LESSON 3.1

98-366 Networking Fundamentals

LESSON 3.1

98-366 Networking Fundamentals

Understand the OSI Model
Part 1

Lesson Overview

In this lesson, you will learn about:

- Internetwork
- IETF
- ISO/OSI
- ITU-T
- Protocols

Internetwork

- A collection of individual networks, connected by intermediate networking devices, that functions as a single large network
- Formed from different kinds of network technologies that can be interconnected by routers and other networking devices
- Offers a solution to three key problems:
  - Isolated LANs
  - Duplication of resources
  - A lack of network management
- Many issues including configuration, security, redundancy, reliability, centralization, and performance, must be adequately dealt with for the internetwork to function smoothly.

ISO (International Organization for Standardization)

- The world's largest developer and publisher of International Standards. ISO is now considered the primary architectural model for intercomputer communications.

OSI (Open System Interconnection model)

- Defines a networking framework for implementing protocols in seven layers

ITU-T (International Telecommunications Union-Telecommunication)

- The standardization division of the ITU that develops communications recommendations for all analog and digital communications

IETF (Internet Engineering Task Force)

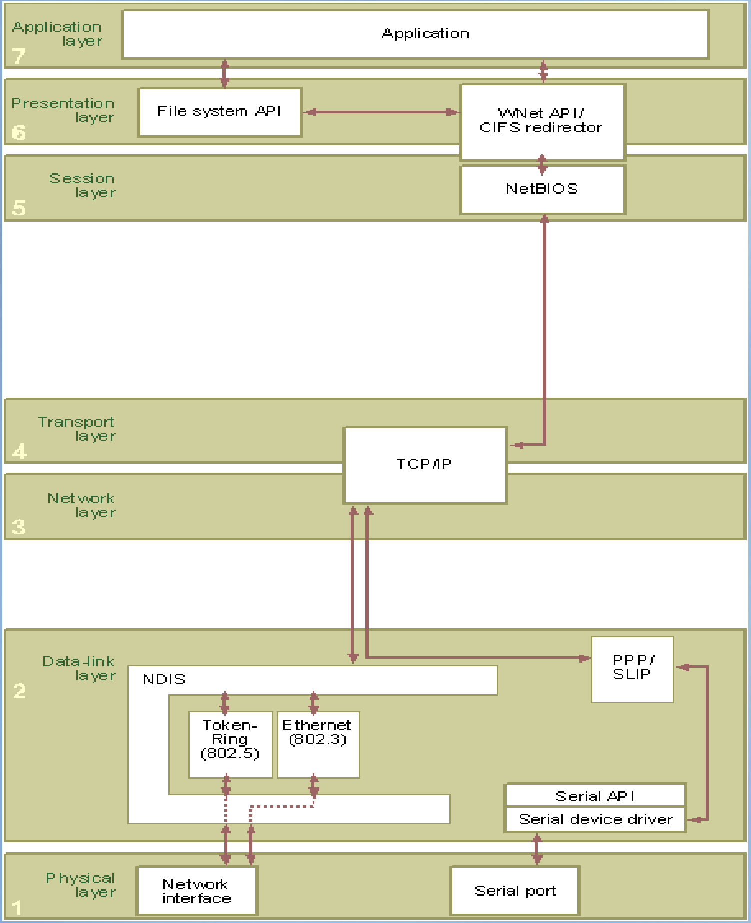
- Charged with studying technical problems facing the Internet and proposing solutions to the Internet Architecture Board ; the standards agency for TCP/IP

LESSON 3.1

98-366 Networking Fundamentals

Open System Interconnection (OSI) Reference Model

- How information from a software application in one computer moves through a network medium to a software application in another computer.
- In the International Organization for Standardization Open Systems Interconnection (ISO/OSI) model for network communications, WNet functions operate across the presentation and session layers.



The data enter as they transmit, going down the seven layers, and exit as they are received at the right, going up the layers.

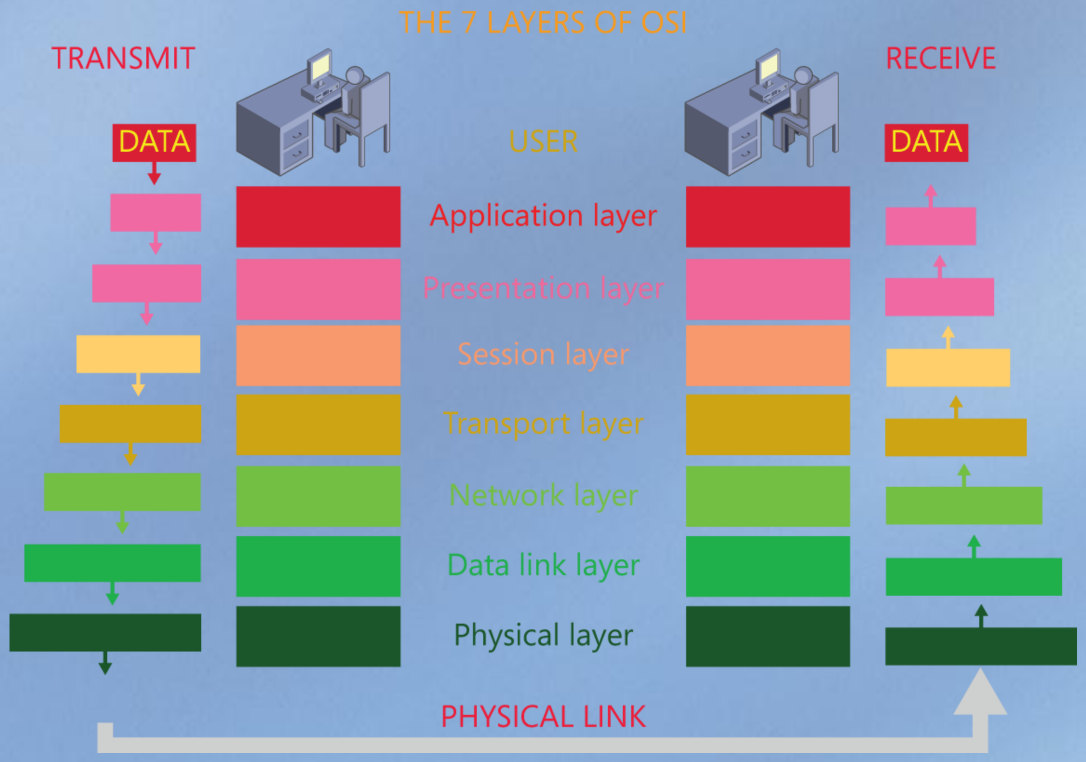


Image courtesy of The Abdus Salam International Centre for Theoretical Physics.

Characteristics of the OSI Layers

- Each of the seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers.
- Application issues implemented only in software is part of the **upper layer** of the OSI model. It is the highest layer and closest to the end user.
- Software applications that contain a communications component are used both by the users and the application layer process.

Protocols

- A set of rules that direct the way computers exchange information
- Communication protocols enable communication and execute the functions of one or more of the OSI layers.
  - At the physical and data link layers of the OSI model **LAN protocols** define communication over the various LAN media.
  - At the lowest three layers of the OSI model **WAN protocols** define communication over the various wide-area media.
  - **Routing protocols** control the exchange of information between routers so that the routers can select the proper path for traffic.
  - **Network protocols** apply to various upper-layer protocols.

OSI Model and Communication Between Systems

- The OSI layers are where information being transferred from a software application in one computer system to a software application in another must pass.
- The application layer then passes the information to the presentation layer (Layer 6), which sends the data to the session layer (Layer 5), and so on down to the physical layer (Layer 1).
- At the physical layer, the data are placed on the physical network medium and are relayed across the medium to System 2.
- The physical layer of System 2 removes the data from the physical medium, and then passes the information up to the data link layer (Layer 2), which passes it to the network layer (Layer 3), and so on, until it reaches the application layer (Layer 7) of System 2.
- Lastly, the application layer of System 2 passes the data to the recipient application to complete the communication process.

Interaction Between OSI Model Layers

- A specified layer in the OSI model generally communicates with three other OSI layers:
  - the layer directly above it
  - the layer directly below it
  - its peer layer in other networked computer systems
- The data link layer in System 1, communicates with the network layer of System 1, the physical layer of System 1, and the data link layer in System 2.

OSI Layer Services

- One OSI layer communicates with another layer to make use of the services provided by the second layer.
- The services provided by adjacent layers help a given OSI layer communicate with its peer layer in other computer systems.
- Three basic elements are involved in layer services:
  1. The service user—Layer that requests services from the next OSI layer
  2. The service provider —Layer that provides services to service users
  3. The service access point (SAP) —Intangible place at which one OSI layer can request the services of another layer.

Encapsulation

- The OSI Model Layers and Information Exchange is done by the use of communication control to communicate with the peer layers in other computer systems and consists of specific requests and instructions that are exchanged between peer OSI layers.
- The data portion of an information unit at a stated OSI layer can contain headers that have been passed down from upper layers.
- The data that has been passed down from upper layers are appended to trailers.
- The data portion of an information unit at a given OSI layer can contain headers, trailers, and data from all the higher layers. This is known as **encapsulation.**

Activity:

How well do you really know the OSI networking model?

