



Course Code: GCS-II08



Global CyberSoft

Network Fundamental

By : Trung Le Tran
Date : Aug, 2005
Duration: 3 hours
Revision: 1.0



Global CyberSoft

Course Outline

- [Network Introduction](#)
- [OSI Model](#)
- [LAN Protocols](#)
- [LAN Switching](#)
- [TCP/IP Protocol Suite](#)
- [Networking with TCP/IP: address, subnet, protocols](#)
- [Upper layer protocols](#)
- [TCP Utilities](#)
- [Routing Basic: static routing, dynamic routing. Routing protocol](#)
- [Broadcast and Multicast](#)
- [Network Address Translation](#)
- [IPv6 and ICMPv6](#)



Introduction

● Contents:

- Network
- Type of network
- Internetwork

● What is network?

- A group of computers and other devices that are connected by some type of transmission media, usually wire or cable.
- Networks enable multiple users to share devices and data, that are referred to as the network's resource.
- Type of network: peer-to-peer network, server-based network.

Introduction

● Elements common to all server-based network

- Client
- Server
- Workstation
- Network interface card (NIC)
- Network operating system (NOS)
- Host
- Node
- Topology
- Protocol
- Data packets
- Addressing
- Transmission media

Introduction

What is Internetwork?

- A collection of individual networks, connected by intermediate networking devices, that functions as a single large network.
- Internetworking refers to the industry, products, and procedures that meet the challenge of creating and administering internetworks

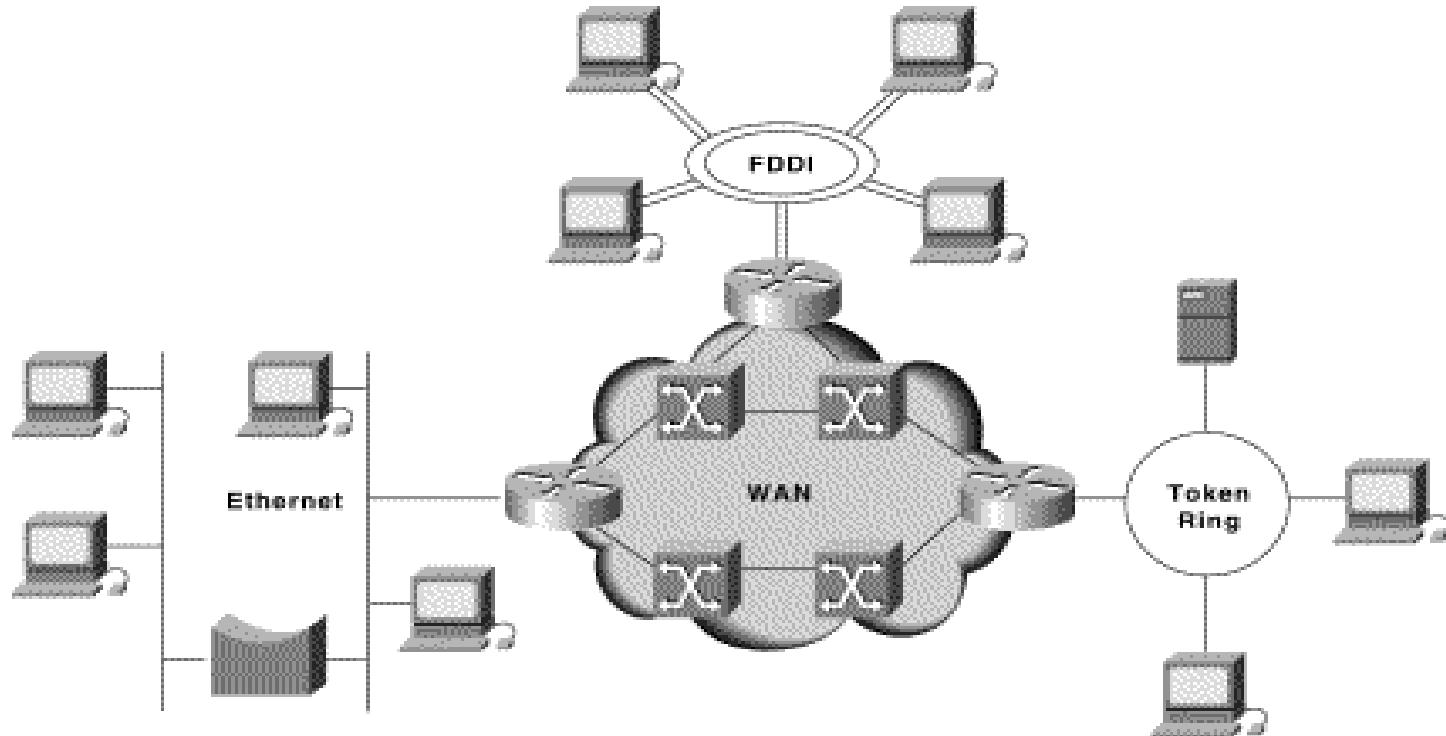


Figure 1-1: Different Network Technologies Can Be Connected to Create an Internetwork



The OSI Model

7 Application

6 Presentation

5 Session

4 Transport

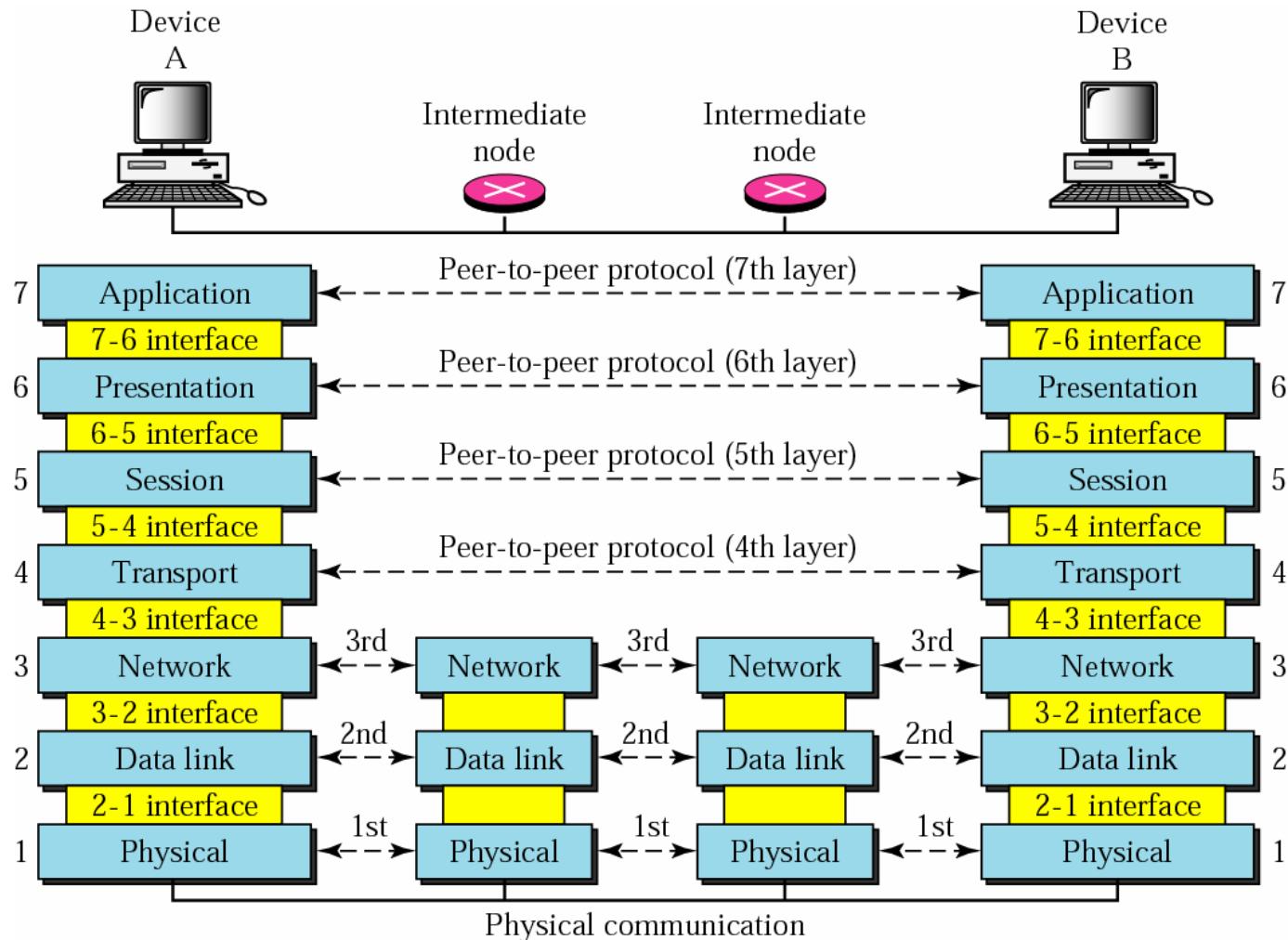
3 Network

2 Data link

1 Physical



The OSI Model





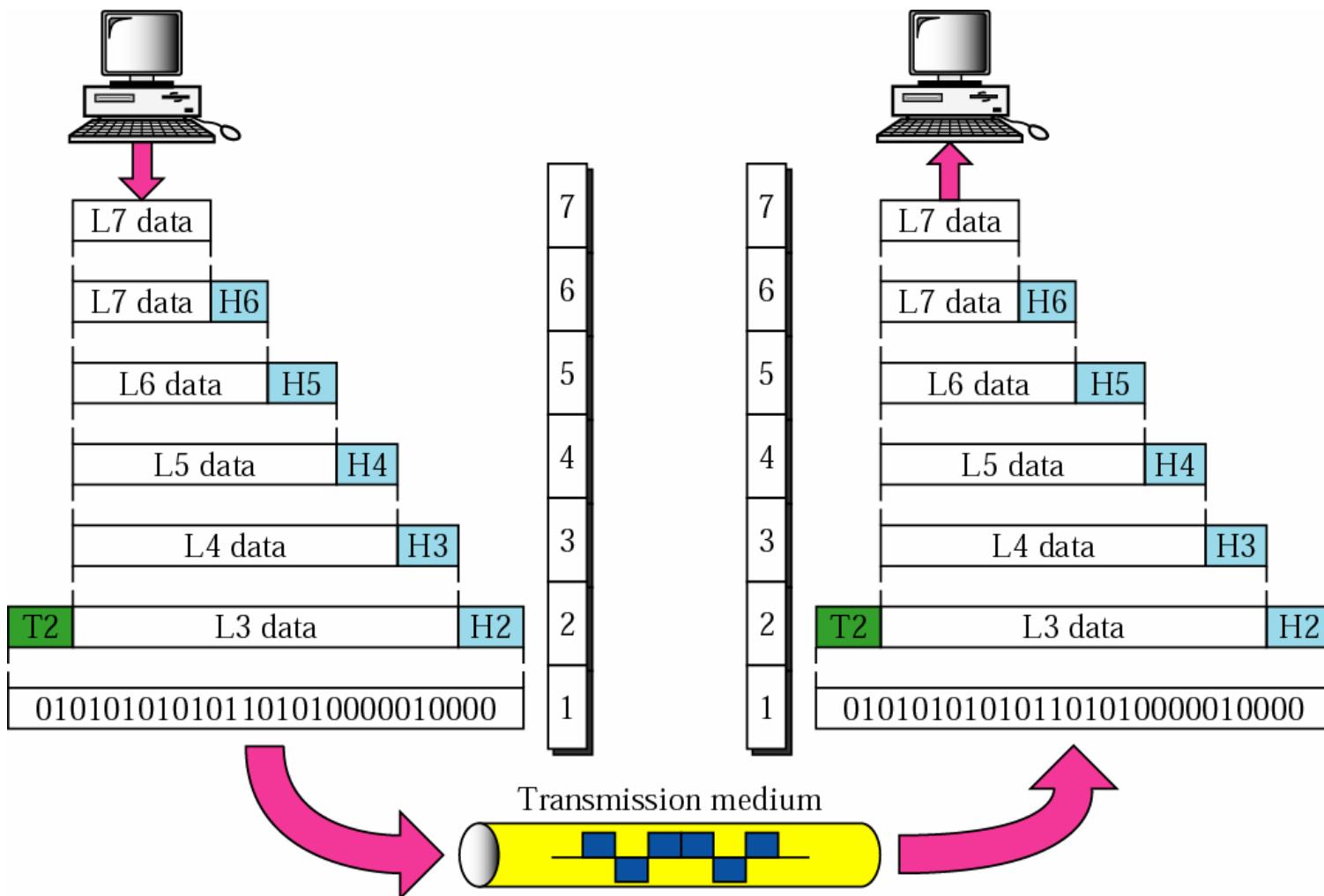
The OSI Model

Note

*Headers are added
to the data at layers
6, 5, 4, 3, and 2.
Trailers are usually
added only at layer 2.*



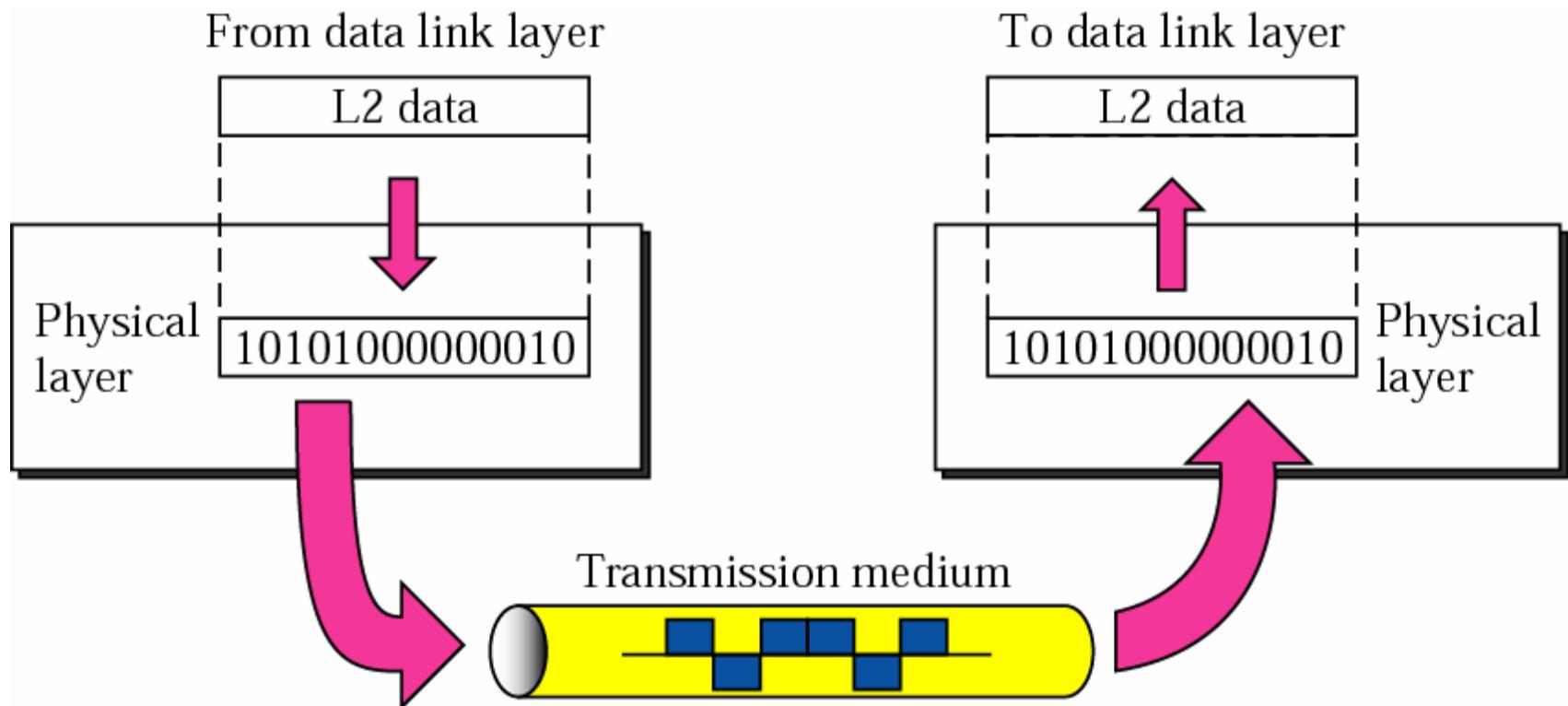
The OSI Model





The OSI Layers

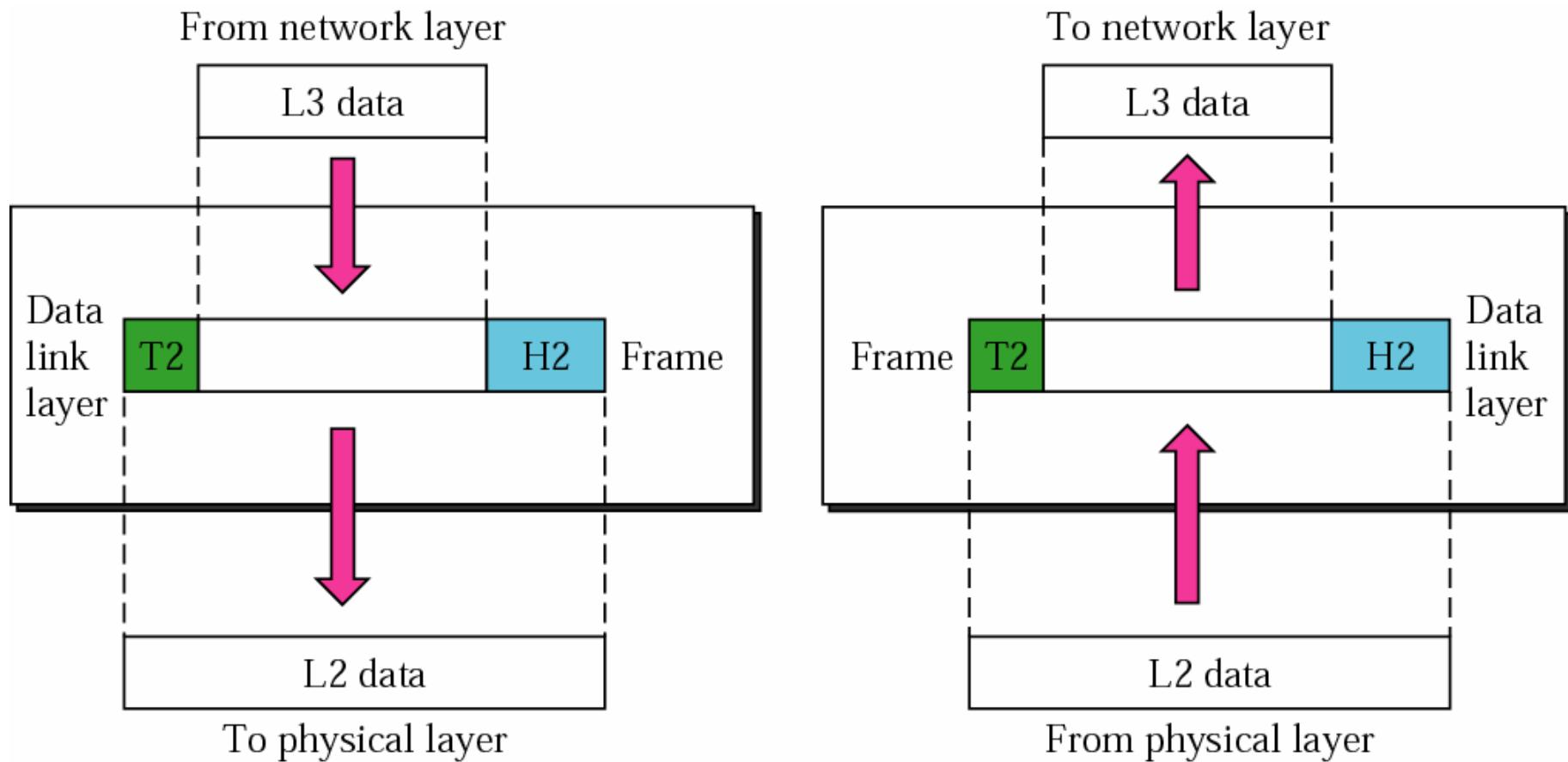
Physical Layer





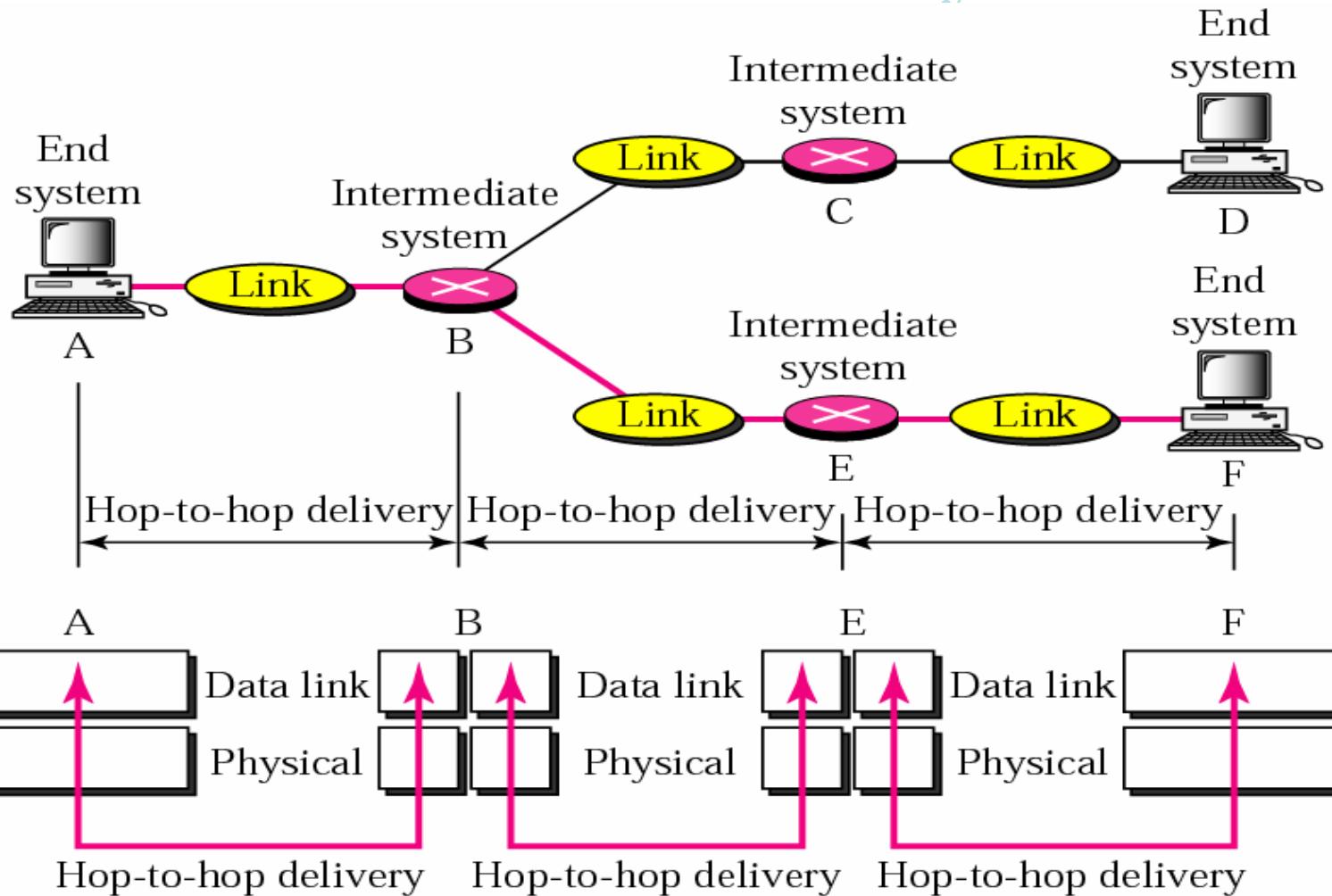
The OSI Layers

Data Link Layer



The OSI Layers

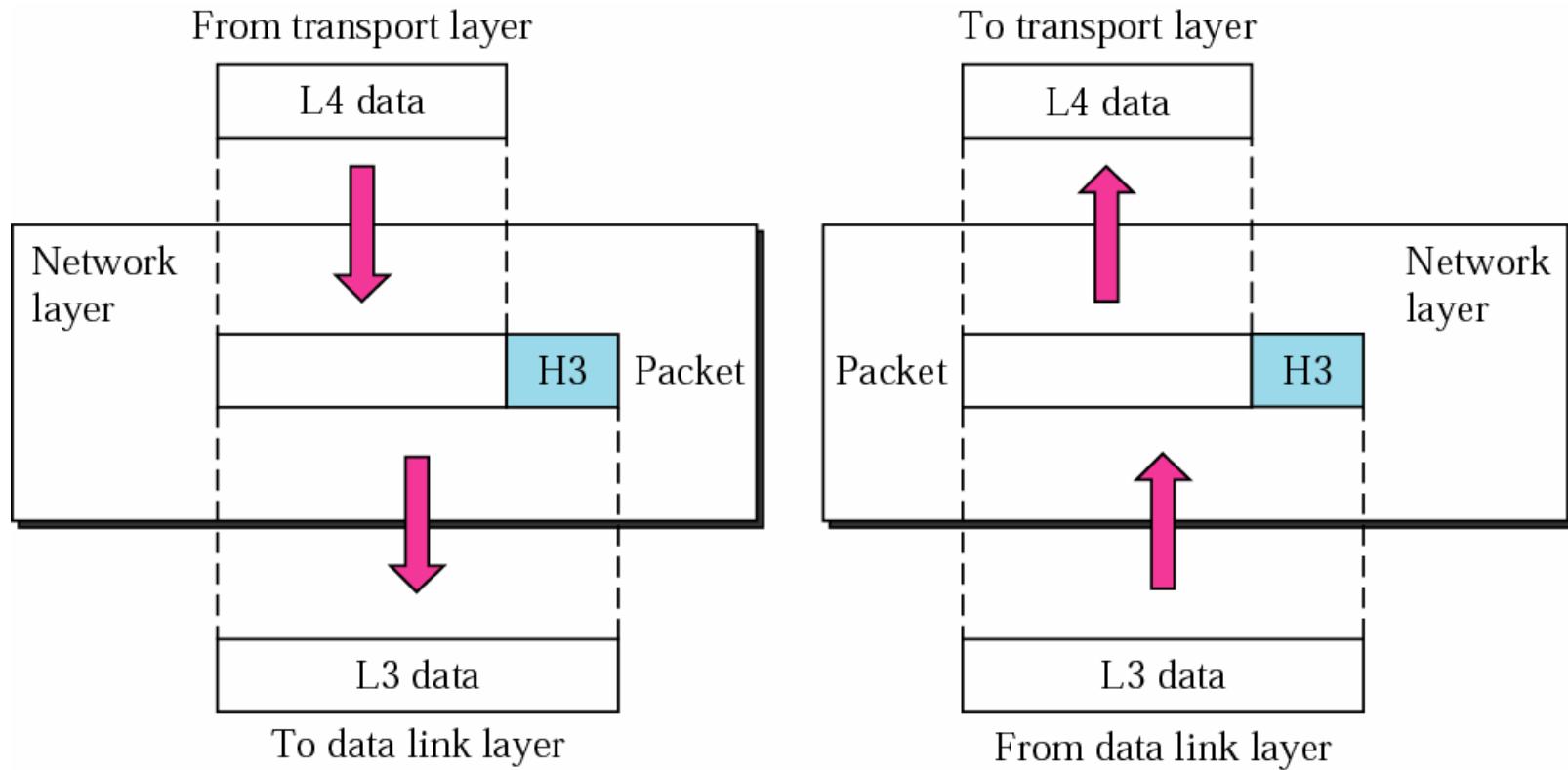
Node-to-node delivery





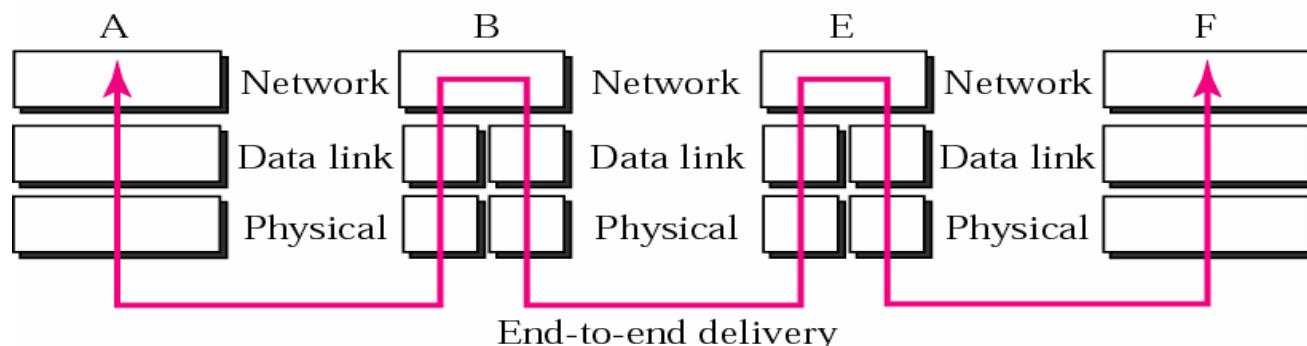
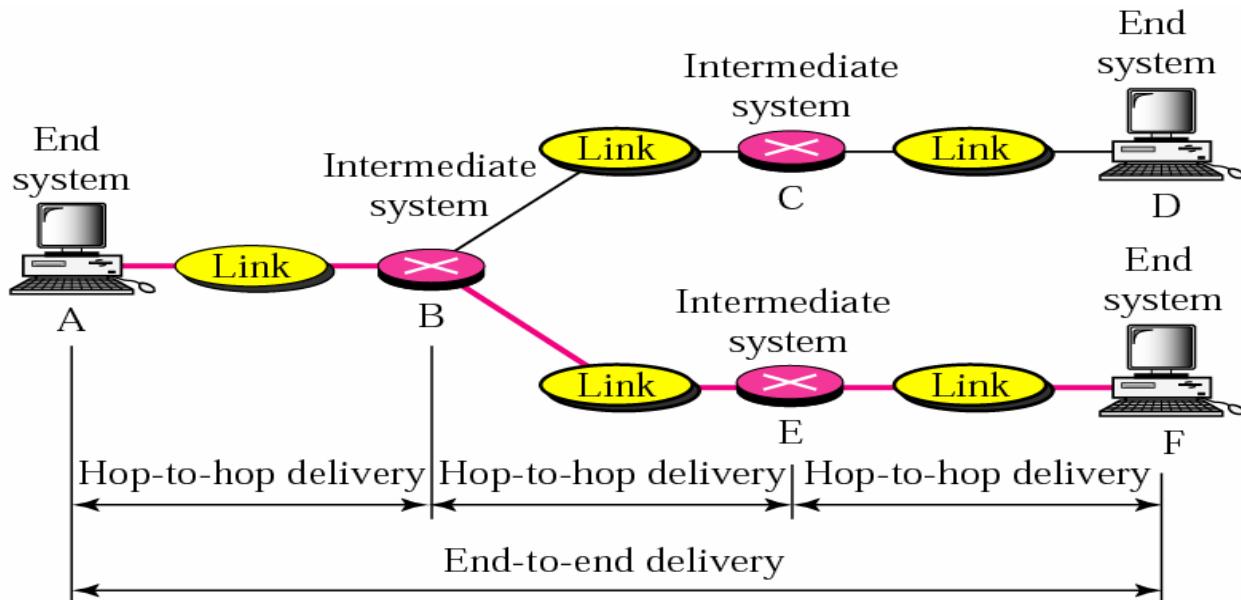
The OSI Layers

