131.107.0.0.
- **All host bits set to 1** You are not allowed to assign a system an IP address that has all the host bits set to 1 because this corresponds to the broadcast address of the network. An example of this type of illegal address is 131.107.255.255.
- **A duplicate address** You are not allowed to assign a system an address that another system is using because this results in a duplicate IP address error.

EXERCISE 1-2

Understanding Valid Addresses

In this exercise, you will practice identifying valid addresses by recording whether each of the following addresses is valid. A valid address is an address that can be assigned to a system on the network. If an address is invalid, you must specify why.

Address	Valid?
10.0.40.10	
127.54.67.89	
131.107.34.0	
45.12.0.0	
216.83.11.255	
63.256.4.78	
200.67.34.0	
131.107.23.255	

Understanding TCP/IP Protocols

Now that you understand the fundamentals of IP addressing, let's talk about the different protocols that exist in the TCP/IP protocol suite. As a security professional who will be responsible for configuring firewalls and access lists on routers, it is critical that you understand each of the TCP/IP protocols.

Transmission Control Protocol

The Transmission Control Protocol (TCP) is responsible for providing connection-oriented communication and for ensuring delivery of the data (known as reliable delivery). Connection-oriented communication involves first establishing a connection between two systems and then ensuring data sent across the connection reaches the destination. TCP will make sure that the data reaches its destination by retransmitting any data that is lost or corrupt. TCP is used by applications that require a reliable transport, but this transport has more overhead than a connectionless protocol because of the construction of the session and the monitoring and retransmission of any data across that session.

Another factor to remember about TCP is that the protocol requires that the recipient acknowledge the successful receipt of data. Of course, all the acknowledgments, known as ACKs, generate additional traffic on the network, which reduces the amount of data that can be passed within a given time frame. The extra overhead involved in the creation, monitoring, and ending of the TCP session is worth the certainty that TCP will ensure that the data will reach its destination.

TCP ensures that data is delivered by using what known as sequence numbers and acknowledgment numbers. A *sequence number* is a number assigned to each piece of data that is sent. After a system receives a piece of data, it acknowledges that it has received the data by sending an acknowledgment message back to the sender, with the original sequence number being the acknowledgment number of the reply message.

TCP Three-Way Handshake Before a system can communicate over TCP, it must first establish a connection to the remote system. To establish a connection to the remote system, TCP uses what is called the TCP three-way handshake. The three phases to the TCP three-way handshake (as shown in Figure 1-16) are

- **SYN** In the first phase, the sending system sends a SYN message to the receiving system. Each packet sent is assigned a sequence number, which is a unique number assigned to the packet. The SYN message contains the *initial sequence number (ISN)*, which is the first sequence number to be used. In this example, Computer A is connecting to the web site on Computer B, so a SYN message is sent to port 80 on Computer B.
- **ACK/SYN** The second phase is known as the ACK/SYN phase because this message is acknowledging the first message but at the same time is indicating its initial sequence number. In this example, Computer B sends back the ACK/SYN message that is acknowledging that it has received packet 123 (by acknowledging that 124 is the next sequence number), but has also specified that its ISN is 326.
- **ACK** The final phase of the three-way handshake is the acknowledgment message, which acknowledges that the packet sent in the second phase has been received. In this example, Computer A sends the ACK to acknowledge that it has received packet 326 by acknowledging that the next packet will be sequence number 327.

FIGURE 1-16

The TCP three-way handshake

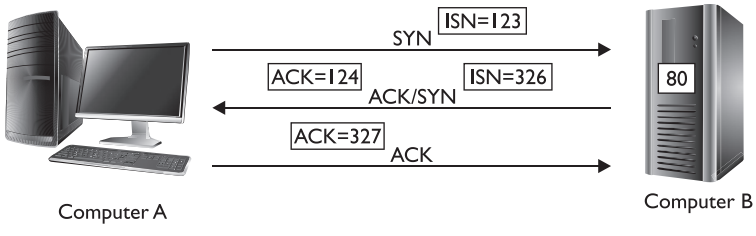
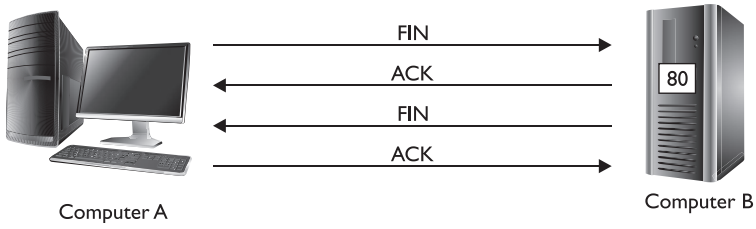


FIGURE 1-17

Terminating a TCP connection



Disconnecting from a TCP Session Just as TCP has a three-way handshake to create a connection between two systems that wish to communicate, TCP also has a process to have a participant disconnect from the conversation. Looking at Figure 1-17, you can see that if Computer A wants to disconnect from a TCP session, it must first send a FIN flag to signal that it wants to end the conversation.

When Computer B receives the FIN message, it replies with an acknowledgment and then sends its own FIN message back to Computer A. As a final step to this process, Computer A must acknowledge that it has received the FIN message from Computer B. This is similar to talking to someone on the phone—to end the conversation, you say goodbye and then wait for the other person to say goodbye before hanging up. I describe this as ending the conversation in a "polite" way.

There is also a way to end a conversation in an "impolite" manner. Back to the telephone analogy: you can end the conversation impolitely by hanging up the phone without saying goodbye. In the TCP world, you can "hang up" by sending a TCP message with the RST (reset) flag set.

TCP Ports When applications use TCP to communicate over the network, each application must be uniquely identified by using a unique port number. A *port* is a unique address assigned to the application. When a client wants to communicate with one of those applications (also known as a service), they must send the request to the appropriate port number on the system.

As a security professional, it is critical that you know some of the port numbers used by popular services. Table 1-7 identifies common TCP port numbers you should know for the Security+ certification exam.

TCP Flags The TCP protocol uses what is known as TCP flags to identify important types of packets. The following are the common TCP flags you should be familiar with for the Security+ certification exam. Figure 1-18 displays the flags in a packet capture. Note that instead of showing the actual flag, the value is interpreted

