CHAPTER 20

Understanding Protocols

Protocols provide the common language for devices to talk, and they also provide the rules for communicating. To put this into context, Chapter 18 covers devices such as routers, switches, and computers. Chapter 19 covers the different types of cables and how they connect the devices together. This chapter covers many of the common networking protocols.

Exam 220-801 objectives in this chapter:

- 2.3 Explain properties and characteristics of TCP/IP.
  - Client-side DNS
- 2.4 Explain common TCP and UDP ports, protocols, and their purpose.
  - Ports
    - 21 – FTP
    - 23 – TELNET
    - 25 – SMTP
    - 53 – DNS
    - 80 – HTTP
    - 110 – POP3
    - 143 – IMAP
    - 443 – HTTPS
    - 3389 – RDP
  - Protocols
    - DNS
    - LDAP
    - SNMP
    - SMB
    - SSH
    - SFTP
  - TCP vs. UDP

REAL WORLD **A SUCCESSFUL TEST TAKING STRATEGY**

You might need to simply memorize some of the information you learn during your A+ studies. The information is valuable, but you might not have an opportunity to apply the knowledge right away. For example, in this chapter, you'll learn several port numbers that you might not be able to apply in day-to-day work. However, you'll probably be tested on them, so you might want to memorize these port numbers.

There's a common test-taking strategy you can use to help you remember this information when you take the A+ exam. You can't carry notes with you into the exam, but you'll be given something to write on, such as a mini white board or piece of paper. As soon as you start the exam, you can write down notes from your memory.

For example, Table 20-3 in this chapter includes a list of port numbers. If you re-create Table 20-3 as soon as you start, you'll be able to answer port questions simply by looking at your newly created note sheet. Of course, you need to have the notes fresh in your mind when you start so that you can write them down. Also, you need to write your notes down as soon as you start, while your mind is clear and alert. If you wait until question 50 before writing your notes, the information won't be as clear.

Many test takers successfully use this strategy, and you can too.

Introducing Network Protocols

Computers and other devices on a network must follow specific rules when communicating with each other. These rules are defined in a multitude of network protocols.

This is similar to how people communicate. If you're speaking English and I'm speaking Mandarin, we can talk all day long but we probably won't be communicating very well. Actually, even if two people are speaking English, they don't always communicate very well. If one person doesn't listen, filters the words, or changes the meaning, the result is miscommunication. Protocols provide the common language for network communication and help prevent miscommunication problems from occurring.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is a full suite of protocols used on the Internet and on internal networks. It includes TCP, IP, and many more. You might see TCP/IP referred to as though it were a single protocol, but it's important to remember that it's just the name for the full suite.

It's easy to take this for granted because it works so effectively. However, there is a great deal of depth to what these protocols control.

For example, imagine that you wanted to mail all 1,440 pages of *War and Peace* to someone in London but that you could only paste a copy of one page at a time to the back of the postcard. You'd need to figure out a system to ensure that all pages were received and that your friend could put them back in order. If a page was lost in the mail, your friend would need to be able to identify the missing page and ask you to resend it.

Similarly, when you transfer files, TCP/IP ensures that it reaches the destination. If you include a 4-MB file of "War and Peace" as an email attachment, TCP/IP doesn't send it as a single 4-MB file. Instead, it breaks the file up into smaller pieces, transfers these smaller pieces, and puts them together on the other end. If any single piece doesn't make the trip successfully, TCP/IP senses the failure and requests the missing piece.

***NOTE* PACKETS, FRAMES, AND SEGMENTS**

Data transferred over a network are grouped together as individual packets. Packets are also called frames, segments, and protocol data units (PDUs) in different contexts, but in general they're called *packets*. Each packet includes the data and additional information. For example, it identifies where the packet came from and where the packet is going, using source and destination information in the packet. It also includes error checking information used to detect whether the packet has become corrupted.

Connectivity Protocols

Two core protocols used within TCP/IP are *Transmission Control Protocol (TCP)* and *User Datagram Protocol (UDP)*. Almost every connection uses either TCP or UDP.

The following sections cover both TCP and UDP, but for comparison, Table 20-1 summarizes important points related to them.

TABLE 20-1 Comparing TCP and UDP

TCP	UDP
Connection-oriented	Connectionless
Reliable, guaranteed delivery	Best effort delivery
Data receipt acknowledged	No acknowledgments
Uses three-way handshake	No handshake

NOTE **CONNECTION-ORIENTED AND CONNECTIONLESS**

UDP and TCP are both used on wired and wireless networks. That is, "connection-oriented" and "connectionless" don't refer to physical network connectivity; they refer only to creating a logical connection.

To help clarify the comparison between connection-oriented and connectionless in Table 20-1, you can compare connection-oriented to making a phone call, and connectionless to sending a text message. The phone provides two-way communication before the message is sent. The text message is simply sent without a guarantee of delivery.

Imagine that a friend of yours just won the lottery. He wants to give you $10,000 if you pick him up at 8 a.m. tomorrow and give him a ride to pick up his winnings. If he calls and talks to you, he'd know that you received the message. The phone call provides two-way communication and guarantees delivery of the message.

On the other hand, if he sends you a text message, you will probably receive it, but it's not guaranteed. Text messages usually make it to the intended recipient without any problem. However, if your text message device was lost, stolen, or just run over by a bus, your friend wouldn't know. And you might lose $10,000.

TCP

Every TCP connection begins with a three-way handshake that verifies that both devices can connect. It's called a three-way handshake because three data packets are exchanged between the two systems.

For example, consider Figure 20-1. Lori is trying to connect to a server to access a file. Lori's system sends out a SYN (synchronize) packet, similar to asking, "Are you there?" The server responds with a SYN/ACK (synchronize/acknowledge) packet to acknowledge the connection attempt. Lori's system responds with an ACK packet that completes the TCP three-way handshake.

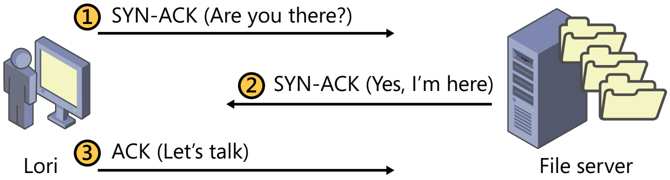


FIGURE 20-1 DNS servers on internal network and on the Internet.

