Networking 101

What's the definition of networking? Have you ever wondered just how all of the network connections work, or what it takes to set up your own network? This networking tutorial will walk you through tasks associated with setting up and maintaining a network. You'll learn about networking software, networking security concepts and technologies and learn how to set up a common server.

Lessons

1. Networking definitions: terms, concepts and technologies
   This lesson helps you to understand what a network is, how it works,and what kinds of technologies play a role in networked communications. You'll build on this foundation in all of the lessons that follow.
2. Understanding networking software
   This lesson explores networking software operating systems and how they provide communication across the network. You'll also look at client versus server operating systems, and how applications share data.
3. Connecting a wireless network
   Whether wired or wireless, every network uses some type of layout and requires addresses to connect to and communicate with other devices. This lesson covers basic network layout and design, network addressing and access and more.
4. Network tutorial: working with servers
   In this lesson, you'll delve into server setup and management and learn about different uses for servers. Next, you'll determine which factors will help you make a wise decision about whether to host your own services or have someone else do it.
5. Managing network security
   In this lesson, you'll learn what it takes to properly maintain a wired or wireless network. You'll learn about network performance optimization, how to make sure your network is secure and how to establish a network maintenance routine.
6. Troubleshooting: a networking toolkit
   This final lesson helps you understand how to identify and address common problems that affect a network. You'll learn how to effectively troubleshoot issues so your network stays healthy.

Networking definitions: terms, concepts and technologies

This lesson helps you to understand what a network is, how it works,and what kinds of technologies play a role in networked communications. You'll build on this foundation in all of the lessons that follow.

Welcome to Networking 101!

This class offers a primer on basic networking, and explores the hardware, software, and protocols whereby one computer communicates with another across any number of intermediate links between them. You begin with an introduction to key networking terms, concepts, and technologies, and then move on to understand networking software in more detail, particularly where operating system capabilities come into play. Later lessons focus on how to connect PCs to a network, using network cables and wireless technologies. You'll also learn about networking a printer, wired and wireless networking security, troubleshooting network problems, and other computer networking solutions.

This class is for SMB (small- to medium-size business) professionals without a significant technology background.

»Compaq Presario CQ50Z series

With thin lines, a cool touchpad design, and a sleek, touch-control panel, this 7.0 lb., 15.4" laptop PC redefines simplicity. In addition to being ultra stylish,

What to expect in the class

This class covers important technologies related to networking, related elements that anybody should keep in a networking tool kit, and techniques whereby you can create a working network and keep it running smoothly. Along the way, you'll have the opportunity to dig more deeply into the covered topics by working through the accompanying assignments and quizzes.

Here's a summary of the lessons:

- Lesson 1: Covers key terms and concepts, plus important hardware and software technologies involved in connecting PCs to and using computer networks.
- Lesson 2: Explains networking software in more detail, including key components that supply network access, network communications, and network intelligence and capability.
- Lesson 3: Delves into how networks are laid out, and which kinds of information are necessary for a computer to communicate with other devices on a network.
- Lesson 4: Explores what's involved in working with servers, including their setup, management, and how servers are most commonly put to use.
- Lesson 5: Covers two vital areas of great networking concern -- network management and networking security.
- Lesson 6: Explains what to do when trouble occurs on a network, and describes basic troubleshooting skills and routines.

Beyond the lessons, complete the assignments and quizzes. When you're done with them, visit the message board. It's the perfect place to discuss class topics and swap questions and comments with classmates and your instructor.

Take a few moments to meet your instructor and fellow students on the class message board and let them know a little about you.

Now it's time to get started with the topics in Lesson 1.

Understanding basic networking principles

Why do we have networks? Networks were developed to enable people to share information and devices. A network is a group of computers and other devices that can communicate with one another to share information. This can range from two home computers connected by a single cable to the most complex network that includes many computers, cables, and devices spanning multiple time zones or continents.

When computers can communicate with each other, they can share resources. These resources can be:

- Data: This includes documents or spreadsheets, and applications such as Microsoft Word or Microsoft Excel, which you use to create files.
- Hardware: This includes printers, scanners, and other devices.

A computer that's not connected to another computer is called a standalone computer, shown in Figure 1-1. A standalone computer doesn't communicate or share resources with any other computer on a network.

the PCs in the Presario CQ50Z series are durable, powerful, and value-priced.

»Wireless network adapters

Securely add wireless LAN connectivity through your existing USB port with USB network adapters.

»HP Pavilion Elite PCs

The next generation of home entertainment; access TV, movies, music and photos, when and how you want.

»Desktop PC accessories

From software and storage to cables, mice, and keyboards,

Figure 1-1: A standalone computer with an attached printer.

all the accessories you need for your HP desktop PC are available to make your desktop experience more personal, powerful, and attuned to your specific needs.

To share files on a standalone computer with another computer, you can transfer the files onto a CD, DVD, or flash drive, and then load them onto the other computer. This is known as a sneakernet. The name stems from the fact that you have to walk the files back and forth between the two computers to transfer them from one to the other. A better method is to connect the computers, either with a cable (wired) or wirelessly, to form a simple network. Figure 1-2 illustrates a simple wired network with two computers that can share information and a printer.

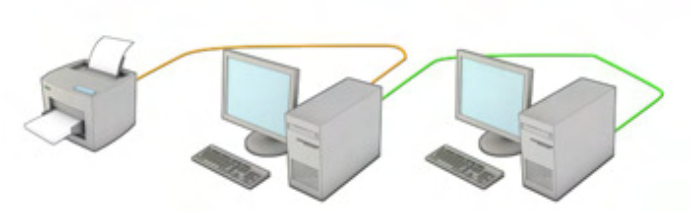


Figure 1-2: A simple wired network.

For these two computers to be able to share information, each computer must have an operating system with networking capabilities, some type of connection (in this instance, a physical cable), and a common method or protocol both use to communicate. Let's define some of these terms a bit further.

An NOS (network operating system) is an operating system designed with built-in services that enable sharing to take place. The devices on a network require a network interface to connect to each other, whether wired or wireless. You'll sometimes hear this called a network card, network adapter, or the most commonly, a NIC (network interface card). Before a network interface may be used, a software or device driver must be installed on the computer. A driver is a small program that communicates between the operating system and a device, as illustrated in Figure 1-3.

Although many PCs include network interfaces built right into the motherboard, thus eliminating the "card" portion, the term NIC remains a widely used synonym for network interface.

Figure 1-3: A driver enables a device to communicate with an operating system.

Last, let's look at the common method of communication across a network. A protocol is a set of rules and conventions that governs how computers exchange information across a network medium, (which can be a cable, radio transmitter, or receiver on a wireless network). In simple terms, a protocol represents the language that computers use to talk to each other. You'll learn about protocols in more detail later in this lesson; however, the next section covers various types of networks, from local to wide area networks.

Exploring various types of networks

Networks come in all shapes and sizes; however, most networks can be categorized as one of three major types of network:

- LAN (local area network): A network usually configured in a small business or home, in one location, and one building. What makes a LAN is the word "local." It's confined to one small physical region. It can be either wired or wireless, depending on the type of equipment in use.
- MAN (metropolitan area network): A network that consists of two or more buildings throughout a single (although sometimes large) geographical area, such as an entire city. It's connected by phone lines, broadband connections, or wireless media. This is the common configuration for a city or local government network.
- WAN (wide area network): A more widely spread network, not limited by geographical location like a LAN or MAN. Offices and networks across states and countries are usually connected by a large communications carrier, such as a global telephone company, to offer the best speed and efficiency possible.

In addition to these types of networks, each one may be subdivided into client/server or peer-to-peer.

Client/server

A dedicated server network is the most sophisticated type of network. It handles resources and services to be distributed to other computers. Figure 1-4 shows a server sharing a printer for the other computers. Unlike a peer-to-peer network, a dedicated server can't be used as a workstation.

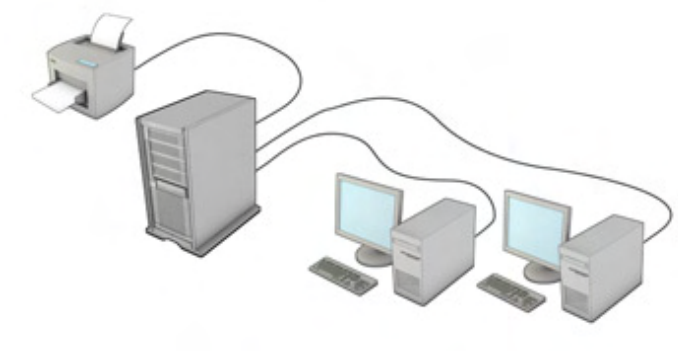


Figure 1-4: A dedicated server network.

This type of network is also called a client/server network. On a client/server network, users or computers are usually placed by departments into groups, such as Accounting and Management. All of the computers in these groups are administered as a unit, called a domain.

You'll learn more about clients and servers in the "Exploring client/server networking" section of this lesson.

Examples of client/server networks are as follows:

- Internet: This is actually the world's biggest WAN. It's a public, complex conglomeration of networks that spans the entire globe.
- Intranet: This is a web-based network much like the internet, but it's used within a single private or public company to enable employees and sometimes contractors to share information internally.
- Extranet: This is similar to an intranet, except that it may involve two or more private or public companies, along with their suppliers, customers, and contractors to share information among all members of the group of entities it encompasses.

Peer-to-peer

»HP Pavilion notebook PCs

Optimized for entertainment, HP Pavilion notebooks have both exquisite design and the powerful features for TV, photos, movies, music and more.

»Notebook PC accessories

From software, memory, and cards to carrying cases and docks, look to HP for all the accessories you need to make your notebook PC more suited to your personal needs.

With some other network operating systems, all workstations on the network can also be servers. This is called a nondedicated server network and is usually found on a peer-to-peer network. Peer networks enable users to access resources on other computers and to share the resources on their computers. A nondedicated server is highly flexible because it functions as a server and a user's workstation. However, the user must take some administrative responsibility and be somewhat network-literate.

Figure 1-5 illustrates a peer-to-peer network. Computers set up in this fashion usually belong to a workgroup. A workgroup is a collection of computers networked for a common purpose, such as accounting or marketing functions.

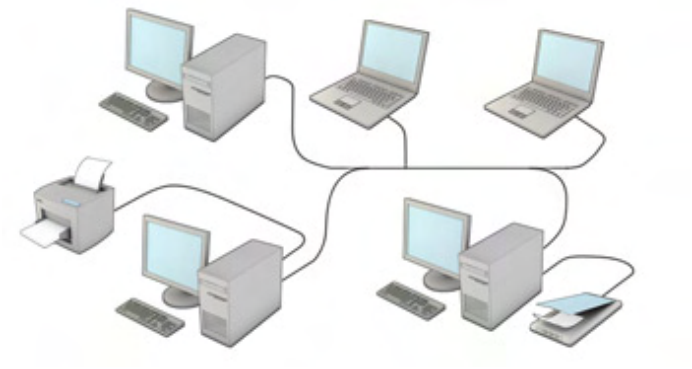


Figure 1-5: A peer-to-peer network.

Now that you've covered the different types of networks available, read on to learn about one of the most common network configurations -- the client/server environment.

Exploring client/server networking

Client/server network operating systems enable the network to centralize services and applications on one or more dedicated servers, as shown in Figure 1-6. The server becomes the core of the system, providing security and access to individual workstations. Microsoft Windows Server 2003 and RHEL (Red Hat Enterprise Linux) are examples of client/server network operating systems.

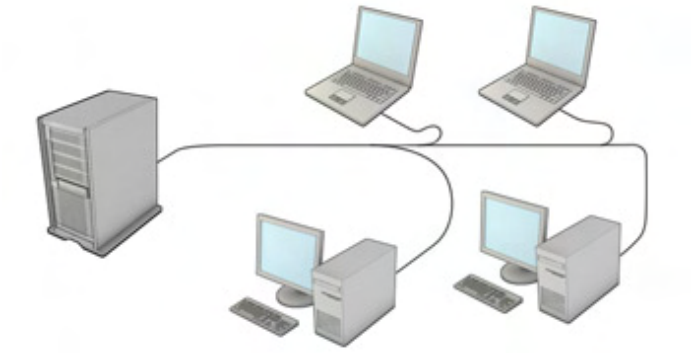


Figure 1-6: A client/server network.

There's usually a clear distinction between client and server network operating system software.

Server software

A server operating system is much more sophisticated than client software. Server software makes network resources and services available to clients. It also provides the following functions:

- Manages a directory that contains user permissions to resources, their security permissions, and passwords.

»HP desktop PCs for everyday computing

HP has a PC with the features and price range to meet your needs. Check out the latest selection today. HP Pavilion PCs provide the versatile technology you need to communicate, create and enjoy your world more.

»Norton Internet Security 2008

Travel the Internet while protected against viruses, hackers, spyware, and spam. Stay safe as you e-mail, swap files, download programs, and chat. You're automatically protected when you've got Norton Internet

- Supports file access compatible with various client operating systems; it tricks the client operating systems so the directories and files look as if they're local.
- Supports a relatively consistent user environment so when a user logs on to the network, she gains access to files, printers, and other resources.
- Helps maintain a productive computing environment by providing interfaces to internet services.

Server software's implementation depends on the type of network operating system in use. For example, Windows Server 2003 and RHEL include capabilities and modules that client operating systems don't need, and thus don't include. Examples are:

- Directory services: These help identify users, servers, and resources, and who's permitted to use resources on a network.
- Network address services: These automatically provide clients and other networked computers with the addresses and access information they need to access the network.

Advantages and disadvantages

Before you get into how a client/server network operates, let's go over its advantages and disadvantages. Advantages include:

- Centralization: Resources and security are under centralized control and management.
- Interoperability: All components work together; so different types of hardware and operating systems can easily share or access resources.
- Scalability: Existing network components can be expanded, or new ones added, as demand increases.
- Flexibility: Newly developed technology can be integrated.

Disadvantages of a client/server network include:

- Expense: Requires initial investment in dedicated server hardware and software.
- Dependence: If a server goes down, network operations are affected.
- Administration: Large networks require dedicated, trained administrative staff to manage and operate them.

Client software

A client operating system is the type of software designed for workstation computers. Its purpose is to interface with the user's operating system, for example, Microsoft Windows Vista, and provide easy access to network resources. It has components that simplify network access by making network resources look local to the user. For example, users can print to a network printer on the second floor as easily as they can print to a directly attached printer. It also enables them to access files on the network as if the files were on their own computers.

Figure 1-7 shows the relationship between the server and the client.

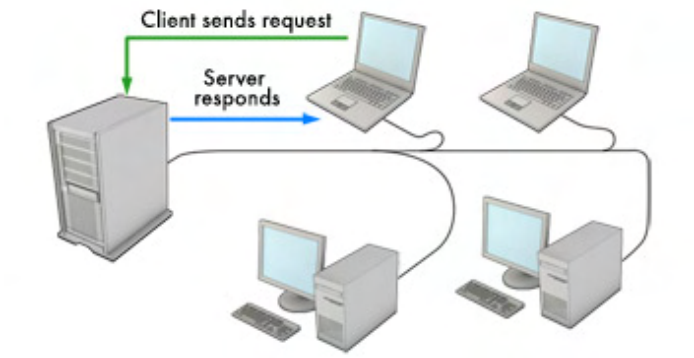


Figure 1-7: A client/server relationship.

Now that you've explored the different types of networks and how client and

Security 2008, updated and enhanced with more features than ever.

server operating systems are related, it's time to look at the methods that might be used to transmit data across a network and how that data is transported from sender to receiver.

Understanding protocols

Protocols are the heart of a network. Remember from earlier in the lesson that a protocol is the language that computers use to talk to each other. Without them, communication is impossible. Data can be sent over the medium using any one of a number of protocols. These protocols are either standard or proprietary:

- A standard protocol lets users purchase equipment from any manufacturer since it's programmed to communicate universally.
- A proprietary protocol is usually protected by patents or other legal stipulations and requires special equipment, normally from a single vendor (or its licensees).

Networking protocols come in layered collections known as protocol stacks because, like a short stack of pancakes, the upper layers rest upon the lower ones. Unlike pancakes, however, upper-layer protocols actually depend on lower-layer protocols to get things done on, and to move data across, a network.

Today, only one protocol stack really matters, and that's the set of protocols used for the internet. Known as TCP/IP, it rests on the names of two key protocols in that stack:

- TCP (Transmission Control Protocol): Provides guaranteed, reliable delivery between clients and servers for all kinds of network services.
- IP (Internet Protocol): Moves information across a network between pairs of senders and receivers, wherever in the whole world they might be.

Today, every major operating system for everything from mainframes to smart phones supports some form of TCP/IP, and nearly all networks from the smallest LANs to the biggest WANs depend on TCP/IP for their communications.

The version of IP in use is what determines this protocol's overall structure and capabilities: today, the most common form is IPv4, which uses 32-bit network addresses. There's also a newer form known as IPv6, which uses 128-bit network addresses. It's becoming more widely supported but isn't yet widely used.

Besides networking protocols, there are some important email and web protocols you should recognize. Here's a short list of the most common ones everyone should know:

- FTP (File Transfer Protocol): Performs basic interactive file transfers between hosts, enabling files to be uploaded and downloaded.
- SMTP (Simple Mail Transfer Protocol): Supports basic message delivery services between mail servers.
- POP (Post Office Protocol): A protocol used to retrieve email from a mail server. It downloads the messages to the client where they're then stored.
- IMAP (Internet Message Access Protocol): Enables creating, deleting, and renaming mailboxes; checking for new messages; and deleting messages. Email stored on an IMAP server can be accessed from a computer at home or office, and while traveling, without the need to transfer messages or files between computers.
- HTTP (Hypertext Transfer Protocol): A low-overhead web browser service protocol that supports the transport of files containing text and graphics.

Next, learn about the hardware you need to create a network.

»HP TouchSmart IQ500 Series

The sleek, next-generation, touch-enabled PC combines a 22" diagonal hi-def[1] widescreen with a powerful energy efficient Intel® Core™2 Duo processor in a single, integrated design. Includes HP TouchSmart software, webcam, media card reader, HP Ambient Light, and premium speakers for fast, easy access to photos, videos, music and applications.

1 High definition (HD) content is required to view HD images.

»Home networking for desktops

Share a high-speed Internet connection, files, printers, and multiplayer games with the flexibility, speed, and security you need.

Exploring networking hardware and media

Most modern notebook and desktop PCs include built-in network interfaces; however, many older computers and even newer servers still use add-in NICs for network connectivity. For wired technologies, this also means running at least one cable per interface to make the connection between it and the networking medium in use. For wireless technologies, this means configuring the transmitter/receiver with the information necessary to find the right frequencies, provide the right identification, and gain access to a wireless networking.

Although computers are the most frequent actors when it comes to sending or receiving networked communications, other hardware devices also play key roles in making networks work:

- Router: A device that specializes in managing the flow of traffic between or among networks. Even the cable or DSL (digital subscriber link) modems that so many small offices and home offices use for internet access usually include router capabilities as well.
- Switch: A device that enables multiple individual computers or other devices to attach to a network, and manages communications so that pairs of devices can access the network as if it were exclusively and solely theirs to use.
- WAP (wireless access point): A device that connects wireless devices to form a network. WAPs generally have a short range -- 50 to 150 feet -- so it's common to have two or more WAPs in a wireless environment.
- Firewall: A device that screens network traffic across network boundaries to look for and block unwanted traffic, or to prevent access to unauthorized or illicit resources and information. Many SOHO (small office/home office) internet access devices combine some or all of these functions in a single box, in fact.