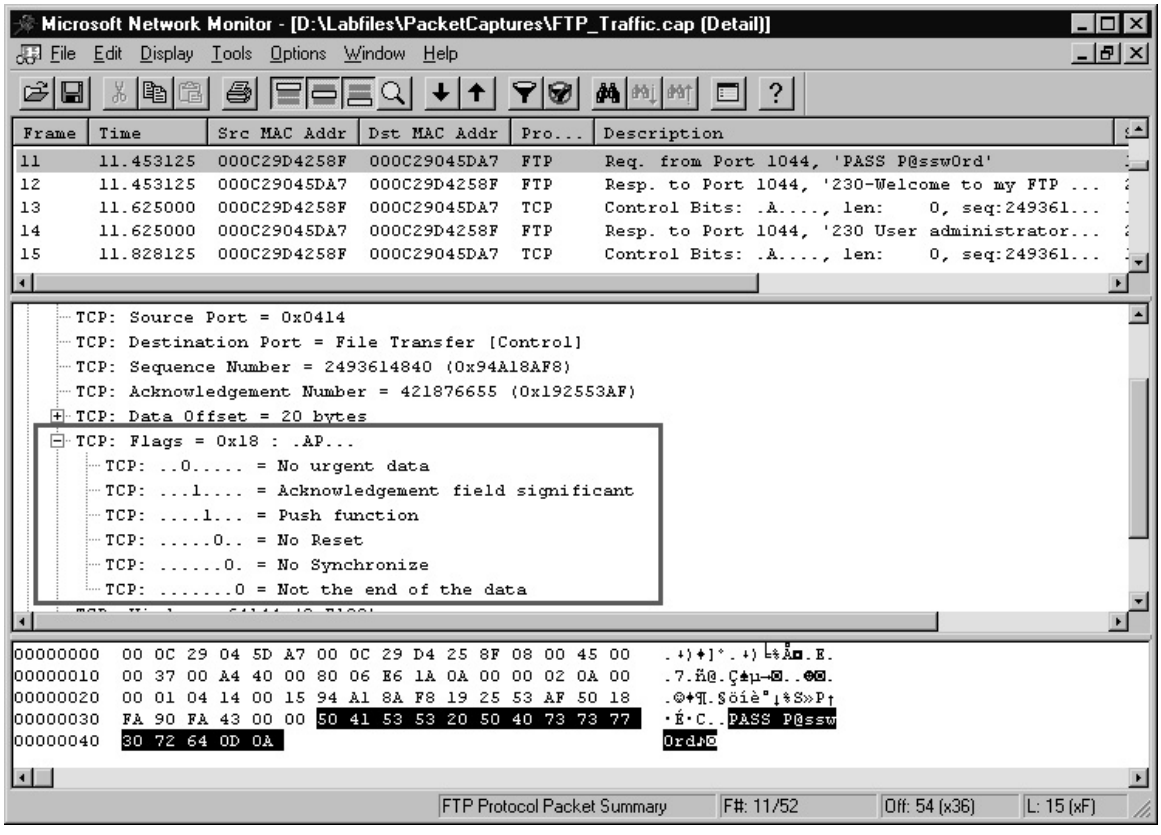
TABLE 1-7 Popular TCP Ports

Port	Service	Description
20	FTP Data	Port used by FTP to send data to a client.
21	FTP Control	Port used by FTP commands sent to the server.
22	SSH	Port used by Secure Shell (SSH) to encrypt remote access communication. It typically is used as a secure replacement to Telnet.
23	Telnet	Port used by Telnet to remotely connect to a system such as a server or router.
25	SMTP	Port used to send Internet e-mail.
53	DNS	Port used for DNS zone transfers.
80	HTTP	Internet protocol for delivering web pages to the browser.
110	POP3	Port used by POP3, which is the Internet protocol to read e-mail.
139	NetBIOS	Port used by the NetBIOS session service and is used to establish a connection between two systems for NetBIOS communication.
143	IMAP	Port used by IMAP, which is a newer Internet protocol to read e-mail.
443	HTTPS	Port used for secure web traffic.
3389	RDP	Port used by Remote Desktop Protocol (RDP) for remote administration of a Windows system.

by Network Monitor and a description is shown instead. For example, instead of seeing the URG flag set to zero, you will see the first flag set to zero with a description of "No urgent data":

- **SYN** The SYN flag is assigned to any packets that are part of the SYN phases of the three-way handshake.
- **ACK** The acknowledgment flag acknowledges that a previous packet has been received.
- **PSH** The push flag is designed to force data on an application.
- **URG** The urgent flag specifies that a packet is an urgent packet.
- **FIN** The finish flag specifies that you would like to finalize, or end, the connection. This is how a TCP connection is ended the polite way—it is like saying goodbye to end a phone conversation.
- **RST** The reset flag is used to end a TCP conversation impolitely. This is like hanging up the phone without saying goodbye.

FIGURE 1-18 TCP flags in the TCP header



exam Watch

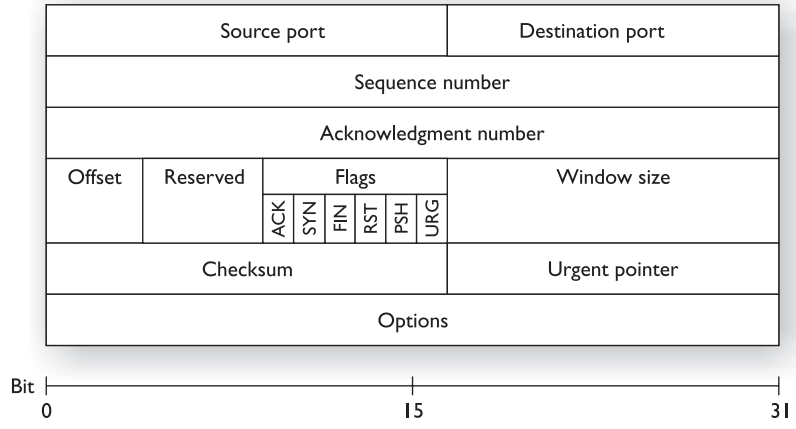
As a security professional and someone taking the Security+ exam, you should be familiar with the different TCP flags because they will help you understand the different types of port scans covered in Chapter 4.

TCP Header Every packet that is sent using the TCP protocol has a TCP header assigned to it, which contains TCP-related information such as the source port, destination port, and the TCP flags. Figure 1-19 displays the different fields in the TCP header. A quick description of each field follows:

- **Source Port** This 16-bit field identifies the port number of the sending system.

FIGURE 1-19

The TCP header



- **Destination Port** This 16-bit field identifies the port number the packet is destined for on the destination system.
- **Sequence Number** This 32-bit field identifies the sequence number of the packet.
- **Acknowledgment Number** This 32-bit field identifies the packet that this packet is acknowledging.
- **Offset** This 4-bit field indicates where the data begins.
- **Reserved** This 6-bit field is always set to 0 and was designed for future use.
- **Flags** This 6-bit field is where the TCP flags are stored. There is a 1-bit field for each of the flags mentioned earlier in this section.
- **Window Size** This 16-bit field determines the amount of information that can be sent before an acknowledgment is expected.
- **Checksum** This 16-bit field is used to verify the integrity of the TCP header.
- **Urgent Pointer** This 16-bit field is used only if the URG flag is set and is a reference to the last piece of information that is urgent.
- **Options** This field is a variable-length field that specifies any additional settings that may be needed in the TCP header.

exam Watch

TCP and UDP are considered layer-4 (transport) protocols.

User Datagram Protocol

The User Datagram Protocol (UDP) is used by applications that do not want to be concerned with ensuring the data reaches the destination system. UDP is used for connectionless communication (unreliable), which means that data is sent to the destination and no effort is made to track the progress of the packet and whether it has reached the destination.

UDP Ports Like TCP, the UDP protocol uses port numbers to identify different types of UDP traffic. Table 1-8 identifies a few examples of UDP traffic and the ports used.

UDP Header Because the UDP protocol does not have to acknowledge the receipt of a packet, the structure of the UDP header is much simpler than the TCP header. For example, the UDP header does not need a sequence number or acknowledgment number; it also does not need flags to indicate special packets such as a SYN message because there is no three-way handshake (because UDP is connectionless). Figure 1-20 displays the UDP header with a listing of the following fields:

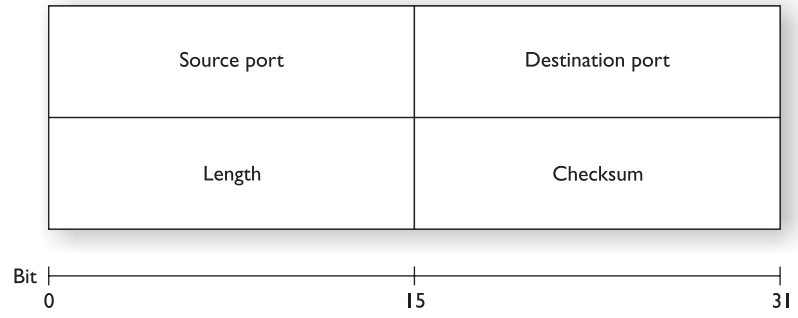
- **Source Port** A 16-bit field that indicates the port used by the sending application on the sending system.
- **Destination Port** A 16-bit field that indicates the port used by the application on the destination system.
- **Length** A 16-bit field that specifies the size of the UDP header in bytes.
- **Checksum** A 16-bit field used to verify the integrity of the UDP header.

TABLE 1-8 Popular UDP Ports

Port	Service	Description
53	DNS	UDP port 53 is used for DNS queries.
67 & 68	DHCP	UDP port 67 is used by the DHCP service, and UDP port 68 is used by client requests.
69	TFTP	Trivial File Transfer Protocol is used to download files without requiring authentication.
137 & 138	NetBIOS	UDP 137 and 138 are used by the NetBIOS name service and datagram service.
161	SNMP	UDP port 161 is used by the Simple Network Management Protocol.

FIGURE 1-20

The UDP header



exam Watch

IP is a layer-3 protocol of the OSI model and is responsible for logical addressing and routing.

Internet Protocol

The Internet Protocol (IP) provides packet delivery for protocols higher in the model. It is a connectionless delivery system that makes a "best-effort" attempt to deliver the packets to the correct destination. IP does not guarantee delivery of the packets—that is the responsibility of transport protocols; IP simply sends the data.