After the connection is established, the two systems exchange data. For example, Lori can download files from the file server. TCP uses additional checks to verify that all the data transfers successfully. If any of the data packets don't arrive, TCP sends a request for the missing packets. If any of the data packets arrive out of order, it arranges them in the original order.

EXAM TIP

TCP provides guaranteed delivery and is referred to as a connection-oriented protocol. It ensures that a logical connection exists before data is transferred. It uses acknowledgements to ensure that all data reaches the destination.

UDP

UDP does not use a three-way handshake and does not establish a connection before sending data. Instead, it just sends the data using its best effort. UDP is used with some protocols where some data loss is acceptable, or when the overhead of creating a connection isn't worth the effort. It is up to the application to provide error correction control.

For example, streaming audio and video often use UDP to provide best effort delivery. If some packets are lost, it's better to allow some gaps in the transmission rather than slow down the transmission. You've probably watched a video on the web where some of the transmission was lost. It skipped or paused for some of the video, but, overall, you were able to get the message.

EXAM TIP

UDP does not provide guaranteed delivery. It does not use a handshake to establish a connection or depend on acknowledgements when sending data.

✓ **Quick Check**

1. What protocol provides guaranteed delivery?
2. What protocol is connectionless?

Quick Check Answers

1. TCP.
2. UDP.

Introducing Ports

Chapter 21 covers IP addresses in greater depth. In short, every computer on a network using TCP/IP has an IP address. For example, my computer has an IP address of 192.168.1.10.

However, just because my computer has only one IP address doesn't mean it can process traffic for only one application at a time. I'm able to use Microsoft Outlook to send and receive email, use Internet Explorer to surf the Internet, and play music in the background streamed from a music site. Each of these applications is running at the same time, and my computer is using only a single IP address.

TCP/IP uses port numbers to identify specific protocols and services. When TCP/IP traffic reaches a computer, it uses the port number to determine which service or application will process the data.

Imagine entering a search on Bing.com with Internet Explorer. TCP/IP uses the IP address to get it to the Bing.com web server. The web server then looks at the port number to forward it to the application that will process the search query. In this case, it is an application on the web server that creates a webpage and sends it back to you.

Web browsers and web servers use Hypertext Transfer Protocol (HTTP) to transfer web traffic. Instead of using the words *Hypertext Transfer Protocol* in the packet, TCP/IP uses the port number *80* to identify HTTP.

NOTE **LOGICAL VS. PHYSICAL PORTS**

These port numbers are logical ports and do not relate to physical ports. In contrast, an RJ-45 port on a switch is a physical port that you can touch, and you can plug a twisted-pair cable into an RJ-45 port. You can't touch the port number 80 that represents HTTP.

Port Ranges

The number 80 isn't random. The Internet Assigned Numbers Authority (IANA), a part of the Internet Corporation for Assigned Names and Numbers (ICANN), has designated specific numbers to represent specific protocols. Table 20-2 shows the three ranges of ports.

TABLE 20-2 Port Ranges

Name	Port Range	Comments
Well-known	0 to 1023	Used by specific protocols or services and assigned by IANA.
Registered	1024 to 49,151	Companies use these to identify applications. Many are assigned by IANA.
Dynamic (or ephemeral)	49,152 to 65,535	Used by internal services and processes.

You don't have to remember which protocol or service maps to every one of these ports. However, you do need to know the number of several ports based on their protocol. As protocols are introduced in this chapter, you'll also see the port if it is relevant for the A+ exam. At the end of this chapter is a realistic example of how the ports are used. Most importantly for the A+ exam, Table 20-3 provides a summary of important port numbers to remember.

Ports and Firewalls

Chapter 22 covers firewalls in more depth, but in brief, a firewall can control the traffic in and out of a network. One of the ways it does so is by allowing or blocking traffic based on the port.

For example, if you want to allow users to visit websites, the firewall needs to allow HTTP traffic out. HTTP traffic uses port 80, so you need to allow outgoing traffic using port 80. On the other hand, if you want to prevent users from visiting any websites, you can block all outgoing traffic using port 80.

EXAM TIP

You create exception rules on firewalls to allow traffic. Most firewalls will block all traffic unless it has an exception to allow traffic. For example, if you want to allow HTTP traffic, the firewall must have an exception rule to allow traffic on port 80. This also known as *opening the port*.

✓ **Quick Check**

1. **What does TCP/IP use to get a packet to a remote system?**
2. **What does TCP/IP use to get a packet to a specific service or application after it makes it to the remote system?**

Quick Check Answers

1. **IP address.**
2. **Port number.**

Exploring Network Protocols

Many of the protocols used on networks and the Internet are very common. You need a basic understanding of them to be a successful technician and to pass the A+ exam. This section provides an overview of the commonly used protocols.

Encryption Protocols

It's relatively easy to capture data sent over a network. It can be tedious to analyze the data, but it is usually not difficult.

Administrators often use protocol analyzers (also called sniffers) to capture network traffic and analyze it. Attackers use the same tools to capture and analyze data. If data isn't protected, the attackers might be able to access secrets simply by listening on a network, just as an eavesdropper can listen in on conversations.

Encryption protocols scramble the data in such a way that it is not readable. More specifically, encryption creates cypher text that is not readable by unauthorized users. Authorized systems automatically decrypt the scrambled data to create readable text, but unauthorized systems or users cannot read it. Some common encryption protocols include the following:

- **Secure Shell (SSH).** SSH is often used within a network to encrypt traffic. Several protocols use it to encrypt traffic. For example, secure copy (SCP) uses it to copy files securely between two systems. SSH uses port 22 by default.
- **Secure Sockets Layer (SSL).** Many types of web traffic are encrypted with SSL. It often uses port 443 but may use other ports, depending on the protocol being encrypted.
- **Transport Layer Security (TLS).** TLS is the designated replacement for SSL. It can be used anywhere SSL is used.