»Notebook PCs

HP makes it easy to go wireless. Our notebooks are light, powerful, durable...and surprisingly affordable.

»Home networking for notebooks

From wireless routers to network adapters, HP's wide range of networking products help you get connected.

Networking media

Computers must share common media to communicate successfully. Network media may be a physical cable or a wireless radio connection. Regardless of type, a network medium's main function is to carry data from one device to the next. There are two primary methods of sending signals across a medium: baseband and broadband.

Baseband

Baseband uses a digital transmission pulse at a single fixed frequency. This means the entire bandwidth of the medium is used to transmit one data signal. Because baseband uses a single fixed frequency, as the signal travels further down the medium its strength decreases and can distort. Special devices called repeaters refresh the signal to its original strength and quality. The Ethernet standard for wired communication is baseband, referred to as 802.3. Ethernet is the most common network medium in use today.

Broadband

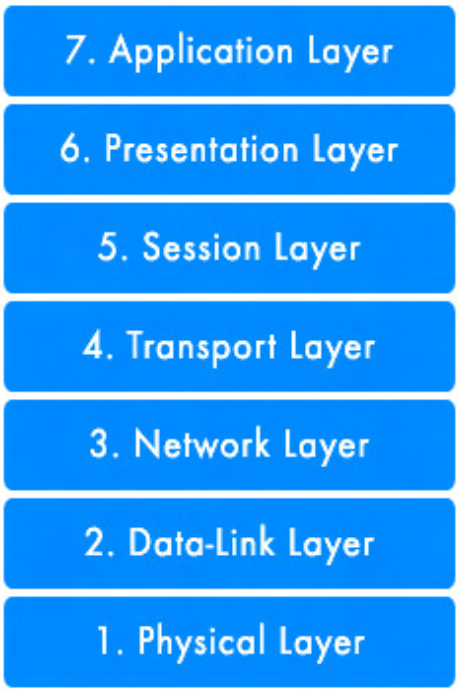
Broadband uses analog transmission over a continuous range of values. It travels one way from sender to receiver. Thus, it's necessary to have two channels for complete broadband communication: one for receiving and one for sending data. If the medium supports sufficient bandwidth, more than one transmission can travel simultaneously across a single cable. If this happens, you need a tuner to pick up the correct signal. As with baseband, if a signal travels too far, it needs to be strengthened. The device used to do this is called an amplifier. An amplifier detects weak signals, strengthens them, and then rebroadcasts them. Cable modems and DSL use broadband for communications.

Wireless networking requires the use of technology that deals with data transmission over radio frequencies. The most widely used standard is the IEEE (Institute of Electrical and Electronics Engineers) 802.11 standard, which defines all aspects of Radio Frequency Wireless networking. Because standards operate on radio frequencies, one of the issues with the current wireless technology is that it's a broadcast signal, which makes it easy for anyone to pick up within its broadcast range. Wireless technologies can also use infrared or microwave signals.

In the final section of this lesson, you'll learn about the most common network model in use today -- the OSI Network Reference model.

Exploring the OSI Network Reference model

The OSI (Open Systems Interconnection) was the brainchild of the ISO (International Organization for Standardization), which explains why you'll sometimes see this model called the ISO/OSI Network Reference model. Basically, it defines a standard, abstract model for how networks behave and exchange data.



The seven layers of the OSI Network Reference are described in the following table.

Layer	Name	Brief explanation
7	Application	Not a producing or consuming application, per se, but usually some kind of programming or data interface that can pipe data into or out of a separate and distinct application or service.
6	Presentation	Handles conversion from platform-specific data representations into generic ones for transmission, then reverses the process upon reception, so any two computers that share a common protocol can exchange data successfully.
5	Session	Deals with establishing ongoing communications between a sender and receiver, much like making a phone call: establishing the connection, managing the connection as long as it's needed, then breaking the connection when the conversation ends.
4	Transport	Deals with moving data from sender to receiver,

»HP desktop PCs for everyday computing

HP has a PC with the features and price range to meet your needs. Check out the latest selection today. HP Pavilion PCs provide the versatile technology you need to communicate, create and enjoy your world more.

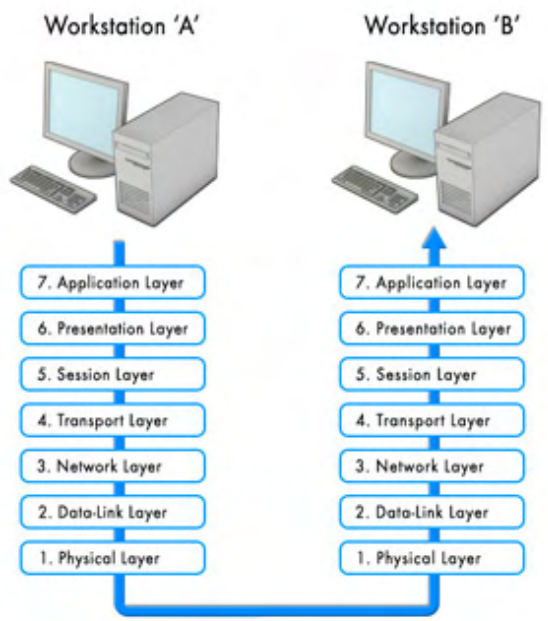
»Home networking for desktops

Share a high-speed Internet connection, files, printers, and multiplayer games with the flexibility, speed, and security you need.

		including breaking large messages up into right-sized chunks for transmission across a network medium, along with delivery guarantees where they apply, sequencing information, and reassembly upon reception.
3	Network	Deals with network addressing and naming, and how network messages might be routed from a sender to a receiver, between however many pairs of routers must be transited en route from the former to the latter.
2	Data Link	Deals with how one network interface can address and access another network interface across the networking medium, and how to translate bits into signals for transmission and signals into bits upon reception.
1	Physical	Deals with hardware devices and media: cards, cables, connectors, as well as electrical characteristics involved in signaling and controlling transmission and reception using some kind of networking media.

Table 1-1: The layers of the OSI Network Reference model.

In this model, lower layers provide services and pass information up this collection of layers, also known as a stack, for eventual delivery to some network service or network aware applications. Traveling up the stack generally corresponds to handling incoming information from the network bound for use on the target computer.



Enlarge image

On the other hand, upper layers handle various aspects of information processing necessary to transmit data across a network. As you go down the stack, you begin at fairly abstract levels related to sending emails, transferring files, controlling a system remotely, and so forth. The data is progressively broken down into more concrete messages with specific network address information, message size limits to fit the network media in use, sequence data to help put messages of arbitrary size back together, and so forth.

You've covered a lot about networking essentials in this first lesson. These terms and concepts are important to know throughout the class, so take a few moments to review any sections that might have been difficult to comprehend during the first pass.

Moving on

In this lesson, you explored the fundamental principles of networking. Lesson 2 introduces you to network hardware components and discusses what their function is and when you should implement them on a network. Before you move on, complete the assignment and take the quiz for this lesson. In addition, visit the message board to find out what your classmates and instructor are up to.

Assignment #1

For this assignment:

1. Design a simple network for a small office or department. Make a drawing that includes a server (dedicated or nondedicated), client workstations, a router, a WAP (for wireless clients), and a few printers. Show how you'd connect the computers and devices.
2. Visit the website for Charles Kozierok's outstanding book, TCP/IP Guide (No Starch Press, 2005, ISBN: 159327047X), and read his explanation of the OSI Reference model.

Quiz #1

Question 1:
What's a network operating system?

A) ◯ A set of rules and conventions that governs how computers exchange information over the network medium.
B) ◯ An operating system designed with services built-in to enable sharing to take place.
C) ◯ Files, applications, and hardware that are shared for computers to access.
D) ◯ A web-based network much like the internet, but it's used for internal purposes by private companies to enable employees, vendors, and business partners to share information.

Question 2:
What are the three main types of networks?

A) ◯ Internet, intranet, and LAN
B) ◯ Intranet, LAN, and WAN
C) ◯ LAN, MAN, and WAN
D) ◯ Internet, LAN, and MAN

Question 3:
What's the general name for the cable or wireless communication used to ferry signals from one device to another on a network?

A) ◯ Repeater
B) ◯ Amplifier
C) ◯ Medium or media
D) ◯ Protocol

Question 4:
What's a set of rules and conventions that governs how computers exchange information over a network medium?

A) ◯ Media
B) ◯ Protocol
C) ◯ Server
D) ◯ Network operating system

Question 5:
Which protocol is considered the language of the internet and probably the most widely used protocol today?

A) ◯ POP
B) ◯ IMAP
C) ◯ TCP/IP
D) SMTP

Understanding networking software

This lesson explores networking software operating systems and how they provide communication across the network. You'll also look at client versus server operating systems, and how applications share data.

Network operating system basics

Welcome back. In Lesson 1, you learned the essentials of a networked environment and the hardware necessary to set up a network. However hardware is just hardware and a network can't function without software. This lesson dives into the software -- mainly the network operating system -- needed to make a network work. You'll also explore the client operating system and, finally, how applications share data.

In today's networking world, the environment consists of a group of interconnected computers, peripherals, and devices. The network has one or more shared servers, which provide access to files and shared hardware resources. The network operating system:

- Acts as a director to manage communication across the LAN and keep the network running smoothly.
- Connects all computers and peripherals on a network by coordinating and controlling how these devices communicate across the network.
- Supports security and privacy for the network and individual users by controlling access to resources.
- Advertises and manages resources from a centralized directory, providing mechanisms to easily add or remove services, and reconfigures these resources as needed.

Some of the commonly available network operating systems that run on servers include Microsoft Windows Server, Linux, Novell NetWare, SunOS/Solaris, FreeBSD, and Unix.

The network operating system provides basic mechanisms that support operating system- and application-based services. These mechanisms include a feature called IPC (Inter-Process Communication), which enables processes to share information. In other words, IPC makes the exchange of data possible between one process and another, either within the same computer or across a network. Processes that share resources must communicate to coordinate their efforts, as well as to prevent situations in which one process could disrupt another.

Once you've installed an operating system, even a client operating system such as Microsoft Windows XP or Windows Vista, look at the shares. (Just select the Run command, enter cmd, and then enter net share at the command line.) You'll see a screen similar to Figure 2-1. An IPC share is automatically created when a modern version of Windows is installed.

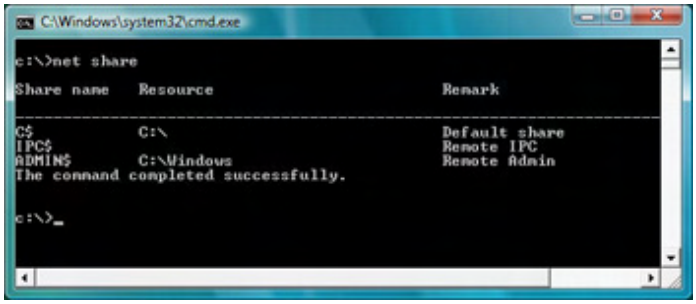


Figure 2-1: An IPC share.

Enlarge image

»HP Pavilion notebook PCs

Optimized for entertainment, HP Pavilion notebooks have both exquisite design and the powerful features for TV, photos, movies, music and more.

»Wireless network adapters

Securely add wireless LAN connectivity through your existing USB port with USB network adapters.

Besides the mechanisms for supporting services and processes, the network operating system also needs to maximize the hardware's features and capacities. One way of doing this is through a process called multitasking, which means doing more than one thing at a time. There are two types of multitasking:

- Preemptive: The processes are assigned CPU (central processing unit) time slots by the operating system. Once the time slot expires, the process is halted and the next process gets computing time.
- Cooperative: The operating system has no control over the processes. Once a process has control of the CPU, it cannot be interrupted. It finishes its computing needs before another process can use the CPU.

When deciding on an operating system, preemptive multitasking should be your choice because it enables processes to share the CPU time for better performance. Windows 2000 and newer versions support preemptive multitasking.

Now that you know some of the basics of a network operating system, let's look at some terms you should become familiar with: drivers, bindings, and stacks.

Understanding drivers and bindings

In Lesson 1, you learned that a NIC is a network interface card that enables the devices on the network to connect to each other. All connections, whether wired or wireless, enable devices to connect through this interface.

The NIC operates separately from the CPU. The two main functions of a NIC are to establish and handle the computer's network connection and to translate the digital data into signals understood by the outgoing media. In essence, the NIC is the link between a computer and a network. Figure 2-2 shows how a NIC functions. In the figure, the network cable is replaced by an access point on a wireless network.

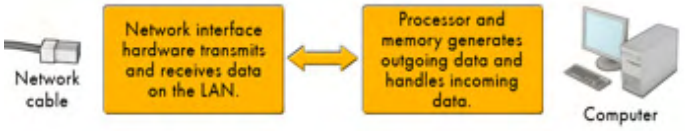


Figure 2-2: NIC communication functions.

Enlarge image

Remember that before the card can be used, software, or a device driver, must be installed on the computer. A driver is a program that interacts with either a particular device or type of software. The driver contains specific information about the device or software interface. In personal computers, a driver is often packaged as a DLL (dynamic link library) file. Some driver technologies you might recognize include:

- NDIS (Network Device Interface System): This is a communication interface that enables Microsoft Windows operating systems to communicate multiple protocols to the NIC.
- ODI (Open Data-Link Interface): Similar to NDIS except it supports Novell and Apple systems. It enables these operating systems to communicate multiple protocols to the NIC.
- WDM (Win32 Driver model): This architecture works by channeling some of the work of the device driver into portions of the code that are integrated into the operating system. This isn't restricted to just NICs; it's also used for printers, scanners, and other network devices.

Another phrase you may hear is binding a stack, which refers to linking a

»HP Pavilion dv4t series

Cutting-edge design meets powerful entertainment in our HP Pavilion dv4t Entertainment Notebook. This lightweight 14.1" diagonal mobile machine is perfect for TV shows, photos, movies, and music.

»Home networking for notebooks

From wireless routers to network adapters, HP's wide range of networking products help you get connected.

set of network protocols to a NIC. A stack is a set of network protocol layers that work together. Every NIC must have at least one stack bound to it. The protocol stack runs on top of the driver software, and uses the driver to access your hardware. In other words, protocol stacks supply the software that enables computers to talk to each other across the network. Nowadays, this refers more or less exclusively to the TCP/IP protocol stack.

Bindings are links that enable communication between network adapter card drivers, protocols, and services. Bindings establish a logical link between protocols on the NIC to provide interoperability. This enables one system to support and run any number of network protocols. The number of protocols run and the order of the bindings on the client side can impact network performance. If too many protocols are running, you'll receive poor network performance because you have devices saying the same thing in many different languages.

Sometimes network technicians install unnecessary protocols because they either misunderstand the function of the protocol or think they may need them at some future time. However, you shouldn't install additional protocols unless they're required. The more protocols installed, the more network traffic's created. For PCs running only TCP/IP, however, you shouldn't need to change bindings.

The most frequently used protocol, service, or adapter should be bound first. Figure 2-3 shows the binding order for Windows Vista. Notice the up and down arrows, on the right side of the bindings window, used to move the protocols into the proper order.

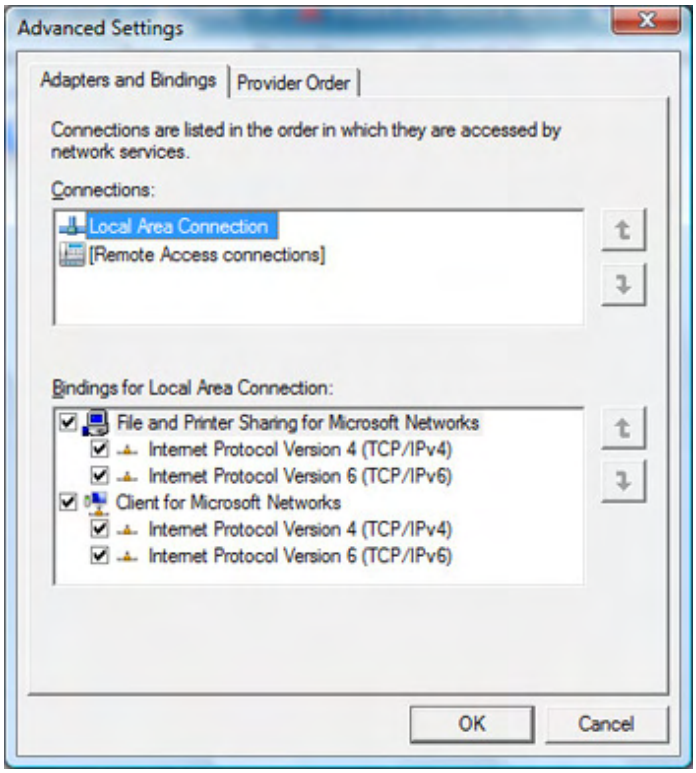


Figure 2-3: Adapter and Bindings tab.

Now that we've discussed the basics of an operating system and how drivers, protocol stacks, and bindings help the operating system and hardware communicate, it's time to look at how communications take place on a server-based network.

Understanding server services

»Desktop PCs

Network operating system services tend to be much more complex than those provided by client operating systems. In addition, the implementation of these services often requires multiple devices, message passing, and server processes. The set of typical services provided by a network operating system can include directory or naming, file, communication, email, and printing. Of these, the two most used shared resources are directory and printing services.

The services installed vary from server to server and depend on the server's role. This lesson discusses only directory services because file, email, and printing services are discussed in Lesson 4.

A network of computers managed by a network operating system can be large, making information about location and availability of services difficult to maintain. How would the client know whether the particular service it's interested in is available, and if so, on which server?

Directory services

Directory services, sometimes called name services, address such problems. The directory service is a database of service names and service addresses. Techniques for maintaining location information vary with operating systems. However; because all servers register themselves with the directory service at startup, they all supply a client with enough information about contacting the directory service.

Directory services handle service addresses as well as users, groups, printers, folders, and web information. For example, when you browse the network, the directory service is responsible for showing you which computers, printers, and other devices are available.

Windows Server offers directory services support in the form of Active Directory. Active Directory is an essential component of the Windows Server 2003 and Windows Server 2008 architecture that acts as the central authority for network security. It enables organizations to centrally manage and share information about network resources and users. Figure 2-4 illustrates this concept.

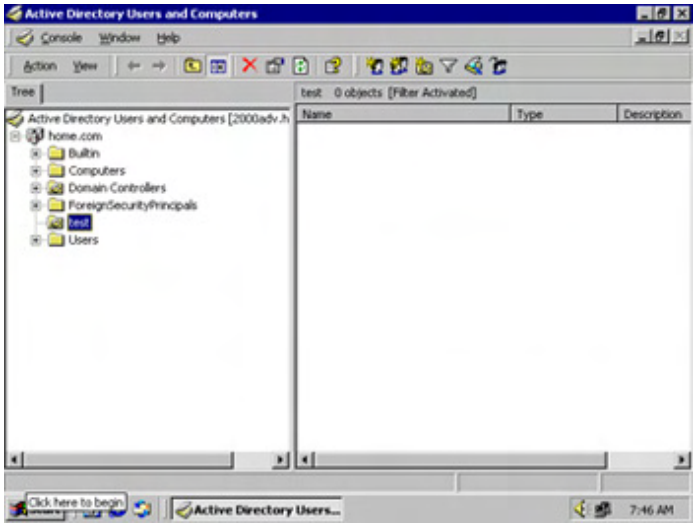


Figure 2-4: Windows 2003 Active Directory Users and Computers screen.