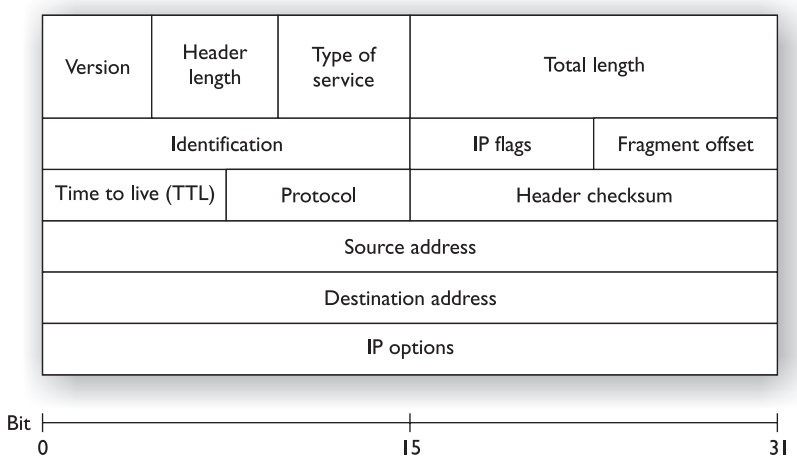
The IP protocol is also responsible for the logical addressing and routing of TCP/IP and therefore is considered a layer-3 protocol of the OSI model. The IP protocol on the router is responsible for decrementing (usually by a value of 1) the TTL (time to live) of the packet to prevent it from running in a "network loop." Windows operating systems have a default TTL of 128.

exam Watch

Although the OSI model is more of a Network+ topic, it is important to remember it for the Security+ exam because it serves as background that can help you understand networking technologies such as network devices and access control lists. For example, if you read of a firewall technology that can filter based on layer-3 or layer-4 information, if you know the OSI model, you would know that is source and destination IP address (layer 3).

FIGURE 1-21

The IP header



IP Header The IP header in the packet contains information that helps the packet make its way from the source to the destination. The following is a listing of the fields and their meaning, while Figure 1-21 displays the IP header structure:

- **Version** A 4-bit field that identifies the version of IP being used, for example, 4 or 6.
- **Header Length** A 4-bit field that indicates the size of the IP header.
- **Type of Service** An 8-bit field that indicates how the packet should be handled by the system. For example, if the low delay option is specified here, it means that the system should deal with the packet right away.
- **Total Length** A 16-bit field that indicates the size of the IP header.
- **Identification** A 16-bit field. Networks can only handle packets of a specific maximum size—known as a *maximum transmission unit (MTU)*—so the system may break the data being sent into multiple fragments. This field uniquely identifies the fragment.
- **IP Flags** A 3-bit field that specifies how fragments are going to be dealt with. For example, a More Fragments (MF) flag indicates more fragments are to come. Also, a bit known as Don't Fragment (DF) specifies not to fragment the packet.
- **Fragment Offset** A 13-bit field that specifies the order that the fragments are to be put back together when the packet is assembled.

- **Time to Live (TTL)** An 8-bit field that specifies when the packet is to expire. The TTL is a value that is decremented with every router the packet passes through. When the TTL reaches 0, the packet is discarded.
- **Protocol** An 8-bit field that specifies what layer-4 protocol (TCP or UDP) the packet should use.
- **Header Checksum** A 16-bit field that verifies the integrity of the IP header.
- **Source Address** A 32-bit field that represents the IP address of the sending system. This is how the receiving system knows where to send the reply message.
- **Destination Address** A 32-bit field that represents the IP address of the system the packet is destined for.
- **IP Options** A variable-length field that is used to specify any other settings in the IP header.

Internet Control Message Protocol

Internet Control Message Protocol (ICMP) enables systems on a TCP/IP network to share status and error information. You can use the status information to detect network trouble. ICMP messages are encapsulated within IP datagrams so that they can be routed throughout a network. Two programs that use ICMP messages are Ping and Tracert.

exam Watch

ICMP is the protocol in the TCP/IP protocol suite that is responsible for error and status reporting. Programs such as Ping and Tracert use ICMP.

You can use Ping to send ICMP echo requests to an IP address and wait for ICMP echo responses. Ping reports the time interval between sending the request and receiving the response. With Ping, you can determine whether a particular IP system on your network is functioning correctly. You can use many different options with the Ping utility.

Tracert traces the path taken to a particular host. This utility can be very useful in troubleshooting internetworks. Tracert sends ICMP echo requests to an IP address while it increments the TTL field in the IP header by a count of 1 after starting at 1 and then analyzing the ICMP errors that are returned. Each succeeding echo request should get one further into the network before the TTL field reaches 0 and an "ICMP time exceeded" error message is returned by the router attempting to forward it.

ICMP Types and Codes ICMP does not use port numbers, but instead uses ICMP types and codes to identify the different types of messages. For example, an echo request message that is used by the Ping request uses ICMP type 8, while the Ping reply comes back with an ICMP type 0 message.

Some of the ICMP types are broken down to finer levels with different codes in the type. For example, ICMP type 3 is a destination unreachable message, but because there are many possible reasons why a destination is unreachable, the type is subdivided into different codes. Each code is for a different message in the type (see Table 1-9).

exam Watch

To be good at monitoring networks and identifying suspicious traffic, you need to understand each of the protocol headers discussed in this chapter.

For the exam, know that ICMP type 8 is used by the echo request message, and ICMP type 0 is used by echo reply.

ICMP Header The ICMP header is a very small header compared to the IP header and the TCP header. Figure 1-22 displays the ICMP header, and a listing of the fields follows:

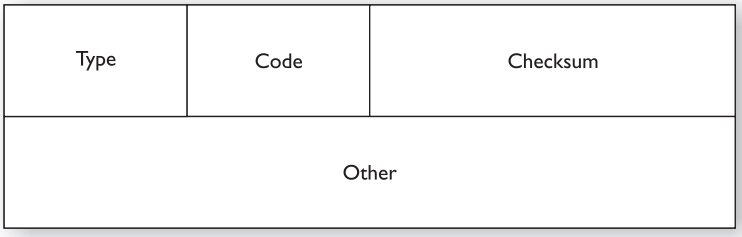
- **Type** An 8-bit field that indicates the ICMP type being used.
- **Code** An 8-bit field indicating the ICMP code being used.
- **Checksum** A 16-bit field that is used to verify the integrity of the ICMP header.
- **Other** A field that stores any data within the ICMP header. For example, Microsoft operating systems place part of the alphabet in this field for echo request messages.

TABLE 1-9 Common ICMP Types and Codes

Type	Code	Description
0—Echo Reply	0	Echo reply message
3—Destination Unreachable	0	Destination network
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
8—Echo Request	0	Echo request message

FIGURE 1-22

The ICMP header



Address Resolution Protocol

Address Resolution Protocol (ARP) provides logical-address-to-physical-address resolution on a TCP/IP network, which is converting the IP address to a MAC address. To accomplish this feat, ARP sends out a broadcast message with an ARP request packet that contains the IP address of the system it is trying to find. All systems on the local network see the message, and the system that owns the IP address for which ARP is looking replies by sending its physical address to the originating system in an ARP reply packet. The physical/IP address combo is then stored in the ARP cache of the originating system for future use.

exam Watch

ARP is responsible for converting an IP address (layer-3 address) to the physical MAC address (layer-2 address).

All systems maintain ARP caches that include IP-address-to-physical-address mappings. The ARP cache is always checked for an IP-address-to-physical-address mapping before initiating a broadcast.

EXERCISE 1-3

Viewing Protocol Information with Network Monitor

In this exercise, you will install a network-monitoring tool known as Network Monitor, which you can download from Microsoft's web site. You will look at network traffic that was captured previously in a file. The example is that a user has entered a credit card number into a web site and you have captured the traffic. Your goal is to find the credit card number in the packet.