Email Protocols

There are three primary protocols used for email. They are *Simple Mail Transfer Protocol (SMTP)*, *Post Office Protocol version 3 (POP3)*, and *Internet Message Access Protocol (IMAP)*.

- **SMTP.** This protocol is used to send email from user computers to email servers. SMTP uses port 25 by default. I often think of the “SM” in SMTP as “send mail” to remind me that SMTP is used to send email.
- **POP3.** This protocol is used to receive email from email servers. POP3 uses port 110 by default. Many POP email servers will delete the email after it has been downloaded by the user. I often imagine the email messages “popping” off the server as I receive them to help me remember that POP is used for receiving email.
- **IMAP.** This protocol is similar to POP except that messages are retained on the IMAP server in addition to being sent to users. IMAP uses port 143 by default, and the current version is IMAP4. IMAP provides more capabilities than POP, such as the ability to organize email in folders or to search through all the email for specific content.

EXAM TIP

SMTP uses port 25, and user computers use SMTP to send email to SMTP servers. POP3 uses port 110, and users receive email from POP3 servers. IMAP4 uses port 143, and it allows users to organize and search email on an IMAP4 server.

When you initially set up a computer for a user, you often need to configure the addresses of the SMTP, POP, and/or IMAP servers. The Internet Service Provider (ISP) will provide these addresses. For example, my ISP is Cox Communications and I have configured my email accounts with smtp.east.cox.net (to send email to their SMTP server) and pop.east.cox.net (to receive email from their POP3 server).

Chapter 9 introduces SMTP, POP3, and IMAP in the context of configuring tablet devices to send and receive email. Each protocol can be encrypted with SSL or TLS as *SMTPS*, *POP3S*, and *IMAPS*. The default ports for these are as follows:

- SMTPS: port 465
- IMAPS: port 993
- POP3S: port 995

Quick Check

1. **What port and protocol are used for receiving email?**
2. **What port and protocol are used for sending email?**

Quick Check Answers

1. **POP3 uses port 110.**
2. **SMTP uses port 25.**

Web Browser Protocols

Web browsers display webpages formatted in a language called *Hypertext Markup Language (HTML)*. They retrieve HTML webpages from web servers using two primary protocols: *Hypertext Transfer Protocol (HTTP)* and *Hypertext Transfer Protocol Secure (HTTPS)*.

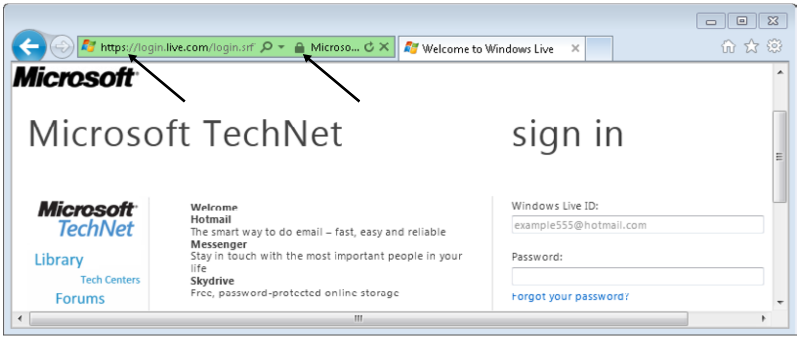
- **HTTP.** This is the primary protocol used to transfer data over the World Wide Web (WWW). HTTP uses port 80 by default.
- **HTTPS.** This protocol provides security for HTTP connections by encrypting the data. HTTPS uses port 443 by default, and it is secured with SSL or TLS.

EXAM TIP

HTTP uses port 80, and HTTPS uses port 443. SSL and TLS also use port 443 by default when used with HTTPS, and SSL and TLS can be used to encrypt other types of traffic. For example, virtual private network (VPN) connections sometimes use SSL over port 443.

Most web sessions don’t need to be encrypted, so they use HTTP. However, some data needs to be encrypted to prevent unauthorized users from seeing it. For example, if you make a purchase with a credit card, you probably don’t want anyone to be able to view your credit card data. Similarly, you wouldn’t want others to see your user name and password as you log on to a website. In these situations, you want to ensure that you are using HTTPS.

Figure 20-2 shows an example of how you can tell whether you have a secure HTTPS connection with Internet Explorer. The first arrow points to the address line where https is listed (instead of http). The second arrow points to a lock icon indicating a secure connection. Different web browsers might put the lock icon in different places, but they will usually have a lock icon somewhere.



Microsoft TechNet

sign in

Welcome
Hotmail
The smart way to do email – fast, easy and reliable
Messenger
Stay in touch with the most important people in your life
Skydrive
Free, password-protected online storage

Windows Live ID: example555@hotmail.com

Password:

Forgot your password?

FIGURE 20-2 Verifying HTTPS is being used.

WWW and the Internet

The World Wide Web (WWW) and the Internet are not the same thing, although they are often confused. The WWW, commonly called the *web*, is used to transfer hypertext documents displayed in web browsers. The Internet is a network of networks that connects computers together from around the world.

Webpages are transferred over the Internet, but the Internet is also used to transfer much more. For example, email is transferred over the Internet by using SMTP and POP3 protocols. SMTP and POP3 aren't transferred over the web.

You can think of the Internet as a massive highway system. Trucks and cars travel over the highways, but the trucks and cars are not the highway. Similarly, webpages created by web servers make up the World Wide Web and send data over the Internet, but the webpages and web servers are not the Internet.