Enlarge image

Linux Directory Services integrates several protocols to provide a secure network directory services architecture. NDS (Novell Directory Services) is an implementation of directory services that enables sophisticated naming schemes and databases across network-wide resources. This architecture

View our wide selection of desktop PCs to see reliable HP quality at a great value. We'll even help you choose the right desktop for your unique needs.

»Home networking for desktops

Share a high-speed Internet connection, files, printers, and multiplayer games with the flexibility, speed, and security you need.

provides access to all network resources regardless of where the resources are physically located.

If a directory service provides access to network resources regardless of where they're located, why does everything look like it's on your machine when you browse the network? This is a function of the redirector, which is discussed next.

Exploring the redirector

The most important component of a network operating system is redirection. Redirection in computing is exactly that, taking something headed in one direction and making it go in another direction. The component that does this is called the redirector. It operates at the Presentation layer of the OSI Network Reference model, and its function is to accept requests from applications and determine whether network access is needed. If it is, it sends the request over the network to the server. If the request is for a local resource, the redirector passes the request to the CPU for processing. Figure 2-5 shows this process.

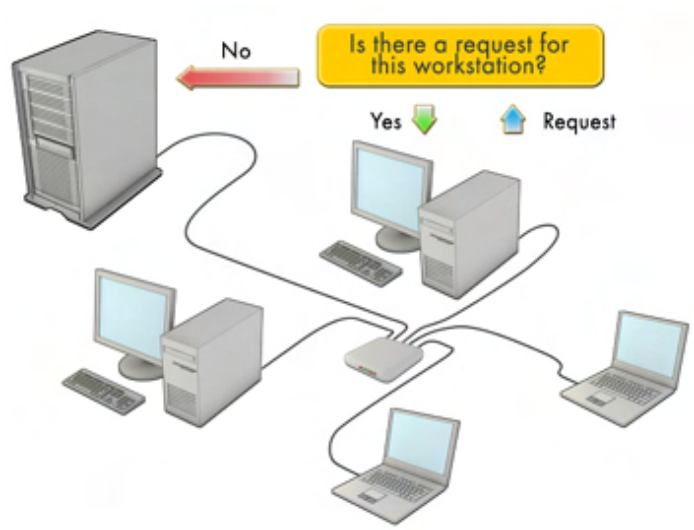


Figure 2-5: The redirector process.

For example, if you type copy C:\myfile.doc J: at a command prompt, myfile.doc is copied from your local drive C to the network drive J. The network operating system makes it appear to the copy command that drive J is local, although it really resides on another computer somewhere on the same network. The copy command doesn't know or care that drive J is across the network. The network operating system reroutes the file across the network to drive J by means of the redirector.

For myfile.doc from the user's PC to be redirected successfully, the computer with drive J must expect data. At the server, the network operating system makes the drive available to network users as part of its built-in capabilities. The same kind of redirection may also be applied to printers and other peripherals. This process is called the requestor in NetWare operating systems and in Unix.

Not all machines need to run server software, because not all computers need to share their resources. However; all networked workstations must run redirector software because every client has to read from or write data to the network.

A designator is another process used in many network operating systems. It works in coordination with the redirector and is associated with drive mapping. It manages associations between locally mapped drive letters and the correct network addresses for related directory shares. In other words, if the server has a shared folder on the C drive and you mapped it to the letter J, the designator

»HP TouchSmart IQ500 Series

The sleek, next-generation, touch-enabled PC combines a 22" diagonal hi-def[1] widescreen with a powerful energy efficient Intel® Core™2 Duo processor in a single, integrated design. Includes HP TouchSmart software, webcam, media card reader, HP Ambient Light, and premium speakers for fast, easy access to photos, videos, music and applications.
1 High definition (HD) content is required to view HD images.

»Desktop PC accessories

From software and storage to cables, mice, and keyboards, all the accessories you need for your HP desktop PC are available to make your desktop experience more personal, powerful, and attuned to your specific needs.

takes you to the shared folder on the server's C drive even though you click the J drive. This is the process that makes shared network resources appear as if they're local to your computer rather than residing on a computer elsewhere on the network.

What if you decide that a server network is too much work or you just have a few machines to connect? You can set up a peer-to-peer network instead. Let's shift gears to cover this type of network configuration, which may suit your needs and budget better than setting up a dedicated server.

More on client operating systems and peer-to-peer networks

There's generally a clear distinction between client and server network operating system software. Client software is simpler. A client operating system is software designed for workstation computers that enables simple sharing and use of network resources. Its main purpose is to interface with a user's operating system, such as Windows Vista, and to provide easy access to network resources. It has components that simplify network access by making network resources look local to the users. For example, it lets you access files or printers on the network as if they were on your own computer.

Microsoft offers client operating systems, such as Windows 2000 Professional, Windows XP Professional, and several versions of Windows Vista. Many Linux distributions also offer distinct client operating systems, such as Red Hat Enterprise Linux Desktop. However, there's no Novell client operating system. Likewise, network operating system features are integrated with Unix client operating systems.

If the total number of networked PCs is small, you may use a client operating system running on a PC as a nondedicated server. You can also connect all the computers on a peer-to-peer network.

Advantages of a peer-to-peer network include:

- Less initial expense: You don't have to purchase a separate dedicated server.
- Less setup: You can use the current client operating system already in place.

Disadvantages of a peer-to-peer network include:

- Decentralized: You have no central place to store files and applications.
- Security: The security available on a client/server network isn't provided.
- Availability: Access to shared resources, such as a printer or scanner, relies on the availability of the computer to which they're attached.
- Performance: Some performance degradation can occur when a computer is used simultaneously as a workstation and a server.

For example, a printer is attached to a computer belonging to someone who's out of the office. That computer is turned off and you need to print a document. You have two options:

- You can wait for print output until that person returns to the office.
- You can turn on her computer. However, you must have a login password to make the printer accessible.

Another situation might be that the same workstation had the only printer in the office attached to it and everyone used it. At month's end, the financial person runs large print jobs and the sales person prints material to send to customers. This could cause performance issues on the computer sharing the printer.

Now you know how operating systems work and the difference between server

»HP Pavilion dv5t series

Strike the right balance between mobility, size, and visual performance with our HP Pavilion dv5z Series Entertainment Notebook PC. This 15.4" diagonal size notebook is ready to rock your entertainment world.

»Notebook PC accessories

From software, memory, and cards to carrying cases and docks, look to HP for all the accessories you need to make your notebook PC more suited to your personal needs.

and client operating systems. It's time to take a look at how applications work across a network.

Exploring shared applications

Computing styles have evolved from highly centralized systems with mainframes to decentralized and distributed systems with workstations and PCs. The principal reason the PC evolution has been successful is the rapid development in both processing power and the bandwidth of connections between computers.

In many organizations, the information technology infrastructure incorporates different products from various vendors. This produces increased requirements for integration and flexibility in applications. Just as there's a difference between server and client operating systems, there are also different types of architectures for network applications. Here are the five most common styles:

- Client/server: Part of the application resides on the server and part resides on the client. This enables processes to be done on the server and passed back to the client.
- Distributed: In addition to a client component, the backend elements involve two or more servers working cooperatively to deliver data and services to end users. This might involve a web server that interacts with users and talks to a database server for catalog and parts information, plus an e-commerce server that handles a shopping cart and payment processing.
- Centralized: The application resides only on the server and is accessed using a terminal emulator interface. In this case, even the client portion of processing is handled on the server, and screen data is the only thing that moves back and forth between the end user and the server. This is sometimes called a terminal server.
- File-system sharing: The application resides on each client; however, common information, such as a database or directory, is shared by all clients.
- SOA (service-oriented architecture): An SOA is much like a distributed application but might include "software as a service" capabilities. It invariably involves multiple types of servers in its activities. In many implementations, multiple entities may be involved in handling different servers and contract with end-user organizations to deliver services using a highly distributed collection of servers.

The client/server style is sometimes referred to as request/reply architecture. In this type of architecture, a central exchange service exists, which all participating processes connect to. Services assign themselves a name, and export the methods for accessing these services remotely. Client services are then able to make calls against the exported methods. The processes are always connected through a central exchange process, such as IPC, to avoid the time of setting up and ripping down individual connections for each request.

So, in essence, the client establishes a connection and then requests information and waits while it's searched for. This can happen either on the internet or on the network. It also covers the essence of networking from the simplest file-system sharing scenarios, to the most complex SOA setups imaginable.

Moving on

In this lesson, you learned about network operating system software, client operating systems, and the nature of shared applications. In Lesson 3, you'll cover basic network layout and design, network addressing and access, resolving addressing issues, and connecting a network to the internet. Before you move on, don't forget to do the assignment and take the quiz for this lesson. In addition, visit the message board to find out what your fellow students and instructor are up to.

Middleware

Middleware is software that connects applications, enabling them to exchange data. Essentially, it's a general term for any programming that provides services so two separate and often already existing applications can communicate. It enables multiple processes running on one or more computers to interact across a network. A common application of middleware is enabling programs written for access to a specific database to access other databases.

»HP Pavilion Elite PCs

The next generation of home entertainment; access TV, movies, music and photos, when and how you want.

»Norton Internet Security 2008

Travel the Internet while protected against viruses, hackers, spyware, and spam. Stay safe as you e-mail, swap files, download programs, and chat. You're automatically protected when you've got Norton Internet Security 2008, updated and enhanced with more features than ever.

Assignment #2

For this assignment:

1. Pick two network operating systems and two client operating systems mentioned in Lesson 2 that you'd like to learn more about. Create a simple spreadsheet that includes a table of the operating system and the following operating system requirements:

   Hard disk space

   RAM

   Number and type of processors

   Other important features

   Cost for 1, 5, and 25 licenses

1. Research the requirements of each operating system and track your results in the spreadsheet.
2. Sketch a rough map of the computers in your office (or department, if you work at a site with more than 25 users). Identify the client computers, printers, and servers in use.
3. Decide which network and client operating systems you should implement in your environment. Common factors include cost limits, capability requirements, and type of network in use.

Quiz #2

Question 1:
Which of the following are considered advantages of peer-to-peer networking? (Check all that apply.)

A) ☐ A server has to be installed and configured.
B) ☐ Peer-to-peer networking is inexpensive to purchase and operate.
C) ☐ Individual users control their own shared resources.
D) ☐ A current client operating system already in place may be used.

Question 2:
Which component operates at the Presentation layer of the OSI model, accepts requests from applications, and determines whether network access is needed?

A) ○ Driver
B) ○ Redirector
C) ○ Directory service
D) ○ Bindings

Question 3:
Which of the following is a database of service names and service addresses?

A) ○ Driver
B) ○ Bindings
C) ○ Directory service
D) ○ Redirector

Question 4:
Which of the following is a general term for any programming that provides services so two separate applications can communicate?

A) ◯ Operating system
B) ◯ IPC
C) ◯ Application
D) ◯ Middleware

Question 5:
Which kinds of applications or services depend on multiple servers working together to handle user requests? (Check all that apply.)

A) ☐ Distributed
B) ☐ Centralized
C) ☐ File-system sharing
D) ☐ SOA

Connecting a wireless network

Whether wired or wireless, every network uses some type of layout and requires addresses to connect to and communicate with other devices. This lesson covers basic network layout and design, network addressing and access and more.

Understanding network topologies

You became familiar with networking hardware and software in lessons 1 and 2. This lesson moves into network layout and design, and then covers network addressing and connecting to the internet. First you'll learn about network topologies.

The physical layout of a network is called its topology. The topology includes the physical layout and the method of communication.

When designing a network, you should always include room for expansion. It's much easier to adapt a current network than to replace one because it was poorly designed from the start.

The following sections cover the most common topologies on which all devices share media: bus, ring, star, mesh, and hybrid.

Bus topology

A bus topology consists of computers connected by a backbone. In a cabled environment, the backbone is a single cable, as shown in Figure 3-1. In a small wireless environment, the backbone is the connection between the computers and the WAP.

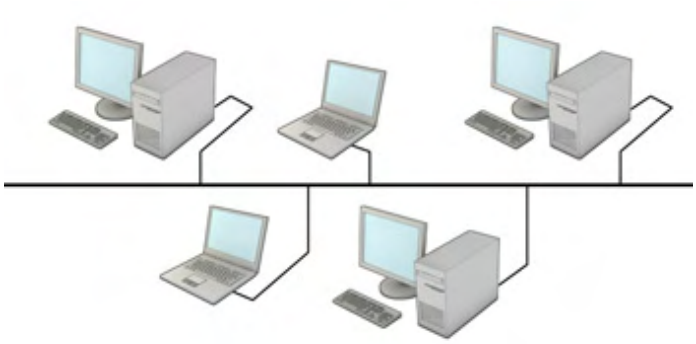


Figure 3-1: Bus topology network.

All the computers on a bus share its capacity. This is the simplest method for connecting computers. In a cabled Ethernet bus environment, coaxial cable is used, which is referred to as 10Base2. Because all devices on the same bus (or WAP) also share bandwidth, the more devices it services, the slower the

»Compaq Presario CQ50Z series

With thin lines, a cool touchpad design, and a sleek, touch-control panel, this 7.0 lb., 15.4" laptop PC redefines simplicity. In addition to being ultra stylish, the PCs in the Presario CQ50Z series are durable, powerful, and value-priced.

»Notebook PC accessories

From software, memory, and cards to carrying cases and docks, look to HP for all the accessories you need to make your notebook PC more suited to your personal needs.

network responds to communication requests.

For many bus technologies, it's not advisable for more than 10 workstations to share a single cable segment or WAP.

In a bus topology, computers only listen for data being sent to them -- they don't forward data. If one computer fails, it doesn't affect the rest of the network. This is called a passive topology. A generated signal moves from one end of the bus to the other end. If it's not stopped, it continues bouncing back and forth, preventing the computers from sending data. To avoid this, each end of the cable has a terminator.

Because the computers are all connected by the same cable, if one segment has an issue, the whole network goes down. On wireless networks, the failure of a single WAP affects only the users who depend on its services and not the entire network.

The following table shows the advantages and disadvantages of the bus topology.

Advantages	Disadvantages
Cable use is economical because all computers are in one line.	Difficult to isolate problems because one break affects the entire network segment.
Cabling is easy to work with and extend, as well as cost-effective.	One break or bad termination brings down the entire network.
Layout is simple.	Heavy traffic can slow it down because all computers share the same bandwidth.

Table 3-1: Advantages and disadvantages of the bus topology.

Ring topology

In a ring topology, shown in Figure 3-2, each computer connects directly to the next one in line, forming a circle. Data travels in a clockwise direction and each computer or device accepts the information intended for it and passes on information for other machines. A ring topology uses a token, which is a small packet, to send information.

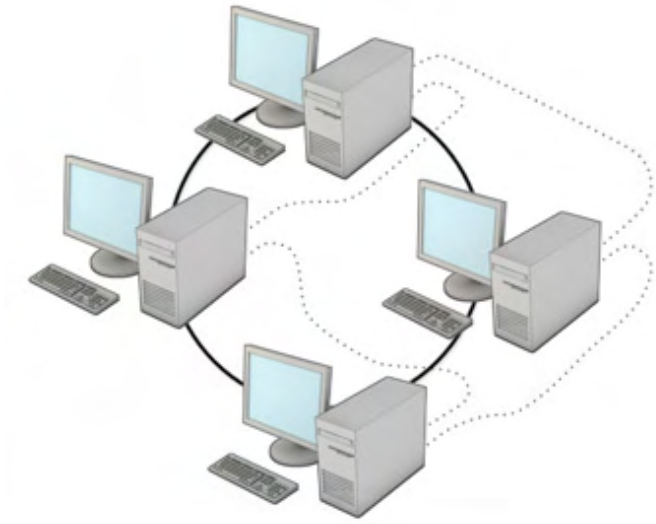


Figure 3-2: A ring topology.

Every computer on the ring is responsible for passing the token or creating a new one. When a computer has information to send, it modifies the token and

passes it on. Once the token reaches its final destination, it lets the sender know it arrived safely; the sender then makes a new token and the process starts over. Most ring networks use fiber or twisted-pair cable for their physical medium.

In a ring topology, if one computer fails, the entire network goes down. This is known as an active topology, because each workstation is responsible for sending the token.

Many ring networks implement a dual-ring network or use smart hubs to help alleviate this issue. In a dual-ring environment, two rings are used for redundancy while smart hubs remove the failed computer from the ring. The following table shows advantages and disadvantages of the ring topology.

Advantages	Disadvantages
Equal access is granted to all computers.	Difficult to isolate problems because one break affects the entire network.
Network performance is consistent due to token passing.	If one computer fails, it brings down the entire network.
	The entire network is disrupted when adding or removing computers.

Table 3-2: Advantages and disadvantages of the ring topology.

Star topology

In a star topology, shown in Figure 3-3, the computers are connected to a central hub by a cable segment. (This is also a good analogy for how a wireless network is set up, because each computer maintains its own separate connection to the WAP.) A star network requires more cabling than ring or bus topologies; however, each computer is connected to the hub by its own cable. Because each workstation has its own connection, it's much easier to move them around or connect them to other networks. You can use 10BaseT to 100BaseFX cabling with a star topology.

A star topology can support up to 1,024 workstations; however, it might not be feasible to connect them all to the same logical network.

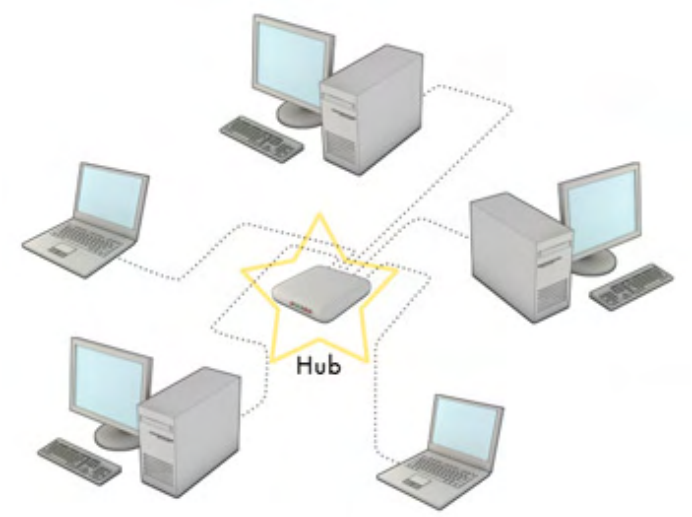


Figure 3-3: A star topology.

If one computer connection goes down, it doesn't affect the rest of the network because each connects to the central hub individually. The following table shows advantages and disadvantages of the star topology.

Advantages	Disadvantages
The entire network isn't disrupted when adding or removing computers.	Requires more cabling since each machine needs a separate connection to the central hub.
If one computer fails, it doesn't affect the rest of the network.	If the central hub fails, it brings down the entire network.
Easy to manage and monitor.	N/A

Table 3-3: Advantages and disadvantages of the star topology.

Mesh topology

In a mesh topology, shown in Figure 3-4, all devices are connected to each other more than once to create fault tolerance when a system's hardware or software must recover from failure. A single device or cable failure doesn't affect the performance because the devices are connected by more than one means. This is more expensive than other topologies because it requires more hardware and cabling.

