

Core TCP/IP Protocols

An important part of understanding networking is understanding networking protocols. TCP/IP is the primary protocol suite used in networks today, including the Internet. TCP and UDP are two important protocols that are integral to most networking communications, but there are many more.

This chapter presents many of the more popular protocols with a high-level overview of these protocols and their purpose. It's important to understand the basics of TCP and UDP, such as which one is connection-oriented and which is connection-less. However, you don't need in-depth knowledge of the common protocols other than understanding their primary purpose. Many common protocols also use specific ports identified as well-known ports. You should also have a good understanding of how ports work and the well-known ports used with specific protocols.

- ▶ **Understanding TCP and UDP**
- ▶ **Exploring Common Protocols**
- ▶ **Understanding Ports**

Understanding TCP and UDP

Transmission Control Protocol (TCP) and *User Datagram Protocol* (UDP) are the two primary protocols used to transport data across a network. They both operate on the Transport layer of the OSI Model, but they have distinctive differences.

The primary difference between these two is the delivery mechanism. TCP provides guaranteed delivery with acknowledgments, sequence numbers, and flow control. UDP provides best-effort delivery without a guarantee.

Chapter 3 introduced these two protocols with two important points:

TCP Is a Connection-Oriented Protocol TCP starts with an established session using a three-way handshake process. This three-way handshake ensures a connection is established before data is transmitted.

UDP Is a Connection-less Protocol UDP sends data using a best-effort method. It doesn't establish a session, so it doesn't provide guaranteed delivery.

The last section of this chapter covers ports in more depth. These TCP and UDP ports are an important element of application protocols.

Application protocols use TCP, UDP, or both to transfer application data. These protocols are identified using logical ports. For example, HTTP uses TCP port 80. When a system receives data using TCP port 80, it is processed as HTTP.

Exploring TCP

TCP provides guaranteed delivery by starting with the three-way handshake process shown in Figure 4.1. Imagine that Sally's computer wants to transfer information to Bob's computer. Before the data transfer starts, the computers establish a connection with each using this three-way handshake.

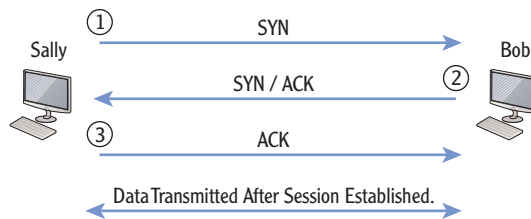


FIGURE 4.1 TCP handshake process

A flag is simply a single binary bit set to a 1. For example, the SYN flag is set by setting a specific bit in the packet to a 1.

Sally's computer starts by sending a packet with the *synchronize* (SYN) flag set. When Bob's computer receives the packet, it responds with another packet with both the SYN and the *acknowledge* (ACK) flags set. Sally's computer then completes the three-way handshake by sending a third packet with the ACK flag set.

At this point, both computers have an established session. They both have assurances that the other computer is operational and they are able to communicate with it. Data is then transmitted between the two computers after the session is established.

You can compare this to using different methods to get a message to a friend. One way is to make a phone call. This also uses a three-way handshake process, as follows:

1. Sally initiates the phone call to Bob.
2. Bob answers the call with "Hello, this is Bob." Sally recognizes Bob's voice and knows it's him.
3. Sally says "Hi. This is Sally." Bob recognizes Sally's voice and knows it's her.

Figure 4.2 illustrates the three steps of the phone call.

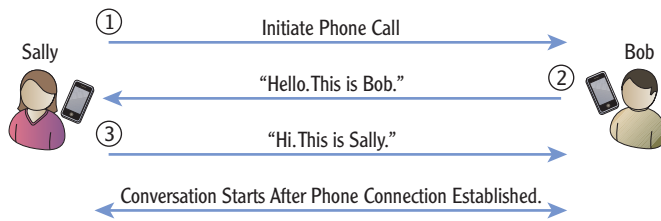


FIGURE 4.2 Phone call uses a similar handshake process

Admittedly, the phone call may not be so formal between two friends. With caller ID, Bob may recognize Sally right away and just say something like “Yo!” Still, the conversation doesn’t start until the phone connection is established.

Of course, in a conversation, both people talk. If you were talking to a friend, you’d expect your friend to occasionally acknowledge what you’re saying with agreement or comments. You can’t just talk for an hour without your friend saying anything back. At least I hope not! Instead, you pass on your information in separate pieces.

TCP also divides the data into smaller segments. For example, the data could be a 1 MB file. TCP could divide this file into 250 segments that are 4 KB. These 4 KB segments can travel over the network more efficiently than a single 1 MB file. TCP uses sequence numbers to track these segments.

When the data is segmented, each separate segment is assigned different sequence numbers such as 1 through 250. The receiving computer then receives each of these segments and uses these sequence numbers to put the data back together in the correct order.

However, the sending computer doesn’t just throw all of these segments onto the network and hope the other computer receives them. TCP coordinates this process between the two computers.

Imagine that Sally wants to download music from Bob’s computer. The TCP handshake process starts the process. Next, the two computers decide on how big the individual segments can be and how many segments can be sent between acknowledgments. The number of segments that can be sent at a time is the TCP sliding window.