File Transfer Protocols

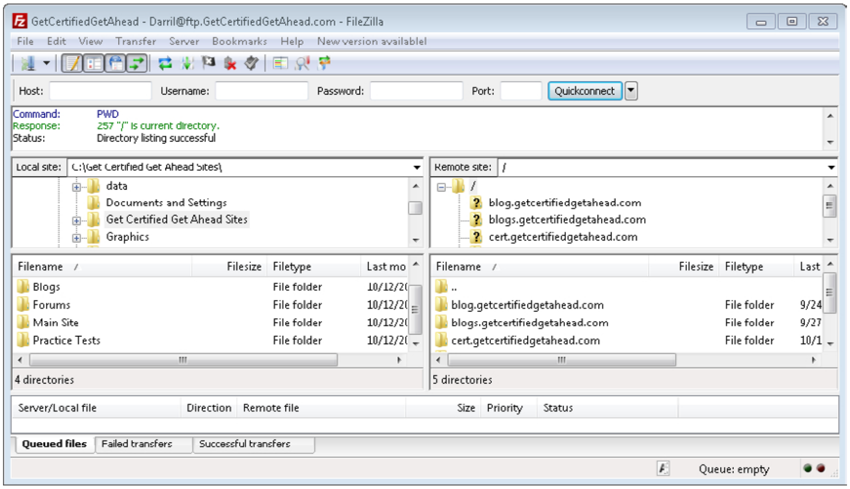
While many files are transferred over the Internet by using HTTP and HTTPS, this isn't always the best method. Files transferred with HTTP and HTTPS are displayed in a web browser, but sometimes you just want to upload or download files without displaying them.

FTP, TFTP, and SFTP

File Transfer Protocol (FTP) is used to upload and download files to and from FTP servers. FTP uses port 21 by default to send control signals to the FTP server and uses a second port for transferring data. The port number of the second port is dependent on the mode FTP is using. If it's using Standard (or passive) mode, FTP uses port 20 with port 21. If it's using Active mode, it dynamically assigns a second port number, up to port 65,535.

An FTP server is a server that is running FTP, but the server can be used for other purposes. It's common to have a web server also running as an FTP server.

For example, I manage some websites, and the servers hosting these websites run FTP. This allows me to upload and download files with an FTP application. I often use FileZilla, which is free (from Filezilla-project.org), efficient, and easy to use. Figure 20-3 shows a screen shot of FileZilla connected to a web server using FTP.



```
Command:    PWD
Response:   257 "/" is current directory.
Status:     Directory listing successful
```

Local site tree: data; Documents and Settings; Get Certified Get Ahead Sites; Graphics

Remote site tree: /; blog.getcertifiedgetahead.com; blogs.getcertifiedgetahead.com; cert.getcertifiedgetahead.com

Filename	Filesize	Filetype	Last mo
Blogs		File folder	10/12/2(
Forums		File folder	10/12/2(
Main Site		File folder	10/12/2(
Practice Tests		File folder	10/12/2(

4 directories

Filename	Filesize	Filetype	Last
..			
blog.getcertifiedgetahead.com		File folder	9/24
blogs.getcertifiedgetahead.com		File folder	9/27
cert.getcertifiedgetahead.com		File folder	10/1

5 directories

Server/Local file	Direction	Remote file	Size	Priority	Status

FIGURE 20-3 Using an FTP application.

Many operating systems include FTP. For example, Windows 7 includes an FTP client that you can access from the command prompt. Open the command prompt, type **FTP**, and press Enter to start it. The problem is that you need to know all the relevant FTP commands. The command prompt is useful in many situations, but for FTP, an application like FileZilla is easier. It allows you to upload and download files with just a few clicks.

EXAM TIP

Many firewalls block FTP traffic by default. To allow FTP traffic, you need to ensure that the firewall has port 21 open to allow outgoing FTP requests. This is also known as creating an exception on the firewall. Firewalls will allow return FTP traffic if outgoing FTP traffic is allowed. Therefore, you usually do not need to open the second port using FTP.

Trivial File Transfer Protocol (TFTP) is a streamlined, or "lite," version of FTP. TFTP uses port 69 by default. It uses the connectionless UDP, so it has less overhead than FTP, which uses the connection-oriented TCP.

Many network administrators use TFTP to upload or download files to routers or switches. For example, after configuring a router, they might use TFTP to download the configuration file as a backup. If the router ever fails, they can upload the configuration file and apply it rather than reconfiguring the router from scratch.

FTP traffic is normally sent over a network in clear text. This can sometimes include user names and passwords, along with associated data. If someone is using a sniffer, this data can easily be viewed.

Secure FTP (SFTP) uses SSH to encrypt the FTP traffic, including the user name, password, and data, so that it is not readable by unauthorized users. When secured by SSH, SFTP uses port 22 by default—the default port of SSH.

SMB

Server Message Block (SMB) is a protocol used to transfer files over a network. It is primarily used in Microsoft networks and is transparent to the user. For example, when a user sends a print job to a printer, the operating system uses SMB to transfer the data.

Similarly, when users access shared files over a network, Windows-based systems use SMB to create the connection and transfer the files. SMB typically uses Network Basic Input/Output System (NetBIOS) over TCP with ports 137, 138, and 139 by default. If used directly over TCP, it uses port 445.

✓ **Quick Check**

1. **What are the ports used for HTTP traffic and encrypted HTTP traffic?**
2. **What are the ports used by FTP and TFTP?**
3. **What is used to encrypt web traffic displayed in Internet Explorer, and on what port?**
4. **What can you use to encrypt FTP traffic, and on what port?**

Quick Check Answers

1. **HTTP uses port 80, and HTTPS uses port 443.**
2. **FTP uses port 20 (and sometimes port 21), and TFTP uses port 69.**
3. **HTTPS using port 443.**
4. **SSH on port 22.**

Name Resolution Protocols

Most of us can remember names and words easier than numbers. However, computers work with numbers better than they do with names. Because of this, humans often identify computers with a name while the computers themselves use numbers.

The two types of computer names used with TCP/IP are as follows:

- **Host names.** Host names are used on the Internet and internal networks. Host names are often combined with a domain name to give a fully qualified domain name (FQDN). For example, a web server named www hosting a website for Margie's Travel has a FQDN of www.margiestravel.com. Similarly, a mail server named mail2 on an internal domain named contoso.com has an FQDN of mail2.contoso.com.

- **Network Basic Input/Output System (NetBIOS) names.** The NetBIOS name is usually the same as the host name. That is, the server with a host name of mail2 also has a NetBIOS name of mail2. NetBIOS names are used only on internal networks, not on the Internet.

The following sections describe how these names are resolved to IP addresses.

DNS

main Name System (DNS) is the primary method used to map host names to IP addresses. It you want to go to MSN.com, you simply type **msn.com** into your *uniform resource locator (URL)* address line. However, your computer can't reach MSN.com until it knows its IP address.