Network Layer



The OSI Layers

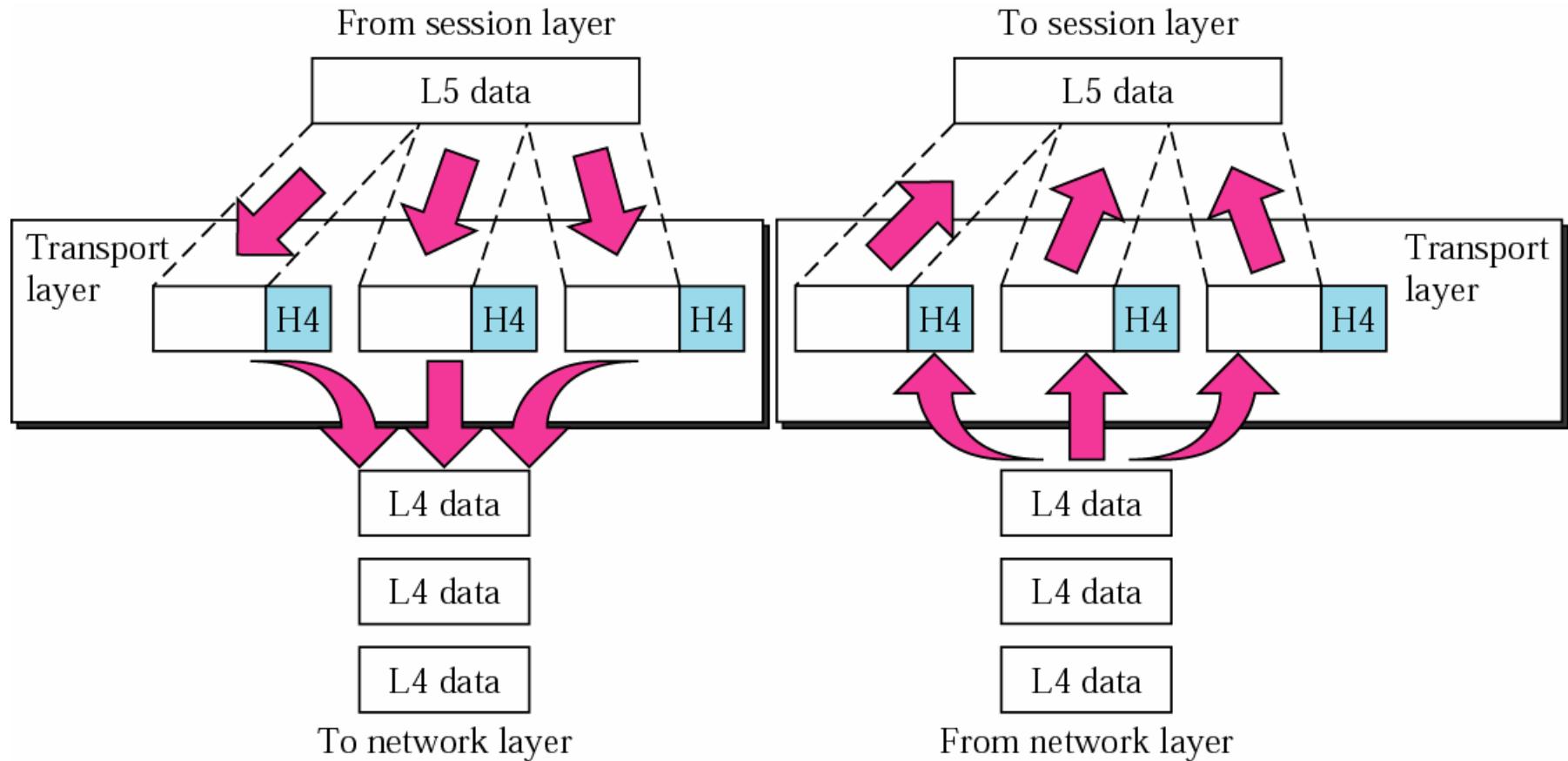
End-to-end delivery



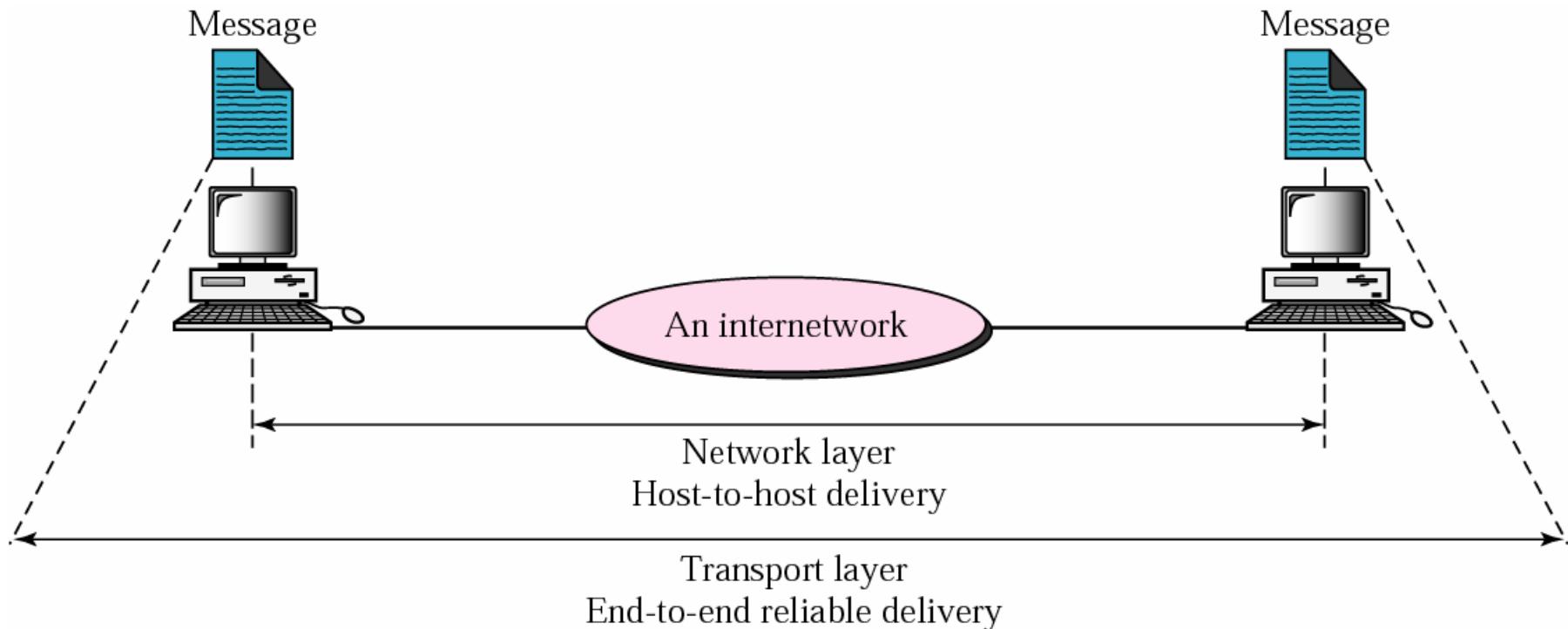


The OSI Layers

Transport Layer



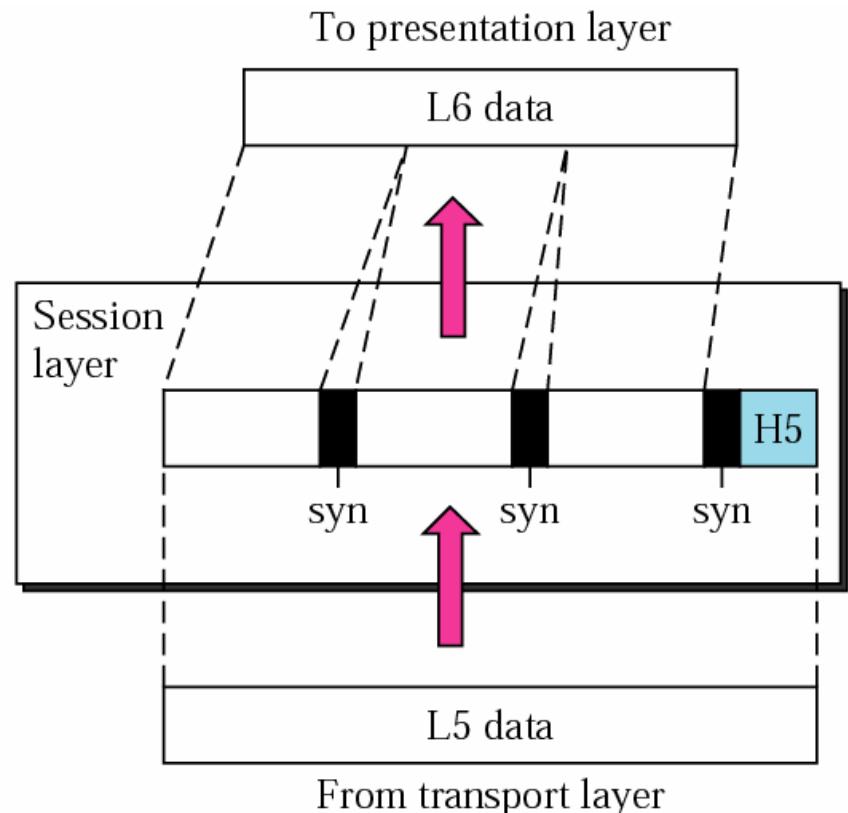
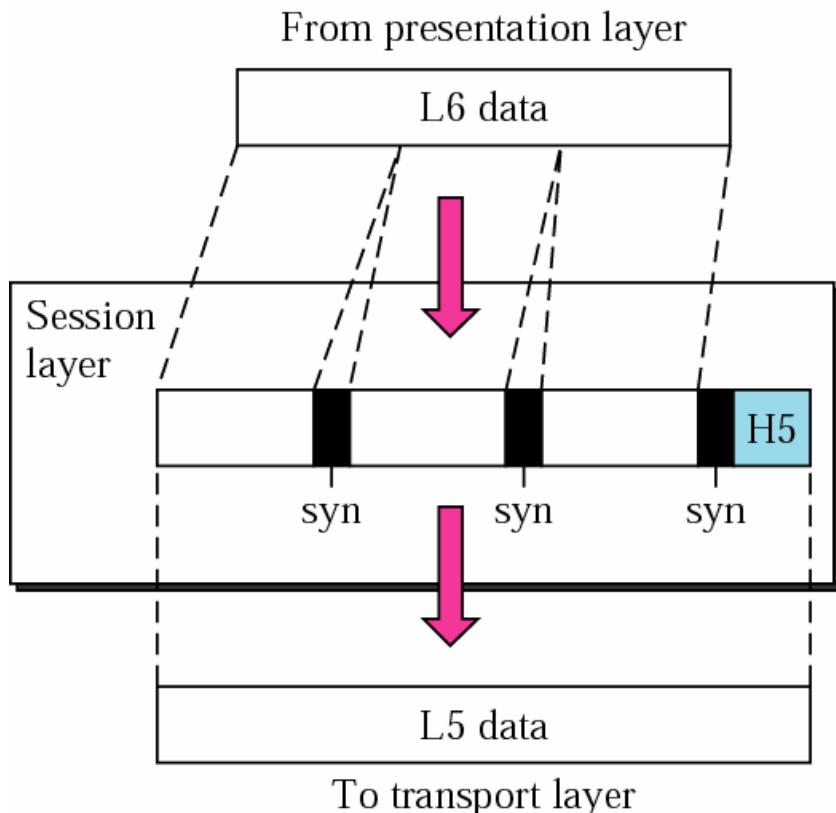
Reliable end-to-end delivery of a message



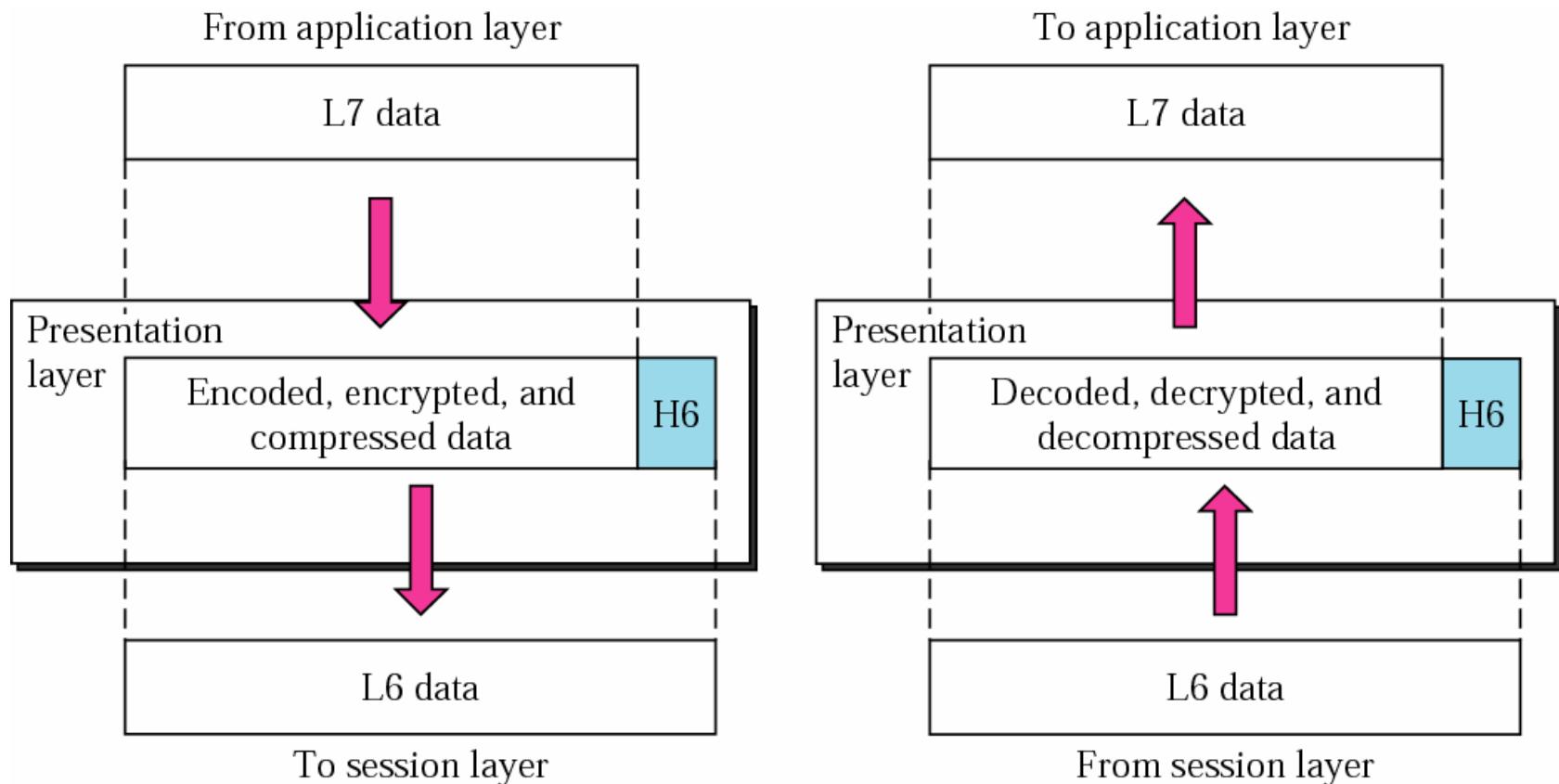


The OSI Layers

Session Layer



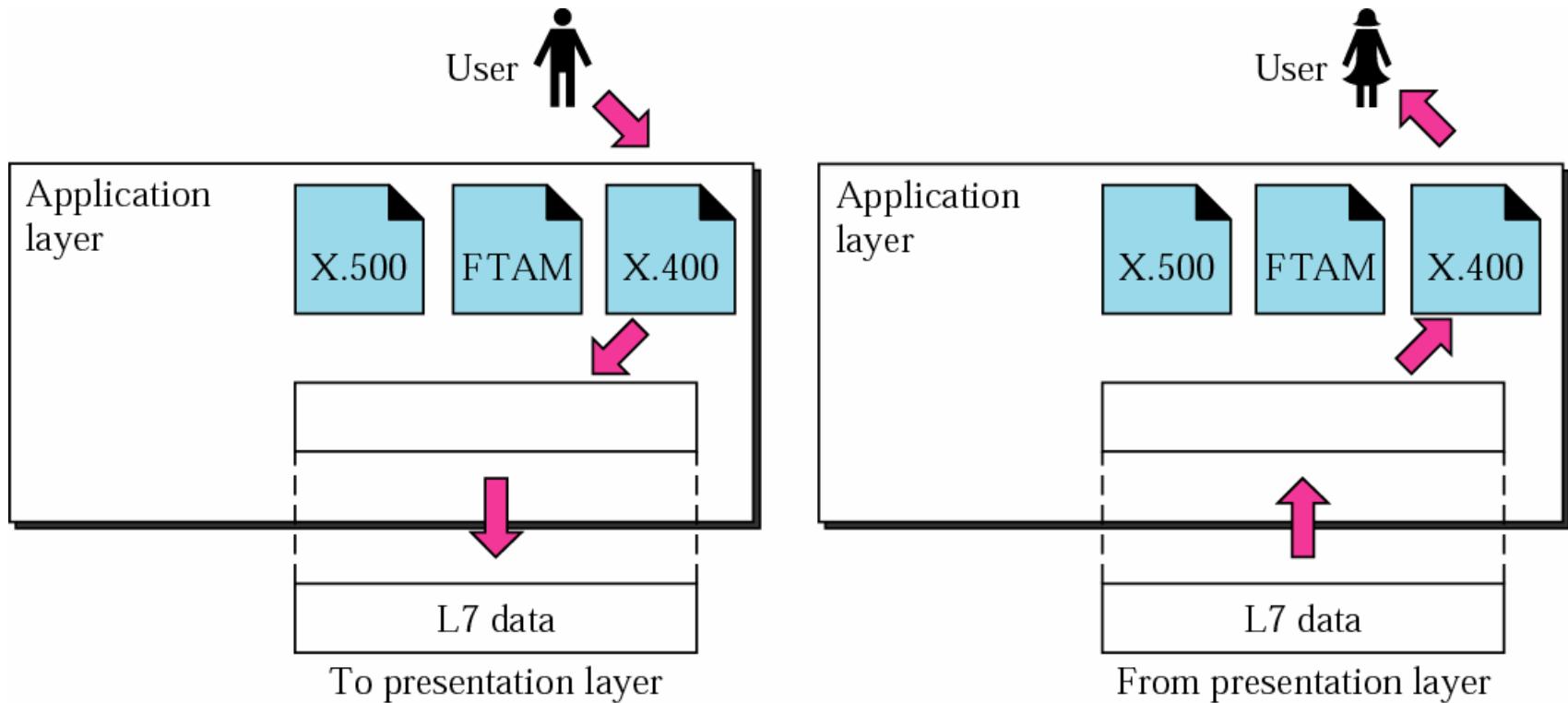
Presentation Layer





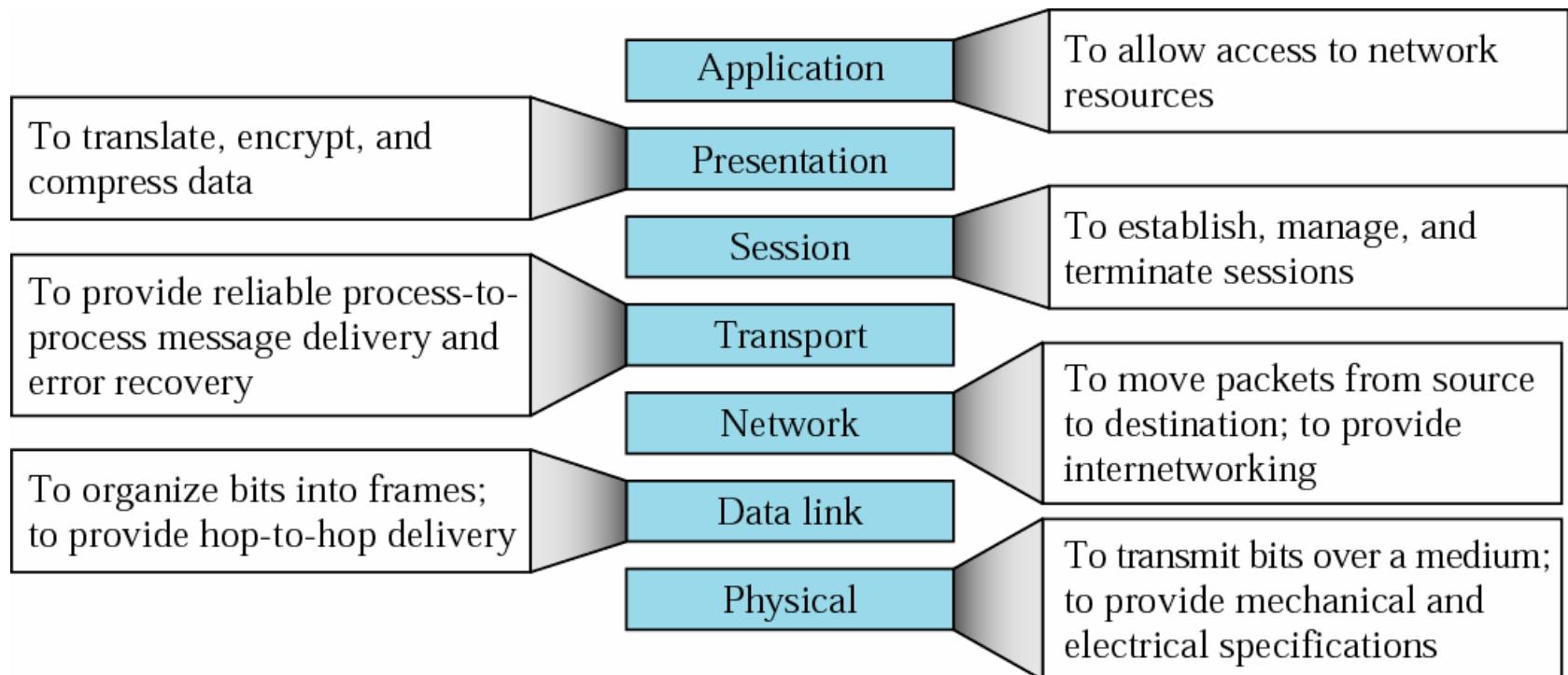
The OSI Layers

Application Layer



The OSI Layers

Summary of layers





Global CyberSoft

LAN Protocols

● Contents:

- What is LAN?
- LAN Protocols and OSI Reference Model
- LAN Transmission Methods
- LAN Topologies
- LAN Devices

What is LAN

- LAN: Local Area Network
- A high-speed data network that covers a relatively small geographic area.
- Typically connects workstations, personal computers, printers, servers, and other devices.
- Offer computer users many advantages, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications.



What is LAN

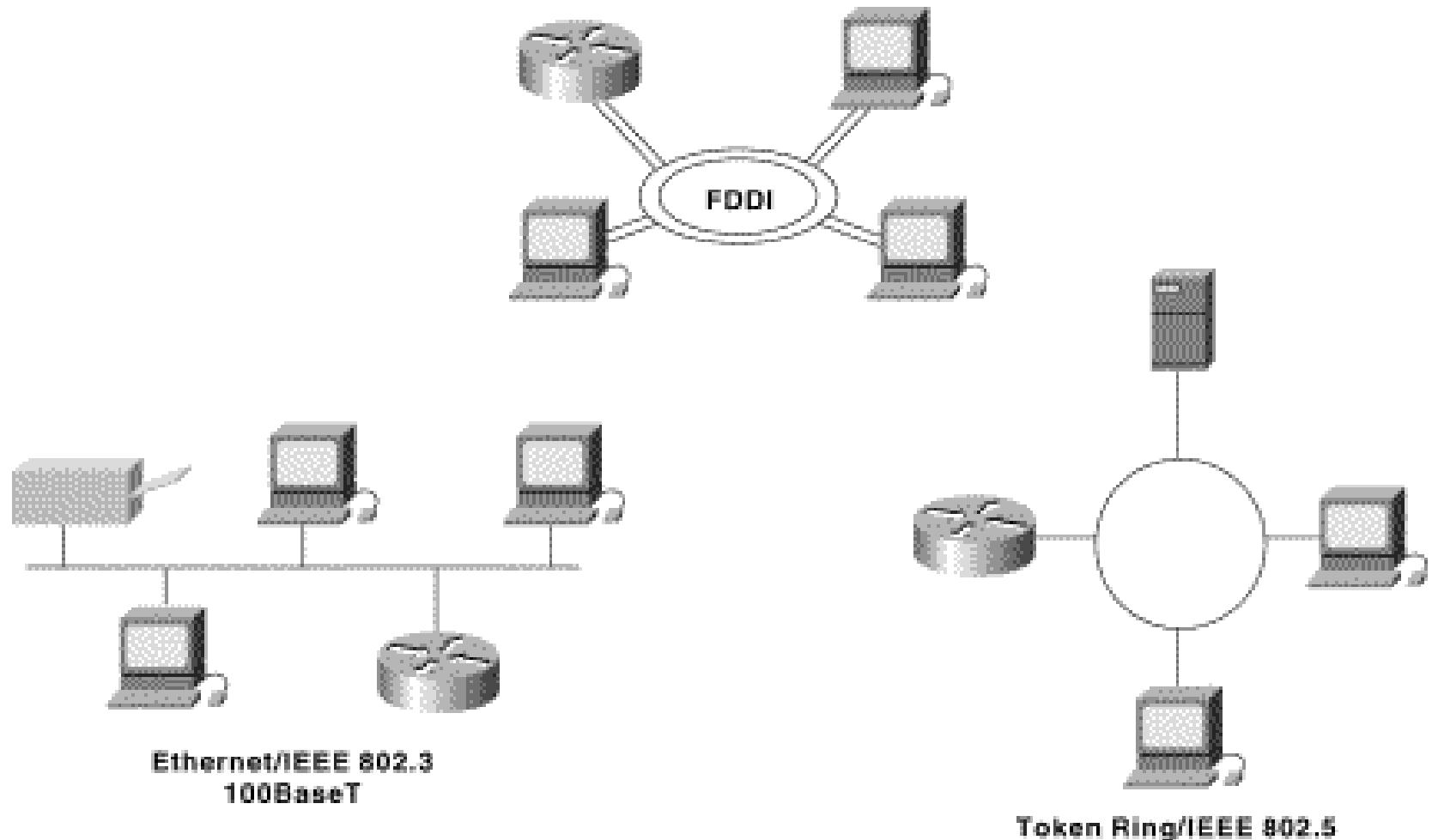


Figure 2-1: Three LAN Implementations Are Used Most Commonly

LAN Protocols and OSI Reference Model

- Function at the lowest two layers of the OSI reference model

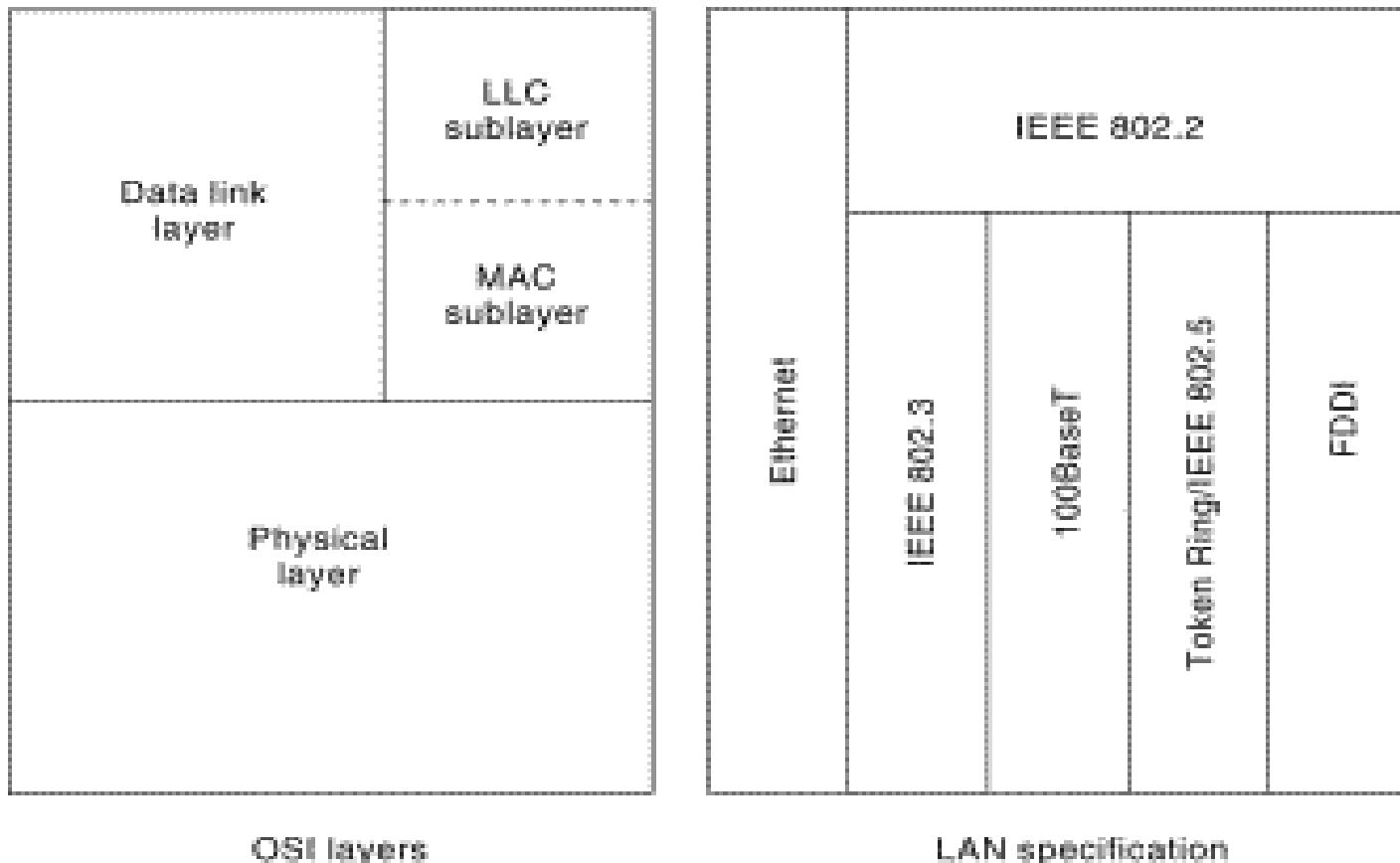


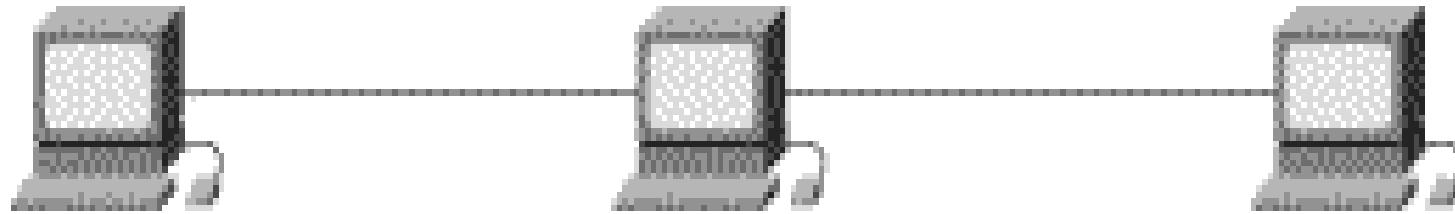
Figure 2-2: Popular LAN Protocols Mapped to the OSI Reference Model

LAN Transmission Methods

- Unicast transmission: a single packet is sent from the source to a destination on a network.
- Multicast transmission
 - a single data packet that is copied and sent to a specific subset of nodes on the network
 - source node addresses the packet by using a multicast address
- Broadcast transmission:
 - a single data packet that is copied and sent to all nodes on the network
 - the source node addresses the packet by using the broadcast address

LAN Topologies

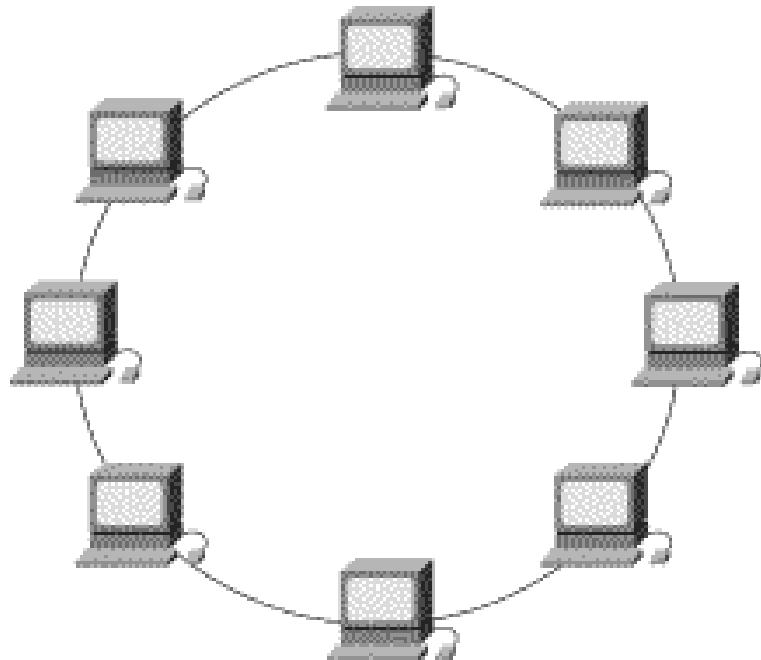
- Define the manner in which network devices are organized
- Four common LAN topologies: bus, ring, star, and tree.
- Bus topology: linear LAN architecture, transmissions from network stations propagate the length of the medium and are received by all other stations





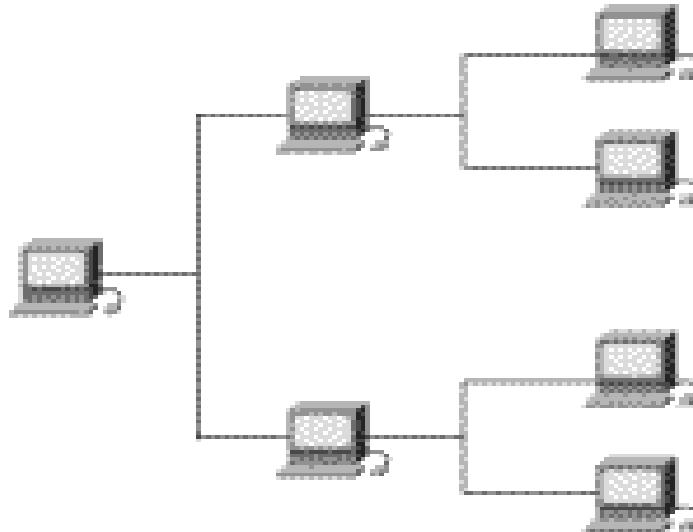
LAN Topologies

- Ring topology : consists of a series of devices connected to one another by unidirectional transmission links to form a single closed loop.