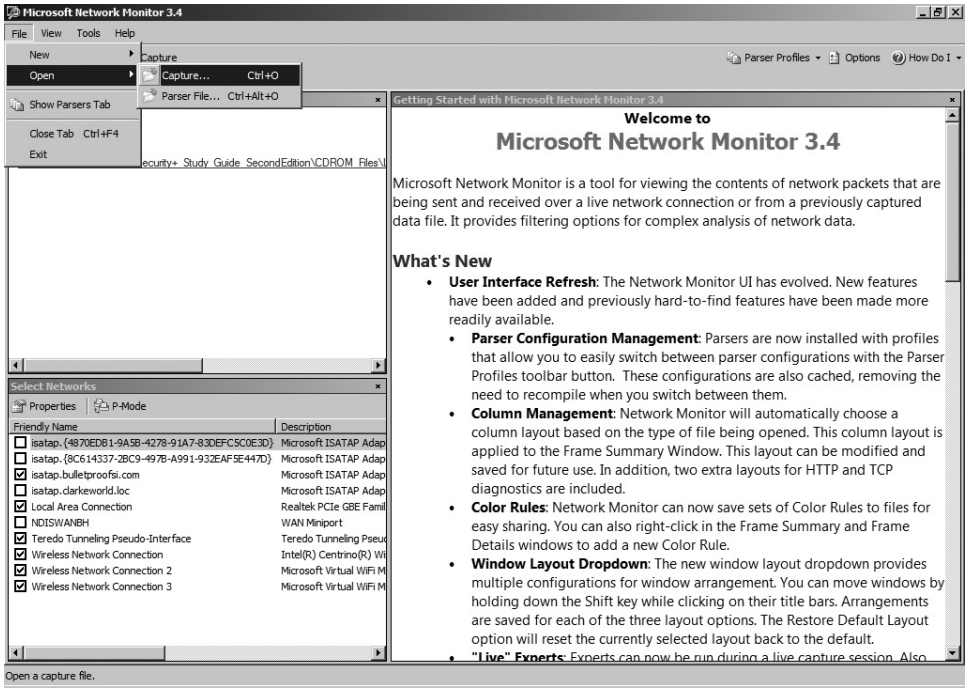
Let's start the exercise by installing the Network Monitor software on your system. These steps were written for Network Monitor, but you could perform similar steps using monitoring software such as Wireshark.

Installing Network Monitor

Download and install the latest version of Microsoft Network Monitor from Microsoft's web site.

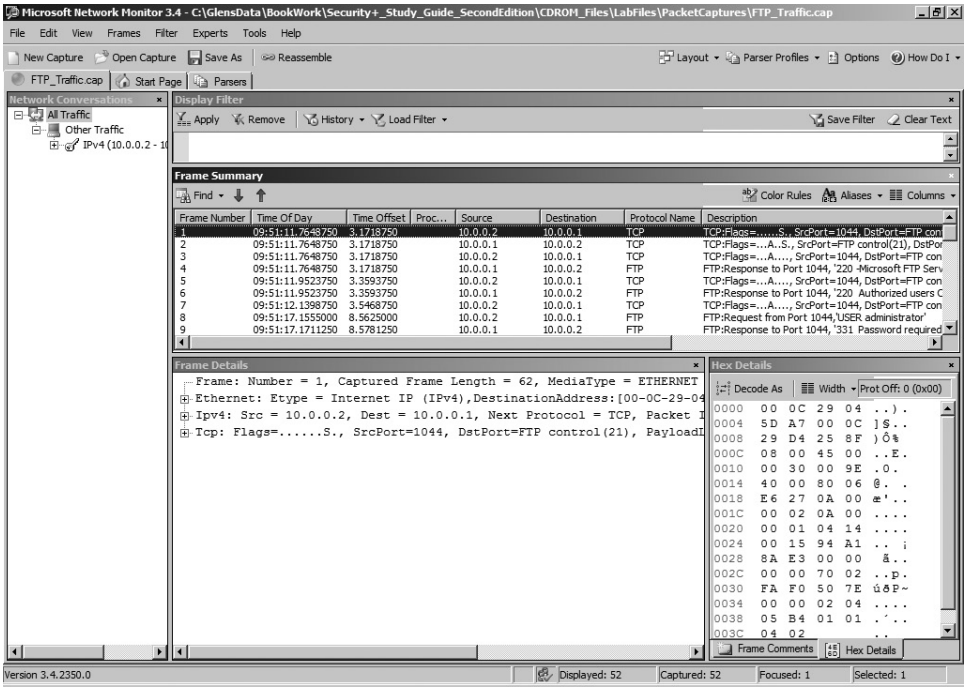
Viewing Packet Data with Network Monitor

1. Start Network Monitor by launching the program with the shortcut found on the desktop.
2. Once Network Monitor is started, open a capture file by choosing File | Open | Capture.



3. In the Open dialog box, open the FTP_Traffic.cap file located in the Labfiles\PacketCaptures folder.

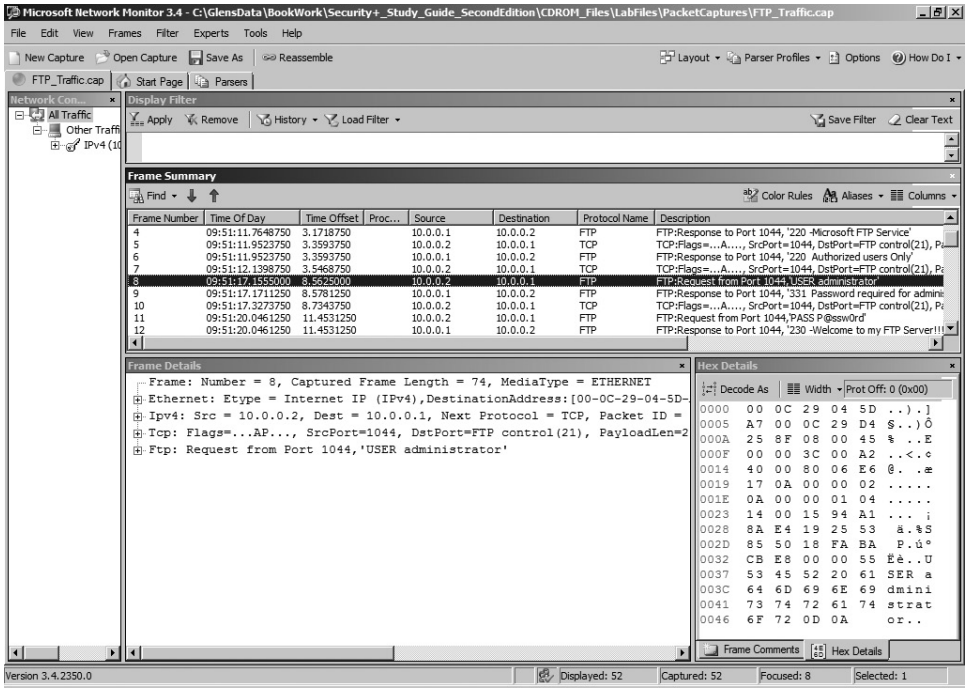
4. The contents of the packet capture are displayed. Notice that 52 frames (numbers listed down the left side in the Frame Summary section located in the middle of the screen) are captured (you can also see the Capture: 52 in the status bar). In the middle of the screen, locate frame 4 and notice that it is the first FTP packet (look in the Protocol Name column).



5. Notice in the Description column that the first three frames are the TCP three-way handshake. You can see this by looking at the Protocol Name column first to see TCP and then the Description column shows the flags of *S* for SYN and *A* for ACK.

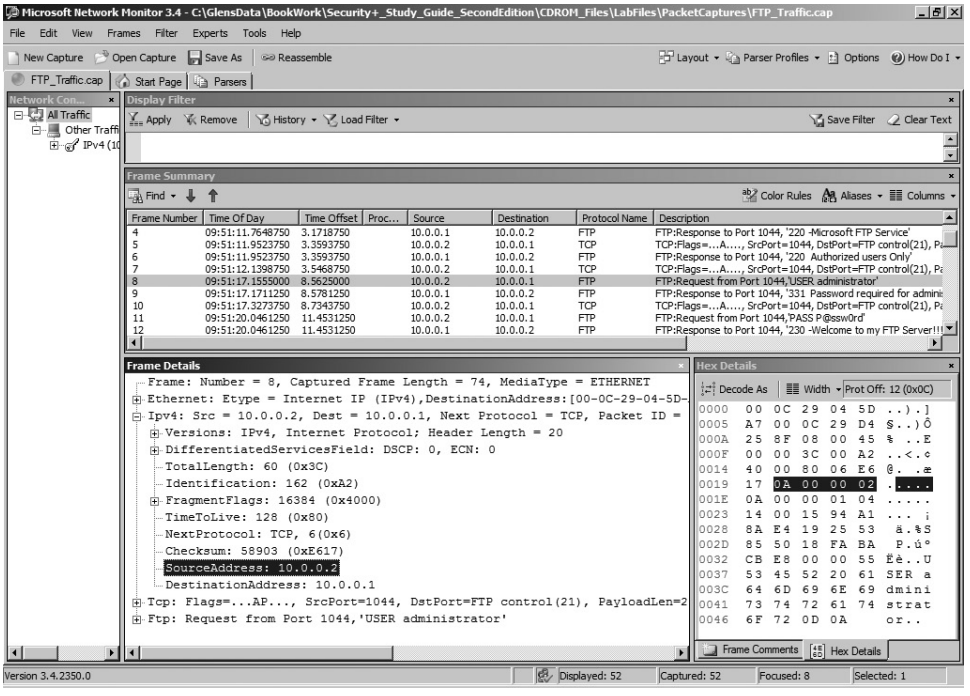
6. Select frame 8. Notice that in the Description column you can see the username that is used to log on to the FTP server. What is the username?