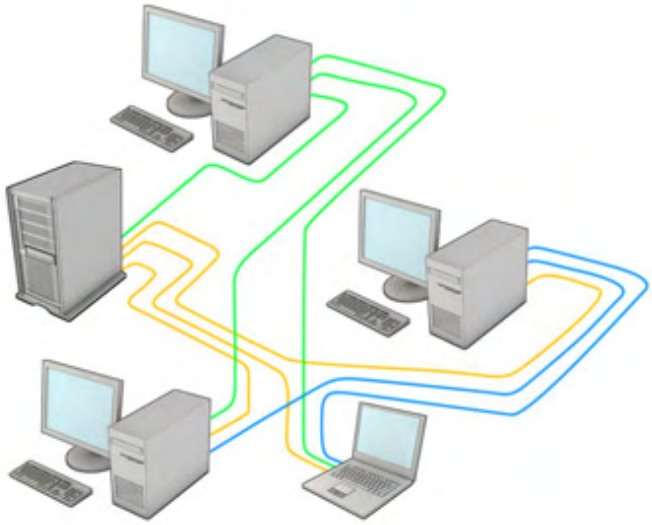


Figure 3-4: A mesh topology.

Hybrid

There are also hybrid topologies that combine different types of topology. The two most common of these are the star bus and the star ring.

In a star bus topology, shown in Figure 3-5, computers are connected to hubs in a star formation and then the hubs are connected via bus topology. Although it's more expensive to implement, this topology spans longer distances and makes it easier to isolate individual networks.

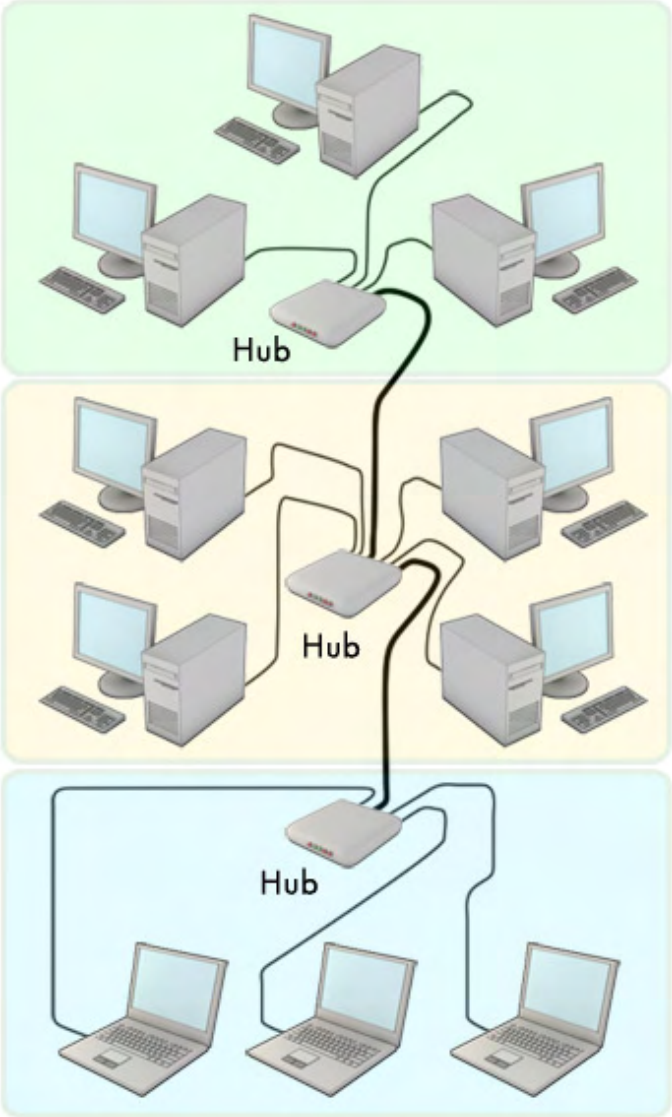


Figure 3-5: A star bus topology.

In a star ring topology, shown in Figure 3-6, data is sent in a circular motion around the star. This eliminates the single point of failure that happens in a ring topology. It uses token-passing data transmission with the physical layout of a star.

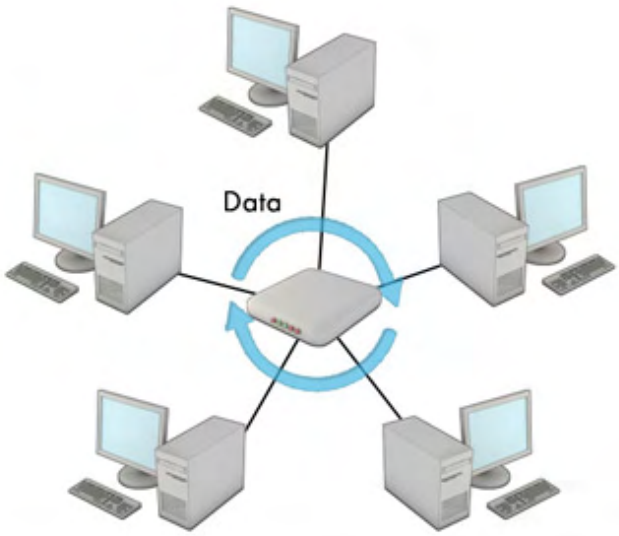


Figure 3-6: A star ring topology.

Large networks are typically organized as hierarchies. A hierarchical organization provides such advantages as ease of management, flexibility, and a reduction in unnecessary traffic. In a hierarchical network structure, a high-speed backbone usually connects the servers at the core, and individual network segments interconnect computers at the periphery.

Now that you have a general idea of how networks can be laid out, let's see how devices determine where to send data.

Understanding addressing

The two most important addresses for devices are their physical and logical addresses. This section covers both types of addresses in detail.

Understanding physical addresses

Most network technologies employ a physical addressing scheme that uniquely identifies devices (or network interfaces) on the network. This unique physical address is also called a hardware address, or MAC (Media Access Control) address, which is 48 bits long.

> A MAC address is usually represented in hexadecimal numbers, which may be separated by dashes (00-10-A4-A8-DA-D0) or colons (00:10:A4:A8:DA:D0).

The IEEE (Institute of Electrical and Electronics Engineers) is the organization that assigns unique blocks of MAC addresses to device manufacturers. Each time a network interface is manufactured, a unique MAC address is burned or built into that interface.

To determine the MAC address assigned to any network interface, just open a Windows command prompt and enter ipconfig /all, as shown in Figure 3-7. The MAC address is labeled Physical Address in the resulting output.

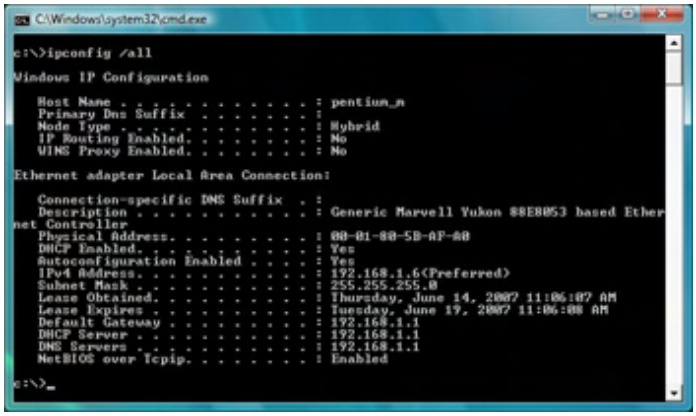


Figure 3-7: The Physical Address is the MAC address.

Enlarge image

The network interface operates separately from the CPU (central processing unit), transmitting outgoing data and accepting incoming data, if the destination address matches its own physical address. These days, many network interfaces can be configured for more than one type of media. MAC addresses are used in Layer 2 of the OSI Network Reference model.

Understanding logical addresses

Besides physical addresses, devices also have logical addresses called IP addresses. An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages (packets of data) based on the IP address of the destination. An IP address is 32 bits or 4 bytes long and is a decimal number between 0 and 255, which is expressed as four

»HP Pavilion Elite PCs

The next generation of home entertainment; access TV, movies, music and photos, when and how you want.

»Desktop PC accessories

From software and storage to cables, mice, and keyboards, all the accessories you need for your HP desktop PC are available to make your desktop experience more personal, powerful, and attuned to your specific needs.

octets in dotted decimal notation. For example, 192.168.1.6 is a valid IP address.

Currently, two types of IP addresses are in active use: IP version 4 (IPv4), which is the method described in this section, and IPv6 (IP version 6). IPv4 is the most commonly used version. IPv6 addresses are 128-bit numbers and are conventionally expressed using hexadecimal strings. For example, 1080:0:9:F:8:800:200C:417B. Both IPv4 and IPv6 addresses are assigned by ISPs (internet service providers).

The four octets serve a purpose beyond just separating the numbers. They're used to create classes of IP addresses that can be assigned to a particular organization (business, government agency, and so on) based on size and need. These octets are split into two sections: network and host ID. The network section is used to identify the network that a computer belongs to whereas the host identifies the actual computer on the network.

As the data traverses a network, IP addresses are used by Layer 3 devices, such as routers, to determine whether to forward the data to the next router or whether to keep it in its own network.

IP address space is divided into five classes: A, B, C, D, and E. The first byte of the address determines the class to which an address belongs:

- Network addresses with the first byte between 1 and 126 are Class A and can accommodate about 17 million hosts each. This class is for very large networks, such as a major international company or government agency.
- Network addresses with the first byte between 128 and 191 are Class B and can accommodate about 65,000 hosts each. Class B is used for medium-size networks. A good example is a large college campus.
- Network addresses with the first byte between 192 and 223 are Class C and can accommodate only 256 hosts. Class C addresses are commonly used for small- to medium-size businesses.
- Network addresses with the first byte between 224 and 239 are Class D and are used for multicasting (delivering information from a single sender to multiple receivers).
- Network addresses with the first byte between 240 and 255 are Class E and are used as experimental addresses.
- Messages that are intended for all computers on a network are sent as broadcasts. These messages always use the "all ones" IP address 255.255.255.255.
- The IP address 127.0.0.1 is used for the loopback address. This means that it's used by the host computer to send a message back to itself. It's commonly used for troubleshooting and network testing.

There's much more to know about IP addressing. To learn more, visit Learn to Subnet.com, which provides some great tutorials on IP addressing.

Internal versus external IP addresses

As mentioned in the previous section, IP addresses are assigned by ISPs and are public addresses. In fact, if you go to Register.com and type a domain name, you can easily find the IP address for a company's server. In Figure 3-8, Microsoft.com was queried. As you can see, it lists the server name and two associated IP addresses.

»HP Pavilion notebook PCs

Optimized for entertainment, HP Pavilion notebooks have both exquisite design and the

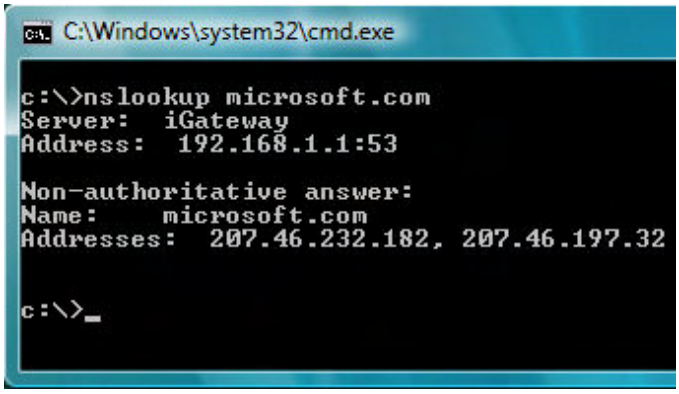


Figure 3-8: Public IP addresses.

For this reason, it's not secure to use publicly routed IP addressing for your internal LAN. Not only does it enable direct communications between outside hosts and internal clients (at least in theory), it also wastes scarce public IPv4 addresses. Until IPv6 is widely deployed, and because it's more secure to use private addressing internally, the following private address ranges have been reserved for internal use:

- Class A: 10.0.0.0 network. Valid host IDs are from 10.0.0.1 to 10.255.255.254.
- Class B: 172.16.0.0 through 172.31.0.0 networks. Valid host IDs are from 172.16.0.1 to 172.31.255.254.
- Class C: 192.168.0.0 network. Valid host IDs are from 192.168.0.1 to 192.168.255.254.

When you set up internal networks, each computer or networked device should use one of the internal address ranges.

Next, you'll learn about a handy technology that automates the administration of IP addresses on a network.

Automating IP address assignments

You now know that all networked devices have IP addresses, and you should use internal addresses on a network. However, if you have many computers and devices, how do you assign and keep track of all those addresses? Luckily, there's a technology that can do that; it's called DHCP (Dynamic Host Configuration Protocol).

DHCP provides a framework for passing configuration information to hosts or clients in a TCP/IP environment. It enables individual computers to automatically obtain their network configurations from a server rather than requiring an administrator to configure them manually. In this way administrative overhead and configuration errors are significantly reduced.

With DHCP, you can add a new computer to a network without much administrative effort. All users are dynamically assigned an address when they connect for service.

DHCP is a TCP/IP function and isn't supported by all network operating systems. For example, DHCP doesn't work with AppleTalk or IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange). These protocols have no need for DHCP because they have their own automated mechanisms for assigning network addresses.

In the next section, you'll learn about connecting your network to the internet.

powerful features for TV, photos, movies, music and more.

»Wireless network adapters

Securely add wireless LAN connectivity through your existing USB port with USB network adapters.

»Compaq Presario CQ50Z series

With thin lines, a cool touchpad design, and a sleek, touch-control panel, this 7.0 lb., 15.4" laptop PC redefines simplicity. In addition to being ultra stylish, the PCs in the Presario CQ50Z series are durable, powerful, and value-priced.

»Wireless network cards

An HP notebook with a wireless network card allows you to work from anywhere that has wireless access. Wireless cards are the key to your computing freedom.

Accessing the internet

The internet is a network of interconnected yet independent networks. Each host is directly connected to a particular network. Two hosts on the same network communicate with each other using the same set of protocols, which then would be used to communicate with hosts on distant networks. The language of the internet is TCP/IP. This protocol calls for data to be broken into packets, which are designed with a header that includes the IP address. These headers enable packets to be routed across many networks to arrive at their proper destination.

Packets are passed across the networks by devices called routers, as shown in Figure 3-9, which read the headers to determine if the packet belongs to its network or should be passed on. This is much like sending a letter through the U.S. Postal Service. The ZIP code is the ultimate destination for the letter. So, a letter you send from California to New York goes to various post offices or terminals in between and is forwarded to the appropriate destination based on the ZIP code. In networking terms, think of the IP address as the data packets ZIP code.

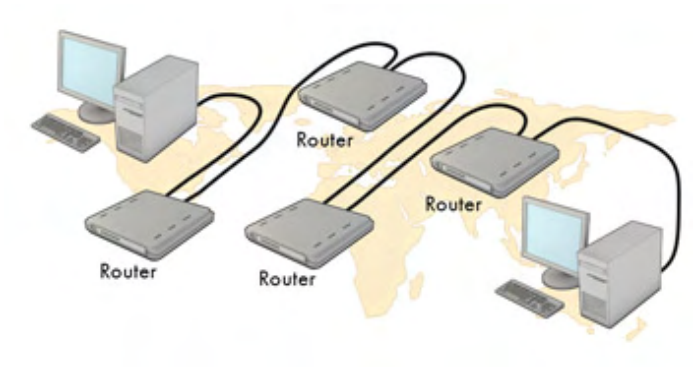


Figure 3-9: Data is transported across the internet via routers.

For the packets to reach the internet there must be a connection between the computer and the internet. This connection is called a gateway, and it's often provided by an ISP. Because IP addresses are numbers and are difficult to remember, hosts are usually found by their domain name. This allows easier navigation on the internet. An example of a domain name is microsoft.com or hp.com. All domain names are mapped to IP addresses and, as you learned previously, it's simple to find the IP addresses that are mapped to domains. In fact, next time you use a web browser to visit a website, watch the bar across the bottom of the screen. The first thing you'll see is the IP address.

Moving on

In this lesson, you learned about basic network layout and design, network addressing and access, resolving addressing issues, and connecting the network to the internet. In Lesson 4, you'll delve into server setup and management, learn about different uses for servers, and understand what factors will help you make a wise decision about whether to host your own services or have someone else do it. Before you move on, don't forget to do the assignment and take the quiz for this lesson. In addition, be sure to visit the message board to find out what your fellow students and instructor are talking about.

Assignment #3

Building on Lesson 2's assignment:

1. Determine the best network topology for your organization.
2. Assign a range of IP addresses based on a Class C internal network. (Hint: Use an

»HP TouchSmart IQ500 Series

The sleek, next-generation, touch-enabled PC combines a 22" diagonal hi-def[1] widescreen with a powerful energy efficient Intel® Core™2 Duo processor in a single, integrated design. Includes HP TouchSmart software, webcam, media card reader, HP Ambient Light, and premium speakers for fast, easy access to photos, videos, music and applications.
1 High definition (HD) content is required to view HD images.

»Home networking for desktops

Share a high-speed Internet connection, files, printers, and multiplayer games with the flexibility, speed, and security you need.

address in the 192.168.x.x range, as per private address allocations.)

Quiz #3

Question 1:
Which of the following is a disadvantage of a ring topology?

A) All computers have equal access to the rest of the network.
B) Even with many users, network performance is even.
C) A single computer failure can impact the entire network.
D) None of the above.

Question 2:
Which of the following isn't true of the bus topology?

A) Wired networks require less cabling than a star or ring topology.
B) In a wireless environment, the backbone is the connection between the computers and the WAP.
C) On a wired network, any single cable failure can bring the network down.
D) On a wired network, all computers are arranged in a spoke-and-axle fashion around a central hub.

Question 3:
Which of the following are valid IP addresses? (Check all that apply.)

A) 100.100.100.100
B) 14.325.19.18
C) 172.21.22.36
D) 75.25.50.100

Question 4:
Which of the following are valid private IP addresses? (Check all that apply.)

A) 10.100.100.100
B) 172.31.15.8
C) 25.219.45.10
D) 192.168.5.3

Question 5:
Which of the following technologies enables individual computers to automatically obtain their network configurations from a server rather than be configured manually?

A) MAC address
B) DHCP
C) TCP/IP
D) Packets

Network tutorial: working with servers

In this lesson, you'll delve into server setup and management and learn about different uses for servers. Next, you'll determine which factors will help you make a wise decision about whether to host your own services or have someone else do it.

Identifying server types

In the previous lessons, you learned about networking hardware, operating systems, topologies, and addressing. Now it's time to learn how to set up a server and what it entails.

The first step is planning. Just as you've drawn network plans in a few of the lesson assignments, you must also plan which role or roles your servers will provide along with the services, protocols, and applications required to meet your business needs.

»HP TouchSmart IQ500 Series

The sleek, next-generation,

Overlooking the planning phase can prove disastrous. Many times though, businesses skip this phase because the server must go up immediately.

The world of technology changes constantly; your network needs to change to accommodate new ways of doing business. Each operating system has its own set of protocols and tools. You can't possibly cover all the bases efficiently and effectively without proper planning. By identifying the role each server plays, it's easier to determine which services and protocols are required or needed. Here are some common server roles:

- Application server: Hosts applications, such as custom accounting packages or office productivity and collaboration suites.
- Database server: Provides access to large databases and related applications (query, report, business intelligence, data mining, and so forth).
- Email server: Provides email services and can also be used to host public folders and groupware applications.
- File server: Provides access to common user files and home directories.
- FTP server: Stores files for upload or download (may be internal or external).
- Logon server: Authenticates users when they log on to their workstations. These servers can also function as other types of servers, such as file or application servers.
- Network services server: Hosts services required for the network to function properly, such as DHCP, Domain Name System, and so forth.
- News/Usenet (NNTP) server: Provides newsgroup services where users can post and retrieve messages in a common location.
- Print server: Provides access to shared network printers.
- Web server: Hosts web-based applications and internal or external websites.