LAN Topologies

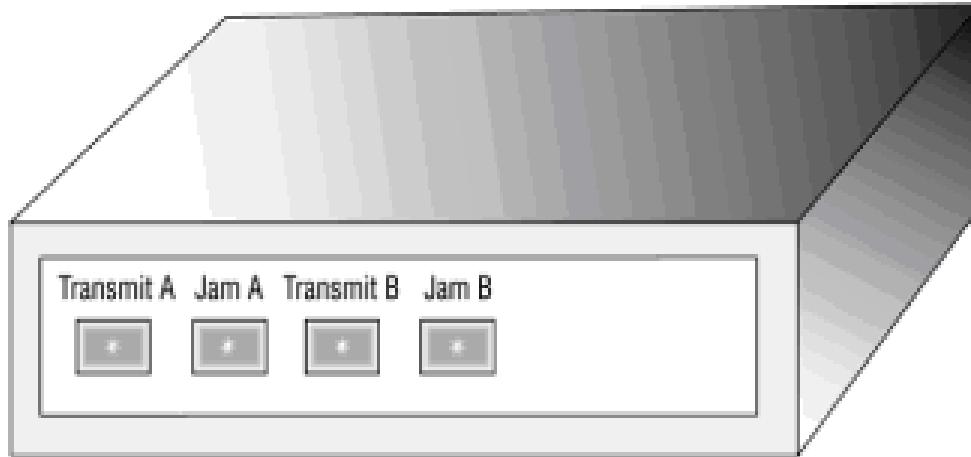
- star topology: endpoints on a network are connected to a common central hub, or switch, by dedicated links
- tree topology: identical to the bus topology, except that branches with multiple nodes are possible in this case





● Repeater

- a physical layer device used to interconnect the media segments of an extended network
- used in a bus topology to extend the maximum distance that can be spanned on a cable run

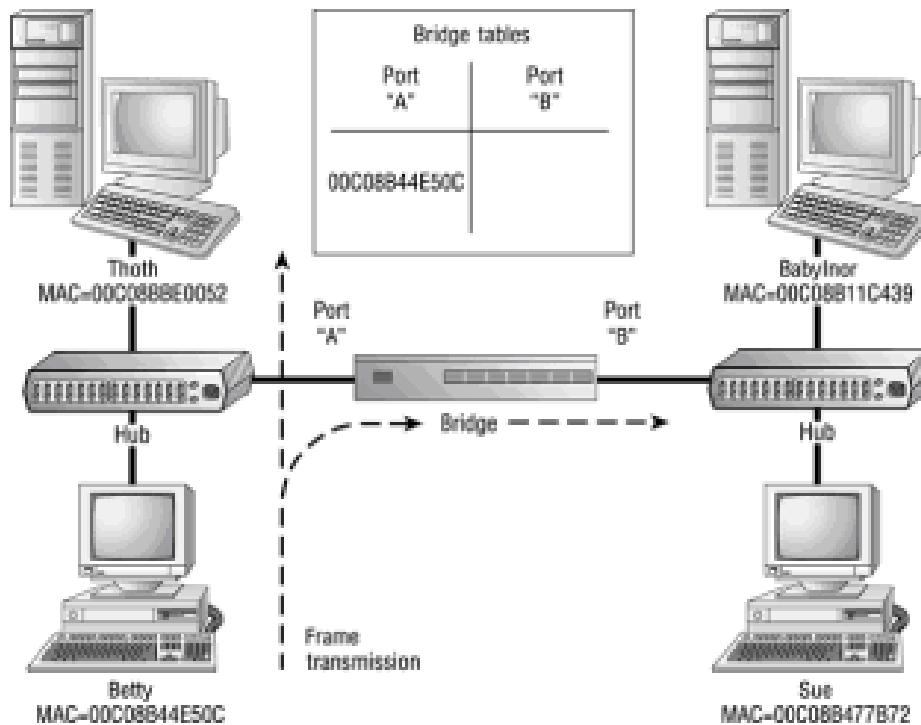


● Hub

- a physical layer device that connects multiple user stations, each via a dedicated cable, multiport repeater.
- common piece of network hardware after network interface cards
- Used in in a star topology.
- *chassis hub:*
 - the expansion card slots
 - The number of stations a hub can support depends on the *port density* of each card and how many such cards are installed.
 - Drawbacks: single point of failure, difficult to trace wires.
- *stackable hubs:*
 - slim-line boxes that usually contain between six and 32 ports.
 - simply buy another hub and stack it on top of the first.

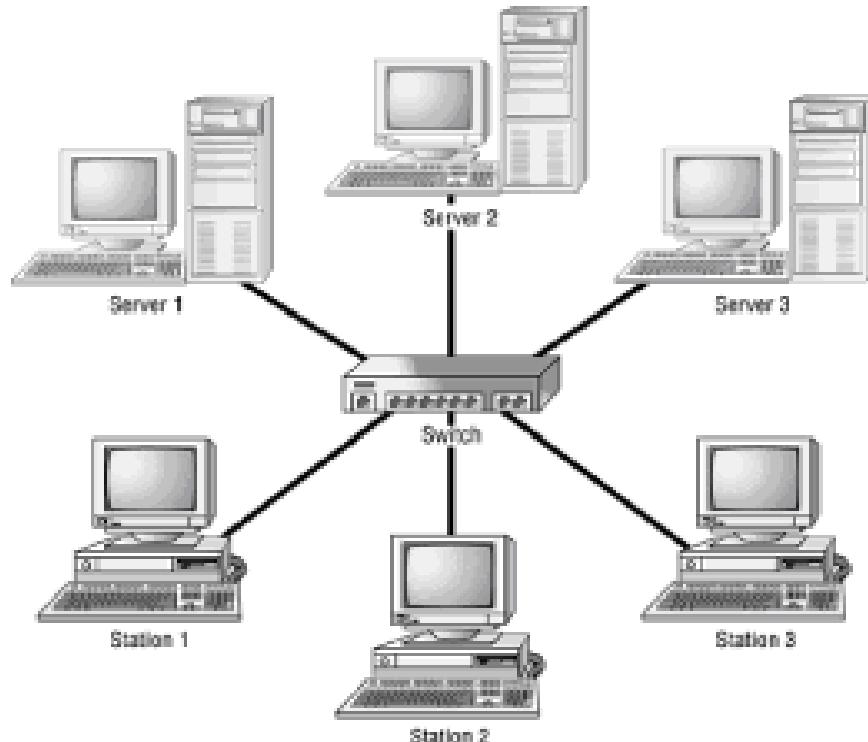
Bridge

- small box with two network connectors that attach to two separate portions of the network, in layer 2
- Bridges put frame header information to use by monitoring the source and destination MAC address on each frame of data. By monitoring the source address, the bridge will learn where all the network systems are located



Switch:

- the marriage of hub and bridge technology, layer 2 or layer 3
- keep track of the MAC addresses attached to each of its ports and route traffic destined for a certain address only to the appropriate port





LAN Devices

- Router: layer 3 multiport device that makes decisions on how to handle a frame, based on protocol and network address.



LAN Switching

● Contents:

- What is LAN switching?
- LAN switch and OSI Model
- LAN switch operation

What is LAN switching

- LAN switch : a device that provides much higher port density at a lower cost than traditional bridges.
- Forwards frames based on either the frame's Layer 2 address (Layer 2 LAN switch) or, in some cases, the frame's Layer 3 address (multilayer LAN switch).
- Also called a frame switch because it forwards Layer 2 frames

LAN Switch and the OSI Model

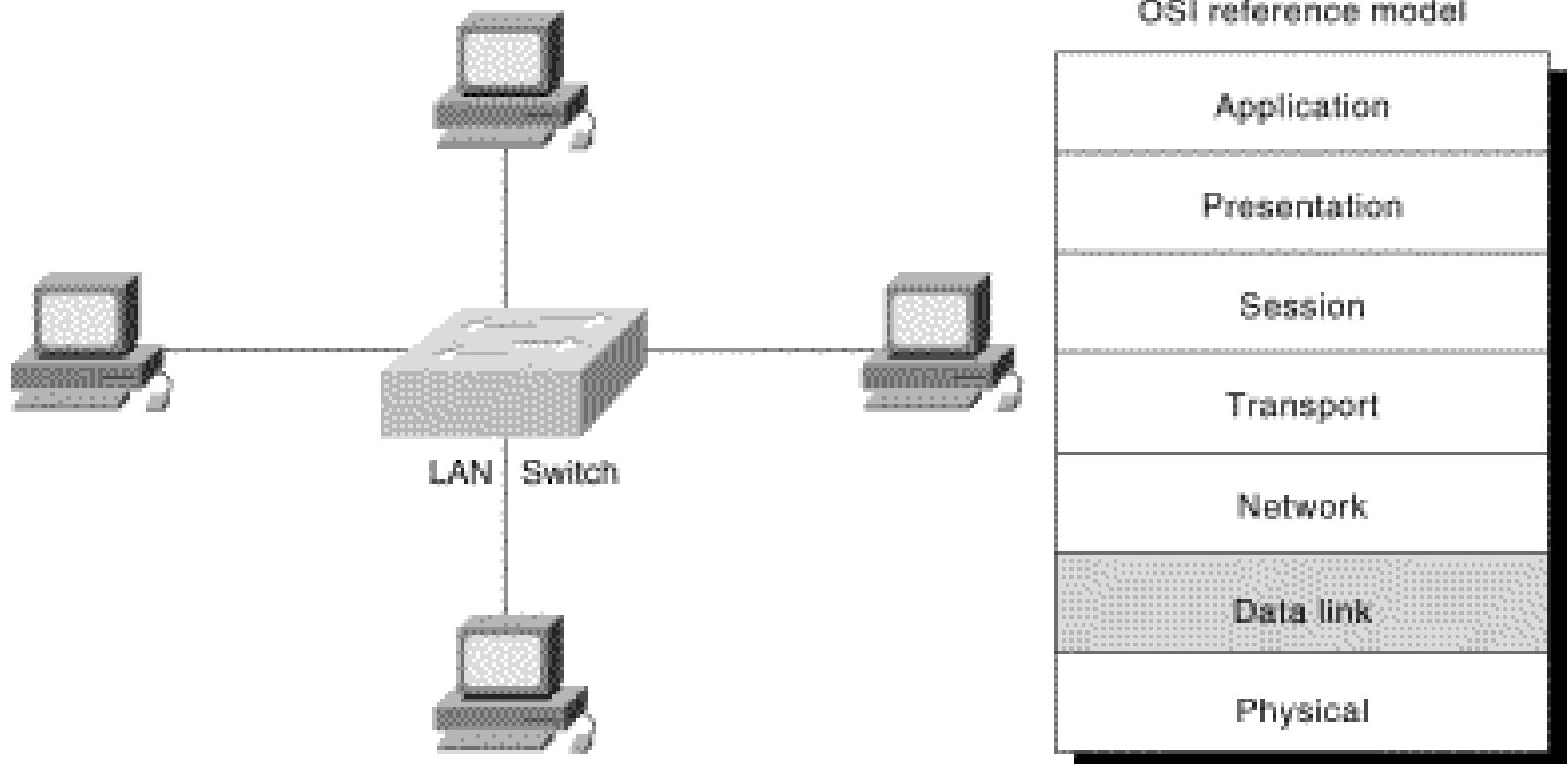


Figure 3-1: A LAN Switch Is a Data Link Layer Device

LAN switch operation

● LAN Switching Forwarding:

- store-and-forward switching method:
 - copies the entire frame into its onboard buffers
 - computes the cyclic redundancy check (CRC)
 - looks up the destination address in its forwarding, or switching, table and determines the outgoing interface
 - forwards the frame toward its destination
- cut-through switching method:
 - copies only the destination address.
 - looks up the destination address in its switching table, determines the outgoing interface.
 - forwards the frame toward its destination.

● LAN switches must use store-and-forward techniques to support multilayer switching

LAN switch operation

● LAN Switching Bandwidth

- *Asymmetric LAN switch* provides switched connections between ports of unlike bandwidths.
- *Symmetric switch* provides switched connections between ports with the same bandwidth.

● Network manager must evaluate the needed amount of bandwidth for connections between devices to accommodate the data flow of network-based applications when deciding to select an asymmetric or symmetric switch



Global CyberSoft

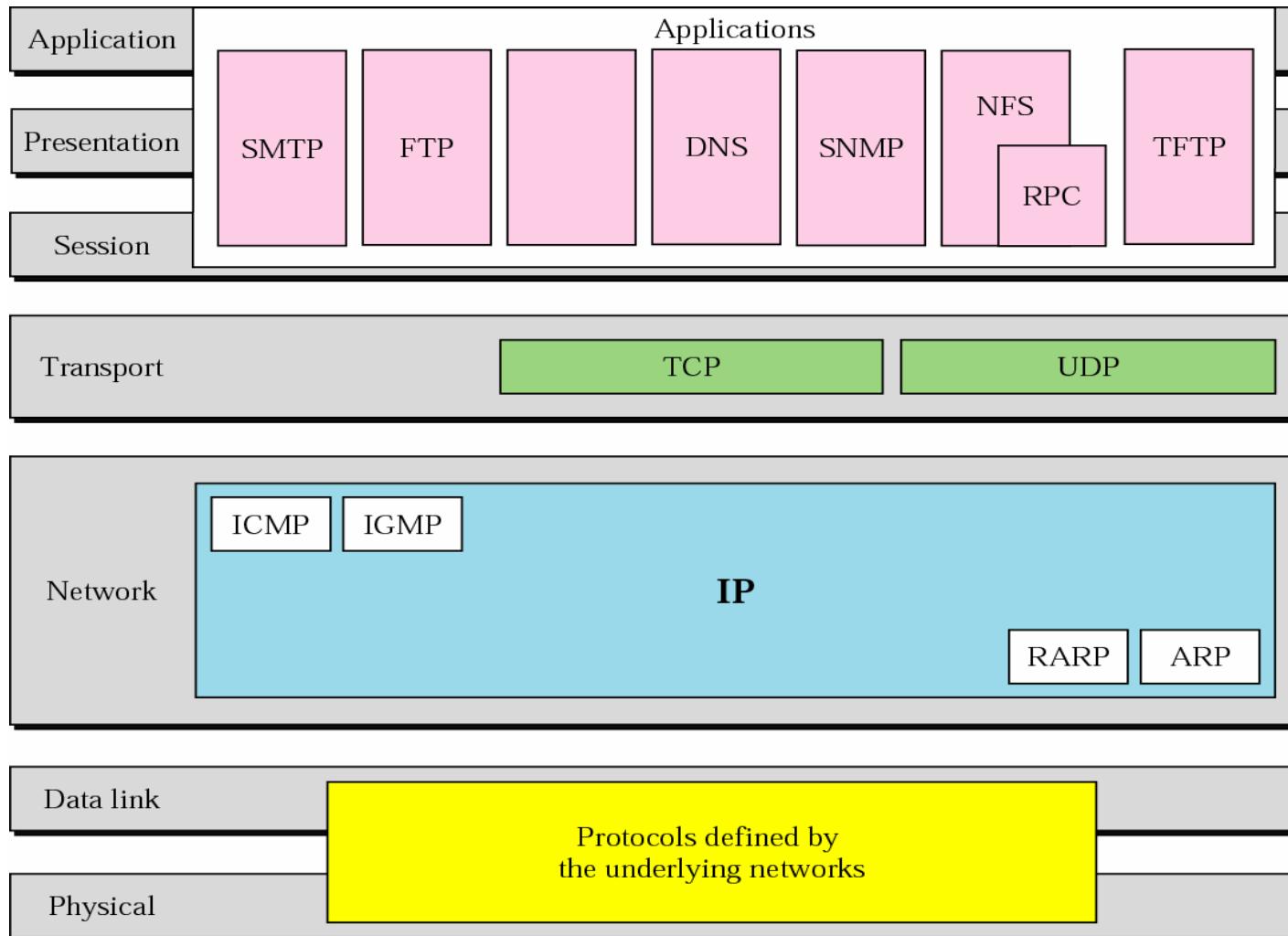
TCP/IP Protocol Suite

- Content:

- TCP/IP Protocol Suite
- Address in TCP/IP

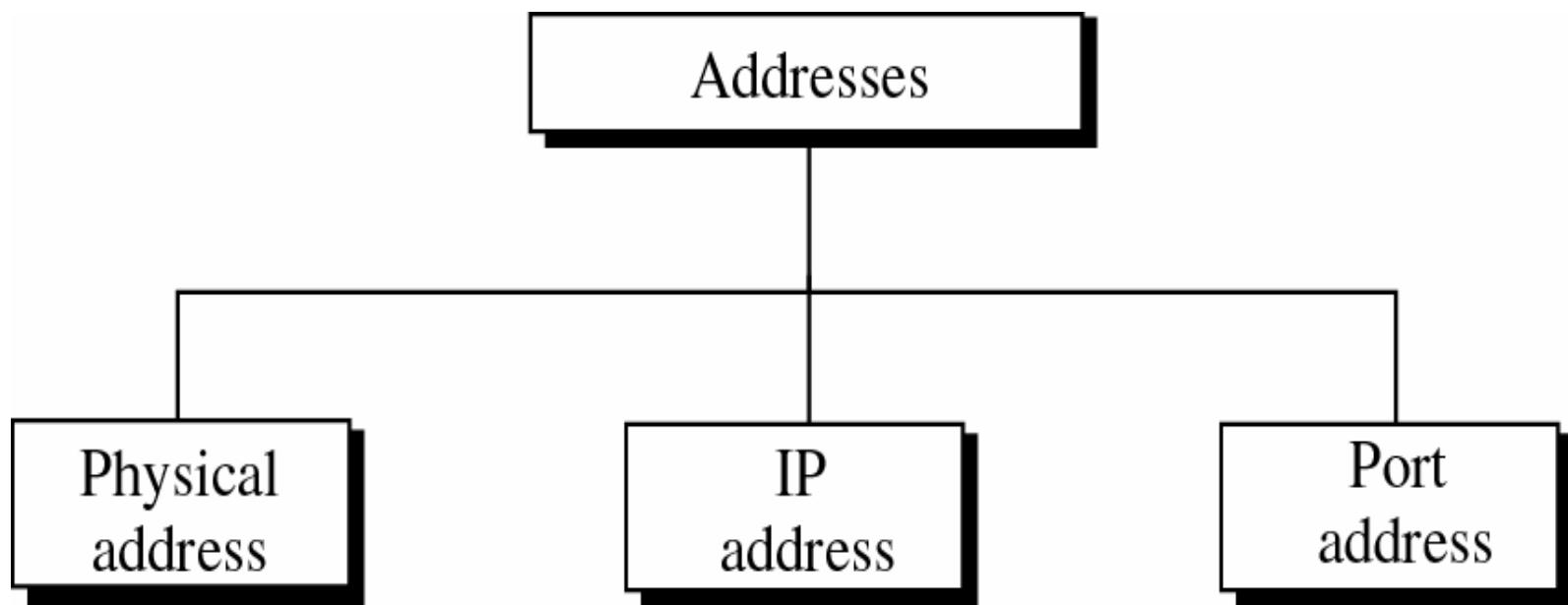
The TCP/IP Protocol Suite

TCP/IP and OSI model



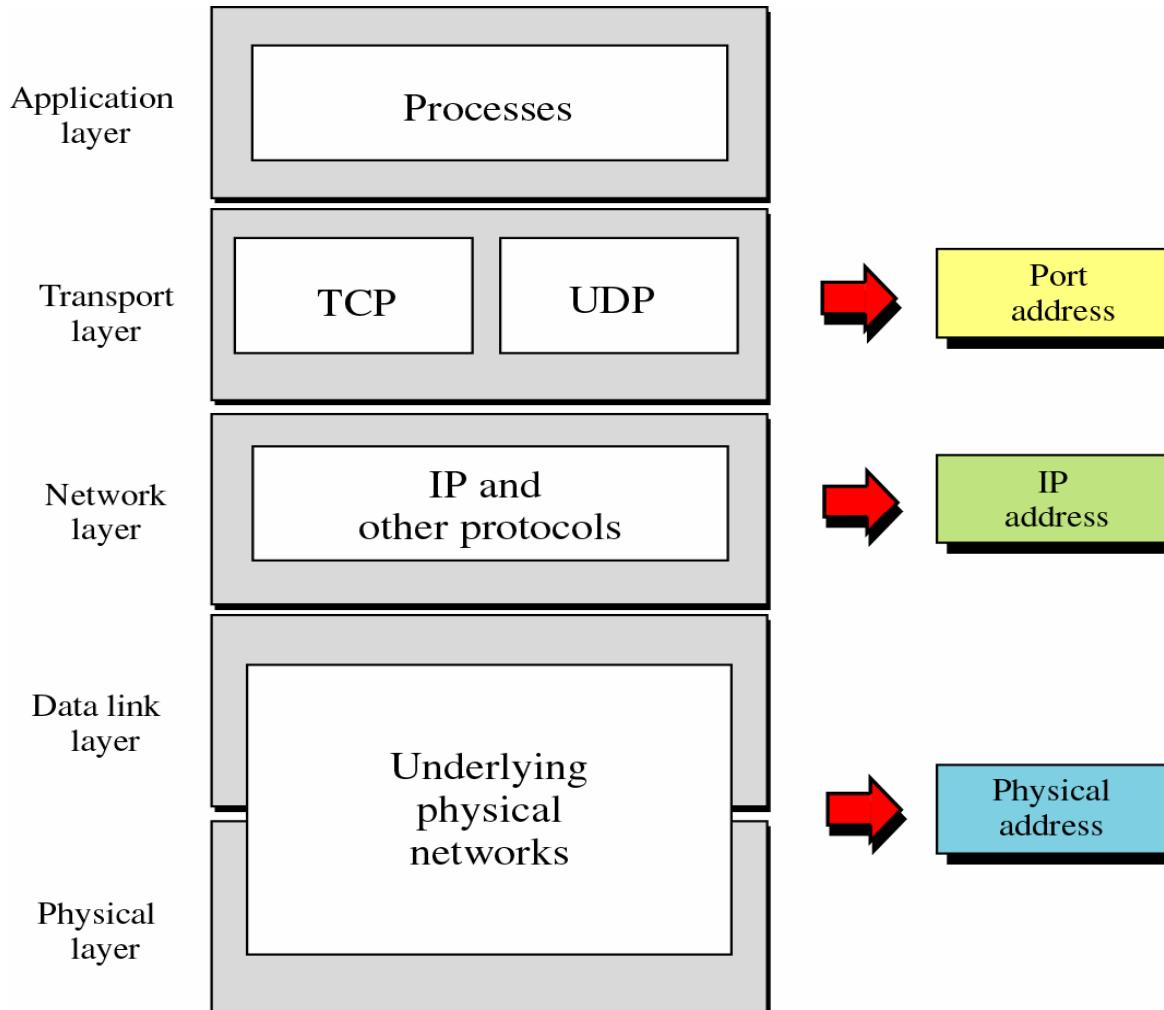


Address in TCP/IP: IP version 4



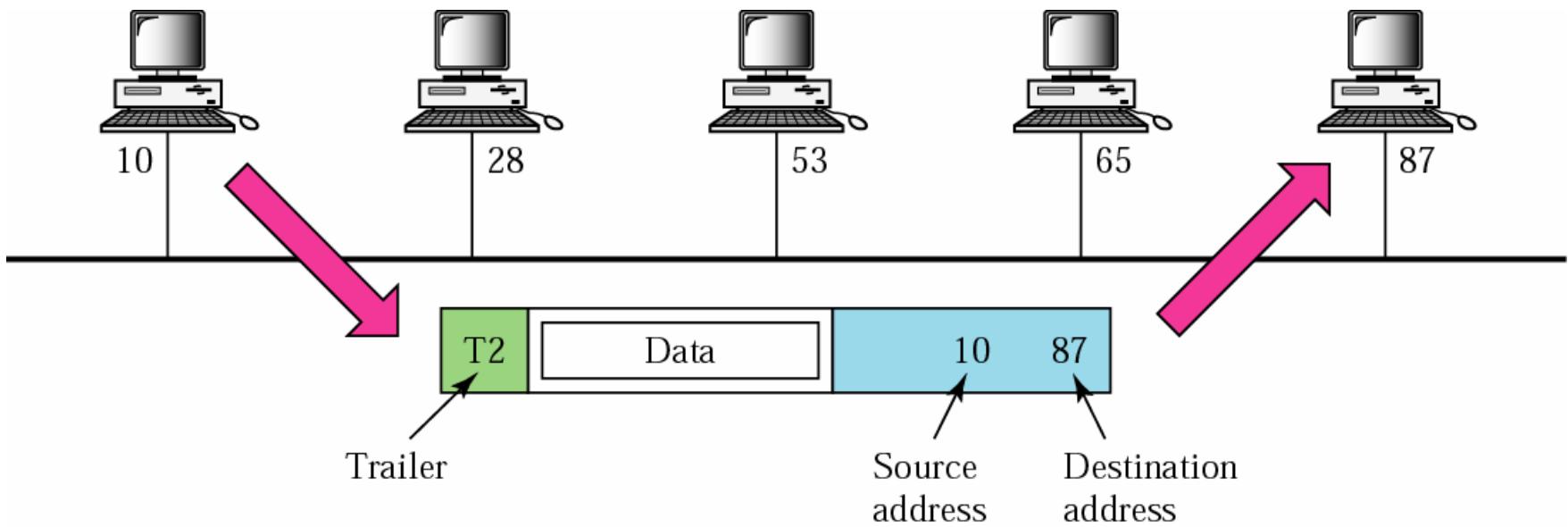
Address in TCP/IP

Relationship of layers and addresses in TCP/IP





Address in TCP/IP: Physical Address



Address in TCP/IP: Physical address

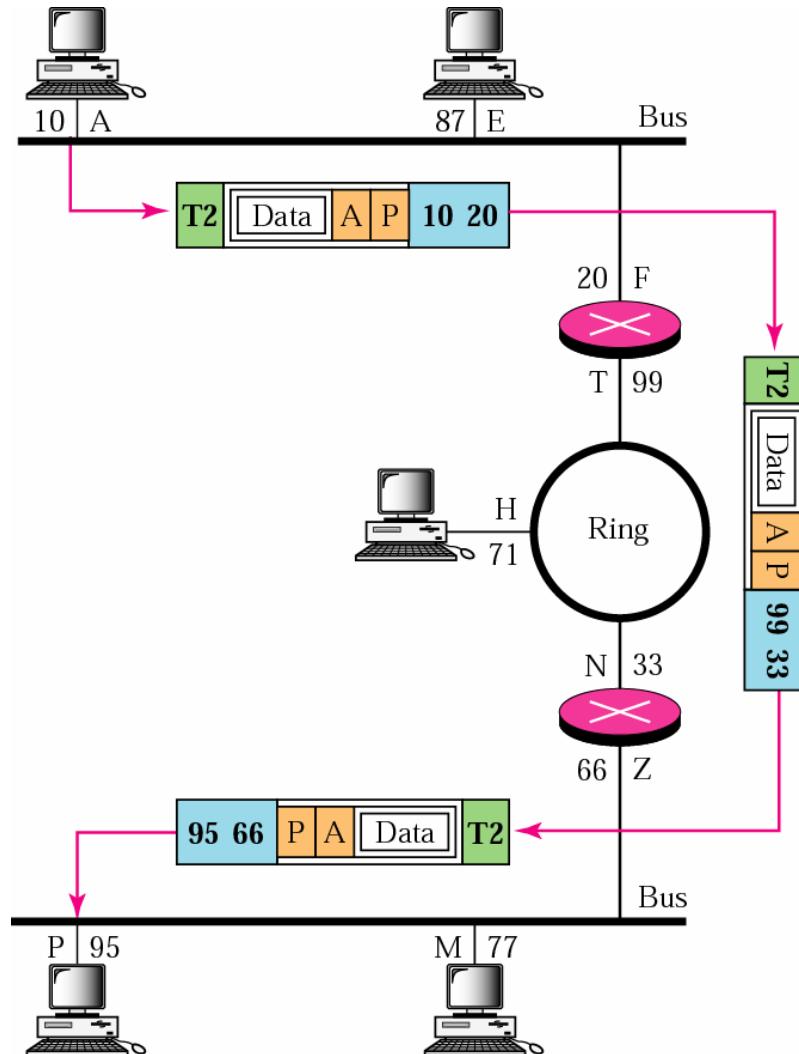
Most local area networks use a 48-bit (6 bytes) physical address written as 12 hexadecimal digits, with every 2 bytes separated by a hyphen as shown below:

07-01-02-01-2C-4B

A 6-byte (12 hexadecimal digits) physical address



Address in TCP/IP: IP address



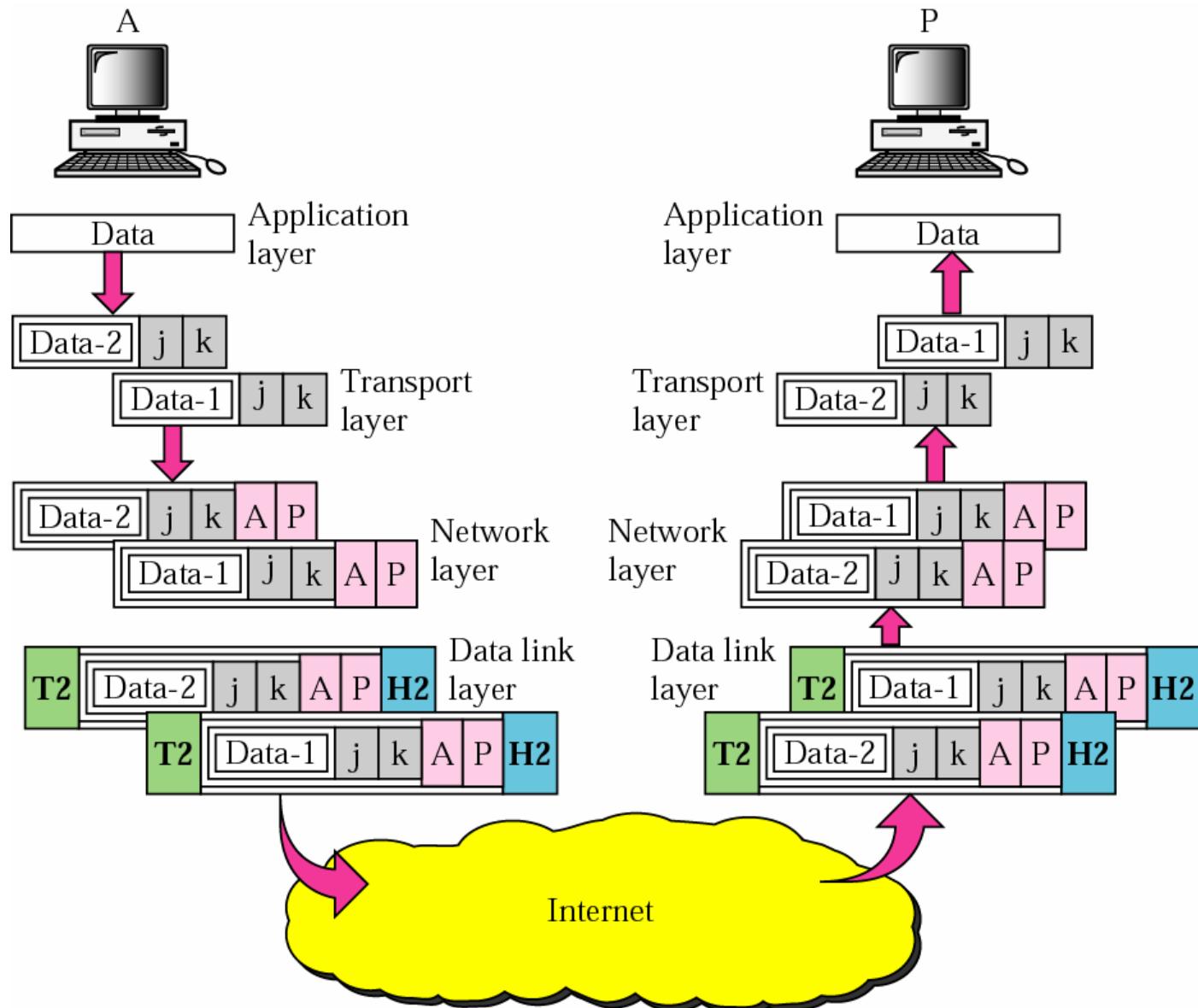


Address in TCP/IP: IP Address

- Internet address (in IPv4) is 32 bits in length, normally written as four decimal numbers, with each number representing 1 byte. The numbers are separated by a dot. Below is an example of such an address:

172.16.1.6

Address in TCP/IP: Port Address





Address in TCP/IP: Port Address

A port address is a 16-bit address represented by one decimal number as shown below

753

A 16-bit port address

Content:

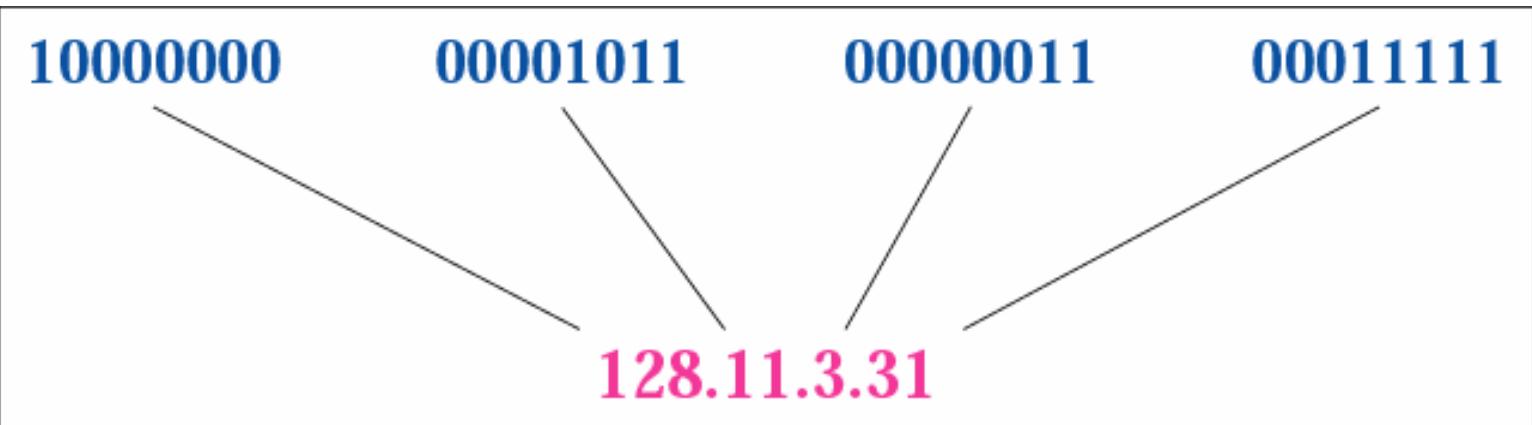
- Addressing.
- Classful Addressing.
- Subnetting.
- Protocols.

Addressing

- IP Address:
 - 32-bit address.
 - Unique.
- If a protocol uses N bits to define an address, the address space is 2^N because each bit can have two different values (0 and 1) and N bits can have 2^N values.
- The address space of IPv4 is 2^{32} or 4,294,967,296
- Binary notation:

01110101 10010101 00011101 11101010

- Dotted-decimal notation



Addressing

- Hexa-decimal notation

0111 0101 1001 0101 0001 1101 1110 1010

75

95

1D

EA

0x75951DEA



Classful Addressing

Global CyberSoft

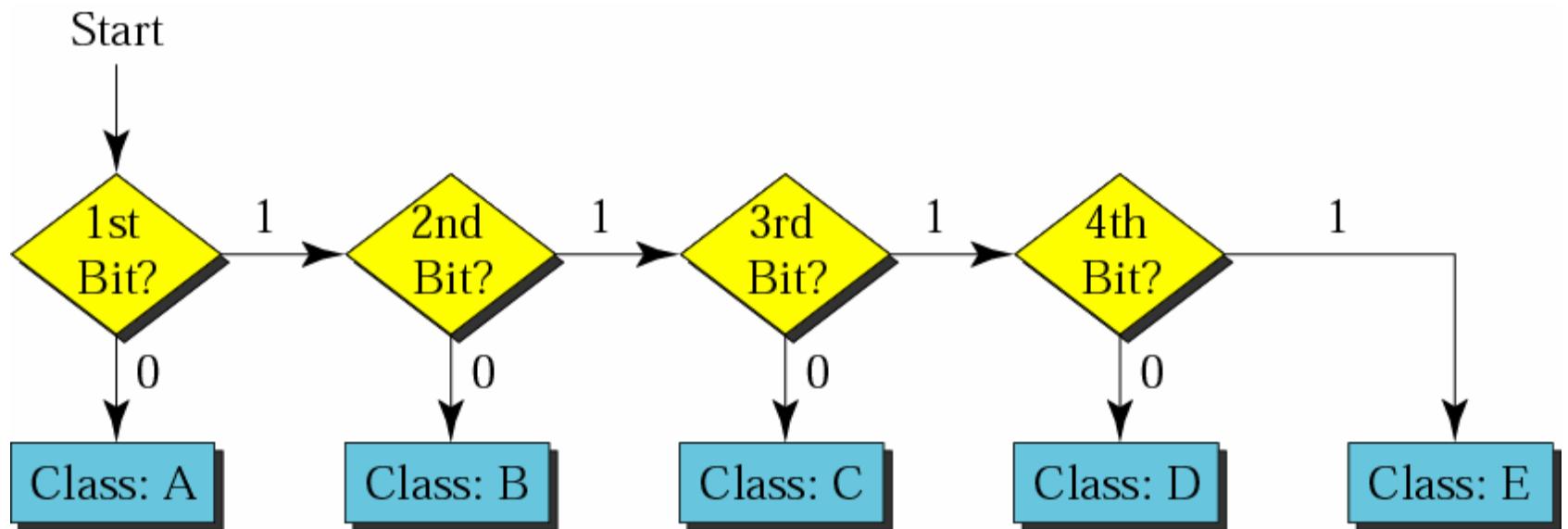
- The address space is divided into 4 class: A, B, C, D, E.

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			



Classful Addressing

- Finding the address class





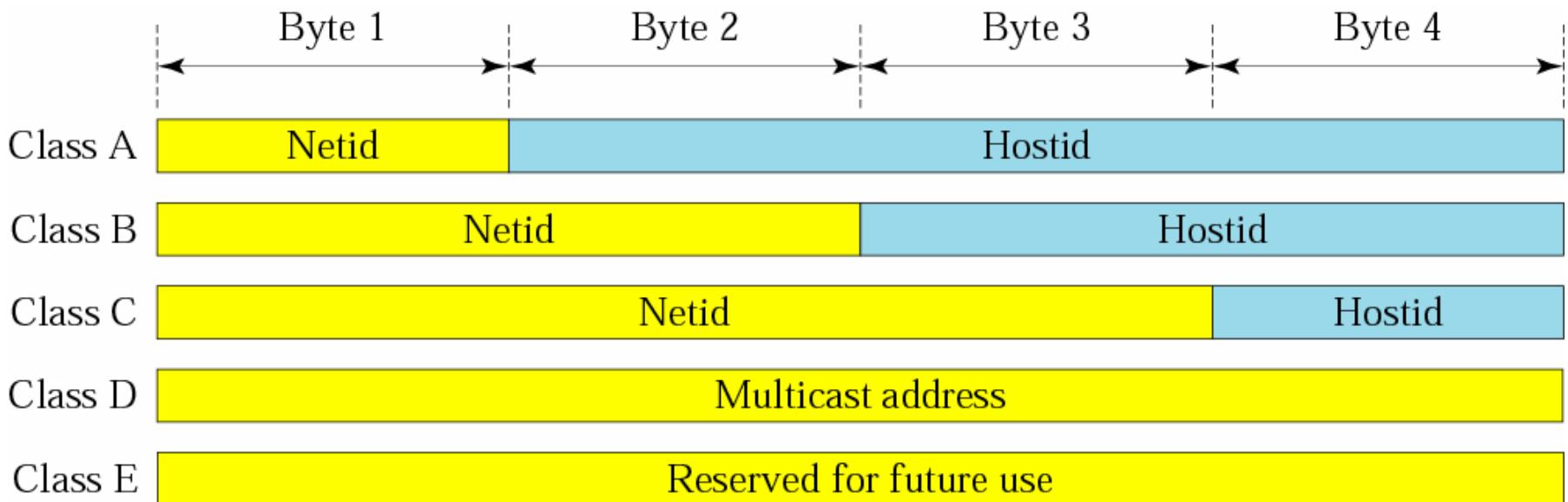
Classfull Addressing

	First byte	Second byte	Third byte	Fourth byte
Class A	0 to 127			
Class B	128 to 191			
Class C	192 to 223			
Class D	224 to 239			
Class E	240 to 255			



Classful Addressing

- Netid and hostId

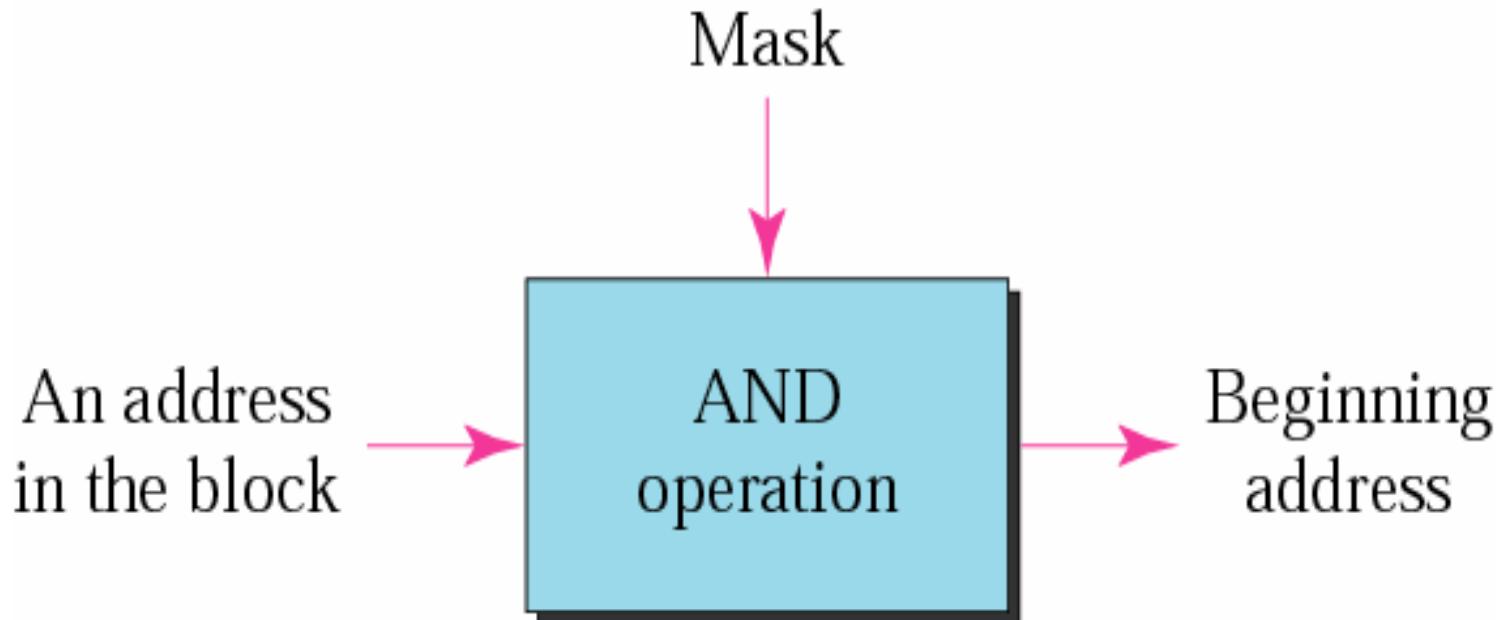


Classful Addressing: Network Address

- The network address is the first address.
- The network address defines the network to the rest of the Internet
- Given the network address, we can find the class of the address, the block, and the range of the addresses in the block.
- Network address is assigned to the organization.

Classful Addressing: Mask

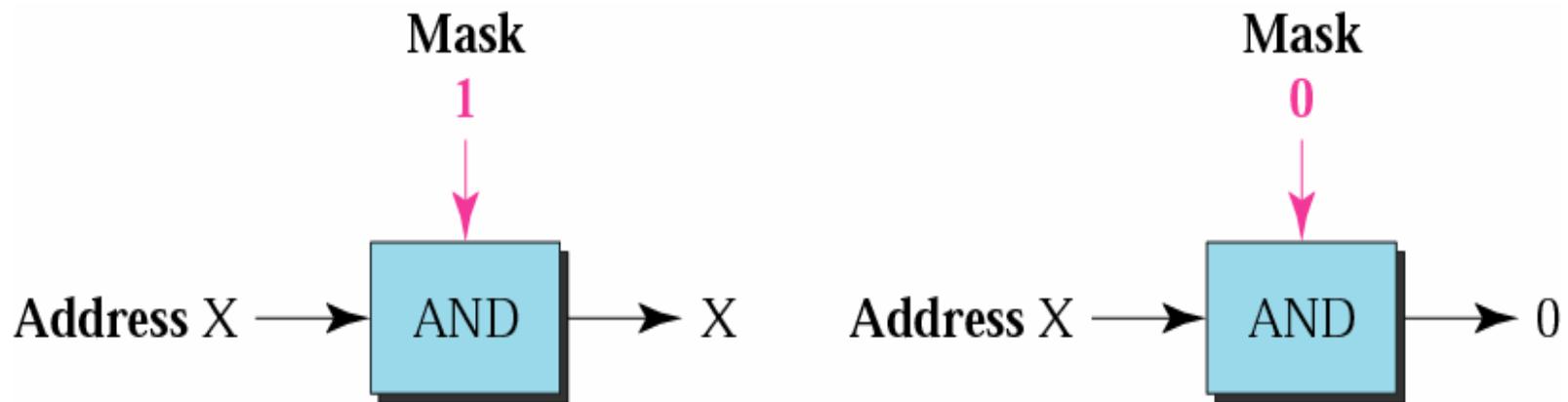
- A 32-bit binary number that gives the first address in the block (the network address) when bitwise ANDed with an address in the block.
- Concept





Classful Addressing: Mask

- And operation



Classful Addressing: Note

- The network address is the beginning address of each block.
- It can be found by applying the default mask to any of the addresses in the block (including itself). It retains the **netid** of the block and sets the **hostid** to zero.

Example 1

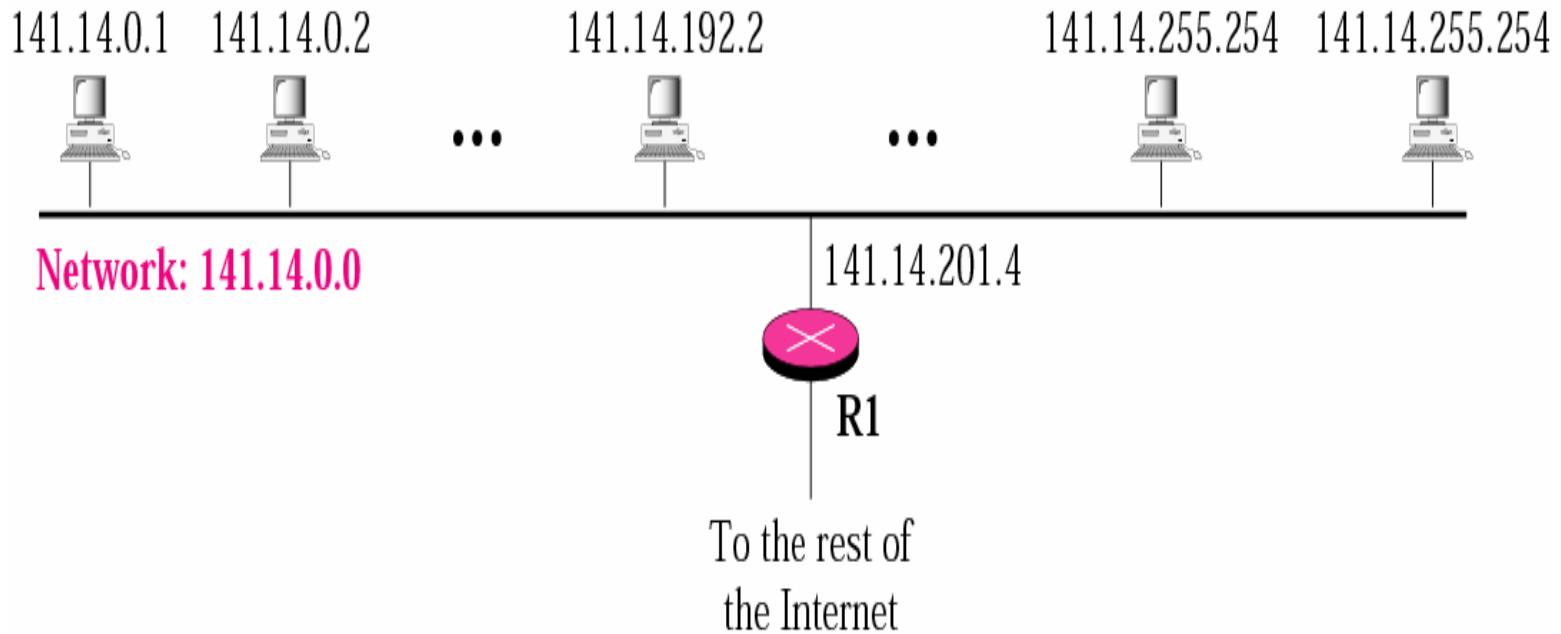
- Given the address 23.56.7.91 and the default class A mask, find the beginning address (network address).
- Solution: The default mask is 255.0.0.0, which means that only the first byte is preserved and the other 3 bytes are set to 0s. The network address is 23.0.0.0

Example 2

- Given the address 201.180.56.5 and the class C default mask, find the beginning address (network address).
- Solution: The default mask is 255.255.255.0, which means that the first 3 bytes are preserved and the last byte is set to 0. The network address is 201.180.56.0

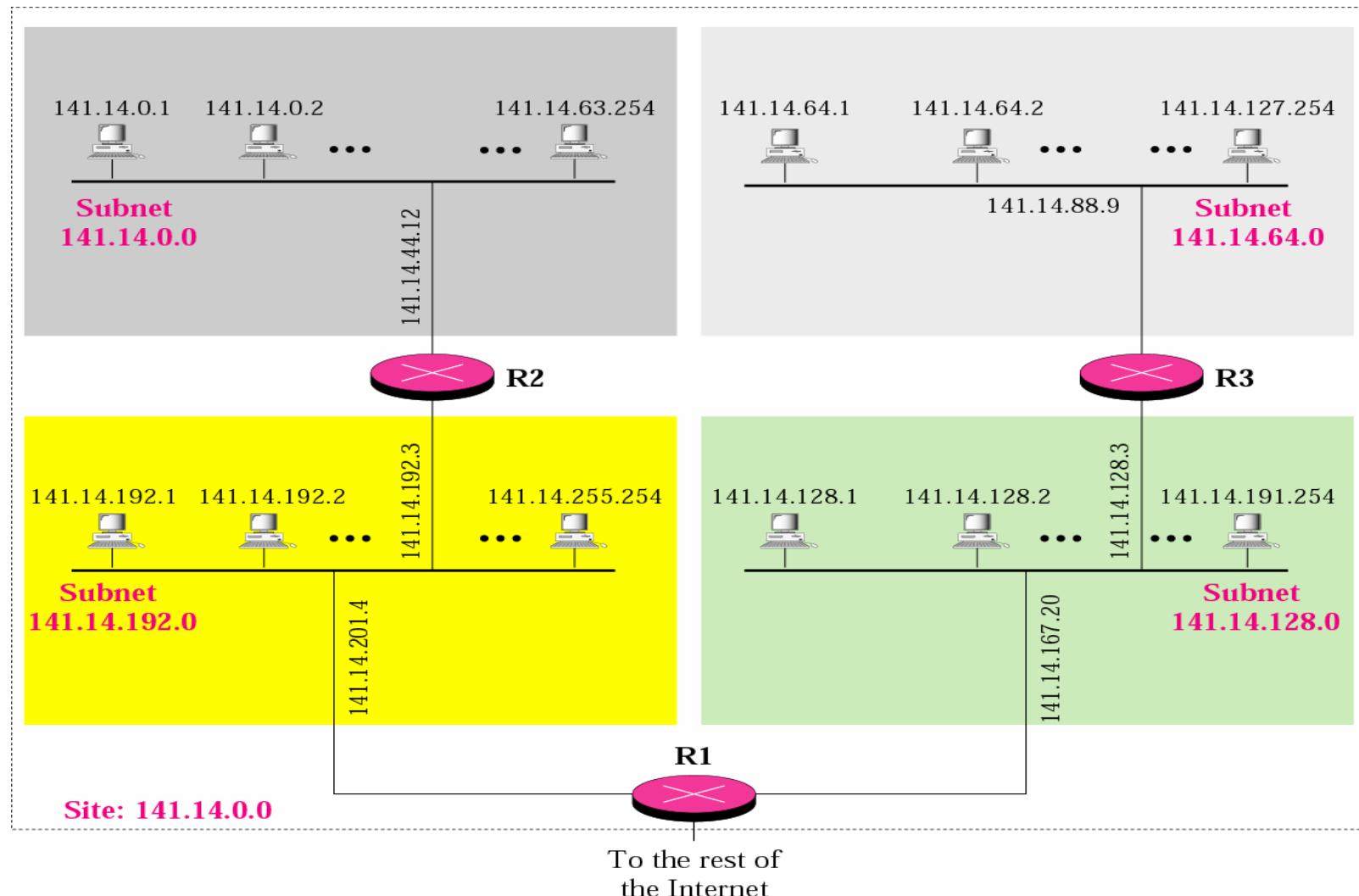
Subnetting

● Network without subnetting



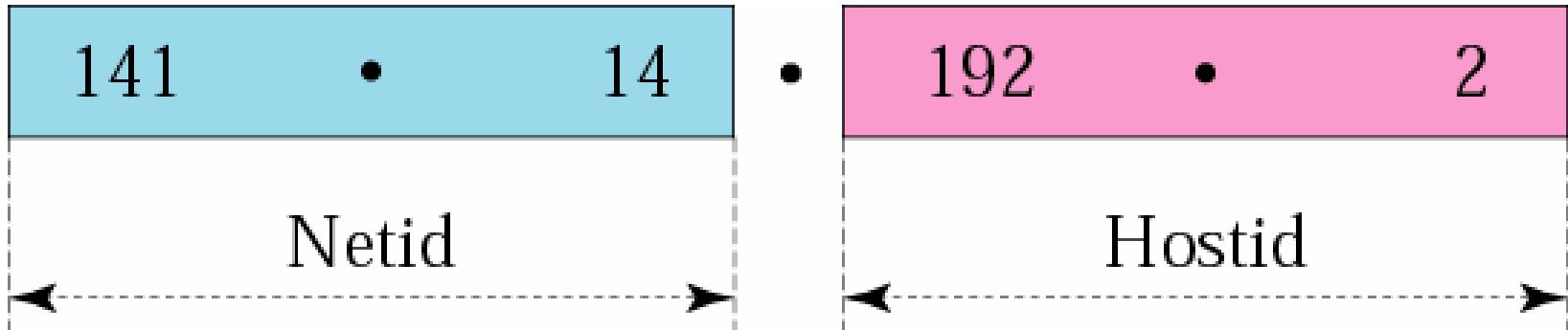
Subnetting

Network with subnetting

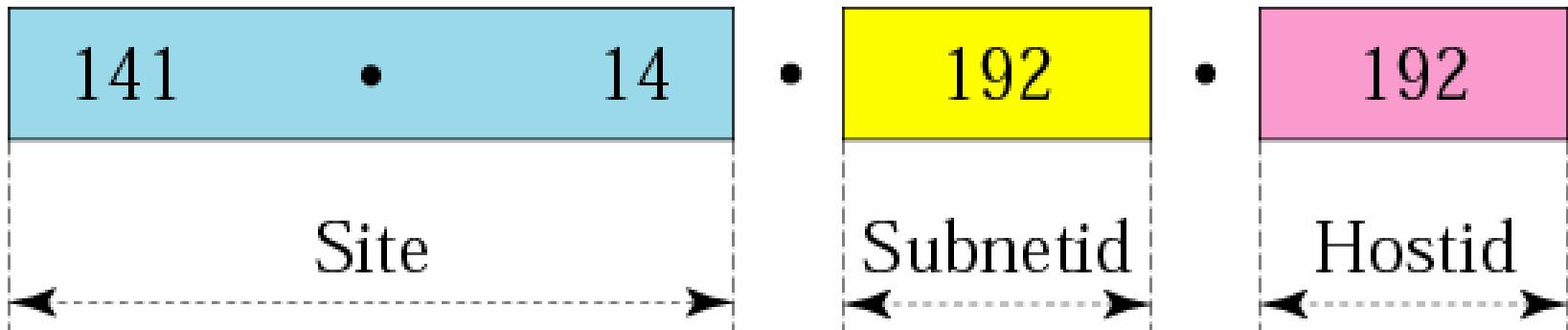


Subnetting

- Address in network with and without subnetting



a. Without subnetting

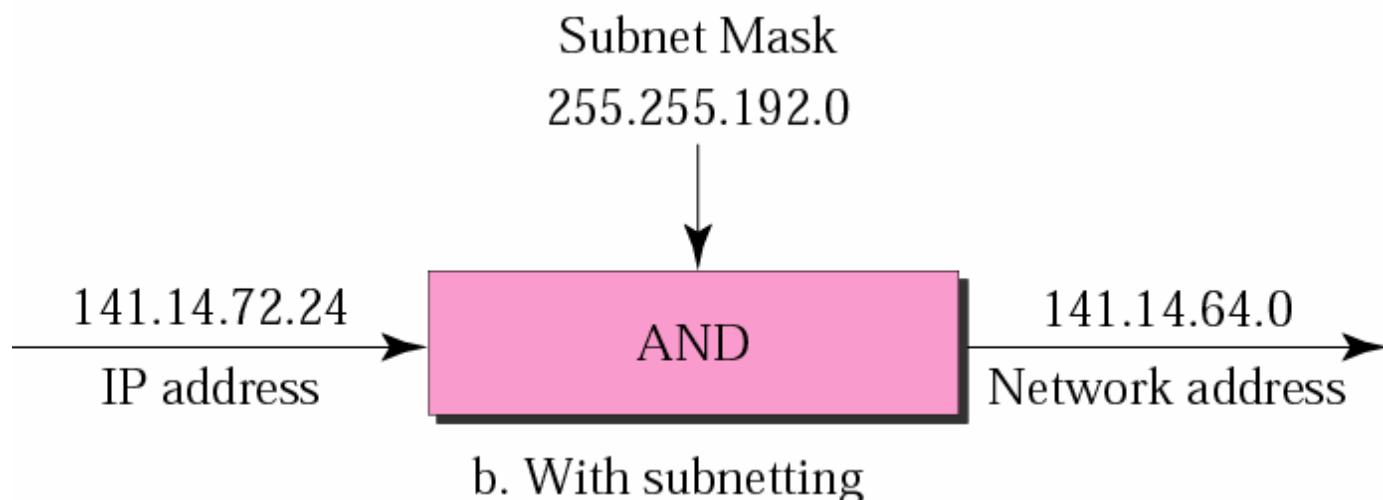
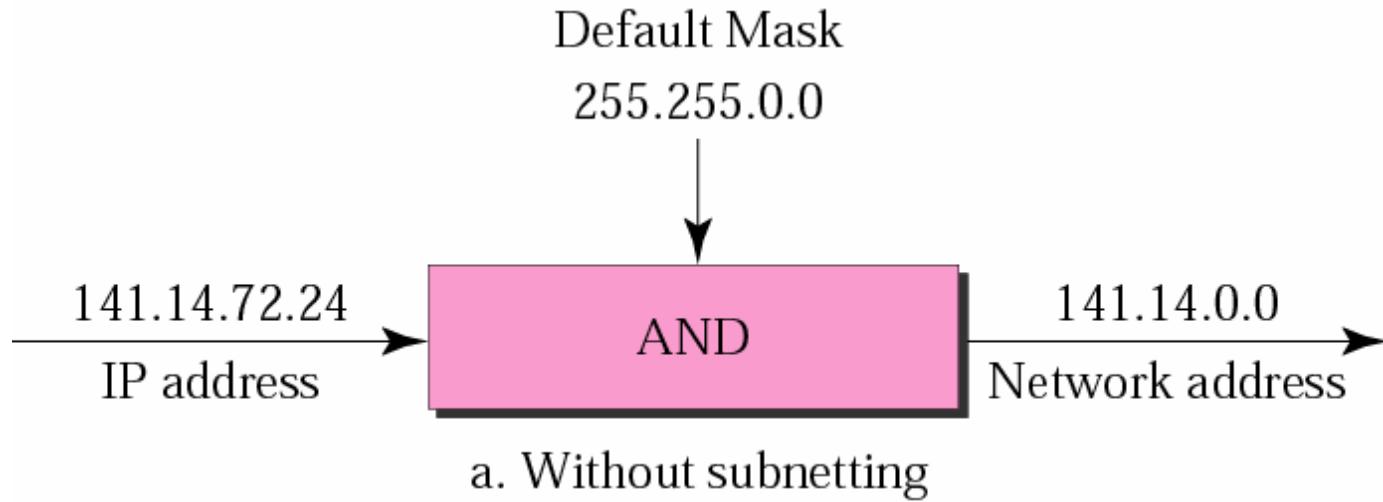


b. With subnetting



Subnetting

Default mask and subnet mask



Subnetting

- Finding the subnet address:

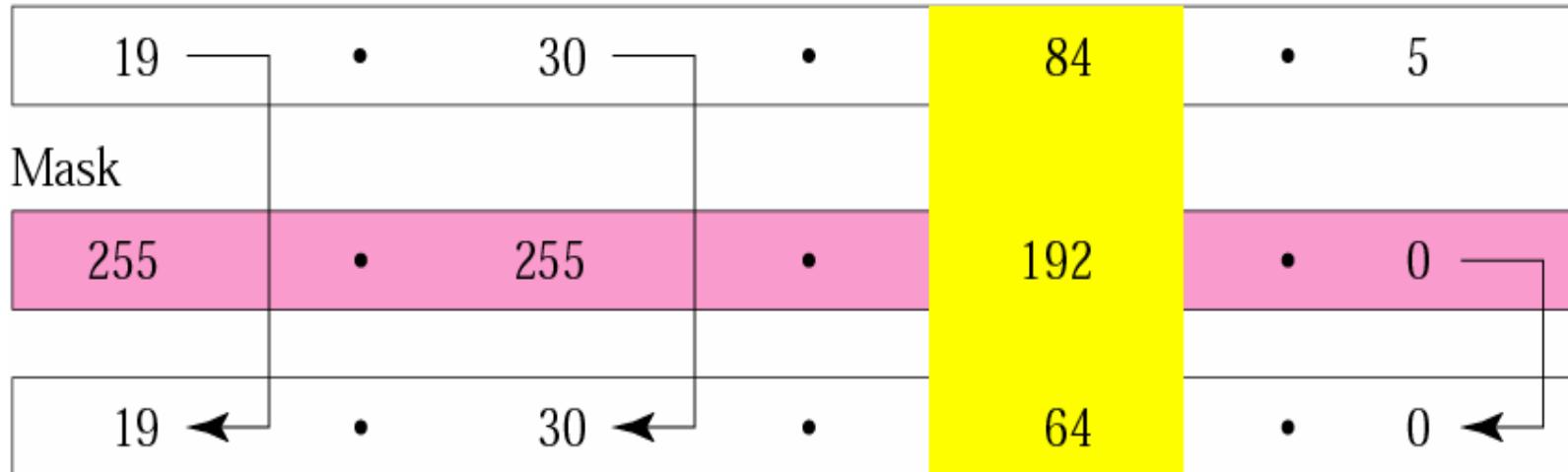
- Using binary notation for both the address and the mask and then apply the AND operation to find the subnet address.
- Short-Cut Method
 - If the byte in the mask is 255, copy the byte in the address.
 - If the byte in the mask is 0, replace the byte in the address with 0.
 - If the byte in the mask is neither 255 nor 0, we write the mask and the address in binary and apply the AND operation



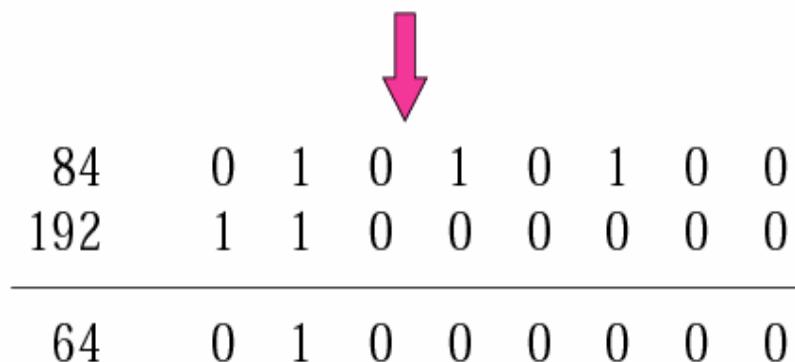
Subnetting

Global CyberSoft

- Use binary notation / Short cut
- IP Address



Subnet Address



Subnetting

- Rules:
 - The number of blocks must be a power of 2 (1, 2, 4, 8, 16, . . .).
 - The blocks must be contiguous in the address space (no gaps between the blocks).
 - The third byte of the first address in the superblock must be evenly divisible by the number of blocks. In other words, if the number of blocks is N , the third byte must be divisible by N .
- In subnetting, we need the first address of the subnet and the subnet mask to define the range of addresses

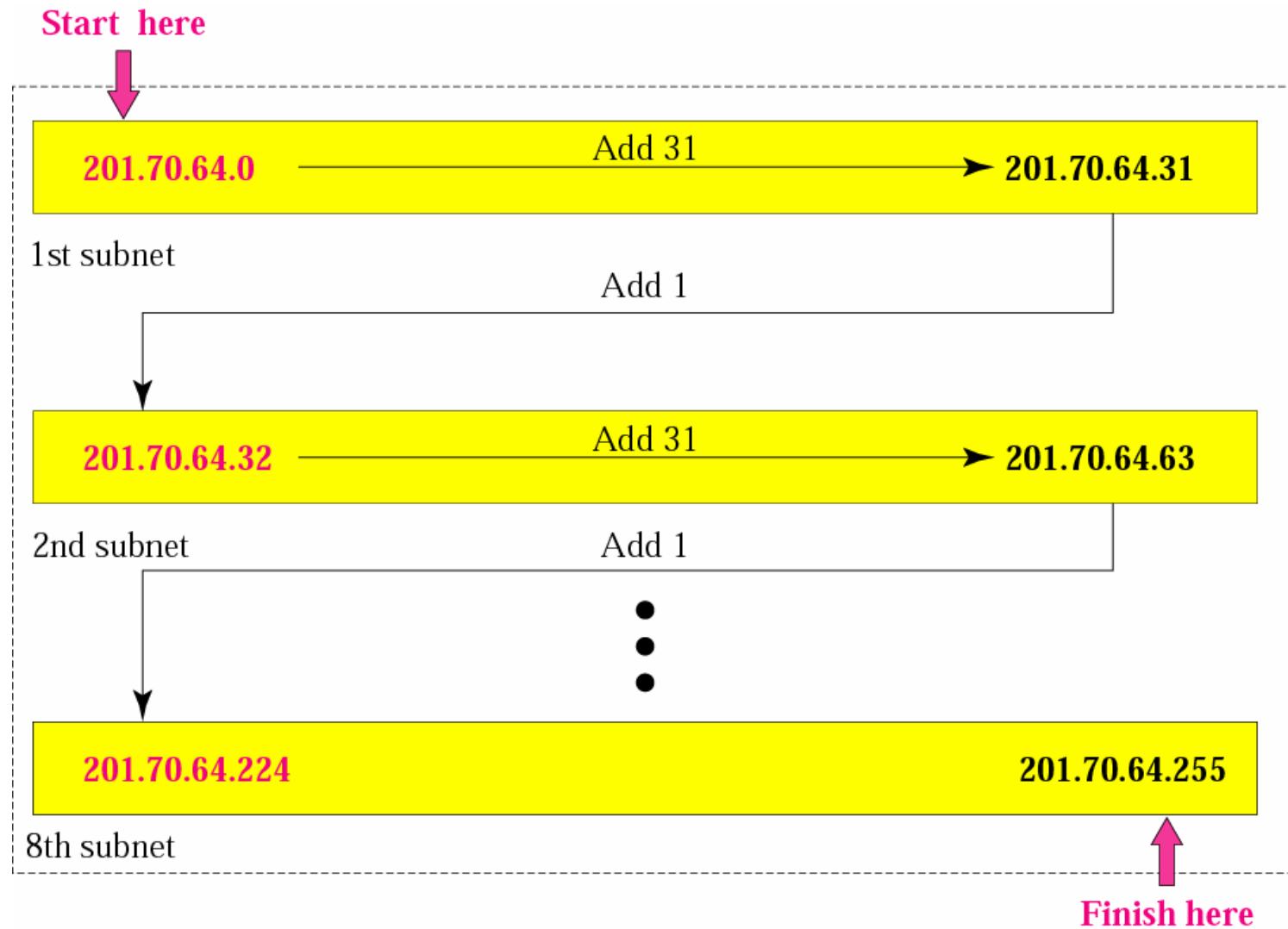
Subnetting: example

- A company is granted the site address 201.70.64.0 (class C).
The company needs six subnets. Design the subnets.
- The number of 1s in the default mask is 24 (class C).
- The company needs six subnets. This number 6 is not a power of 2. The next number that is a power of 2 is 8 (2³). We need 3 more 1s in the subnet mask. The total number of 1s in the subnet mask is 27 (24 + 3).
- The total number of 0s is 5 ($32 - 27$). The mask is
11111111 11111111 11100000

or

255.255.255.224

- The number of subnets is 8.
- The number of addresses in each subnet is 2^5 (5 is the number of 0s) or 32.





Slash Notation

A.B.C.D/*n*

Slash Notation

- Slash notation is also called CIDR (Classless Interdomain Routing) notation
- A block in classes A, B, and C can easily be represented in slash notation as $A.B.C.D/n$ where n is either 8 (class A), 16 (class B), or 24 (class C).

Example

- What is the network address if one of the addresses is 167.199.170.82/27
- Solution: The prefix length is 27, which means that we must keep the first 27 bits as is and change the remaining bits (5) to 0s. The 5 bits affect only the last byte. The last byte is 01010010. Changing the last 5 bits to 0s, we get 01000000 or 64. The network address is 167.199.170.64/27



Protocols

- Internet Protocol
- ARP and RARP
- BOOTP and DHCP
- UDP
- TCP
- ICMP
- IGMP



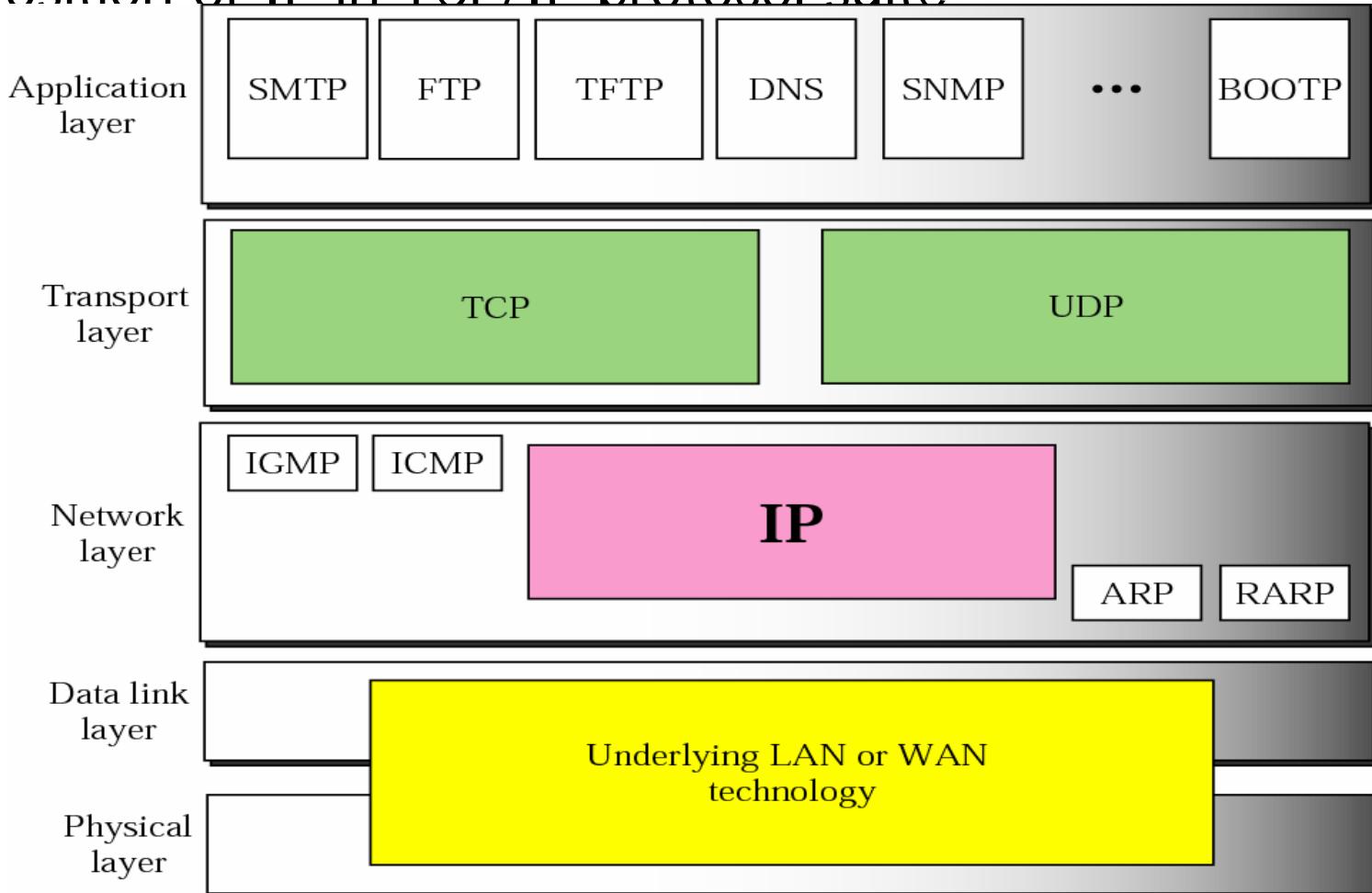
Global CyberSoft

Internet Protocol

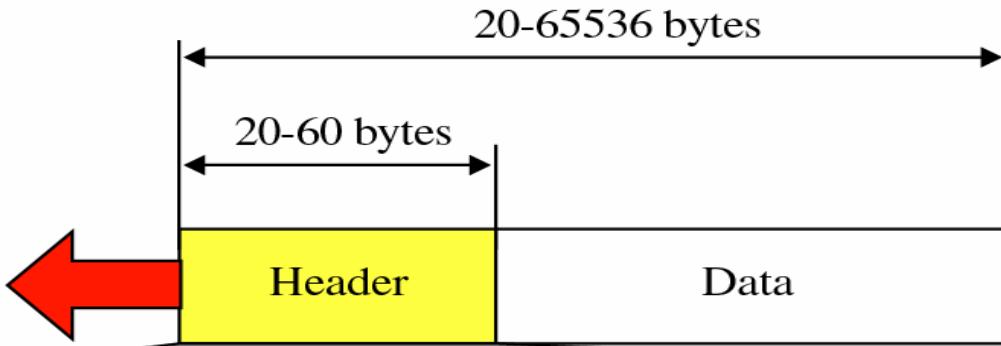
- DATAGRAM
- FRAGMENTATION
- OPTIONS
- CHECKSUM
- IP PACKAGE

Internet Protocol

Position of IP in TCP/IP protocol suite



Datagram



VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits						
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits						
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits							
Source IP address									
Destination IP address									
Option									

Datagram

- current protocol *version* is 4, so IP is sometimes called IPv4
- *header length* is the number of 32-bit words in the header, including any options. Since this is a 4-bit field, it limits the header to 60 bytes
- *type-of-service* field (TOS) is composed of a 3-bit precedence field (which is ignored today)
- *total length* field is the total length of the IP datagram in bytes. Using this field and the header length field, we know where the data portion of the IP datagram starts, and its length. Since this is a 16-bit field, the maximum size of an IP datagram is 65535 bytes
- The *identification* field uniquely identifies each datagram sent by a host. It normally increments by one each time a datagram is sent
- The *time-to-live* field, or *TTL*, sets an upper limit on the number of routers through which a datagram can pass. It limits the lifetime of the datagram. It is initialized by the sender to some value (often 32 or 64) and decremented by one by every router that handles the datagram. When this field reaches 0, the datagram is thrown away, and the sender is notified with an ICMP message. This prevents packets from getting caught in routing loops forever



Datagram

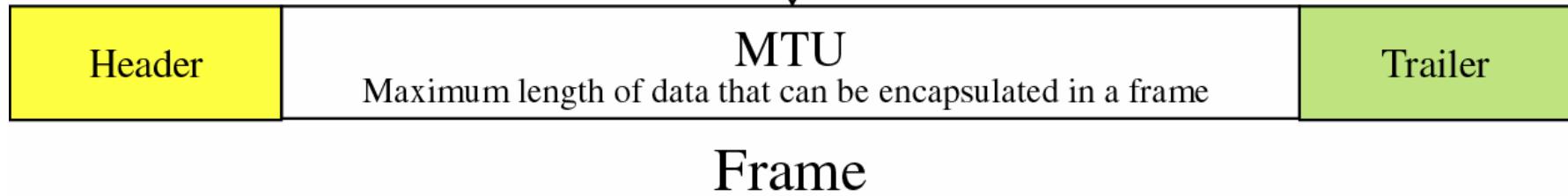
- The *header checksum* is calculated over the IP header only. It does *not* cover any data that follows the header. ICMP, IGMP, UDP, and TCP all have a checksum in their own headers to cover their header and data

Fragmentation

- MTU

Interface Number	MTU
.....

IP datagram



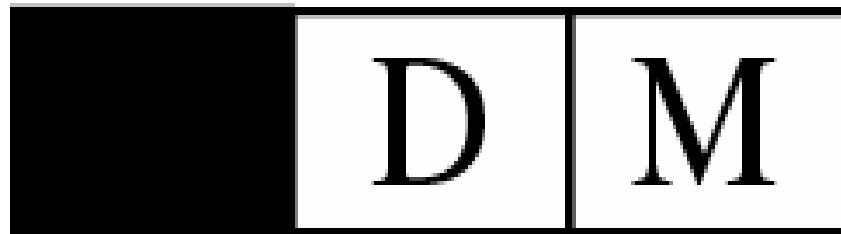


Fragmentation

- Flag field

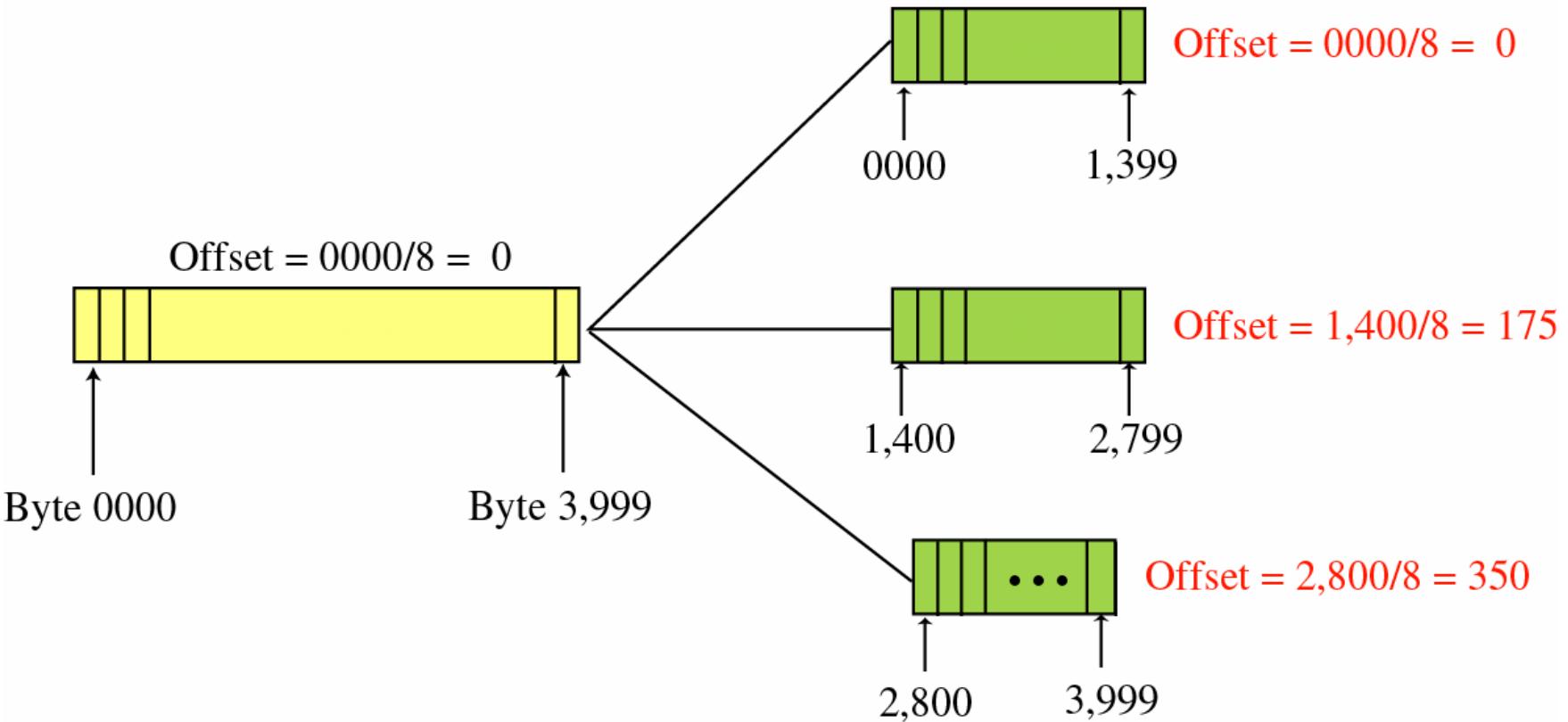
D: Do not fragment

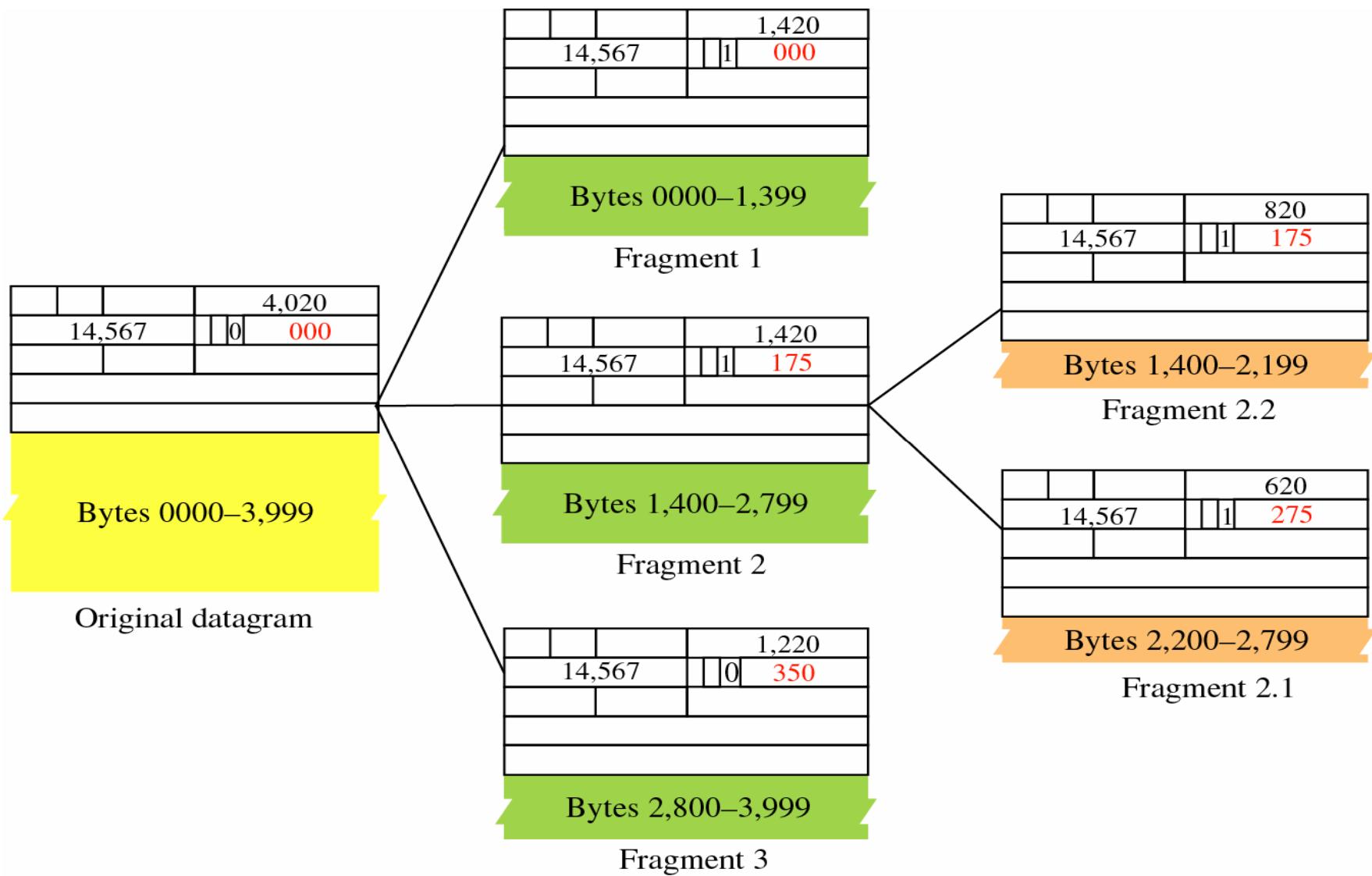
M: More fragments





Fragmentation

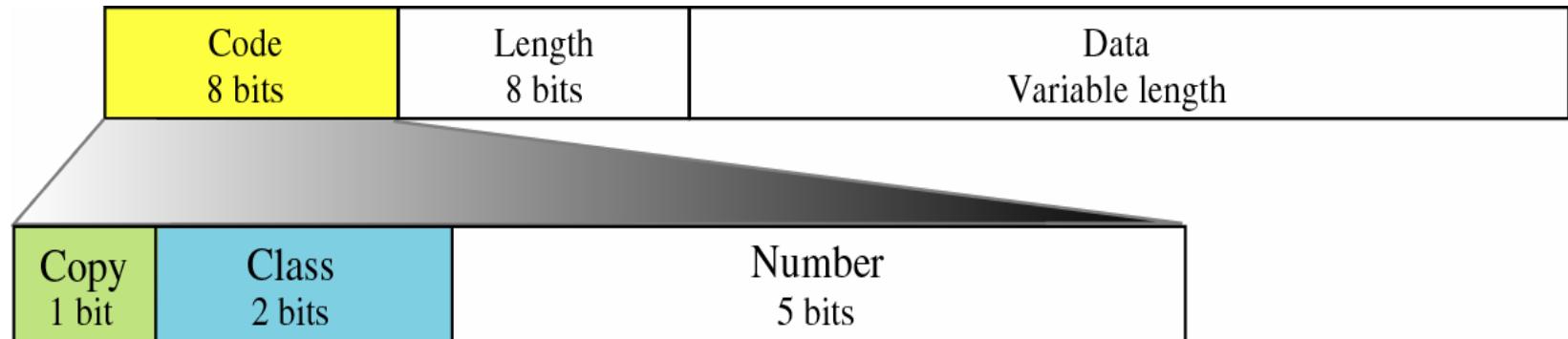






Option

Global CyberSoft



Copy

- 0 Copy only in first fragment
- 1 Copy into all fragments

Class

- 00 Datagram control
- 01 Reserved
- 10 Debugging and management
- 11 Reserved

Number

- 00000 End of option
- 00001 No operation
- 00011 Loose source route
- 00100 Timestamp
- 00111 Record route
- 01001 Strict source route

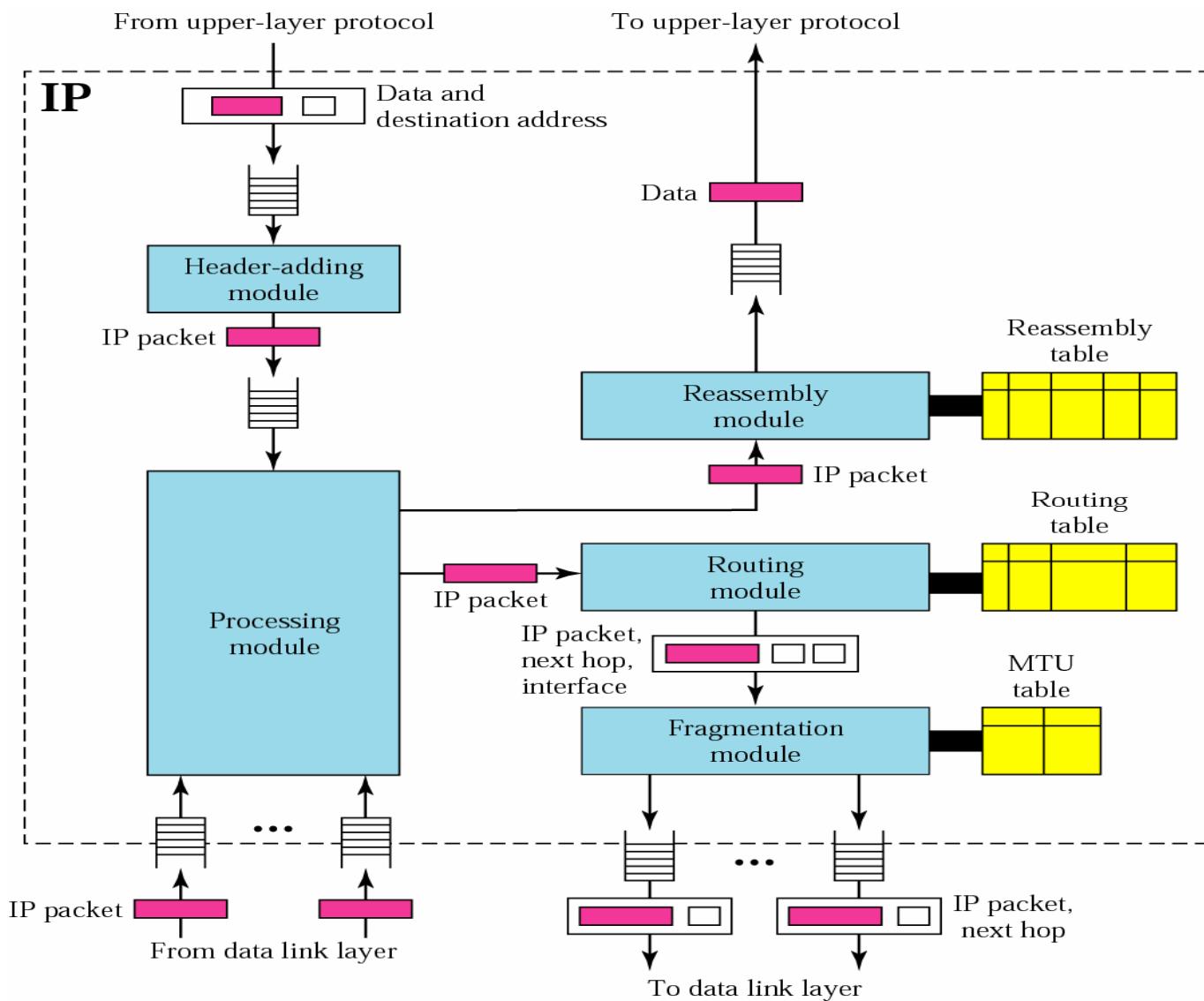


Checksum

- To create the checksum the sender does the following:
 - The packet is divided into k sections, each of n bits.
 - All sections are added together using one's complement arithmetic.
 - The final result is complemented to make the checksum.