_____



7. Ensure frame 8 is still selected in the Summary window.
8. Notice below the Summary window you have the Frame Detail window showing the packet details for the frame selected. Notice to the right of Frame Details, you have the Hex Details window showing you the hex data for the selected frame. Ensure that frame 8 is still selected in the summary window so that you can investigate this packet.

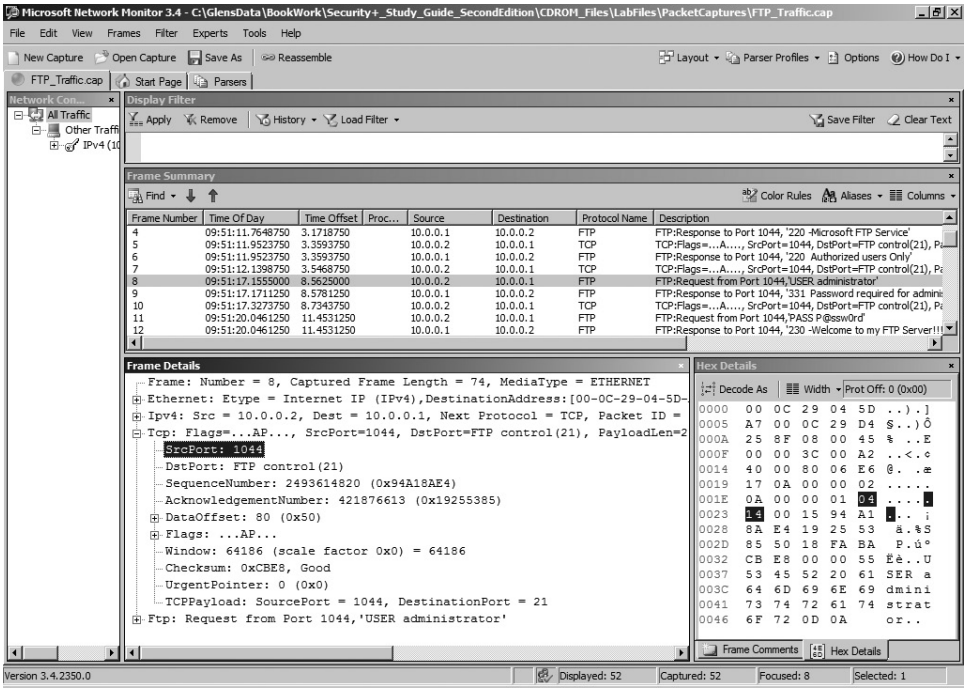
9. Expand the IPv4 section in the Frame Details window to view the IP header of the packet and record the following information:



a. Source IP Address: _____

b. Destination IP Address: _____

10. Expand the TCP header in Frame Details and locate the following information:



a. Source Port: _____

b. Destination Port: _____

c. Sequence Number: _____

d. Flags Set: _____

11. Select frame 11 and locate the FTP password in the packet capture. What is the password being used (look in the Description column of the Summary window or the FTP section in the Frame Details window)? _____

12. Close Network Monitor.

Application Layer Protocols

When preparing for the Security+ certification exam, you are required to understand various protocols that are used by applications for communication. In this section you will learn about common protocols used by Internet applications and network applications.

HTTP and HTTPS

The Hypertext Transfer Protocol (HTTP) is used on the Internet to allow clients to request web pages from web servers and to allow client interaction with those web servers. HTTP is a stateless protocol, meaning that the web servers are unaware of what a client has or has not requested and cannot track users who have requested specific content. This system does not allow for good interaction with the web server, but does allow for retrieving the HTML pages stored on web sites. To aid in tracking client requests, we use cookies—small files stored on the client computer that allow the web server to store data on the client that the client will send back with each request to the server.

The Hypertext Transfer Protocol, Secure (HTTPS) allows you to connect to a web site and to receive and send content in an encrypted format using Secure Sockets Layer (SSL). HTTPS is most commonly used on e-commerce sites to allow you to send personal information, especially credit card numbers and other confidential data, without worrying that an Internet hacker is viewing this information. You can determine when HTTPS is being used because the address of the web site starts with https:// and not http://, which marks the regular HTTP protocol. Another sign that HTTPS is in use: in Internet Explorer a lock appears in the status bar of a page—the lock is either closed or locked (as shown in Figure 1-23).

Normally, HTTPS is not used for an entire e-commerce site because the encryption and decryption processes slow the connection time, so only the part of the site that requests personal information uses HTTPS.

exam Watch

For the exam, remember that HTTP uses TCP port 80, while HTTPS uses TCP port 443.

DNS

The Domain Name System (DNS) service is used to convert fully qualified domain names (FQDNs) to IP addresses. When accessing Internet sites or servers on the Internet, you use names such as www.gleneclarke.com to connect to the system.

FIGURE 1-23 Identifying the use of secure traffic by the lock in Internet Explorer

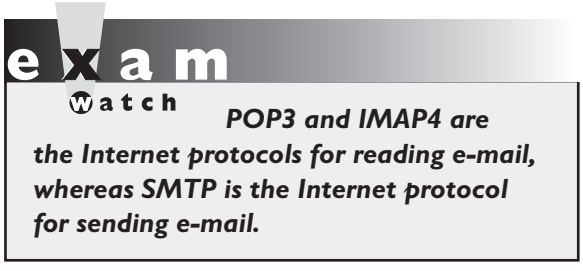
Before a connection is attempted, your system queries a DNS server over UDP port 53 and asks the DNS server for the IP address of that system. Once your system has the IP address of the target system, it makes a connection to that system by using the IP address.

Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol (SMTP) is used to send or route mail over a TCP/IP network such as the Internet. Most e-mail server products support SMTP (TCP port 25) in order to send e-mail out of the corporation and onto the Internet.

Post Office Protocol 3 (POP3)

The Post Office Protocol version 3 (POP3) is the Internet protocol used to retrieve e-mail from a mail server down to the POP3 client over TCP port 110. The e-mail is "popped" or downloaded to the client after the client has been authenticated to its mailbox. POP3 has limited capabilities as far as folder support is concerned. A POP3 client supports only an inbox, an outbox, sent items, and deleted items. If additional folder support is required, you would need to use an IMAP4 client.



Internet Message Access Protocol 4 (IMAP4)

The Internet Message Access Protocol version 4 (IMAP4) is another protocol similar to POP3 that allows clients to retrieve messages from a mail server using TCP port 143. IMAP4 allows additional folders other than the four basic ones provided with POP3. For example, you can use an IMAP4 client to connect to public folders stored on an Exchange Server.

Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is an Internet standard that provides a simple method for remotely managing virtually any network device that supports SNMP over UDP port 161. A network device can be a network card in a server, a program or service running on a server, or a network device such as a hub, switch, or router.

The SNMP standard defines a two-tiered approach to network device management: a central management system and the management information base (MIB) located on the managed device. The management system can monitor one or many MIBs, allowing for centralized management of a network. From a management system, you can see valuable performance and network device operation statistics, enabling you to diagnose network health without leaving your office.

The goal of a management system is to provide centralized network management. Any computer running SNMP management software is referred to as a management system. For a management system to be able to perform centralized network management, it must be able to collect and analyze many types of data, including the following:

- Network protocol identification and statistics
- Dynamic identification of computers attached to the network (referred to as *discovery*)

- Hardware and software configuration data
- Computer performance and usage statistics
- Computer event and error messages
- Program and application usage statistics

File Transfer Protocol (FTP)

The File Transfer Protocol (FTP) is a TCP/IP protocol that exists to upload and download files between FTP servers and clients. Like Telnet and Ping, FTP can establish a connection to a remote computer by using either the hostname or the IP address and must resolve hostnames to IP addresses to establish communication with the remote computer.

exam Watch

For the exam, remember that FTP is a protocol that uses two ports. TCP port 21 carries the FTP commands from one system to another, while TCP port 20 is responsible for transferring the data between two hosts in an FTP session.

When TCP/IP is installed on the system, an FTP utility is available, but a number of third-party graphical user interface (GUI) FTP clients are also available for all operating systems. If you use FTP a great deal, a GUI FTP client could save you a lot of time and frustration in dealing with FTP commands.

