Networking Concepts

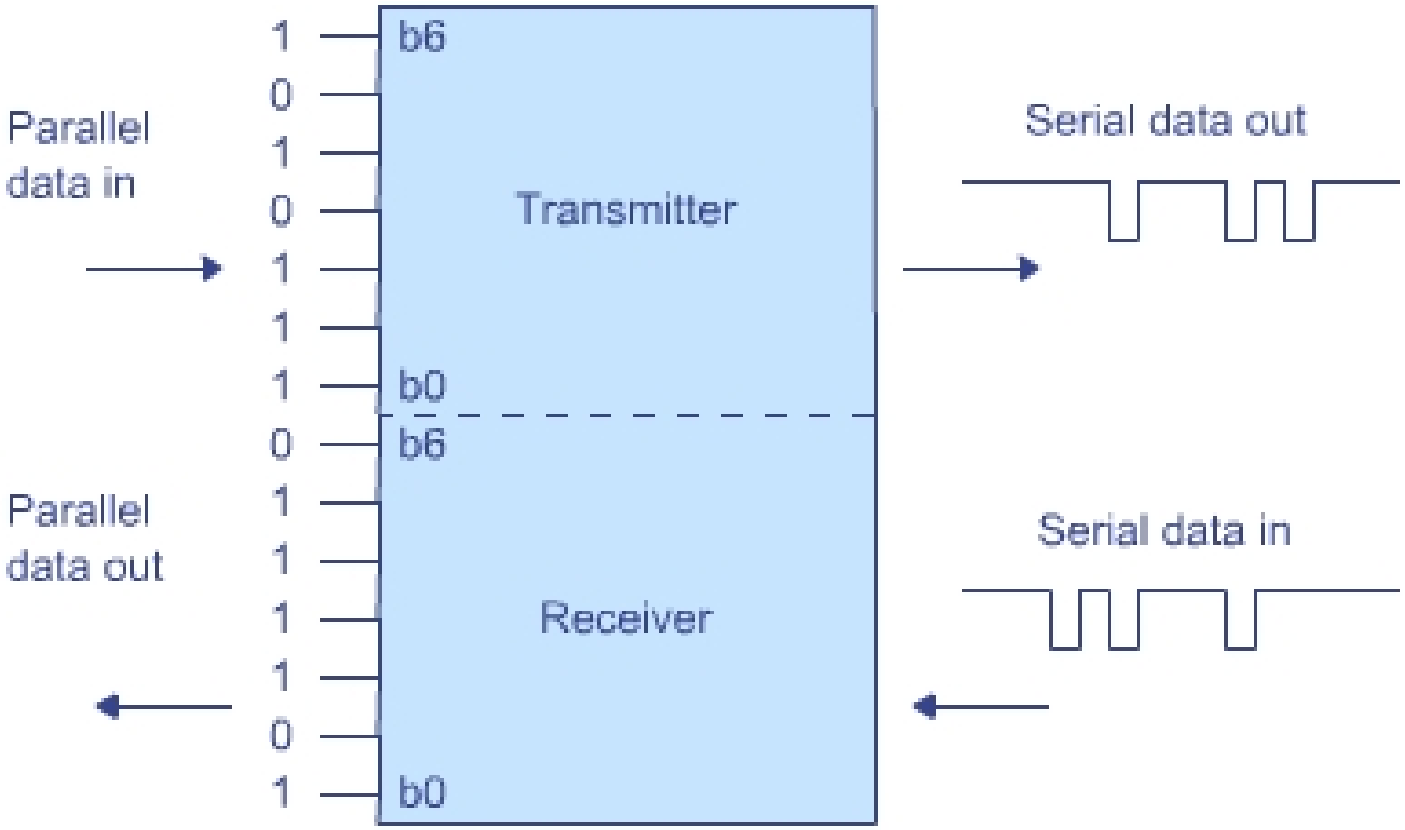
Unit 4,Chapter 6

Low Level (802.2) Protocols

Serial Data Communication

- Serial data communication takes place one bit at a time over a single communication line.
- A single transmit wire and a single receive wire, not possible to send a clock signal with the waveform. (asynchronous communication)
- Start and stop bits are used to synchronize the transmitter and receiver

Serial Data Communication:
The UART



- Universal Asynchronous Receiver Transmitter – converts parallel data to serial output or serial input data is converted into parallel output data.

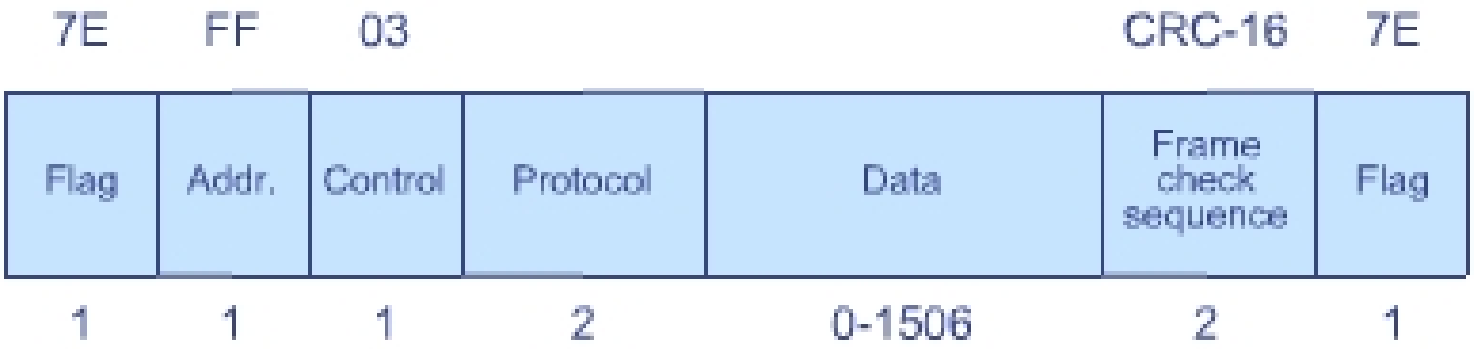
SLIP – Serial Line Interface Protocol

Features of Slip

- Static IP addresses
- Supports TCP/IP only
- Asynchronous
- No compression
- No security
- 56 Kbps maximum
- No link testing
- Layer 1 operation

First protocol used to transmit the Transmission Control Protocol/Internet Protocol (TCP/IP) over dial up phone line.

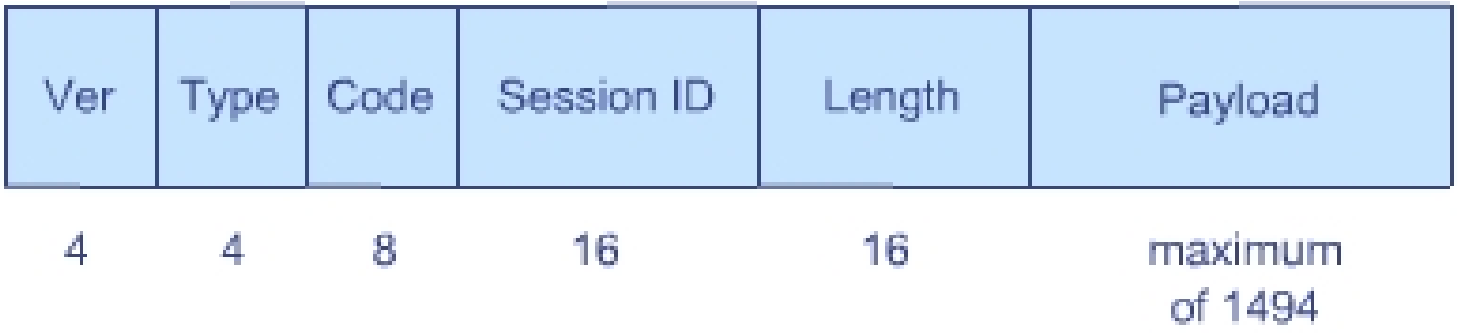
Point to Point Protocol:
PPP Frame Format



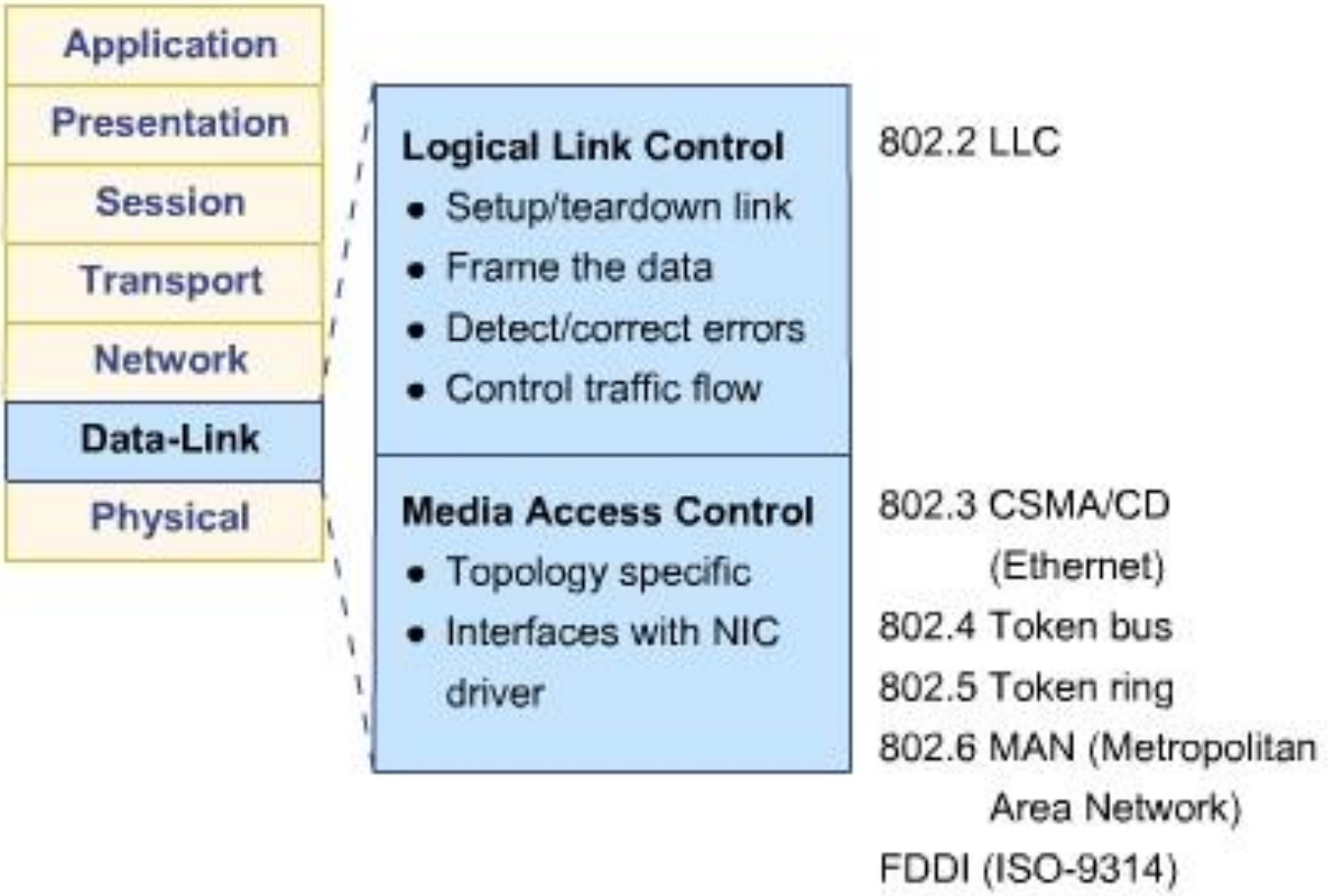
Point to Point Protocol:
Comparing SLP and PPP

SLIP	PPP
Static IP addresses	Dynamic IP addresses
Supports TCP/IP only	Supports TCP/IP, IPX, NetBUI, AppleTalk, and others
Asynchronous	Asynchronous and synchronous
No compression	Compression supported
No security	Security supported
56 Kbps maximum	No speed limit
No link testing	Link testing supported
Layer 1 operation	Layers 1 and 2 operation

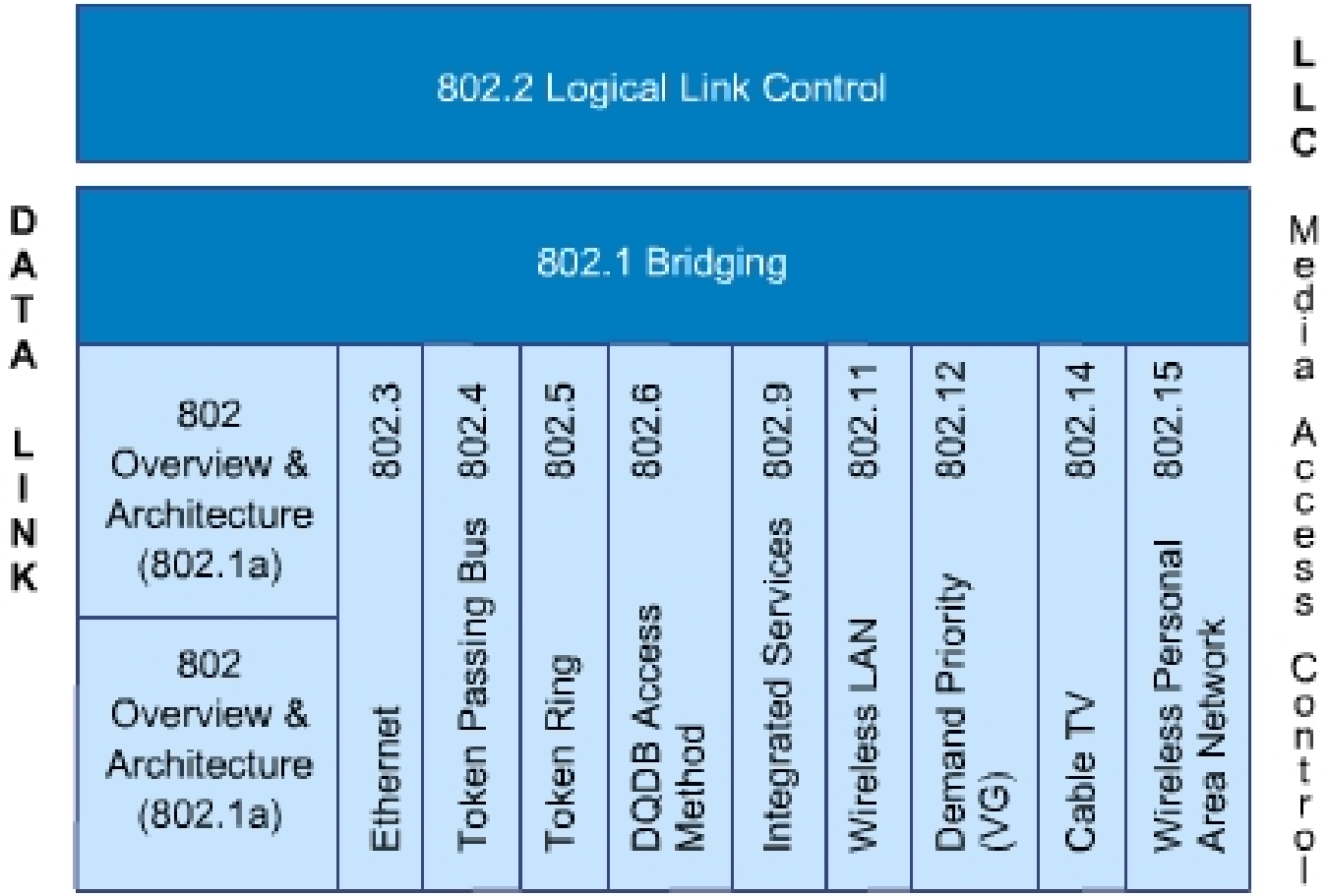
PPPoE Frame Format



Logical Link Control:
Data-Link Layer Details



Logical Link Control:
LLC Protocol Data Unit



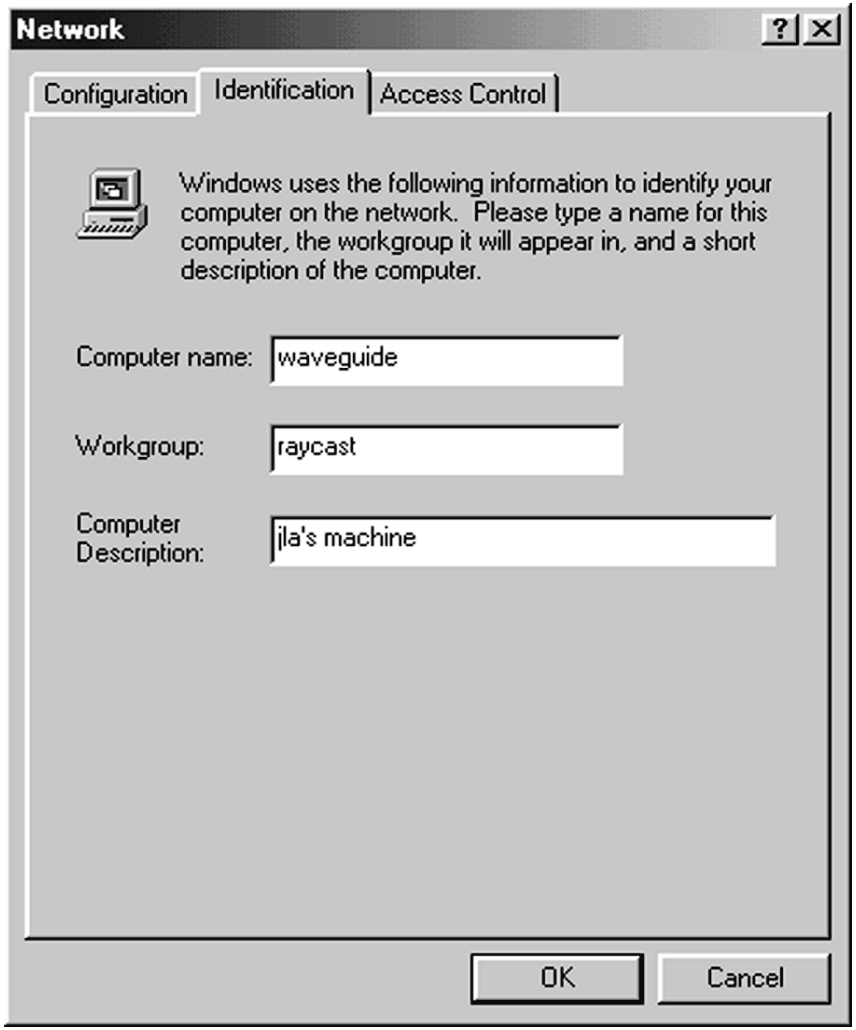
NetBIOS

- Network Basic Input/Output System
- Provides the functionality needed to share resources between networked computer
- Three types of services
  - Name: Finding and naming machines
  - Session: Connection-oriented reliable transfer of messages
  - Datagram: Connectionless non-reliable datagram transfer
- Main component is the Server Message Block (SMB)

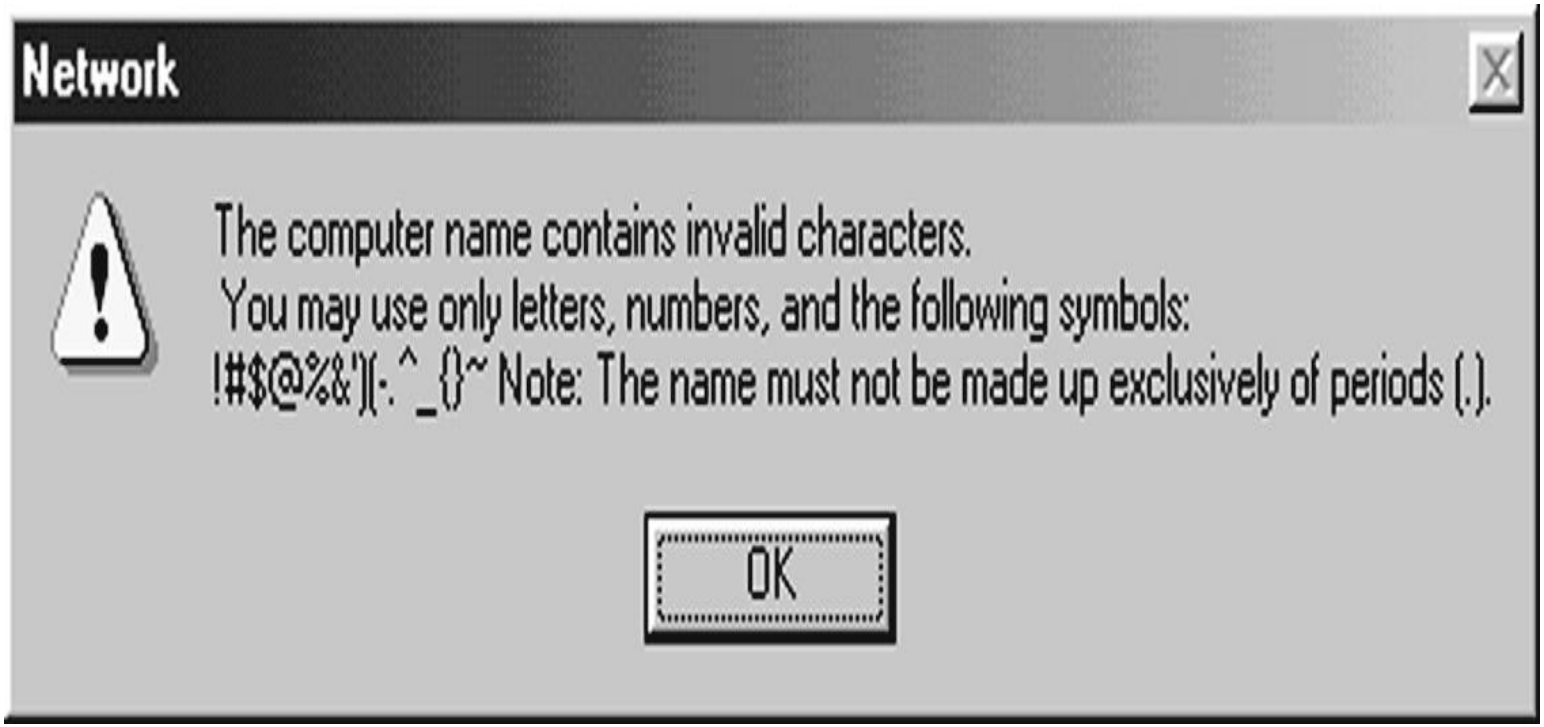
NetBIOS:
Sample NetBIOS Commands

Command	Description
Bad command	Invalid SMB command
Change/check dir	Change to directory or check path
Change password	Change password of user
Copy file	Copy file to specified path
Delete file	Delete the specified file
Find unique	Search directory for specified file
Get resources	Get availability of server resources
Mailslot message	Mail slot transaction message
Named pipe call	Open, write, read, or close named pipe
Rename file	Rename the specified file to a new name
Reserve resources	Reserve resources on the server
Session setup	Log-in with consumer-based authentication

NetBIOS:
Network Identification



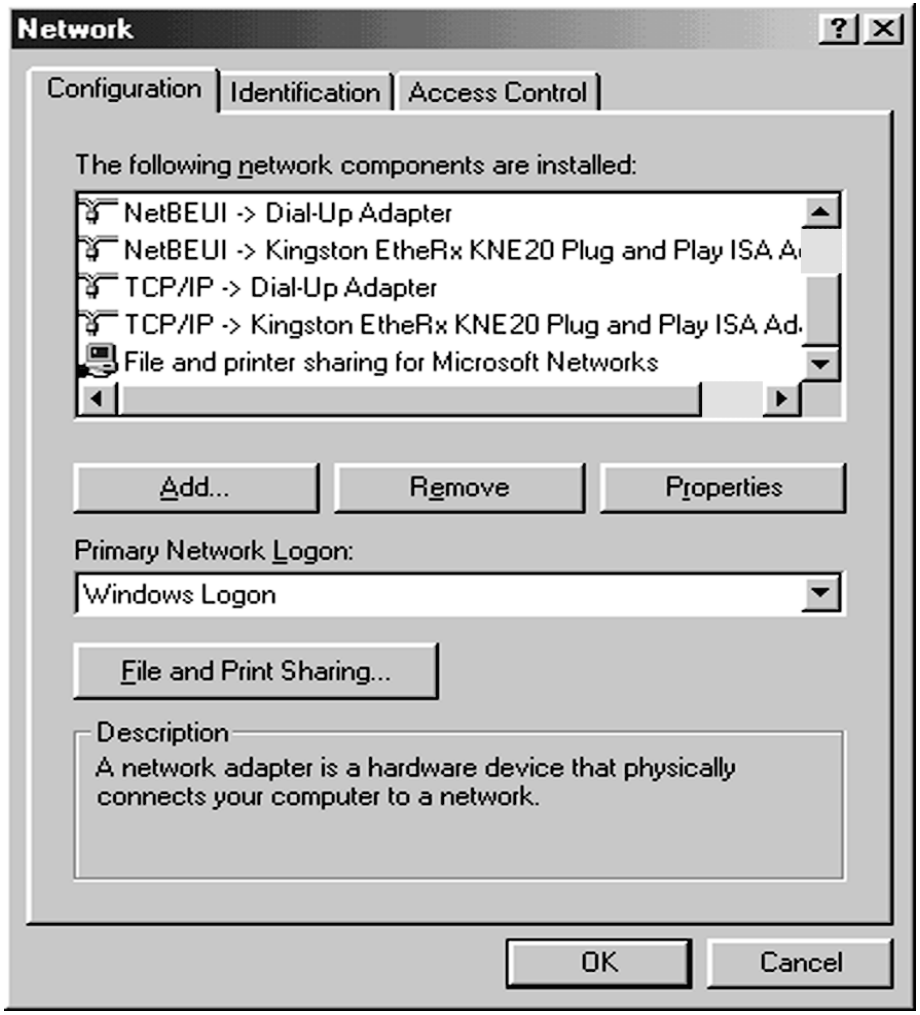
NetBIOS:
Error Messages



NetBEUI

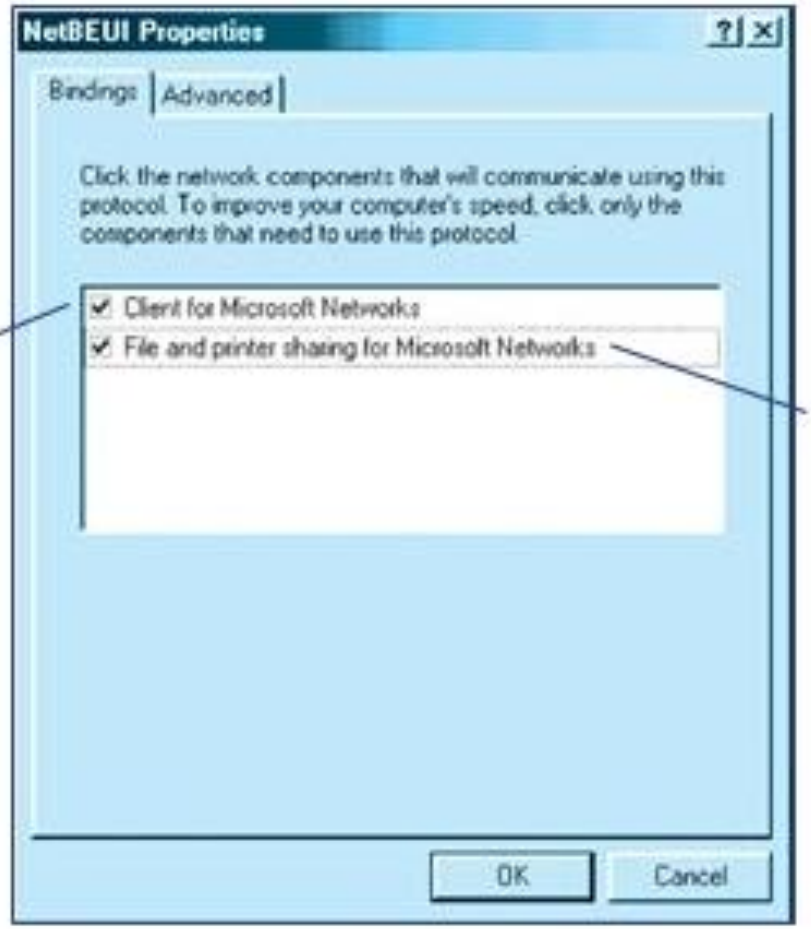
- Provides a transport mechanism to deliver NetBIOS message over a LAN.
- Does not conform to the OSI model
  - Uses transport, network and LLC part of Data-Link
- Windows Internet Name Service (WINS) maps NetBIOS name to IP addresses when larger network are needed.
- Invented by IBM for LAN Manager
- Adapted by Microsoft for use in Window for Workgroups 3.11

NetBEUI:
Configuration



NetBEUI:

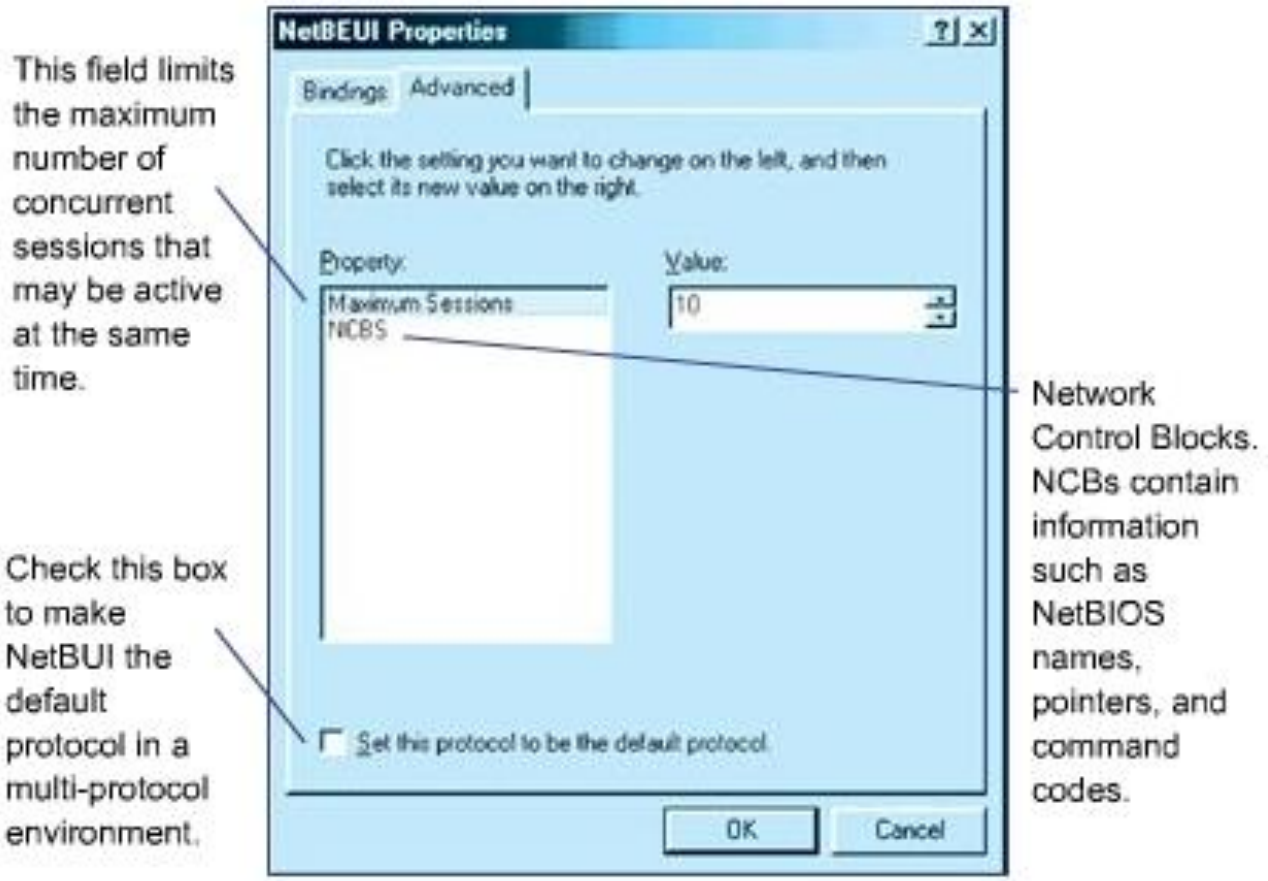
NetBEUI Properties Window: Bindings Tab



This box must be checked to participate in a Microsoft network (i.e., show up in Network Neighborhood, share files, map network drivers).

This box must be checked in order to share files and printers on a Mircosoft network.

NetBEUI:
Network Properties Window: Advanced Tab



Networking Concepts

Unit 4, Chapter 7

The TCP/IP Protocols

Objectives

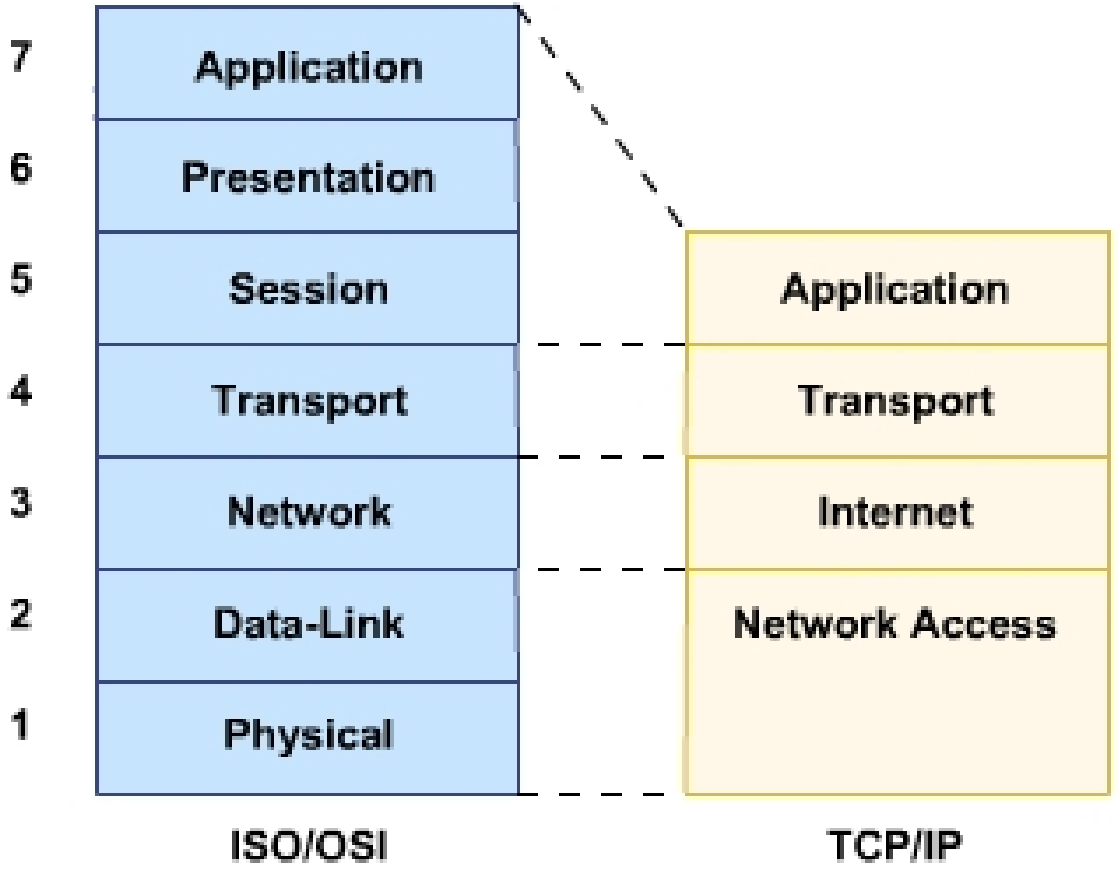
- Identify each layer of the TCP/IP protocol stack.
- Compare the TCP/IP suite with layers of the OSI model.
- Identify the PDU for each step of data encapsulation for each layer of the OSI model.

TCP/IP

- Transmission Control Protocol/Internet Protocol suite.
- One of the most popular networking protocols ever developed.
- Used in the 1960's to connect large mainframe computer together to share information among the research community and the Department of Defense.
- Now used to support the internet

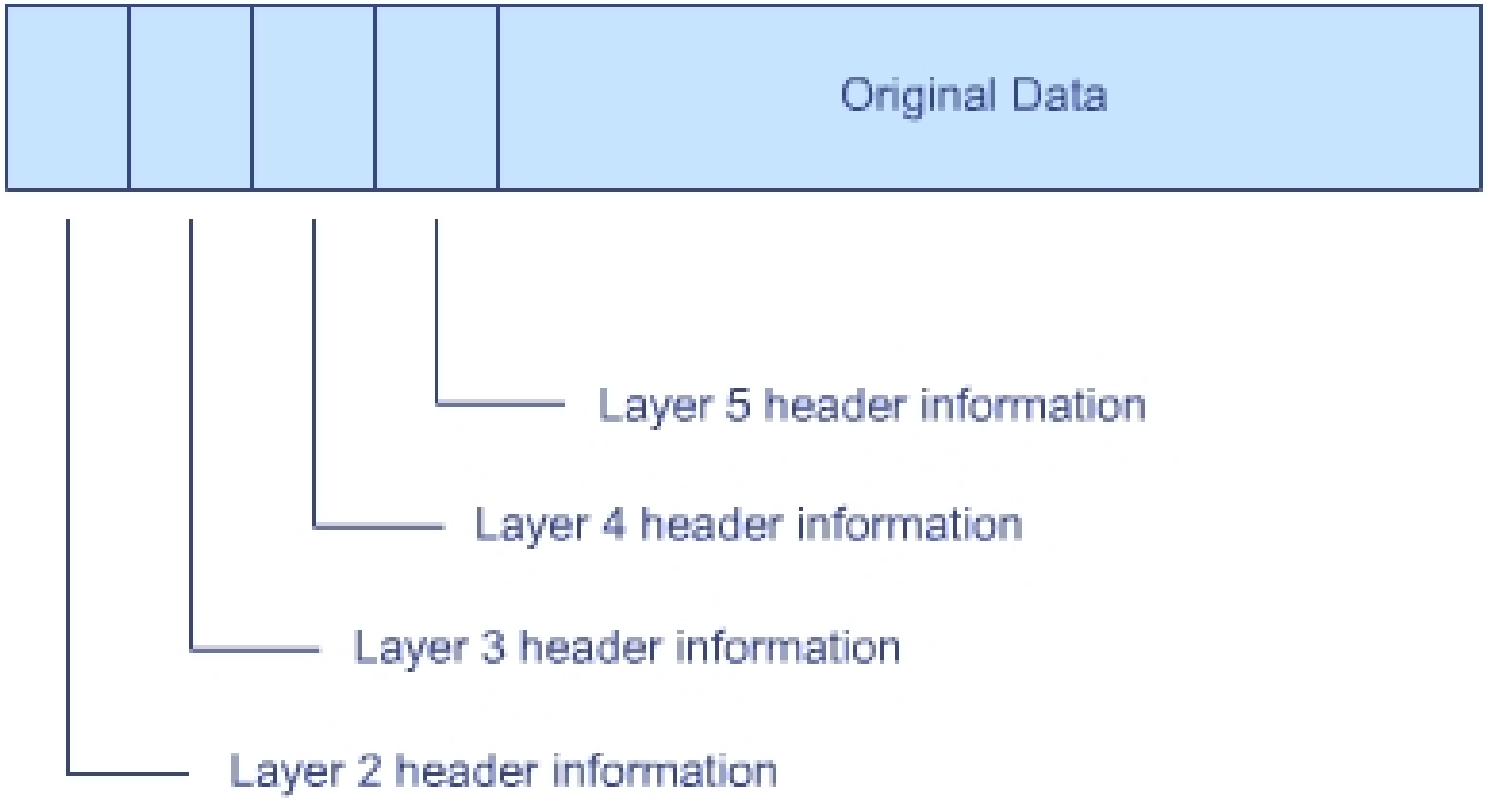
OSI Model versus TCP/IP Model:

OSI vs TCP/IP Model

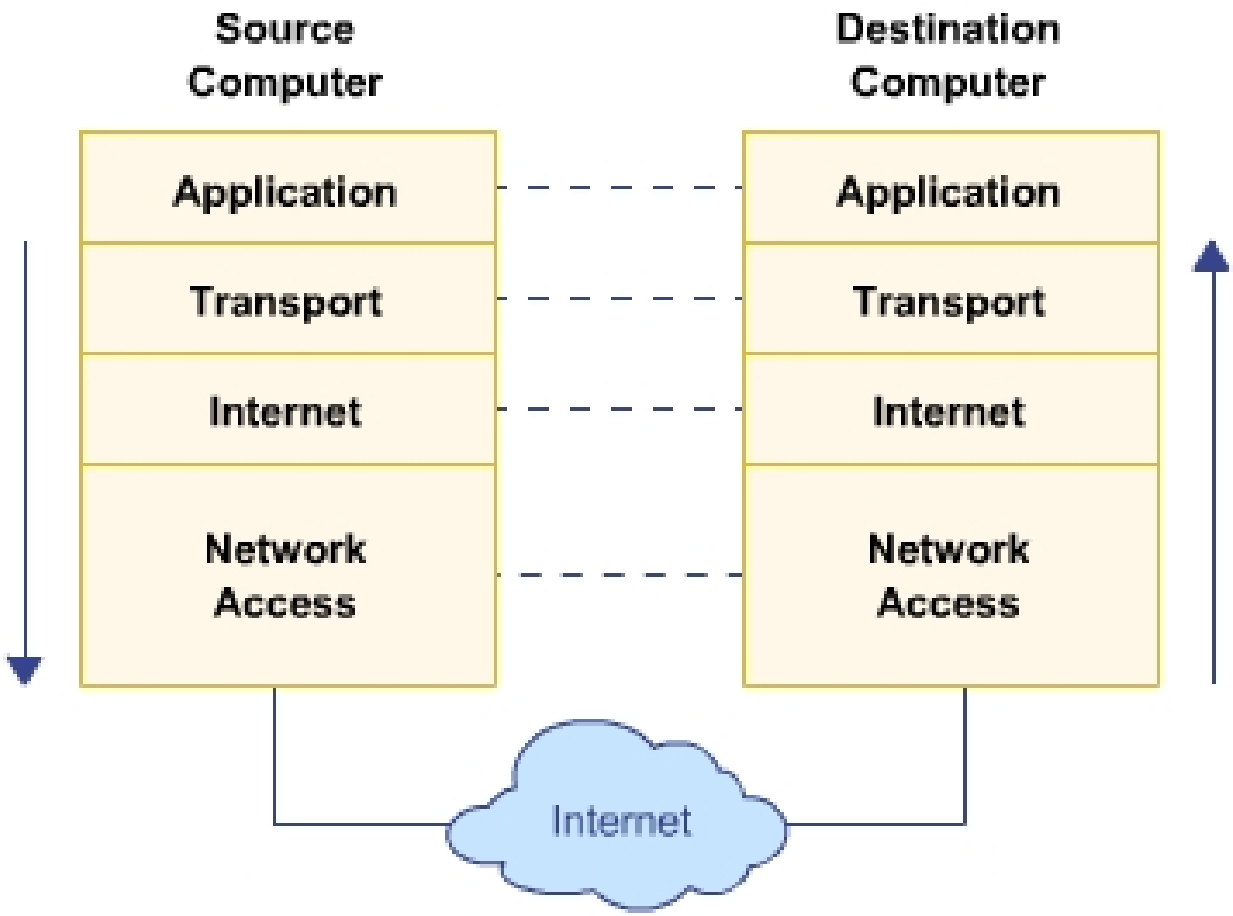


TCP/IP Stack Layering

The packet of data that is transmitted from the source computer contains an informational header for each layer in the protocol stack (except layer 1)



TCP/IP Message Layering



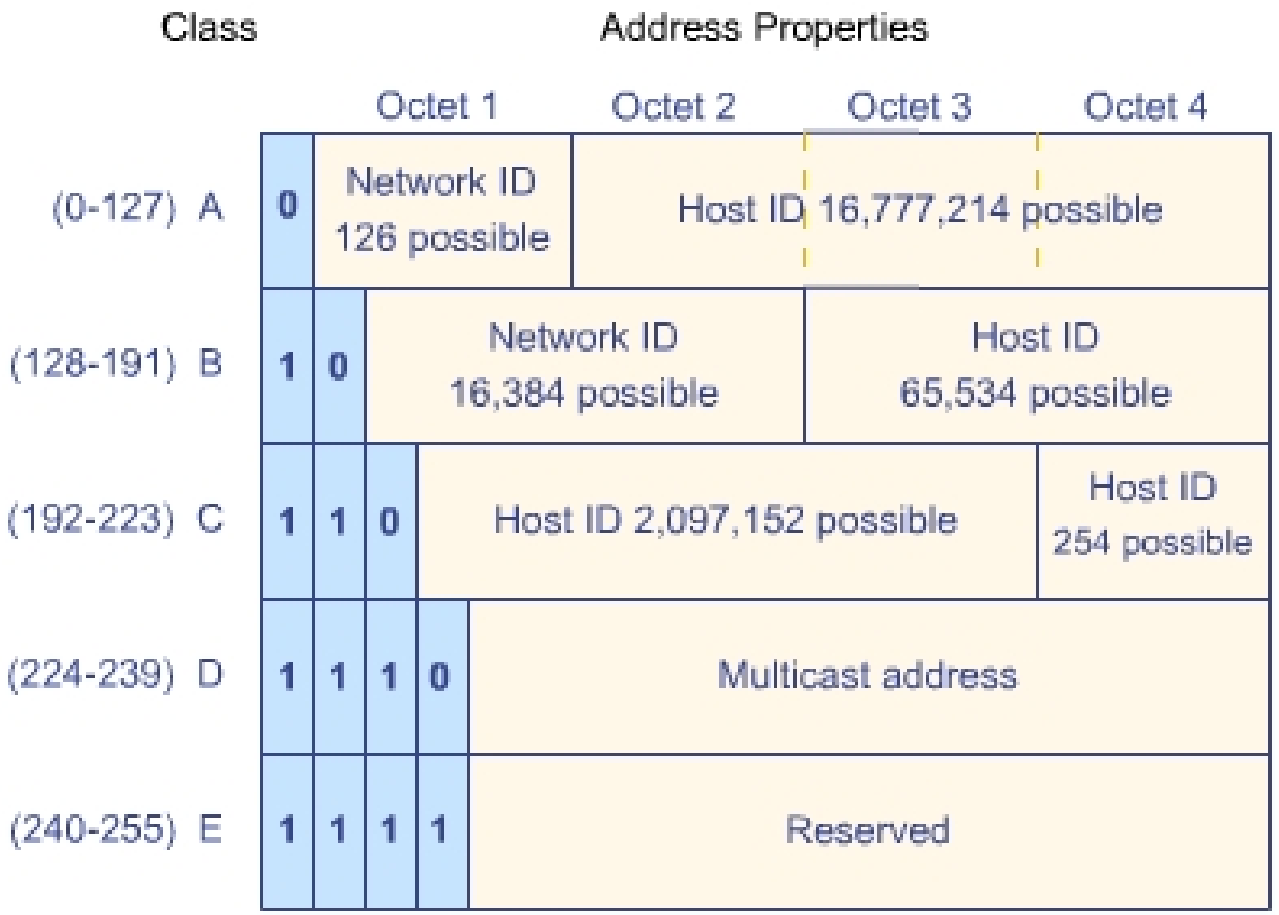
IP

- Base Layer of the TCP/IP suite
- Internet layer in the TCP/IP stack
- No direct link between the source and destination computer on the Internet. Packet may be placed out of order.
- IP is considered to be unreliable since there is no guarantee the datagram will reach its destination.
- IP provides what is called best effort delivery.

IP Addresses

- 32 bit number
- Divided into four sections containing 8 bits each (octets)
- Four values are divided by periods (dotted decimal notation)
- Assigned by software (statically or dynamically)
- Must be unique on the network

Address Classes:
IP Address Classes



Address Classes:
IP Address Rule I

RULE #1

You cannot assign an IP address to a host if the address has all zeros in the network portion of the IP address nor can you use an address that has all zeros in the host portion of the address.

0.0.0.0	Null Network ID
10.0.0.0	Network ID
10.0.3.1	Network Address with a Host ID

Address Classes:
IP Address Rule II

RULE #2

All ones in the network portion of an IP address are not allowed. All ones are used as a broadcast address. All ones in the host portion of the address are not allowed. All ones in the host portion of an IP address are used to send a layer 3 broadcast to every host on that specific network. This is what is called a directed broadcast.

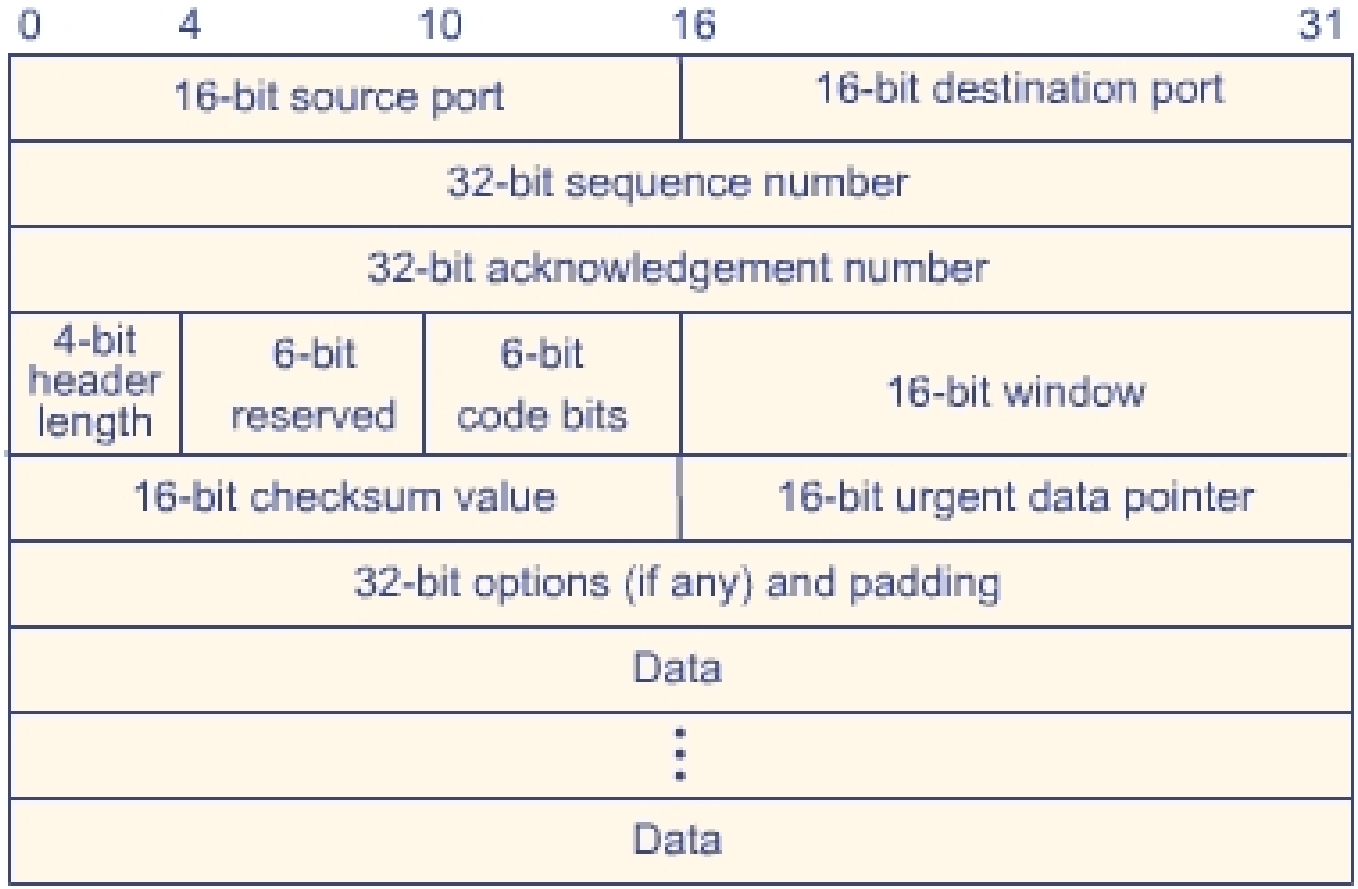
10.0.0.0	Network ID
10.0.3.1	Network Address with a Host ID

Address Classes:
IP Address Rule III

RULE #3

The final rule, the Class A 127.x.x.x network is set aside for loopback testing of the TCP/IP protocol stack (pinging your computer for testing purposes). Formally the specific IP address of 127.0.0.1 is designated as the loopback address but normally you can use any 127.x.x.x address for testing (stick to using 127.0.0.1 and you will do better on those certification tests). This address is actually used for testing proper installation of the TCP/IP protocol stack. This tests the stack all the way down to the LLC layer of the OSI model.

TCP/IP Header:
TCP Header Format



TCP

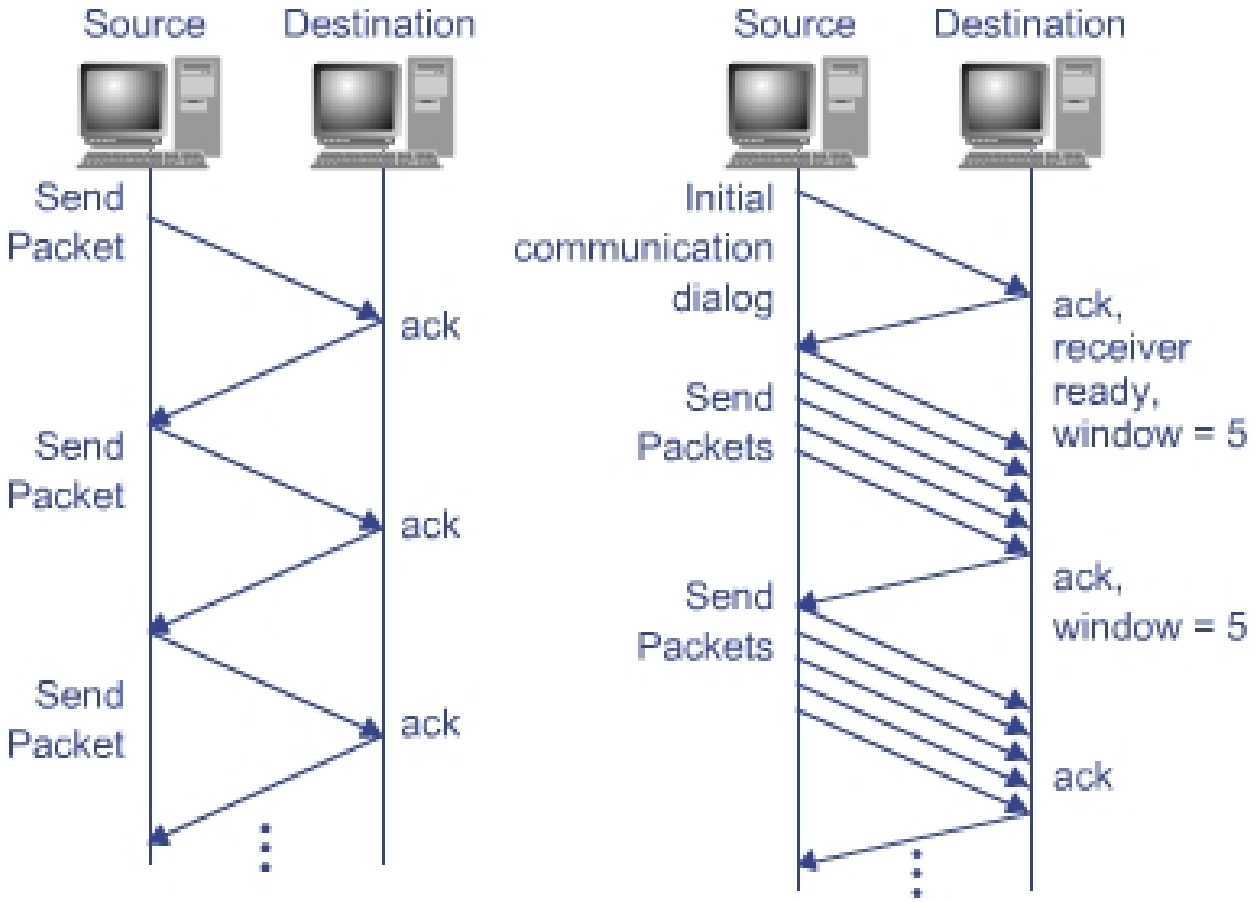
- Defines a standard way that two computers can reliably communicate together over interconnected networks.
- Establish connections through the use of predefined ports or sockets.
- Reliable with error checking

TCP/IP Header:
TCP Header Field Information

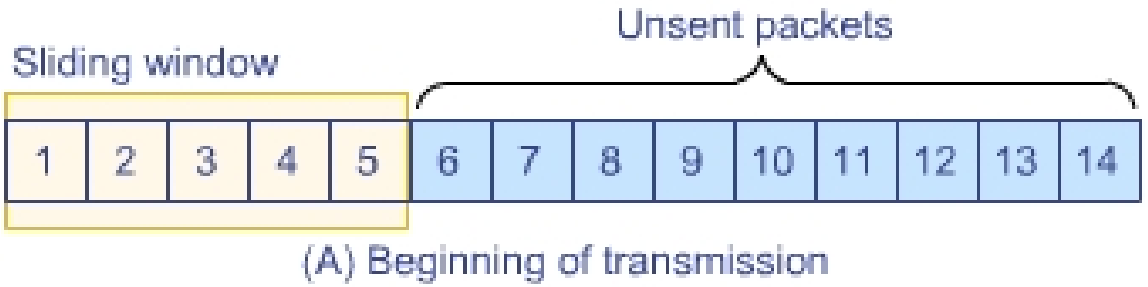
Header Field	Size	Meaning
Source Port	16 bits	Source port service access point
Destination Port	16 bits	Destination port service access point
Sequence Number	32 bits	Sequence number of the current data segment
Acknowledgment Number	32 bits	The acknowledgement number contains the sequence number of the next data byte that TCP expects to receive
Header Length	4 bits	Number of 32-bit words in the TCP header
Reserved	6 bits	Flags reserved for future use
Code Bits	6 bits	Flags used to control the Urgent pointer, Acknowledgment field, Push function, Reset function, Sequence number synchronization, and final data indication
Window	16 bits	Contains the number of data bytes starting with the one in the acknowledgment field
Checksum	16 bits	The checksum value of the entire data segment to be transmitted
Urgent Pointer	16 bits	Indicates the amount of urgent data in the segment
Options and Padding	32 bits	One option currently defined that specifies the maximum data segment size that will be accepted

TCP/IP Header:

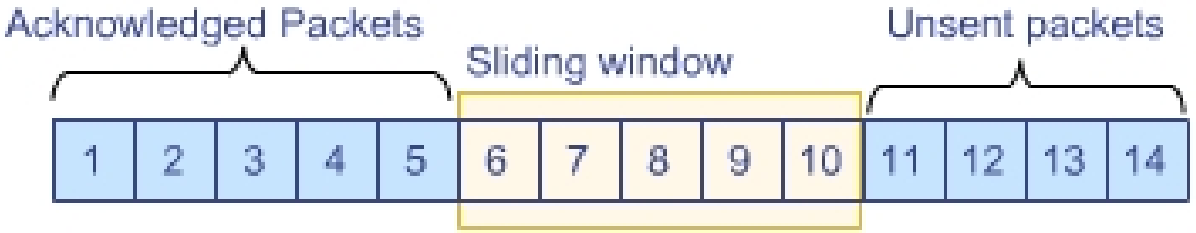
Stop-and-Go (left) versus Sliding Window Flow Control (right)



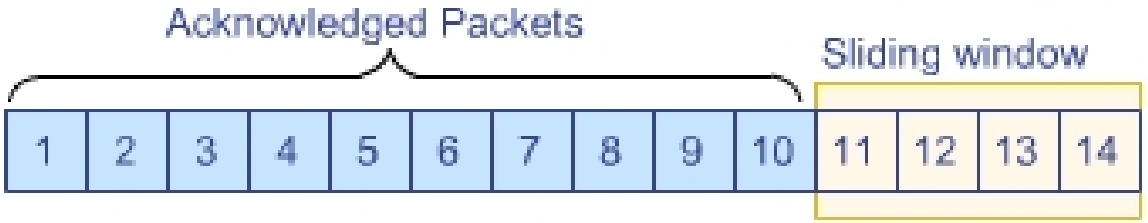
TCP/IP Header:
Sliding Window Flow Control in Operation



(A) Beginning of transmission



(B) After one acknowledgments.



(C) After two acknowledgments.

TCP/UDP Port Number:
Selected Well-Known Port Numbers

Port	TCP	UDP	Protocol
20			FTP Data
21	✓		FTP Control
22	✓		SSH (Secure Shell)
23	✓		Telnet
25	✓		SMTP
53	✓	✓	DNS
69		✓	TFTP
80	✓		HTTP

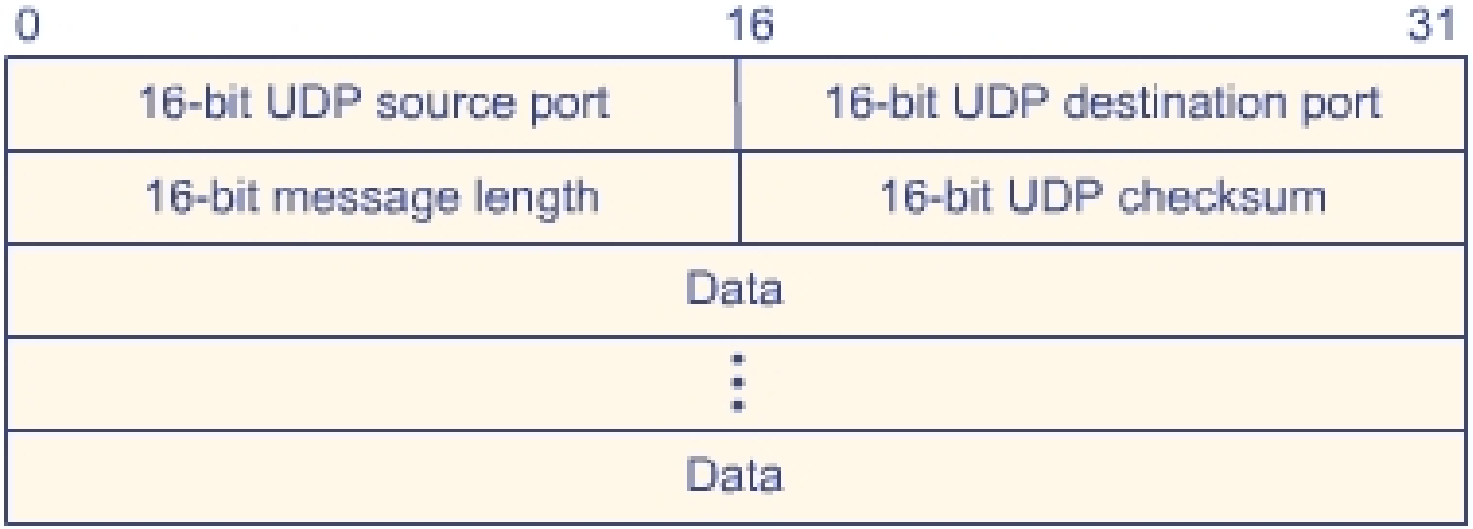
TCP/UDP Port Number:
Selected Well-Known Port Numbers

PORT	TCP	UDP	Protocol
110	✓		POP3
111	✓	✓	SUN RPC
119	✓		NNTP
123	✓	✓	NTP
137	✓	✓	NetBIOS Name
138	✓	✓	NetBIOS Datagram
139	✓	✓	NetBIOS Session
143	✓		IMAP v2
161		✓	SNMP
179	✓		BGP
194		✓	IRC
220	✓		IMAP v3

UDP

- User Datagram Protocol
- Connectionless and unreliable
- Used for:
  - DNS
  - DHCP
  - Network games
- Will retransmit the request if a response is not obtained in a timely fashion

UDP Header:
UDP Diagram Format



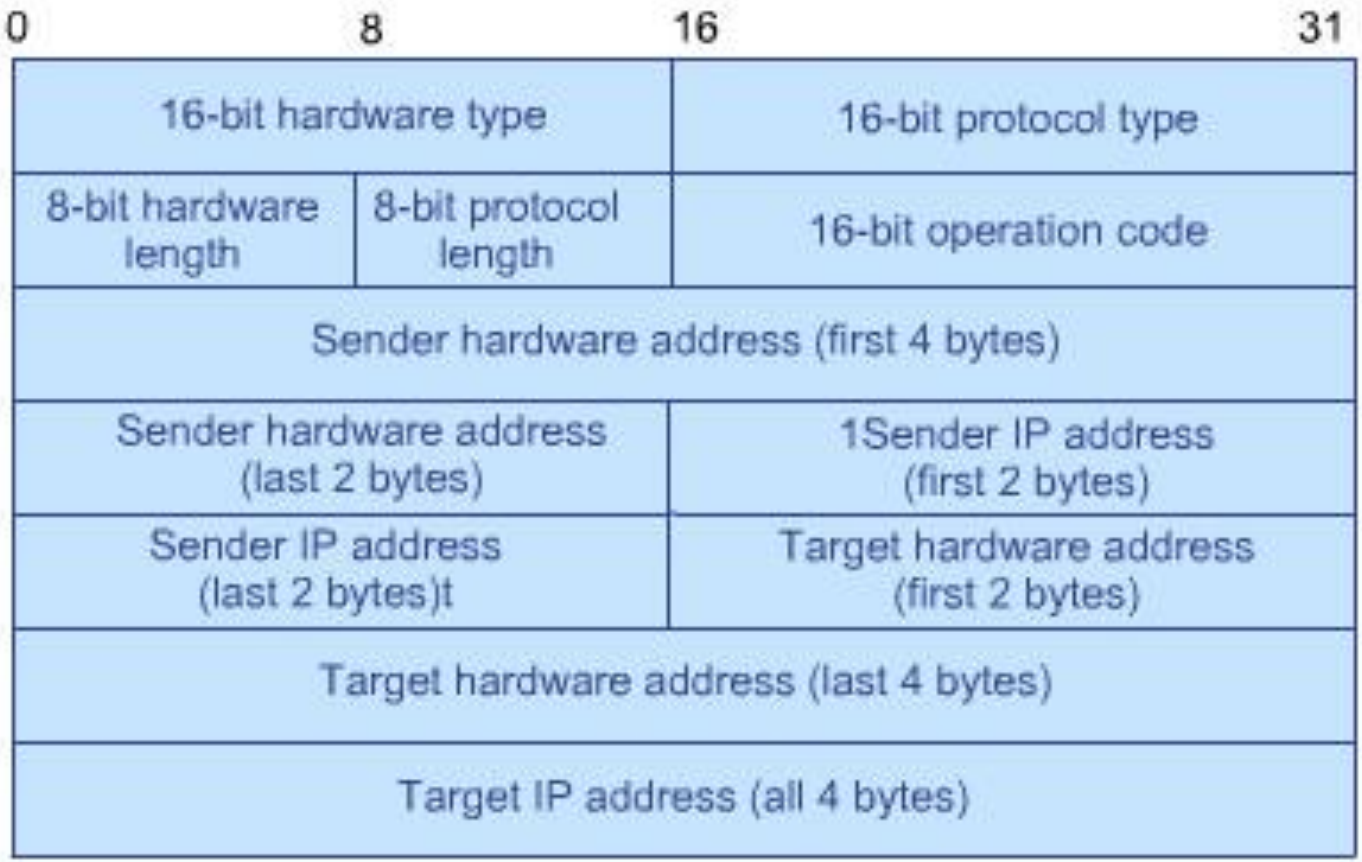
UDP Header:
IP Header Field Information

Header Field	Size	Meaning
Source Port	16 bits	Source port service access point
Destination Port	16 bits	Destination port service access point
Length	16 bits	Contains the length of the segment including the header field and the data
Checksum	16 bits	The checksum value of the complete data segment

ARP and RARP

- The hardware address of the destination computer must be known before any packet can be transmitted from one networked computer to another.
- Uses Media Access control (MAC) address
- ARP uses a direct broadcast message to obtain the MAC address for a given address
- RARP provides the IP address for a specific MAC address

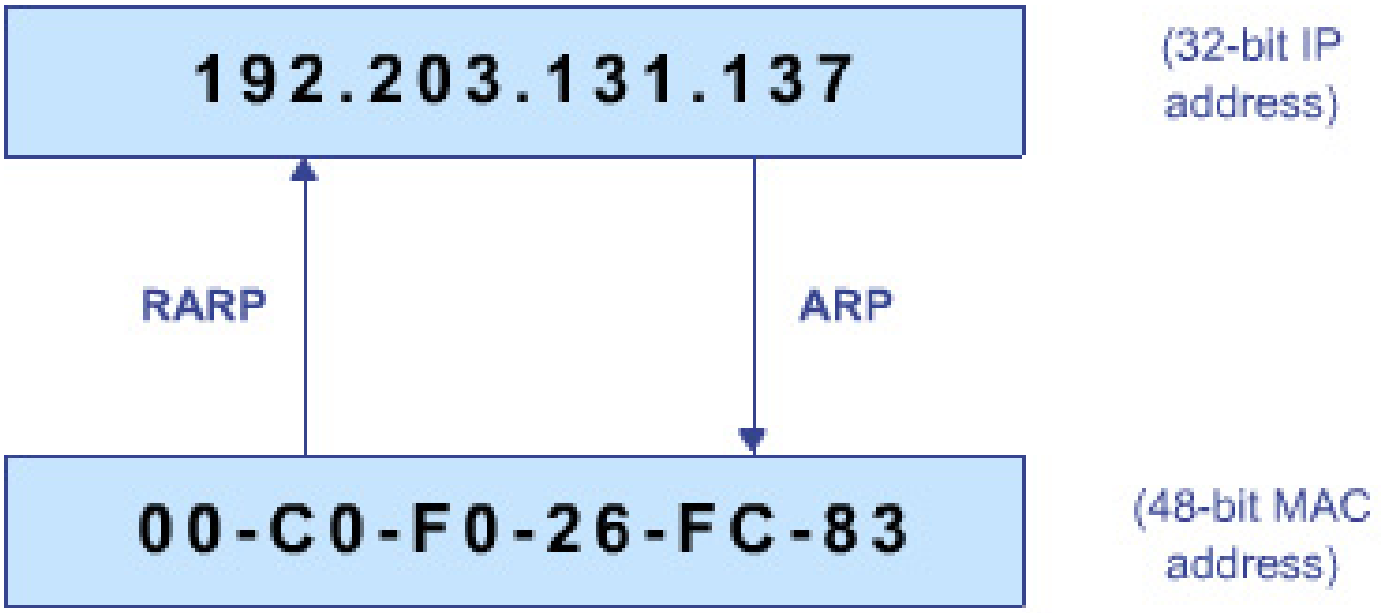
ARP and RARP:
Message Format



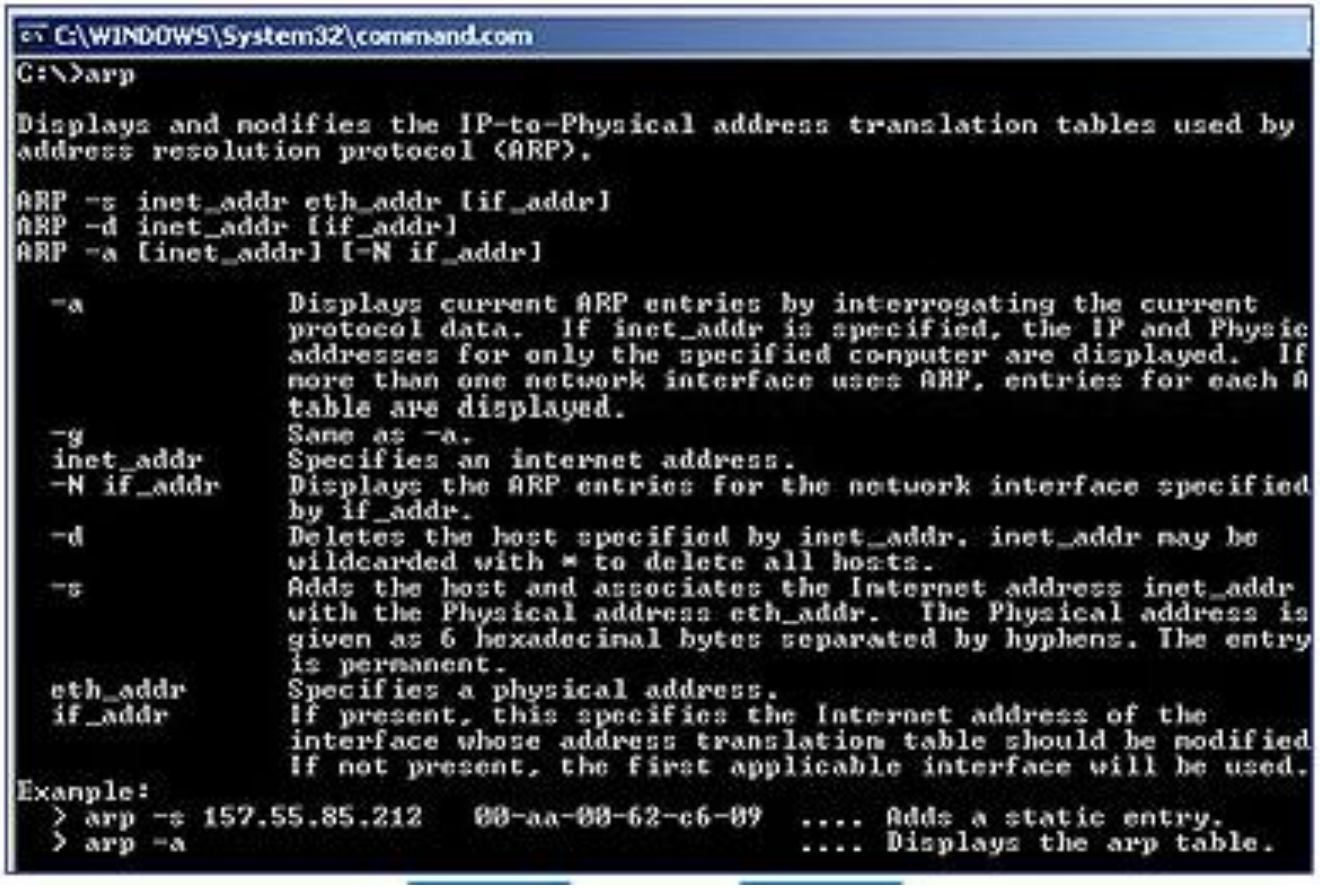
ARP and RARP:
Header Field Information

Meaning	Size	Meaning
Hardware Type	16 bits	Specifies the type of hardware interface
Protocol Type	16 bits	Specfies the type of high level protocol to get
Hardware Length	16 bits	Indicates the length of the hardware address
Protocol Length	16 bits	Indicates the length of the protocol address
Operation Code	16 bits	Specifies the ARP/RARP operation (request or reply) to perform
Sender Hardware Address	48 bits	Identifies the sender's hardware address
Sender Protocol Address	32 bits	Identifies the sender's IP address
Target Hardware Address	48 bits	Place for the target hardware address to be stored (contains zeros in ARP request)
Target Protocol Address	32 bits	Identifies the target computer IP address

ARP and RARP:
Using ARP and RARP



ARP and RARP:
ARP Help Messages



ARP and RARP:
ARP Output

```
C:\WINDOWS>arp -a

Interface: 24.24.78.84 on Interface 0x1000002
Internet Address      Physical Address      Type
24.24.78.1            08-00-3e-02-07-8d     dynamic

ARP table may contain several entries:
Interface: 192.168.1.112 on Interface 0x2000003
Internet Address      Physical Address      Type
192.168.1.1           00-20-78-c6-78-14     dynamic
192.168.1.101         00-03-47-8f-15-f5     dynamic
192.168.1.102         00-03-47-8f-05-7a     dynamic
192.168.1.103         00-d0-b7-b5-12-24     dynamic

Another possible output from ARP:
C:\WINDOWS\arp -a
No ARP Entries Found
```

DNS

- Domain Name System
- Each component on the network has a unique IP address
- A host name can be associated with an IP address

DHCP

- Dynamic Host Configuration Protocol
- Protocol for dynamically assigning IP addresses to devices on a network
- Happen during the bootstrap process
- Device may be assigned a different IP address each time it connects to a network

DHCP:
Operation and Properties

Operation of DHCP:

1. The DHCP client sends a DHCPDISCOVER broadcast message at boot time.
2. The DHCP server offers an IP address to the client (DHCPOFFER).
3. The client notifies the server of its request to use the offered address (DHCPREQUEST).
4. The server acknowledges the client's request (DHCPACK).

Additional properties of DHCP:

- Carried by UDP datagrams
- Based on earlier BOOTP protocol
- Found in RFCs 1533, 1534, 1541, and 1542
- DHCP client support is built into most operating systems including Windows, UNIX/Linux, and many others.
- DHCP server support is provided by Windows NT Server, UNIX/Linux, and other mainframe operating systems. Refer to Chapter 18 for additional information about running a DHCP server on Windows NT.

ICMP

- Internet Control Message Protocol
- Error message may or may not be returned to the sender due to the use of the use of the UDP as the transport protocol

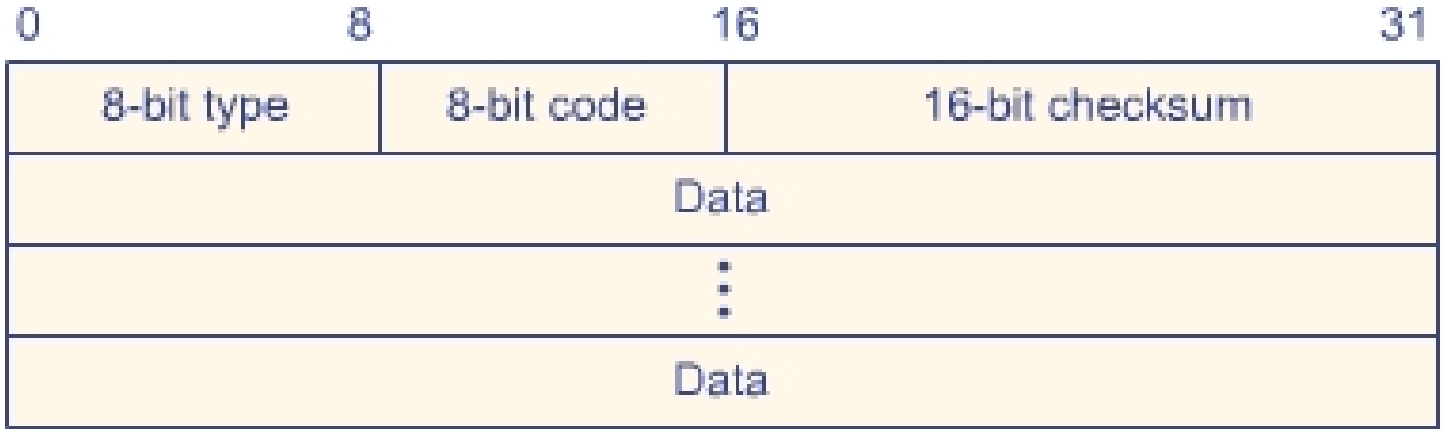
SMTP

- Simple Mail Transport Protocol
- Responsible for routing e-mail on the Internet using TCP and IP

SNMP

- Simple Network Management Protocol
- Defines the format and meaning of messages exchanged
- Used by the network manager to interrogate network devices to determine their status and retrieve stats

ICMP, SMTP, and SNMP:
ICMP Message Format



ICMP, SMTP, and SNMP:
ICMP Header Field Information (1)

Type	Code	Description	Query	Error
0	0	Echo reply	✓	
3		Destination unreachable		✓
	0	network unreachable		✓
	1	host unreachable		✓
	2	protocol unreachable		✓
	3	port unreachable		✓
	4	port unreachable		✓
	5	fragmentation needed but don't fragment bit set		✓
	6	source route failed		✓
	7	destination host unknown		✓
	8	source host isolated (obsolete)		✓
	9	destination network administratively prohibited		✓
	10	destination host administratively prohibited		✓
	11	network unreachable for TOS		✓
	12	host unreachable for TOS		✓
	13	communication administratively prohibited by filtering		✓
	14	host precedence violation		✓
	15	precedence cutoff in effect		✓
4	0	Source quench (elementary flow control)		✓

ICMP, SMTP, and SNMP:
ICMP Header Field Information (2)

Type	Code	Description	Query	Error
5		Redirect		
	0	redirect for network		✓
	1	redirect for host		✓
	2	redirect for type-of-service and network		✓
	3	redirect for type-of-service and host		✓
8	0	Echo request	✓	
9	0	Router advertisement	✓	
10	0	Router solicitation	✓	
11		Time exceeded		
	0	time to live equals 0 during transit (trace route)		✓
	1	time to live equals 0 during assembly		✓
12		Parameter problem		
	0	IP header bad (catchall error)		✓
	1	required option missing		✓
13		Timestamp request	✓	
14		Timestamp reply	✓	
15		Information request (obsolete)	✓	
16		Information reply (obsolete)	✓	
17		Address mask request	✓	
18		Address mask reply	✓	

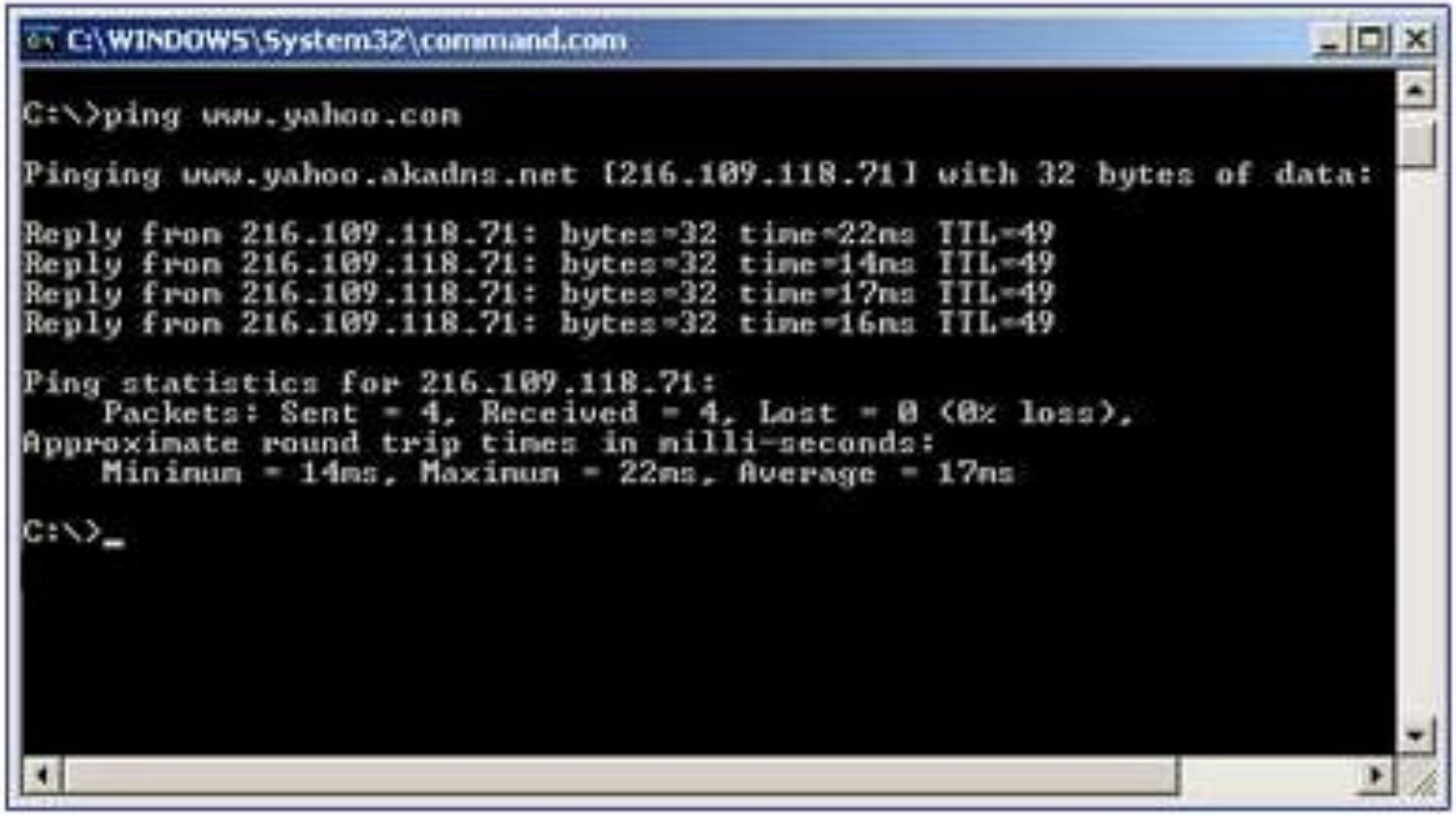
HTTP

- HyperText Transport Protocol
- Used to transfer multimedia information over the Internet
- Carried via TCP not UDP

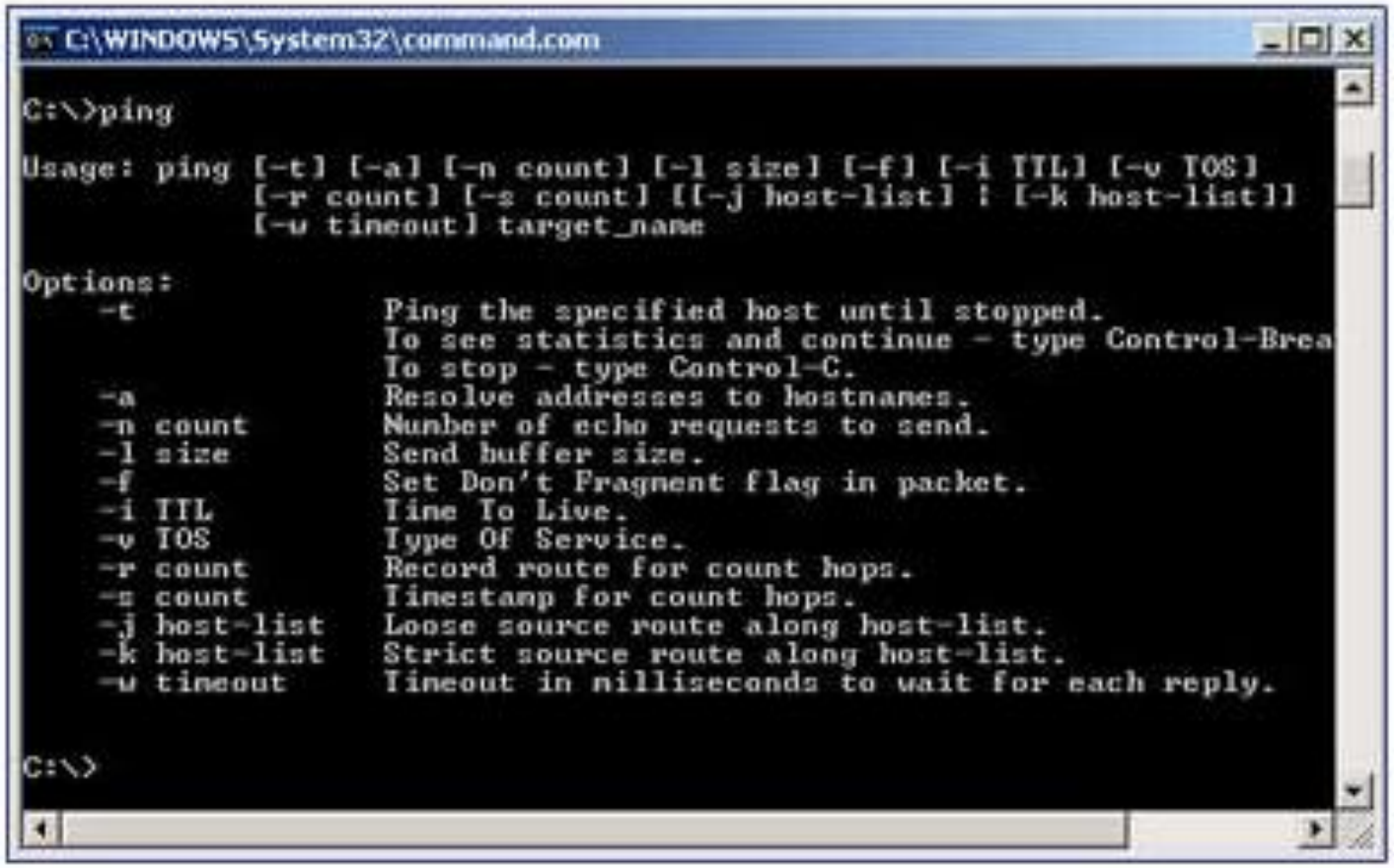
HTTPS

- HyperText Transfer Protocol over Secure Socket Layer
- Used to exchange encrypted web pages between a client/server connection
- Used port 443
- Default secure socket layer uses a 40-bit key but a higher-strength 128-bit key version is available (and used for most sites and browsers)

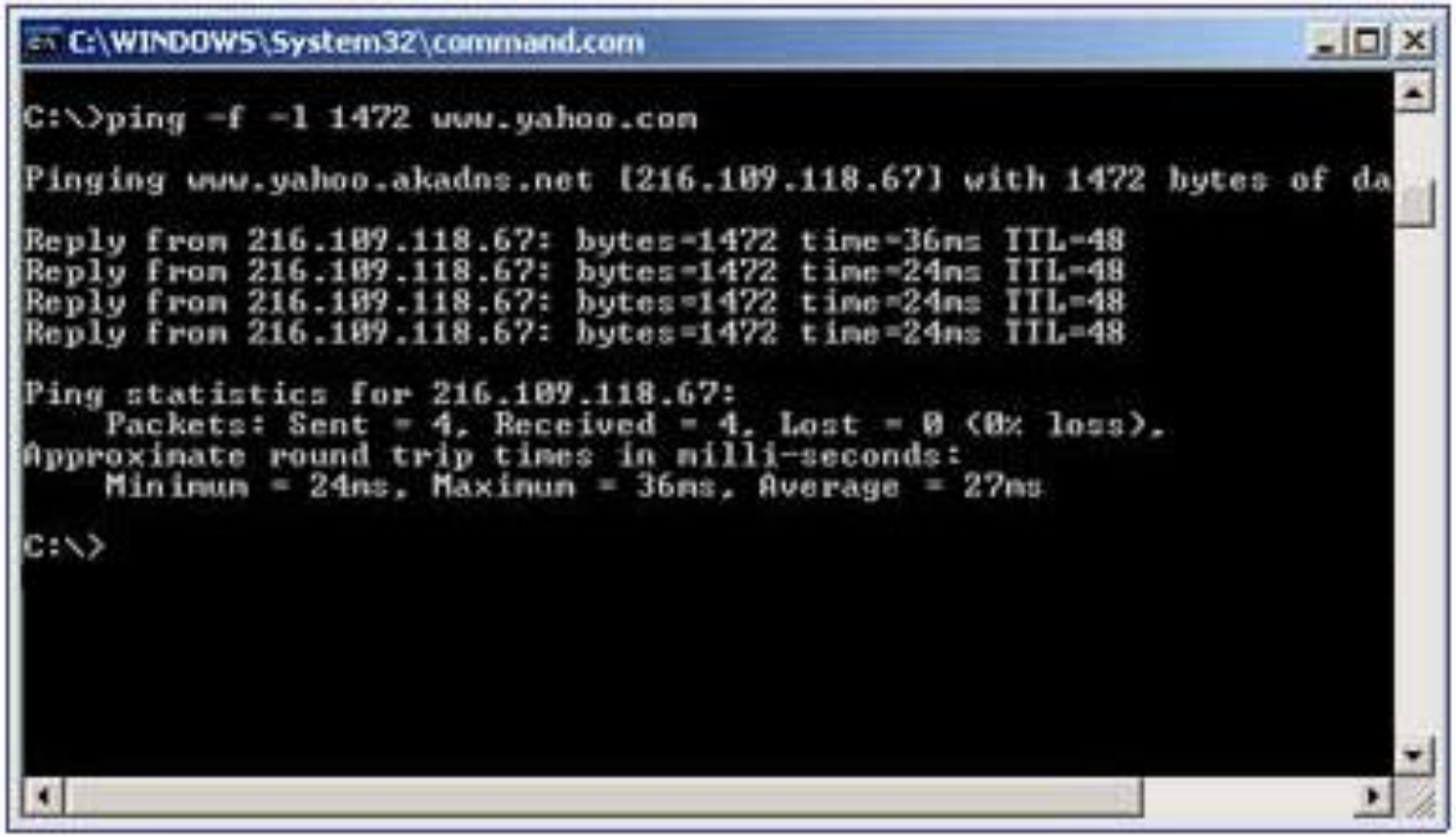
PING and Tracert:
Example 1



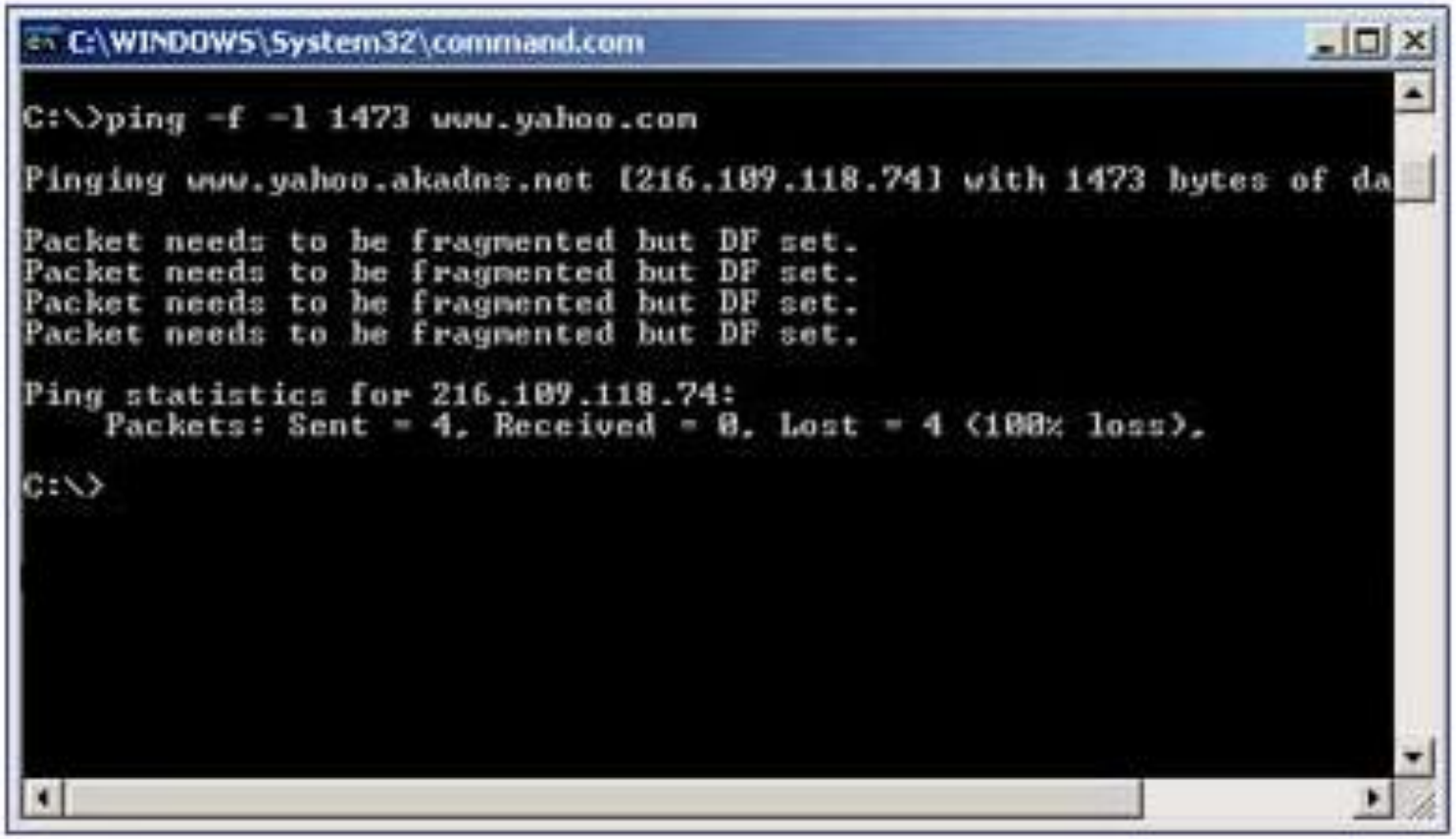
PING and Tracert:
Example 2



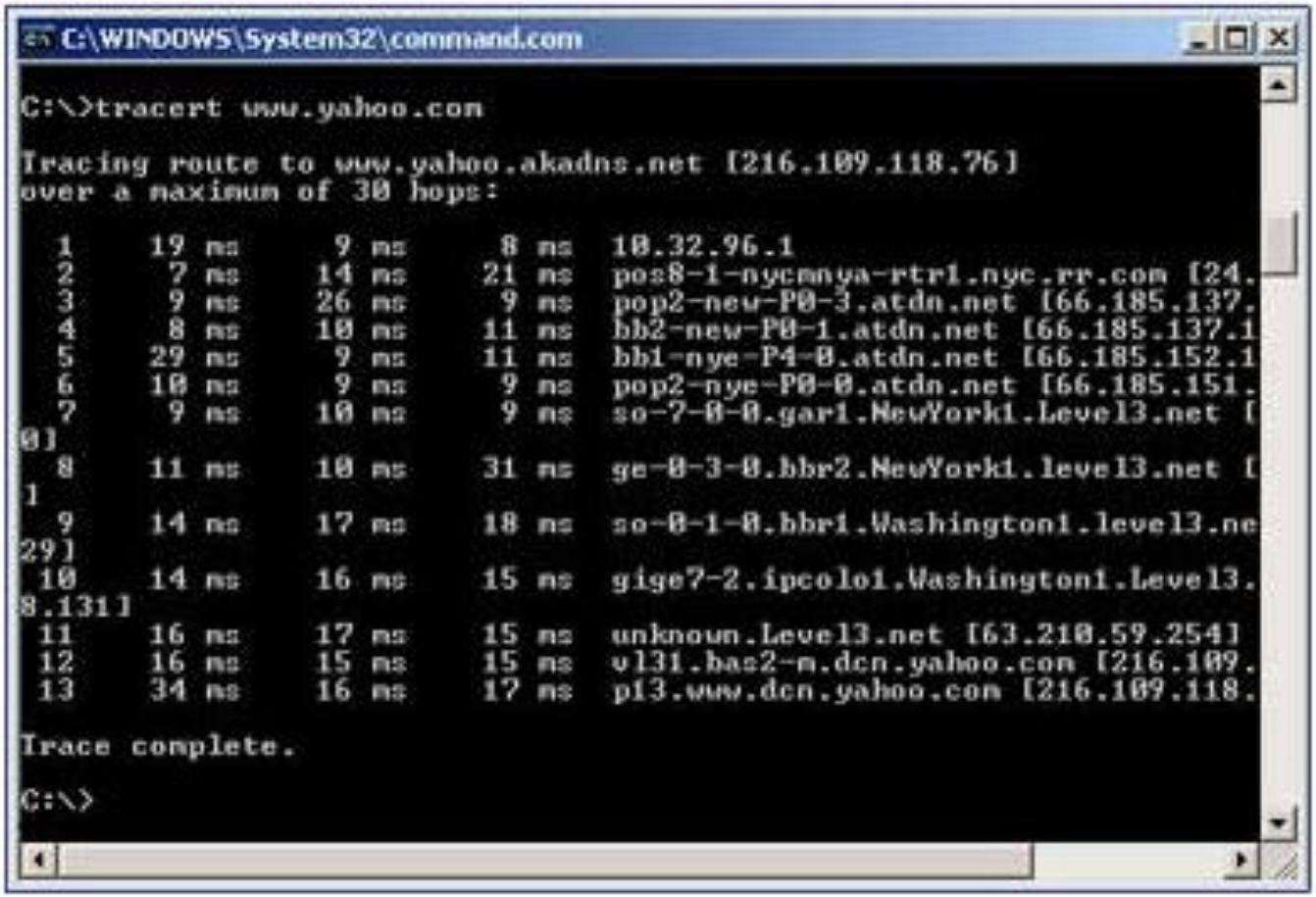
PING and Tracert:
Example 3



PING and Tracert:
Example 4

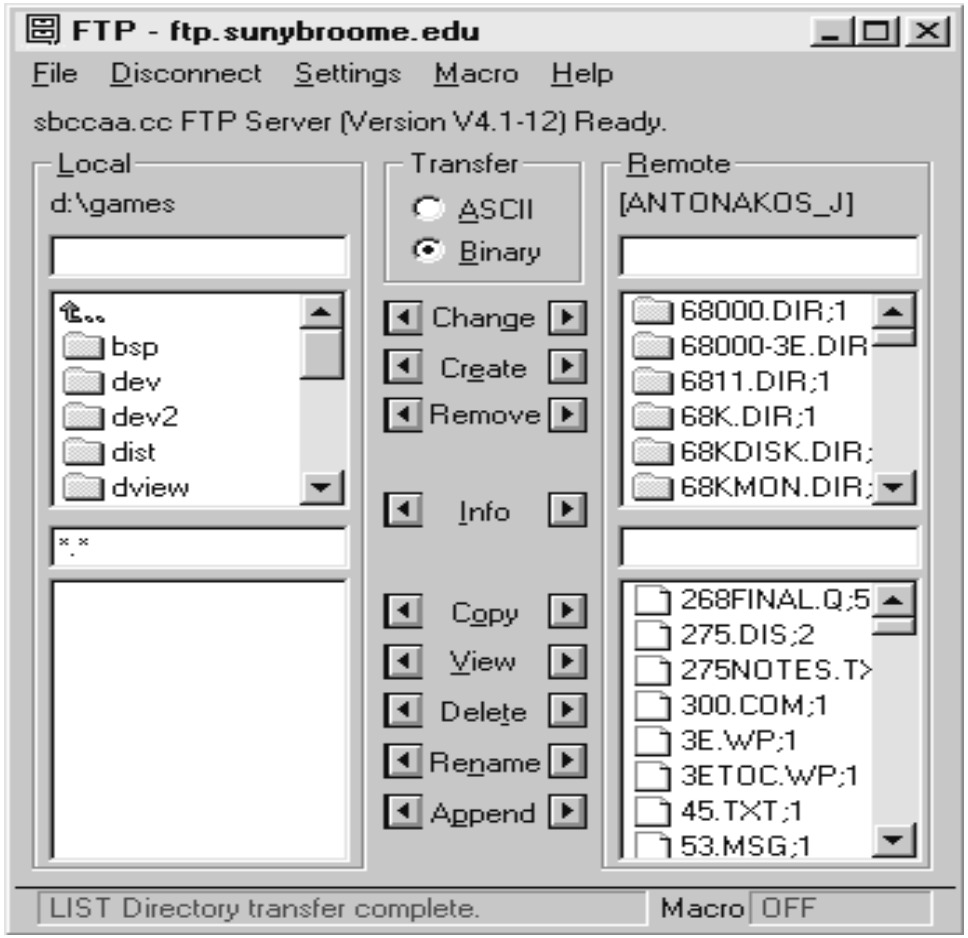


PING and Tracert:
Example 5

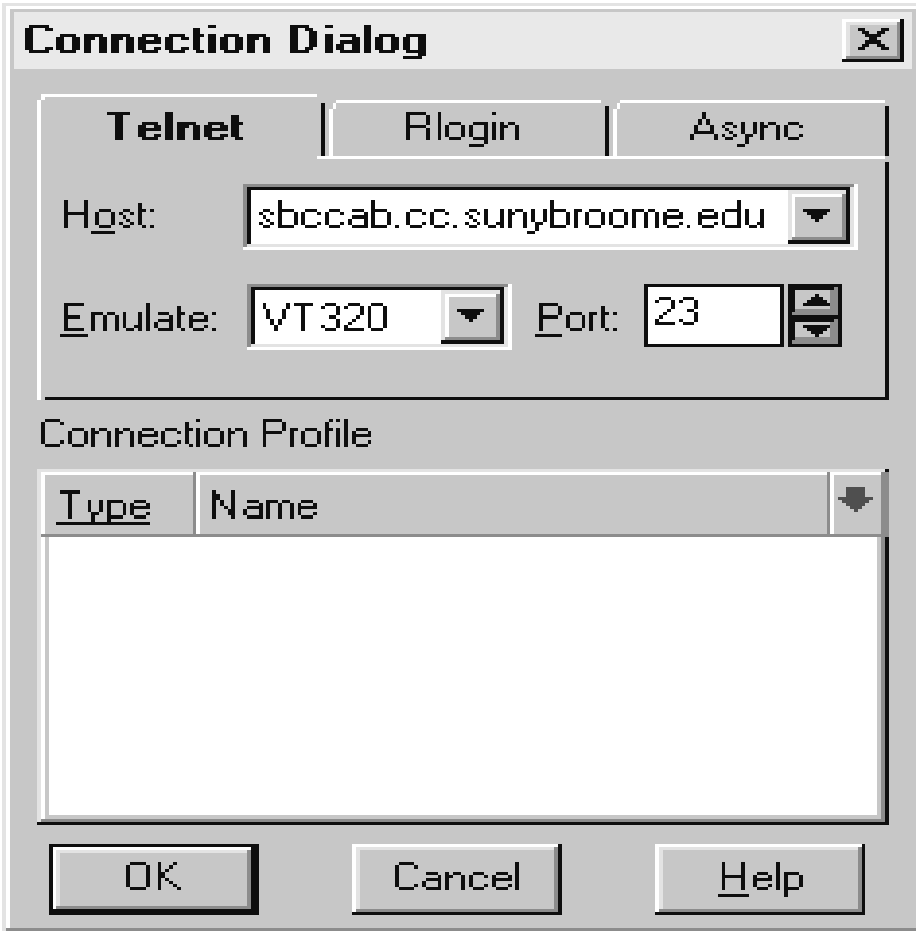


PING and Tracert:
Example 6

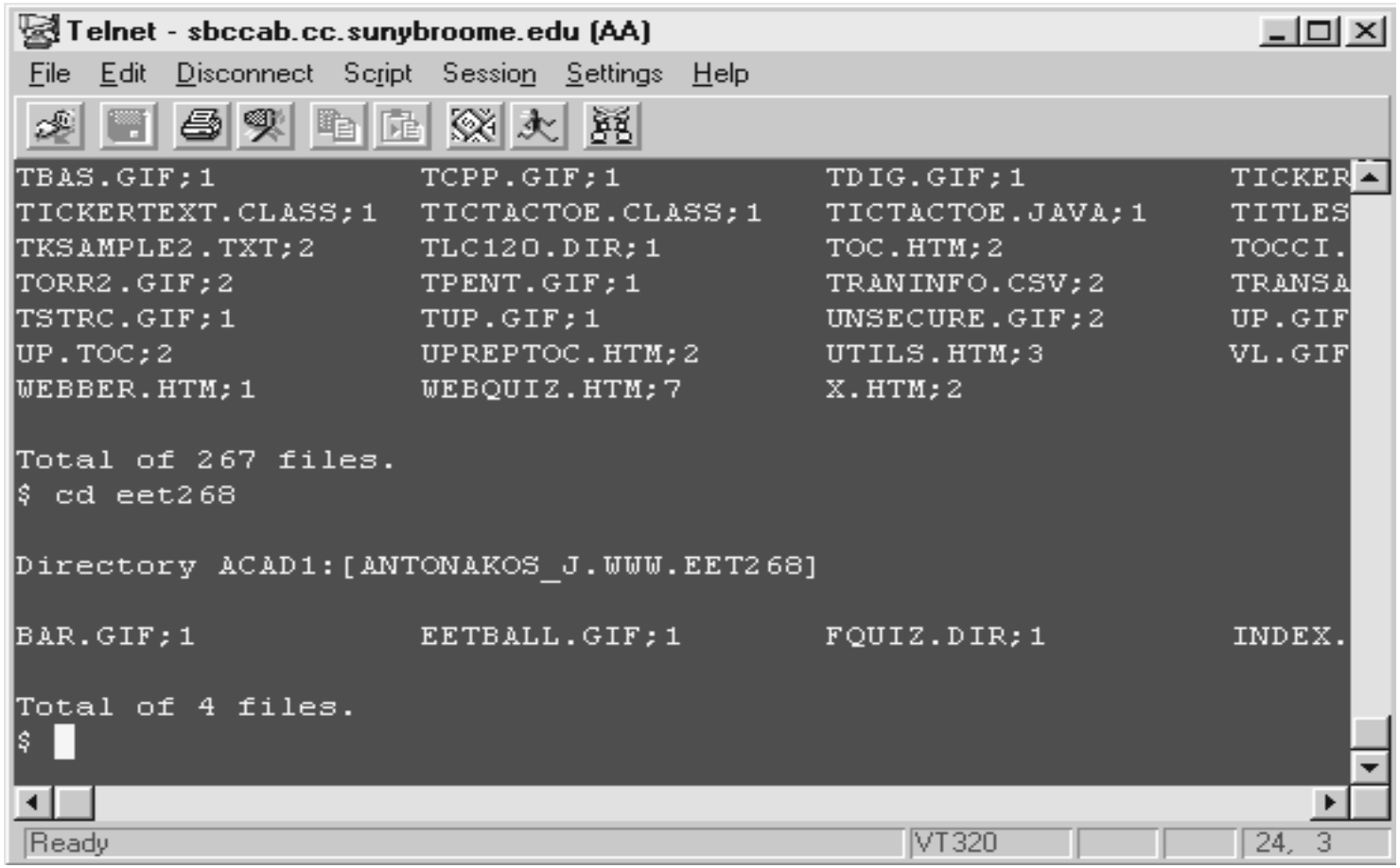
FTP and Telnet:
Example 1



FTP and Telnet:
Example 2



FTP and Telnet:
Example 3



FTP and Telnet:
IPv6 Address Example

F300:2AC9:0000:0000:0000:00C0:F027:64E2

Each 4-digit hexadecimal group represents 16 bits of binary addressing information.

FTP and Telnet:
Subnetting in IPv6

F300:0000:0000:0000:00C0:F0FF:FE27:64E2/48

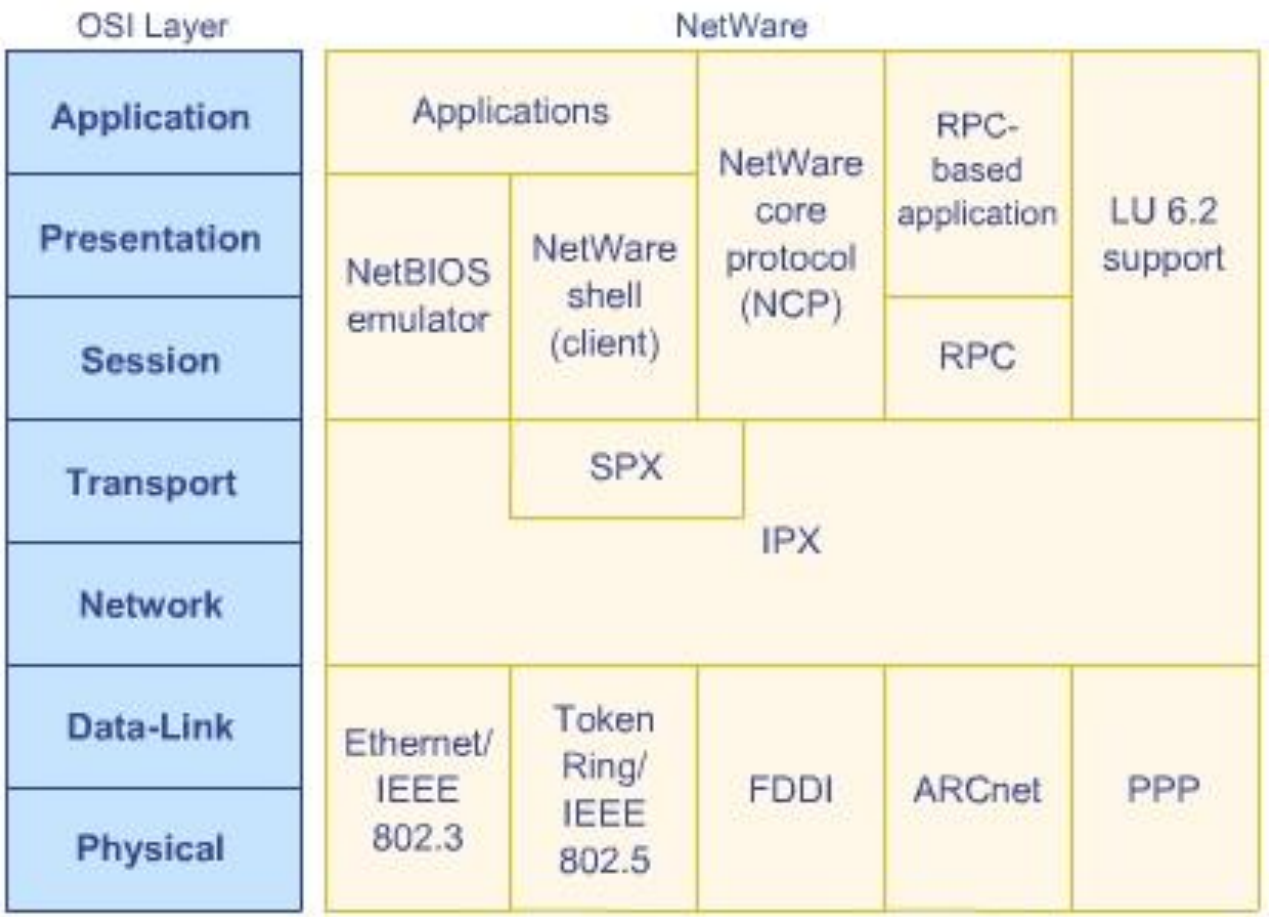
(or F300::00C0:F0FF:FE27:64E2/48)

FTP and Telnet:
Shorthand Technique for an IPv6 Address

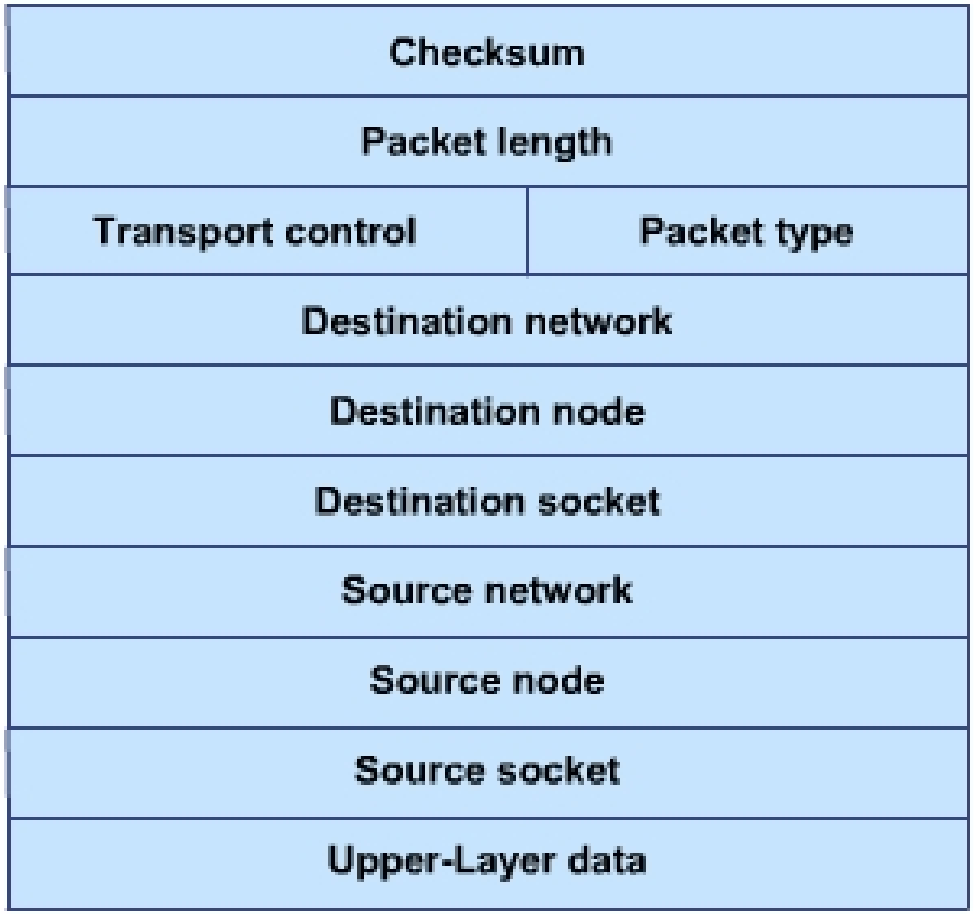
F300:2AC9::00C0:F027:64E2

The address indicates that 48 bits are used for the network address (leaving 64 bits for the host address and 16 bits for additional subnetting).

IPX /SPX:
NetWare Protocol Suite



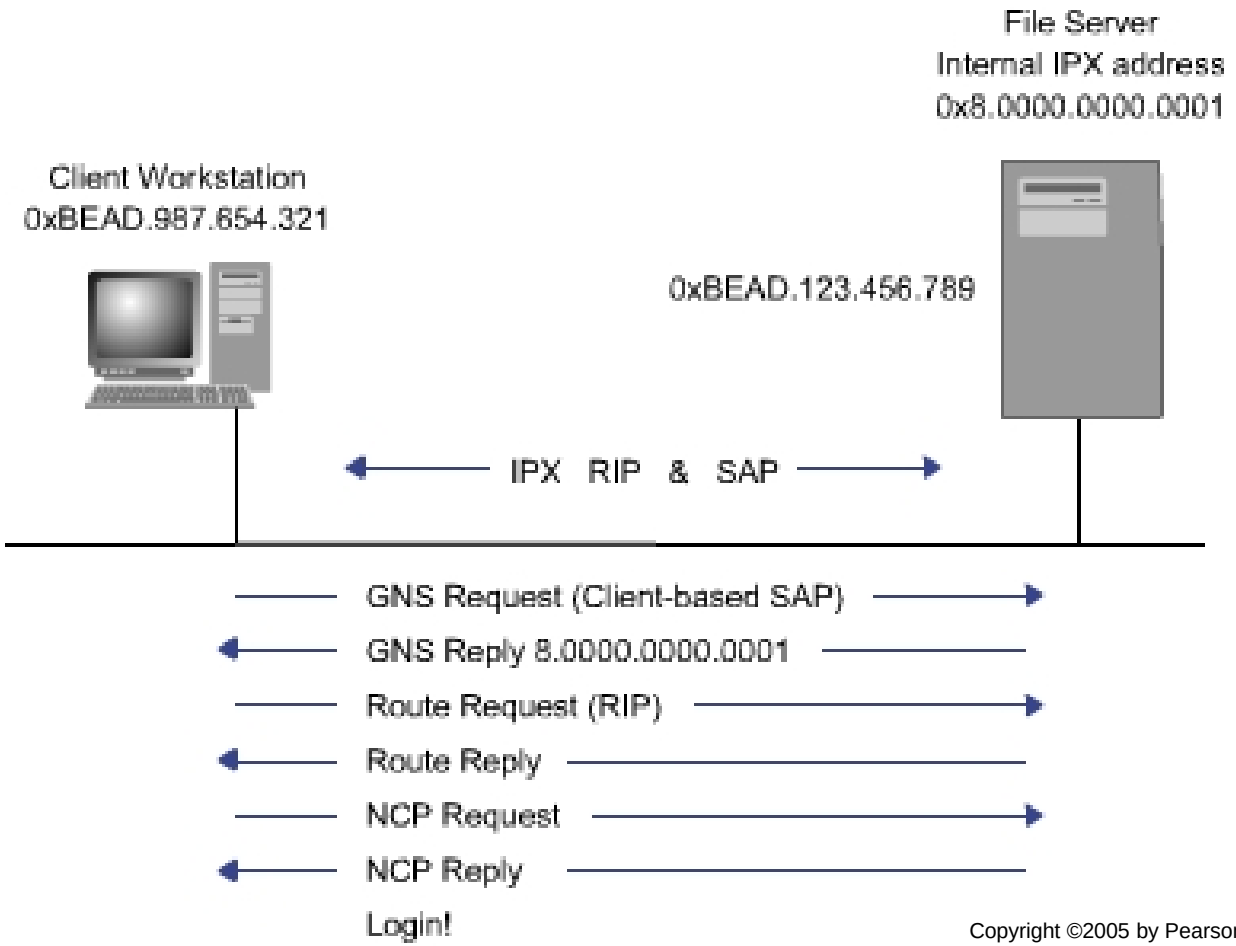
IPX:
IPX Packet Structure



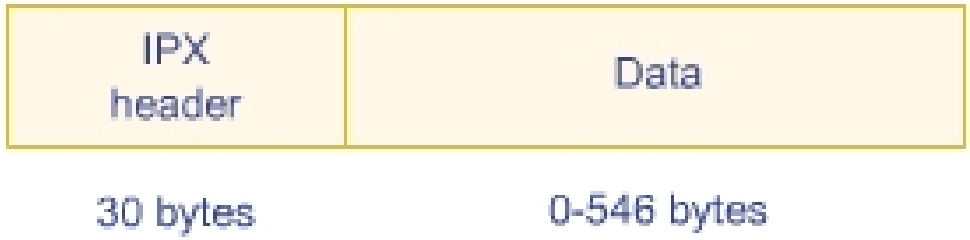
IPX:
IPX Packet Types

Packet Type Value	Protocol
0	Unknown
1	RIP
2	Echo packet
3	Error packet
4	PEP
5	SPX
17	NCP

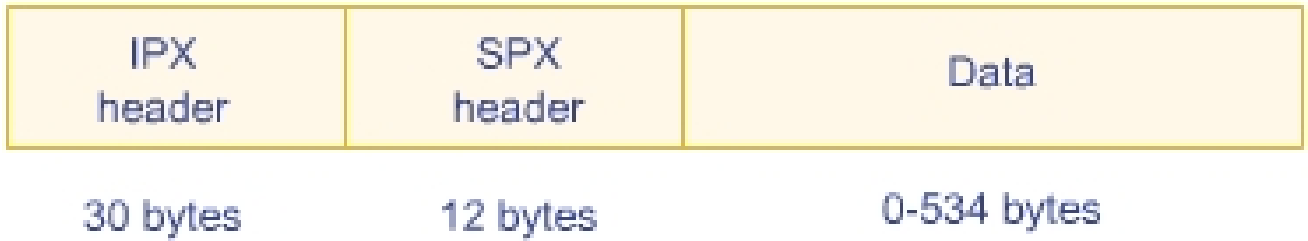
NCP



SPX:
Different Types of IPX Packets

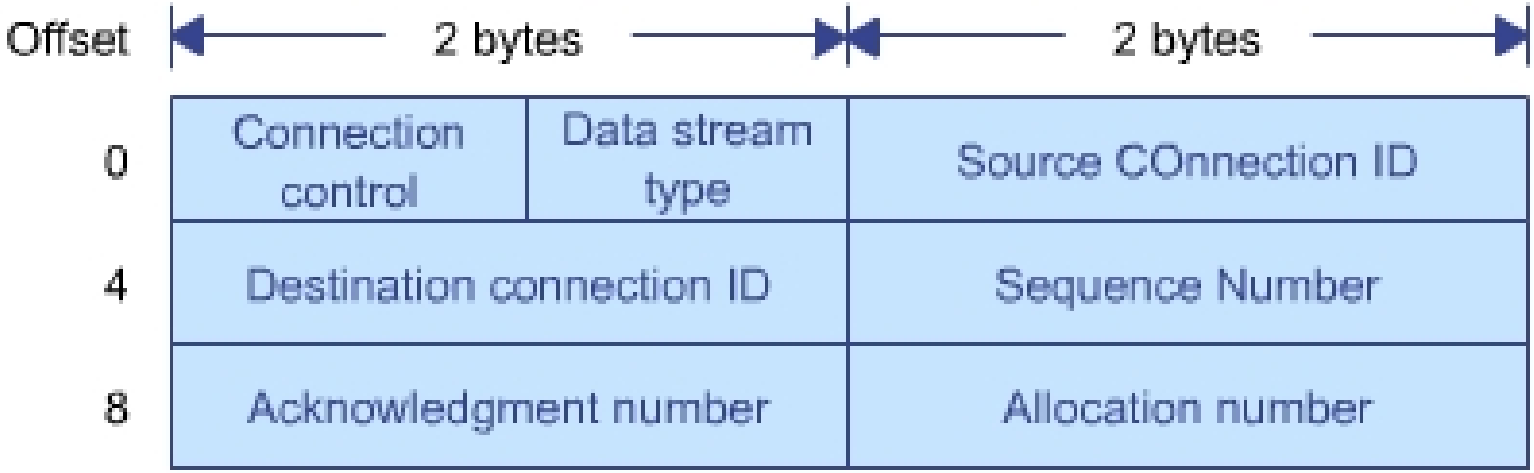


(A) IPX Packet transporting some data



(B) Connection oriented SPX packet transporting data

SPX:
SPX Header



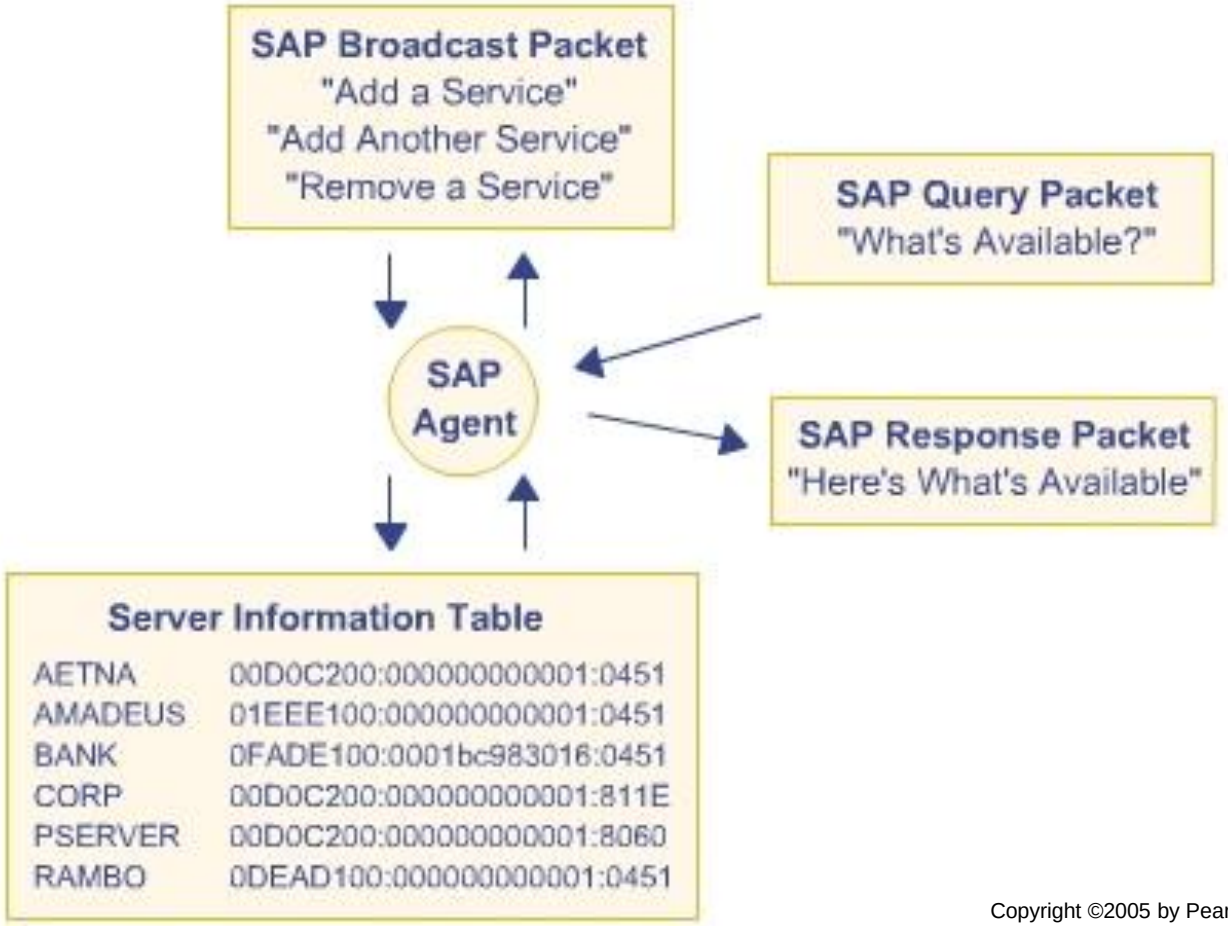
SPX:
Connection Control Flag Values

Connection Control Flag	Meaning
10H (bit 4)	Last packet in message
20H (bit 5)	Attention
40 H (bit 6)	Acknowledgment
80H (bit 7)	System packet

SPX:
Data Stream Type Values

Data Stream Type	Meaning
0-253	Ignored by SPX
254	End of connection
255	End of connection Ack

SAP – Service Advertising Protocol



AppleTalk

- Suite of protocol developed for Macintosh computers
- Uses connectionless (DDP) and connection-oriented (ADSP)
- File sharing is accomplished using AFP