IP package





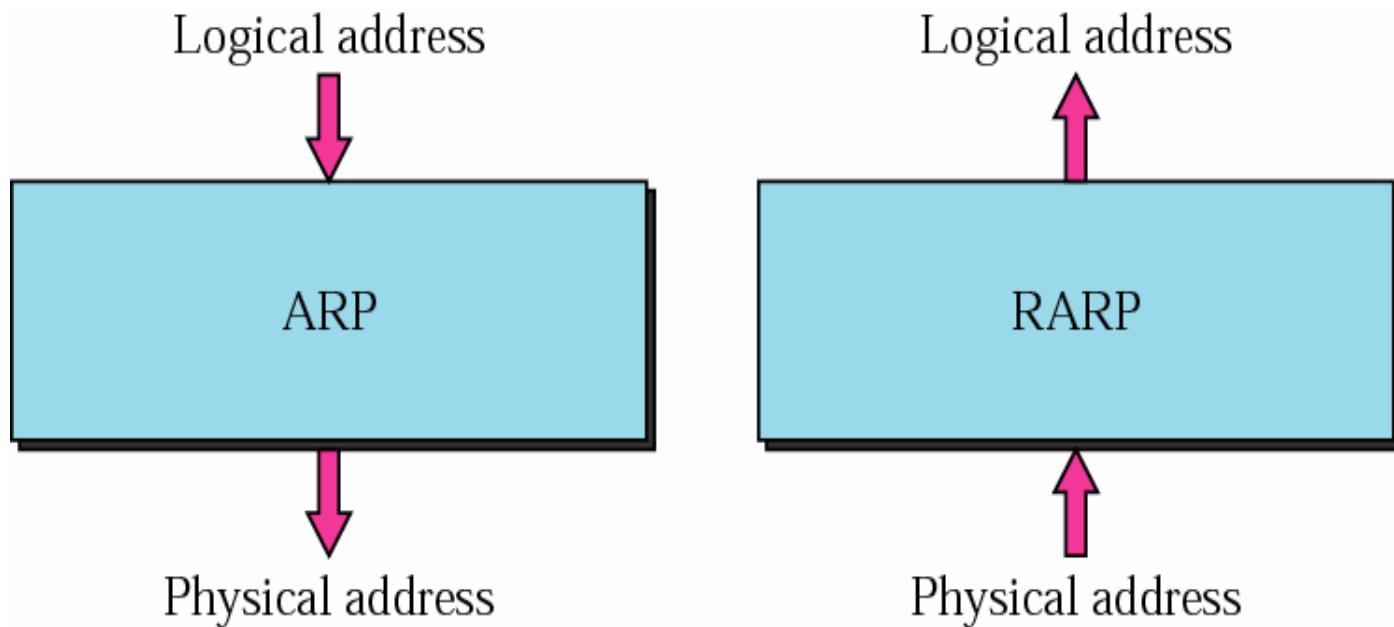
Global CyberSoft

ARP and RARP

- ARP
- ARP Package
- RARP



ARP and RARP

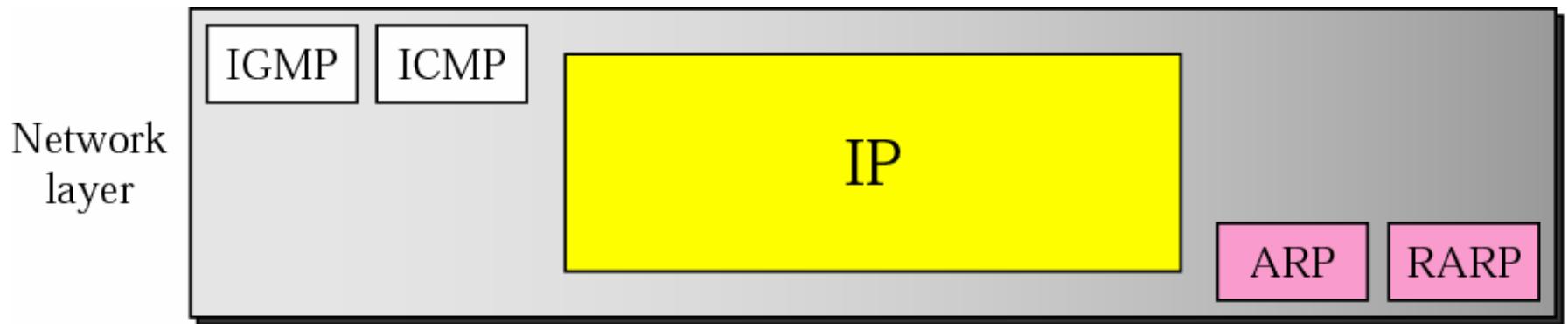




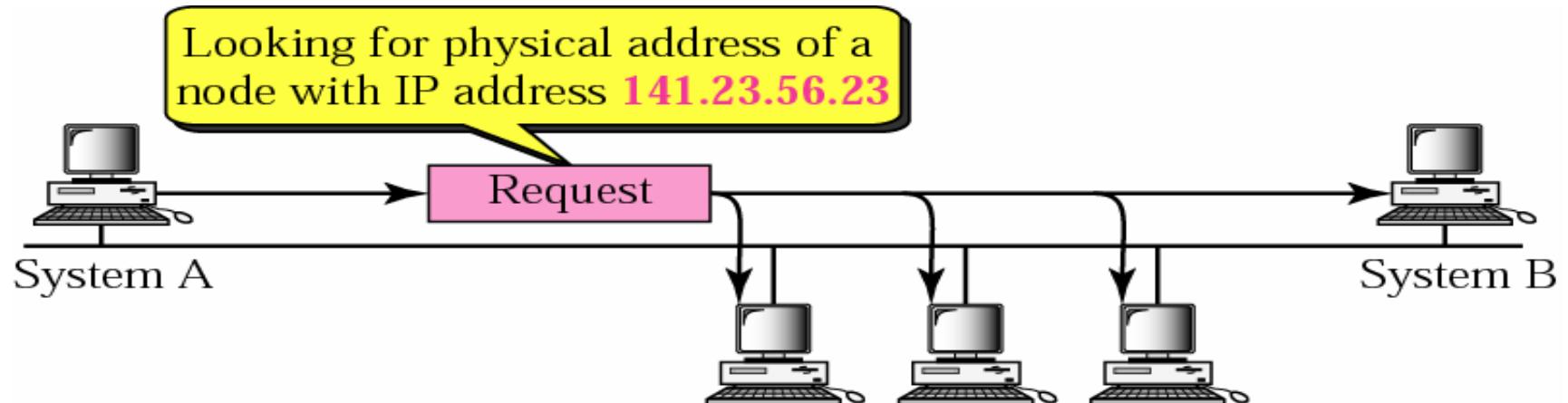
ARP and RARP

Global CyberSoft

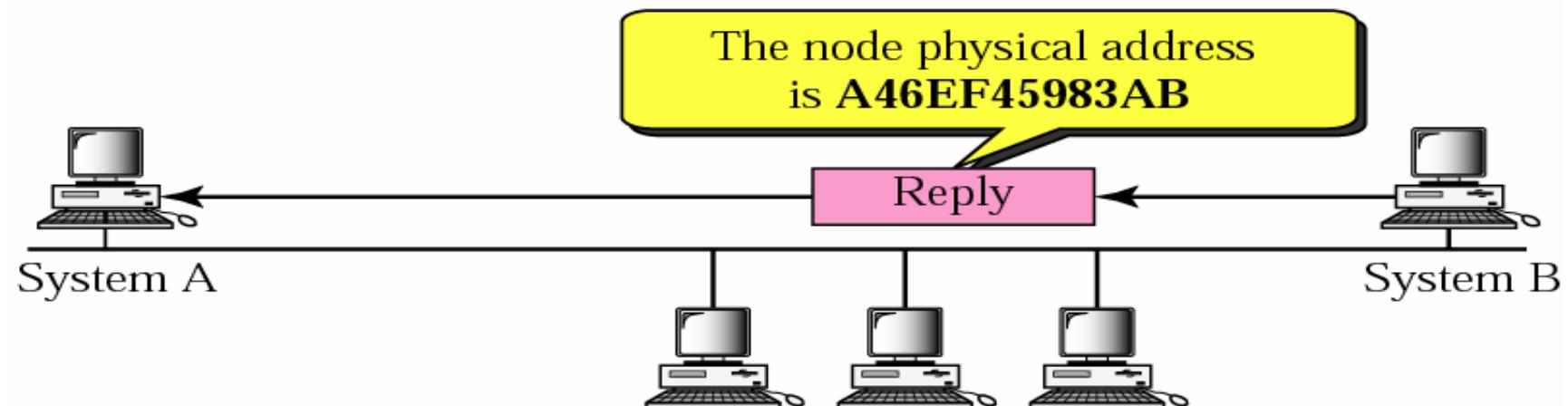
- Position of ARP and RARP in TCP/IP protocol suite



ARP: Operation



a. ARP request is broadcast



b. ARP reply is unicast



ARP: Packet

Hardware Type	Protocol Type
Hardware length	Protocol length
Sender hardware address (For example, 6 bytes for Ethernet)	
Sender protocol address (For example, 4 bytes for IP)	
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)	
Target protocol address (For example, 4 bytes for IP)	

ARP: Four using cases

Target IP address:

Destination address in the IP datagram

Sender



Host

• • •

LAN

Host



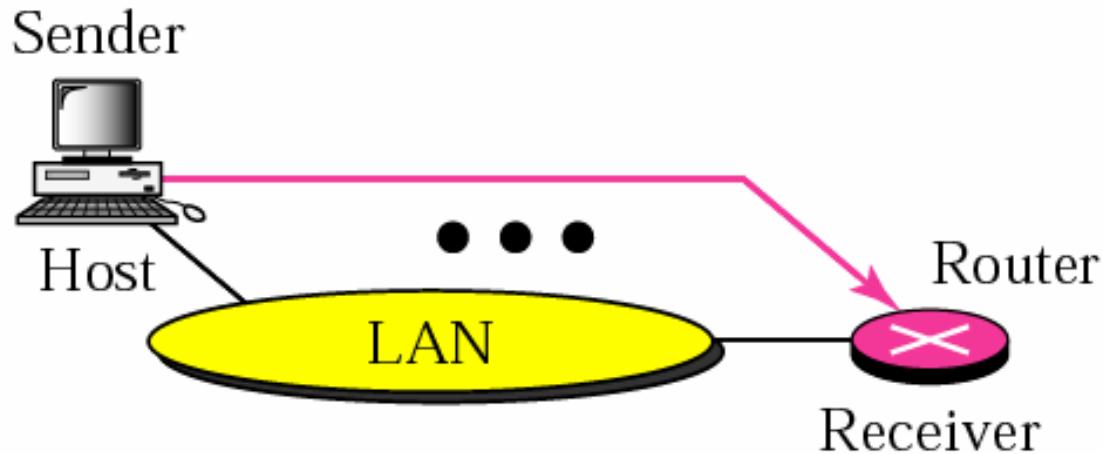
Receiver

Case 1. A host has a packet to send to another host on the same network.



ARP: Four using cases

Target IP address:
IP address of a router

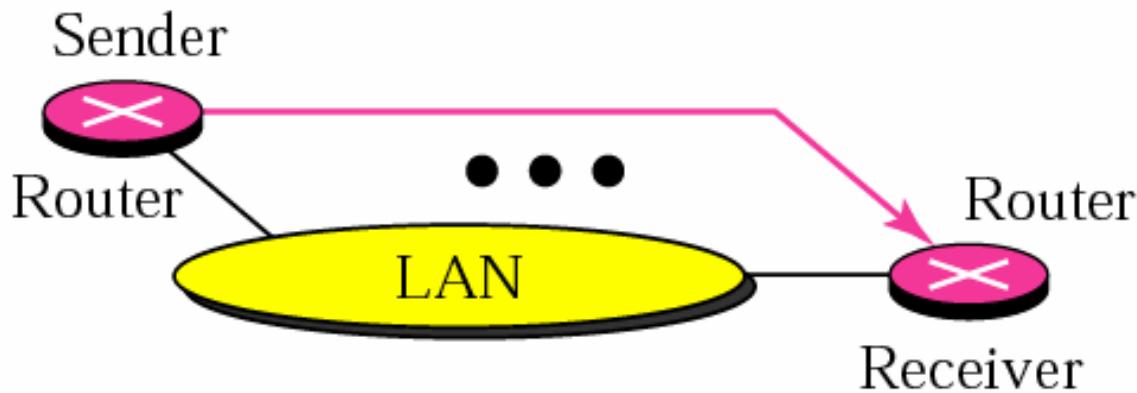


Case 2. A host wants to send a packet to another host on another network.
It must first be delivered to a router.

ARP: Four using cases

Target IP address:

IP address of the appropriate router
found in the routing table



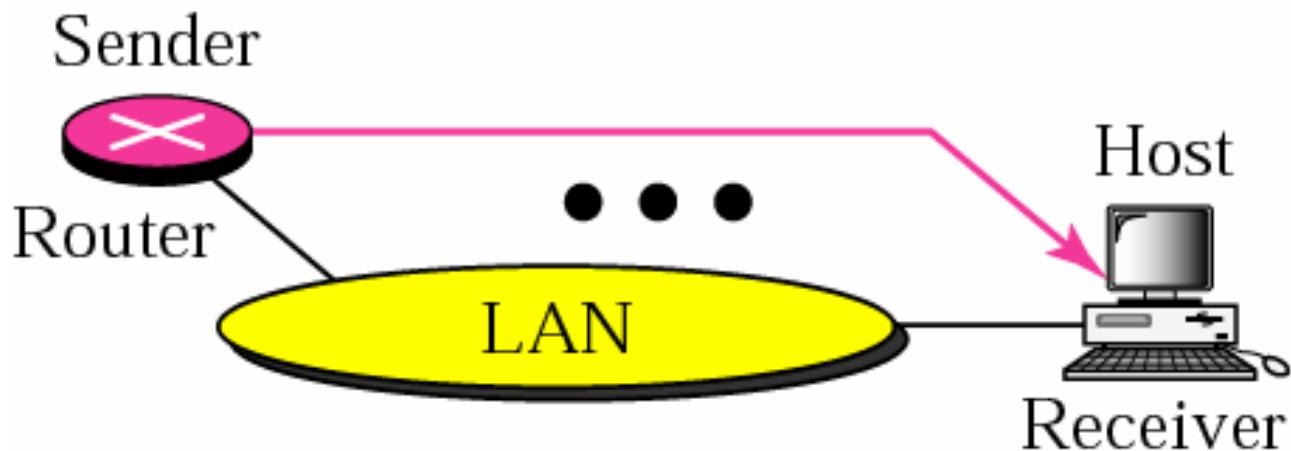
Case 3. A router receives a packet to be sent to a host on another network.

It must first be delivered to the appropriate router.

ARP: Four using cases

Target IP address:

Destination address in the IP datagram



Case 4. A router receives a packet to be sent to a host on the same network.



Note

*An ARP request is **broadcast**;*
*an ARP reply is **unicast**.*



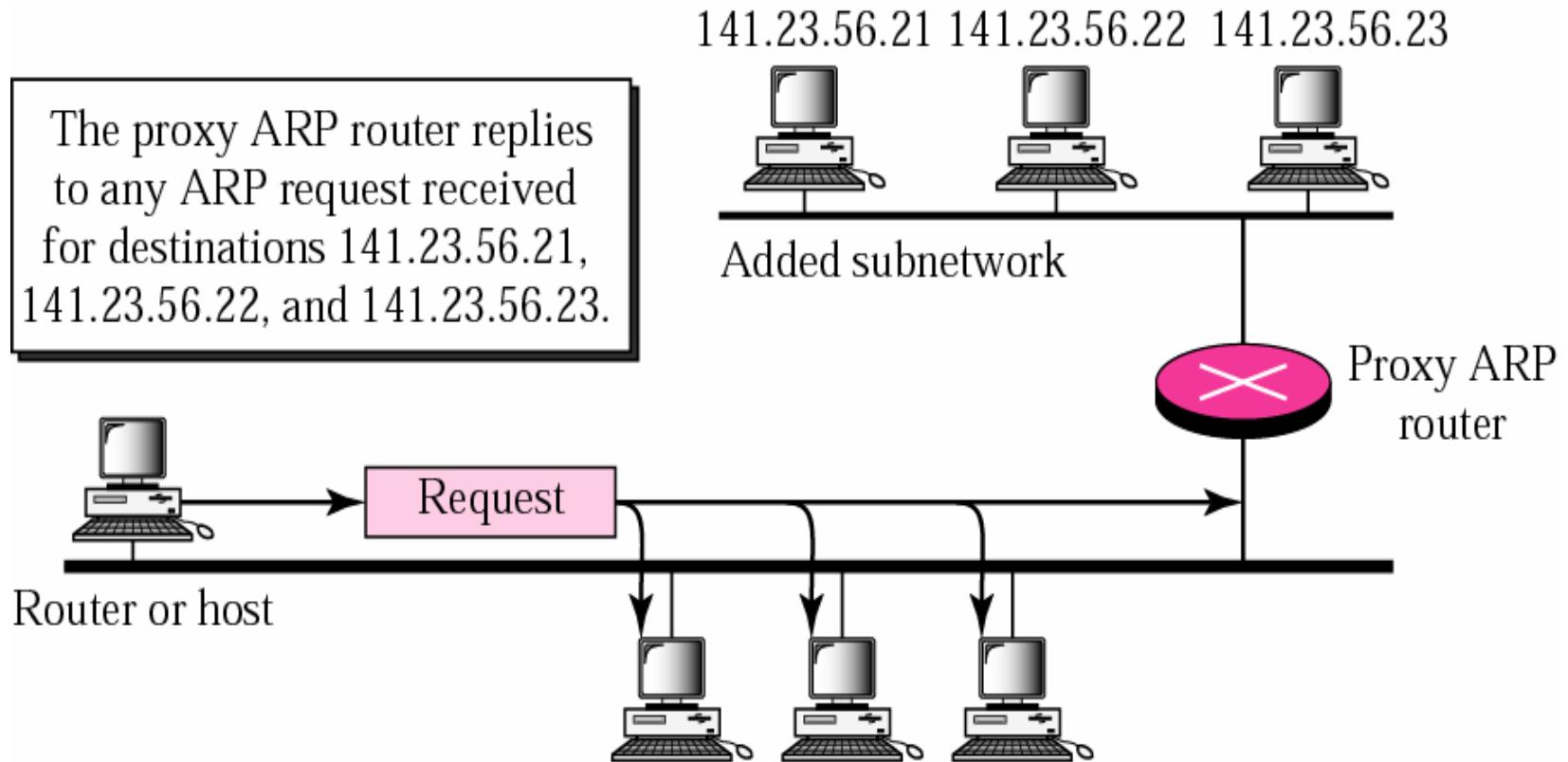
Global CyberSoft

Traffic Example

- 0:0:c0:6f:2d:40 ff:ff:ff:ff:ff:ff arp 60:
arp who-has svr4 tell bsdi 20.002174 (0.0022)
0:0:c0:c2:9b:26 0:0:c0:6f:2d:40 arp 60: arp reply
svr4 is-at 0:0:c0:c2:9b:26

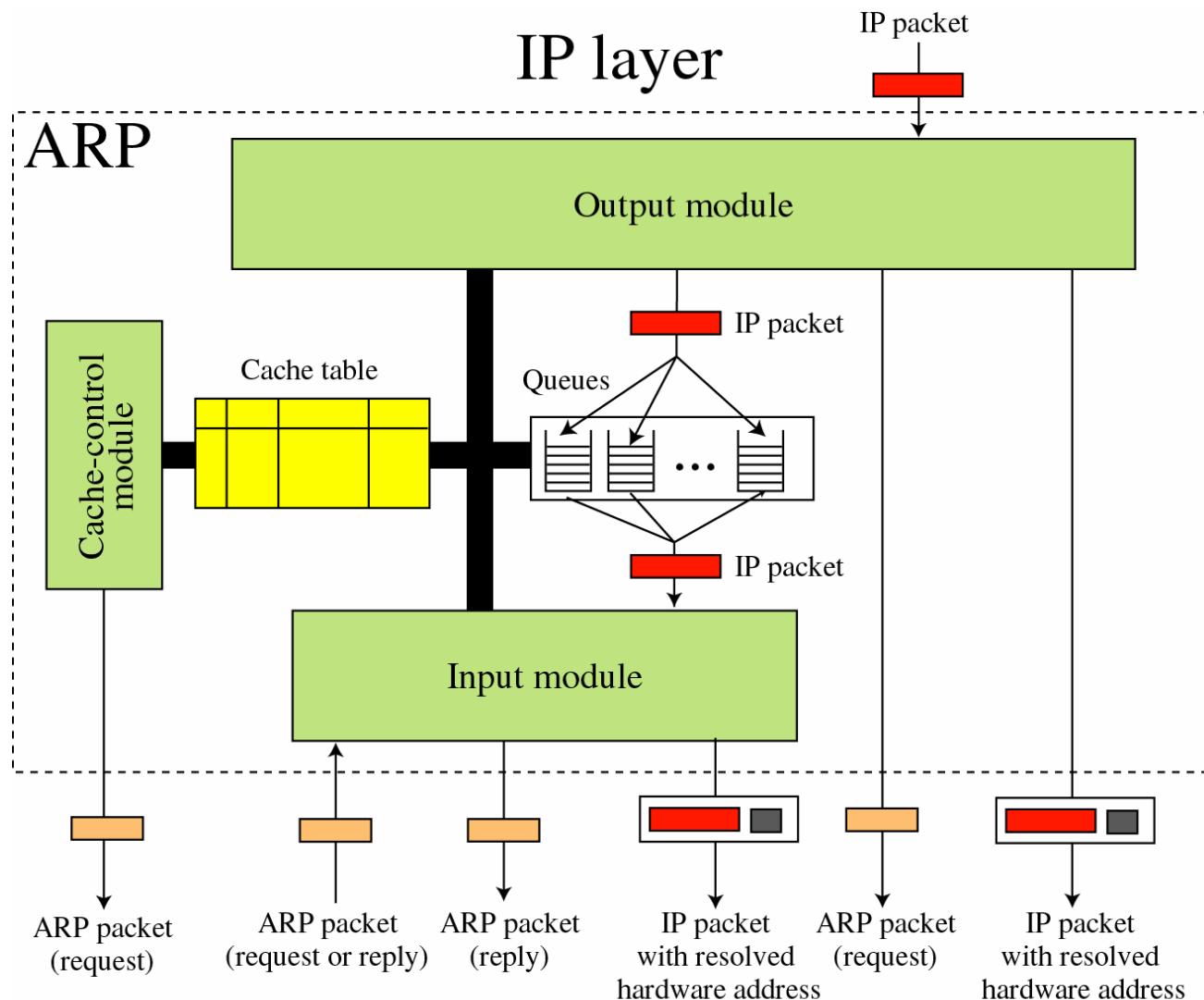
Proxy ARP

The proxy ARP router replies to any ARP request received for destinations 141.23.56.21, 141.23.56.22, and 141.23.56.23.



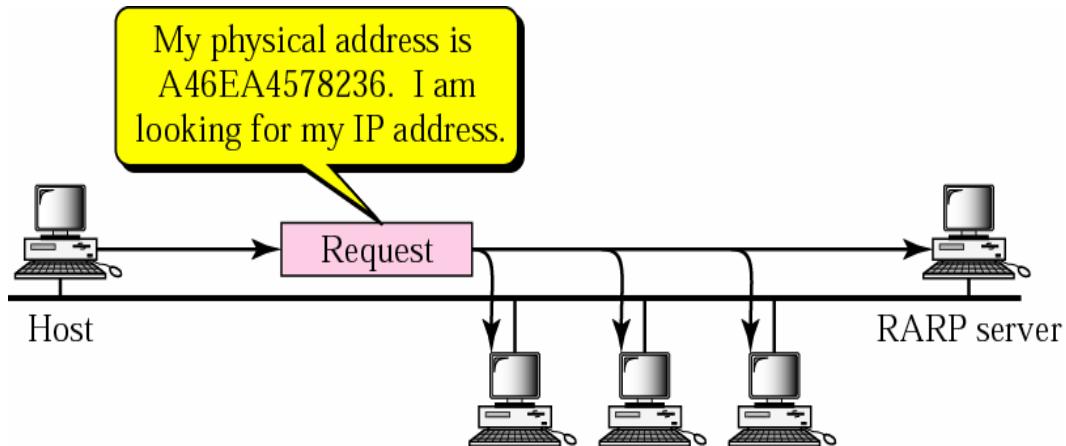


ARP Package

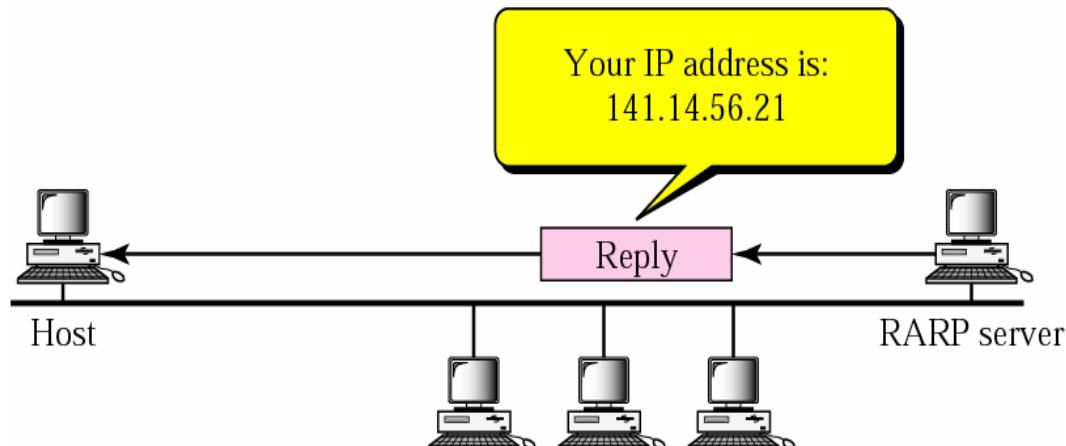


Data link layer

RARP: Operation



a. RARP request is broadcast



b. RARP reply is unicast



Note

*The RARP request packets are **broadcast**;
the RARP reply packets are **unicast**.*



RARP Packet

Global CyberSoft

Hardware type	Protocol type	
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP) (It is not filled for request)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled for request)		
Target protocol address (For example, 4 bytes for IP) (It is not filled for request)		

RARP: Alternative Solution

- When a diskless computer is booted, it needs more information in addition to its IP address. It needs to know its subnet mask, the IP address of a router, and the IP address of a name server. RARP cannot provide this extra information. New protocols have been developed to provide this information, BOOTP and DHCP, that can be used instead of RARP.