Trivial File Transfer Protocol (TFTP)

The Trivial File Transfer Protocol (TFTP) is a simple protocol compared with FTP and supports only reading and writing to files. TFTP does not support features such as listing directory contents or authentication. TFTP uses UDP as the transport protocol, and FTP uses TCP. TFTP is typically used to copy router and switch configuration from the device to the TFTP server over UDP port 69. TFTP can also be used to boot a device by loading the configuration that is stored on a TFTP server.

Secure File Transfer Protocol (SFTP)

The Secure File Transfer Protocol (SFTP) is an interactive file transfer protocol similar to FTP, but it encrypts all traffic between the SFTP client and the SFTP server. SFTP supports additional features such as public key authentication and compression. Unlike TFTP, SFTP does support a number of commands in its interactive shell such as listing directory contents, creating directories, downloading files, and uploading files.

Telnet

Telnet is a terminal emulation protocol that runs on TCP port 23 and allows a client to run or emulate the program running on the server. A number of devices allow you to telnet into the device and perform remote administration of the network device using the command set available to the telnet session.

Secure Shell (SSH)

The Secure Shell (SSH) is a program used to create a shell, or session, with a remote system using a secure connection over TCP port 22. Once the remote session is established, the client can execute commands within this shell and copy files to the local system. The major purpose of SSH is to support remote shells with support for secure authentication and encrypted communication.

Secure Copy Protocol (SCP)

The Secure Copy Protocol (SCP) is responsible for copying files from a remote server to the local system over a secure connection, ensuring that data in transit is kept confidential. A number of SCP products use an SSH connection to ensure the security of the secure copy operation.

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is used to synchronize the clocks of PCs on a network or the Internet. This is accomplished by configuring a server to be the time server, which then is the server from which all other PCs on the network synchronize their time.

On earlier Windows networks, you can manage time synchronization by placing a command in a logon script to synchronize the time on the client with the time server. Use the following command:

```
NET TIME \\computername /SET
```

Newer Microsoft networks such as Active Directory networks have the PDC (Primary Domain Controller) emulator provide the time to all servers and clients automatically, so there is no need to create a logon script for the clients to synchronize the time with the time server. PDC emulators can also retrieve their time from Internet NTP servers.

Time servers on the Internet allow you to synchronize your PC's clock with the exact time kept by atomic clocks. The time synchronization takes into account time

zone settings of your operating system and allows you to synchronize with a time server even if it is not set for your local time zone.

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is the TCP/IP protocol for directory service access that is supported by all the principal directory services such as Novell's eDirectory and Microsoft's Active Directory. LDAP is a protocol that allows LDAP clients to connect to the network database, or directory, and to query the database for information about its objects such as user accounts and printers. For example, a user on the network could find the phone number of another user by using the LDAP protocol.

exam Watch

LDAP is the industry-standard protocol for accessing a directory service and is supported by Active Directory and Novell's eDirectory. LDAP uses TCP port 389 by default.

NetBIOS

Network Basic Input/Output System (NetBIOS) is an application programming interface (API) that is used to make network calls to remote systems and is used for session management functionality. NetBIOS is a session layer protocol that is installed with other routable protocols such as IPX/SPX or TCP/IP to allow NetBIOS traffic to travel across networks. NetBIOS has two communication modes:

- **Session mode** Used for connection-oriented communication in which NetBIOS would be responsible for establishing a session with the target system, monitoring the session to detect any errors in transmission, and then recovering from those errors by retransmitting any data that went missing or was corrupt.
- **Datagram mode** Used for connectionless communication in which a session is not needed. Datagram mode also is used for any broadcast by NetBIOS. Datagram mode does not support error detection and correction services, which are therefore the responsibility of the application using NetBIOS.

Microsoft uses NetBIOS names, also known as computer names, as a method of identifying systems on the network. A NetBIOS name can be a maximum of 16 bytes long—15 bytes for the name and 1 byte for the NetBIOS name suffix (a code at the end of the name representing the service running). The NetBIOS computer name must be unique on the LAN.

Network Storage Protocols

There are multiple protocols that allow a system to communicate with a disk storage device located on the network:

- **Fibre Channel** A technology that transmits data of up to a projected 4 Gbps and uses special optical cables to connect the shared storage devices to servers.
- **iSCSI** Internet Small Computer Systems Interface, an IP-based protocol used to communicate with storage devices. iSCSI traffic carries SCSI disk commands from a host to a storage device on the network. The benefit of iSCSI compared to Fibre Channel is that you do not require special hardware to connect to the shared disk solution; you can use your existing network infrastructure, along with iSCSI, to communicate with shared disks on the network.
- **FCoE** Stands for Fibre Channel over Ethernet and is a protocol used to carry Fibre Channel commands over an Ethernet network in Ethernet frames. It is important to note that Fibre Channel runs at layer 2, so it is not routable across IP networks (whereas iSCSI is IP-based, so it is routable).

A Review of IPv6

The Security+ exam focuses on TCP/IP version 4 (IPv4) for any TCP/IP-related content, but you are expected to understand how things have changed with IPv6. The first major difference is in the addressing scheme—IPv4 is based on a 32-bit address scheme, while IPv6 is based on a 128-bit address scheme.

exam Watch

IPv4 uses a 32-bit addressing scheme, while IPv6 is a 128-bit address scheme that uses a hexadecimal address format. For the Security+ exam, you will need to know the basics about the IPv6 address schemes.

Parts of the Internet are already using IPv6, and new areas are being upgraded on a daily basis. IPv6 is based on a 128-bit address scheme because the 32-bit address scheme of IPv4 proved to not create enough addresses. One of the focuses of the IPv6 protocol was to address the shortage of addresses that exists with IPv4, so the protocol is using a 128-bit address scheme.

IPv6 Addresses

An IPv6 address is a 128-bit address that is displayed in the hexadecimal format and not in the dotted-decimal notation that is used by IPv4. The IPv6 address is divided into eight 16-bit groups, each separated by a colon (:). The following is an example of an IPv6 address:

```
65b3:b834:45a3:0000:0000:762e:0270:5224
```

exam Watch

For the Security+ exam, you need to know that IPv6 uses a 128-bit address space. You may also be asked to identify the IPv6 loopback address, 0:0:0:0:0:0:0:1.

An IPv6 address is not case-sensitive, and you do not need to place leading zeros at the beginning of the address when referencing a system that has leading zeros at the beginning. You can also replace consecutive zeros with double colons (::) when referencing an address that has a group of zeros in the address. For example, the loopback address in IPv6 is 0:0:0:0:0:0:0:1 and can be shortened to ::1, with the **::** replacing all the consecutive zeros at the beginning of the address. This process is known as *compressing zeros*.

IPv6 uses three types of addresses—unicast, multicast, and anycast:

- **Unicast** Used for one-to-one communication.
- **Multicast** Used to send data to a group of systems.
- **Anycast** Applied to a group of systems providing a service. Clients that send data to the anycast address could have the data sent to any of the systems that are part of the anycast address.

To make life more complicated, you should be familiar with different types of unicast addresses for the Security+ exam: global unicast, site-local unicast, and link-local unicast addresses handle different types of unicast traffic. Following is a quick breakdown of each of the different types of unicast addresses:

- **Global unicast** A public IPv6 address that is routable on the Internet. The address assigned to the host must be unique on the Internet. This address type is equivalent to a public IP address with IPv4.
- **Site-local unicast** A private address for the IPv6 protocol; the address always starts with *FEC0*. Assigning a site-local address to a system is equivalent to using a private address in IPv4 such as 10.0.0.0. The site-local

address cannot be used to communicate off the local site or network and is not reachable by other sites or systems on the Internet.

- **Link-local unicast** An address that is self-assigned and is used to communicate only with other nodes on the link. Link-local addresses always start with *FE80*. This address type is equivalent to an APIPA address with IPv4.

on the job

You should be familiar with two of the reserved addresses in IPv6: the loopback address, which is 0:0:0:0:0:0:0:1 (or ::1), and the address for a system with no address specified, 0:0:0:0:0:0:0:0 (or ::).

IPv6 Protocols

Not only has the address scheme changed with IPv6, but so have the protocols that exist in the IPv6 protocol suite. Here's a quick breakdown of a few of the protocols that are used in the IPv6 protocol suite.

IPv6 The new version of IP is responsible for logical addressing and routing functions, as was IPv4. It is a connectionless protocol that relies on upper-layer protocols such as TCP to guarantee delivery.

ICMPv6 The ICMP protocol is responsible for error and status information as in IPv4, but it has been changed. ICMPv6 uses codes, while ICMPv4 used types and codes. For ICMPv6, each code indicates the type of message. Codes from 0 to 127 are used by error messages, while codes 128 to 255 are for information messages. For example, the echo request message is code 128 with ICMPv6, and the echo reply message is code 129.