You can configure a single server to provide several roles. However, as your network grows and demand increases on that server, you need to add more servers and separate roles to provide availability and reliability to your users.

You must also determine whether the server will be accessed from the internal network, from the outside world, or both, which also helps to identify necessary services and protocols. Internal and external network access is covered in the next section.

Exploring internal and external network access

Certain servers, such as logon, application, file, and print servers, are normally accessed internally but not from outside your network for security reasons. However, what about services such as web and email? Figure 4-1 shows what a typical network with file, database, email, and web services looks like.

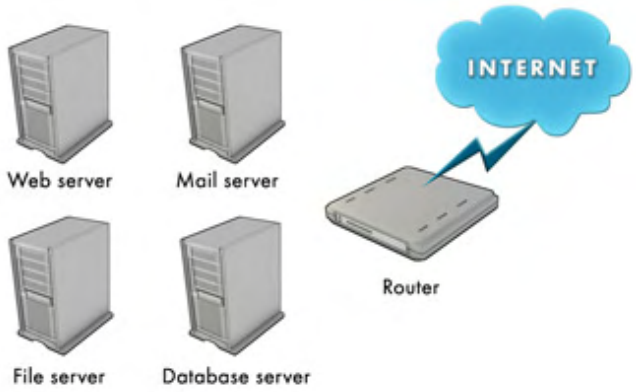


Figure 4-1: Typical server layout.

In this type of layout, all servers are accessible on the inside network and a router decides which traffic may enter from the internet, filtering packets based

touch-enabled PC combines a 22" diagonal hi-def[1] widescreen with a powerful energy efficient Intel® Core™2 Duo processor in a single, integrated design. Includes HP TouchSmart software, webcam, media card reader, HP Ambient Light, and premium speakers for fast, easy access to photos, videos, music and applications.
1 High definition (HD) content is required to view HD images.

»Home networking for desktops

Share a high-speed Internet connection, files, printers, and multiplayer games with the flexibility, speed, and security you need.

»HP Pavilion Elite m9300t series

With Intel's latest dual and quad core processors, our Pavilion Elite m9300t is ready for all your digital adventures.

»Desktop PC accessories

on IP addresses, ports, or protocols. The routers operate at the Network layer (Layer 3) of the OSI Network Reference model. Packet-filtering solutions are not generally considered very secure because they may permit unwanted packets to enter the network. Their main advantages are ease of use and speed.

Figure 4-2 shows a different perspective: a server layout with a firewall. In this scenario, a firewall works in tandem with a router. A firewall is a component placed between computers and networks to help eliminate undesired access by the outside world. It might be comprised of hardware, software, or a combination of the two. A firewall is a good first line of defense for a network.

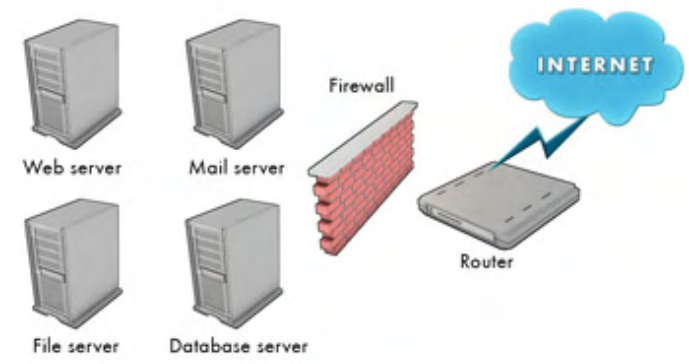


Figure 4-2: Typical server layout with a firewall.

In Figure 4-2, the firewall is on the private network and communicates directly with the router. This screening router filters data packets, routing permitted packets to the firewall. The firewall then redirects the packets to an appropriate server or workstation. This process works in reverse for outgoing communications.

Figure 4-3 shows two firewall devices that isolate the LAN from the internet. Essentially, an insulated network -- known as a DMZ (demilitarized zone) -- exists between the internet and the internal network. The internet and the internal network can access the DMZ, but neither can access each other directly. A special type of service, called a proxy, must be invoked to let inside clients access outside resources and vice versa.

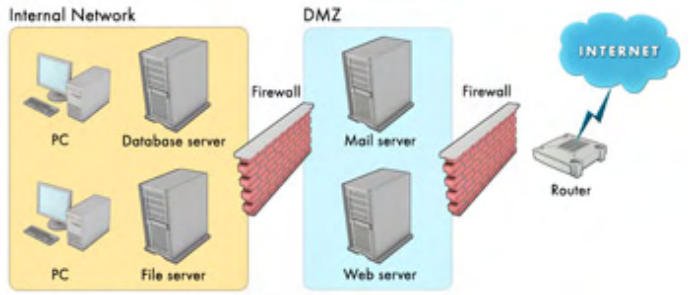


Figure 4-3: Typical server layout with a DMZ.

Enlarge image

Administrators often place web and email servers in the DMZ, and limit internal and external users' access to the servers in this area. Public inbound traffic is permitted only into the DMZ, whereas outbound traffic flows through the DMZ to get to the internet.

This type of setup works well for companies that sell products online. For example, suppose your company sells widgets on the internet. You have a large database that contains all product information, including descriptions and prices. You want to allow customers access to the web server to purchase products but you don't want them to gain access to the database where the descriptions and prices can be modified. A network with a DMZ provides access where it's desired and protection where it's needed.

From software and storage to cables, mice, and keyboards, all the accessories you need for your HP desktop PC are available to make your desktop experience more personal, powerful, and attuned to your specific needs.

Now that you understand server roles and services, and the difference between internal and external access, it's time to install a network operating system on your servers.

Installing a network operating system

Every network operating system, whether it's Microsoft, Linux, or another, has minimum hardware requirements. In addition, all operating systems can derive from upgrade installations or new installations. Although new installations are much cleaner and give you a chance to get rid of old files and settings, it sometimes makes more business sense to upgrade, because it's often faster and easier than a new, clean installation.

All network operating system installations begin by:

- Selecting an installation method
- Partitioning the hard disk
- Formatting a file system

These days, most network operating systems are installed from CD-ROM or DVD, or across a network if you have a shared directory and a network boot disc.

Let's look at a few popular server operating system installation methods. These are brief overviews; you can find additional information about these installation methods along with the minimum hardware requirements on each manufacturer's website.

Microsoft Windows Server

There are three different sections to the Microsoft Windows Server installation: text-based, GUI (graphical user interface), and networking.

During the text-based portion of the installation, you partition and format hard disks with a file system. During the GUI phase, you select the license mode, assign the computer name, assign a password to the administrator account, and install additional components. During the networking portion, you set up the domain or workgroup and install networking components. As with all network operating systems, you must reboot the computer after the installation.

Linux

Earlier versions were text based only and, many times, hardware support had to be compiled into the kernel manually. Newer versions support GUI-based installations, which makes this process less complex.

The Linux server installation process is much like a Windows Server installation. You install the operating system from a set of CDs or a DVD, or across the network. The setup walks you through creating Linux partitions, selecting the devices, and setting a root password.

As mentioned, you must select a file system during server installation. Details of that process are covered in the next section.

Selecting a file system

»HP Pavilion notebook PCs

Optimized for entertainment, HP Pavilion notebooks have both exquisite design and the powerful features for TV, photos, movies, music and more.

»Notebook PC accessories

From software, memory, and cards to carrying cases and docks, look to HP for all the accessories you need to make your notebook PC more suited to your personal needs.

The term file system describes an operating system's method of organizing, managing, and accessing files through logical hard disk structures. The hard disk is a big array of fixed-size chunks of space, and the job of the operating system is to implement a file system from these chunks.

A hard disk can have multiple partitions (virtual separations on a single hard disk that enable it to act like multiple hard disks). Operating systems add a directory structure to break a partition into smaller files, assign names to each file, and manage available free space to create new files.

When more than one operating system is installed on a hard disk, which can often entail multiple types of file systems, it's called a multi-boot or dual-boot configuration. Dual-boot configurations are good for testing and learning purposes; normally they aren't used on a live network server.

File systems interact with the operating system to ensure the operating system can read and write files on the hard disk. The file system keeps a table of contents for all files on the disk. When a file is requested, the table of contents is searched to locate and access the file. When a file is written, the table of contents is consulted to make sure unused space is used and the file is listed for subsequent access.

The most common file systems are:

- FAT (File Allocation Table): Used by DOS and supported by all other operating systems. FAT is simple, reliable, and imposes little storage overhead. FAT uses a traditional 8.3 file-naming convention. The name of a file or directory can be up to eight characters long, with a period (.) separator, and up to a three-character extension, for example, myfile.doc.

VFAT (Virtual FAT), or FAT32, is an enhanced version of the FAT file system, enabling files to have longer names than the 8.3 convention and accommodating the use of smaller allocation units on a disk.

- CIFS (Common Internet File System): CIFS is widely used in many operating systems, including Windows, Linux, and Mac OS, as well as in open source Samba implementations. CIFS offers the simplicity of FAT with the richer naming conventions available to VFAT and NTFS (or Linux and other operating systems).
- NTFS (New Technology File System): Developed expressly for versions of Windows NT and later versions of Windows Server. NTFS supports long file names, large volumes, data security, and universal file sharing, which are especially desirable for high-end systems and file servers.

NTFS 5.0 supports Windows 2000, NTFS 5.1 supports Windows XP, and NTFS 5.2 supports Windows Server 2003. (The version number for NTFS in Windows Server 2008 will probably be 5.3 or 6.0).

Next, learn why standard naming conventions and creating directories are important for the computers, devices, files and folders on your network.

Selecting naming conventions

A naming convention is a scheme to create names for servers, workstations, and other networked devices, in addition to user accounts, network shares, folders, and files, for uniformity and logical structure. Your naming convention should make devising new names easy by modeling them on the composition of existing names. The names should be descriptive enough to enable any user to locate devices quickly yet not be silly or arbitrary.

»HP Pavilion Elite d5000t ATX series

Get premium performance and maximum expandability with our Pavilion Elite d5000t ATX series. With quad-core processor technology and discrete graphics on a full ATX motherboard, this dynamic PC will meet your most demanding business and entertainment needs. Note: this series is only available online.

»Desktop PC accessories

From software and storage to cables, mice, and keyboards, all the accessories you need for your HP desktop PC are available to make your desktop experience more personal, powerful, and attuned to your specific needs.

How many printers are on your network?

If one user is hogging the network printer with his large

For example, consider a workplace where all the printers are named after Dilbert characters. How do you know where Alice or Dogbert are located? Do you know which printer is handling you job? Chances are you don't. Here are some general guidelines for naming devices:

- Construct user names from the first and last name of the user, and identify their job title or department, such as PriceJmktg. This method uses last name first, first initial, and then department.
- Construct group names from resource types, or the name of the department, location, project, or a combination, such as PhxMKTprinter1.
- Construct computer names for servers and clients from their location, department, or type, such as PhxMKTS01 (server) and PhxMKTW01 (workstation).

Check the network operating system's limitations for the length or number of characters permitted in naming conventions. For example, in most Linux environments, server names can be as long as 255 characters, although practical limitations and required typing time mean they're seldom longer than 32 characters. However, in a Windows networking environment, the limit may be 15 characters, depending on the version of the network operating system you're running.

Directory structure

Once you've selected a naming convention, you'll want to organize your files and folders in a logical manner. Directory structure is the way files and folders are organized. Directories will normally be several layers deep. When you first set up a server, some directories are created automatically by the operating system. As you add applications and users, you'll also create new directories, although the operating system automatically creates some user folders as well. The way you structure your directories depends on what a server is used for. Look at the following example of a file and application server. Figure 4-4 shows what can happen if the directory structure isn't properly controlled.

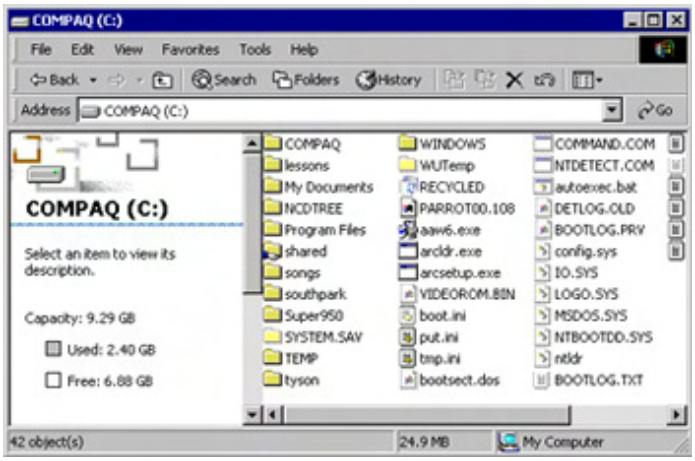


Figure 4-4: Poorly organized directory structure.

Enlarge image

As you can see, someone made a folder named southpark, apparently for cartoons; there's another folder named songs, and another one called tyson. In a network environment, you want the directory structure to be more like the one in Figure 4-5, where there's a discernibly logical structure for the folders you see.

print projects, adding more printers to the network allows all the users the choice to print immediately rather than waiting in a queue.

»Desktop PCs

View our wide selection of desktop PCs to see reliable HP quality at a great value. We'll even help you choose the right desktop for your unique needs.

»Home networking for desktops

Share a high-speed Internet connection, files, printers, and multiplayer games with the flexibility, speed, and security you need.

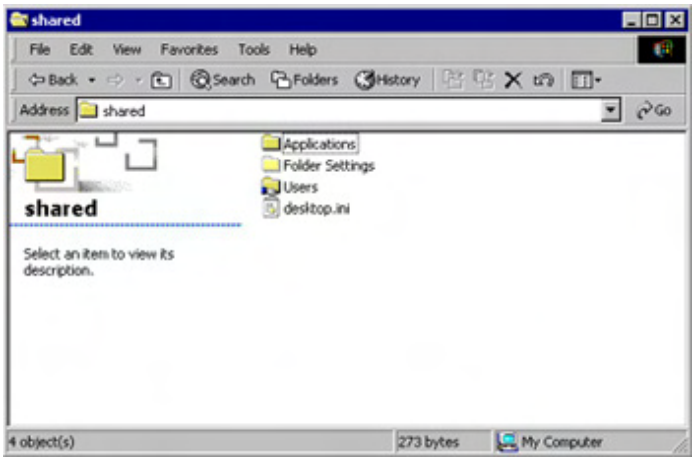


Figure 4-5: Well-organized directory structure.

Enlarge image

Notice that folders for applications and users reside inside the shared folder. Also notice that there are no miscellaneous files in Figure 4-5.

Next, find out how to select applications that work well with your network operating system.

Selecting applications

The applications you decide to run depend on the server's role and the network operating system you use. For application servers, you might have proprietary or out-of-the-box applications. For example, if you're running a Windows Server operating system, you might decide to use all Microsoft products. If you're running a Linux distribution, you might select open source applications designed for Linux environments. However, two of the most important decisions you'll make concern email and web applications.

Email applications

Email was one of the first internet applications. Today, email applications enable users to send messages along with files, text, and embedded data as attachments. Email uses a store-and-forward method of transmission. In other words, the messages are stored in an electronic mailbox and when a user logs on, the messages are downloaded. Likewise, outgoing email can be stored until it's forwarded.

Windows and Linux use different versions of email software, such as Microsoft Outlook (Windows) and Sendmail (Linux). These software packages use a server portion and a client portion. You can also use web-based email systems, such as HotMail and Yahoo!Mail, accessible from a web browser. Web-based email lets you access email from virtually any location without connecting to a corporate email server using client software. Besides message delivery, many email products offer address books for storing contact information, filtering software for eliminating junk mail, and the ability to create distribution lists, among many other features.

To receive email, you must have an account on a mail server. To send email, you need a connection to the internet and access to the mail server that forwards your email.

Three primary protocols are used for email:

- POP (Post Office Protocol): A protocol used to retrieve email from a mail server to a client. In POP3, the client does all mailbox and message

»HP Pavilion notebook PCs

Optimized for entertainment, HP Pavilion notebooks have both exquisite design and the powerful features for TV, photos, movies, music and more.

»Home networking for notebooks

From wireless routers to network adapters, HP's wide range of networking products help you get connected.

management.

- IMAP (Internet Message Access Protocol): Email stored on an IMAP server can be accessed from a computer at home, at the office, and while traveling, without requiring the transfer of messages or files back and forth between computers.
- SMTP (Simple Mail Transfer Protocol): Used as a transport protocol to send email server-to-server. When you send an email message, your computer routes it to an SMTP server. The server looks at the email address, and then forwards it to the recipient's mail server, where it's stored until the addressee retrieves it.

Web applications

Web-based applications are slightly more complicated because accessing web pages uses three main elements:

- HTML (Hypertext Markup Language): The language used to create pages on the web. This isn't the only markup language used to create web pages; however, it's the most common. Other widely used markup languages include the eXtensible Markup Language (XML), and an XML-based version of HTML called XHTML.
- HTTP (Hypertext Transfer Protocol): The internet protocol web clients and servers use to communicate with each other.
- URL (Uniform Resource Locator): A unique electronic address that enables your browser to locate pages.

A web browser is the client software that enables you to access and view any document on the web. A number of web browsers are available, such as Microsoft Internet Explorer, Mozilla Firefox, and Opera. The images in a web page are actually separate files from the text. Your browser assembles the document and formats the text and graphics according to the programming for that particular page.

> The web consists of your computer, web browser software, a connection to an ISP, servers that host data, and routers or switches that direct the flow of information.

The web is based on a client/server architecture. Remember from Lesson 2 that in a client/server architecture, the client requests a service or data from the server. The client sends the request and waits for a response. The server receives the request, does the processing, and returns the data requested. In most cases, the client then displays the data, or shows the text of a status message if the data's unavailable. In a nutshell, that's how the web works.

While we're on the subject of web servers and URLs, let's look at how a URL helps locate web pages.

Exploring DNS

You've learned that services help the operating system and applications communicate with each other. Perhaps one of the most important is the naming service. DNS (Domain Name System) resolves the name you type into a web browser to the proper network IP address. DNS is most commonly used by applications to translate domain names of hosts to IP addresses.

To administer an internet-connected network successfully, it's important to have a basic understanding of how DNS works. First look at the hierarchy of internet host names shown in Figure 4-6. The last portion of a host name, such as .com, is the top-level domain to which the host belongs. Seven original top-level domains are assigned by the InterNIC (Internet Network Information Center), the coordinating body for internet name services:

»HP Pavilion notebook PCs

Optimized for entertainment, HP Pavilion notebooks have both exquisite design and the powerful features for TV, photos, movies, music and more.