BOOTP and DHCP

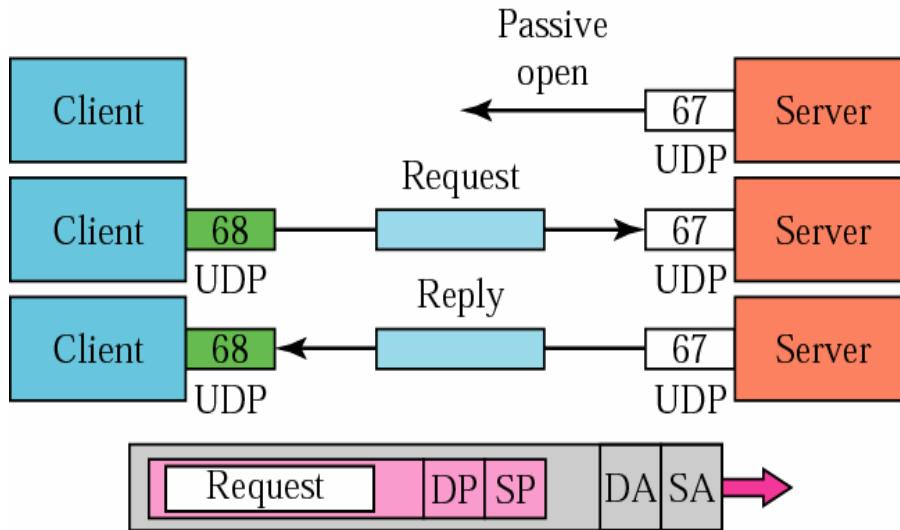
- BOOTP
- DHCP



BOOTP Packet Format

Operation code	Hardware type	Hardware length	Hop count		
Transaction ID					
Number of seconds		Unused			
Client IP address					
Your IP address					
Server IP address					
Gateway IP address					
Client hardware address (16 bytes)					
Server name (64 bytes)					
Boot file name (128 bytes)					
Options					

BOOTP Operation



SP: Source port (68)

DP: Destination port (67)

SA: Source address (All 0s)

DA: Destination address (All 1s)



SP: Source port (67)

DP: Destination port (68)

SA: Source address (Server unicast address)

DA: Destination address (All 1s or client unicast address)

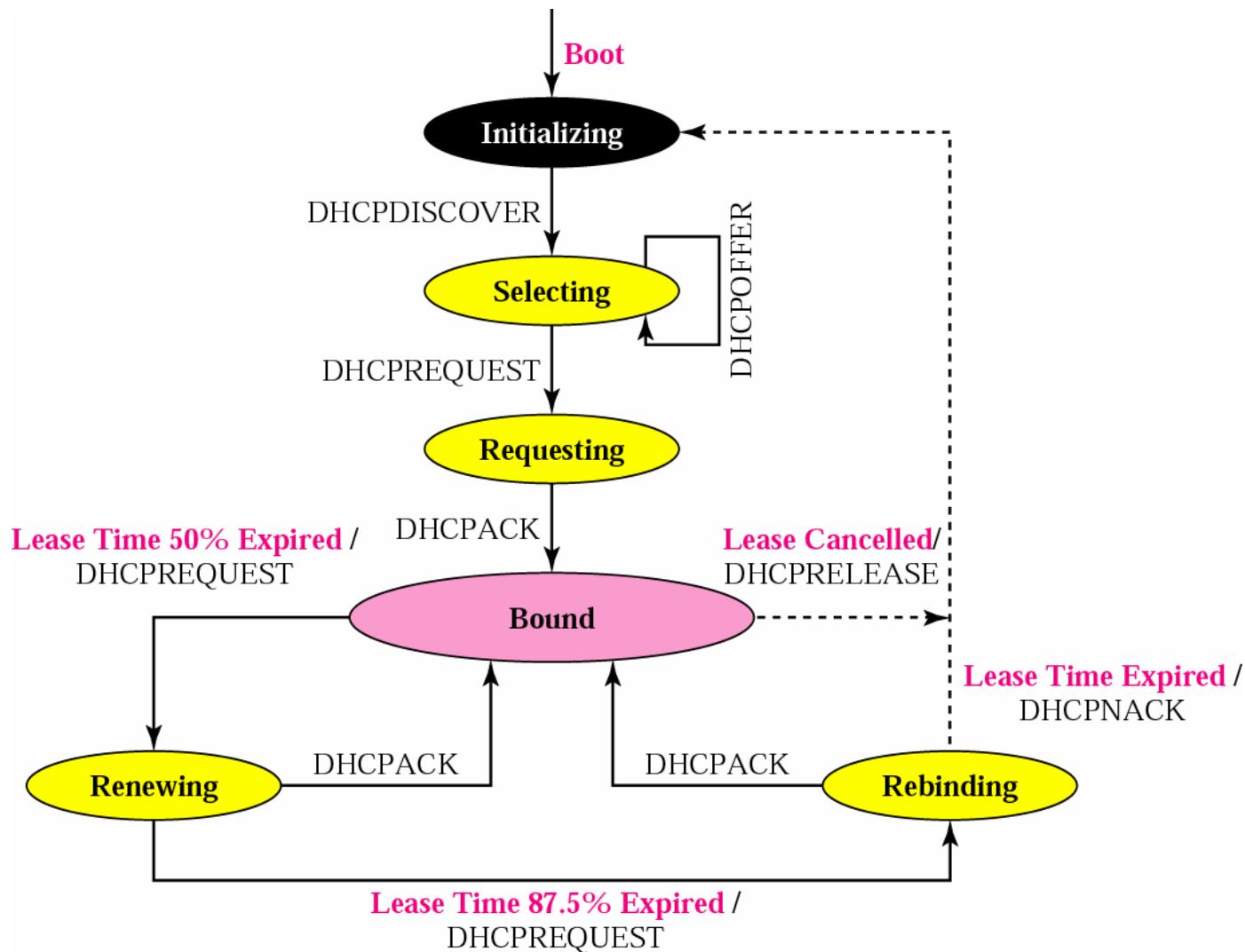


DHCP Packet

Operation code	Hardware type	Hardware length	Hop count
Transaction ID			
Number of seconds	F	Unused	
Client IP address			
Your IP address			
Server IP address			
Gateway IP address			
Client hardware address (16 bytes)			
Server name (64 bytes)			
Boot file name (128 bytes)			
Options (Variable length)			

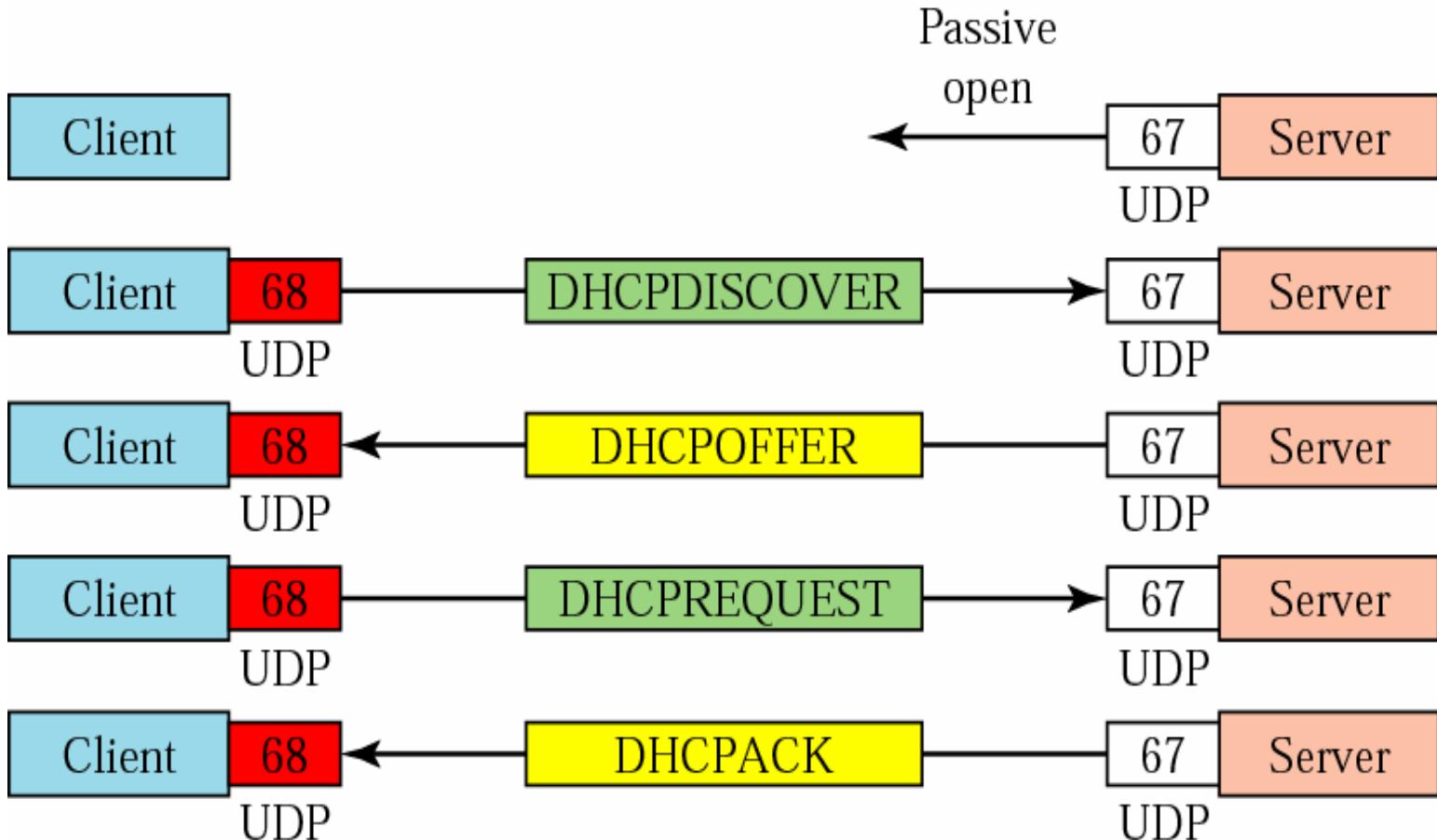


DHCP Transition Diagram

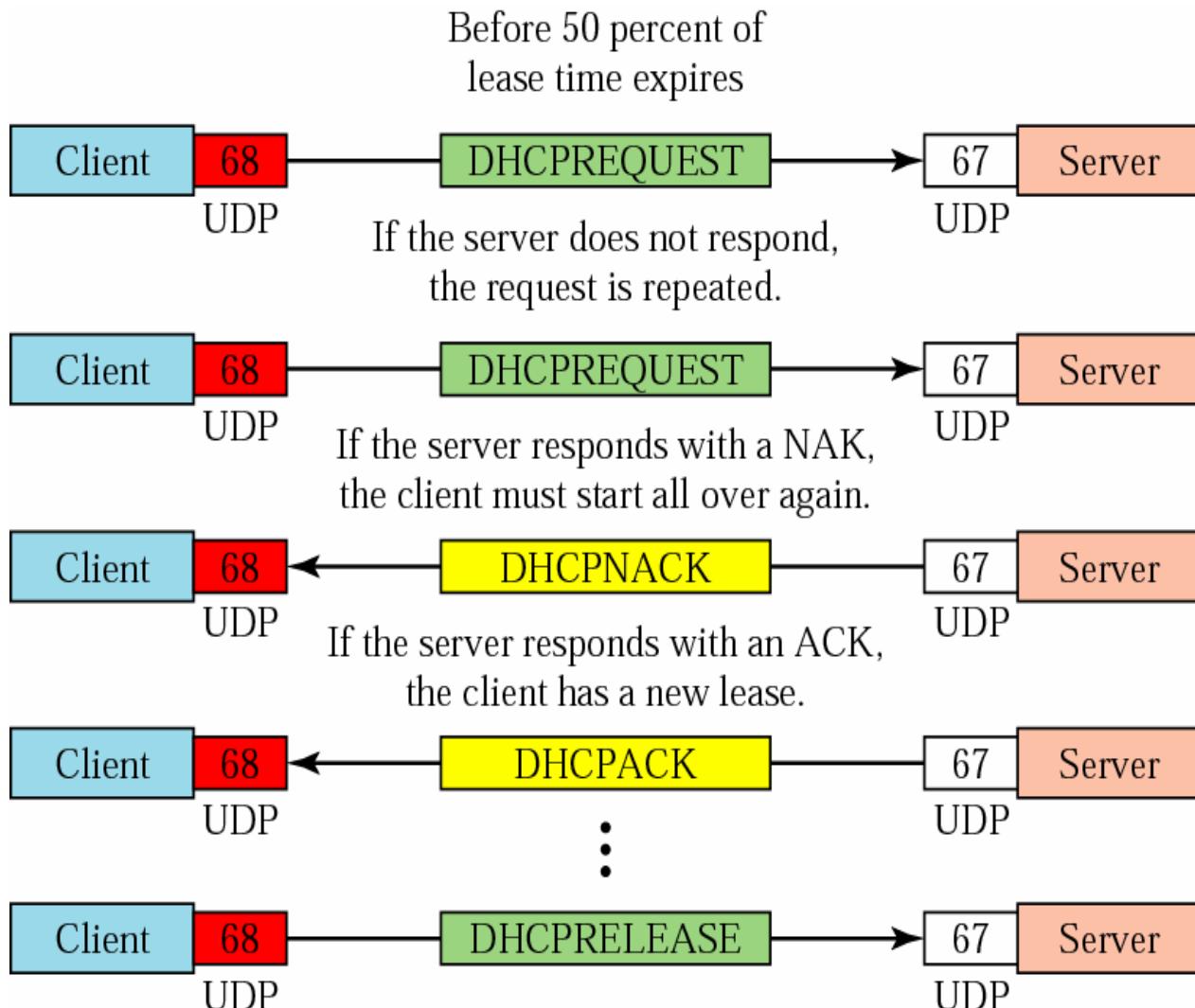




DHCP: Exchange Message Part I



DHCP: Exchange Message Part I



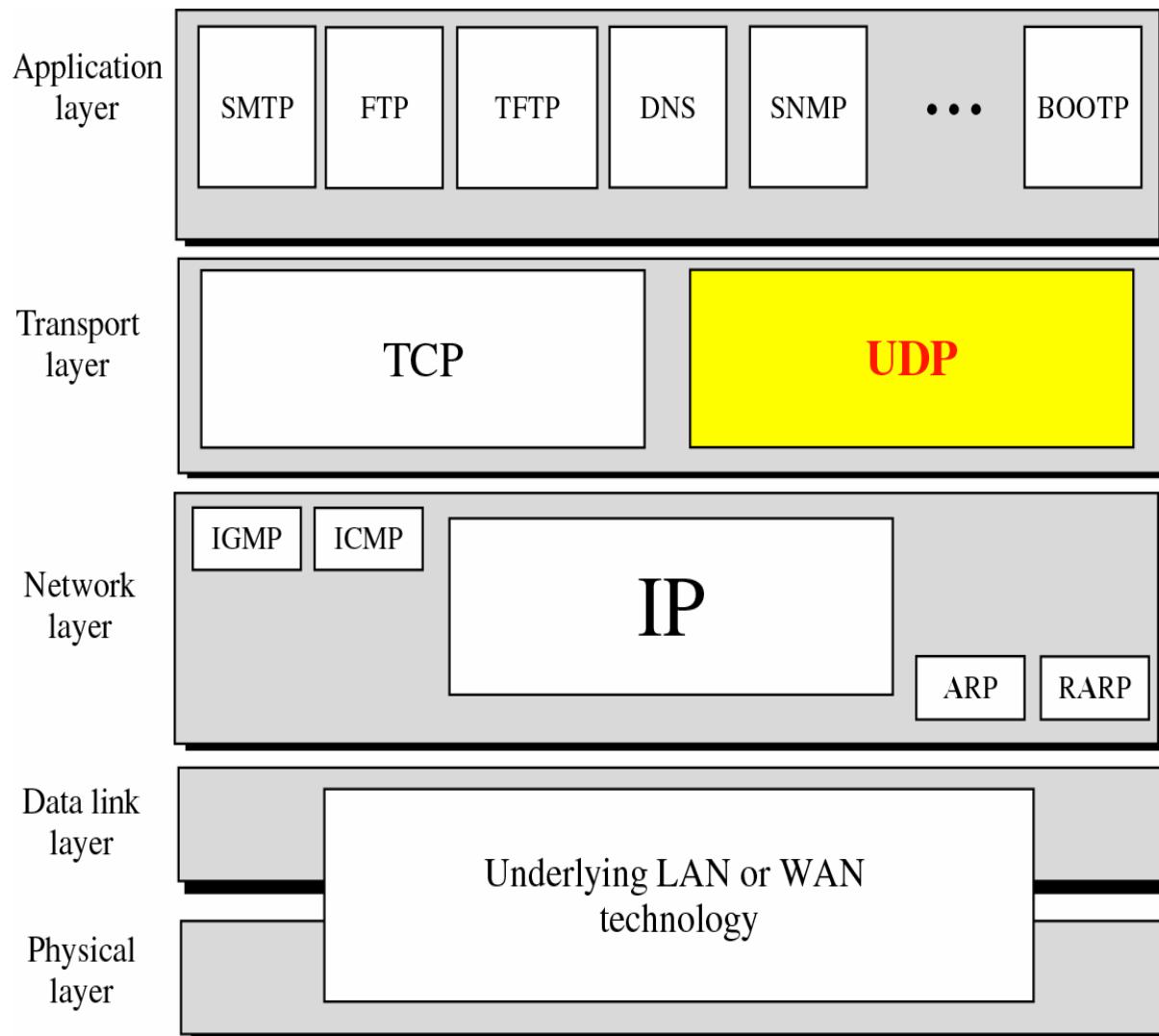


Global CyberSoft

User Datagram Protocol

- PROCESS-TO-PROCESS COMMUNICATION
- USER DATAGRAM
- CHECKSUM
- UDP OPERATION
- UDP PACKAGE

UDP: Position in TCP/IP protocol suite





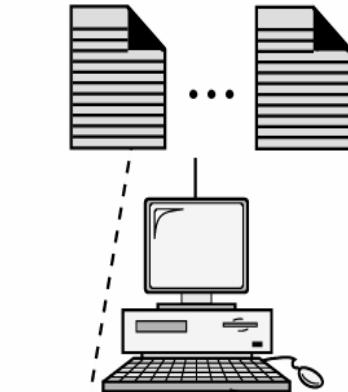
Global CyberSoft

Process to process communication

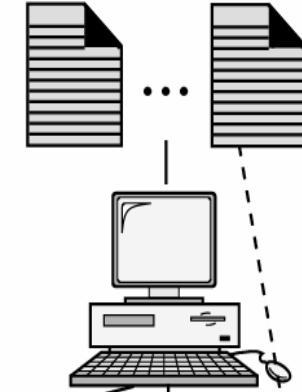
- UDP versus IP
- Port Number
- Socket Address

UDP versus IP

Processes
(Running application programs)



Processes
(Running application programs)



Internet

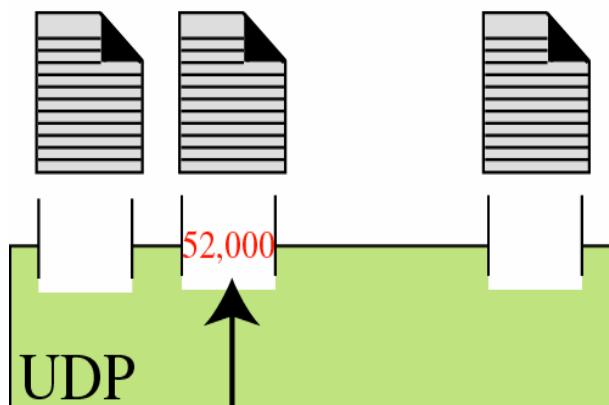
Domain of IP protocol

Domain of UDP protocol

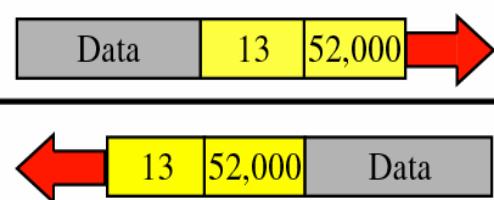
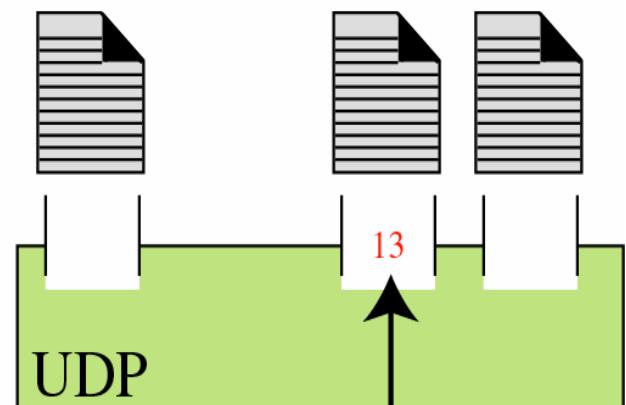