ICMPv6 has expanded on its features from the ICMPv4 days. You should be familiar with the following two features of the ICMPv6 protocol:

- **Multicast Listener Discovery (MLD)** Replaces the multicast protocol in IPv4 known as Internet Group Management Protocol (IGMP) and is used for multicast communication
- **Neighboring Discovery (ND)** Replaces ARP from the IPv4 days by performing the same function, but it's also responsible for neighboring router discovery, automatic address assignment, and duplicate address detection, to name a few features

IPv6 has been totally redesigned and offers many additional new features, but for the Security+ exam, you only need to worry about the basics. Further information on IPv6 can be found at http://technet.microsoft.com/en-ca/network/bb530961.aspx.

EXERCISE 1-4

Identifying Protocols in TCP/IP

In this exercise, you will practice identifying the different TCP/IP protocols by associating the protocol with the corresponding scenario.

Protocol	Scenario
____ TCP	A. Converts FQDNs to IP addresses
____ IP	B. Responsible for error reporting and status information
____ DNS	C. Protocol used to download files
____ HTTPS	D. Responsible for network monitoring and management
____ UDP	E. Converts logical address to physical address
____ FTP	F. Protocol used for secure web traffic
____ ICMP	G. Responsible for unreliable delivery
____ ARP	H. Responsible for logical addressing and routing
____ SNMP	I. Responsible for reliable delivery

CERTIFICATION OBJECTIVE 1.03

Network Security Best Practices

This chapter has exposed you to a number of networking concepts, protocols, and devices to act as a review of Network+, but more importantly to ensure that you understand key networking concepts related to some of the security topics in later chapters. Before moving into the next chapter, I want to summarize some key points surrounding security best practices with networking devices and protocols.

Device Usage

Earlier in the chapter, you learned about the purpose of devices like routers, switches, and proxy servers. The following are some key points to remember involving network device usage to help create a secure network environment.

Physical Security

Ensure that all servers and networking devices such as routers and switches are stored in a secure location such as a locked server room. You want to also ensure that you control and monitor who has access to these physical components of the network.

Do Not Use Hubs

Most environments today are using switches instead of hubs, but if you notice an old hub connected to the network, remember that it should be replaced with a switch so that the traffic is sent only to the port that the destination system resides on.

Configure Passwords

Most networking devices such as routers and switches allow you to configure passwords on the device, which lets you control who is authorized to administer the device. Cisco routers and switches have a number of different passwords such as a console port password, auxiliary port password, and Telnet passwords. Be sure to configure each of these passwords by using a complex password. The following code displays the commands to configure a console password:

```
HAL-R1>enable
HAL-R1#config term
HAL-R1(config)#line con 0
HAL-R1(config-line)#password C0nP@$$
HAL-R1(config-line)#login
```

Use Port Security

You should also ensure that any ports on the switch that are not being used are disabled to help prevent unauthorized individuals from connecting to an available port. In highly secure environments, you should configure port security on the ports, which is a method to specify which MAC addresses are allowed to connect to a particular port.

Port security is also a great countermeasure against MAC *flooding,* which involves the hacker sending frames to the switch that contain different source MAC addresses. This could cause two things to occur: one, the switch will see all of the bogus entries in the MAC address table and no longer trust the table, which results in the switch flooding all frames to all ports (known as a fail-open state).

exam Watch

For the Security+ exam, remember that MAC flooding is when the hacker confuses the switch into flooding all frames to all ports. This allows the hacker to connect to any port on the switch and be able to receive all traffic on the network.

Two, MAC flooding could also result in overwriting entries in the MAC address table so that the switch does not know at what port valid MAC addresses are located. When a switch does not know the location of a particular MAC address, it then *floods* the frame to all ports on the switch, which gives the hacker the opportunity to capture the traffic because the switch is no longer filtering traffic.

Another method that a hacker can use to bypass the filtering feature of the switch is that they could perform an ARP poison attack on all systems so that all systems send data to the hacker's system in order to get out to the Internet. The hacker captures the traffic and then routes it out to the Internet for the user! You will learn more about ARP poisoning in Chapter 4.

Use VLANs

Another important feature of a switch that should be used is VLANs because they offer a way for you to create different communication boundaries by placing ports into the VLAN. Remember that by default a system that is in one VLAN cannot communicate with systems in another VLAN.

Cable and Protocol Usage

When it comes to network cabling in highly secure environments, you should be using fiber-optic cabling because the transmission is carried through pulses of light and not through an electrical signal. This has great security benefits because data carried through copper cabling as an electrical signal is susceptible to interference from other electrical components, whereas data over fiber optics is immune to electrical interference.

exam Watch

For the Security+ exam, remember the most secure cable type to use is fiber-optic cabling.

Fiber-optic cabling also doesn't lend itself to *tapping* into the line as easily as coax or twisted-pair communication. It is possible for a hacker to tap into the fiber-optic line by reflecting some of the light and then converting that light to electrical information to be looked at by the hacker's computer. Although this attack is possible, it is also easy to detect the loss in light that is caused by this attack with the appropriate intrusion detection system on the cable.

Another best practice when working in large networks that involve secure and unsecured systems, or what some organizations call protected and unprotected systems, is to use different-colored cables for a protected system versus an unprotected system. Then when assessing security, you can quickly ensure that the protected system is connected to a protected network and not to an unprotected network. A *protected network* is a controlled network that is not connected to the Internet, while an *unprotected network* is one that is connected to the Internet. In high-security environments, it is critical that a protected system is never connected to an unprotected network because it could be exposed to malicious software from the Internet.

As far as protocols are concerned, ensure that you are using the most secure protocols at all times in environments that require the security. For example, instead of using Telnet to remotely connect to your routers and switches, you should be using SSH. The following secure protocols should be used instead of their insecure equivalent:

- SSH should be used instead of Telnet.
- The secure copy (SCP) command should be used to securely copy information between systems.
- Secure FTP (SFTP or FTPS) should be used instead of FTP to download and upload files.
- HTTPS should be used instead of HTTP to encrypt web content between the client and server.

CERTIFICATION SUMMARY

In this chapter you reviewed the fundamentals of networks by reading about types of devices and protocols that exist in most networking environments today. From a security point of view, it is critical that you understand the types of devices, cables, and protocols that help create a secure environment. The following are some key points to remember about networking fundamentals for the Security+ exam:

- Network switches should be used instead of hubs so that traffic is sent only to the port that has the destination system. This helps protect the data being transmitted from being intercepted.
- Routers create broadcast domains and are responsible for routing (sending) data from one network to another.
- VLANs, an important feature of a switch, create a communication boundary. Each VLAN on a switch is a separate broadcast domain, and a router must be used to allow a system on one VLAN to talk to another VLAN.
- TCP/IP is a suite of protocols; the most important protocols to know are TCP, UDP, IP, and ARP. (Your Security+ exam will definitely have several questions on some of these TCP/IP protocol suite members.)
- TCP/IP addressing involves the IP address, subnet mask, network classes, and special reserved addresses. (Memorize each network class for the exam.)

With a strong understanding of the material presented in this chapter, you will have no problems with any TCP/IP-related questions on your exam. Not only is the material presented here important for the exam, but it will also be important after you ace the exam and continue on to a career as a networking professional.

TWO-MINUTE DRILL

Understanding Network Devices and Cabling

- Switches should be used instead of hubs because they filter traffic by sending the data only to the port on the switch that the destination system resides on. A hub sends the data to all ports on the hub, which allows someone to view all network traffic.
- Switches have great security features such as being able to disable unused ports and configure port security, which allows you to control what systems can connect to a port by MAC address.
- Routers are layer-3 devices that are used to route data from one network to another. Routers are also used to break a network into multiple broadcast domains.
- A proxy server is used to send outbound Internet requests on behalf of clients and is typically used to filter the web sites a user can visit and the types of applications they can use for outbound communication.
- Coax and twisted-pair cabling use a copper core to carry an electrical signal, while fiber-optic cabling is used to carry pulses of light. Fiber-optic cabling is the cabling of choice for highly secure environments.

Understanding TCP/IP

- The IP protocol is responsible for logical addressing and routing.
- The TCP protocol is used for reliable delivery. Communication over TCP starts with the three-way handshake. TCP guarantees delivery by using sequence numbers and acknowledgment numbers.
- TCP uses flags to identify important types of packets. The TCP flags are SYN, ACK, FIN, RST, URG, and PSH.
- UDP is used for connectionless communication.
- TCP and UDP use port numbers to identify the sending and receiving application of the data. For the Security+ exam, know the common ports discussed in this chapter.