- .com: Unrestricted; intended for commercial registrants
- .edu: For use by United States educational institutions
- .gov: For use by the United States government
- .int: For use by organizations established by international treaties between governments
- .mil: For use by the United States military
- .net: Unrestricted; intended for network providers and similar organizations
- .org: Unrestricted; intended for nonprofit organizations or organizations that don't fit elsewhere

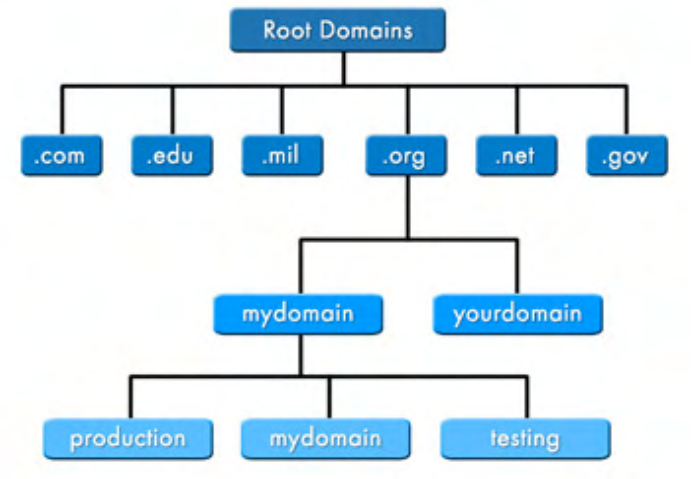


Figure 4-6: DNS hierarchy.

Top-level domains with two letters, such as .us, .uk, and .jp, were established for over 240 countries and external territories. In 2001, additional top-level domains were introduced, such as .biz, .info, and .aero.

When you type www.hp.com in the location field, the browser sends a request to the closest name server. If that server has ever had a request for www.hp.com, it locates the information in its cache (a temporary storage location for frequently accessed files) and replies. Name servers don't have complete information; often it's necessary to obtain information from more than one server to resolve a query. If the name server is unfamiliar with the domain name, it asks a server farther up the tree. If that doesn't work, the second server asks yet another, and another, until it finds one that knows. Once the information is located, it's passed back to your browser, as shown in Figure 4-7.

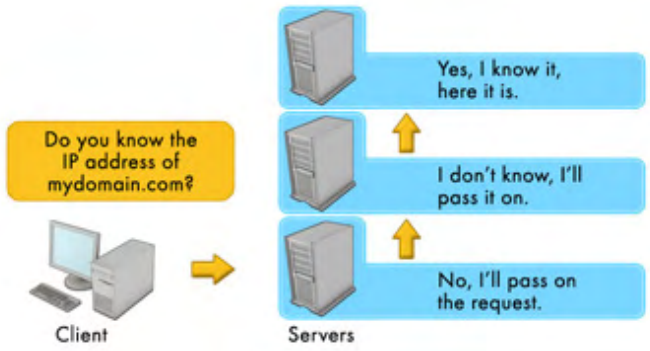


Figure 4-7: DNS name resolution.

Each name server manages a group of records called a zone. Zones are set up to help resolve names more easily. Each zone contains records that specify how to resolve the host names associated with that zone. Depending on the operating system used, the zone types can be primary and secondary or master and slave. Each of these types might then be either a forward zone, which maps names to addresses, or a reverse zone, which maps addresses to names.

Don't worry if all this DNS stuff seems too complicated -- there's a way around it. Read on.

»Wireless network adapters

Securely add wireless LAN connectivity through your existing USB port with USB network adapters.

Understanding server hosting

There are two basic ways to configure DNS and email servers. One option is to use your ISP's DNS and/or mail server. Another option is to set up a DNS and mail server on your own network. If your network-support staff is small and your needs are simple, turning to your ISP to obtain these services is the best option. The three steps to this process are listed below.

1. Tell your ISP that it's providing both primary and secondary DNS services for your organization.
2. Use the IP addresses of the primary and secondary DNS servers your ISP gives you to configure your users' workstations.
3. Provide your ISP with the DNS records you wish to publish to enable outside users to interact with your network.

In addition, if you want to receive email from the internet, you need an MX (Mail Exchange) record for your domain in your ISP's DNS database.

Remember, you can either administer your own DNS and email servers or have an ISP do it for you. If you administer the servers yourself, you'll have to maintain the DNS records and email accounts. Each time you add a new record or email account, you'll be responsible for setting it up and managing it.

Moving on

In this lesson, you learned about server roles, setup, and application management. You'll learn what it takes to maintain a network, optimize network performance, and establish a proactive management routine in Lesson 5. Before you move on, do the assignment and take the quiz for this lesson. In addition, stop by the message board to post questions and join the discussion on server roles with your classmates.

»HP TouchSmart IQ500 Series

The sleek, next-generation, touch-enabled PC combines a 22" diagonal hi-def[1] widescreen with a powerful energy efficient Intel® Core™2 Duo processor in a single, integrated design. Includes HP TouchSmart software, webcam, media card reader, HP Ambient Light, and premium speakers for fast, easy access to photos, videos, music and applications.

1 High definition (HD) content is required to view HD images.

»Desktop PC accessories

From software and storage to cables, mice, and keyboards, all the accessories you need for your HP desktop PC are available to make your desktop experience more personal, powerful, and attuned to your specific needs.

Assignment #4

For this assignment:

1. Determine the server roles necessary for your network and the number of servers you need to accommodate current and anticipated users for the next two years.
2. (Optional) Install the server software and configure server roles.
3. Determine the email software package you'll deploy on your network.

Quiz #4

Question 1:
What's SMTP used for?

A) ◯ Network file transfers
B) ◯ Email transfers
C) ◯ Name resolution
D) ◯ Network management

Question 2:
What's HTML used for?

A) Downloading email
B) Remote terminal management
C) Creating web pages
D) Transferring web data

Question 3:
The web consists of your computer, a connection to an ISP, servers that host data, routers or switches that direct the flow of information, and _____.

A) an internal network
B) email client software
C) web browser software
D) a file server

Question 4:
Which of the following are valid types of servers? (Check all that apply.)

A) File
B) Application
C) Print
D) Personal

Question 5:
Which type of organization is most likely to use the .org top-level domain suffix address?

A) Noncommercial groups
B) Government
C) Educational institutions
D) Military organizations

Managing network security

In this lesson, you'll learn what it takes to properly maintain a wired or wireless network. You'll learn about network performance optimization, how to make sure your network is secure and how to establish a network maintenance routine.

Setting up user accounts

In Lesson 4, you learned about server setup, selecting applications to run on your server, using DNS, and setting up appropriate naming conventions for files, folders, computers, and so on. Building on that, several key server management tasks are covered in this lesson, such as setting up user accounts, optimizing performance, and establishing a secure environment.

A user account holds information about a specific user, such as user name, password, and the level of permission the user has. Figure 5-1 shows a Microsoft Windows Server 2003 server user account.

»HP Pavilion notebook PCs

Optimized for entertainment, HP Pavilion notebooks have both exquisite design and the powerful features for TV, photos, movies, music and more.

»Wireless network adapters

Securely add wireless LAN connectivity through your existing USB port with USB

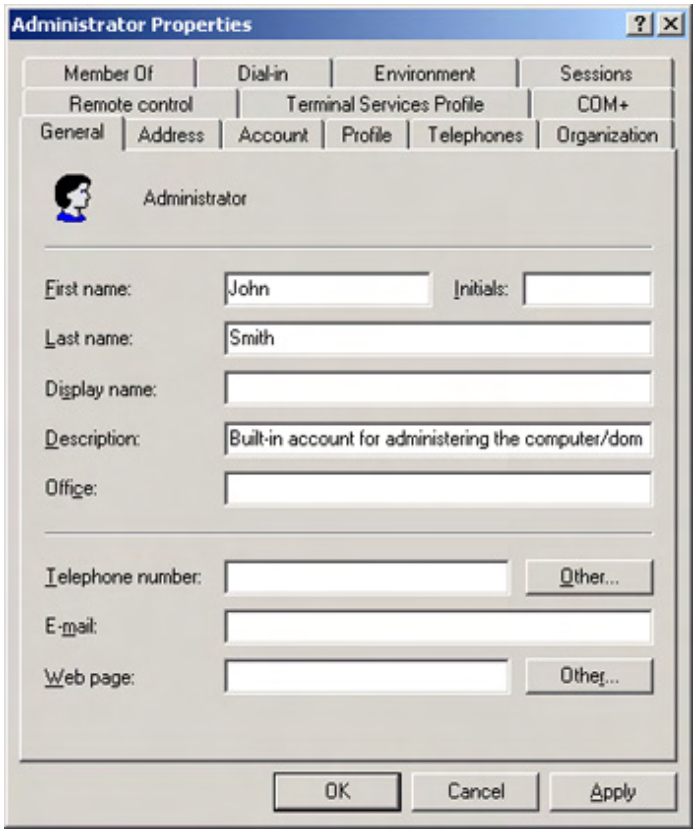


Figure 5-1: Microsoft Windows 2003 user account.

Enlarge image

You can create groups to make the sharing of resources more manageable. A group contains users that access the same resources with the same permissions. For example, the marketing staff requires access to a folder that contains the proposed sales material. Instead of giving each individual access to the folder, you can create a group called Marketing and grant all users in that group access to the folder. Figure 5-2 shows a Microsoft Windows Server 2003 group account in Computer Management.

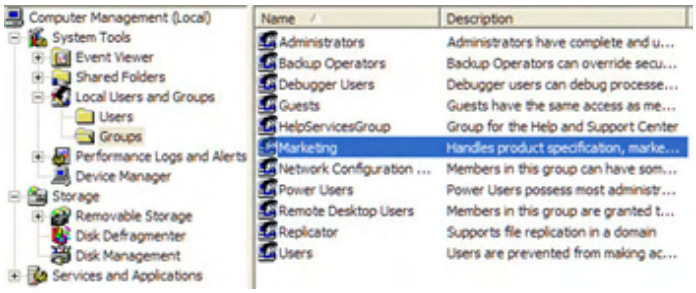


Figure 5-2: Microsoft Windows Server 2003 group account.

Enlarge image

Besides groups and user accounts, all operating systems have an administrative account that manages the system. In Linux or Unix, this account is called root, and in Microsoft Windows, it's called Administrator.

> The administrative account should only be used by an administrator. Granting ordinary users this type of access can be disastrous.

Most operating systems set the administrative account up during installation. The network administrator sets up additional user accounts after the installation is complete, assigning rights and setting permissions.

Once the network and servers are set up and running, it's imperative that you monitor performance. This keeps the network running properly. Next we'll cover

network adapters.

some of the basics of performance monitoring, and then introduce you to some tools used for that purpose.

Using performance tools

Before you can measure the performance of your network, know its normal behavior. The measure of normal activity is called a baseline. Baselining your network and application processes helps you establish whether you have a hardware or software issue. Sometimes, applications have memory leaks or a new version might cause performance issues. Without having a baseline on applications, you might spend a long time determining the problem.

Create a baseline during normal business hours under normal conditions. Taking a baseline on a day when there's little activity might cause alarm when there's most likely nothing to be alarmed about.

Once you've performed a baseline, several tools are available to monitor server performance. In Microsoft Windows Server, those tools are Event Viewer, Task Manager, Performance Console, and Network Monitor. Other operating systems have comparable programs; you can purchase third-party tools that will do the job as well. We'll look at some of the Microsoft tools show how to monitor network activity.

- Event Viewer: Enables you to audit certain events. Event Viewer maintains three log files, as shown in Figure 5-3, one for system processes, one for security information and one for applications.

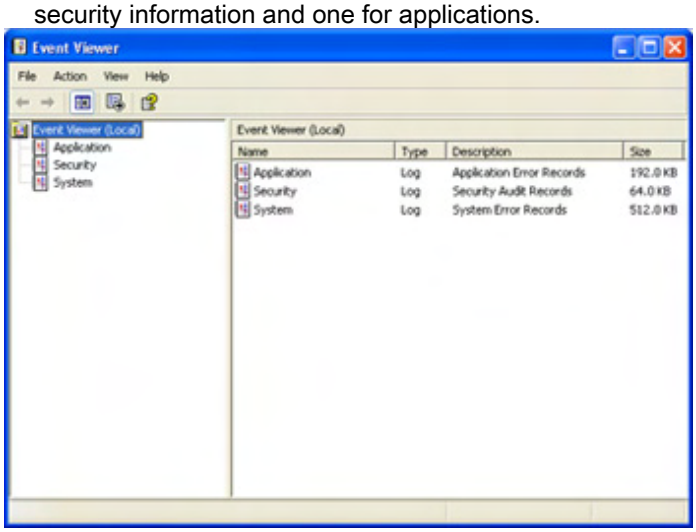


Figure 5-3: Event Viewer.

Enlarge image

The security log records security events and is available for view only to administrators. For security events to be monitored, auditing must be enabled. The application log can indicate how well an application is running. The system log shows events that happen on the individual system. The application and system logs are viewable for all users.

- Task Manager: Use to end processes or applications that are hung or cause the operating system to become unstable without having to reboot the computer. It also gives you an instant view of CPU and memory usage. It's one of the first places to check when something seems awry. Figure 5-4 shows the processes tab of the Task Manager screen.

Monitor logs

Log files are generated when you install operating systems, applications, and auditing. Most applications produce a file called INSTALL.LOG. Besides installation log files, there are various other log files created by auditing and Event Viewer that can help you avoid issues before they happen. Make time every day to view your log files. If you do this first thing every workday morning, you'll avoid potential problems.

»HP Pavilion notebook PCs

Optimized for entertainment, HP Pavilion notebooks have both exquisite design and the powerful features for TV, photos, movies, music and more.

»Notebook PC accessories

From software, memory, and cards to carrying cases and docks, look to HP for all the accessories you need to make your notebook PC more suited to your personal needs.

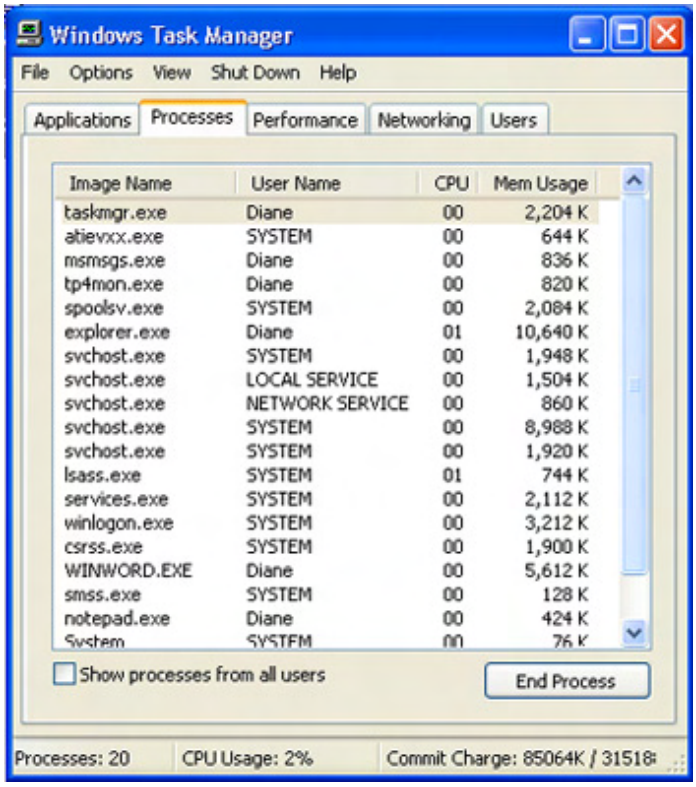


Figure 5-4: Processes tab.

- Performance Console: Use to track and view the utilization of operating system resources. You can view information you've tracked in charts, alerts, logs, and reports. The Performance console keeps track of set counters for system objects. An example of the Performance Console screen is shown in Figure 5-5.

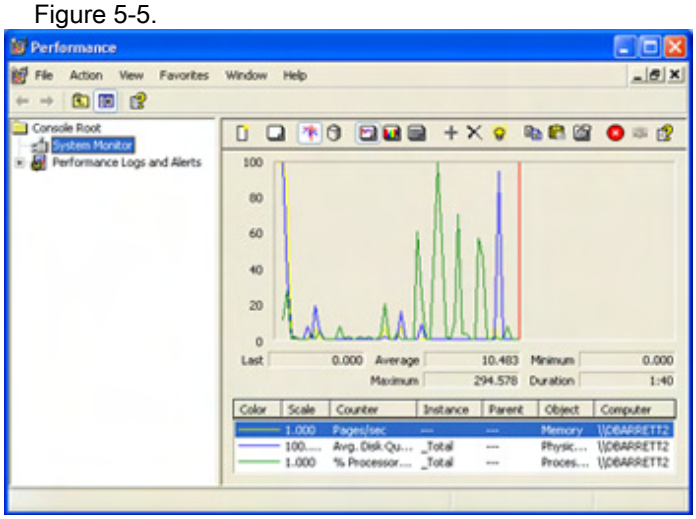


Figure 5-5: Performance Console.

Enlarge image

This tool is used to properly monitor the physical disks, memory, and processor, along with other services. It can also send alerts to an assigned administrator or user when thresholds hit a certain level and monitor more than one server at a time.

- Network Monitor: A protocol analyzer. It captures network traffic and generates statistics for creating reports. In the Unix environment, many administrators use Open Source tools such as Wireshark or Ethereal. Figure 5-6 shows the Network Monitor screen.

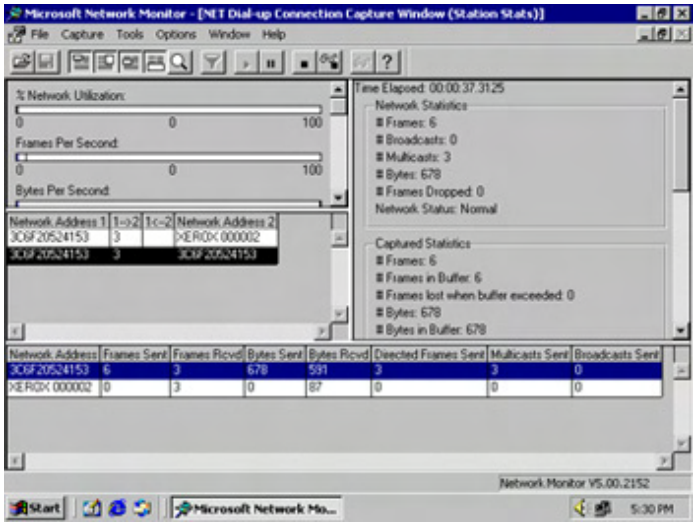


Figure 5-6: Network Monitor.

Enlarge image

You can use Network Monitor in conjunction with Microsoft SMS (System Management Server) across routers to resolve IP addresses from names.

Now that you've been introduced to baselines and performance tools, it's time to move on to troubleshooting.

Identifying bottlenecks and segmenting the network

A bottleneck occurs when too much data is pushed through a narrow opening. As a result, it jams up and has to wait. Internet and network traffic commonly bottleneck because of insufficient bandwidth.

To pinpoint bottlenecks, you should first examine the processor. Two specific counters to look at in Performance Console are:

- Object: Processor
- Counter: % processor time

> If this value rises above 75 percent on average, the CPU is working pretty hard. If it remains 80 percent or higher (without the same type of values for disk and network counters), the processor might be a bottleneck. When looking at these values, keep in mind that when an application or program starts, it automatically causes the CPU to spike to 100 percent. This is normal.

When you're monitoring the processor, you should see the utilization spike up and down. However, if the usage goes to 100 percent and stays there, there's an issue.

To eliminate a processor bottleneck, you can add more processors or upgrade to a faster processor. Another option is to move some of the load to a different server.

One of the most common bottlenecks on Windows systems is memory. Windows servers are designed to page data out of memory into a paging file when not in use or if the memory is needed for other data. So by design, in most Microsoft systems, the more memory you have, the better. There are counters that you can measure that show how well the system is using the

»Desktop PCs

View our wide selection of desktop PCs to see reliable HP quality at a great value. We'll even help you choose the right desktop for your unique needs.