Figure 4.3 shows the two computers with an established session. They have negotiated a segment size of 1500 bytes and a sliding window of 3. When Sally’s computer receives three segments, it verifies the data is intact and then sends an acknowledgment (ACK) message. Bob’s computer then sends three more segments.

If even a single bit is lost in the transmission, the data in the segment is no longer valid. TCP uses an error checking process called a *cyclical redundancy*

check (CRC). This CRC verifies the data is intact in each segment. If the three segments are received without errors, Sally's computer sends an ACK packet saying "Give me three more."

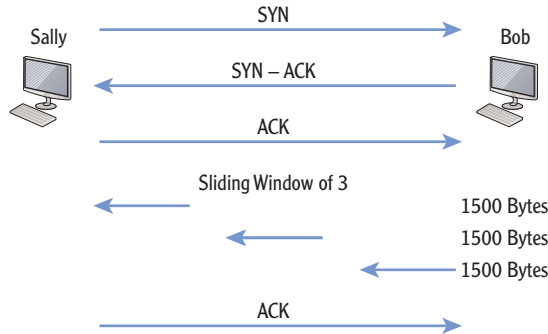


FIGURE 4.3 TCP sliding window

However, if any of the segments are missing or corrupt, Sally's computer sends a *negative acknowledge* (NACK) packet instead, requesting the missing or corrupt segment. If the sending computer receives a NACK, it retransmits the segments in the sliding window. Eventually, Sally's computer will receive all the segments and be able to reassemble them into the original MP3 file sent by Bob's computer.

Exploring UDP

UDP is a best-effort protocol. Delivery is not guaranteed like it is with TCP, but UDP will do its best to get data to its destination. UDP does not use a three-way handshake. It simply sends the data to the destination.

Imagine you have a message you want to get to your friend as soon as possible. You could call, but what if your friend doesn't answer? You could leave a message. You could send a text message. You could even send a letter through the regular mail. However, none of these methods provides any assurance that your message was received. Still, you are making a best effort to pass on the message, and these methods normally work.

This is exactly what UDP does. It makes a best effort to pass on messages, but it doesn't have any of the overhead of TCP. UDP doesn't use the TCP three-way handshake process to establish the session. It doesn't use periodic ACKs and NACKs to verify data was transmitted or request retransmissions of corrupt data.

A logical question comes to mind. If UDP is unreliable, why is it used? The reason is that some data doesn't need guaranteed delivery. In addition, some data transmissions are slowed down by the extra overhead required by TCP.

Because UDP doesn't use the guaranteed delivery mechanisms of TCP, it is referred to as unreliable. Also, it doesn't check for out-of-order messages.



For example, streaming media such as streaming audio, streaming video, and Voice over IP (VoIP) all use UDP. These methods frequently lose packets here and there, but the overall message is still received. Have you ever watched a video online? It may occasionally be jumpy or miss some of the audio. This is because UDP is used and some of the packets are lost. Still, you're able to get the overall message.

If TCP was used instead, the transmission would be a lot slower. If you needed to ensure that you received the full video, you may be able to download the actual video file, instead of having it streamed to you. The file download would use TCP, and the entire file would be intact.

Even though UDP does not verify a connection before sending data or include a check for out-of-order messages, it does validate the data. UDP does use a checksum similar to how TCP uses a checksum. The checksum can indicate to the receiving computer that the data has been modified (perhaps by just dropping a single bit) and isn't valid.

Exploring Common Protocols

TCP and UDP are primary protocols used for data transmission. However, several other protocols are important to understand. Chapter 2 introduced many of these protocols and listed the OSI layer where they operate. This section provides a deeper explanation of them.

The protocols used in this section are commonly used within Microsoft networks and/or on the Internet.

Address Resolution Protocol

The *Address Resolution Protocol* (ARP) uses broadcast transmissions to identify the Media Access Control (MAC) address of computers.

The IP address routes the traffic to the correct subnet. When the destination subnet is reached, the ARP protocol broadcasts the IP address to all computers on the subnet, as shown in Figure 4.4. This ARP broadcast asks, "Who owns this IP address?"

Each computer that receives the ARP broadcast looks to see whether it has the broadcasted IP address. If so, the computer responds with its MAC address.

When a computer resolves a MAC address using ARP, it stores it in a cache for two to ten minutes, depending on the operating system. If it wants to communicate with the computer again, it doesn't have to send another ARP broadcast to get the MAC address but instead retrieves it from cache.

The MAC address is also known as the physical address. It is expressed in hexadecimal characters such as 01-23-45-AB-CD-EF.



Cache is an area of memory used for short-term storage. Many applications and devices use cache.



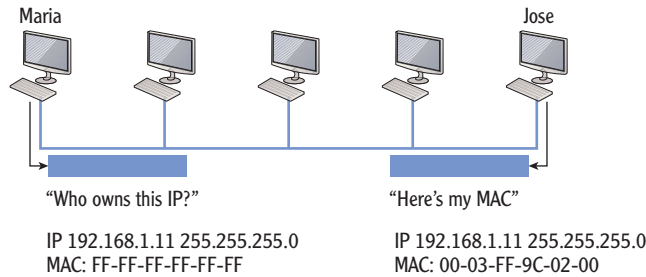


FIGURE 4.4 ARP translates the IP address to a MAC address.