Your system will query a server running DNS (commonly called a DNS server) with the name, and the DNS server responds with an IP address. This is called name mapping or name resolution.

EXAM TIP

DNS maps host names to IP addresses. Systems can query the DNS server with a name, and the DNS server responds with an IP address. It is the primary method of name resolution on the Internet, and it is used on many internal networks.

Internet Service Providers (ISPs) host DNS servers, and many medium-to-large-size businesses have their own internal DNS servers. For example, consider the network shown in Figure 20-4. If internal users need to access systems on the internal network, they will query their internal DNS server. This server holds the mapping to all the names and IP addresses of internal systems.

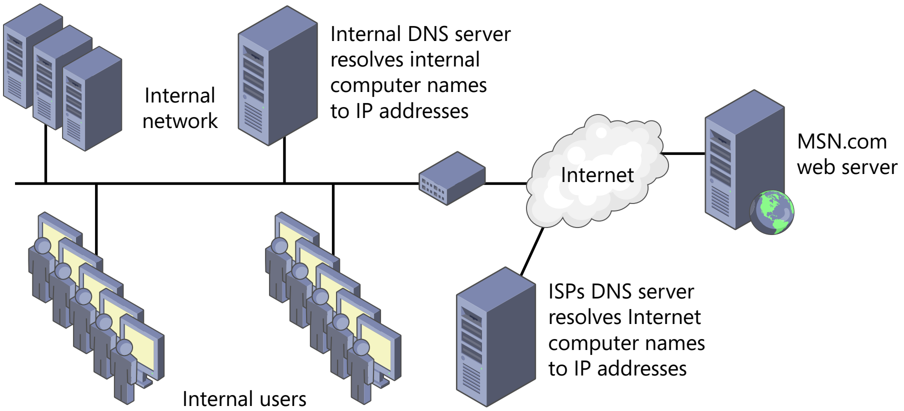

Internal network
Internal DNS server resolves internal computer names to IP addresses
Internet
MSN.com web server
ISPs DNS server resolves Internet computer names to IP addresses
Internal users

FIGURE 20-4 DNS servers on internal network and on the Internet.

If the users need to access an external site, they will still query the internal DNS server, but this server then queries the ISP's DNS server. The ISP's DNS server might know the answer, or it might need to query other DNS servers on the Internet. When it gets the answer, it gives it back to the internal DNS server and then to the user that requested it. All DNS traffic uses port 53 by default.

Many small office home office (SOHO) networks don't use an internal DNS server. A common configuration is with a wireless router (explained in Chapter 23) that uses the ISP's DNS server. The router forwards all DNS requests to the ISP's DNS server and returns the IP addresses to the user.

Client-Side DNS

Names can be resolved by the client without querying DNS. One of the ways is by adding names and IP addresses to a file named hosts. On Windows-based systems, this is located in the C:\Windows\system32\drivers\etc folder by default. If this file includes the name and IP address, the client does not query DNS; it uses the IP address in the file. NetBIOS names can be resolved by the client with a similar file called lmhosts.

Additionally, when a name is resolved by any method, it is placed in the host cache (sometimes called the DNS cache). If the name is in the cache, the client uses it instead of querying DNS again.

MORE INFO **CHAPTER 24**

Chapter 24 shows methods you can use to view and manipulate the cache with the ipconfig command.

WINS

Many internal networks use Windows Internet Name System (WINS) to resolve NetBIOS names to IP addresses. NetBIOS names and WINS servers are never used on the Internet. You'll see them only on internal networks, and their usage is dwindling.

NOTE **WINS IS NOT USED ON THE INTERNET**

Don't be fooled by the word *Internet* within Windows Internet Name Service. WINS has absolutely nothing to do with the Internet or resolving Internet names to IP addresses. It is used only to resolve NetBIOS names.

Quick Check

1. **What are the two types of names used in networks?**
2. **What maps computer names to IP addresses on the Internet?**

Quick Check Answers

1. **Host names and NetBIOS names.**
2. **DNS.**

Remote Connectivity Protocols

There are two primary remote connectivity protocols relevant for an A+ technician. Both are used to create connections with remote systems. They are the Remote Desktop Protocol (RDP) and Telnet.

RDP

Remote Desktop Protocol (RDP) is used in Microsoft networks. Two primary applications that use RDP are Remote Desktop Connection and Remote Assistance. Both use RDP over a default port of 3389.

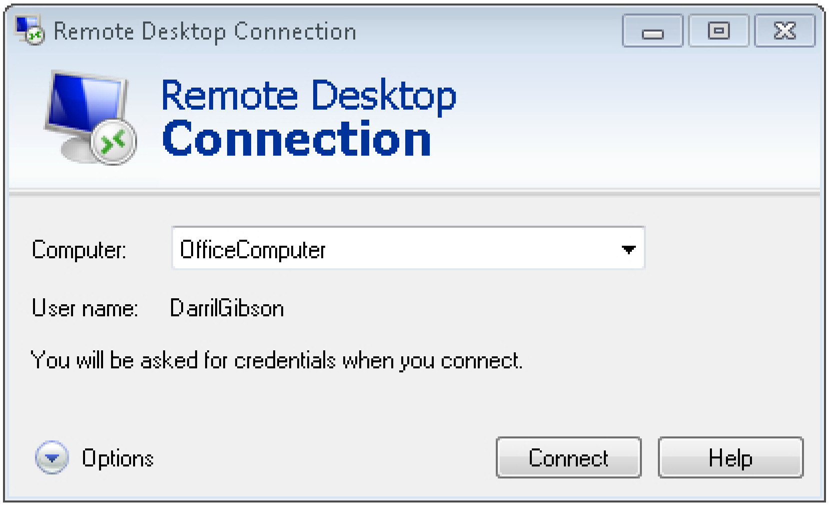
- **Remote Desktop Connection**. You can use this to connect to another system and log on. Administrators frequently use this to manage servers located in server rooms while they sit at a comfortable desk with a view out a window.
- **Remote Assistance**. This is used to provide assistance to other users. A novice can send out a remote assistance request, and a helper can use it to access the novice's computer from a remote location. If the novice grants permission, the helper can take control of the novice's computer and show how to accomplish specific tasks. As the helper moves the mouse and opens windows, the novice can view the activity. It even includes a chat window.

