Basic Networking Concepts and Technologies

Bandwidth

When data is sent over a computer network, it is broken up into small chunks called packets. Each packet contains source and destination address information. The packet, along with the address information, is called a frame. It also contains information that describes how to put all of the packets back together again at the destination. The bandwidth determines the number of packets that can be transmitted within a fixed period of time.

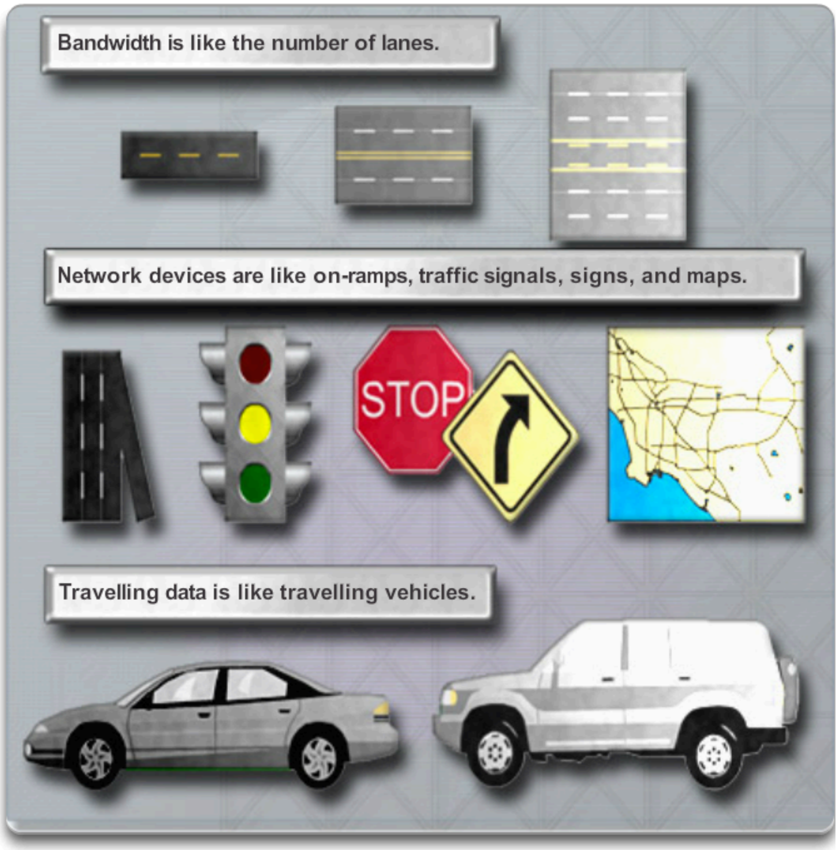
Bandwidth is measured in bits per second and is usually denoted by any of the following units of measure:

- **b/s -** bits per second
- **kb/s -** kilobits per second
- **Mb/s -** megabits per second
- **Gb/s -** gigabits per second

NOTE: 1 byte is equal to 8 bits, and is abbreviated with a capital letter B. 1 MB/s is approximately 8 Mb/s.

The figure shows how bandwidth on a network can be compared to a highway. In the highway example, the cars and trucks represent the data. The number of lanes on the highway represents the amount of cars that could travel on the highway at the same time. An eight-lane highway can handle four times the number of cars that a two-lane highway can hold.

Highway Analogy


Bandwidth is like the number of lanes.
Network devices are like on-ramps, traffic signals, signs, and maps.
STOP
Travelling data is like travelling vehicles.

The amount of time it takes data to travel from source to destination is called latency. Like a car traveling across town that encounters stop lights or detours, data is delayed by network devices and cable length. Network devices add latency when processing and forwarding data. When surfing the Web or downloading a file, latency does not normally cause problems. Time critical applications, such as Internet telephone calls, video, and gaming, can be significantly affected by latency.

Data Transmission

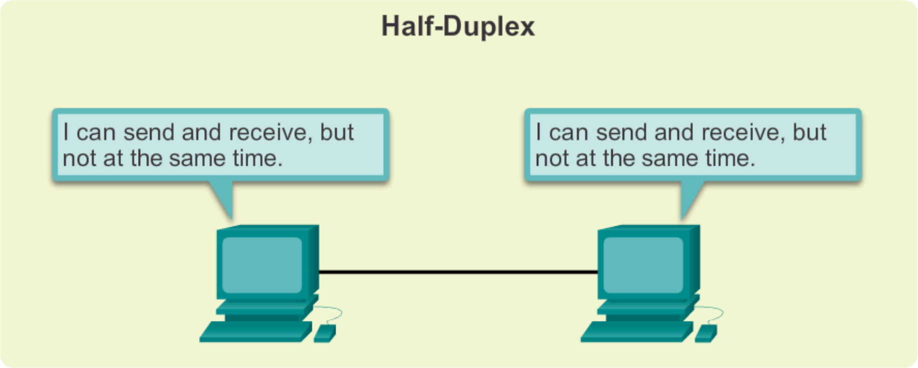
The data that is transmitted over the network can flow using one of three modes: simplex, half-duplex, or full-duplex.

Simplex

Simplex, also called unidirectional, is a single, one-way transmission. An example of simplex transmission is the signal that is sent from a TV station to your home TV.

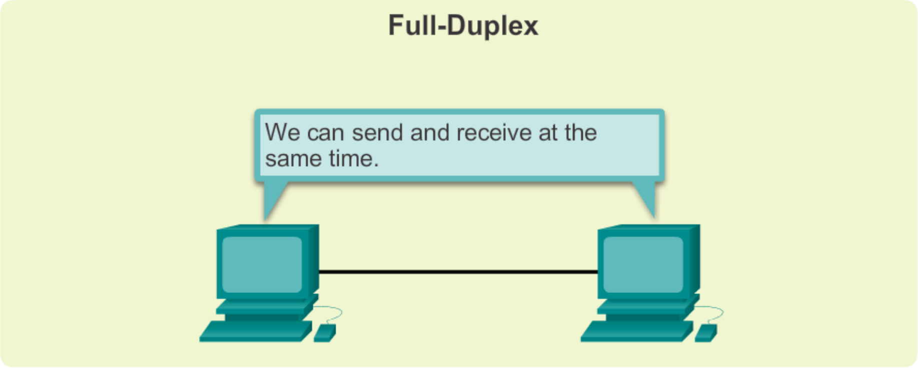
Half-Duplex

When data flows in one direction at a time it is known as half-duplex, as shown in the figure. With half-duplex, the channel of communications allows alternating transmission in two directions, but not in both directions simultaneously. Two-way radios, such as police or emergency communications mobile radios, work with half-duplex transmissions. When you press the button on the microphone to transmit, you cannot hear the person on the other end. If people at both ends try to talk at the same time, neither transmission gets through.


Half-Duplex
I can send and receive, but not at the same time.
I can send and receive, but not at the same time.

Full-Duplex

When data flows in both directions at the same time it is known as full-duplex, as shown in the figure. Although the data flows in both directions, the bandwidth is measured in only one direction. A network cable with 100 Mb/s in full-duplex mode has a bandwidth of 100 Mb/s.



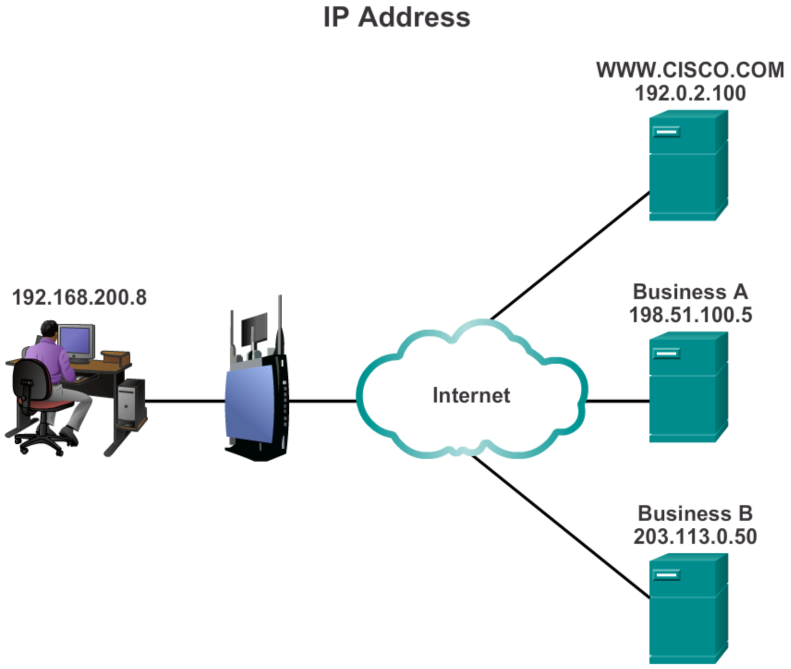
A telephone conversation is an example of full-duplex communication. Both people can talk and be heard at the same time.

Full-duplex networking technology increases network performance because data can be sent and received at the same time. Broadband technologies, such as digital subscriber line (DSL) and cable, operate in full-duplex mode. Broadband technology allows multiple signals to travel on the same wire simultaneously. With a DSL connection, for example, users can download data to the computer and talk on the telephone at the same time.

IP Addressing

Transmission Control Protocol/Internet Protocol (TCP/IP) defines the rules computers must follow to communicate with each other over the Internet. TCP is the primary Internet protocol for the reliable delivery of data. IP provides an addressing structure that is responsible for delivering data from the source computer to the destination computer.

An IP address is a number that is used to identify a device on the network. Each device on a network must have a unique IP address to communicate with other network devices. As noted earlier, a host is a device that sends or receives information on the network. Network devices are devices that move data across the network.



A person's fingerprints usually do not change. They provide a way to physically identify people. The mailing address of a person can change, as it relates to where the person lives or picks up mail. This address can change. On a host, the Media Access Control (MAC) address is assigned to the host NIC and is known as the physical address. The physical address remains the same regardless of where the host is placed on the network, in the same way that fingerprints remain with the person regardless of where the person goes. MAC addresses consist of 6 groupings of 2 hexadecimal values separated by either a dash (-) or a colon (:), for example, 00-26-6C-FC-D5-AE. Hexadecimal values are defined as a range of the numbers from 0-9 and the letters a-f.

The IP address is similar to the mailing address of a person. It is known as a logical address because it is logically assigned based on the host location. The IP address, or network address, is based on the local network and is assigned to each host by a network administrator. This process is similar to the local government assigning a street address based on the logical description of the city or village and neighborhood.

IPv4 and IPv6

In the early 1990s there was a concern about running out of IPv4 network addresses, which lead the Internet Engineering Task Force to begin looking for a replacement. This led to the development of what is now known as IPv6. Currently IPv6 is operating alongside and is beginning to replace IPv4.

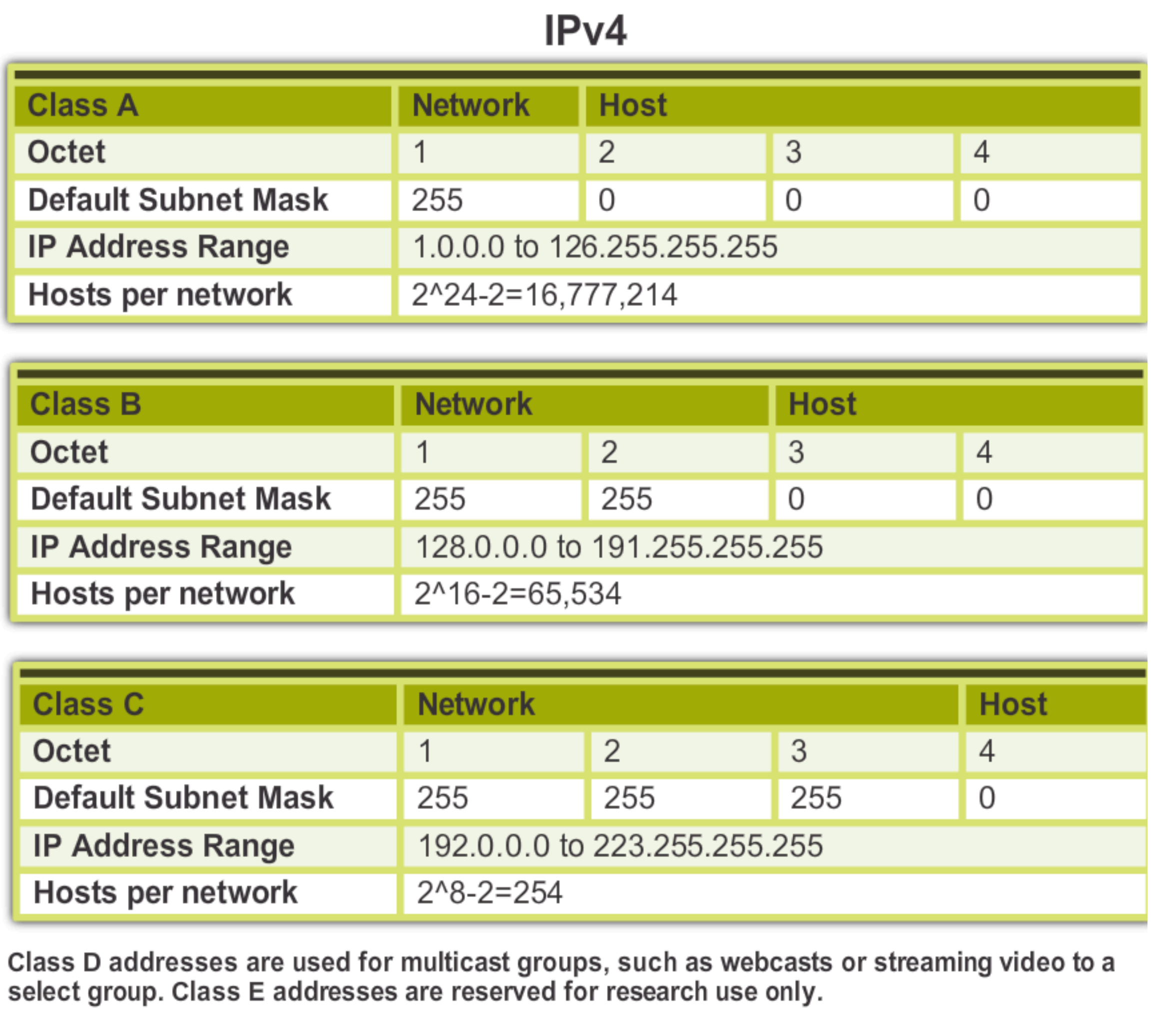
An IPv4 address consists of 32 bits with a potential address space of 2^32. In decimal notation that is approximately a 4 followed by 9 zeroes, an IPv6 address consists of 128 bits with a potential address space of 2^128. In decimal notation, that is approximately a 3 followed by 38 zeroes. With IPv6, the number of addresses available per person is approximately 10^30. If the IPv4 address space is represented by a marble, then the IPv6 address space is represented by a sphere that is almost the size of the planet Saturn.

IPv4

An IPv4 address consists of a series of 32 binary bits (ones and zeros). It is difficult for humans to read a binary IPv4 address. For this reason, the 32 bits are grouped into four segments of 8 bits called octets. An IPv4 address, even in this grouped format, is hard for humans to read, write, and remember. Therefore, each octet is presented as its decimal value, separated by a decimal point or period. This format is referred to as dotted-decimal notation.

When a host is configured with an IPv4 address, it is entered as a dotted-decimal number, such as 192.168.1.5. Imagine if you had to enter the 32-bit binary equivalent of this: 11000000101010000000000100000101. If just one bit were mistyped, the address would be different, and the host might not be able to communicate on the network.

The logical 32-bit IPv4 address is hierarchical and is composed of two parts. The first part identifies the network, and the second part identifies a host on that network. Both parts are required. For example, if a host has the IPv4 address 192.168.18.57, the first three octets, 192.168.18, identify the network portion of the address, and the last octet, 57 identifies the host. This is known as hierarchical addressing, because routers only need to communicate with networks and not individual hosts. A router is a networking device that forwards data packets across networks toward their destinations.



IPv4

Class A	Network	Host		
Octet	1	2	3	4
Default Subnet Mask	255	0	0	0
IP Address Range	1.0.0.0 to 126.255.255.255			
Hosts per network	2^24-2=16,777,214			

Class B	Network		Host	
Octet	1	2	3	4
Default Subnet Mask	255	255	0	0
IP Address Range	128.0.0.0 to 191.255.255.255			
Hosts per network	2^16-2=65,534			

Class C	Network			Host
Octet	1	2	3	4
Default Subnet Mask	255	255	255	0
IP Address Range	192.0.0.0 to 223.255.255.255			
Hosts per network	2^8-2=254			

Class D addresses are used for multicast groups, such as webcasts or streaming video to a select group. Class E addresses are reserved for research use only.

IPv4 addresses are divided into the following classes:

- **Class A** - 10.0.0.0 to 10.255.255.255
- **Class B** - 172.16.0.0 to 172.31.255.255
- **Class C** - 192.168.0.0 to 192.168.255.255

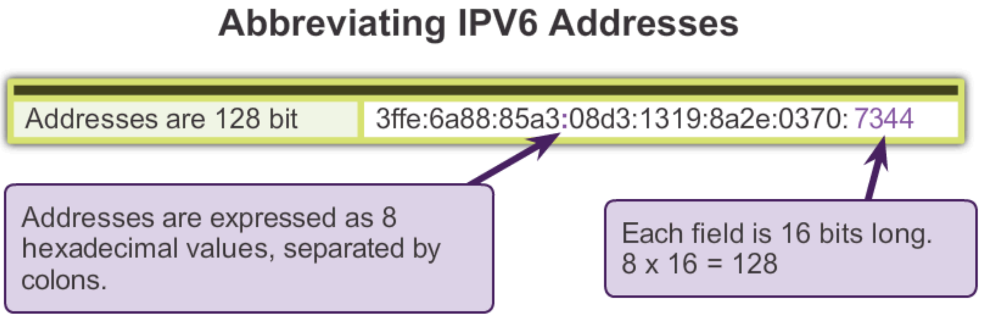
IPv4 Subnet Mask

The subnet mask indicates the network portion of an IPv4 address. Like the IPv4 address, the subnet mask is a dotted-decimal number. Usually all hosts within a LAN use the same subnet mask. The figure shows the default subnet masks for usable IPv4 addresses that are mapped to the first three classes of IPv4 addresses:

- **255.0.0.0** - Class A, which indicates that the first octet of the IPv4 address is the network portion
- **255.255.0.0** - Class B, which indicates that the first two octets of the IPv4 address is the network portion
- **255.255.255.0** - Class C, which indicates that the first three octets of the IPv4 address is the network portion

If an organization owns one Class B network but needs to provide IPv4 addresses for four LANs, the organization must subdivide the Class B address into four smaller parts. Subnetting is a logical division of a network. It provides a way to divide a network, and the subnet mask specifies how it is subdivided. An experienced network administrator typically performs subnetting. After the subnetting scheme has been created, the proper IPv4 addresses and subnet masks can be configured on the hosts in the four LANs. These skills are taught in the Cisco Networking Academy courses related to Cisco Certified Network Associate (CCNA) level networking skills.

IPv6



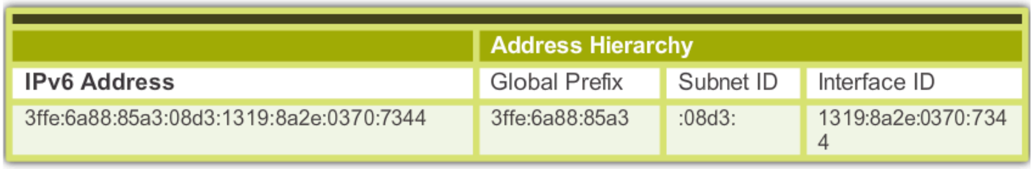
Abbreviating IPV6 Addresses

Addresses are 128 bit | 3ffe:6a88:85a3:08d3:1319:8a2e:0370: 7344

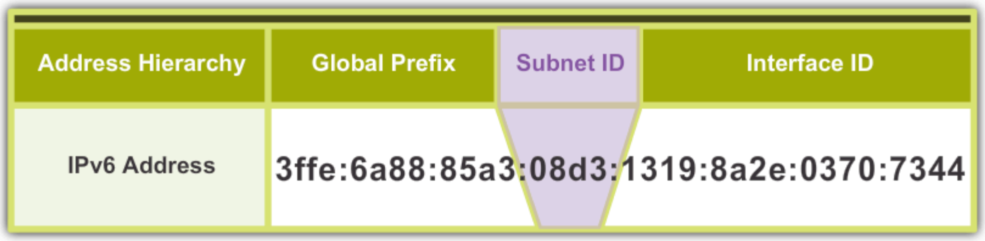
Addresses are expressed as 8 hexadecimal values, separated by colons.

Each field is 16 bits long. 8 x 16 = 128

Working with 128-bit numbers is difficult, so the IPv6 address notation represents the 128 bits as 32 hexadecimal values. The 32 hexadecimal values are further subdivided into eight fields of four hexadecimal values, using colons as delimiters. Each field of four hexadecimal values is called a block.



	Address Hierarchy		
IPv6 Address	Global Prefix	Subnet ID	Interface ID
3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344	3ffe:6a88:85a3	:08d3:	1319:8a2e:0370:7344



Address Hierarchy	Global Prefix	Subnet ID	Interface ID
IPv6 Address	3ffe:6a88:85a3	:08d3:	1319:8a2e:0370:7344

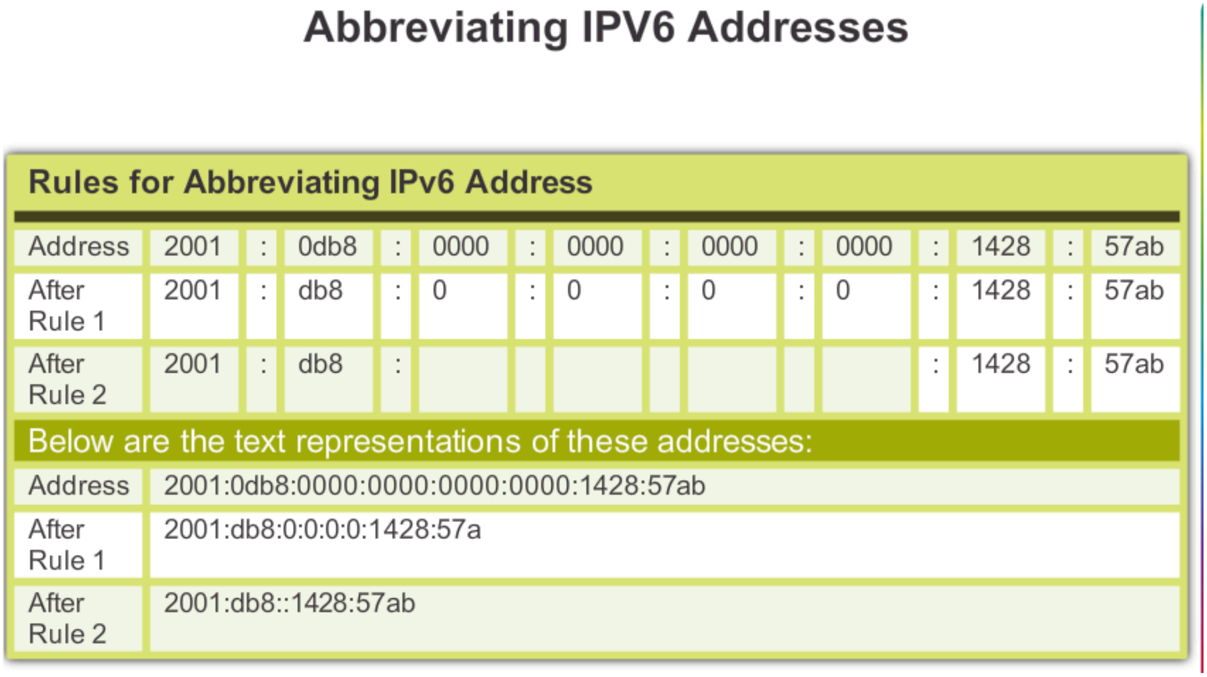
The IPv6 address has a three-part hierarchy, as shown. The global prefix, also called a site prefix, is the first three blocks of the address and is assigned to an organization by an Internet names registry. The subnet ID includes the fourth block of the address, and the interface ID includes the last four blocks of the address. The network administrator controls both the subnet and interface ID.

As an example, if a host has an IPv6 address 3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344, the global prefix address is 3ffe:6a88:85a3, the subnet ID address is 08d3, and the interface ID address is 1319:8a2e:0370:7344.

An IPv6 address can be abbreviated with the following rules:

- Omit leading zeroes in a 16-bit value.
- Replace one group of consecutive zeroes by a double colon.

Figure 2 is an example of how these rules are applied.



Abbreviating IPV6 Addresses

Rules for Abbreviating IPv6 Address

Address	2001	:	0db8	:	0000	:	0000	:	0000	:	0000	:	1428	:	57ab
After Rule 1	2001	:	db8	:	0	:	0	:	0	:	0	:	1428	:	57ab
After Rule 2	2001	:	db8	:								:	1428	:	57ab

Below are the text representations of these addresses:

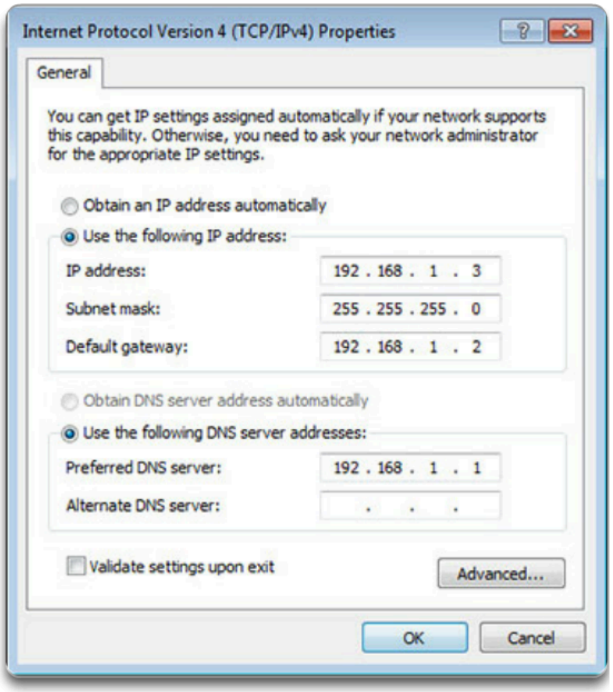
Address	2001:0db8:0000:0000:0000:0000:1428:57ab
After Rule 1	2001:db8:0:0:0:0:1428:57a
After Rule 2	2001:db8::1428:57ab

Static Addressing

In a network with a small number of hosts, it is easy to manually configure each device with the proper IP address. A network administrator who understands IP addressing should assign the addresses and should know how to choose a valid address for a particular network. The IP address that is assigned is unique for each host within the same network or subnet. This is known as static IP addressing.

To configure a static IP address on a host, go to the TCP/IPv4 Properties window of the NIC, as shown. The NIC enables a computer to connect to a network using a MAC address. Whereas the IP address is a logical address that is defined by the network administrator, a MAC address, as shown, is permanently programmed (or burned in) into the NIC when it is manufactured. The IP address of a NIC can be changed, but the MAC address never changes.

Configure Static IP Address



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 3

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 2

○ Obtain DNS server address automatically

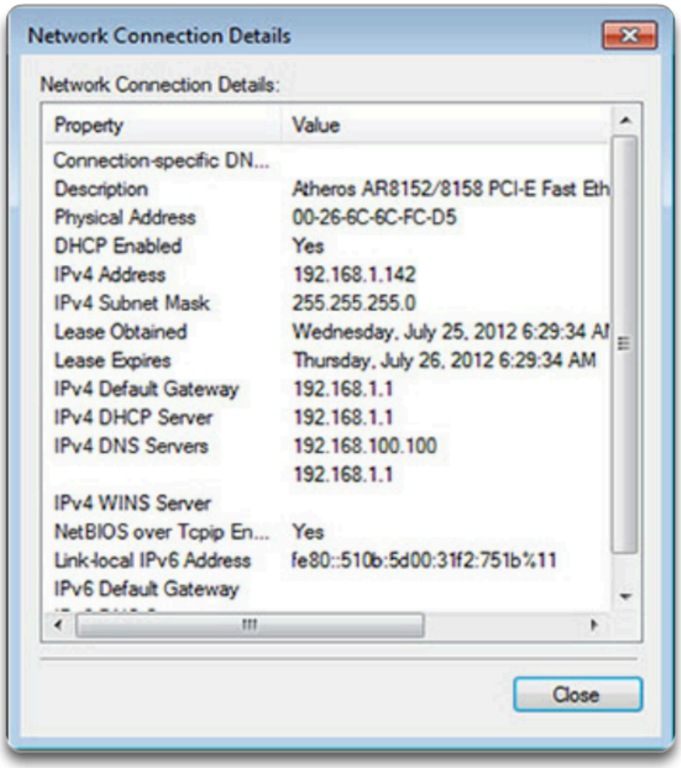
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

MAC (Physical) Address



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Atheros AR8152/8158 PCI-E Fast Eth
Physical Address	00-26-6C-6C-FC-D5
DHCP Enabled	Yes
IPv4 Address	192.168.1.142
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, July 25, 2012 6:29:34 AI
Lease Expires	Thursday, July 26, 2012 6:29:34 AM
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Servers	192.168.100.100 192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::510b:5d00:31f2:751b%11
IPv6 Default Gateway	

You can assign the following IP address configuration information to a host:

- **IP address** - identifies the computer on the network
- **Subnet mask** - is used to identify the network on which the computer is connected
- **Default gateway** - identifies the device that the computer uses to access the Internet or another network
- **Optional values** - such as the preferred Domain Name System (DNS) server address and the alternate DNS server address

In Windows 7, use the following path:

Start > Control Panel > Network and Sharing Center > Change adapter setting > right-click **Local Area Connection > Properties > TCP/IPv4 > Properties > Use the following IP address > Use the following DNS server addresses > OK > OK**

In Windows Vista, use the following path:

Start > Control Panel > Network and Sharing Center > Manage network connections > right-click **Local Area Connection > Properties > TCP/IPv4 > Properties > Use the following IP address > Use the following DNS server addresses > OK > OK**

In Windows XP, use the following path:

Start > Control Panel > Network Connections > right-click **Local Area Connection > Properties > TCP/IP > Properties > Use the following IP address > Use the following DNS server addresses > OK > OK**

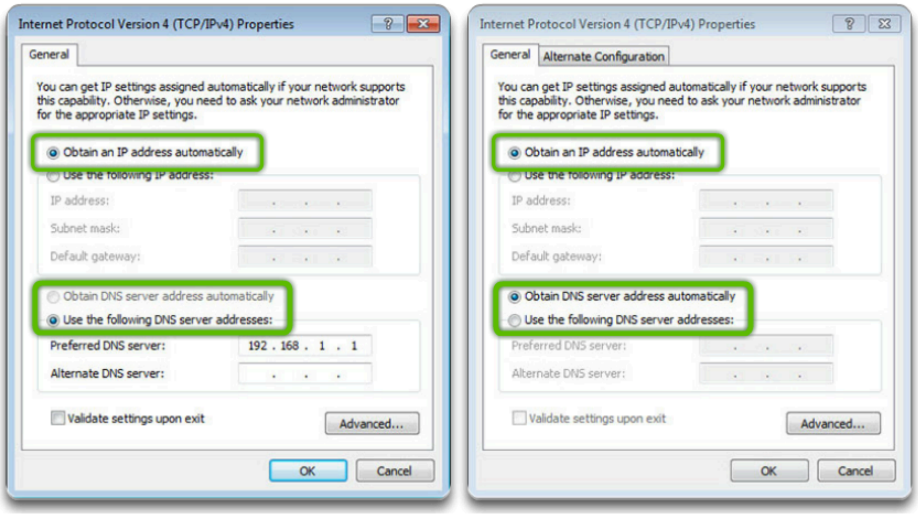
DHCP Addressing

If more than a few computers are a part of the LAN, manually configuring IP addresses for every host on the network can be time consuming and prone to errors. A Dynamic Host Configuration Protocol (DHCP) server automatically assigns IP addresses, which simplifies the addressing process. Automatically configuring TCP/IP also reduces the possibility of assigning duplicate or invalid IP addresses.

The DHCP server maintains a list of IP addresses to assign and manages the process so that every device on the network receives a unique IP address. When the DHCP server receives a request from a host, the server selects IP address information from a set of predefined addresses that are stored in a database. When the IP address information is selected, the DHCP server offers these values to the requesting host on the network. If the host accepts the offer, the DHCP server assigns the IP address for a specific period of time. This is called leasing. When the lease expires, the DHCP server can use this address for another computer that joins the network. A device, however, can renew its lease to retain the IP address.

Before a computer on the network can take advantage of the DHCP services, the computer must be able to identify the server on the local network. A computer can be configured to accept an IP address from a DHCP server by selecting the **Obtain an IP address automatically** option in the NIC configuration window, as shown in Figure 1. When a computer is set to obtain an IP address automatically, all other IP addressing configuration boxes are not available. The DHCP settings are configured the same for a wired or wireless NIC.

DNS Configurations While Using DHCP



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

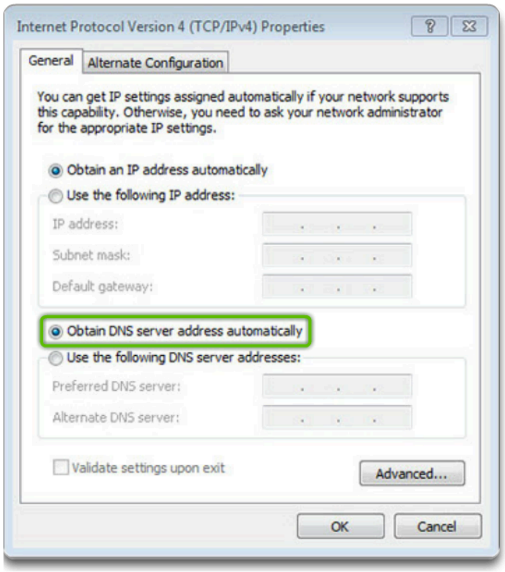
● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

A computer continually requests an IP address at 5-minute intervals from a DHCP server. If your computer cannot communicate with the DHCP server to obtain an IP address, the Windows OS automatically assigns a link-local IP. If your computer is assigned a link-local IP address, which is in the range of 169.254.0.0 to 169.254.255.255, your computer can only communicate with computers connected to the same network within this IP address range.

Obtain DNS Address from DHCP



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

A DHCP server automatically assigns the following IP address configuration information to a host:

- IP address
- Subnet mask
- Default gateway
- Optional values, such as a DNS server address, as shown in Figure 2

In Windows 7, use the following path:

Start > Control Panel > Network and Sharing Center > Change adapter setting > right-click **Local Area Connection > Properties > TCP/IPv4 > Properties >** select radio button **Obtain an IP address automatically > OK > OK**

In Windows Vista, use the following path:

Start > Control Panel > Network and Sharing Center > Manage network connections > right-click **Local Area Connection > Properties > TCP/IPv4 > Properties >** select radio button **Obtain an IP address automatically > OK > OK**

In Windows XP, use the following path:

Start > Control Panel > Network Connections > right-click **Local Area Connection > Properties > TCP/IP > Properties >** select radio button **Obtain an IP address automatically > OK > OK**

Configuring Alternate IP Settings

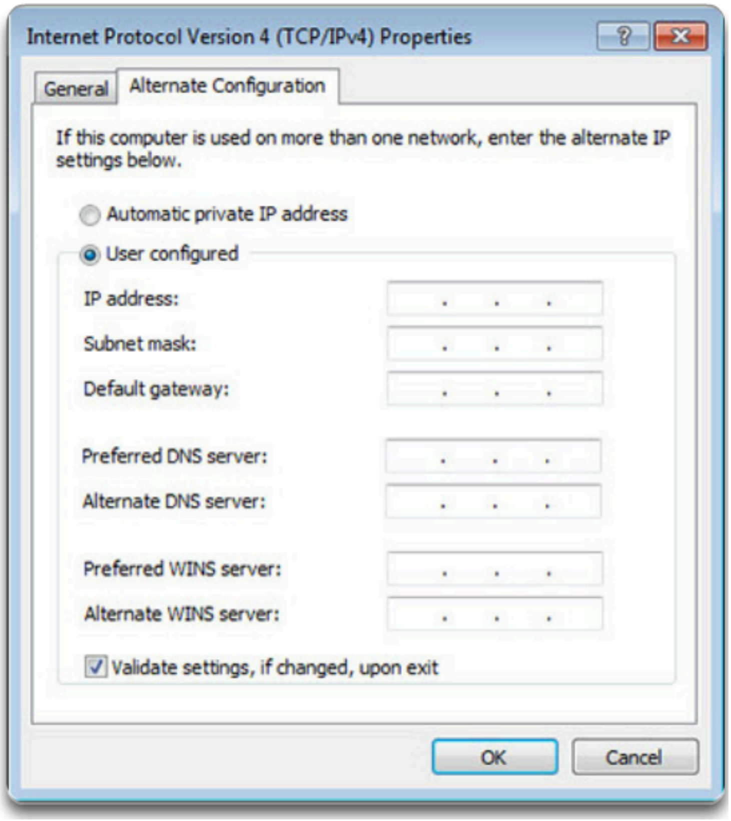
Setting up an alternate IP configuration in Windows simplifies moving between a network that requires using DHCP and a network that uses static IP settings. If a computer cannot communicate with the DHCP server on the network, Windows uses the alternate IP configuration assigned to the NIC. The alternate IP configuration also replaces the Automatic IP Addressing (APIPA) address that is assigned by Windows when a DHCP server cannot be contacted.

To create the alternate IP configuration, as shown in Figure 3, click the **Alternate Configuration** tab located in the NIC Properties window.

To access a DNS server, a computer uses the IP address configured in the DNS settings of the NIC in the computer. DNS resolves or maps host names and URLs to IP addresses.

All Windows computers contain a DNS cache that stores host names that have recently been resolved. The cache is the first place that the DNS client looks for host name resolution. Because it is a location in memory, the cache retrieves resolved IP addresses more quickly than using a DNS server and does not create network traffic.

Alternate IP Configuration



If this computer is used on more than one network, enter the alternate IP settings below.

○ Automatic private IP address

● User configured

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

Preferred DNS server: . . .

Alternate DNS server: . . .

Preferred WINS server: . . .

Alternate WINS server: . . .

☑ Validate settings, if changed, upon exit

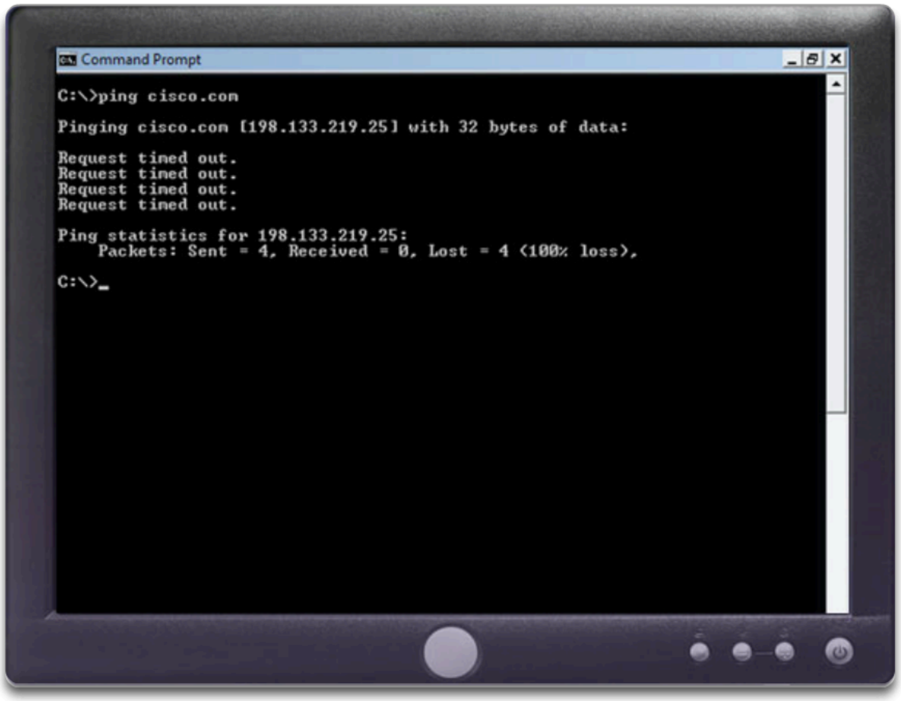
ICMP

Internet Control Message Protocol (ICMP) is used by devices on a network to send control and error messages to computers and servers. There are several different uses for ICMP, such as announcing network errors, announcing network congestion, and troubleshooting.

Ping is commonly used to test connections between computers. **Ping** is a simple but highly useful command-line utility used to determine whether a specific IP address is accessible. To see a list of options that you can use with the **ping** command, type C:\>**ping /?** in the Command Prompt window.

The **ipconfig** command is another useful command-line utility used to verify that a NIC has a valid IP address. To display full configuration information of all network adapters, type C:\> **ipconfig /all** in the Command Prompt window. You can **ping** the IP address obtained from the **ipconfig /all** command to test IP connectivity.

Use the Ping Command to Find an IP Address



```
C:\>ping cisco.com

Pinging cisco.com [198.133.219.25] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>_
```

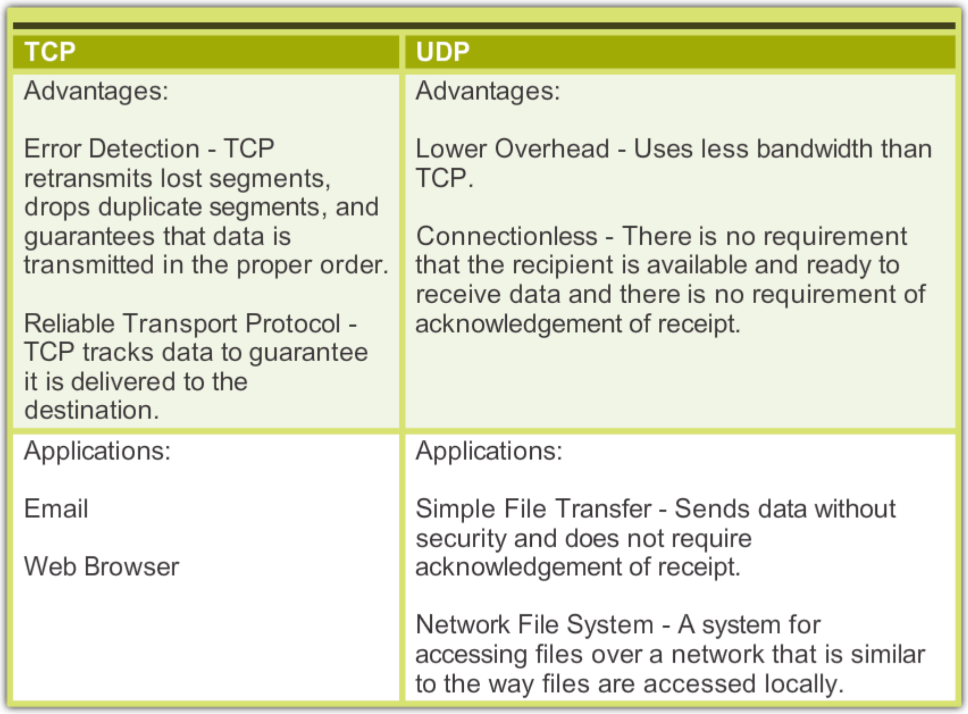
Ping works by sending an ICMP echo request to a destination computer or other network device. The receiving device then sends back an ICMP echo reply message to confirm connectivity. Echo requests and echo replies are test messages that determine if devices can send packets to each other. Four ICMP echo requests (pings) are sent to the destination computer. If it is reachable, the destination computer responds with four ICMP echo replies. The percentage of successful replies can help you to determine the reliability and accessibility of the destination computer. Other ICMP messages report undelivered packets and whether a device is too busy to handle the packet.

You can also use **ping** to find the IP address of a host when that host's name is known. If you **ping** the name of a website, for example, cisco.com, as shown in the figure, the IP address of the server displays.

Common Ports and Protocols TCP & UDP

A protocol is a set of rules. Internet protocols are sets of rules governing communication within and between computers on a network. Protocol specifications define the format of the messages that are exchanged. A letter sent through the postal system also uses protocols. Part of the protocol specifies where the delivery address on the envelope needs to be written. If the delivery address is written in the wrong place, the letter cannot be delivered.

Timing is crucial for the reliable delivery of packets. Protocols require messages to arrive within certain time intervals so that computers do not wait indefinitely for messages that might have been lost. Systems maintain one or more timers during the transmission of data. Protocols also initiate alternative actions if the network does not meet the timing rules.



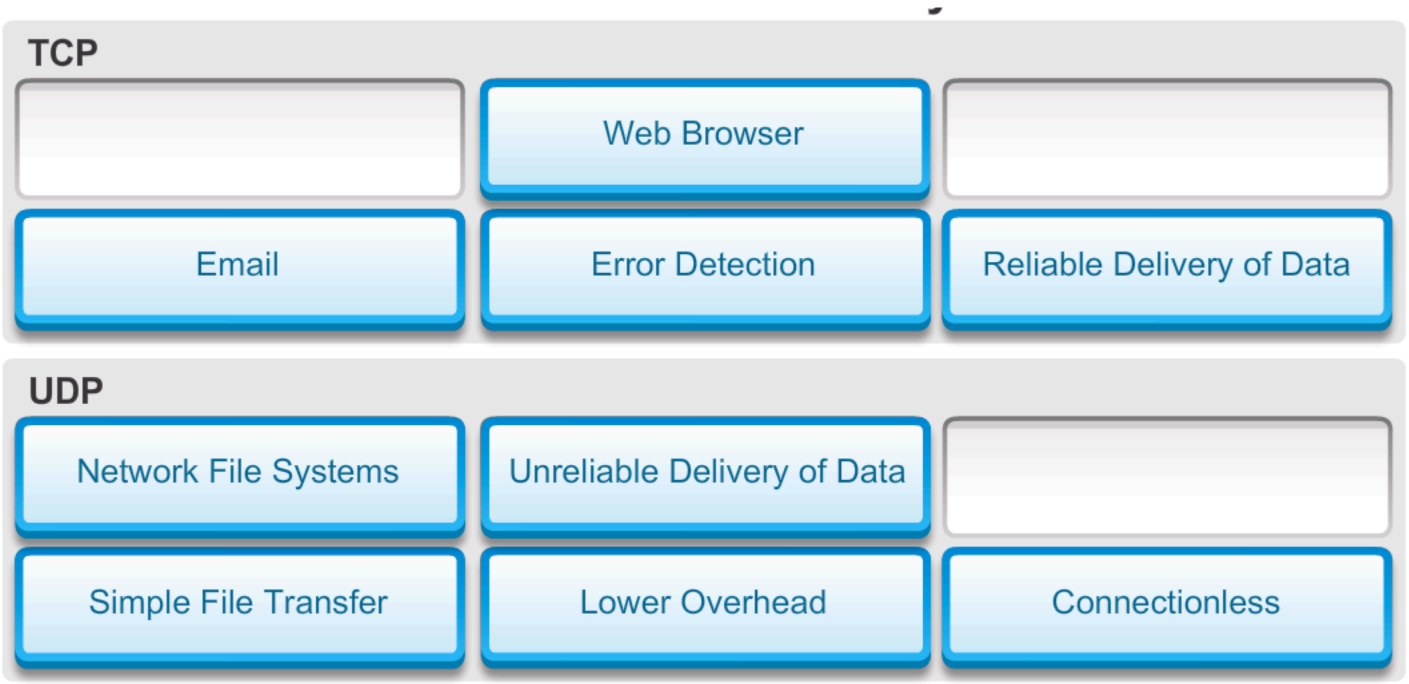
TCP	UDP
Advantages: Error Detection - TCP retransmits lost segments, drops duplicate segments, and guarantees that data is transmitted in the proper order. Reliable Transport Protocol - TCP tracks data to guarantee it is delivered to the destination.	Advantages: Lower Overhead - Uses less bandwidth than TCP. Connectionless - There is no requirement that the recipient is available and ready to receive data and there is no requirement of acknowledgement of receipt.
Applications: Email Web Browser	Applications: Simple File Transfer - Sends data without security and does not require acknowledgement of receipt. Network File System - A system for accessing files over a network that is similar to the way files are accessed locally.

These are the main functions of protocols:

- Identifying and handling errors
- Compressing the data
- Deciding how data is to be divided and packaged
- Addressing data packets
- Deciding how to announce the sending and receiving of data packets

Devices and computers connected to the Internet use a protocol suite called TCP/IP to communicate with each other. The information is transmitted most often via two protocols, TCP and UDP, as shown in the figure.

In the design of a network, you must determine the protocols that are going to be used. Some protocols are proprietary and only work on specific equipment, while other protocols are open standard and work on a variety of equipment.



TCP

Web Browser

Email

Error Detection

Reliable Delivery of Data

UDP

Network File Systems

Unreliable Delivery of Data

Simple File Transfer

Lower Overhead

Connectionless

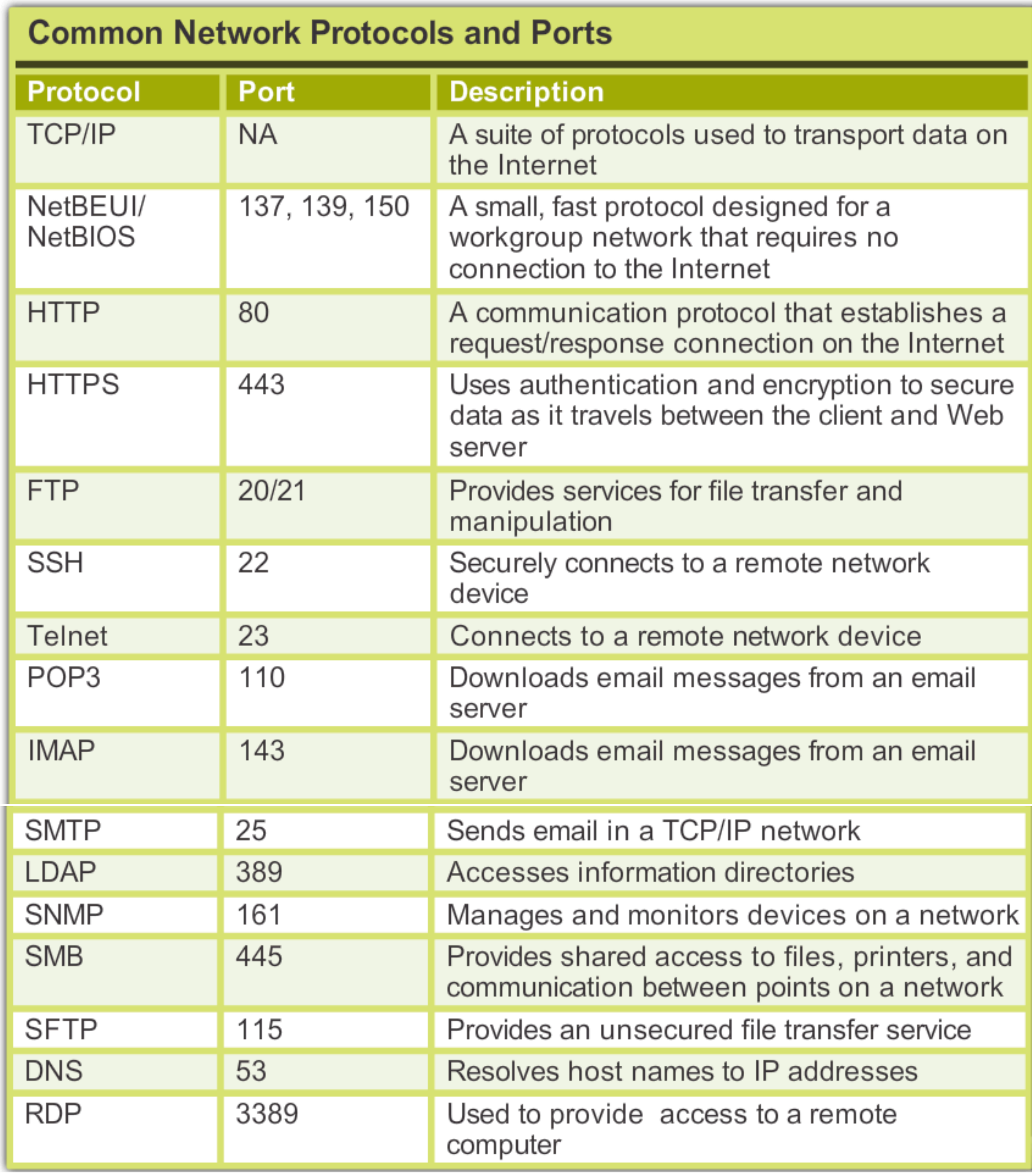
TCP and UDP Protocols and Ports

When the TCP/IP protocol stack is enabled, other protocols can communicate on specific ports. For example, HTTP uses port 80 by default. A port is a numeric identifier used to keep track of specific conversations. Every message that a host sends contains both a source and destination port.

Network software applications use these protocols and ports to perform functions over the Internet or over a network. Some network software applications include services to host a web page, send email, and transfer files. These services may be provided by a single server or by several servers. Clients use well-known ports for each service so that the client requests can be identified by using a specific destination port.

To understand how networks and the Internet work, you must be familiar with commonly used protocols and associated ports. Some uses of these protocols are to connect to a remote network device, convert a website URL to an IP address, and transfer data files. You will encounter other protocols as your experience in IT grows, but they are not used as often as the common protocols described here.

The figure summarizes some of the more common network and Internet protocols, and the port number used by these protocols. The more you understand about each of these protocols, the more you will understand how networks and the Internet work.



Common Network Protocols and Ports

Protocol	Port	Description
TCP/IP	NA	A suite of protocols used to transport data on the Internet
NetBEUI/ NetBIOS	137, 139, 150	A small, fast protocol designed for a workgroup network that requires no connection to the Internet
HTTP	80	A communication protocol that establishes a request/response connection on the Internet
HTTPS	443	Uses authentication and encryption to secure data as it travels between the client and Web server
FTP	20/21	Provides services for file transfer and manipulation
SSH	22	Securely connects to a remote network device
Telnet	23	Connects to a remote network device
POP3	110	Downloads email messages from an email server
IMAP	143	Downloads email messages from an email server
SMTP	25	Sends email in a TCP/IP network
LDAP	389	Accesses information directories
SNMP	161	Manages and monitors devices on a network
SMB	445	Provides shared access to files, printers, and communication between points on a network
SFTP	115	Provides an unsecured file transfer service
DNS	53	Resolves host names to IP addresses
RDP	3389	Used to provide access to a remote computer