These steps will work on a variety of Windows systems, including Windows 7 and Windows Server 2008.

The ARP protocol is part of the TCP/IP protocol suite, but there is also a command-line tool named `arp`. You can view the ARP cache from the command line by following these steps in a Windows system:

1. Click Start > Run.
2. Type `cmd` in the Run box, and press Enter.
3. At the command prompt, type `arp -a`, and press Enter.

Figure 4.5 shows the `arp` command (specifically `arp -a`) used to show the contents of the ARP cache.

```

Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>arp -a
Interface: 192.168.1.10 --- 0xa
 Internet Address      Physical Address      Type
 192.168.1.11         00-03-ff-9c-02-00    dynamic
C:\Users\Administrator>

```

FIGURE 4.5 Viewing the ARP cache

Hypertext Transfer Protocol

Hypertext Transfer Protocol (HTTP) defines how files on the World Wide Web (WWW) are formatted, transmitted, and rendered in web browsers. Figure 4.6 shows Internet Explorer accessing the site **bing.com**. The address bar shows the Uniform Resource Locator (URL) as **http://www.bing.com**.

Some sites use encryption to protect the data transmission. For example, if you purchase something over the Internet, you’ll provide information such as your name, address, and maybe credit card data. This needs to be protected as it goes over the Internet. HTTP over Secure Sockets Layer (SSL), or HTTPS, provides this protection.

HTTP is different from Hypertext Markup Language (HTML). HTML is the Internet standard for formatting and displaying documents on the Internet.

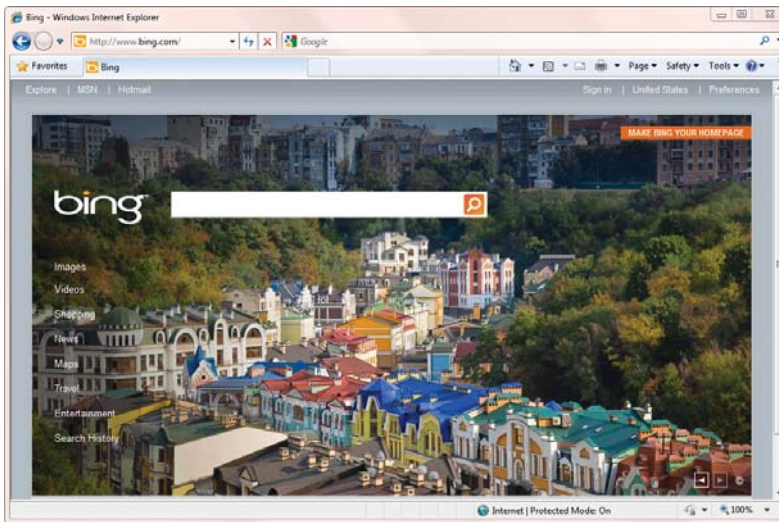


FIGURE 4.6 Web browser accessing a web page with the URL

You can tell whether HTTPS is being used from the URL. Instead of HTTP, it will list it as HTTPS. Additionally, most web browsers include a lock icon somewhere on the page. For example, Internet Explorer 8 shows a lock icon at the end of the URL.

If HTTPS is not in the URL or the lock icon is not displayed, information you enter and submit to websites can be intercepted and read by eavesdroppers on the Internet.

HTTP uses TCP port 80 by default. HTTPS uses TCP port 443.

File Transfer Protocol

File Transfer Protocol (FTP) is used to upload and download files to and from computers on the Internet and within some internal networks. FTP uses TCP for guaranteed delivery of the files.

You can access FTP from the command prompt from many operating systems such as Windows 7. Get commands can download files, and Put commands upload files. Windows Explorer provides some basic FTP functionality including drag-and-drop features. However, there are applications that make the process much simpler. Figure 4.7 shows an FTP application named FileZilla, which is available for free. It's easy to use and can manage the upload and download of multiple files at a time.

Encryption protocols scramble data from plain text into cipher text. Nonauthorized users are not able to read the cipher text.

Many FTP clients are freely available. You can search on the Internet for *download free ftp* to find others.

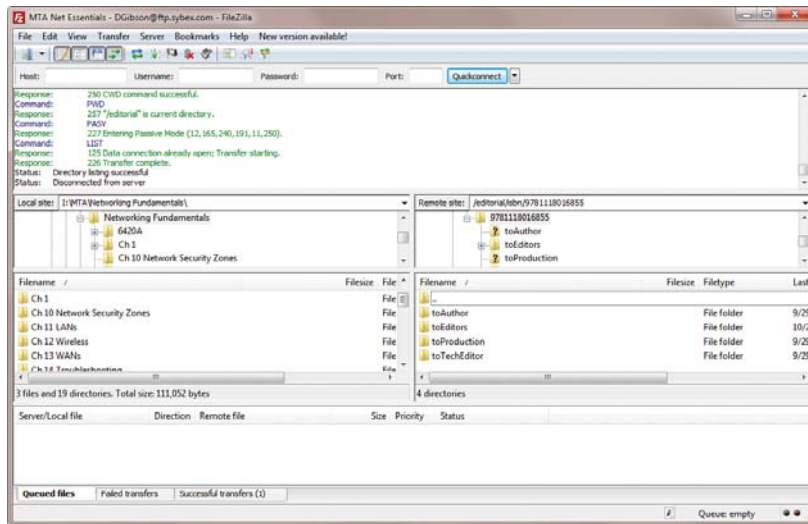


FIGURE 4.7 Using FileZilla to upload and download files

In the figure, a publisher is hosting a website used by authors, editors, and graphics artists to upload and download files to collaborate on a book. The contributors on the book can be located around the world yet share their files as easily as if they worked side by side.