»Home networking for desktops

Share a high-speed Internet connection, files, printers, and multiplayer games with the flexibility, speed, and security you need.

RAM (random access memory) and can help you determine if you need more. When the operating system runs out of physical RAM, it temporarily moves data out of RAM and into the paging file. If this file shows heavy usage, you know that the system is probably low on RAM. Here are some counters to check:

- Object: Memory
- Counter: Pages/sec
- Object: Logical disk (disk that is the location of the pagefile)
- Counter: Avg. disk sec/transfer

Sometimes the physical disk drives affect the performance of the rest of the system. Remember, if there's a bottleneck with physical RAM, there'll be excessive disk usage as the system swaps memory in and out to disk. Some counters to look at include:

- Object: Physical disk
- Counter: % disk time
- Counter: Average disk sec/transfer
- Counter: Current disk queue length
- Counter: Disk bytes/sec

Several options are available if your disks present a bottleneck to your system. The first is to purchase faster disks or disk controllers. Another option is to add more drives and reconfigure them in what is called RAID (Redundant Array of Inexpensive Disks) configurations. (You'll learn about RAID later in this lesson.) A third option is to move some data or applications off the disk volumes causing the bottleneck and onto other drives or different systems with more storage space and processing power available.

Segmenting the network

Network segments or lack of them might affect performance as well. If you've determined there's too much traffic on your network, you should segment a portion of it. Many times, performance will be an issue only to find out that several 10 MB (megabyte) hubs have been daisy-chained together where a large-capacity port switch should be. In this same area, network cards should be similar, with the highest speed available on the network and if possible, from the same manufacturer. This just makes it easier to troubleshoot.

Now you know about improving network performance, let's move on to security.

Setting up network printing

Network printing can present issues because configuring and managing network printing services is different from working with a printer connected to a workstation. With network printing, there might be different operating systems, printer languages, and various user or department requirements to service. As with other network devices, network printers deliver different levels of performance, depending on the quality of the printer and driver. There are three ways a printer can be networked:

- Connect via parallel, USB (universal serial bus), or Ethernet to a server
- Connect via parallel, USB, or Ethernet to a remote print server
- Connect via an internal network interface card, such as HP JetDirect's Ethernet interface, or a printer with built-in wireless or wired Ethernet capabilities

Managing print services is more than connecting printers, creating printer objects, and sharing them. You need to establish access, redirect print jobs, or establish print job priorities in print queues. Here are some considerations when selecting a strategy for network printing:

- Determine which speed the connection should be, such as 10 or 100 Mb

»HP TouchSmart IQ500 Series

The sleek, next-generation, touch-enabled PC combines a 22" diagonal hi-def[1] widescreen with a powerful energy efficient Intel® Core™2 Duo processor in a single, integrated design. Includes HP TouchSmart software, webcam, media card reader, HP Ambient Light, and premium speakers

Ethernet.

- Check the amount of RAM in the printer. If users often send large print jobs, a printer lacking sufficient memory will result in slow printing.
- A poorly written driver can significantly degrade print performance. Vendors update their print drivers periodically and make them available on their websites. Make sure new versions of the drivers are downloaded when they become available.
- It might be better to deploy several smaller printers rather than one large printer. If your only printer breaks, the users have to wait for it to be repaired.
- Keep the printer, print server, and users close to each other if possible.

Next, learn the essentials of network and data security.

for fast, easy access to photos, videos, music and applications.
1 High definition (HD) content is required to view HD images.

»Desktop PC accessories

From software and storage to cables, mice, and keyboards, all the accessories you need for your HP desktop PC are available to make your desktop experience more personal, powerful, and attuned to your specific needs.

Implementing network security

Network security is often defined as the tools, techniques, and methods used to protect a company's or organization's investments in IT technology. The data and services computers provide, as well as the equipment that provides them, all require protection. Because a RAID array provides mechanisms to maintain data access even in the face of disk drive or controller failures, it too, has something to offer in helping to keep data safe and accessible.

Backing up your data

Because a backup can become the only method for recovering from serious insult or failure to computer systems, it might be an essential ingredient when bringing systems back up after outages. There are several different backup types and backup media.

Backup types

Let's first look at the types of backups you can perform:

- Full backup: This is a complete backup of all data.
- Incremental backup: Contains only information that has changed or been modified since the last backup.
- Differential backup: Copies all information that has changed since the last full backup, regardless of if or when the last differential backup was made.
- Copy backup: Similar to full backup, it copies all selected files.

Backups should include only data. You don't need to back up application files and operating system files during daily backups because they can be reinstalled if necessary. Clearly mark or label backup media so you can find and identify them easily in the event the data needs to be restored.

Consider storing copies of your backups offsite to help you recover in case the entire facility is destroyed.

Test backup tapes or images regularly to ensure you can restore from them; and confirm that your staff is trained and experienced enough to successfully restore backups as needed.

Security alerts online

There are many online resources you can use to investigate virus hoaxes. Visit the Symantec Security Response website , the McAfee Virus Information website , or one of our favorites, Snopes .

»Norton Internet Security 2008

Travel the Internet while protected against viruses, hackers, spyware, and spam. Stay safe as you e-mail, swap files, download programs, and chat. You're automatically protected when you've got Norton Internet Security 2008, updated and enhanced with more features than ever.

»HP Pavilion dv9700t series

Backup media

Tape devices use magnetic storage media and are extremely popular in backup technologies because of the amount of data that fits on a tape. Several types of magnetic media can be used to back up important data; however, the DLT (Digital Linear Tape) is currently one of the most popular and reliable types of media.

Many companies and organizations decide to back up their systems to extra hard disks over the network, and then perhaps back up the data from the hard disks to tape as an extra measure of protection.

Using RAID

RAID (Redundant Array of Inexpensive Disks) organizes multiple disks into a large, high performance logical disk. In other words, if you have three hard drives, you can configure them in a RAID to look like one big drive. This can be done with hardware or software.

There are many types of RAID; however, RAID 0, RAID 1, and RAID 5 are the most common. When selecting a method of redundancy, select a level of RAID that's supported by the operating system. Not all operating systems support all versions of RAID. Another point to keep in mind is that even though you set up the server for redundancy, you still must back up your data. RAID doesn't protect you from multiple disk failures. For information on RAID levels, go to Raid.edu or The RAID Tutorial.

Auditing

Auditing is the process of tracking users and their actions on the network. Auditing of access use and rights changes should be implemented to prevent unauthorized or unintentional access for a guest or restricted user account access to sensitive or protected resources. An audit logs details of what users are doing on the network so that you can track malicious or unintended activities. Most audit systems provide event alarms to warn administrators when certain levels or conditions are met.

Some activities that can be audited include users doing the following:

- Reading, modifying, or deleting files
- Logging on or off the network
- Using services, such as remote access or Terminal Services
- Using devices, such as printers

Resource auditing is the most common form of auditing. You can use it to track how users use resources such as disk space. Many network operating systems enable administrators to set a disk usage limit so that users don't fill up the server with music and movie files. Software metering and licensing is another area that requires auditing to track when the number of allowable licenses for a software package has been exceeded so additional licenses can be purchased.

Using protection software and keeping system software updated

Protecting your network and data also entails keeping software updated. The three major areas to look at are antimalware software, service packs, and patches.

Offering the latest in multitasking and multimedia, the dv9700z, a recent addition to our dv9000 series, is a desktop-replacement-level entertainment powerhouse. It's also packed with innovative optional features, including a fingerprint reader, and it's beautifully designed in our cool new "Radiance" pattern.

Antimalware software includes a variety of protections to deal with viruses, worms, Trojans, and other self-replicating forms of unwanted or malicious software (also known as malware), as well as handling spyware, adware, rootkits, and so forth. Your servers always should include up-to-date antimalware software.

A service pack updates an existing software release and includes solutions to known problems along with other product enhancements. It might have bug fixes, system tools, and drivers. Between service packs, patches are issued to provide bug fixes for individual components. Depending on the operating system you're using, these can be applied different ways. Most operating system manufacturers recommend installing service packs or patches as soon as they're released. It's always a good idea to test these updates before installing them.

Read your operating system documentation to find out where to find the latest updates and patches, or if there's a utility built into the operating system to track and manage updates.

Many virus and vulnerability attacks occur because operating systems aren't updated or patched. Applying the latest manufacturer's operating system patches or fixes can help prevent attacks. Subscribing to newsgroups and checking security websites daily ensures awareness of the latest attacks and exploits, which requires constant vigilance.

Securing ports and disabling services

There are 65,535 ports accessible on a computer. The well-known ports are those from 0 to 1023. These are assigned by the IANA (Internet Assigned Numbers Authority) and can only be used by system processes. The registered ports are those from 1024 to 49151; the dynamic or private ports are those from 49152 to 65535. Incoming connections communicate on the well-known ports that listen for particular services, which are controlled by system processes or services.

Whenever a client requests services from the server, the client establishes a connection. To establish a connection, a computer needs to know the IP address and port number on which the application communicates. Most servers come with a wide range of services, protocols, and ports, many of which are turned on by default. This leaves them open to unauthorized access or threats -- especially if you're unaware these services are running.

It's important to know which services and protocols are running on your servers to properly protect them from intrusion. In addition, it's important to close ports and disable unnecessary services.

For a full listing of the services and protocols and the ports they operate on, visit the Internet Security Systems, Inc. Port Knowledgebase.

Employing firewalls

Recall from Lesson 4 that a firewall is a component placed between computers and networks to eliminate undesired access by the outside world. It can be comprised of hardware, software, or a combination of both. A firewall is the first line of defense for a network, and should be set up during network installation.

Even though a firewall is an important part of your defense, you shouldn't rely

on it exclusively for network protection. Combine a firewall with all the security solutions outlined in this section.

Scanning

To reduce security risks, you should regularly use a network scanner to check your network for rogue access points (unauthorized access points) and other threats. Many products are available; however, Netstumbler is a popular sniffer that tells you which wireless networks and access points are available in your area.

You learned ways to provide system security in this section. Next find out the best procedures to protect your network.

Following security best practices

Best practices are really just a set of good controls. When putting together your network protection plan, your practices should include prevention, detection, response, and vigilance. Here are some best practices for detecting network attacks:

- Come in everyday assuming that a new vulnerability has surfaced.
- Make it part of your daily routine to check the log files from firewalls and servers.
- Have a list of all the security products that you use and check vendor websites for updates.
- Know your network structure so you can detect abnormal behavior.
- Question odd patterns and behavior, then look for answers.

The following is an example of best practices for password policies:

- Make the password length at least eight characters and require the use of uppercase and lowercase letters, numbers, and special characters.
- Lock user accounts after three to five failed logon attempts. This stops programs from deciphering the passwords on locked accounts.
- Monitor the network for use of questionable tools. If password files are captured, they can be run though password-guessing programs on another machine.

As you can see, putting best practices into place makes the computing environment a much safer and secure place. It takes planning, testing, and education. Even though each company must have its own unique security plan, best practices can be shared among companies. The following websites offer good information on best practices:

- FASP (Federal Agency Security Practices)
- CERT Security Improvement Modules
- SANS' Information Security Reading Room
- Security Focus

Establishing security policies

Where security is concerned, the best thing a company or organization can do is create a thoughtful, thorough, and well-designed collection of documents that describes all security requirements, assesses its vulnerabilities, and defines its commitment to avoid, offset, or remediate those risks. In security circles, this is known as a security policy, and normally consists of a security mission statement, a set of goals, and multiple policy documents. The policy documents cover many topics, from antimalware protection to employee security and training, remote access, service providers and contractors, firewalls and DMZs, auditing and remediation, and so on.

Moving on

»HP Pavilion Elite m9300t series

With Intel's latest dual and quad core processors, our Pavilion Elite m9300t is ready for all your digital adventures.

»Desktop PC accessories

From software and storage to cables, mice, and keyboards, all the accessories you need for your HP desktop PC are available to make your desktop experience more personal, powerful, and attuned to your specific needs.

In this lesson, you learned about maintaining and optimizing a network, and implementing security controls. Before you move on, do the assignment and take the quiz for this lesson. In addition, stop by the message board to post comments or questions, or just join the discussion on networking. After that, you'll be ready for the final lesson in this class, in which you'll learn how to troubleshoot network issues.

Assignment #5

For this assignment, perform some common security tasks:

1. Check the log files on your firewalls and servers to determine if any suspicious activity has taken place in the last 24 hours.
2. Check your gateway's firewall program and identify which ports are open. Your firewall program might be Windows Firewall or a product by Symantec, McAfee, Trend Micro, and so on.
3. Check your server's administrative password. Is the length at least eight characters? Does it require the use of uppercase and lowercase letters, numbers, and special characters?
4. Check your server's user account settings to determine if account access is locked after three to five failed logon attempts.
5. Monitor the network for use of questionable tools.

Solution

Here are solutions for the various performance-related elements in the assignment:

1. Check the log files on your firewalls and servers to determine if any suspicious activity has taken place in the last 24 hours. Your tools and techniques will vary according to the firewalls in place on your network; however, on Windows Servers, you can check the System, Application, and Security logs in Event Viewer (Start > Control Panel > Administrative Tools > Event Viewer, and then pick the appropriate tabs).
2. Check your gateway's firewall program and identify which ports are open. Your firewall program might be Windows Firewall or a product by Symantec, McAfee, Trend Micro, and so on. Alternatively, you can visit a website like http://grc.com (Gibson Research Corporation) and use the ShieldsUP! Service to probe the ports on your internet interface and the firewall that should be guarding it.
3. Check your server's administrative password. Is the length at least eight characters? Does it require the use of uppercase and lowercase letters, numbers, and special characters? Most strong password policies require a minimum of eight characters, and the use of mixed-case alphabetic characters, as well as at least one non-alphabetic character, to make them harder to guess.
4. Check your server's user account settings to determine if account access is locked after three to five failed logon attempts. By default, Windows locks login attempts after three failed logins (check Account Lockout and Password Policy nodes of the Default Domain policy settings to see what's up).
5. Monitor the network for the use of questionable tools. Network Monitor can tell you if other instances of itself are running, and third-party tools, such as GFI LANGuard, can identify protocol analyzers, port scanners, and other potentially suspect tools in use.

Quiz #5

Question 1:
It's essential to identify a network's typical behavior so you can identify abnormal behavior in the future. What's the measure of normal activity called?

A) Benchmark
B) Baseline
C) Protocol analysis
D) Case study

Question 2:
You can use a variety of tools to monitor network performance. Which of the following tools are designed for

Microsoft Windows operating systems? (Check all that apply.)

A) ☐ Task Manager
B) ☐ Network Monitor
C) ☐ Event Viewer
D) ☐ Server Manager

Question 3:
Groups are created for which of the following reasons?

A) ○ To hold information about the specific user
B) ○ To manage the system
C) ○ To measure the performance of your network
D) ○ To make the sharing of resources more manageable

Question 4:
How many port numbers can be accessed on a machine running TCP/IP?

A) ○ 65,535
B) ○ 250
C) ○ 7,564,323
D) ○ 6,655

Question 5:
What's the collection of documents called that describes a company's or organization's security posture, assesses its vulnerabilities, and defines its commitment to avoid, offset, or remediate those risks?

A) ○ Security policy
B) ○ Security practices and procedures
C) ○ Employee security handbook
D) ○ Security guidelines

Troubleshooting: a networking toolkit

This final lesson helps you understand how to identify and address common problems that affect a network. You'll learn how to effectively troubleshoot issues so your network stays healthy.

Developing basic troubleshooting skills

In Lesson 5, you learned about server management, how to detect and eliminate bottlenecks, network security, and more. This lesson focuses on network troubleshooting methods and techniques for keeping your network running well.

As much as we want to believe that if we plan properly, a network will run trouble-free; that's highly unlikely. Systems crash, applications hang, and hardware fails. This is part of everyday life in a networked environment. When something does go wrong, you need to know how to fix it as quickly as possible to reduce or eliminate downtime and maintain user productivity. Troubleshooting skills are invariably acquired through experimentation and experience.

> Although you can't learn a resolution for every problem that exists, you can learn a methodology to find and diagnose nearly every problem in a systematic and logical manner.

The most common causes of network problems are:

- User error: You'll often find that users try to do things the network doesn't support or that they make mistakes. Many times, you'll discover changed settings or deleted files have caused the problems you must fix.

»HP TouchSmart IQ500 Series

The sleek, next-generation, touch-enabled PC combines a 22" diagonal hi-def[1] widescreen with a powerful energy efficient Intel® Core™2 Duo processor in a single, integrated design. Includes HP TouchSmart software, webcam, media card reader, HP Ambient Light, and premium speakers for fast, easy access to photos, videos, music and applications.
1 High definition (HD) content is required to view HD images.

- Physical connections: Verify that all cables are plugged in and that you have lights on the network interfaces and hubs. Check for loose or unsecured cables.
- Reboot: Often, system processes or software applications hang and the only way to get them to unlock is to reboot the computer. You'll find this true especially with Microsoft Windows operating systems. When all else fails, reboot.

Although the nature of troubleshooting might be different depending on the specific problem, some common steps apply to every situation.

Step 1: determine the scope of the problem

Determine the scope of the problem by identifying the symptoms. Asking questions such as "Is anyone else in the area having the same problem?" or "Can you print from other applications?" can help you establish the scope right away. This is important because you need to determine whether it's a problem with a specific machine or if it's a network problem. If more than one computer manifests the same problem at one time, it's obvious that it's a network problem and not a computer-specific problem.

Most of the time, users make general or vague statements such as, "The printer isn't working." or "I can't access the network." Ask specific questions about the circumstances to collect enough information to diagnose a cause, and then fix it. Here are some questions you might ask:

- What exactly is happening? Does it happen all the time or just sometimes?
- What has changed? Have you installed any new applications or programs?
- When was the last time it worked properly? Have you tried to fix it yourself?

Step 2: establish possible causes

After you've a listed the probable causes, begin to isolate the problem by testing each of the causes, starting with the most obvious first. You might attempt to re-create the problem at this stage. While you're trying to isolate the problem, it's important to make only one change at a time and test it. If you change too many things at once and the problem is solved, you won't know what actually fixed it. Or, if the problem gets worse, you'll have no idea what created additional issues or made conditions worse.

Read the documentation that came with any new product you're installing. It's also important to have an accurate and detailed map of your current network environment on hand to easily identify the location of connectivity problems.

Possibly the most important requirement in any network environment is to have current and accurate information about the network available when it's needed.

By using a defined strategy for network troubleshooting, you can approach a problem methodically and resolve it with minimal disruption to network users. Next, learn how to troubleshoot connectivity problems.

Identifying connectivity issues

So now that you know some of the basics behind troubleshooting, it's time to look at one of the most common network issues: a computer or device that can't access the network or the internet. Connectivity problems occur when a workstation can't communicate with its own devices or other devices on the LAN or WAN. More than 70 percent of all computer problems are related to cabling and connections.

»Home networking for desktops

Share a high-speed Internet connection, files, printers, and multiplayer games with the flexibility, speed, and security you need.

»Compaq Presario CQ50Z series

Checking for power

Many times power buttons are bumped accidentally, either by the user or perhaps someone cleaning the area. The absence of a power light means the device has no power or the power light is burned out. If the power light isn't visible, check that the device is receiving proper power and that it's turned on. If not, check the power supply, power cable, power outlet, and the wall connector. If you've verified all power connections, the device might have to be repaired or replaced.