EXAM TIP

RDP uses port 3389. You need to ensure that this port is open on firewalls and routers between both systems. Otherwise, RDP traffic will be blocked.

Some users use RDP to access their home computers even when they're away. They enable port forwarding on their home router and configure it to allow the remote desktop session. Chapter 22 discusses port forwarding in more depth.

You can open Remote Desktop Connection on Windows 7 by clicking Start, typing in **mstsc**, and pressing Enter. You'll see a window similar to Figure 20-5. Type in the name of the computer you want to access, and if it's available and configured to accept remote desktop connections, you'll be prompted to enter a user name and password.



Computer: OfficeComputer

User name: DarrilGibson

You will be asked for credentials when you connect.

FIGURE 20-5 Using Remote Desktop Connection.

After you're connected, it works almost exactly like you just logged on while sitting in front of the computer. This can work with other computers besides your home computer. For example, you might be able to connect to your work computer from home. However, you should ensure that you're authorized to connect to the remote computer before trying. Additionally, ensure that you have permission to use RDP on a work computer before trying to use it to connect to a remote computer.

NOTE **MSTSC**

MSTSC is short for *Microsoft Terminal Services Connection*. Remote Desktop Services was previously called *Terminal Services*.

Telnet

Telnet is a command-line tool you can use to connect to remote systems. You can use this connection to execute commands through the telnet prompt. The default port used by Telnet is port 23. Telnet sends traffic in clear text making it easy for others to view the data with a sniffer. When security is needed, SSH is often used instead.

Technicians sometimes use Telnet for troubleshooting because it allows you to easily identify whether a system is listening and responding to traffic on a specific port.

For example, imagine a user is having problems with their email. You might want to verify that the email server (named mail2 in this example) is operational and listening for SMTP commands. You can enter the following command from the command prompt: **telnet mail2 25**.

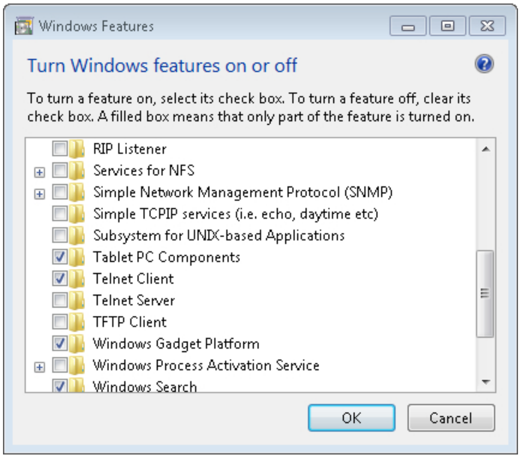
The command will attempt to connect to the email server by using SMTPS default port 25. If successful, you'll have a blank screen waiting for you to enter SMTP commands. This tells you that the email server is operational and listening on port 25. If the mail server is not running, you'll get an error.

EXAM TIP

Telnet uses port 23 by default. You can use it to connect to remote systems using different ports and enter commands on the remote system.

The Telnet Client is not enabled by default on Windows Vista or Windows 7. You can use the following steps to enable it:

1. Click Start and select Control Panel.
2. Type **Feature** in the Search Control Panel text box.
3. Select Turn Windows Features On Or Off. If prompted by UAC, click Continue.
4. Select the check box for Telnet client, as shown in the following graphic.



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ RIP Listener
- ⊞ □ Services for NFS
- ⊞ □ Simple Network Management Protocol (SNMP)
- □ Simple TCPIP services (i.e. echo, daytime etc)
- □ Subsystem for UNIX-based Applications
- ☑ Tablet PC Components
- ☑ Telnet Client
- □ Telnet Server
- □ TFTP Client
- ☑ Windows Gadget Platform
- ⊞ □ Windows Process Activation Service
- ☑ Windows Search

5. Click OK. After the feature is installed, you can close Control Panel and open a command prompt to use Telnet.

MORE INFO **CHAPTER 14, "USING THE COMMAND PROMPT"**

Chapter 14 covers the command prompt in greater depth, including how to open it. As with any command-line commands, you can get help on Telnet with the help switch. Type in telnet /?, and press Enter to view the help.

SNMP

Simple Network Management Protocol (SNMP) is used to communicate with and manage network devices such as routers and switches. There are three versions: SNMPv1, SNMPv2, and SNMPv3. SNMPv3 provides the highest level of security.

SNMP uses agents on each managed device. An agent is a software application that monitors a system for certain events (called traps) and reports them to a central SNMP monitoring system. The central system will often be running on a server within the network and it can send queries to SNMP agents.

LDAP

Lightweight Directory Access Protocol (LDAP) is used to interact with a special type of database called a directory. In this context, a directory has nothing to do with the folders used in Windows even though those folders are also called directories. Instead, a directory is a group of objects, such as users, computers, and groups, that are centrally managed and maintained.

For example, Microsoft uses Active Directory Domain Services (AD DS) to host all the objects within a domain. If a computer is joined to the domain, a computer object is created within AD DS. Similarly, when a user account object is created within AD DS, users can log in to the domain. LDAP is used to join computers to a domain, to log in users to accounts, and for any other type of interaction with AD DS.

✓ **Quick Check**

1. **What port must be opened to use Remote Desktop Connection?**
2. **What is the Telnet command to connect to an HTTP server named Web1?**
3. **What port does Telnet use by default?**

Quick Check Answers

1. 3389.
2. Telnet Web1 80.
3. 23.

Summarizing Well-Known Ports

The first 1024 ports (0 to 1023) are called the well-known ports. There are several ports in this range that you should memorize for typical on-the-job work and the A+ exams. Table 20-3 summarizes the most important ports.