FTP clients such as FileZilla allow you to browse the folders on the destination computer. You can then pick what files you want to upload or download. Most FTP clients allow you to simply right-click a file and select to upload or download depending on what you're trying to do.

Most FTP servers require you to have an account with a password before you can upload files. This prevents malicious users from filling the FTP server with unwanted data. Additionally, FTP sites can limit permissions so that accounts can open and upload files only to certain folders but not others.

However, many FTP servers allow you to download data anonymously. You can use an account name of “anonymous” and then use an email address as a password. The email address is not verified to determine whether it's real, but it is often checked to ensure it's in the format of an email address. For example, `d@g.com` is a valid format for an email address but it isn't an actual email address. You could use `d@g.com` as a password for some FTP servers.

Trivial File Transfer Protocol

Trivial File Transfer Protocol (TFTP) is a scaled-down version of FTP. TFTP uses UDP as its transport protocol, which reduces overhead and keeps traffic to a minimum. In contrast, FTP uses TCP, providing guaranteed delivery of the files.

Network administrators often use TFTP when transferring configuration files to network devices such as routers and switches. TFTP should not be used to communicate with FTP servers on the Internet because of its lack of data security features.

Telnet

Telnet is a command-line interface that allows bidirectional communication with network devices and other systems on the network. As a command-line interface, all commands are typed at a command prompt instead of using point-and-click methods within a Windows graphical user interface (GUI).

One of the benefits of Telnet is that it allows terminal emulation. In other words, you can connect to a Telnet server remotely, and it acts as though you are sitting right in front of the server accessing the local terminal. Telnet sessions include a Telnet server, a Telnet client, a Telnet window on the client (usually a command prompt) for issuing commands and viewing data on the server, and the Telnet protocol that transfers the commands between the two.

Remote Desktop Services

Microsoft Windows servers include *Remote Desktop Services* (RDS) as an additional role. An RDS can host applications or entire desktops that are accessible to users on the network.

For example, a client with limited processing power could connect to an RDS server and run Windows 7 from the server. Even though the Windows 7 desktop is running on the server, the end user has full access to all of the Windows 7 capabilities on the older computer.


Similarly, a user running Windows 7 system might need to run a legacy application that is not compatible with Windows 7. The RDS server could host the application, and the user could then run the application from the server without having any compatibility problems.

Telnet is widely recognized as insecure since it transmits traffic in clear text. Secure Shell (SSH) has replaced Telnet in many applications.

RDS was previously known as Terminal Services. Its name changed to RDS with Windows Server 2008 R2.

RDS uses the *Remote Desktop Protocol*. This is the same protocol used by Windows 7 for Remote Assistance. Remote Assistance allows a help-desk professional to take control of an end user's desktop (with permission) and provide assistance. RDS uses TCP port 3389.

Secure Sockets Layer

 The current version of SSL is 3.0, which was released in 1996.

SSL is an encryption protocol used for a wide assortment of purposes. As mentioned previously, SSL protects HTTP as HTTPS. SSL provides security in several key areas:

Confidentiality Secret data is protected from unauthorized disclosure through encryption. SSL encrypts data into cipher text to ensure that secret data remains secret.


Integrity Unauthorized users should not modify data. If they do, the data loses integrity and can no longer be trusted as valid. SSL helps ensure integrity by checking the data at different points to ensure it has not been modified.

Authentication Users and computers need to prove who their identity. Based on their identity, access is granted or denied based on access controls such as permissions. However, the first step is authentication.

SSL uses digital certificates for confidentiality, integrity, and authentication. The digital certificate is a file that includes data used to encrypt the data for confidentiality. It also includes basic information to prove the identity of the certificate holder.

In recent years, many VPNs have emerged using SSL as a tunneling protocol. SSL-based VPNs have the advantage of being able to be used via a web browser rather than requiring a separate VPN client program.

Transport Layer Security

 TLS has been upgraded. RFC 5246 defined TLS version 1.2 in August 2008.

Transport Layer Security (TLS) is another security protocol, similar to SSL. It can also provide confidentiality, integrity, and authentication. RFC 2246 defined TLS in 1999, and TLS is designated as a replacement for SSL.

It's interesting to note that even though TLS came out more than 10 years ago as a replacement to SSL, it still hasn't replaced it. SSL is still going strong. Part of the reason for this is that SSL is a strong security protocol.

DIGITAL CERTIFICATES, PKI, AND CAs

In the simplest terms, a digital certificate is just a file stored on a computer. However, this file has a lot of support behind it. Specifically, a Public Key Infrastructure (PKI) includes several elements to support digital certificates.