- ICMP is used for status and error reporting. ICMP uses types and codes to identify the different types of messages. Type 8 is used for echo request, and type 0 is used for echo reply.
- ARP is responsible for converting the logical address (IP address) to a physical address (MAC address).

Network Security Best Practices

- Ensure that you use fiber-optic cabling instead of twisted-pair because fiber-optic cabling is a bit more challenging to tap into and is immune to electrical interference.
- Use secure versions of protocols to encrypt communication. Examples of secure protocols are SSH, SCP, HTTPS, and FTPS.
- Make sure that you use features of the switch, such as port security, to control which systems can connect to the switch.
- Disable all unused ports on the switch.

SELF TEST

The following questions will help you measure your understanding of the material presented in this chapter. Read all the choices carefully because there might be more than one correct answer. Choose all correct answers for each question.

Understanding Network Devices and Cabling

1. What feature of a network switch allows the network administrator to capture network traffic when monitoring or troubleshooting the network?
   A. Port security
   B. VLAN
   C. Collision domain
   D. Port mirroring
2. Your manager has been reading about hackers capturing network traffic in a switched network environment and is wondering how it is possible that hackers can do this. (Select two.)
   A. ARP poisoning
   B. Port mirroring
   C. Port security
   D. MAC flooding
   E. VLANs
3. Your company has a web application that seems to be running slowly. Your manager is wondering what can be done to improve the performance of the application.
   A. Install a proxy server
   B. Install a load balancer
   C. Configure the web site in a VLAN
   D. Configure port security
4. Which of the following devices could be used to limit which web sites users on the network can visit?
   A. Router
   B. Load balancer
   C. Proxy server
   D. CAT 5e

Understanding TCP/IP

5. Which TCP/IP protocol is used to convert the IP address to a MAC address?
   A. ARP
   B. TCP
   C. ICMP
   D. UDP
6. What ICMP type is used to identify echo request messages?
   A. 0
   B. 4
   C. 8
   D. 9
7. Which of the following identifies the stages of the three-way handshake?
   A. ACK/SYN, ACK, SYN
   B. SYN, ACK/SYN, ACK
   C. ACK, SYN, ACK/SYN
   D. SYN, ACK, ACK/SYN
8. Which of the following represents ports used by secure TCP applications? (Select all that apply.)
   A. 23
   B. 22
   C. 80
   D. 143
   E. 443

Network Security Best Practices

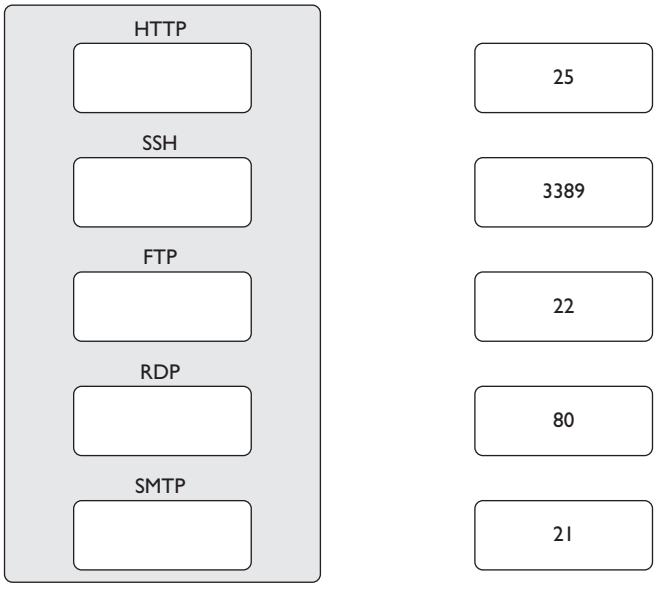
9. You are the network administrator for a small company, and you wish to follow security best practices that relate to the switch. Which of the following should you do? (Select all that apply.)
   A. Disable unused ports
   B. Enable all unused ports
   C. Configure port security
   D. Disable port security
   E. Enable console password
   F. Disable console password

10. What popular feature of a switch allows you to create communication boundaries between systems connected to the switch?

A. ARP poisoning
B. Port mirroring
C. Port security
D. MAC flooding
E. VLANs

Performance-Based Question

11. You have a server with a number of networking services installed. Using the diagram, match the port number on the right to the service on the left.



SELF TEST ANSWERS

Understanding Network Devices and Cabling

1. ☑ **D.** The port mirroring feature of a network switch is designed to send a copy of any data destined for a group of ports to a monitored port. The network administrator connects their monitoring station to the monitored port in order to monitor the network traffic.
   ☒ **A, B,** and **C** are incorrect. Port security is a feature that allows you to control which systems can connect to different ports by their MAC address. A VLAN is a method of creating a communication boundary on a switch. A collision domain is created by each port on a switch and is a group of systems that can have their data collide with one another.
2. ☑ **A** and **D.** Hackers can use a few different techniques to bypass the filtering feature of a switch. The hacker can use ARP poisoning, which poisons the ARP cache on all systems, forcing them to send data to the hacker's system. Another technique is MAC flooding, which involves the hacker sending bogus MAC addresses to the switch, which causes the switch to not trust the MAC address table. As a result, the switch starts flooding all frames (sends the frames to every port) where the hacker is connected and running sniffer software.
   ☒ **B, C,** and **E** are incorrect. Port mirroring is a method used by the administrator to capture network traffic—not the hacker. Port security allows the administrator to control who connects to a port on the switch by MAC address, and VLANs allow you to create a communication boundary.
3. ☑ **B.** A load balancer can be used to split the workload between multiple systems, in this case multiple web servers. Load balancing is a common solution for optimizing performance on web sites or even mail servers.
   ☒ **A, C,** and **D** are incorrect. Proxy servers are used to control outbound Internet access by filtering the web sites users can surf and the applications they can use. VLANs are a security measure to control communication to a group of systems, and port security is used to control which system can connect to a port on a switch by its MAC address.
4. ☑ **C.** Proxy servers are used to control outbound Internet access by filtering web sites users can surf and applications they can use.
   ☒ **A, B,** and **D** are incorrect. A router is a device that sends data from one network to another. A load balancer is used to optimize performance by splitting the workload between all systems in the load balance solution. CAT 5e is a cable type and not a device.

Understanding TCP/IP

5. ☑ **A.** The ARP protocol is responsible for converting the IP address to a MAC address.
☒ **B, C,** and **D** are incorrect. TCP is used for reliable delivery, while UDP is used for unreliable delivery. ICMP is used for error reporting and status information.

6. ☑ **C.** The ICMP type for echo request messages is ICMP type 8.
☒ **A, B,** and **D** are incorrect; they are not the ICMP types for an echo request message.

7. ☑ **B.** The order of the packets for a three-way handshake is SYN, ACK/SYN, and then ACK.
☒ **A, C,** and **D** are incorrect because they do not reflect the order of a three-way handshake.

8. ☑ **B** and **E.** SSH, which is a secure protocol to replace Telnet, uses port 22, while HTTPS is a secure replacement for HTTP traffic and uses port 443.
☒ **A, C,** and **D** are incorrect because they represent ports used by unsecure protocols. Port 23 is used by Telnet, port 80 is used by HTTP, and port 143 is used by IMAP—all of which do not encrypt the traffic between the sender and receiver.

Network Security Best Practices

9. ☑ **A, C,** and **E.** When securing devices such as a switch, ensure the administration port, such as a console port, has a password configured. Also disable any unused port and configure port security on the ports.
☒ **B, D,** and **F** are incorrect. Unused ports should be disabled, port security should be configured, and a password on the console port should be enabled.

10. ☑ **E.** When you place systems in a VLAN, by default they cannot communicate with systems outside the VLAN. You can have a router route the information from one VLAN to another.
☒ **A, B, C,** and **D** are incorrect. ARP poisoning is an attack type that hackers perform to allow them to sniff traffic on the network. Port mirroring is a feature on the switch that allows the administrator to have a copy of all traffic sent to a port on the switch that the administrator connects a monitoring system to. Port security is a feature that controls which systems may connect to a port by MAC address. MAC flooding is an attack type that a hacker performs in order to confuse the switch into sending all traffic to all ports.

Performance-Based Question

11. The Security+ exam will present to you similar questions like this, and you are required to drag the boxes from one side to the other on the real exam. The following shows the matching of port numbers to the network service: