How Computers Find Each Other on Networks

Objectives

- Describe how computers and other devices are addressed on a network
- Explain how host names and domain names work
- Identify how ports and sockets work at the OSI Transport layer
- Demonstrate how IP addresses are assigned and formatted at the OSI Network layer
- Use command-line tools to troubleshoot problems with network addresses

An Overview of Addressing on Networks

- Four addressing methods:
  - Application layer FQDNs, computer names, and host names www.vanierCollege.qc.ca
  - Transport layer port numbers
  - Network layer IP address
    - IPv4 addresses have 32 bits and are written as four decimal numbers called octets
    - IPv6 addresses have 128 bits and are written as eight blocks of hexadecimal numbers
  - Data Link layer MAC address
    - Also called physical address

MAC Addresses

- Traditional MAC addresses contain two parts
  - First 24 bits are known as the OUI (Organizationally Unique Identifier) or block ID or company-ID
    - Assigned by the IEEE
  - Last 24 bits make up the extension identifier or device ID
    - Manufacturer's assign each NIC a unique device ID

MAC Addresses

Figure 2-1 NIC with MAC address

How Host Names and Domain Names Work

- Character-based names are easier to remember than numeric IP addresses
- Last part of an FQDN is called the top-level domain (TLD)
- Domain names must be registered with an Internet naming authority that works on behalf of ICANN
  - ICANN restricts what type of hosts can be associated with .arpa, .mil, .int, .edu, and .gov
- Name resolution is the process of discovering the IP address of a host when you know the FQDN

How Host Names and Domain Names Work

Table 2-1 Some well-known top-level domains

Domain suffix	Type of organization
ARPA	Reverse lookup domain (special Internet function)
COM	Commercial
EDU	Educational
GOV	Government
ORG	Noncommercial organization (such as a nonprofit agency)
NET	Network (such as an ISP)
INT	International Treaty Organization
MIL	United States military organization
BIZ	Businesses
INFO	Unrestricted use
AERO	Air-transport industry
COOP	Cooperatives

DNS (Domain Name System)

- DNS is an Application layer client-server system of computers and databases made up of these elements:
  - namespace - the entire collection of computer names and their associated IP addresses stored in databases on DNS name servers around the globe
  - name servers - hold databases, which are organized in a hierarchical structure
  - resolvers - a DNS client that requests information from DNS name servers

How Name Servers Are Organized

- DNS name servers are organized in a hierarchical structure
- At the root level, 13 clusters of root server hold information used to locate top-level domain (TLD) servers
- TLD servers hold information about authoritative servers
  - The authority on computer names and their IP address for computer in their domains

How Name Servers Are Organized

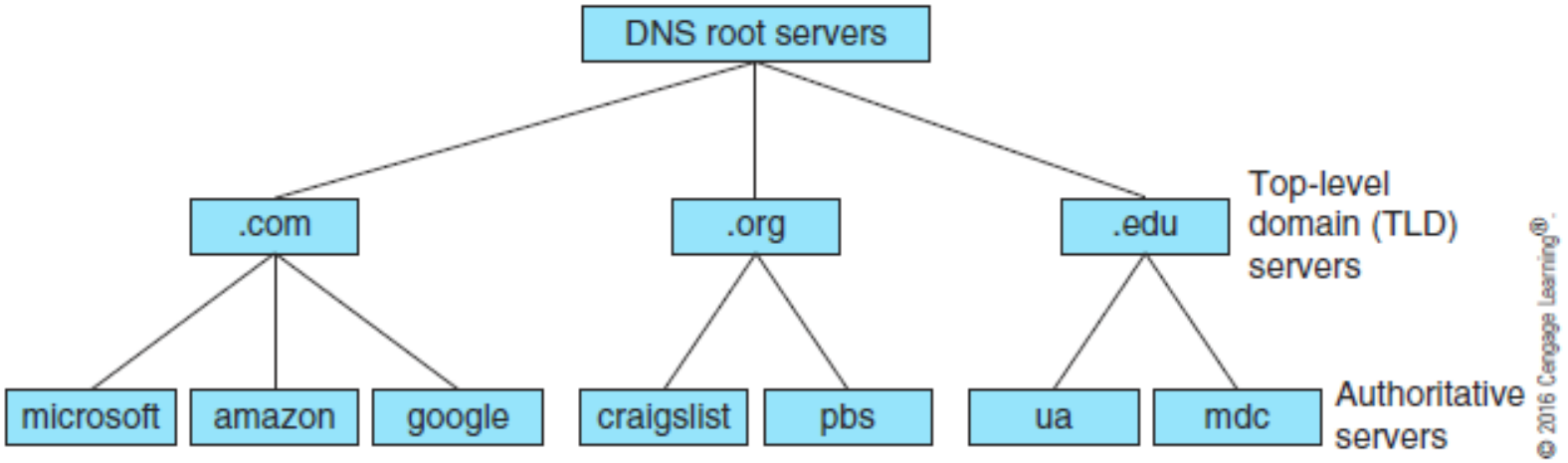

Figure 2-6 Hierarchy of name servers

How Name Servers Are Organized

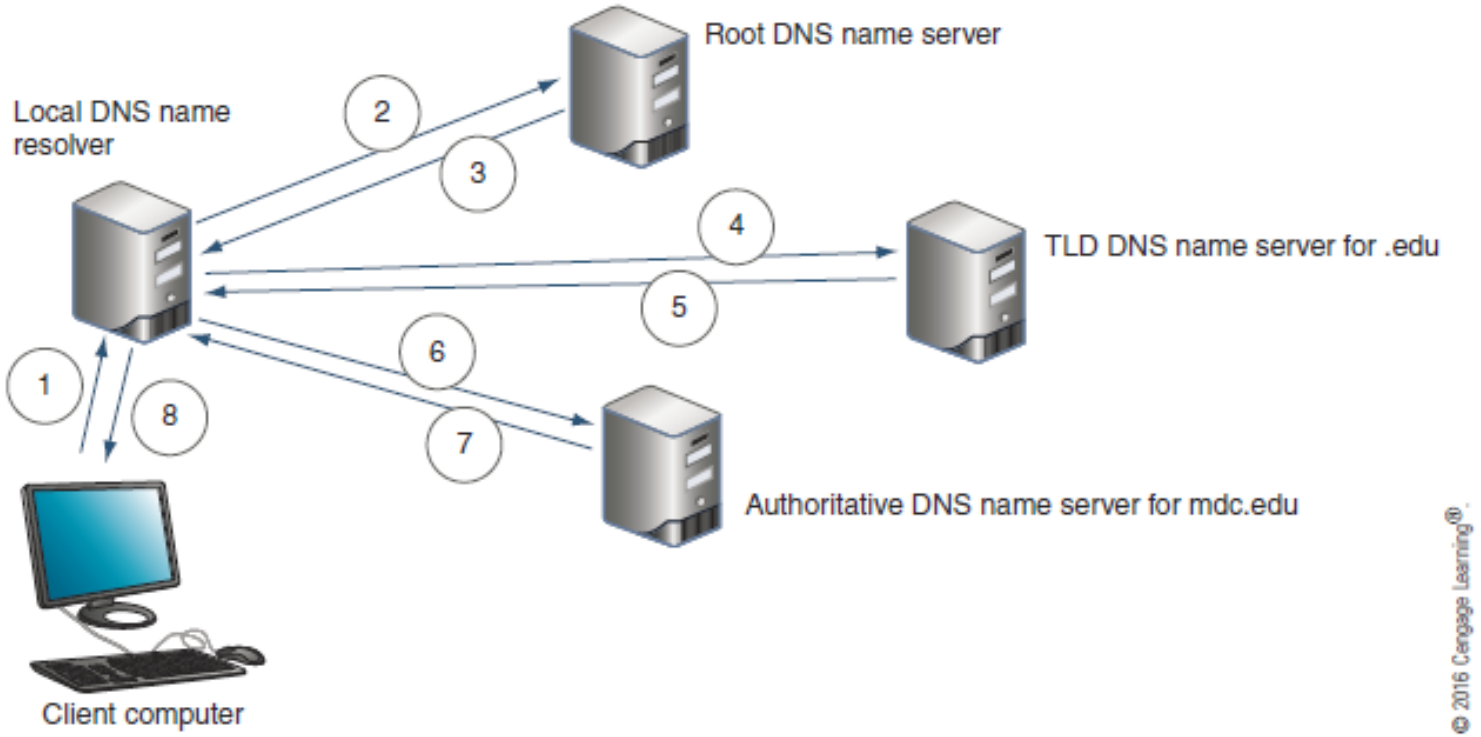

Figure 2-7 Queries for name resolution for *www.mdc.edu*

How Name Servers Are Organized

- Ways the resolution process can get more complex:
  - Caching-only server - when it receives a request for information that is not stored in its DNS cache, it will first query the company's authoritative name server
  - Name servers within a company might not have access to root servers
  - A TLD name server might be aware of an intermediate name server rather than the authoritative name server

Recursive and Iterative Queries

- Two types of DNS requests:
  - Recursive - a query that demands a resolution or the answer “It can’t be found”
  - Iterative - a query where the local server issues queries to other servers
    - Other servers only provide information if they have it
    - Do not demand a resolution

DNS Zones and Zone Transfers

- DNS follows a distributed database model
  - Data is distributed over thousands of server so that DNS will not fail if one or a handful of servers experience errors
- DNS zone - the domains an organization is responsible for managing
- Primary DNS server holds the authoritative DNS database for the organization
- Zone transfer - the process where a secondary DNS server makes a request to the primary server for a database update

DNS Server Software

- BIND (Berkeley Internet Name Domain) - most popular DNS server software
  - Open source - the term for software whose code is publicly available for use and modification
- Microsoft DNS Server - built-in DNS service in the Windows Server OS
- Split DNS design - Internal and external DNS queries are handled by different DNS servers
  - Also called a split-horizon DNS

DNS Server Software

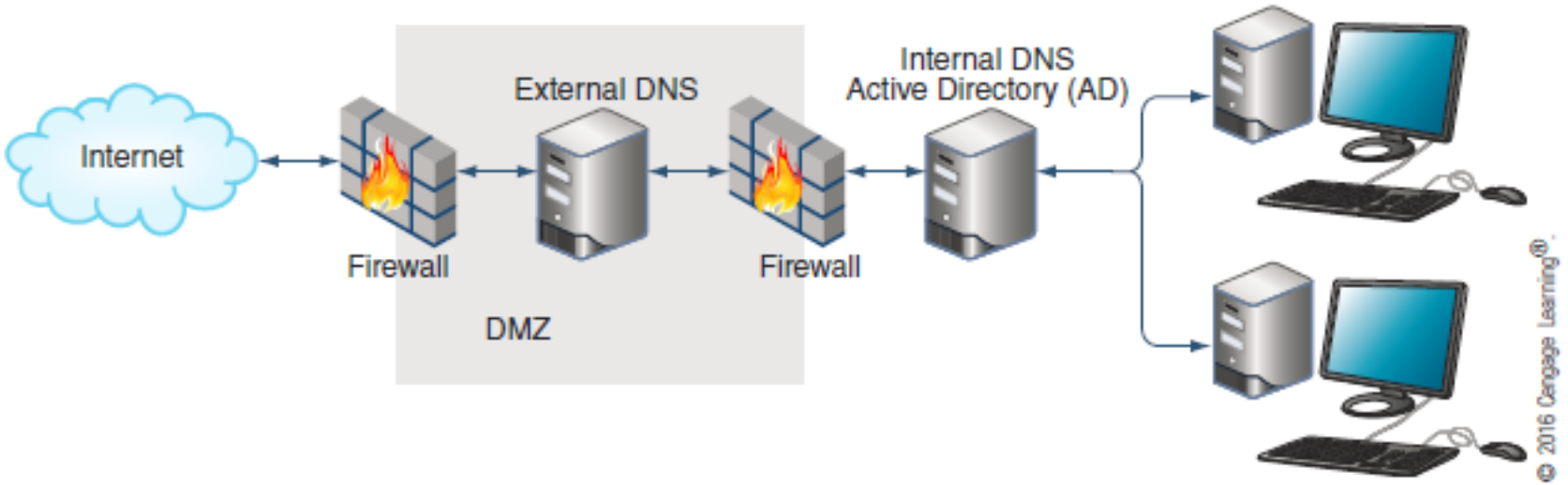

Figure 2-8 DNS services handled by two different servers so that the internal network remains protected

DDNS (Dynamic DNS)

- DDNS - a protocol used along with monitoring software to monitor the IP addresses dynamically assigned to your home network by your ISP
  - Manages dynamic updates to its DNS records for domain names for home Web sites
- Home routers sometimes provide the monitoring software embedded in the router firmware

How Ports and Sockets Work

- Port numbers - ensure data is transmitted to the correct application
- Socket - consists of host's IP address and the port number of an application running on the host
  - Colon separates the two values
  - Example - 10.43.3.87:23
- Port numbers are divided into three types:
  - Well-known ports - 0 to 1023
  - Registered ports - 1024 to 49151
  - Dynamic and private ports - 49152 to 65535

How Ports and Sockets Work

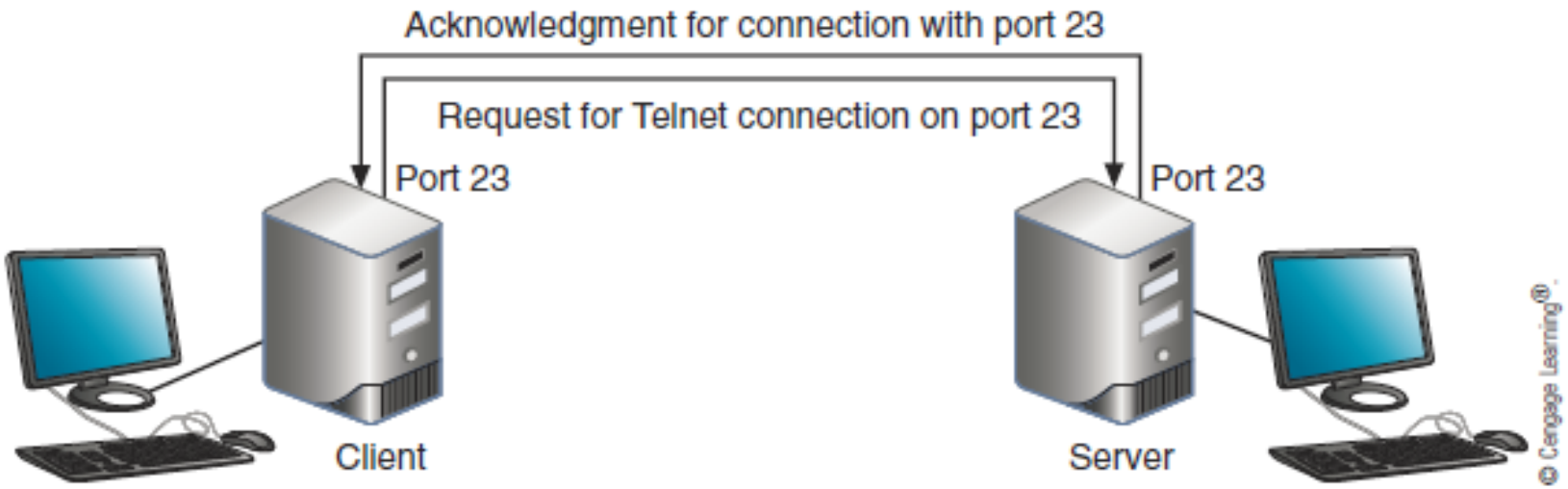

Figure 2-10 A virtual connection for the Telnet service

How IP Addresses Are Formatted and Assigned

- Two types of IP addresses:
  - IPv4 - a 32-bit address
  - IPv6 - a 128-bit address

How IPv4 Addresses Are Formatted and Assigned

- IPv4 addresses
  - 32-bit address organized into four groups of 8 bits each (known as octets)
  - Each of the four octets can be any number from 0 to 255
  - Some IP addresses are reserved

Classes of IP Addresses

- IPv4 addresses are divided into five classes:
  - Class A, Class B, Class C, Class D, and Class E
- When class licenses were available from IANA:
  - Class A license was for a single octet
  - Class B license was for the first two octets
  - Class C license was for the first three octets
  - Class D and Class E addresses were not available for general use
    - Class D begin with 224-239 and are used for multicasting and Class E begin with octets 240-254 and are used for research

Classes of IP Addresses

Table 2-4 IP address classes

Class	Network octets*	Approximate number of possible networks or licenses	Approximate number of possible IP addresses in each network
A	1.x.y.z to 126.x.y.z	126	16 million
B	128.0.x.y to 191.255.x.y	16,000	65,000
C	192.0.0.x to 223.255.255.x	2 million	254

*An x, y, or z in the IP address stands for an octet that is used to identify hosts.

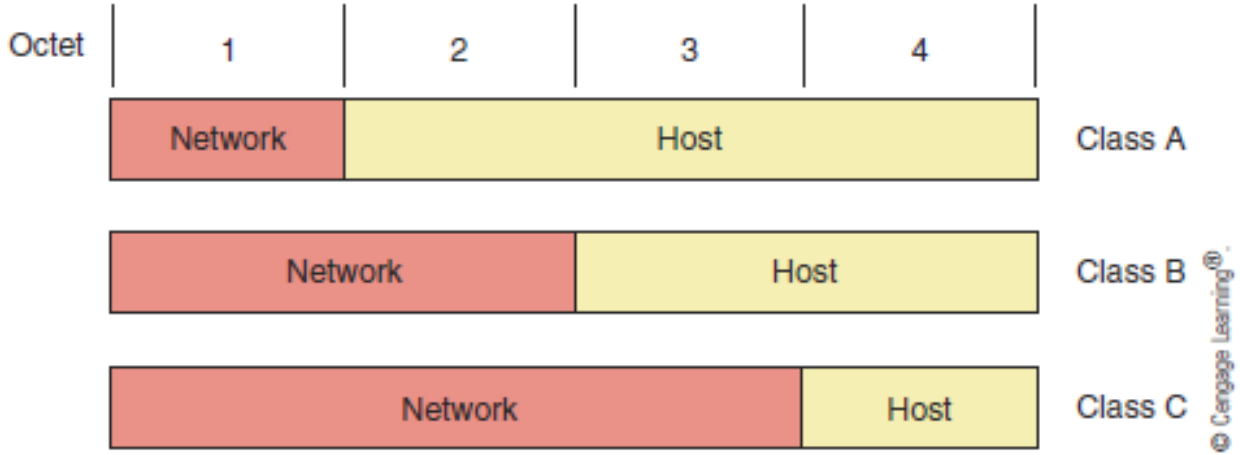

Figure 2-11 The network portion and host portion for each class of IP addresses

Classes of IP Addresses

Table 2-5 Reserved IP addresses

IP address	How it is used
255.255.255.255	Used for broadcast messages by TCP/IP background processes; a broadcast message is read by every node on the network
0.0.0.0	Currently unassigned
127.0.0.1	Indicates your own computer and is called the loopback address

How a DHCP Server Assigns IP Addresses

- Static IP addresses are assigned manually by the network administrator
- Dynamic IP addresses are automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server
- If a computer configured to use DHCP is unable to lease an IPv4 address from the DHCP server
  - It uses an Automatic Private IP Addressing (APIPA) address in the address range 169.254.0.1 through 169.254.255.254

Public and Private IP Addresses

- Class A, B, and C licensed IP addresses are available for use on the Internet
  - Called public IP addresses
- A company can use private IP addresses on its private networks
- IEEE recommends the following IP addresses be used for private networks:
  - 10.0.0.0 through 10.255.255.255
  - 172.16.0.0 through 172.31.255.255
  - 192.168.0.0 through 192.168.255.255

Address Translation, NAT, and PAT

- Network Address Translation (NAT) - a technique designed to conserve public IP addresses needed by a network
- Address translation - process where a gateway device substitutes the private IP addresses with its own public address
  - When these computers need access to other networks or Internet
- Port Address Translation (PAT) - process of assigning a TCP port number to each ongoing session between a local host and Internet host

Address Translation, NAT, and PAT

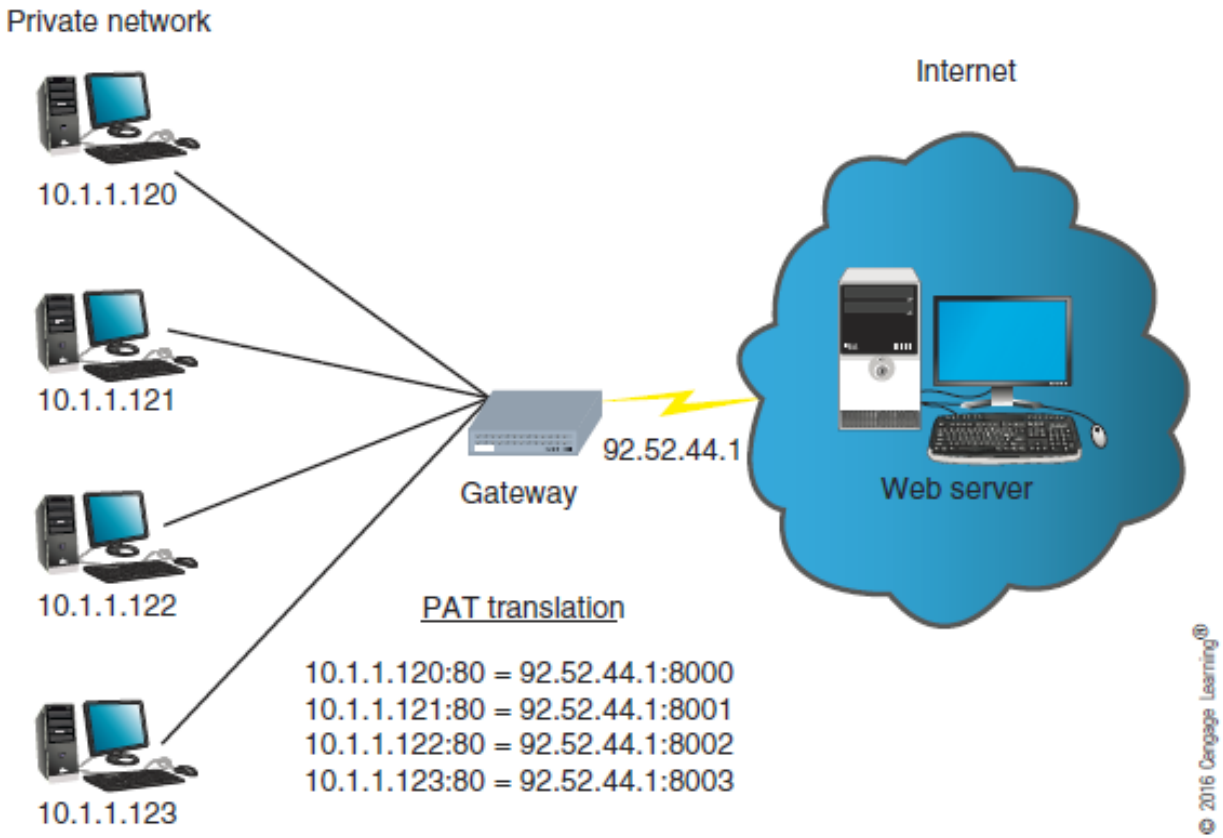

Figure 2-15 PAT (Port Address Translation)

Address Translation, NAT, and PAT

- Two variations of NAT to be aware of:
  - SNAT (Static Network Address Translation) - the gateway assigns the same public IP address to a host each time it makes a request to access the Internet
  - DNAT (Dynamic Network Address Translation) - the gateway has a pool of public address that it is free to assign to a local host when it makes a request to access the Internet

How IPv6 Addresses Are Formatted and Assigned

- An IPv6 address has 128 bits written as eight blocks of hexadecimal numbers separated by colons
  - Ex: 2001:0000:0B80:0000:0000:00D3:9C5A:00CC
  - Each block is 16 bits
  - Leading zeros in a four-character hex block can be eliminated
  - If blocks contain all zeroes, they can be written as double colons (::), only one set of double colons is used in an IP address
  - Therefore, above example can be written:
    - 2001:0000:B80::D3:9C5A:CC

How IPv6 Addresses Are Formatted and Assigned

- IPv6 terminology:
  - Link (sometimes called local link) - any LAN bounded by routers
  - An interface is a node's attachment to a link
  - Tunneling - a method used by IPv6 to transport IPv6 packets through or over an IPv4 network
  - Interface ID - the last 64 bits or four blocks of an IPv6 address that identify the interface
  - Neighbors - two or more nodes on the same link

Types of IP Addresses

- Unicast address - specifies a single node on a network
  - Global unicast address - can be routed on the Internet
  - Link local unicast address - can be used for communicating with nodes in the same link
- Multicast address - packets are delivered to all nodes on a network
- Anycast address - can identify multiple destinations, with packets delivered to the closest destination

Types of IP Addresses

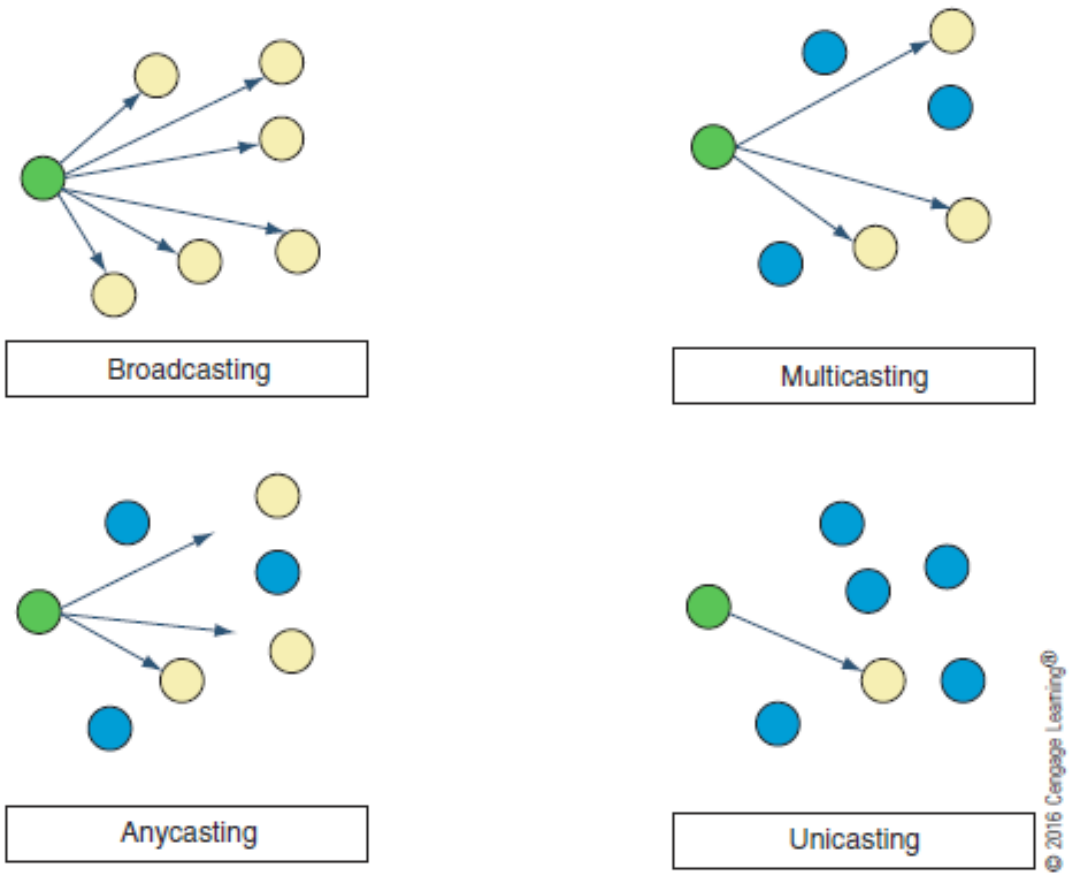

Figure 2-18 Concepts of broadcasting, multicasting, anycasting, and unicasting

Types of IP Addresses

Global address

3 bits	45 bits	16 bits	64 bits
001	Global routing prefix	Subnet ID	Interface ID

Link local address

64 bits	64 bits
1111 1110 1000 0000 0000 0000 0000 .... 0000 FE80::/64	Interface ID

Figure 2-19 Two types of IPv6 addresses

Table 2-6 Address prefixes for types of IPv6 addresses

IP address type	Address prefix	Notes
Global unicast	2000::/3	First 3 bits are always 001
Link local unicast	FE80::/64	First 64 bits are always 1111 1110 1000 0000 0000 0000 0000
Unique local unicast	FC00::/7	First 7 bits are always 1111 110
	FD00::/8	First 8 bits are always 1111 1101
Multicast	FF00::/8	First 8 bits are always 1111 1111

Types of IP Addresses

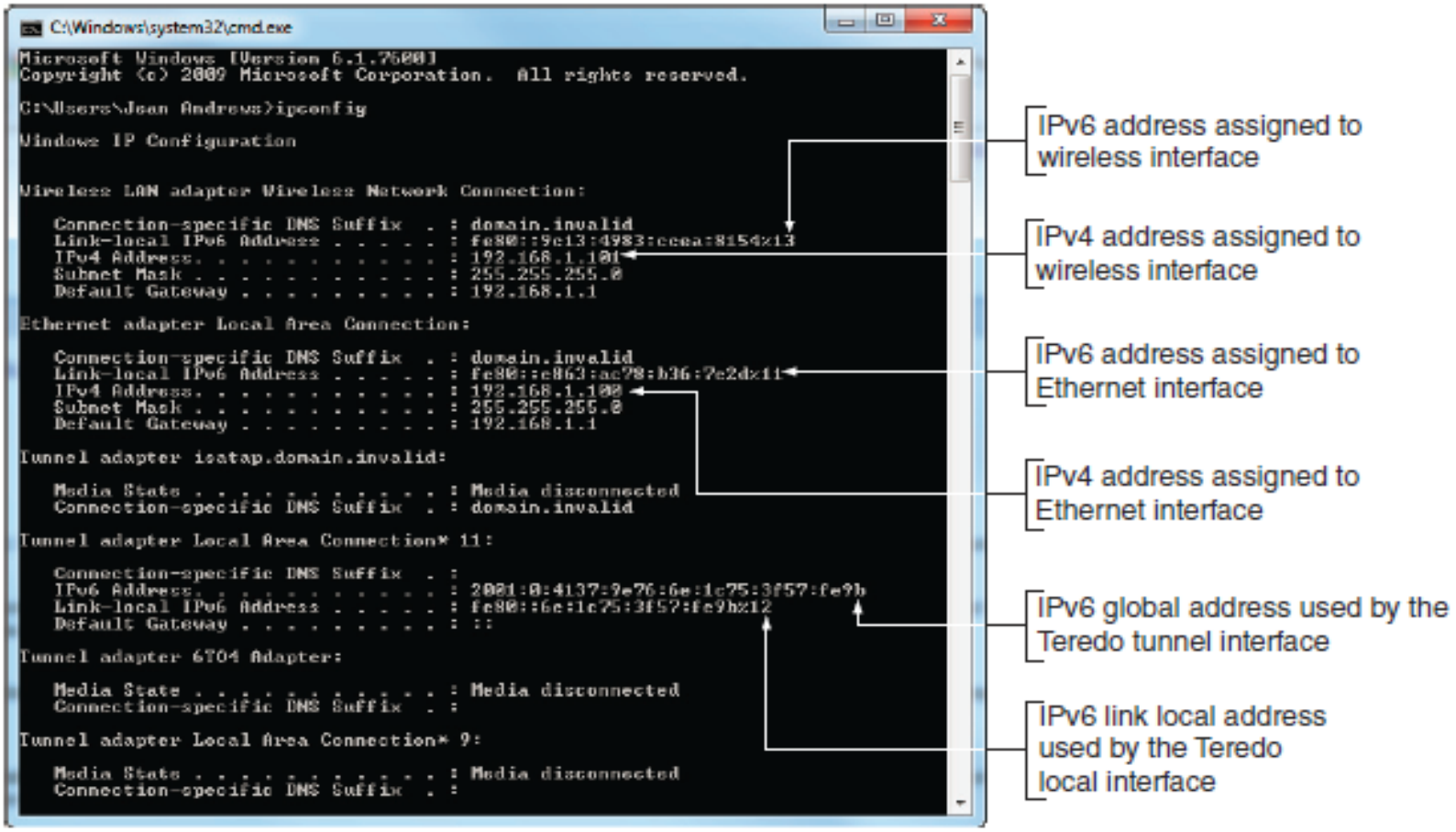

Figure 2-20 The `ipconfig` command shows IPv4 and IPv6 addresses assigned to this computer

Source: Microsoft LLC

IPv6 Autoconfiguration

- IPv6 addressing is designed so that a computer can autoconfigure its own link local IP address
  - Similar to how IPv4 uses an APIPA address
- Step 1 - The computer creates its IPv6 address
  - Uses FE80::/64 as the first 64 bits
  - Last 64 bits can be generated in two ways:
    - Randomly generated
    - Generated from the network adapter's MAC address
- Step 2 - The computer checks to make sure its IP address is unique on the network

IPv6 Autoconfiguration

- Step 3 - The computer asks if a router on the network can provide configuration information
  - If a router responds with DHCP information, the computer uses whatever information this might be
    - Such as the IP addresses of DNS server or the network prefix
- If the network prefix is supplied, this will become the first 64 bits of its own IP address
  - Process is called prefix discovery

Tunneling

- Dual stacked - term given when a network is configured to use both IPv4 and IPv6 protocols
- If packets on this network must traverse other networks where dual stacking is not used, tunneling is used
- Three tunneling protocols:
  - 6to4
  - ISATAP (Intra-Site Automatic Tunnel Addressing)
  - Teredo

Tunneling

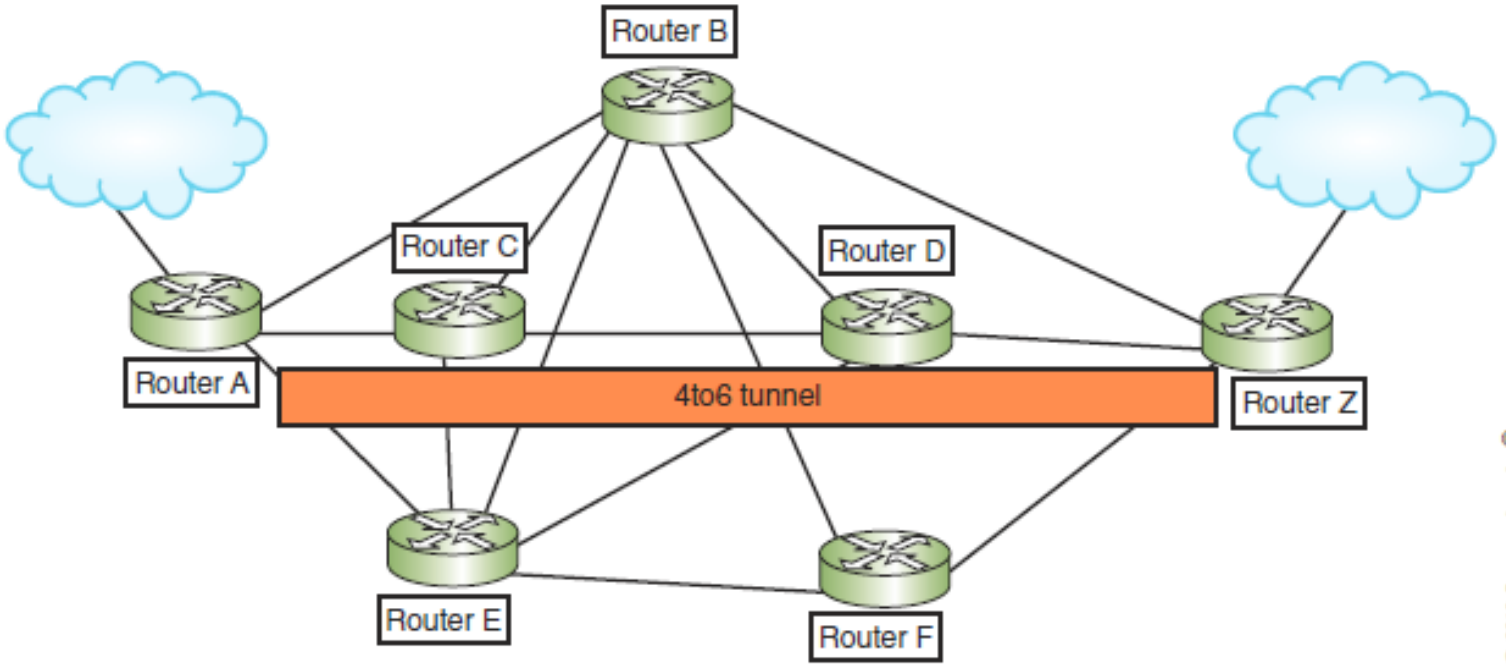

Figure 2-21 A 4to6 tunnel is used to move IPv4 packets through a futuristic IPv6 network that is configured to not use IPv4

Tools for Troubleshooting IP Address Problems

- Event Viewer (eventvwr.msc)- one of the first places to start looking for clues when something goes wron

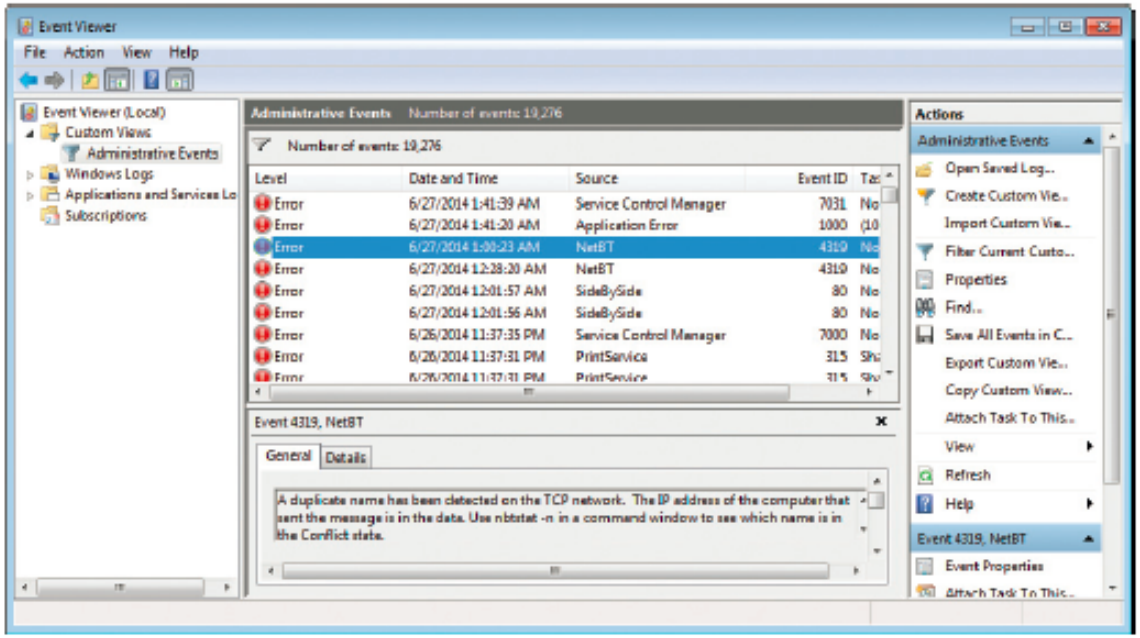

Figure 2-22 Event Viewer provided the diagnosis of a problem and recommended steps to fix the problem

Source: Microsoft LLC

ping

- ping (Packet Internet Groper) - used to verify that TCP/IP is installed, bound to the NIC, configured correctly, and communicating with the network
- The ping utility sends out a signal called an echo request to another device (request for a response)
  - Other computer responds in the form of an echo reply
- ICMP - protocol used by the echo request/reply to carry error messages and information about the network

ping

Table 2-7 Options for the `ping` command

Sample `ping` commands	Description
`ping www.google.com`	You can ping a host using its host name to verify you have Internet access and name resolution. Google.com is a reliable site to use for testing. See the results in Figure 2-23.
`ping 8.8.8.8`	Ping an IP address on the Internet to verify you have Internet access. The address 8.8.8.8, which is easy to remember, points to Google's public DNS servers.
`ping -a 8.8.8.8`	Use the `-a` parameter in the command line to test for name resolution and to display the host name to verify DNS is working.
`ping 92.10.11.200`	In this example, `92.10.11.200` is the address of a host on another subnet in your corporate network. This ping shows if you can reach that subnet.
`ping 192.168.1.1`	In this example, `192.168.1.1` is the address of your default gateway. This ping shows if you can reach it.
`ping 127.0.0.1`	Ping the loopback address, 127.0.0.1, to determine whether your workstation's TCP/IP services are running.
`ping localhost`	This is another way of pinging your loopback address.
`ping -?` or `ping /?`	These two commands display the help text for the `ping` command, including its syntax and a full list of parameters.
`ping -t 192.168.1.1`	The `-t` parameter causes pinging to continue until interrupted. To display statistics, press CTRL+Break. To stop pinging, press CTRL+C.
`ping -n 2 192.168.1.1`	The `-n` parameter defines a number of echo requests to send. By default, ping sends four echo requests. In this example, we've limited it to two.

ping

- IPv6 networks use a version of ICMP called ICMPv6
  - ping6 - on Linux computers running IPv6, use `ping6` to verify whether an IPv6 host is available
  - ping -6 - on Windows computers, use `ping` with the `-6` switch to verify connectivity on IPv6 networks
- For the `ping6` and `ping -6` commands to work over the Internet, you must have access to the IPv6 Internet

ipconfig

Table 2-8 Examples of the `ipconfig` command

ipconfig command	Description
`ipconfig /?` or `ipconfig -?`	Displays the help text for the `ipconfig` command, including its syntax and a full list of parameters.
`ipconfig /all`	Displays TCP/IP configuration information for each network adapter.
`ipconfig /release`	Releases the IP address when dynamic IP addressing is being used. Releasing the IP address effectively disables the computer's communications with the network until a new IP address is assigned.
`ipconfig /release6`	Releases an IPv6 IP address.

`ipconfig /renew`	Leases a new IP address (often the same one you just released) from a DHCP server. To solve problems with duplicate IP addresses, misconfigured DHCP, or misconfigured DNS, reset the TCP/IP connection by using these two commands:
	`ipconfig /release`
	`ipconfig /renew`

`ipconfig /renew6`	Leases a new IPv6 IP address from a DHCP IPv6 server.
`ipconfig /displaydns`	Displays information about name resolutions that Windows currently holds in the DNS resolver cache.
`ipconfig /flushdns`	Flushes—or clears—the name resolver cache, which might solve a problem when the browser cannot find a host on the Internet or when a misconfigured DNS server has sent wrong information to the resolver cache.

ifconfig

- ifconfig - utility to view and manage TCP/IP settings
- If your Linux or UNIX system provides a GUI
  - Open a shell prompt, then type `ifconfig`

Table 2-9 Some `ifconfig` commands

`ifconfig` command	Description
`ifconfig`	Displays basic TCP/IP information and network information, including the MAC address of the NIC.
`ifconfig -a`	Displays TCP/IP information associated with every interface on a Linux device; can be used with other parameters. See Figure 2-26.
`ifconfig down`	Marks the interface, or network connection, as unavailable to the network.
`ifconfig up`	Reinitializes the interface after it has been taken down (via the `ifconfig down` command), so that it is once again available to the network.
`man ifconfig`	Displays the manual pages, called man pages, for the `ifconfig` command, which tells you how to use the command and about command parameters (similar to the `ipconfig /?` command in Windows).

nslookup

- nslookup (name space lookup) - allows you to query the DNS database from any computer on a network
  - To find the host name of a device by specifying its IP address, or vice versa
  - Useful for verifying a host is configured correctly or for troubleshooting DNS resolution problems
- Reverse DNS lookup - to find the host name of a device whose IP address you know
- Two modes:
  - Interactive - to test multiple DNS servers at one time
  - Noninteractive - test a single DNS server

nslookup

Figure 2-27 nslookup shows server and host information

Source: Microsoft LLC

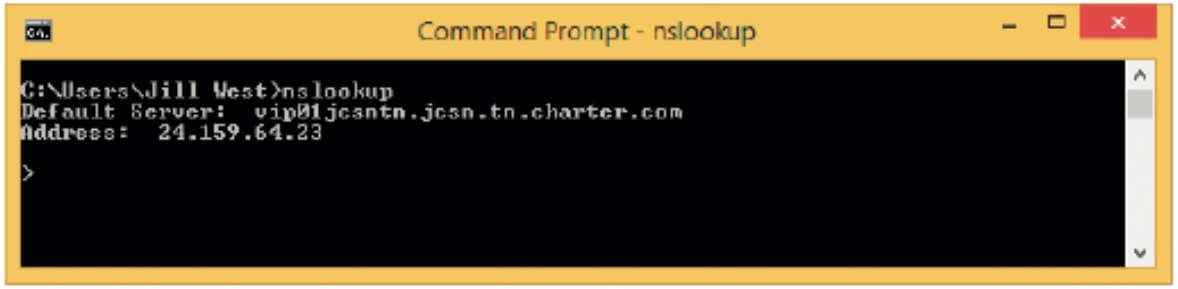

Figure 2-29 Interactive mode of the nslookup utility

Source: Microsoft LLC

nslookup

- You can change DNS servers from within interactive mode with the server subcommand and specifying the IP address of the new DNS server

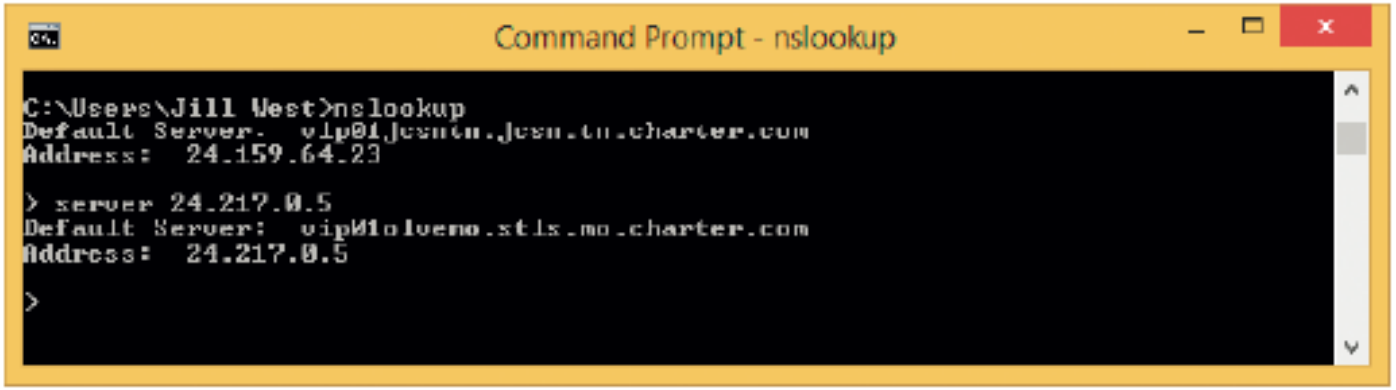

Figure 2-30 The `server` subcommand can be used to change DNS servers

Source: Microsoft LLC

- To exit nslookup's interactive mode, enter `exit`

Summary

- Hosts on a network are assigned host names
- Applications are assigned one or more port numbers to communicate with other applications
- IPv4 addresses have 32 bits and are written as four decimal numbers called octets
- IPv6 addresses have 128 bits and are written as eight blocks of hexadecimal numbers
- Every NIC is assigned a unique 48-bit MAC address
- Use the `ipconfig` command to view IP configuration information

Summary

- A FQDN includes both a host name portion and a domain name portion
- Name resolution is the process of matching an FQDN to its IP address
- DNS is an automated name resolution service that operates at the Application layer
- DNS data is spread throughout the globe in a distributed database model
- An IP address and a port number written together is called a socket

Summary

- Well-known ports range from 0 to 1023 and are assigned by IANA
- You can define a range of available IP addresses in DHCP, or assign a static IP address as a DHCP reservation
- NAT is used to allow devices that have private IP addresses access to the Internet
- Tunneling protocols are used to allow IPv6 packets to travel over or through an IPv4 network
- Three types of IPv6 addresses are unicast, multicast, and anycast addresses

Summary

- The ping utility uses ICMP to verify that TCP/IP is installed, bound to the NIC, configured correctly, and communicating with the network
- ipconfig is useful for viewing and adjusting a Windows computer's TCP/IP settings
- On UNIX and Linux systems, the ifconfig utility is used to view and manage TCP/IP settings
- The nslookup utility allows you to query the DNS database from any computer on the network