One of the core elements of a PKI is a certificate authority (CA). A CA is an organization or a service that issues, manages, and validates digital certificates. Many CAs operate on the Internet, and CAs can also operate on internal networks. If an entity (such as a user or computer) needs a certificate, the entity proves their identity to the CA and provides other information (and often money). The CA then issues a certificate.

This certificate helps verify the entity's identity and helps with other uses such as encryption and integrity. When the certificate is presented to a third party, the third party can then query the CA to verify the certificate is valid.

For example, a website can purchase a certificate from a CA. When a user application (such as Internet Explorer) visits the website, the certificate is passed to the application. The application then queries the CA to verify the certificate is still valid. If so, a secure HTTPS session is created using data from the certificate.

Several protocols can use either SSL or TLS for security. For example, the Lightweight Directory Access Protocol (LDAP) can use either TLS or SSL for security.

Secure Shell

Secure Shell (SSH) is an encryption protocol that creates a secure encrypted session that can be used by other protocols. For example, SFTP is FTP encrypted with SSH. SSH has replaced Telnet in many applications. Telnet transfers data in clear text, while SSH encrypts the data. SSH is more secure than Telnet and more suitable for use on the Internet.

PuTTY (pronounced *putty*) is an example application built on SSH. PuTTY is a free terminal emulator program that encrypts traffic with SSH. Many administrators use PuTTY to manage network devices such as routers and switches.



LDAP is presented later in this chapter.



PuTTY isn't an acronym. It's just a way of capitalizing the name that stuck.

Internet Protocol Security

Internet Protocol Security (IPSec) is another encryption protocol used to encrypt traffic traveling over a network. IPSec provides two primary services:

Authentication IPSec uses an authentication header (AH) to prove the identity of the sender. This provides assurances to the computer receiving the traffic that it was sent by a known computer.

Encryption IPSec uses Encapsulating Security Protocol (ESP) to encrypt traffic. Only authorized users or computers are able to decrypt and read the traffic.

IPSec also provides integrity. The receiving computer is assured that the data was not changed in transit.

Both IPv4 and IPv6 support IPSec. It uses one of two modes:

Tunnel Mode IPSec encrypts the entire IP packet (both data and headers). It encapsulates the original encrypted packet within another IP packet and then sends it across the network. Virtual private networks (VPNs) use tunneling to protect the data. The L2TP/IPSec tunneling protocol is one of the popular VPN protocols.

Transport Mode Only the data is encrypted instead of the entire packet. The source and destination data (such as the IP addresses) within the packet are not encrypted. Transport mode is commonly used to encrypt data within internal networks.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is the primary protocol used to deliver email over the Internet and within internal networks. Email servers use SMTP to send and receive email between each other. Additionally, user systems use SMTP to send email to SMTP servers.

Figure 4.8 shows how SMTP is commonly used. You could be using an email application such as Microsoft Outlook. This allows you to connect with an email server to send your email. The email server receives the email and then sends and receives email with other email servers.

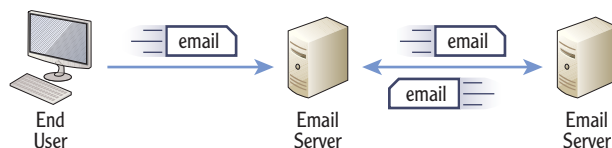


FIGURE 4.8 SMTP used to send and receive email

▶
Many organizations use Microsoft Exchange Server for email services. Exchange typically runs on a dedicated server.

Of course, this brings up a question. If SMTP is used to send email to the server from the end user's computer, how does the end user receive email? Glad you asked.

It depends, but the two common ways that end user's receive email are via a Post Office Protocol (POP) server or an Internet Message Access Protocol (IMAP) server. POP and IMAP are discussed in the next two sections.

Post Office Protocol v3

Post Office Protocol v3 (POP3) is a common protocol used to retrieve email from an email server. The current version is POP3.

As an example, you may use Microsoft Outlook (or another email client) for email at a home computer. You connect to the Internet via an Internet service provider (ISP), and the ISP provides you with email access. When you first configure your email client, you configure it with the name of the POP3 server and the address of an SMTP server. Your computer sends email using the SMTP server, and it receives email using the POP3 server.

The ISP's POP3 server receives email addressed to you and stores it there until you connect to the Internet and contact the server. When you connect to the server, it will then send all your email to your computer. Once your computer receives this email, it's typically removed from the POP3 server.

◀ The POP3 server can be the same server hosting SMTP. They don't have to be separate servers. This is common on smaller networks hosting both SMTP and POP3.

Internet Message Access Protocol

Internet Message Access Protocol (IMAP) is another popular email protocol. It is more commonly used on internal networks rather than on the Internet. The current version is IMAP4.

The primary difference between POP3 and IMAP4 is that messages are not automatically downloaded to the client, and they can be retained on the server with IMAP4. An IMAP4 server allows users to view email message headers individually. They can then choose which email to open. For example, if a user is connected with a slow connection, they can choose to postpone opening an email with a large attachment.

Since messages can be retained on the IMAP server, users can access the server from any computer in the network and still have access to the same email. This is different from a POP3 server that downloads the messages to the user's computer when they connect. With a POP3 server, if they access the server with a different computer, the older messages are no longer on the server.

IMAP is useful for workers who roam the network and don't have a single computer they use all the time. The worker can connect to the IMAP server from any computer and access email on the server.

◀ Messages don't have to be retained on the IMAP server. They can be configured so that email is deleted after it is downloaded.

IMAP also gives users the ability to manage their email in folders. When the email is retained on the IMAP server, users can move email into different folders based on their preferences.

Lightweight Directory Access Protocol

RFC 4510 defines the latest version of LDAP, which is LDAP version 3.

Lightweight Directory Access Protocol (LDAP) is the protocol used to query directories such as Microsoft's Active Directory Domain Services (AD DS). LDAP is derived from the Directory Access Protocol (DAP), which is part of a larger standard known as X.500.

It's easy to confuse the term *directory* since it has two meanings with computers. A directory can be a domain directory in the context of LDAP. A directory can also be a folder on a disk drive, which has nothing to do with LDAP.

Domain Directory A domain directory is a database of objects such as users, computers, and groups. Administrators use the domain to manage users and computers. Figure 4.9 shows Active Directory Users and Computers (ADUC) for a domain named Wiley.com. The Servers organizational unit is selected, and you can see several servers within the domain. Administrators use ADUC to manage the domain, and ADUC uses LDAP to query the AD DS database.

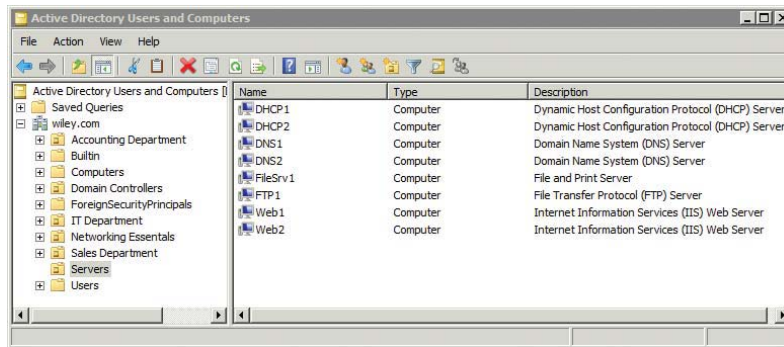


FIGURE 4.9 Active Directory Users and Computers

Disk Drive Folders You can explore Windows disk drives with Windows Explorer. Drives have folders that are also called *directories*. These folders have nothing to do with LDAP. Instead, these folders or directories are only on disk drives.

Although LDAP is integral to a Microsoft domain, it is also used in other non-Microsoft domains. Its purpose is the same, though. LDAP allows individuals to query the directory to locate and manage resources within the domain.

By default, LDAP transmits data across the network in clear text. Tools such as protocol analyzers or sniffers allow people to capture this data and read it. This is commonly known as *eavesdropping* and is similar to a person listening in on another person's private conversation.

Secure LDAP (SLDAP) uses SSL or TLS to prevent attackers from using sniffers to capture the data. Additionally, secure LDAP uses digital certificates for authentication. This ensures that computers communicating with each other with secure LDAP prove their identity prior to transferring data to each other.

LDAP uses TCP port 389 by default. SLDAP uses TCP port 636.

Kerberos

Kerberos is the primary authentication protocol used within a Microsoft domain and is managed as part of Active Directory. It was developed at the Massachusetts Institute of Technology and is used in other non-Microsoft domains.

The name Kerberos comes from Greek mythology. Kerberos was the three-headed dog that guarded the gates of Hades. Instead of guarding Hades, Kerberos is now helping to guard the secrets within Active Directory.

Kerberos uses a complex process of issuing time-stamped tickets to users after they log on. In simple terms, user accounts present these tickets when they try to access resources such as a file or folder. If the tickets are valid, access to the resource is granted. This is similar to you purchasing a ticket to watch a movie. If you have the ticket, you can get in. If not, access is blocked.

These Kerberos tickets need to be protected so that only specific user accounts can use tickets issued to them. Kerberos uses symmetric cryptography to encrypt the tickets.

Kerberos uses TCP port 88 by default.

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) is a VPN protocol. It provides a secure connection over a public network such as the Internet. PPTP is primarily used in Microsoft networks.

The Point-to-Point Protocol (PPP) is used for dial-up networking. PPTP extended PPP to make it useful for VPNs. The Microsoft Point-to-Point Encryption (MPPE) protocol encrypts the PPTP traffic. PPTP uses port 1723.

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) is another tunneling protocol used with VPNs. It's a combination of the Layer 2 Forwarding (L2F) protocol from Cisco and PPTP

Authentication is used to prove identity. For example, a user could provide a username and password to authenticate within a domain.

from Microsoft. However, L2TP is a standard used by more than just Cisco and Microsoft. IPsec is used with L2TP (as L2TP/IPsec) to provide security for the VPN connection.

L2TP uses UDP port 1701 by default.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a management protocol used to manage network devices such as routers and switches. Many different applications are available that use SNMP.