1. Test yourself with our OSI Model game. http://www.gocertify.com/games/osi-game.shtml

Complete Student Activity 3.1

LESSON 3.2

98-366 Networking Fundamentals

Understand the OSI Model

Part 2

Lesson Overview

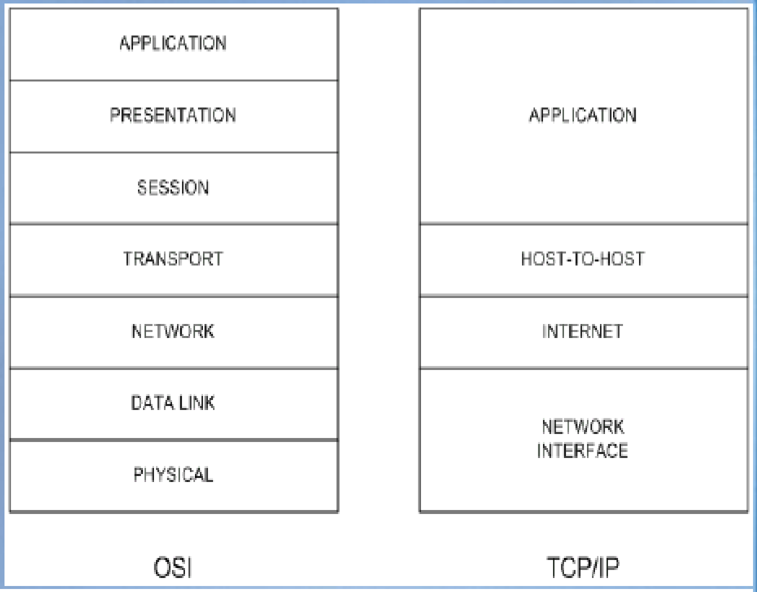
In this lesson, you will learn information about:

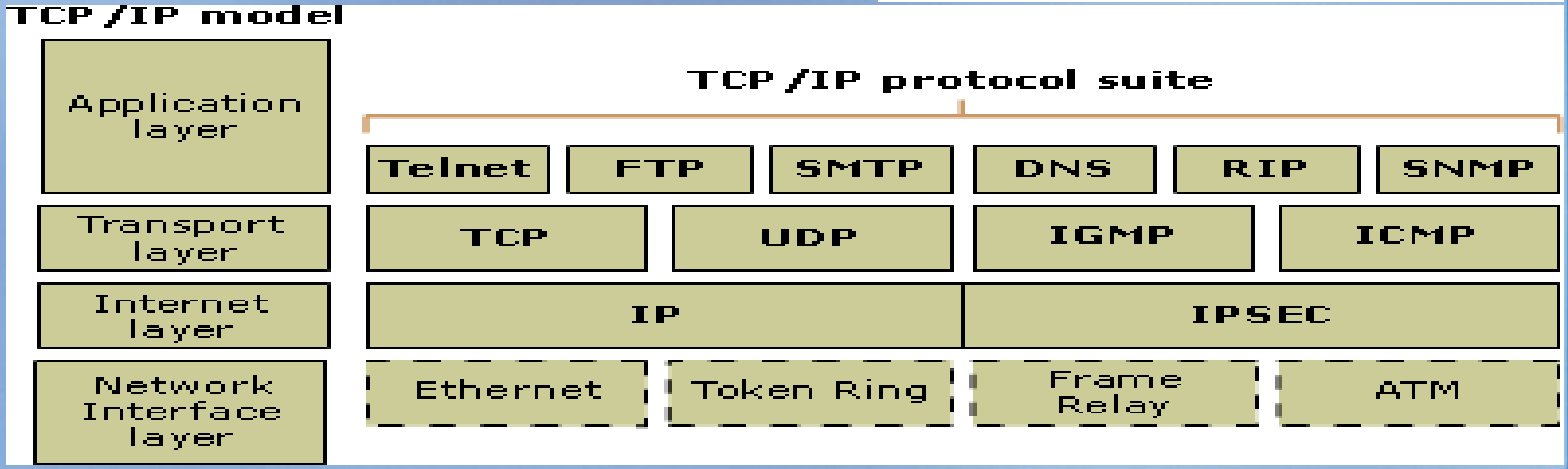
- Frames
- Packets
- Segments
- TCP
- TCP/IP Model
- Well-known ports for most-used purposes

The TCP/IP Protocol Suite

- Includes **Transmission Control Protocol (TCP)** and **Internet Protocol (IP)** and is referred to as **TCP/IP model.**
- Defines general guidelines and implementations of specific networking protocols to enable computers to communicate over a network for common applications (electronic mail, terminal emulation, and file transfer)
- Each layer of the TCP/IP model corresponds to layers of the seven-layer OSI reference model proposed by the ISO.
- **IPSec (Internet Protocol Security)** is a dual mode, end-to-end, security scheme operating at the Internet Layer of the Internet Protocol Suite or OSI model Layer 3.

- The **TCP/IP** is shown in relation to the OSI seven layers.
- TCP delivers an unstructured stream of bytes identified by sequence numbers with stream data transfer.





TCP/IP

- Provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed, and received
- Protocols exist for a variety of communication services between computers.
- The layers near the top are closer to user application, the layers near the bottom are closer to the physical transmission of the data.
- Viewing layers as providing or consuming a service is a method of abstraction to isolate upper layer protocols.
- The lower layers avoid having to know the details of each and every application and its protocol.

Transmission Control Protocol (TCP)

- Assembles bytes into segments and passes to IP for delivery
- Provides end-to-end reliable packet delivery through an internetwork
- Mechanisms deal with lost, delayed, duplicate, or misread packets.
- Time-out mechanisms detect lost packets and request retransmission.
- Provides proficient flow control.
  - When sending responses back to the source, the receiving TCP process indicates the highest sequence number it can receive without overflowing its internal buffers.
- Full-duplex operation processes can both send and receive at the same time.
  - Multiplexing means that numerous concurrent upper-layer conversations can be occurring over a single connection.

- Each host on a **TCP/IP network** is assigned a unique 32-bit logical address that is divided into two main parts:
  1. Network number – identifies a network and must be assigned by the Internet Network Information Center (InterNIC) if the network is to be part of the Internet
  2. Host number – identifies a host on a network and is assigned by the local network administrator

Internet Protocol (IP)

- A network layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed
- IP is documented in RFC 791 – Request For Comments for Internet Protocol, the specification for how traffic travels over the internet and is the primary network layer protocol in the Internet protocol suite
- Allows large data transfer so file applications do not have to cut data into blocks

Well-Known Ports

- Most services work with TCP/IP by configuring the server to use a well-known port number.
- The client connects from a random high port.
- Most of these well-known ports are port numbers below 1,024.
- TCP/IP port assignments on Windows are stored in the \%systemroot%\System32\drivers\etc\services file.

Examples of known services and ports

FTP 20,21	data transfer
SSH 22	secure shell
telnet 23	telnet protocol
DNS 53	domain name service
SMTP 25	simple mail transfer protocol
DHCP 67,68	dynamic host configuration protocol
TFTP 69	trivial file transfer protocol
HTTP 80	hypertext transfer protocol
POP3 110	post office protocol 3
NNTP 119	network news transfer protocol
IMAP4 143	internet message access protocol
HTTPS 443	hypertext transfer protocol over SSL/TLS

User Datagram Protocol (UDP)

- Part of the Internet Protocol suite
- Programs running on different computers on a network can send short messages known as datagrams to one another.
- A datagram is a self-sufficient and self-contained message sent through the network whose arrival, arrival time, and content are not guaranteed.
- UDP can be used in networks where TCP is traditionally implemented but is not reliable.
- Datagrams may go missing without notice, or arrive in a different order from the one in which they were sent.

IP responsibilities in UDP

1. Provide connectionless delivery of datagrams
2. Provide fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes
   - The maximum transmission unit (MTU) of a communications protocol of a layer is the size in bytes of the largest protocol data unit that the layer can pass onward; a packet is encapsulated into one or more frames, depending upon the MTU size.

IP Packets

- All IP packets are structured the same way – an IP header followed by a variable-length data field.
- There are 14 fields in an IP packet header.

0	4	8	16	19 31
Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding

- A packet and a frame are both packages of data moving through a network.
- A packet exists at Layer 3 of the OSI Model, a frame exists at Layer 2 of the OSI Model.
- Layer 2 is the Data Link Layer – the best-known protocol in this layer is Ethernet.
- Layer 3 is the Network Layer – the best-known protocol in this layer is IP (Internet Protocol).
- The TCP segment, encapsulates all higher level protocols above it, a segment at the transport layer and the TCP counterparts for these three items.

Complete Student Activity 3.2

LESSON 3.3

98-366 Networking Fundamentals

Understand IPv4

Lesson Overview

In this lesson, you will learn about:

- APIPA
- addressing
- classful IP addressing and classless IP addressing
- gateway
- IPv4
- local loopback IP
- NAT
- network classes
- reserved address ranges for local use
- subnetting
- static IP

IPv4

- A connectionless protocol for use on packet-switched Link Layer networks like the Ethernet
- At the core of standards-based internetworking methods of the Internet
- Network addressing architecture redesign is underway via classful network design, Classless Inter-Domain Routing, and network address translation (NAT) .
- Microsoft Windows uses TCP/IP for IP version 4 (a networking protocol suite) to communicate over the Internet with other computers.
- It interacts with Windows naming services like WINS and security technologies.
- IPsec helps facilitate the successful and secure transfer of IP packets between computers.
- An IPv4 address shortage has been developing.

Network Classes

- Provide a method for interacting with the network
- All networks have different sizes so IP address space is divided in different classes to meet different requirements.
- Each class fixes a boundary between the network prefix and the host within the 32-bit address.

Class	Leading Bits	Size of *Network Number* Bit field	Size of *Rest* Bit field	Number of Networks	Addresses per Network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

Classful Network

- Divides the address space for Internet Protocol Version 4 (IPv4) into five address classes
- Each class, coded in the first four bits of the address, defines a different network size or a different network type.
- Design for IPv4 – sized the network address as one or more 8-bit groups, resulting in the blocks of Class A, B, or C addresses.

Classless Interdomain Routing (CIDR)

- A tactic of assigning IP addresses and routing Internet Protocol packets
- Allocates address space to Internet service providers and end users on any address bit boundary, instead of on 8-bit segments
- IP addresses consist of two groups of bits in the address:
    1. Most significant part is the *network address*, which identifies a whole network or subnet
    2. Least significant part is the *host identifier*, which specifies a particular host interface on that network

- Under supernetting, the classful subnet masks are extended so that a network address and subnet mask could specify multiple Class C subnets with one address.
- For example, if 1,000 addresses were needed, 4 Class C networks could be supernetted together:

```
192.60.128.0    (11000000.00111100.10000000.00000000)  Class C subnet address
192.60.129.0    (11000000.00111100.10000001.00000000)  Class C subnet address
192.60.130.0    (11000000.00111100.10000010.00000000)  Class C subnet address
192.60.131.0    (11000000.00111100.10000011.00000000)  Class C subnet address
--------------------------------------------------------
192.60.128.0    (11000000.00111100.10000000.00000000)  Supernetted Subnet address
255.255.252.0   (11111111.11111111.11111100.00000000)  Subnet Mask
192.60.131.255  (11000000.00111100.10000011.11111111)  Broadcast address
```

- The subnet 192.60.128.0 includes all the addresses from 192.60.128.0 to 192.60.131.255.

IPv4 Addresses

- Usually written in dot-decimal notation of four octets of the address expressed in decimals and separated by periods
- Base format used in the conversion table. Each octet can be of any of the different bases

Notation	Value	Conversion from dot-decimal
Dot-decimal notation	192.0.2.235	N/A
Dotted Hexadecimal	0xC0.0x00.0x02.0xEB	Each octet is individually converted to hexadecimal form
Dotted Octal	0300.0000.0002.0353	Each octet is individually converted into octal
Hexadecimal	0xC00002EB	Concatenation of the octets from the dotted hexadecimal
Decimal	3221226219	The 32-bit number expressed in decimal
Octal	30000001353	The 32-bit number expressed in octal

Reserved IP Addresses

- Three ranges of address are reserved for private networks.
- Ranges are not routable outside of private networks.
- Private machines cannot directly communicate with public networks.
- Internet Assigned Numbers Authority (IANA) reserved three blocks of IP address space for private internets.
- Confusion results because different authorities name different IP numbers for different addresses.

CIDR address block	Description	Reference
0.0.0.0/8	Current network (only valid as source address)	RFC 1700
10.0.0.0/8	Private network	RFC 1918
127.0.0.0/8	Loopback	RFC 5735
169.254.0.0/16	Link-Local	RFC 3927
172.16.0.0/12	Private network	RFC 1918
192.0.0.0/24	Reserved (IANA)	RFC 5735
192.0.2.0/24	TEST-NET-1, Documentation and example code	RFC 5735
192.88.99.0/24	IPv6 to IPv4 relay	RFC 3068
192.168.0.0/16	Private network	RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
198.51.100.0/24	TEST-NET-2, Documentation and examples	RFC 5737
203.0.113.0/24	TEST-NET-3, Documentation and examples	RFC 5737
224.0.0.0/4	Multicasts (former Class D network)	RFC 3171
240.0.0.0/4	Reserved (former Class E network)	RFC 1700
255.255.255.255		

IANA Reserved Blocks

Name	Address range	Number of addresses	Classful description	Largest CIDR block
24-bit block	10.0.0.0–10.255.255.255	16,777,216	Single Class A	10.0.0.0/8
20-bit block	172.16.0.0–172.31.255.255	1,048,576	Contiguous range of 16 Class B blocks	172.16.0.0/12
16-bit block	192.168.0.0–192.168.255.255	65,536	Contiguous range of 256 Class C blocks	192.168.0.0/16

Automatic Private IP Addressing (APIPA)

- When the address block was reserved, no standards existed for mechanisms of address auto-configuration.
- Filling the void, Microsoft created APIPA implementation.
- APIPA will automatically assign an Internet Protocol address to a computer on which it is installed.
- APIPA has been deployed on millions of machines and has become a de facto standard in the industry.
- IETF defined a formal standard for this functionality, RFC 3927, entitled Dynamic Configuration of IPv4 Link-Local Addresses.

Localhost

- The address range 127.0.0.0–127.255.255.255 is reserved for localhost communication (127.0.0.0/8 in CIDR notation).
- Addresses within this range should never appear outside a host computer and packets sent to this address.
- Addresses are returned as incoming packets on the same virtual network device (known as loopback).
- Loopback or Localhost 127.0.0.0 (or 127/8) should not be used as an address for any station; it is used to ping yourself.

Broadcast Address

- An address that allows information to be sent to all machines on a given subnet
- Found by obtaining the bit complement of the subnet mask and performing a bitwise OR operation with the network identifier
- Example: To broadcast a packet to an entire IPv4 subnet using the private IP address space 172.16.0.0/12 (subnet mask 255.240.0.0), the broadcast address is 172.31.255.255.

- On a Class A, B, or C subnet, the broadcast address always ends in 255.
- Today, there are several driving forces for the acceleration of IPv4 address exhaustion:
  - Mobile devices
  - Always-on devices
  - Rapidly growing number of Internet users

A Gateway Computer Program

- A link between two computer programs allowing them to share information and bypass certain protocols on a host computer
- A telecommunications gateway is a computer or a network that allows or controls access to another computer or network.
- A default gateway is a way out of the subnet and it is also known as a router.
- All traffic that needs to be routed out of the subnet is done through the hosts' routing tables.

Static vs. Dynamic IP Addresses

- Static IP address
  - When a computer is configured to use the same IP address every time it powers up
  - Manually assigned to a computer by an administrator
- Dynamic IP address
  - When the computer's IP address is set automatically
  - Assigned either by the computer interface or host software itself, as in Zeroconf, or assigned by a server using Dynamic Host Configuration Protocol (DHCP)

Complete Student Activity 3.3

LESSON 3.4

98-366 Networking Fundamentals

Understand IPv6 Part 1

Lesson Overview

In this lesson, you will learn about:

- Addressing
- Dual IP stack
- Gateway
- IPv6
- ipv4toipv6 tunneling protocols to ensure backwards compatibility

Tunneling Protocol

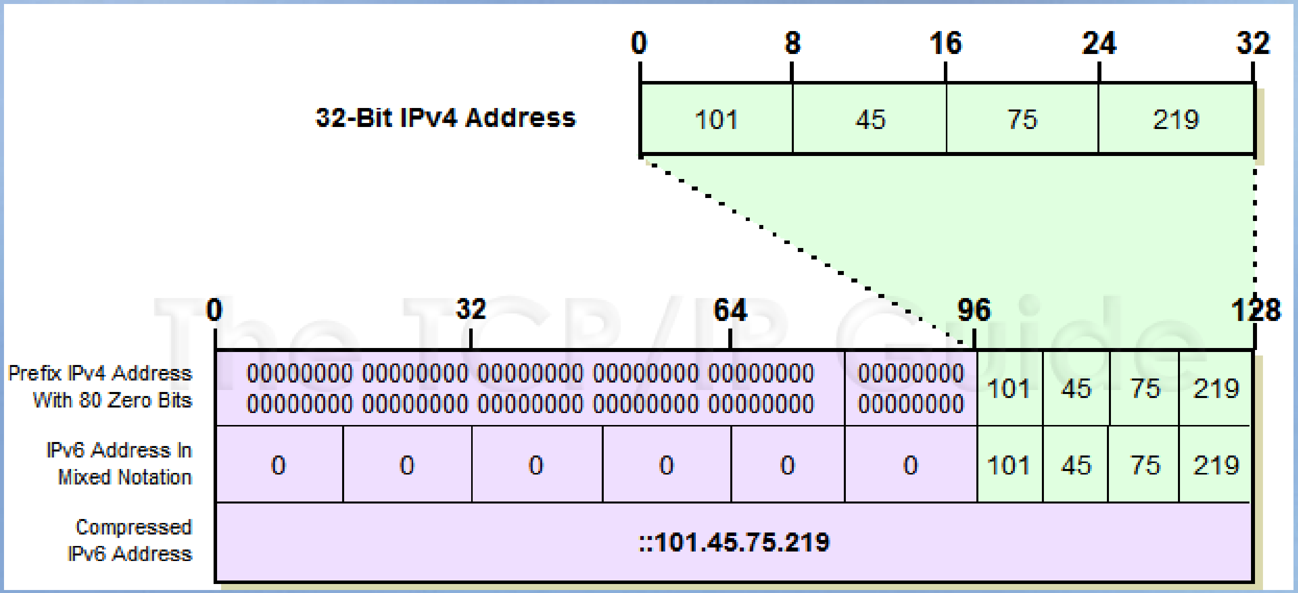
- Used by computer networks when the delivery network protocol encapsulates a different payload protocol

Teredo

- A tunneling protocol intended to grant IPv6 connectivity to nodes that are located behind IPv6-unaware NAT devices.
- Identifies a way of encapsulating IPv6 packets within IPv4 UDP datagrams that can be routed through NAT devices and on the IPv4 internet.
- 6to4 is an Internet conversion mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network with no need to configure explicit tunnels.

  Special relay servers are also in place that permit 6to4 networks to communicate with native IPv6 networks.

- IPv6 has all zeroes for the middle 16 bits; thus, they start off with a string of 96 zeroes, followed by the IPv4 address.

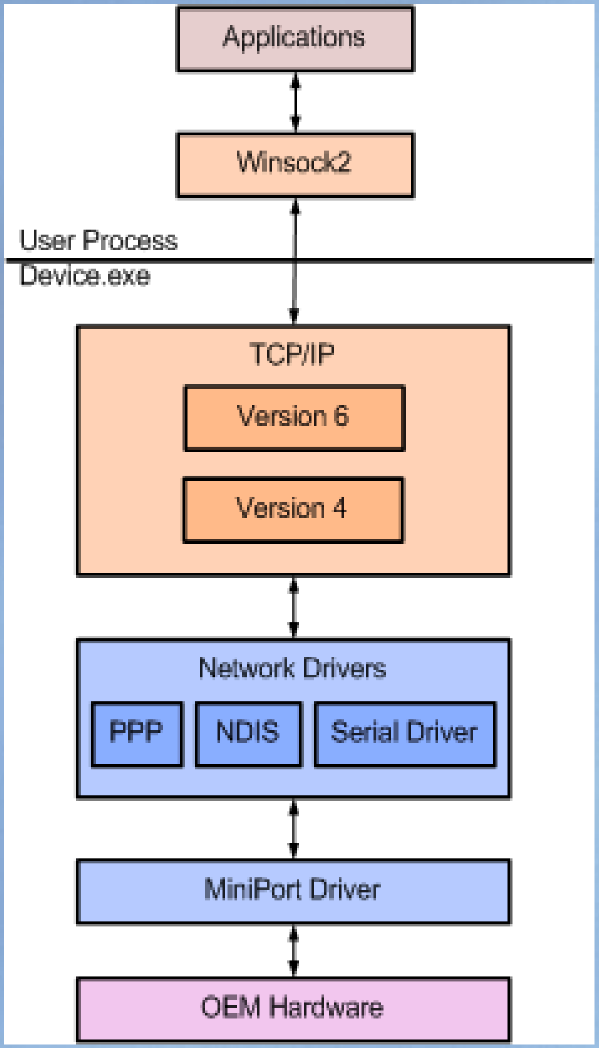


ISATAP

- Intra-Site Automatic Tunnel Addressing Protocol
- An IPv6 transition mechanism meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network
  - Uses IPv4 as a virtual nonbroadcast multiple-access network (NBMA) data link layer, so that it does not require the underlying IPv4 network infrastructure to support multicast.
  - The IP6_ADDRESS structure stores an IPv6 address and the IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to assist an automatic mechanism for forming the host identifier from Link Layer media addressing information (MAC address).

Dual IP Stack

- Special addresses assigned to IPv6-capable devices speak both IPv4 and IPv6.
- **Dual Stack Architecture** involves running IPv4 and IPv6 at the same time where end nodes and routers/switches run both protocols.
- If IPv6 communication is possible that is the preferred protocol.
- Windows uses a dual-stack architecture as shown here.



Dual IP Stack (continued)

- A common dual-stack migration strategy used to create the transition from the core to the edge
  - Enables two TCP/IP protocol stacks on the WAN core routers, secondly perimeter routers and firewalls, next the server-farm routers, and finally the desktop access routers.
  - Allows dual protocol stacks on the servers and then the edge computer systems.
  - Socket can accept connections from both IPv6 and IPv4 TCP clients connecting to port 5001.
  - This can be seen with IPconfig on an Windows XP or later OS.

Gateway

- A computer program link between two computer programs so they can share information and bypass certain protocols on a host computer and/or a network that allows or controls access to another computer or network
  - Default Gateway—A way out of the subnet; also known as a router
  - Network gateway—An internetworking system that can join two networks that use different base protocols and can be implemented completely in software, completely in hardware, or as a combination

GLBP (Gateway Load Balancing Protocol)

- Provides automatic router backup for IPv6 hosts configured with a single default gateway on an IEEE 802.3 LAN
- Benefits include load sharing, multiple virtual routers, preemption, and authentication.
- Can operate at any level of the OSI model depending on the types of protocols they support.
- Appears at the edge of a network, capabilities like firewalls tend to be integrated with it.
- A broadband router often serves as the network gateway although ordinary computers can also be configured to perform equivalent functions on home networks.

Internet Protocol version 6 (IPv6)

- An Internet Protocol version designed to succeed IPv4 with an Internet Layer protocol for packet-switched internetworks
- The main driving force for the redesign of Internet protocol is the foreseeable IPv4 address exhaustion
- IPv6 has a large address space and supports 2^{128} (about $3.4×10^{38}$) addresses
- Provides flexibility in allocating addresses and routing traffic, adding a column.
- Implements new features that simplify aspects of address assignment and network renumbering.
- Subnet size has been standardized as 64 bits, expanded addressing moves us from 32-bit address to a 128-bit addressing method.

Convert from Hexadecimal to Binary

- Translate each hexadecimal digit into its 4-bit binary equivalent.
- Hexadecimal numbers have either and *0x* prefix or an *h* suffix.

For example, the hexadecimal number:

0x3F7A

translates to

0011 1111 0111 1010

Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

- The IPv6 packet header is 40 bits long and consists of Version, Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address, Destination Address, Data, and Payload fields.

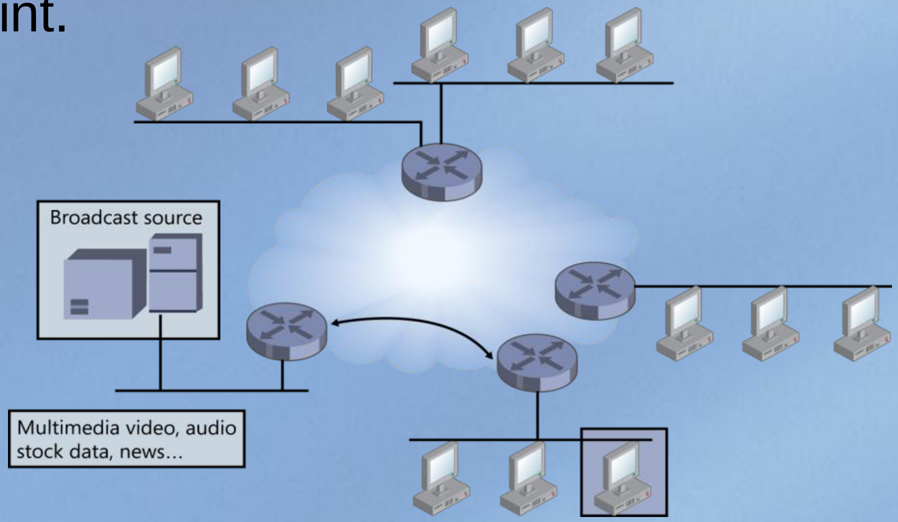
LESSON 3.4

98-366 Networking Fundamentals

IPv6 Broadcasting Methods

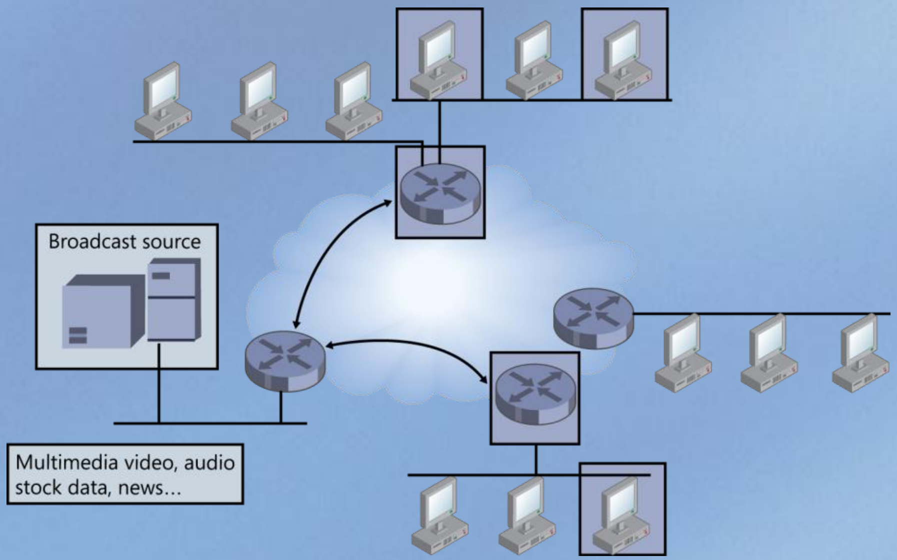
Unicast Broadcast

- A communication between a single host and a single receiver
- Packets sent to a unicast address are delivered to the interface identified by that address.
- There is a **one-to-one** association between network address and network endpoint: each destination address uniquely identifies a single receiver endpoint.



Multicast Broadcast

- A communication between a single host and multiple receivers
- Packets are sent to all interfaces--to every device on a network.
- It is a **one-to-many** association between network addresses and network endpoints: each destination address identifies a set of receiver endpoints, to which all information is replicated.

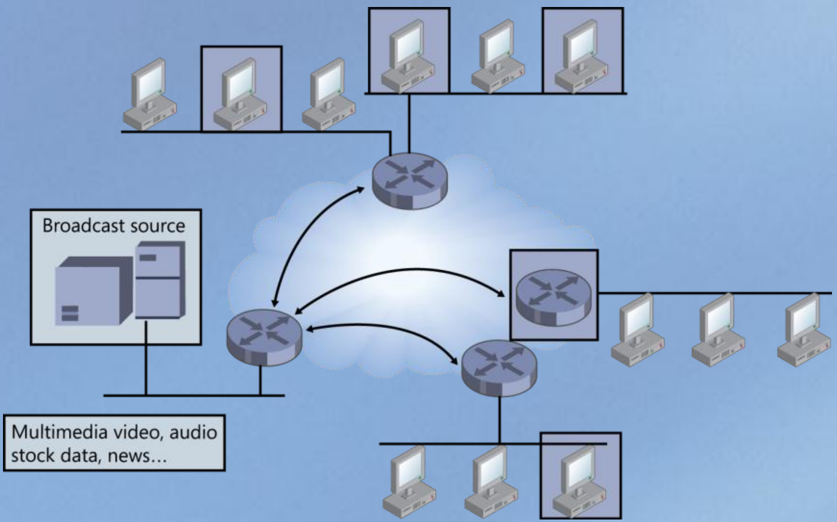


LESSON 3.4

98-366 Networking Fundamentals

Anycast Broadcast

- A communication between a single sender and a list of addresses
- It can contain End Nodes and Routers, and packets are sent to an **anycast** address.
- There is a **one-to-"one-of-many"** association between network addresses and network endpoints: each destination address identifies a set of receiver endpoints, but only one of them is chosen at any given time to receive information from any given sender.



LESSON 3.4

98-366 Networking Fundamentals

Complete Student Activity 3.4

LESSON 3.5

98-366 Networking Fundamentals

Understand IPv6 Part 2

Lesson Overview

In this lesson, you will learn about:

- Ipconfig
- Local loopback IP
- Ports
- Packets
- Subnetting
- Subnetmask
- Reserved address ranges

Ipconfig

- An Internet protocol configuration in Microsoft Windows that is a console application
    1. Displays all current TCP/IP network configuration values
    2. Refreshes Dynamic Host Configuration Protocol (DHCP)
    3. Refreshes domain name system (DNS) settings
- Can be utilized to verify a network connection as well as to verify your network settings
- The default displays only the IP address, subnet mask, and default gateway for each adapter bound to TCP/IP.
- There are differences with each version of windows.

Ipconfig in Windows 7 OS

C:\Windows\system32\cmd.exe

```
C:\Users>ipconfig

Windows IP Configuration


Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : gateway.2wire.net
   Link-local IPv6 Address . . . . . : fe80::bca4:acc5:8e7b:db4f%12
   IPv4 Address. . . . . . . . . . . : 192.168.1.75
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254

Ethernet adapter Netgear:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.gateway.2wire.net:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : gateway.2wire.net

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:4137:9e76:1882:3c:b4c2:bfe8
   Link-local IPv6 Address . . . . . : fe80::1882:3c:b4c2:bfe8%15
   Default Gateway . . . . . . . . . : ::

C:\Users>_
```

Loopback Device in TCP/IP

- A virtual network interface executed in software only, not connected to any hardware
- Any traffic that a computer program sends to the loopback interface is immediately received on the same interface.
- IPv6 assigns only a single address for this function, 0:0:0:0:0:0:0:1 (also written as ::1), having the ::1/128 prefix.
- The loopback device is 127.0.0.1 for IPv4.
- The standard reserved domain name for these addresses is localhost.
- Pinging the special address loopback interface is a standard test of the functionality of the IP stack in the operating system.

Port

- A process-specific software build serving as a communications endpoint and used for multitasking
- Used by transport layer protocols such as transmission control protocol (TCP) and user datagram protocol (UDP)
- Identified by its port number, the IP address associated with, and the protocol used for communication
- Port numbers are divided into three ranges:
  - Well-known ports are from 0 through 1023
  - Registered ports are from 1024 through 49151
  - Dynamic and private ports are from 49152 through 65535

Sample Ports and Allocations

0		42	nameserv, WINS	113	identd/auth
1	tcpmux	43	whois, nickname	115	sftp
3		49	TACACS, Login Host Protocol	116	
4		50	RMCP, re-mail-ck	117	uucp
5	rje	53	DNS	118	
7	echo	57	MTP	119	NNTP
9	discard	59	NFILE	120	CFDP
11	systat	63	whois++	123	NTP
13	daytime	66	sql*net	124	SecureID
15	netstat	67	bootps	129	PWDGEN
17	qotd	68	bootpd/dhcp	133	statsrv
18	send/rwp	69	Trivial File Transfer Protocol (tftp)	135	loc-srv/epmap
19	chargen	70	Gopher	137	netbios-ns
20	ftp-data	79	finger	138	netbios-dgm (UDP)
21	ftp	80	www-http	139	NetBIOS
22	ssh, pcAnywhere	87		143	IMAP
23	Telnet	88	Kerberos, WWW	144	NewS
25	SMTP	95	supdup	150	
27	ETRN	96	DIXIE	152	BFTP
29	msg-icp	98	linuxconf	153	SGMP
31	msg-auth	101	HOSTNAME	156	
33	dsp	102	ISO, X.400, ITOT	161	SNMP
37	time	105	cso	175	vmnet
38	RAP	106	poppassd	177	XDMCP
39	rlp	109	POP2	178	NextStep Window Server
40		110	POP3	179	BGP
41		111	Sun RPC Portmapper	180	SLmail admin

Packets

- A packet mode is a digital networking communications method grouping all transmitted data into blocks.
- Communications links that do not support packets transmit data as a series of bytes, characters, or bits alone.
- When data is formatted into packets, the communication medium bitrate can be better shared among users.
- All data exchanged using IPv6 is contained in packets.

Packets (cont.)

- The IPv6 packet is composed of:
  - the fixed header
  - optional extension headers
  - the payload—the transport layer data carried by the packet
- The control information provides data the network needs to deliver to the user data such as source and destination addresses.
- The user data would be the information being sent.
- An illustration of this concept is sending a letter in an envelope:
  - The envelop has the address.
  - The user data is in the envelope.

Unique Local Addresses (ULA)

- Included in Internet protocol IPv6.
- The address block fc00::/7 has been reserved by IANA as described in RFC 4193.
- Defined as unicast in character and contain a 40-bit random number in the routing prefix to prevent collisions when two private networks are interconnected.
- Despite being inherently local in usage, the IPv6 address scope of unique local addresses is global.

Private Network

- Private network is one scenario that uses a set of standards for private IP address space.
  - Reserved address ranges are for local use.
  - Used for homes and small businesses
  - Also used in corporate networks not connected directly to the Internet for security
- A NAT gateway is usually used to enable Internet connectivity to multiple hosts such as a second computer or a video game with IPv4.
- IPv6 is designed so that network address translator (NAT) goes away.

Private Network (cont.)

- Since IPv6 addresses are 128 bits long, the theoretical maximum address space if all addresses were used is 2^{128} addresses.
  - This number, when fully expressed is $3.4*10^{38}$ or 340,282,366,920,938,463,463,374,607,431,768,211,456.
  - That's about 340 trillion, *trillion*, *trillion* addresses.

Subnets

- To subnet an IPv6 global address prefix, either hexadecimal or decimal methods are used.
- To subnet the IPv6 address space, use subnetting techniques to divide the 16-bit subnet ID field for a 48-bit global.
- For global addresses, Internet Assigned Numbers Authority (IANA) or an ISP assigns an IPv6 address prefix in which the first 48 bits are fixed.
- Subnetting the subnet ID field for a 48-bit global address prefix requires a two-step procedure:
    1. Determine the number of bits to be used for the subnetting
    2. Enumerate the new subnetted address prefixes

Subnets (cont.)

- The number of bits used for subnetting determines the possible number of new subnetted address prefixes that can allocate portions of network based on geographical divisions.
- Based on the number of bits used for subnetting, a list of the new subnetted address prefixes can be created with one of these approaches:
    1. Enumerate the new subnetted address prefixes by using hexadecimal representations of the subnet ID and increment.
    2. Enumerate the new subnetted address prefixes by using decimal representations of the subnet ID and increment.
- Both methods produce an enumerated list of subnetted address prefixes.

Subnet Mask

- A network address plus the bits reserved for identifying the subnetwork
- The bits for the network address are all set to 1.
  - Example: 11111111.11111111.11110000.00000000.
- Called a **mask** because it can be used to identify the subnet to which an IP address belongs by performing a bitwise AND operation on the mask and the IP address
- An IPv6 subnet mask is written in hexadecimal.
- A full IPv6 subnet mask uses the same 8-hex-word format as an IPv6 address.
- Like IPv4, an IPv6 address has a network portion and a device portion.
- Unlike IPv4, an IPv6 address has a dedicated subnetting portion.

Why Use IPv6?

- IPv6 has a vastly larger address space than IPv4.
  - Results from a 128-bit address (IPv4 uses only 32 bits)
- Other benefits of IPv6:
  - Stateless address autoconfiguration
  - Multicast and mobility
  - Mandatory network layer security
  - Simplified processing by routers

IPv6 Address Types

Prefix	Designation and Explanation	IPv4 Equivalent
::/128	**Unspecified** This address may only be used as a source address by an initialising host before it has learned its own address.	0.0.0.0
::1/128	**Loopback** This address is used when a host talks to itself over IPv6. This often happens when one program sends data to another.	127.0.0.1
::ffff/96 Example: ::ffff:192.0.2.47	**IPv4-Mapped** These addresses are used to embed IPv4 addresses in an IPv6 address. One use for this is in a dual stack transition scenario where IPv4 addresses can be mapped into an IPv6 address. See RFC 4038 for more details.	There is no equivalent. However, the mapped IPv4 address can be looked up in the relevant RIR's Whois database.

IPv6 Address Types

Prefix	Designation and Explanation	IPv4 Equivalent
fc00::/7 Example: fdf8:f53b:82e4::53	**Unique Local Addresses (ULAs)** These addresses are reserved for local use in home and enterprise environments and are not public address space. These addresses might not be unique, and there is no formal address registration. Packets with these addresses in the source or destination fields are not intended to be routed on the public Internet but are intended to be routed within the enterprise or organisation. See RFC 4193 for more details.	Private, or RFC 1918 address space: 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16

IPv6 Address Types

Prefix	Designation and Explanation	IPv4 Equivalent
fe80::/10 Example: fe80::200:5aee:feaa:20a2	**Link-Local Addresses** These addresses are used on a single link or a non-routed common access network, such as an Ethernet LAN. They do not need to be unique outside of that link. Link-local addresses may appear as the source or destination of an IPv6 packet. Routers must not forward IPv6 packets if the source or destination contains a link-local address. Link-local addresses may appear as the source or destination of an IPv6 packet. Routers must not forward IPv6 packets if the source or destination contains a link-local address.	169.254.0.0/16

IPv6 Address Types

Prefix	Designation and Explanation	IPv4 Equivalent
2001:0000::/32 Example: 2001:0000:4136:e378: 8000:63bf:3fff:fdd2	**Teredo** This is a mapped address allowing IPv6 tunneling through IPv4 NATs. The address is formed using the Teredo prefix, the server's unique IPv4 address, flags describing the type of NAT, the obfuscated client port and the client IPv4 address, which is probably a private address. It is possible to reverse the process and identify the IPv4 address of the relay server, which can then be looked up in the relevant RIR's Whois database. You can do this on the following webpage: http://www.potaroo.net/cgi-bin/ipv6addr	No equivalent
2001:0002::/48 Example: 2001:0002:6c::430	**Benchmarking** These addresses are reserved for use in documentation. They should not be used as source or destination addresses.	198.18.0.0/15

IPv6 Address Types

Prefix	Designation and Explanation	IPv4 Equivalent
2001:0010::/28 Example: 2001:10:240:ab::a	**Orchid** These addresses are used for a fixed-term experiment. They should only be visible on an end-to-end basis and routers should not see packets using them as source or destination addresses.	No equivalent
2002::/16 Example: 2002:cb0a:3cdd:1::1	**6to4** A 6to4 gateway adds its IPv4 address to this 2002::/16, creating a unique /48 prefix. As the IPv4 address of the gateway router is used to compose the IPv6 prefix, it is possible to reverse the process and identify the IPv4 address, which can then be looked up in the relevant RIR's Whois database. You can do this on the following webpage: **http://www.potaroo.net/cgi-bin/ipv6addr**	There is no equivalent but 192.88.99.0/24 has been reserved as the 6to4 relay anycast address prefix by the IETF.

IPv6 Address Types

Prefix	Designation and Explanation	IPv4 Equivalent
2001:db8::/32 Example: 2001:db8:8:4::2	**Documentation** These addresses are used in examples and documentation. They should never be source or destination addresses.	192.0.2.0/24 198.51.100.0/24 203.0.113.0/24
2000::/3	**Global Unicast** Other than the exceptions documented in this table, the operators of networks using these addresses can be found using the Whois servers of the RIRs listed in the registry at: http://www.iana.org/assignments/ipv6-unicast-address-assignments	No equivalent single block
ff00::/8 Example: ff01:0:0:0:0:0:0:2	**Multicast** These addresses are used to identify multicast groups. They should only be used as destination addresses, never as source addresses.	224.0.0.0/4

Complete Student Activity 3.5

LESSON 3.6

98-366 Networking Fundamentals

Understand Name Resolution

LESSON 3.6

98-366 Networking Fundamentals

Lesson Overview

In this lesson, you will learn about:

- Domain name resolution
- Name resolution process steps
- DNS
- WINS

Name resolution

- **IP address**
  - Identifies a computer on a network by a unique address
  - A string of four numbers separated by periods is the form of the address (for example, 192.168.1.42)
- **Domain name**
  - Used because people remember words better than numbers (for example, www.microsoft.com)
  - The name has to be assigned to a corresponding IP address to access a domain name.
- A **nameserver** is a server that implements a name-service protocol, which maps an identifier to a system-internal, numeric addressing component.

How WINS Works

- By default, when a system is configured to use WINS for its name resolution, it adheres to h-node for name registration.

1. Checks to see if it is the local machine name
2. Checks its cache of remote names. Any name that is resolved is placed in a cache where it remains for 10 minutes.
3. Tries the WINS Server
4. Tries broadcasting
5. Checks the LMHOSTS file to determine if the system is configured to use the LMHOSTS file
6. Tries the HOSTS file and then a DNS, if so configured

Domain Name System (DNS)

- The Internet maintains two principal namespaces, the domain name hierarchy and the Internet protocol (IP) address system.
- The domain name system maintains the domain namespace and translates between these two namespaces.
- Internet name servers implement the domain name system.
- A DNS name server is a server that stores the DNS records, such as address (A) records, name server (NS) records, and mail exchanger (MX) records for a domain name.

- **Resolvers** are programs that run on DNS clients and DNS servers and that create queries to extract information from name servers.
- Domains define different levels of authority in a hierarchical structure. **The top is called the root domain**. The DNS namespace on the Internet has the following structure:
  - The root domain uses a null label, which you write as a single period (.) and is assigned by organization type and by country/region.
  - Second-level domain contains the domains and names for organizations and countries/regions.
  - A zone is a contiguous portion of a domain of the DNS namespace whose database records exist and are managed in a particular DNS database file stored on one or multiple DNS servers.

- DNS defines two types of name servers:
  - A primary name server gets the data from locally stored and maintained files.
    - To change a zone, such as adding subdomains or resource records, you change the zone file at the primary name server.
  - A secondary name server gets the data across the network from another name server.
- The process of obtaining this zone information (that is, the database file) across the network is referred to as a **zone transfer**.

Host Name Resolution Process

- Resolves a host name to an IP address before the source host sends the initial IP packet
- The default order for domain name resolution

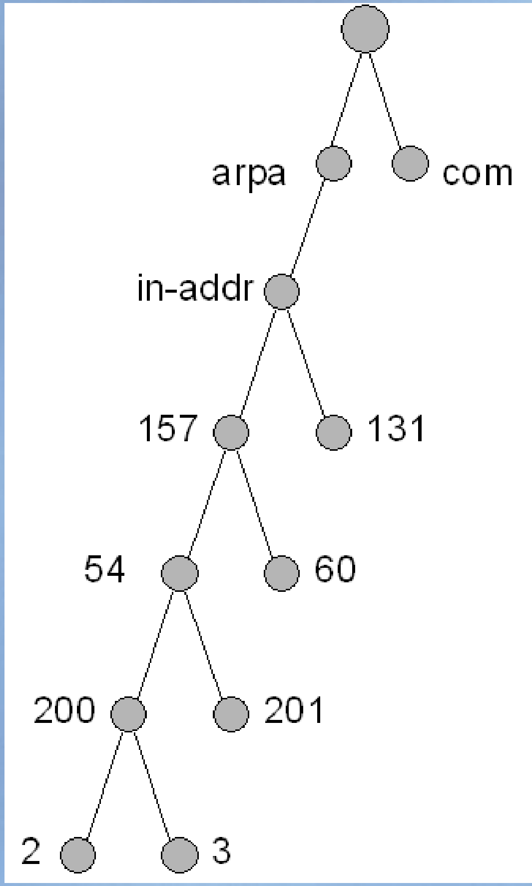
1. Hosts File—There is a file called HOSTS to convert domain names to IP addresses and entries in the HOSTS file dominate mappings that are resolved via a DNS server.
2. Domain Name System —Used for converting domain names to their corresponding IP addresses. The operating system will connect to the DNS server and return to you the IP address for the domain name you queried it with.
3. Netbios—This only applies to Windows machines and will only be used to map names to IP addresses if all previous methods failed. Windows tries NetBIOS name resolution first, then host name resolution.

NetBIOS over TCP/IP Name Resolution <Methods>

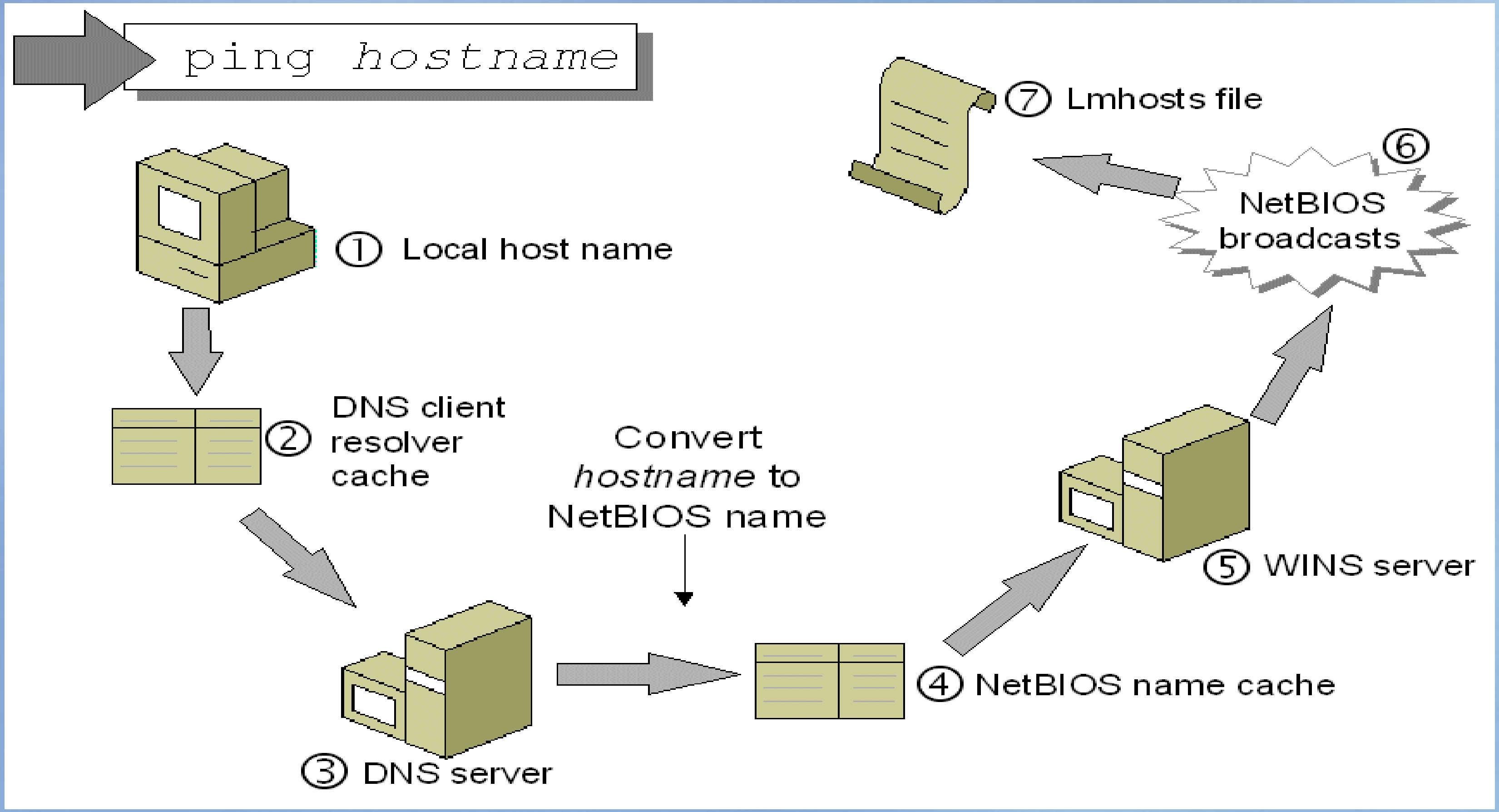
- *b-node*—broadcasts are used for both name registration and name resolution.
- *p-node*—uses point-to-point communications with a name server to resolve names.
- *m-node*—first uses b-node and then, if necessary, p-node to resolve names.
- *h-node*—first uses p-node for name queries and then b-node if the name service is unavailable or if the name is not registered in the database.

Reverse Lookup of the DNS Namespace

- Within the **in-addr.arpa** domain, special pointer (PTR) resource records are added to associate the IPv4 addresses to their corresponding host names.
- To find a host name for the IPv4 address 157.54.200.2, a DNS client sends a DNS query for a PTR record for the name 2.200.54.157.in-addr.arpa.



- All the Methods Used by TCP/IP for Windows XP and Windows Server 2003 for Resolving Host Names



- DNS name resolution is both iterative and recursive resolution.
  1. The user types in a DNS name into a Web browser, which causes a DNS resolution request to be made from her client machine's resolver to a local DNS name server.
  2. That name server agrees to resolve the name recursively on behalf of the resolver, but uses iterative requests to accomplish it.
  3. These requests are sent to a DNS root name server, followed in turn by the name servers for ".edu", "someschool.edu", and "compsci.someschool.edu".
  4. The IP address is passed to the local name server and back to the user's resolver and finally, her Web browser software.

Complete Student Activity 3.6

LESSON 3.7

98-366 Networking Fundamentals

Understand Networking Services

Lesson Overview

In this lesson, you will learn about:

- Networking services
- DHCP
- IPsec
- Remote access

Network Services

- Installed on one server to provide secure shared resources to clients
- Common network services include:
  - Authentication servers—the process by which the system validates a user's logon information
  - Directory services—a service on a network that returns mail addresses of other users or enables a user to locate hosts and services
  - DNS—naming system for computers, services, or any resource connected to the Internet or a private network
  - Network file system—distributed file system accessed over a network
  - E-mail
  - Printing

DHCP—Dynamic Host Configuration Protocol

- An autoconfiguration protocol used on IP networks
- Provides a central way to configure the network settings of all of your networked computers
- If your operating system is configured to use DHCP, users just need to plug in the network cable and are ready to go.
- DHCP can configure:
    - IP address, network mask, DNS address, WINS server address, host name, domain name, gateway address, time server address, print server address
- Keeps track of computers connected to the network and prevents two computers from being configured with the same IP address
- There are two versions of DHCP, one for IPv4 and one for IPv6, with different details of the protocols for each.

Methods of Allocating IP Addresses

- Dynamic—requires use of DHCP
- APIPA—automatically assigns an address as a last resort
- Static—manually assigns an address by an administrator
- DHCP operations fall into four basic phases:
  - IP discovery
  - IP lease offer
  - IP request
  - IP lease acknowledgement

- Where a DHCP client and server are on the same subnet, communication is processed through UDP broadcasts.
- Where the client and server are on different subnets, IP discovery and IP request messages are sent via UDP broadcasts and IP lease offer and IP lease acknowledgement messages are sent via unicast.

Process:

1. A DHCP-configured client connects to a network and sends a broadcast query requesting information from a DHCP server.
2. If the request is valid, the server assigns the client an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters, such as the subnet mask and default gateway.

Remote Access

- Communication with a data processing facility from a remote location through a data link
- Allows you to extend a network beyond the physical boundaries of the wired network
- Available with three models:
  hosting service, software, and appliance

Remote Access Server

- Sometimes called a communication server; is set up to handle users seeking access to network remotely
- Associated with a firewall server to ensure security and a router that can forward requests
- In transport mode, only the payload (the data you transfer) of the packet is encrypted and/or authenticated
- The transport and application layers are always secured by hash, so they cannot be modified in any way.

Internet Protocol Security (IPsec)

- A protocol suite for securing Internet protocol (IP) communications by authenticating and encrypting each IP packet of a data stream
- Includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session
- Protects data flows between a pair of hosts (computer users or servers), between a pair of security gateways (routers or firewalls), or between a security gateway and a host

IPsec (continued)

- IPsec can be used for protecting any application traffic across the Internet and is a framework of open standards.
- Authentication header (AH) provides connectionless integrity and data origin authentication for IP datagrams and provides protection against replay attacks.
- Encapsulating security payload (ESP) is a member of the IPsec protocol suite and provides origin authenticity, integrity, and confidentiality protection of packets.

Complete Student Activity 3.7

LESSON 3.8

98-366 Networking Fundamentals

Understand TCP/IP

Lesson Overview

In this lesson, you will learn about:

- TCP/IP
- Tracert
- Telnet
- Netstat
- Reserved addresses
- Local loopback IP
- Ping
- Pathping
- Ipconfig
- Protocols

Internet Protocol Suite

- Two original components
  - TCP – Transmission Control Protocol
  - IP – Internet Protocol
- TCP operates at a higher level, concerned only with the two end systems such as the Web browser and a Web server.
- IP handles lower-level transmissions from computer to computer as a message makes its way across the Internet.

TCP

- Provides a communication service between an application and the IP
- Provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer
- Controls segment size, flow control, data exchange rate
- Keeps track of the individual units of data transmission, called segments, that a message is divided into for routing through the network
- Applications include e-mail and file transfer, and the Web.

IP

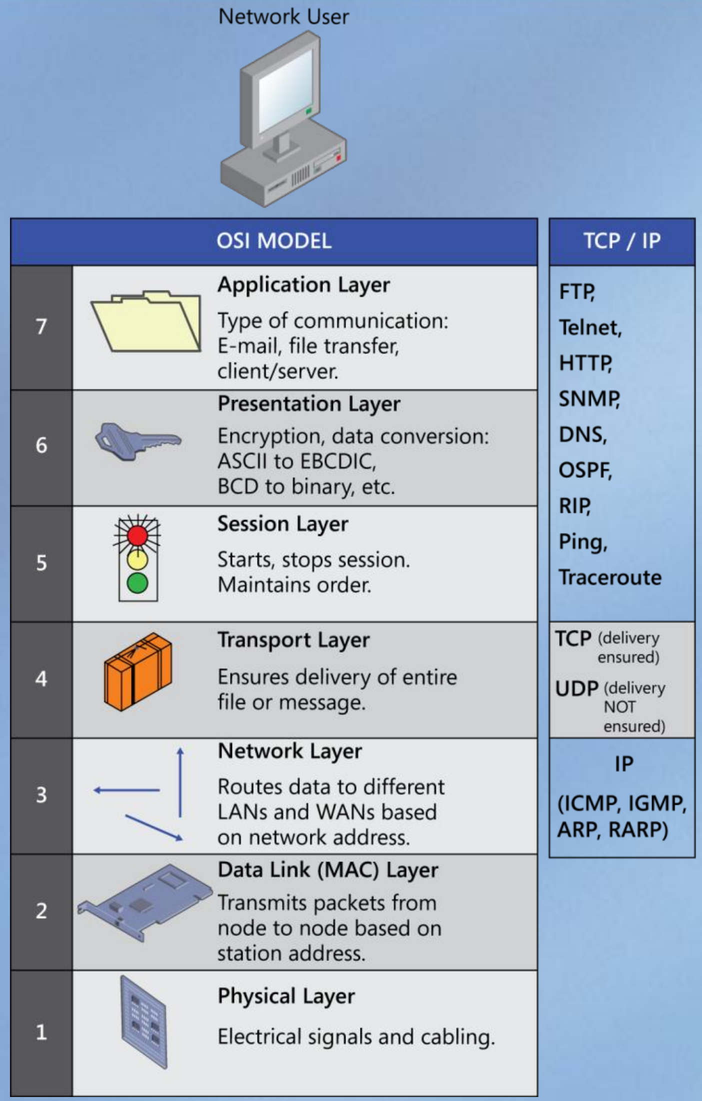
- Handles the actual delivery of the data
- Works by exchanging pieces of information called packets
- For example, when an HTML file is sent from a Web server, the TCP software layer of that server divides the sequence of bytes of the file into segments and forwards them individually to the IP software layer (Internet Layer).
- The Internet layer encapsulates each TCP segment into an IP packet by adding a header that includes (among other data) the destination IP address.

IP Packets

- A sequence of bytes consisting of a *header* and a *body*
  - The header describes the packet's destination and the routers to use for forwarding until it arrives at the final destination.
  - The body contains the data IP it is transmitting.
- IP packets can be lost, duplicated, or delivered out of order.
  - TCP detects these problems, requests retransmission of lost packets, rearranges out-of-order packets, and helps minimize network congestion.
- Individual packets of the same message can be routed on different paths through the network.

TCP/IP Stack

- The TCP or UDP transport layer 4 sends packets to IP network layer 3, which adds its own header and delivers a "datagram" to a data link layer 2 protocol.
- TCP/IP tools are in layers 7, 6, 5.

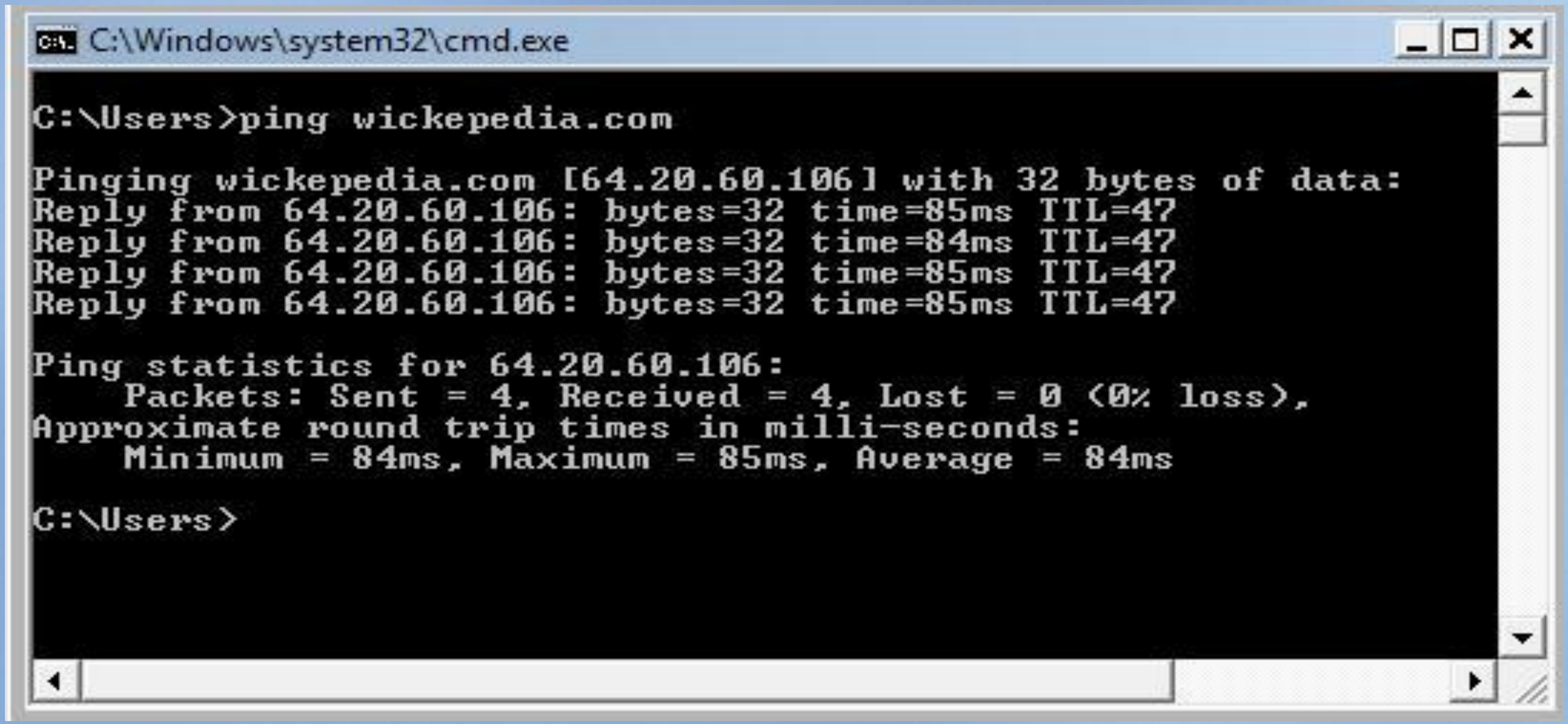


Port Numbers

- TCP uses port numbers to identify sending and receiving application end-points on a host.
- Three basic categories: well-known, registered, and dynamic/private
- Some examples include FTP (21), SSH (22), TELNET (23), SMTP (25) and HTTP (80).

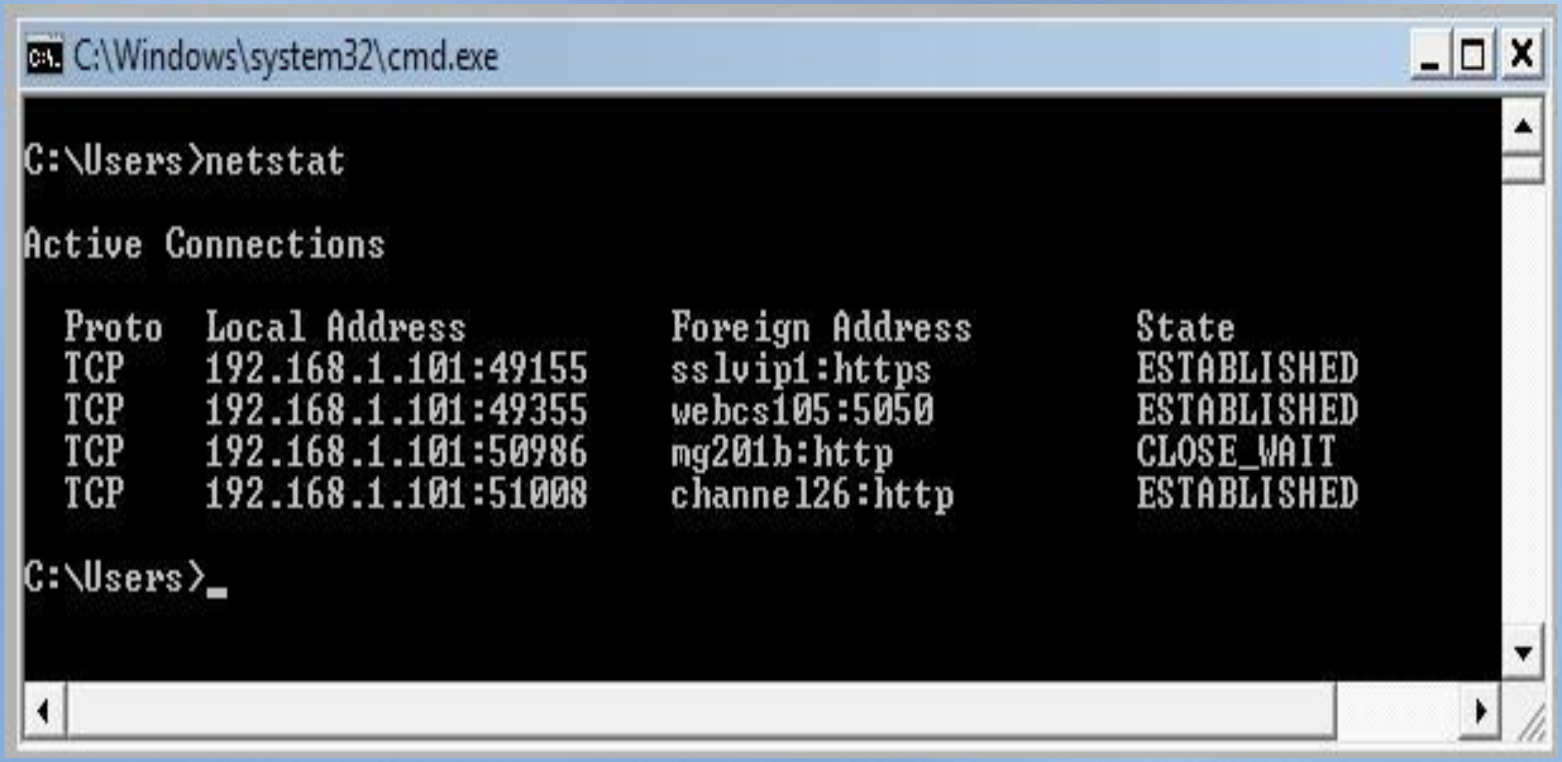
TCP/IP Tools

- **Ping**: Tests if a particular host is reachable across an IP network; measures the round-trip time for packets sent from the local host



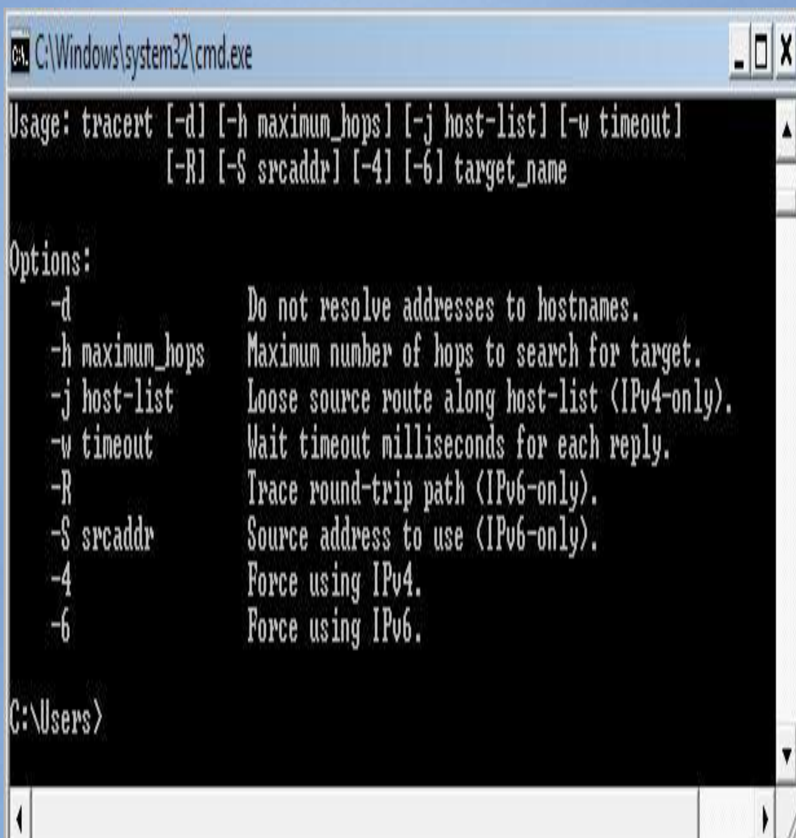
TCP/IP Tools

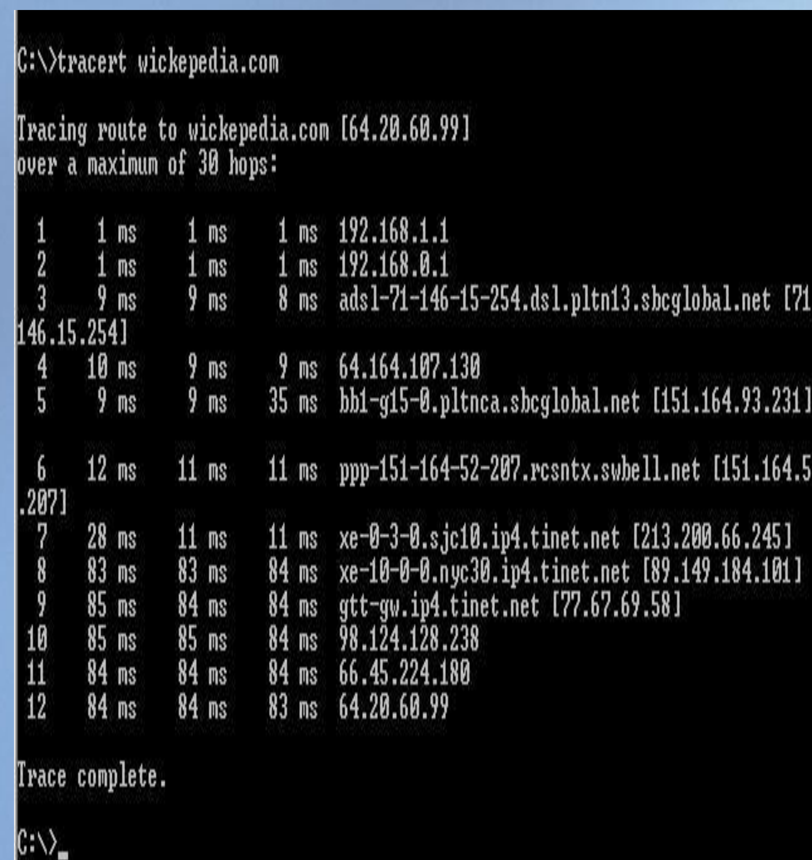
- **Netstat:** Displays current TCP/IP network connections and protocol statistics



TCP/IP Tools

- **Tracert**: Shows the route taken by packets across an IP network





TCP/IP Tools

- **Ipconfig**: Displays all TCP/IP network configuration values and refreshes DHCP and DNS settings
- **/?** Command will play all options available with ipconfig

```
C:\Users>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /allcompartments Display information for all compartments.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                       ... Show information
    > ipconfig /all                  ... Show detailed information
    > ipconfig /renew                ... renew all adapters
    > ipconfig /renew EL*            ... renew any connection that has its
                                         name starting with EL
    > ipconfig /release *Con*        ... release all matching connections,
                                         eg. "Local Area Connection 1" or
                                             "Local Area Connection 2"
    > ipconfig /allcompartments      ... Show information about all
                                         compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                                         compartments

C:\Users>_
```

TCP/IP Tools

- **Pathping**: Displays the degree of packet loss along the path

C:\Windows\system32\cmd.exe

```
C:\Users>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.

C:\Users>_
```

C:\Windows\system32\cmd.exe

```
C:\>pathping wickepedia.com

Tracing route to wickepedia.com [64.20.60.99]
over a maximum of 30 hops:
  0  No resources.

C:\>_
```

TCP/IP Tools

- **Telnet**: A terminal emulation program for TCP/IP networks
- **Local loopback IP**: Tests the TCP/IP protocol implementation on a host -special range of addresses (127.0.0.0 to 127.255.255.255) is set aside
- **Localhost**: Translates to the loopback IP address 127.0.0.1 in IPv4 or ::1 in IPv6

Complete Student Activity 3.8

Complete Quia Test:

MTA NetFund3 Test