Checking cables and connections

If the computer or device is receiving power, ensure all cables are connected firmly. Hard disk ribbon cables, network cables, and power cables can loosen. Equipment is often moved around. Check the microprocessor, memory modules, and cards, such as video and sound, to see they're inserted correctly and didn't unseat in transit.

Checking network connections

Networks are designed to move data from one device to another. If they're not, you must determine why the data isn't traveling as expected and then find a solution. The two most common causes ofunreliable data transmission are broken physical connections, such as an unplugged or broken cable, or a network device that doesn't work properly.

You can fix the problem of an unplugged cable by plugging it back in. Regarding damaged cables, the cable that's most often damaged runs from the workstation to the wall jack. It's usually the most exposed and therefore most vulnerable. To check for damage, replace the suspect cable with a known working cable. If the computer or device still doesn't work, look at the link lights.

A link light is a green or amber LED (light emitting diode) that shines if the networking device detects a network connection. Many network devices, such as routers, hubs, switches, and network interfaces, are equipped with link lights for this very reason. Most network interfaces have two lights -- a link light, which remains illuminated for the duration of the network connection, and a light that displays the current activity of the network card, which pulses as data is transferred to and from the computer or device.

If the power, cables, and link lights are all functioning properly, it's time to resort to other methods to determine the problem. This brings us to using connectivity tools.

Using connectivity utilities

The power, cables, and link lights are all functioning properly, so now what? Recall that addressing was discussed in Lesson 3. Besides a physical address, devices also have a logical address called the IP address. An IP address is an identifier for a computer or device on a TCP/IP network. Software connectivity utilities, such as PING and traceroute, are useful in determining IP-address-related connectivity issues.

With thin lines, a cool touchpad design, and a sleek, touch-control panel, this 7.0 lb., 15.4" laptop PC redefines simplicity. In addition to being ultra stylish, the PCs in the Presario CQ50Z series are durable, powerful, and value-priced.

»Home networking for notebooks

From wireless routers to network adapters, HP's wide range of networking products help you get connected.

»Desktop PCs

Using PING

The PING utility is essentially a system administrator's tool used to see if a computer is operating and also to see if network connections are intact. PING uses a protocol called ICMP (Internet Control Message Protocol). Here's how it works:

1. A small packet containing an ICMP echo message is sent through the network to a particular IP address.
2. The computer that sent the packet waits for a return packet.
3. If the connections are good and the target computer is up, the echo message return packet is received.

PING is one of the most useful network tools available because it tests the most basic function of an IP network. When PING works, it's telling you there's a functioning path between the source and the destination and the computer with the destination IP address is running. A PING example is shown in figure 6-1.

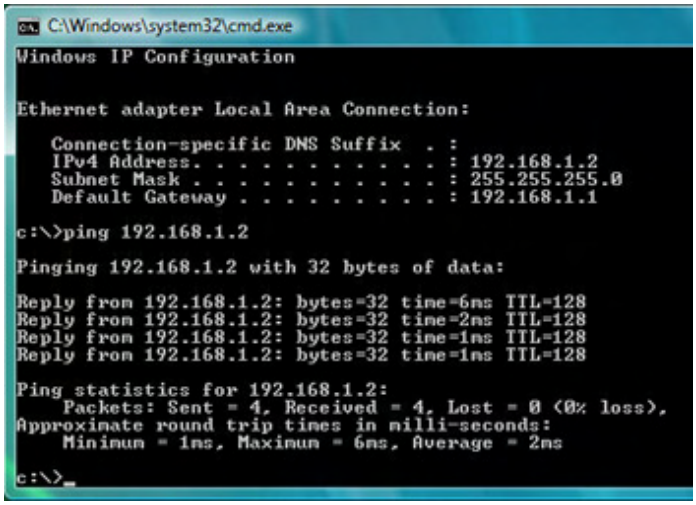


Figure 6-1: Ping command.

Enlarge image

Besides determining whether the remote computer is currently available, PING also provides information pertaining to the general speed or reliability of the network connection. In connectivity issues, first try to PING another computer on the same network. If you receive a response from this computer, then PING the server. Once you receive a proper response, PING a host on a remote network. What happens if, when you use PING, you get a destination host unreachable, as shown in Figure 6-2?

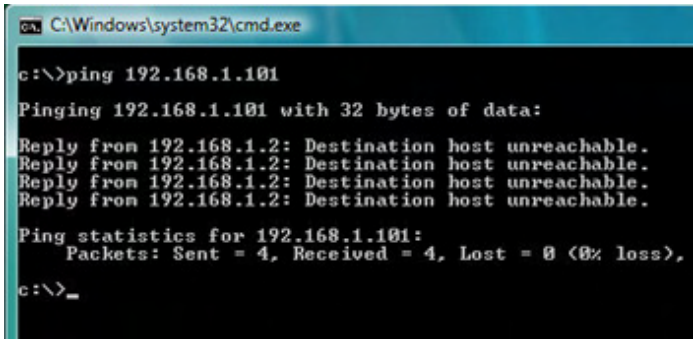


Figure 6-2: Destination host unreachable.

Enlarge image

This return usually means there's a problem with the configuration of the IP address information. To resolve this, issue the ipconfig/all command to view the configuration information, as shown in Figure 6-3.

View our wide selection of desktop PCs to see reliable HP quality at a great value. We'll even help you choose the right desktop for your unique needs.

»Home networking for desktops

Share a high-speed Internet connection, files, printers, and multiplayer games with the flexibility, speed, and security you need.

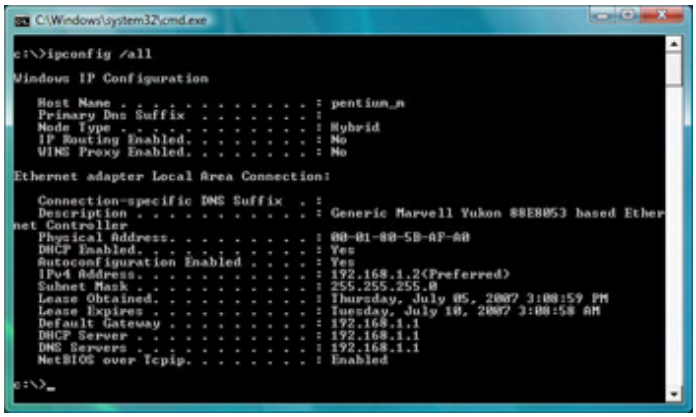


Figure 6-3: Ipconfig/all command.

Enlarge image

Here, you'll see the IP address of the computer and the default gateway. The default gateway is the IP address of a computer or device that enables a networked computer to reach other networks or the internet. They should have the same class address. In other words, if the address of the computer on which you issued the ipconfig command is a Class C address, the default gateway should also be a Class C address. If this information doesn't match, this is the source of the problem.

Notice in Figure 6-3 that the default gateway, the DHCP server, and the DNS server all share the same network address -- 192.168.1.1. That's because DHCP is enabled on the network. The DHCP server itself runs on a network appliance that also acts as the default gateway and masks external DNS servers with a built-in DNS proxy. (Lesson 3 discusses DHCP and DNS briefly; lesson 5 discusses firewalls and proxies.) DHCP automatically gives computers their IP addresses and other configuration information they need for connectivity.

Resolving name resolution problems

Sometimes you can ping a computer using the IP address but still not connect to it due to a name resolution problem. In this case, use host names with the ping command instead of IP addresses. This process uses DNS to translate that name into the address that PING eventually uses.

Nslookup is a command-line tool used to diagnose DNS infrastructure, as shown in Figure 6-4. Notice that when you type the name of a server, the command shows to which IP address the name is being resolved. This helps determine if you need to change the computer's DNS configuration.

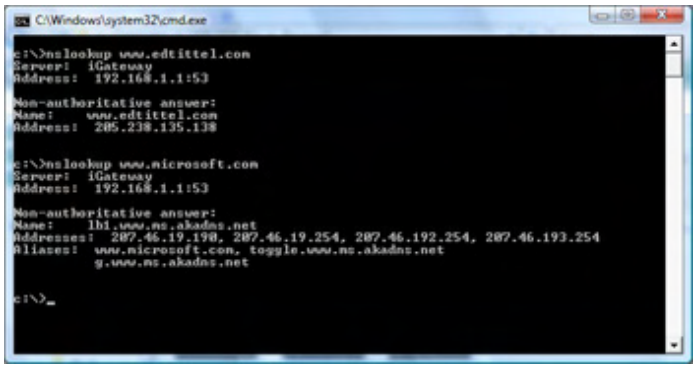


Figure 6-4: Nslookup command.

Enlarge image

Use this checklist of troubleshooting tips when customers or users can't access the web server or website by typing in a URL but can access by PINGing:

- Can you ping the website by domain name?
- Can you ping the website by IP address?
- Does your local DNS server resolve the domain to its correct IP address?

After going through this process, you should be able to resolve the issue by either fixing the incorrect information or notifying your ISP that there's an issue with name resolution.

If all the IP information is correct, it's time to use the traceroute utility to check the path across which data travels.

Using tracert

Traceroute was a utility originally developed for the Unix operating system; tracert is the modified version used in Windows. It tracks the path a packet takes to get to its destination. In other words, it measures how long it takes to travel to each hop (router) to get to its target. It's useful in finding out why a packet isn't reaching its destination, and where it may be going astray or getting lost.

If the destination network is directly attached to the first router, tracert indicates that the destination was reached. If not, it continues to the second router, third router, and so on. Figure 6-5 shows a route that a packet travels to reach its final destination, which can be quite a long way.

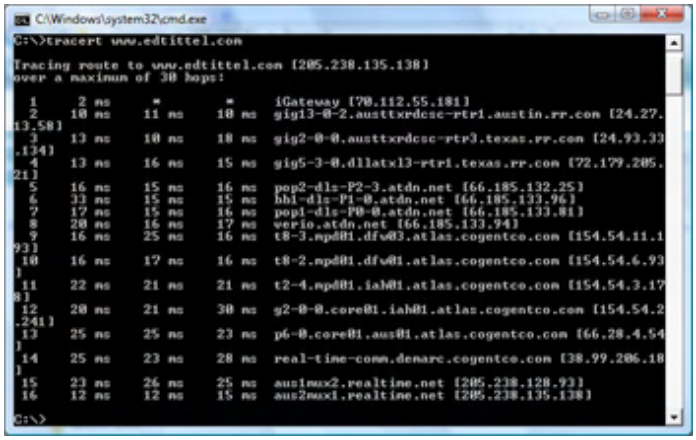


Figure 6-5: Tracert command.

Enlarge image

The tracert command is useful in determining where a packet of data might be getting hung up. For example, sometimes your ISP might be the source of the problem. If the route shows that the packet stops there, you know right away that the problem lies with the ISP and not your network.

> Many firewalls don't allow PING or tracert commands to be serviced; therefore, the tracert client might time-out for one or more hops in the chain between your computer and the target computer. This doesn't necessarily indicate a connectivity problem; it just means that tracert is unable to continue due to firewall or router restrictions.

Using netstat and nbtstat

Two other useful tools for troubleshooting are netstat and nbtstat. Netstat displays a status of active network connections. It shows active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics, and IPv6 statistics, as in Figure 6-6.

```
Command Prompt
c:\>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            pentium_m:0            LISTENING
  TCP    0.0.0.0:49152          pentium_m:0            LISTENING
  TCP    0.0.0.0:49153          pentium_m:0            LISTENING
  TCP    0.0.0.0:49154          pentium_m:0            LISTENING
  TCP    0.0.0.0:49155          pentium_m:0            LISTENING
  TCP    0.0.0.0:49156          pentium_m:0            LISTENING
  TCP    127.0.0.1:10110        pentium_m:0            LISTENING
  TCP    192.168.1.2:139        pentium_m:0            LISTENING
  TCP    192.168.1.2:49669      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49670      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49671      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49677      vcom4:http             ESTABLISHED
  TCP    192.168.1.2:49678      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49679      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49686      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49692      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49693      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49694      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49695      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49696      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49706      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49707      unknown:http           TIME_WAIT
  TCP    192.168.1.2:49708      unknown:http           TIME_WAIT
  TCP    [::]:135               pentium_m:0            LISTENING
  TCP    [::]:445               pentium_m:0            LISTENING
  TCP    [::]:5357              pentium_m:0            LISTENING
  TCP    [::]:49152             pentium_m:0            LISTENING
  TCP    [::]:49153             pentium_m:0            LISTENING
  TCP    [::]:49154             pentium_m:0            LISTENING
  TCP    [::]:49155             pentium_m:0            LISTENING
  TCP    [::]:49156             pentium_m:0            LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:49166          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:49170        *:*
  UDP    127.0.0.1:49240        *:*
  UDP    192.168.1.2:137        *:*
  UDP    192.168.1.2:138        *:*
  UDP    192.168.1.2:1900       *:*
  UDP    192.168.1.2:49169      *:*
  UDP    [::]:123               *:*
  UDP    [::]:500               *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:49167             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:49168            *:*
```

Figure 6-6: Netstat command.

Enlarge image

Nbtstat displays NetBIOS over TCP/IP protocol statistics; NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. Figure 6-7 shows some of the commands and information displayed using nbtstat.

```
C:\Windows\system32\cmd.exe
c:\>nbtstat -c

Local Area Connection:
Node IpAddress: [192.168.1.2] Scope Id: []

                NetBIOS Remote Cache Name Table

     Name            Type       Host Address    Life [sec]
    ------------------------------------------------------------
    DINA_PC        <20>  UNIQUE          192.168.1.3         25

c:\>nbtstat -n

Local Area Connection:
Node IpAddress: [192.168.1.2] Scope Id: []

                NetBIOS Local Name Table

     Name            Type         Status
    ---------------------------------------------
    PENTIUM_M      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    PENTIUM_M      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered

c:\>_
```

Figure 6-7: Nbtstat command.

Enlarge image

We've looked at troubleshooting cables, IP addresses, and name resolutions, but what if the network isn't working the way it should when you install a new application or update? Read on.

Looking for help

Where do you go when you don't know how to solve a problem? You can consult product documentation, online services, IT-related websites, subscription services, books, and magazines. You can also ask another experienced administrator or technician for assistance, or check user groups or newsgroups for network consultants.

One of the best places for troubleshooting a problem is the manufacturer's website. Microsoft provides a knowledge base, which is easy to use and a great place to consult if you use Microsoft products. Linux also has good website resources. Because there are so many different versions of Linux, start

»HP Pavilion Elite m9300t series

With Intel's latest dual and quad core processors, our

with generic websites, such as:

- Linux.com
- Linux Online

Besides general Linux information, there's also information on each specific distribution of Linux, such as RedHat, Fedora, Slackware, Mandrake, and SUSE.

In addition to websites, there are subscriptions services that provide a wealth of information. TechNet is one such service used to support all aspects of networking, with an emphasis on Microsoft products. It's updated via monthly DVDs and is available online. TechNet includes a searchable database of all of Microsoft's articles, documentation on nearly all products, updated drivers, the most recent service packs, and beta copies of new releases and tutorials.

Consult vendor-provided CDs or DVDs for technical information that may include known issues and their resolutions or workarounds. Many technicians overlook these resources and spend countless hours troubleshooting on their own. At a minimum, you should read the readme.txt file on the installation media before you install any product.

After you've exhausted all your resources, you may have to resort to calling the vendor and opening a technical support incident to solve the problem. To improve the proper handling of your technical support incident, have the following information ready to assist the support department:

- The name and version of the operating system you're running
- Which service packs are installed
- Version numbers of hardware and software
- Serial numbers
- Detailed account of the problem
- Troubleshooting steps attempted so far, and the results

Other excellent sources of information are periodicals and white papers. These documents provide valuable information on current and new practices, products, and trends. These resources often can help guide you through procedures, such as setting up perimeter defenses or writing automated scripts.

Moving on

Congratulations on completing the class! You've covered several aspects of networking to help you understand and properly perform tasks associated with setting up and maintaining a network. Before moving on, complete the assignment, take the quiz for this lesson, and stop by the message board a final time to post questions, reply to comments, or just join the discussion. We hope you've enjoyed this class and have learned a lot from it. Consider signing up for another online class to continue developing your skills.

Assignment #6

For this assignment:

1. On a computer running Microsoft Windows, possibly the one that you're currently using, open a command prompt and type the following command:

```
ipconfig /all
```

1. What information does this give you? Write down the IP address of the default gateway or the

Pavilion Elite m9300t is ready for all your digital adventures.

»Norton Internet Security 2008

Travel the Internet while protected against viruses, hackers, spyware, and spam. Stay safe as you e-mail, swap files, download programs, and chat. You're automatically protected when you've got Norton Internet Security 2008, updated and enhanced with more features than ever.

DHCP server. When would you use this information?

2. PING the IP address of the default gateway or the DHCP server. What happens? When would you use this information?
3. (Optional) Type tracert 202.54.115.149, and then press Enter. How many hops did the packet take? When would you use this information?

Solution

The ipconfig /all command provides information about the TCP/IP configuration on the host machine where it's executed. It tells you the host name, the MAC addresses for all enabled network interfaces, if DHCP is turned on or not, and provides the IP address, subnet mask, default gateway, DHCP server and lease information (if active), and DNS servers, on a per interface basis. You would use this information to ensure basic IP address information appears correct and to determine if the local TCP/IP stack is working properly (by PINGing loopback to make sure TCP/IP is working, and PINGing the machine's own IP address to make sure the network interface is working).

You generally PING the default gateway or DHCP server address to determine if you can access another host on your local subnet if troubleshooting reveals that the PC being tested is working and can access the network itself. To access the internet you must be able to access the default gateway, so this is a vital step in checking connectivity. To maintain a current and correct IP address you must be able to access the DHCP server.

(Optional) If you enter tracert 202.54.115.149 at the command line, you'll go through 16 hops before you get a report from the server at 202.54.2.162 that the designated host is unreachable. This tells you that the route can be followed all the way to another Class C network that exists in the same general address space (202.54.2) before it determines the host is unreachable. This very likely indicates the target server isn't responding to tracert requests or is temporarily offline. A second check to nslookup indicates the address resolves to a router in India named fe-11-1-0-RTR-115-149.bomvsb.vsnl.net.in. If you have any problems with 202.54.115.149, try one of the IRS (Internal Revenue Service) IP addresses, such as 199.196.144.95.

Quiz #6

Question 1:
When troubleshooting, which of the following questions should you ask the user about any problems they report? (Check all that apply.)

A) ☐ What exactly is happening?
B) ☐ What has changed?
C) ☐ Have you tried to fix it yourself?
D) ☐ When was the last time it worked properly?

Question 2:
When troubleshooting, which of the following are steps should you take to resolve a problem? (Check all that apply.)

A) ☐ Determine the scope of the problem by identifying the symptoms.
B) ☐ Establish possible causes.
C) ☐ Test each possible cause, starting with the most obvious.
D) ☐ Change several things at one time to quickly resolve the problem.

Question 3:
Which of the following utilities can you use to test connectivity?

A) ○ Netstat
B) ○ Netmon
C) ○ PING
D) ○ Ipconfig

Question 4:
Which of the following utilities can you use to test the path a packet travels?

A) ○ Netstat

B) ◯ Tracert
C) ◯ PING
D) ◯ Ipconfig

Question 5:
Which of the following are resources you can use to find help resolving issues? (Check all that apply.)

A) ☐ Installation media
B) ☐ Websites
C) ☐ User groups
D) ☐ Newsgroups

© 2003 - 2008 Powered, Inc.