One way this is done is by installing SNMP agents on the network devices. The SNMP agents detect when specific events occur and generates a trap message to report back to a primary server to collect the information. Microsoft's System Center Operations Manager (SCOM) is an example of a server application used to monitor the health of devices on the network.

SNMP uses UDP port 161 by default. Since most of the traffic is diagnostic in nature to check the health of the devices, the guaranteed delivery of TCP is not required.

Internet Group Multicast Protocol

Internet Group Multicast Protocol (IGMP) is used for multicast transmissions. As a reminder, unicast transmissions go from one computer to one other computer. Broadcast transmissions go from one computer in a subnet to all other computers in a subnet. Multicast transmissions go from one computer to a select group of other computers.

There is a specific range of multicast addresses known as Class D addresses. Valid multicast addresses are in the range of 224.0.0.0 through 239.255.255.255. IGMP is used with IPv4. IPv6 uses other methods for group multicasting.

Multicasting is commonly used for audio and video transmissions, including different types of video teleconferencing. One computer creates the multicast session using a valid multicast IP address. Other computers can then join the multicast group.

Internet Control Message Protocol

Internet Control Message Protocol (ICMP) is a core protocol used to send error messages. Operating systems use ICMP to communicate the availability or unavailability of services. Additionally, troubleshooting tools such as Ping, PathPing, and TraceRt use ICMP to transfer data. ICMP functions at the Network layer of the OSI model and IP directly.

If you've ever attended a seminar on the Web, or a webinar, then you've probably used IGMP.



Chapter 14 covers several troubleshooting tools including Ping, PathPing, TraceRt, and more.



Understanding Ports

Both TCP and UDP use logical port numbers to identify the contents of a packet. These port numbers help TCP/IP get the packet to the application, service, or protocol that will process the data once it arrives at the computer.

As an example, consider a home user who uses an ISP for access to the Internet including email. The user uses Microsoft Outlook to send and receive email, and Microsoft Outlook has been configured with the IP address of both an SMTP server and a POP3 server, as shown in Figure 4.10.

As a reminder, the IP protocol uses the IP address to get the packet from one computer to another over a network.

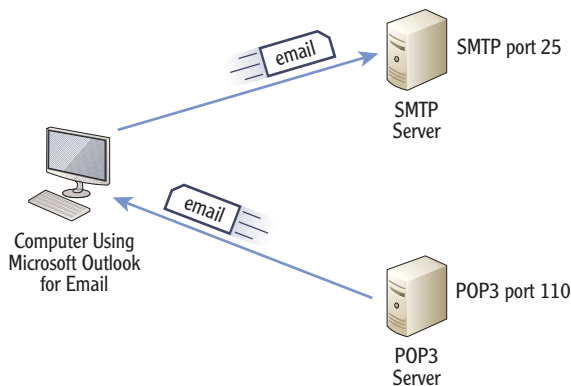


FIGURE 4.10 Using ports to send and receive email

Sending and receiving email are two separate processes. The following steps outline the process for sending SMTP email:

1. The client computer sends the email to the SMTP server with a destination port number of 25.
2. The client computer assigns itself a random unused source port number, such as 49152, and maps it to Microsoft Outlook for SMTP.
3. When the SMTP server receives the data from the client, it recognizes the destination port 25 as SMTP. It then forwards the data to the service handling SMTP.
4. After the email is received, the server sends back an acknowledgment to the computer using port 49152 to confirm the email was received.
5. When the computer receives the packet with port 49152, it sends it to the Microsoft Outlook application. Outlook then moves the email from the Outbox to the Sent folder.

A similar process is used when the computer wants to download email from the POP3 server:

1. The computer sends a request to the POP3 server with a destination port number of 110.
2. The computer assigns itself a random unused source port number, such as 49153, and maps it to Microsoft Outlook for POP3.
3. When the POP3 server receives the request, it recognizes the destination port 110 as POP3. It then forwards the request to the service handling POP3 requests.
4. The POP3 server then sends email to the client using port 49153.
5. When the computer receives the data with port 49153, it sends it to the Microsoft Outlook application. Outlook then moves the email into the Inbox folder.

While the preceding steps showed the process for SMTP and POP3, similar processes are used for many different applications. The IP address gets the packet to the destination computer. The port is then used to get the packet to the correct applications, service, or protocol on the target computer.

There are a total of 65,536 TCP ports and 65,536 UDP ports. *The Internet Assigned Numbers Authority (IANA)* assigns port numbers to protocols. It has divided the ports into different ranges, as shown in Table 4.1. You can view a list of all ports assigned by IANA at www.iana.org/assignments/port-numbers.

IANA also oversees the assignment of public IP addresses on the Internet.

TABLE 4.1 Port ranges for well-known, registered, and dynamic ports

Port names	Port numbers	Comments
Well-known ports	0 through 1023	These ports are associated with specific protocols or applications. Ports and protocols in the well-known port range are registered with IANA.
Registered ports	1024 through 49,151	Some of these ports are registered with IANA for specific protocols, but this is not required. Computers can assign unused ports in this range for applications.
Dynamic ports	49,152 through 65,535	These ports are not registered with IANA and may be used for any purpose.