TABLE 20-3 Some Well-Known Ports

Protocol	Port	Protocol	Port
FTP	20, 21	HTTP	80
SSH	22	POP	110
SSH Port Forwarding	22	IMAP	143
Telnet	23	HTTPS	443
SMTP	25	SSL	443
DNS	53	SMTPS	465
TFTP	69	IMAPS	993
RDP	3389	POP3S	995

Without an explanation of how they're used, ports can be fuzzy concepts for many people. Sure, you can remember that HTTP uses port 80 and that SMTP uses port 25, but how does this really fit together? The following sections provide an example scenario that will help put it into context.

Sending an HTTP Query Using Ports

Kelly is using Internet Explorer to do a search through Bing.com. Imagine that her ISP has assigned her system an IP address of 70.160.136.10 and the IP address of Bing.com is 65.55.175.254. When she enters a search on Bing through her web browser, her system will create a data packet and send it to the Bing web server.

This packet includes destination and source data. In addition to the source and destination IP addresses, it also includes source and destination ports. The IP addresses are used to get the packet the computer. The ports are used to identify what to do with the packet when it arrives.

The Web server is using HTTP, so the destination port is 80. However, the port used by Kelly's system as the source port isn't as simple.

You might remember from earlier in the chapter that ports 49152 through 65,535 are dynamic ports. Systems map these ports to applications when needed. In this example, Kelly's system will assign 49,152 to Internet Explorer. If 49,152 were already mapped to another application or service, Kelly's system would use a different port, such as 49,153 or 49,154. When the packet returns from Bing, this port number tells her system that the data should be handled by Internet Explorer.

Figure 20-6 shows what this outgoing packet would look like. Again, TCP/IP uses the destination IP address to get the packet to the destination computer. When it arrives, TCP/IP uses the port number to get it to the right service on the computer.

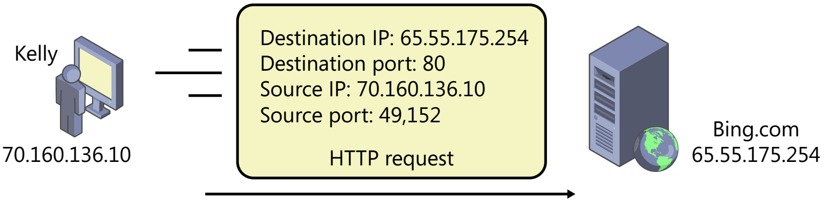


FIGURE 20-6 IP address and port information sent in a webpage request.

A Web Server Response Using Ports

The Bing server receives the packet with the destination port of 80. It knows that port 80 is used for HTTP, so it sends it to the application handling HTTP.

Bing uses Internet Information Services (IIS) as the web server application. IIS creates the webpage to answer Kelly's request. The bing.com server then readdresses the packet to Kelly's system by reversing the source and destination data.

Figure 20-7 shows the source and destination data for the response. It includes Kelly's IP address and the port of 49,152 as the destination, and it includes Bing.com's IP address and port 80 as the source. TCP/IP uses the IP address to get the packet to Kelly's computer.

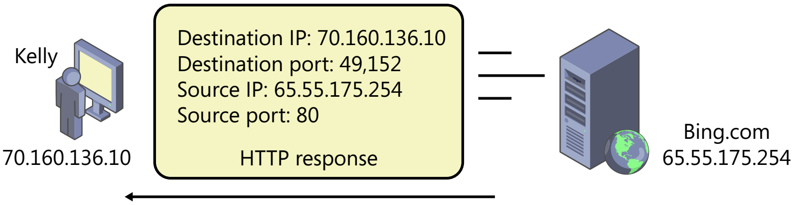


FIGURE 20-7 IP address and port information in the webpage response.

When the return packet arrives, Kelly's system knows that it mapped port 49,152 to Internet Explorer. It sends the HTTP response back to Internet Explorer, which displays the webpage.

NOTE **VIEW OPEN CONNECTIONS**

If you type *netstat -b* and press Enter at an elevated command line, you can see all of the current connections your system has open. (Chapter 14 explains how to open the command line with elevated permissions.) The -b switch will also identify the program or service using each of the open ports. If you have multiple Internet Explorer sessions open, you'll see several lines labeled with [iexplore.exe]. Close all Internet Explorer sessions, and rerun the command. You'll see that the connections are no longer there.

Last, it's worth mentioning that the well-known port numbers are the commonly used ports, but protocols can use different port numbers. You know that HTTP uses the well-known port of 80. If you type in www.bing.com as an address in Internet Explorer, it will actually use *http://www.bing.com:80*. Internet Explorer assumes this is an HTTP-based website and it assumes the default of port 80.

However, the bing.com administrators could configure their server using port 12345 for HTTP instead of port 80. Users would have to include the port number in order to reach the site like this: *http://www.bing.com:12345*. If a user typed in www.bing.com without the port of 12345, the browser would use the default port of 80 and the web server wouldn't respond.

Imagine if every website used a different port number. Not only would you have to remember the name of the website but also the port number. For most situations, it's best to use the well-known port number.

However, there are some times when different port numbers are used. Chapter 22 discusses proxy servers and how many companies use a single proxy server to provide shared Internet access to multiple users. Many proxy servers are configured to listen for HTTP queries on port 8080.

Chapter Summary

- Network protocols provide the rules that devices use to communicate with each other on a network.
- TCP/IP is a suite of protocols used on the Internet and on internal networks.
- TCP is a connection-oriented protocol that provides reliable, guaranteed delivery of data. TCP sessions begin with a three-way handshake.
- UDP is a connectionless protocol that gives a "best effort" to deliver data. It does not use a handshake but instead just sends the data.
- Ports are logical numbers used to identify protocols or services. Ports 0 to l023 are well-known ports.
- Encryption protocols scramble data so that is unreadable to unauthorized users. SSH encrypts traffic within a network such as FTP. SSH uses port 22. SSL and TLS encrypt traffic on the Internet.
- Common email protocols are SMTP, POP3, and IMAP4. Systems use SMTP to send email over port 25. Users receive email from POP3 servers over port 110. IMAP4 allows users to manage email on a server, and it uses port 143. Each can be secured with SSL or TLS.
- HTTP and HTTPS are used to transfer files displayed in web browsers. HTTP uses port 80. HTTPS uses encryption to protect the data, and it uses port 443.
- FTP is used to upload and download files from FTP servers. FTP uses ports 21 and sometimes port 20. TFTP is used for smaller files, and it uses port 69. SFTP uses SSH to encrypt FTP traffic, and it uses port 22.
- DNS maps names to IP addresses. Systems query DNS with a name of a computer, and DNS responds with an IP address. DNS uses port 53.