Controlling Port Traffic with a Firewall

In addition to using ports to get packets to the right protocol, application, or service, ports are also used to control traffic in a network. Firewalls can block traffic based on the TCP or UDP ports they are using.

For example, consider a network that wants to prevent any FTP traffic from being used on the network. FTP uses ports 20 and 21. Figure 4.11 shows how a firewall can block FTP traffic. If the firewall receives any packet with either a source or destination port of 20 or 21, the firewall simply doesn't route the packet.

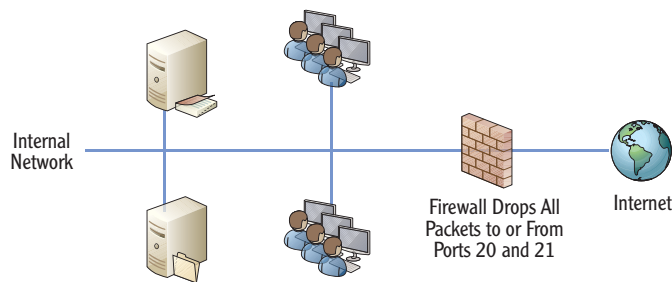


FIGURE 4.11 Using a firewall to block traffic based on ports

Mapping Internally Used Ports and Protocols

Microsoft networks use several different ports and protocols on internal networks. You should have a good understanding of what these ports and protocols are, as shown in Table 4.2. Most protocols use either TCP or UDP, but some (such as DNS) use both.

TABLE 4.2 Commonly used ports

Port	TCP or UDP	Protocol	Comments
20, 21	TCP	FTP	File Transfer Protocol.
22	TCP	SSH	Secure Shell.
23	TCP	Telnet	Can be secured with SSH.
25	TCP	SMTP	Simple Mail Transfer Protocol. Used to send email.
110	TCP	POP3	Post Office Protocol. Used to receive email.

(Continues)

Chapter 10 covers DNS along with other name resolution methods. Name resolution resolves computer names to IP addresses.

TABLE 4.2 (Continued)

Port	TCP or UDP	Protocol	Comments
143	TCP	IMAP4	Internet Message Access Protocol. Used when email stored on server.
80	TCP	HTTP	Hypertext Transfer Protocol. Used for web pages.
443	TCP	HTTPS	Secure HTTPS. Commonly uses SSL for security.
53	TCP/UDP	DNS	Domain Name Service. Used to resolve names to IP addresses.
88	TCP	Kerberos	Primary authentication protocol used by Active Directory.
389	TCP	LDAP	Lightweight Directory Access Protocol (LDAP). Language used to communicate with Active Directory.
636	TCP	SLDAP	Secure LDAP. Uses SSL or TLS to encrypt LDAP communications.
161, 162	UDP	SNMP	Simple Network Management Protocol. Used to manage network devices such as routers and switches.
3389	TCP	Remote Desktop Services	Remote Desktop Services are used for remote assistance and remote desktops in a Microsoft network.
1723	TCP	PPTP	Point-to-Point Tunneling Protocol. Used in VPNs.
1701	UDP	L2TP	Layer 2 Tunneling Protocol. Used in VPNs.

One of the primary reasons you need to know the ports is for configuring firewalls. You can create firewall rules or exceptions to allow or block the traffic based on the port. Firewall administrators have these ports memorized.

THE ESSENTIALS AND BEYOND

TCP and UDP are two primary protocols used to transport data across networks. TCP is connection-oriented and provides guaranteed delivery. UDP is connection-less and uses a best-effort delivery method. Many other application protocols are used within TCP/IP for a wide variety of purposes including email, web pages, encryption, interaction with Active Directory, and more. Application protocols use logical TCP and UDP ports for identification. IANA designates the port numbers for specific applications, and the first 1024 ports are known as well-known ports.

ADDITIONAL EXERCISES

- ▶ Draw the handshake process used by TCP.
- ▶ List two protocols used within a Microsoft domain with Active Directory.
- ▶ View the ARP cache.
- ▶ List the ports used by the three email protocols.

To compare your answers to the author's, please visit www.sybex.com/go/networkingessentials.

REVIEW QUESTIONS

1. Which of the following protocols is considered connection-oriented?

A. UDP	C. ARP
B. TCP	D. DHCP
2. True or false. UDP traffic accepts the loss of some data.
3. What type of traffic commonly uses UDP? (Choose all that apply.)

A. Streaming audio	C. HTTP traffic
B. Streaming video	D. Voice over IP
4. What is used to resolve an IP address to a MAC address?

A. DNS	C. ARP
B. TCP	D. ICMP
5. List three commonly used protocols for email.
6. L2TP is one of many tunneling protocols used for VPNs. What is used to encrypt L2TP traffic?

(Continues)

THE ESSENTIALS AND BEYOND *(Continued)*

7. The _____ protocol is used to manage multicast transmissions.
8. What port is used by RDS?
 - A. 389
 - B. 636
 - C. 1701
 - D. 3389
9. What port is used by LDAP?
 - A. 25
 - B. 389
 - C. 1723
 - D. 3389
10. What port is used by Kerberos?
 - A. 25
 - B. 80
 - C. 88
 - D. 443