- RDP is used by Remote Desktop Connection and Remote Assistance. Remote Desktop Connection can be started with mstsc, and it allows users to connect to remote systems. RDP uses port 3389.
- Telnet is used to connect to remote systems from the command prompt. It can be used to check whether ports are open on remote systems.
- SNMP is used to manage network devices such as routers and switches.
- LDAP is used to interact with directories such as Active Directory Domain Services.

Chapter Review

Use the following questions to test your knowledge of the information in this chapter. The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the "Answers" section at the end of this chapter.

1. Of the following choices, what is a difference between TCP and UDP?
   - **A.** UDP provides guaranteed delivery, but TCP does not.
   - **B.** TCP provides guaranteed delivery, but UDP does not.
   - **C.** TCP is connection-oriented, but UDP does not use wires.
   - **D.** UDP uses a three-way handshake, but TCP does not.
2. Which of the following protocols is used to receive email by a user?
   - **A.** POP
   - **B.** SMTP
   - **C.** FTP
   - **D.** RDP
3. Which of the following protocols uses port 143?
   - **A.** IMAP
   - **B.** SMTP
   - **C.** POP
   - **D.** HTTPS
4. Which of the following are the correct ports for HTTP and HTTPS?
   - **A.** 22 and 25
   - **B.** 80 and 143
   - **C.** 80 and 443
   - **D.** 443 and 3389

5. What protocol could you use to encrypt FTP traffic?

   A. HTTPS

   B. TFTP

   C. RDP

   D. SSH

6. What service provides the IP address of a computer when queried with the name of the computer?

   A. FTP

   B. SMTP

   C. DNS

   D. SSL

7. What port should be opened on a firewall to allow a user to connect to a system using RDP?

   A. 69

   B. 143

   C. 443

   D. 3389

8. You are troubleshooting an email problem for a user. The mail server is named mail, and you suspect that it is not answering SMTP queries. Which of the following commands can you use from the command prompt to test it?

   A. SMTP mail 23

   B. SMTP mail 25

   C. Telnet mail 23

   D. Telnet mail 25

Answers

1. **Correct Answer:** B
   - **A. Incorrect:** UDP does not provide guaranteed delivery, but TCP does.
   - **B. Correct:** TCP provides guaranteed delivery, and UDP uses a best effort to deliver data.
   - **C. Incorrect:** TCP is connection-oriented and UDP is connectionless, but this does not refer to wires.
   - **D. Incorrect:** TCP uses a three-way handshake, but UDP does not.
2. **Correct Answer:** A
   - **A. Correct:** Post Office Protocol (POP) is used to receive email on port 110.
   - **B. Incorrect:** Simple Mail Transfer Protocol (SMTP) is used to send email on port 25.
   - **C. Incorrect:** File Transfer Protocol (FTP) is used to upload and download files from a file server, and it uses port 21.
   - **D. Incorrect:** Remote Desktop Protocol (RDP) is used to connect to remote systems, and it uses port 3389.
3. **Correct Answer:** A
   - **A. Correct:** Internet Message Access Protocol (IMAP) uses port 143.
   - **B. Incorrect:** Simple Mail Transfer Protocol (SMTP) uses port 25.
   - **C. Incorrect:** Post Office Protocol (POP) uses port 110.
   - **D. Incorrect:** Hypertext Transfer Protocol Secure (HTTPS) uses port 443.
4. **Correct Answer:** C
   - **A. Incorrect:** Secure Shell (SSH) uses port 22, and Simple Mail Transfer Protocol (SMTP) uses port 25.
   - **B. Incorrect:** HTTP uses port 80, but Internet Message Access Protocol (IMAP) uses port 143.
   - **C. Correct:** Hypertext Transfer Protocol (HTTP) uses port 80; Hypertext Transfer Protocol Secure (HTTPS) uses port 443.
   - **D. Incorrect:** HTTPS uses port 443, but Remote Desktop Protocol (RDP) uses port 3389.
5. **Correct Answer:** D
   - **A. Incorrect:** Hypertext Transfer Protocol Secure (HTTPS) secures webpages but not FTP traffic.
   - **B. Incorrect:** Trivial File Transfer Protocol (FTP) is a scaled down version of FTP, but it does not encrypt FTP.

   C. **Incorrect:** The Remote Desktop Protocol (RDP) is used to connect to remote systems, but it does not encrypt FTP.

   D. **Correct:** Secure Shell (SSH) can be used to encrypt network traffic including File Transfer Protocol (FTP) traffic.

6. **Correct Answer:** C

   A. **Incorrect:** File Transfer Protocol (FTP) is used to upload and download files to and from an FTP server.

   B. **Incorrect:** Simple Mail Transfer Protocol (SMTP) is used to send email.

   C. **Correct:** Domain Name System (DNS) maps computer names to IP addresses and answers name resolution requests.

   D. **Incorrect:** Secure Sockets Layer (SSL) is used to encrypt HTTPS, and it uses port 443.

7. **Correct Answer:** D

   A. **Incorrect:** Trivial File Transfer Protocol (TFTP) uses port 69 and is unrelated to RDP.

   B. **Incorrect:** Internet Message Access Protocol (IMAP) uses port 143 and is unrelated to RDP.

   C. **Incorrect:** Hypertext Transfer Protocol Secure (HTTPS) uses port 443 and is unrelated to RDP.

   D. **Correct:** Remote Desktop Protocol (RDP) uses port 3389, so this port needs to be opened on the firewall.

8. **Correct Answer:** D

   A. **Incorrect:** There is no such command as SMTP.

   B. **Incorrect:** There is no such command as SMTP.

   C. **Incorrect:** This command will check to see whether Telnet was running on the mail server, because it is using port 23.

   D. **Correct:** The telnet command can connect to a server on specific ports. You want to check the mail server, so you should check the SMTP service on port 25.