Port Number

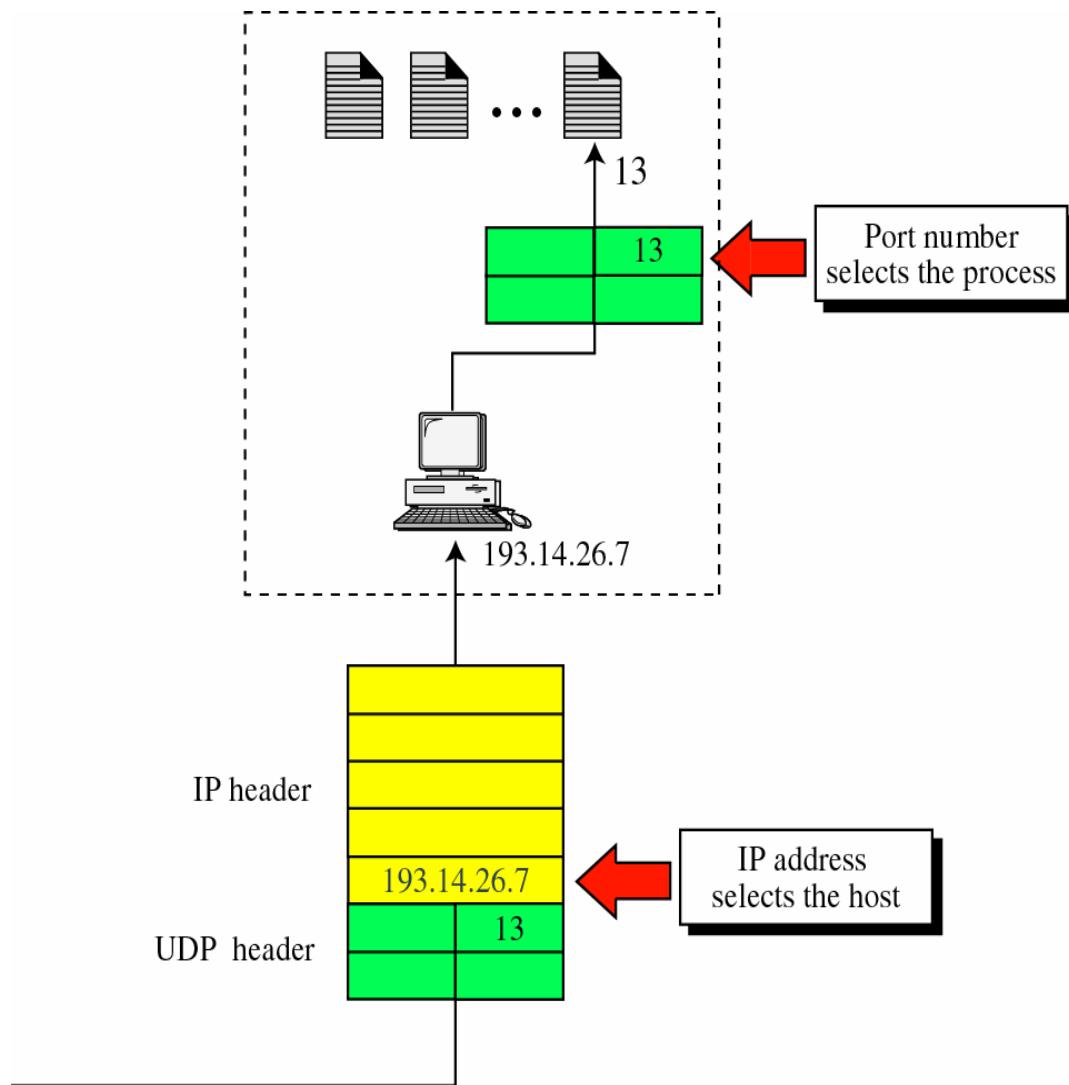
Daytime
client



Daytime
server



IP Address versus port number





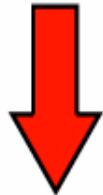
Socket Address

IP address

200.23.56.8

Port number

69



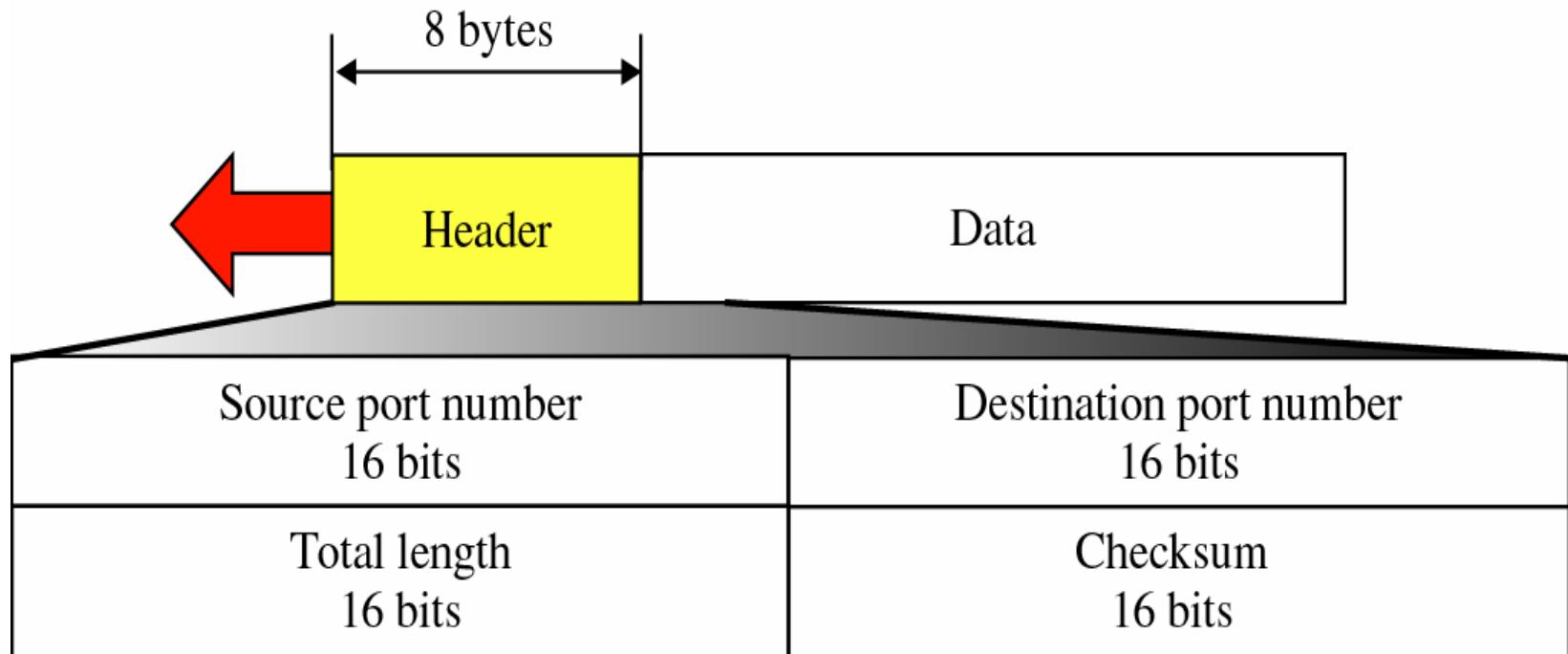
200.23.56.8

69

Socket address



User Datagram Format





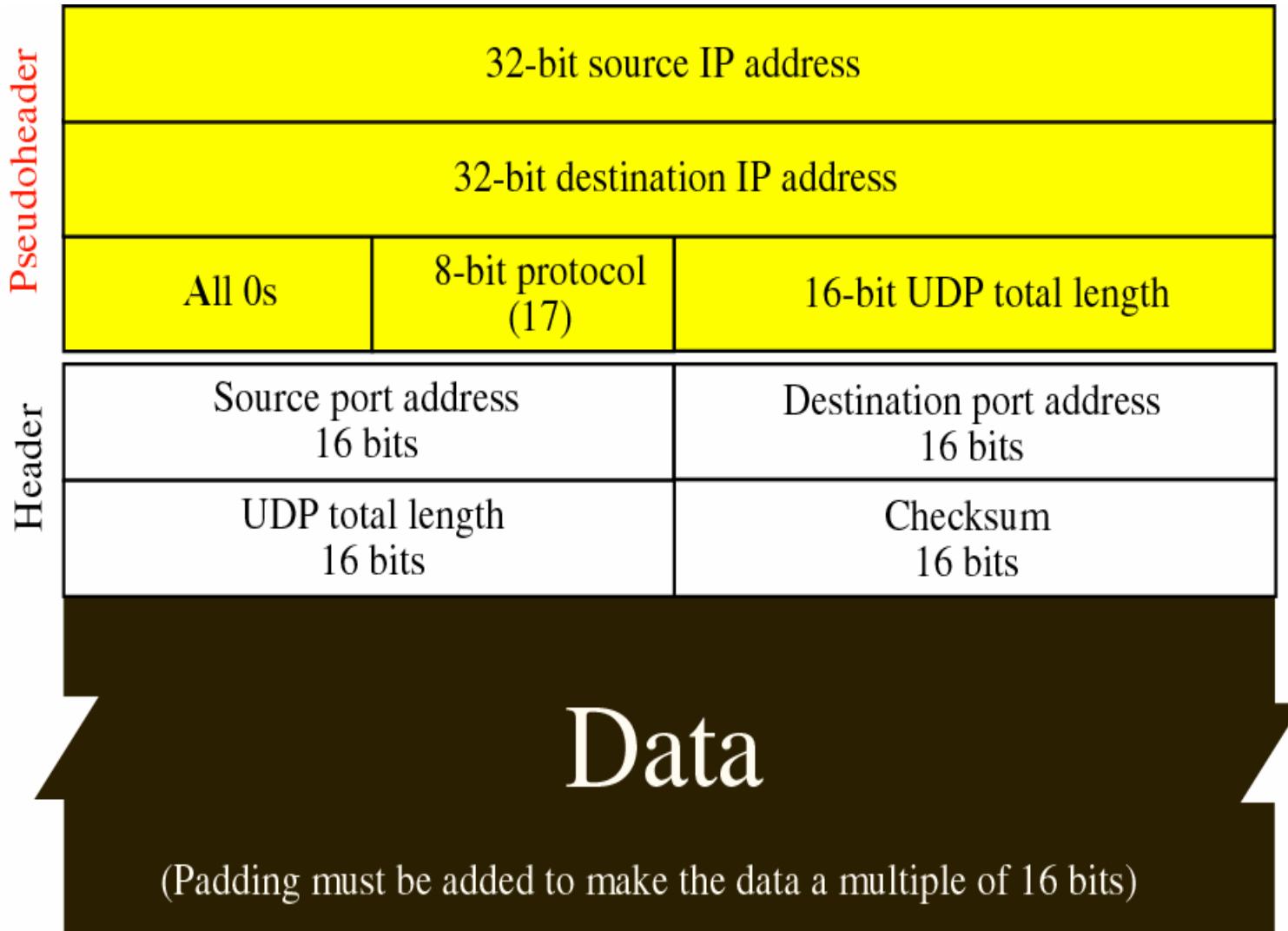
User Datagram Format

Note

*UDP length =
IP length - IP header's length*

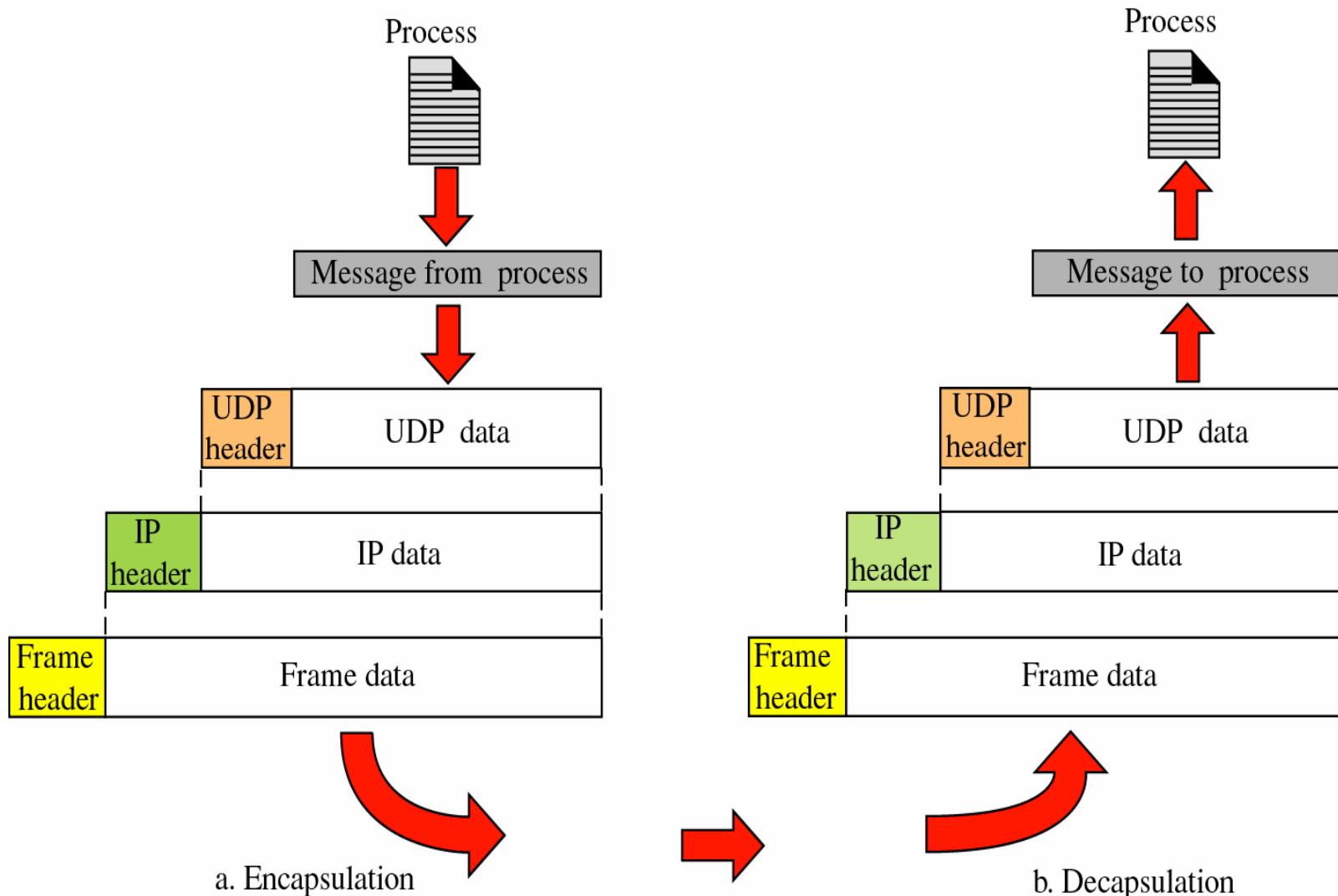


Pseudo header added to UDP datagram



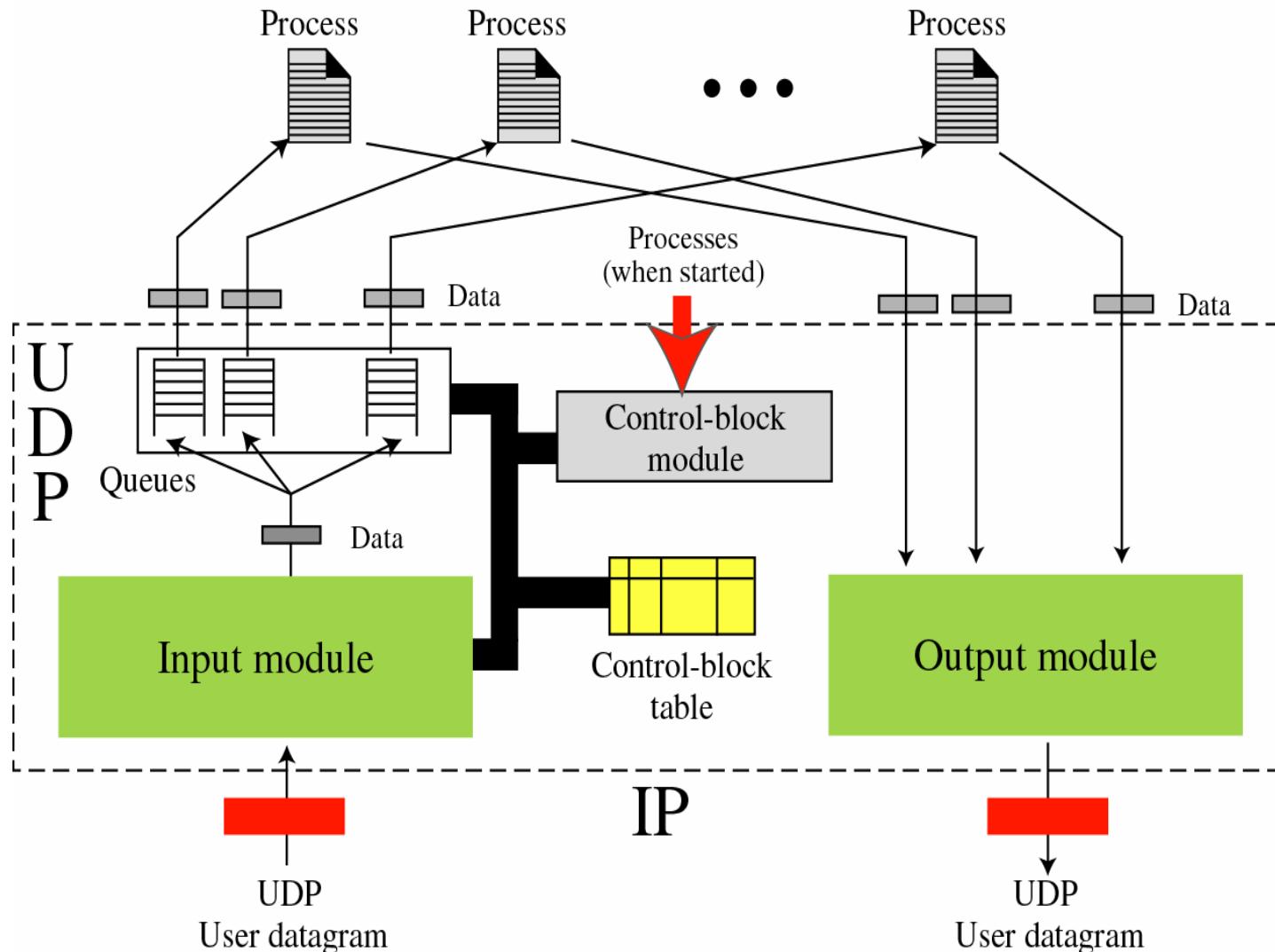


Encapsulation and Decapsulation





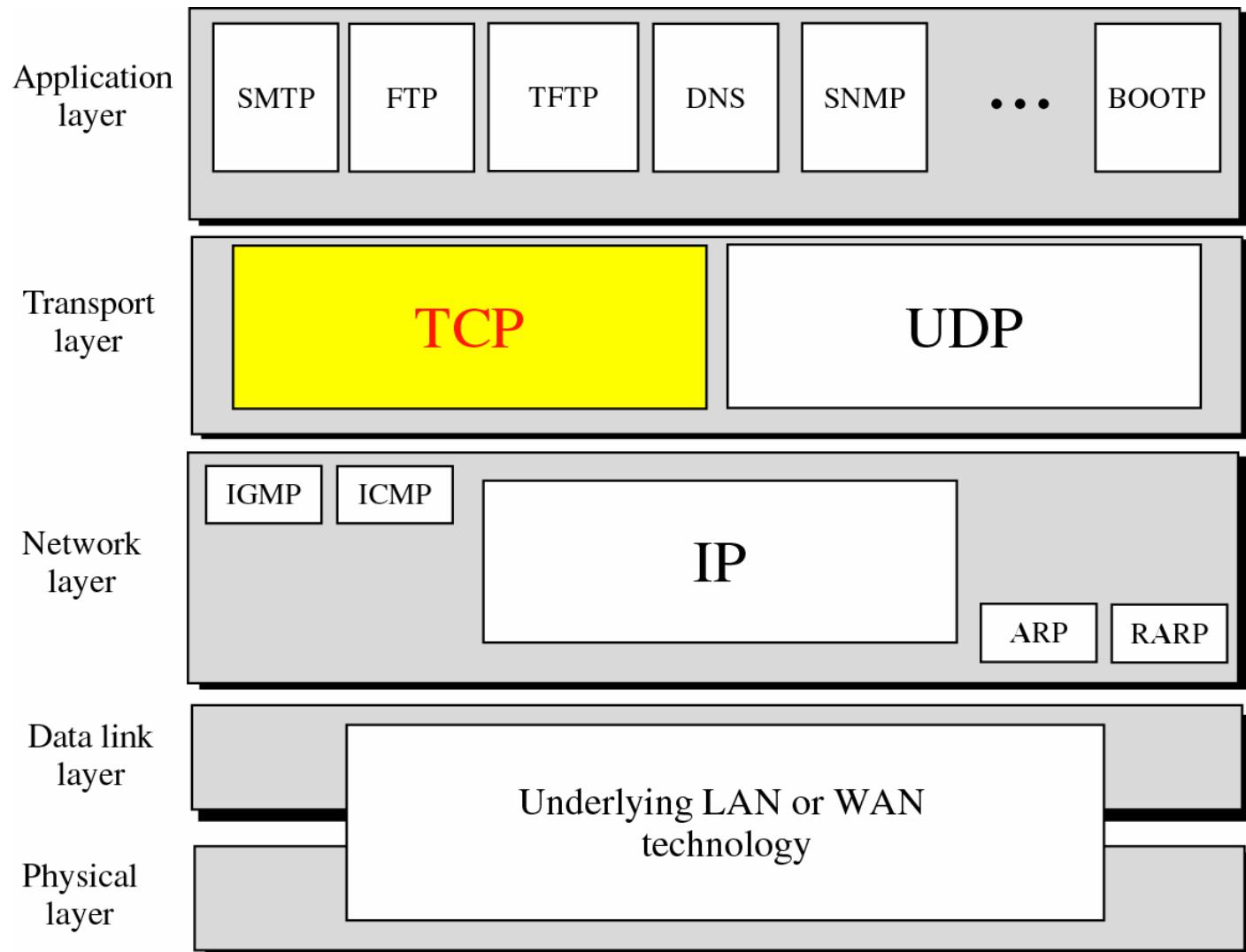
UDP Package



Transmission Control Protocol

- PROCESS-TO-PROCESS COMMUNICATION
- TCP SERVICES
- NUMBERING BYTES
- FLOW CONTROL
- SILLY WINDOW SYNDROME
- ERROR CONTROL
- TCP TIMERS
- CONGESTION CONTROL
- SEGMENT
- OPTIONS
- CHECKSUM
- CONNECTION
- STATE TRANSITION DIAGRAM
- TCP OERATION
- TCP PACKAGE

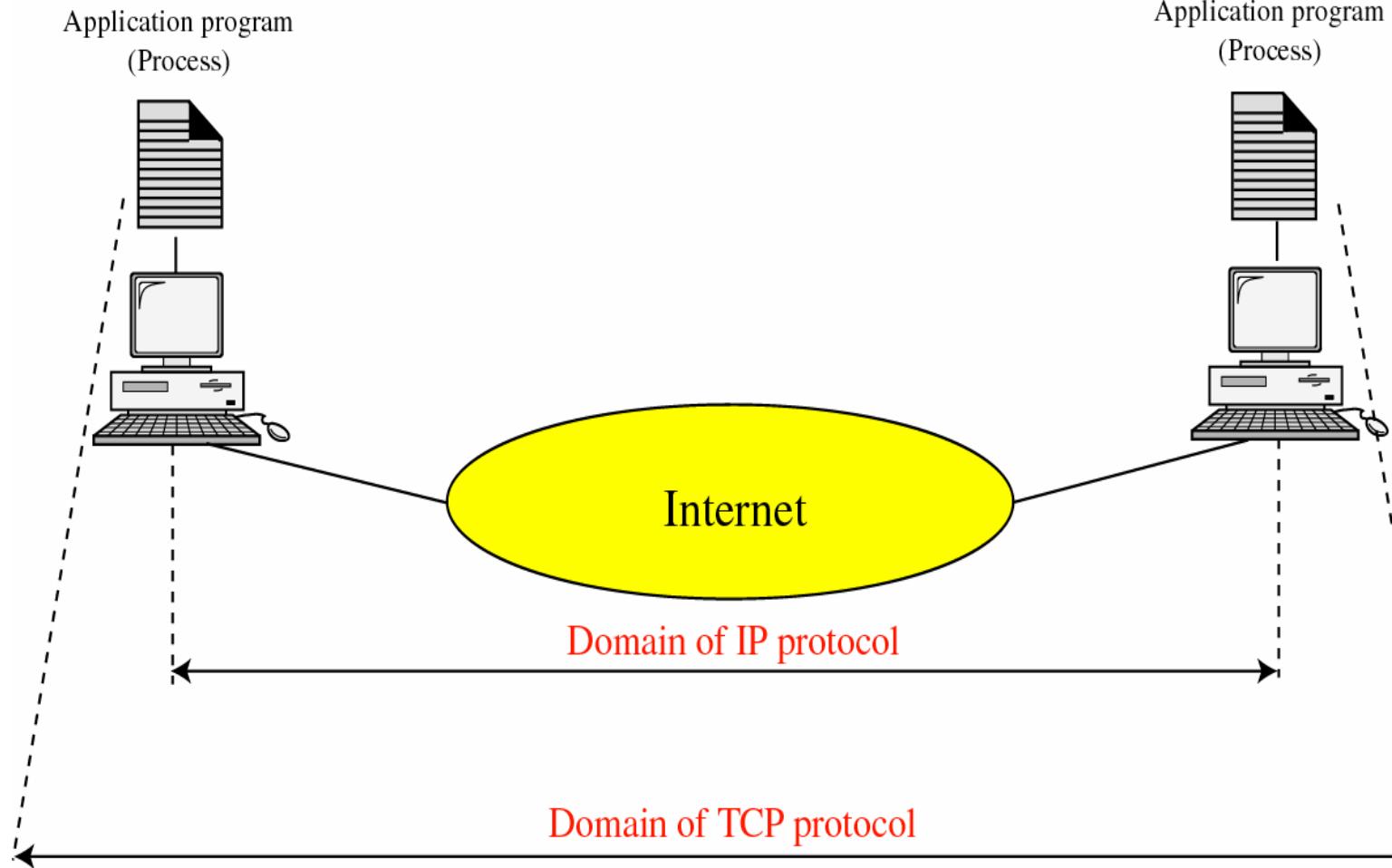
Position in TCP/IP protocol suite





Process to process communication

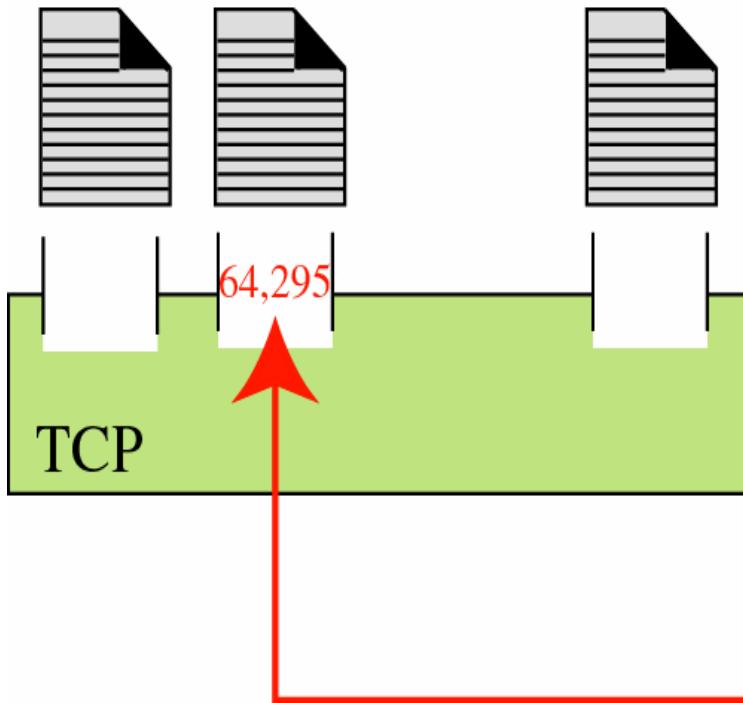
TCP versus IP



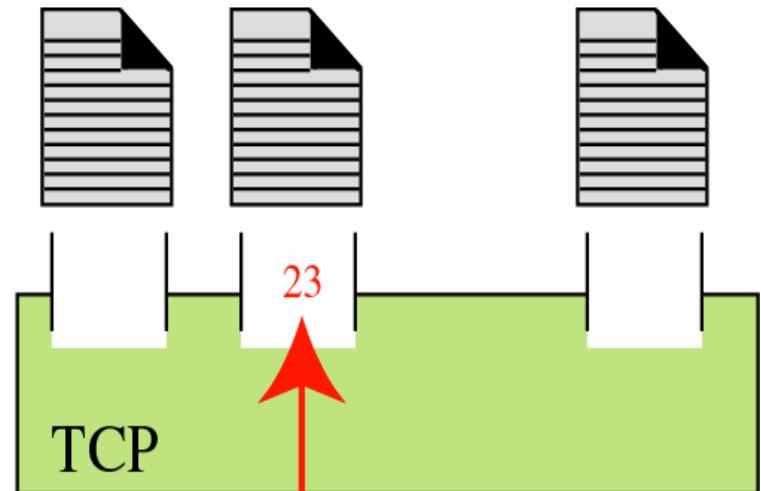


Port Number

TELNET
(Client)

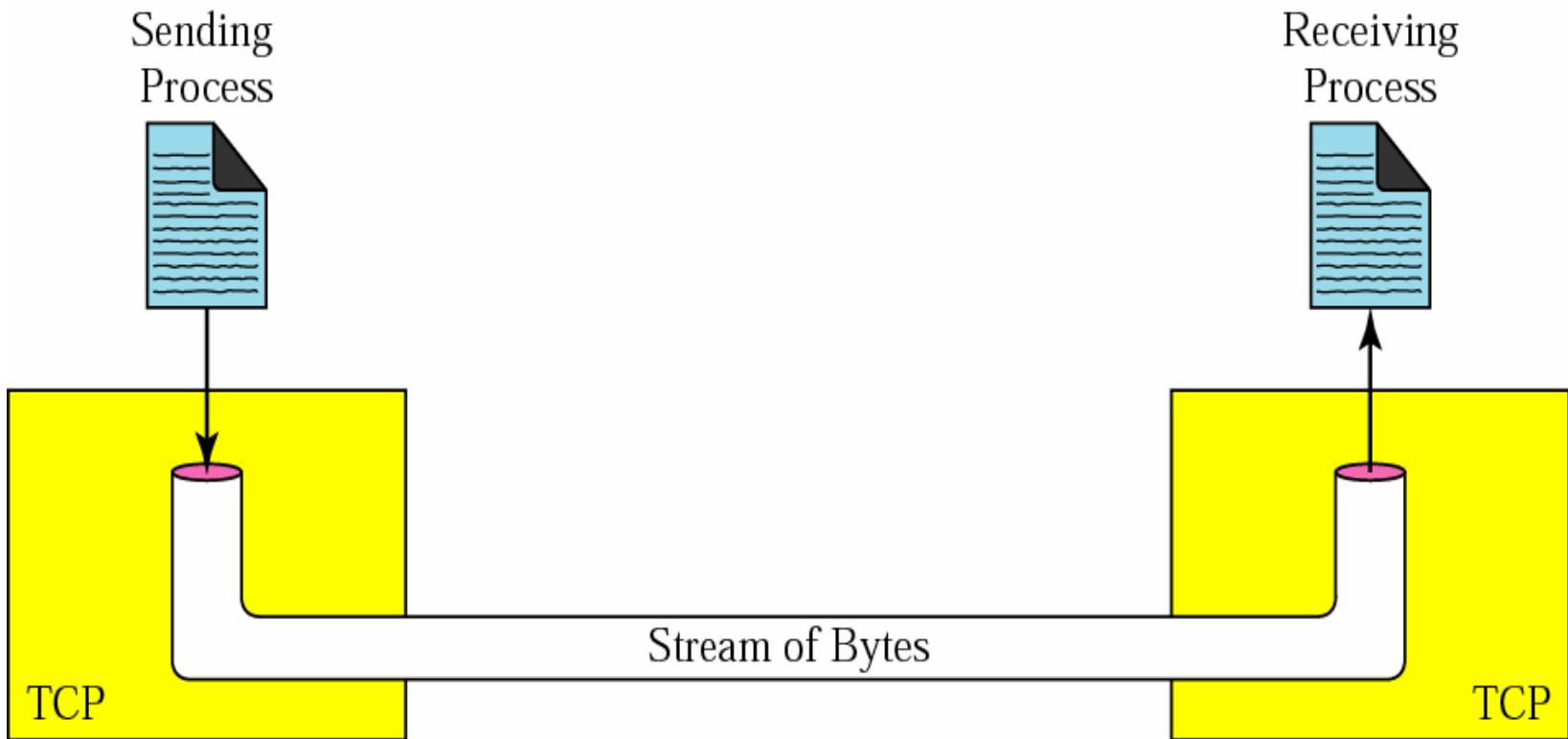


TELNET
(Server)



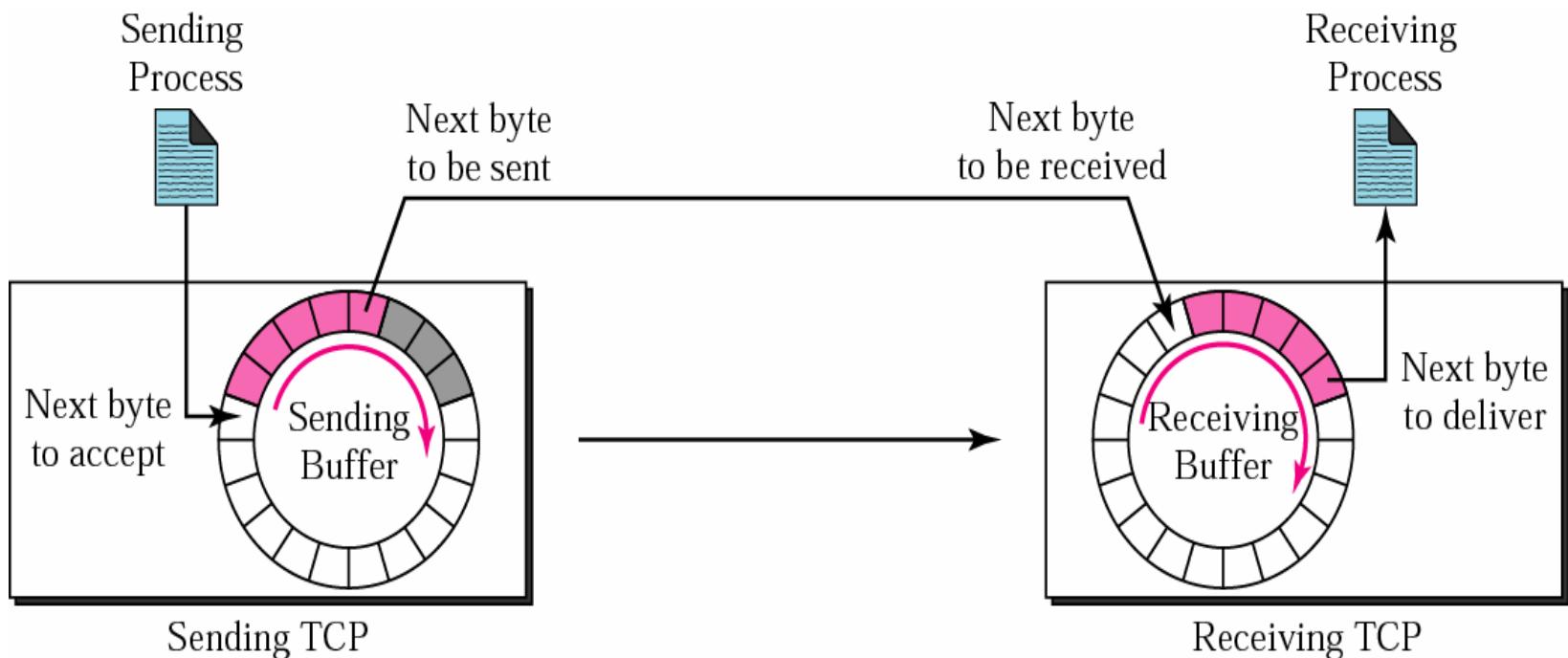


Stream delivery



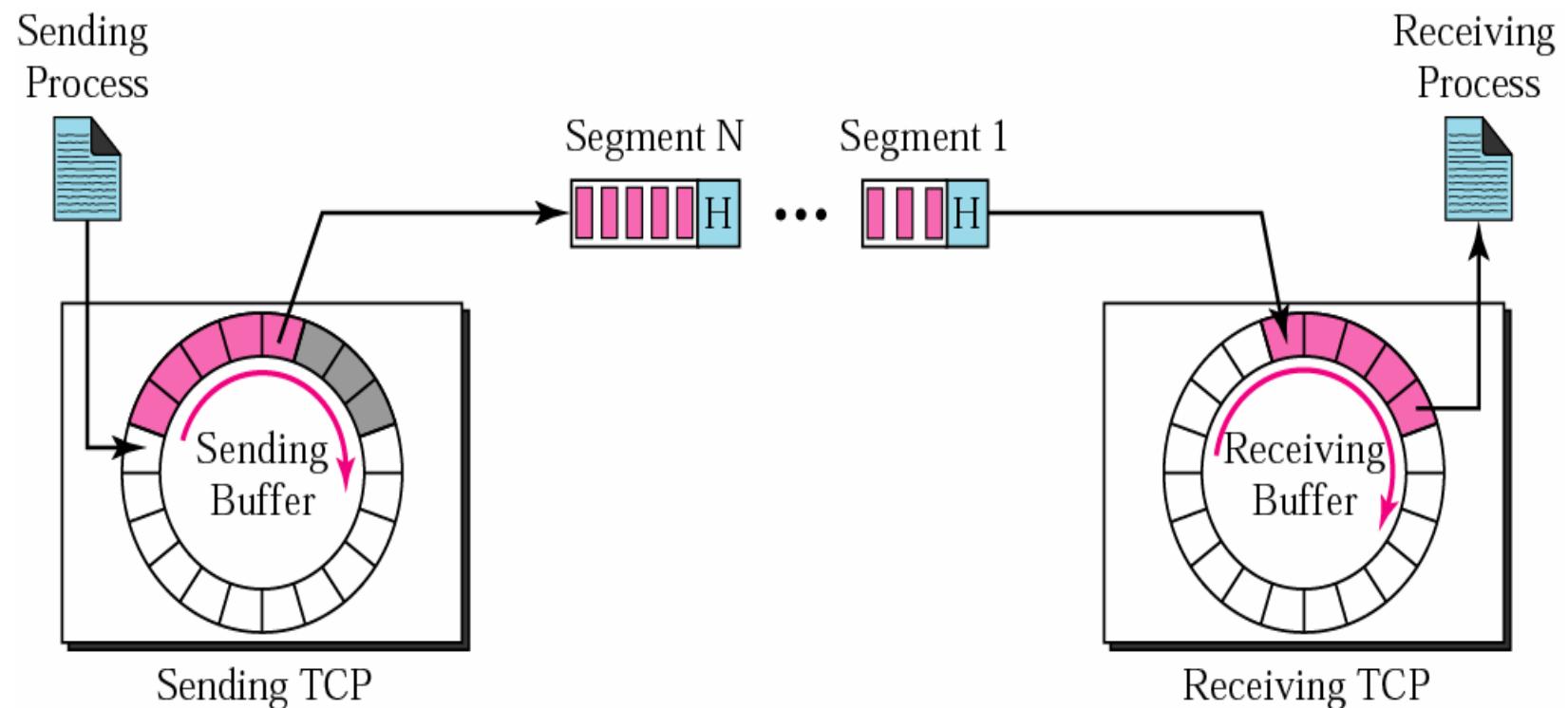


Sending and receiving buffer

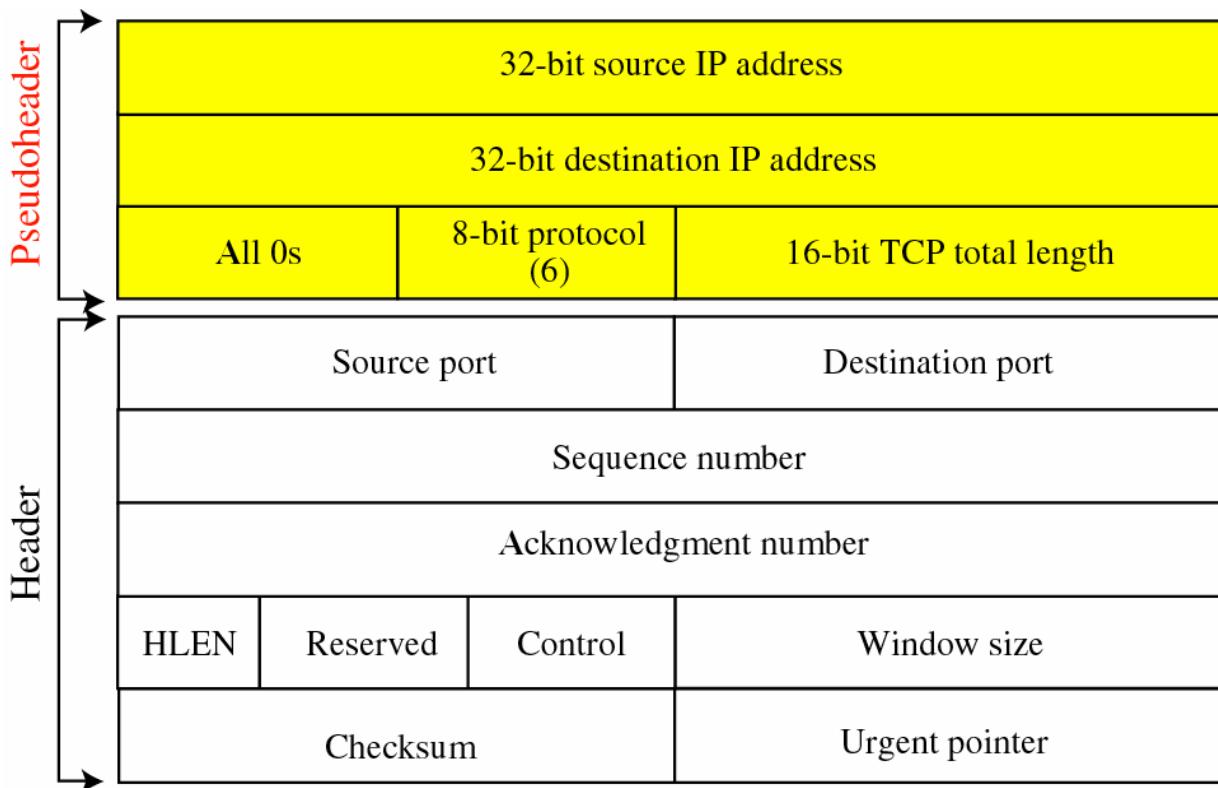




TCP segment



Pseudoheader added to TCP datagram

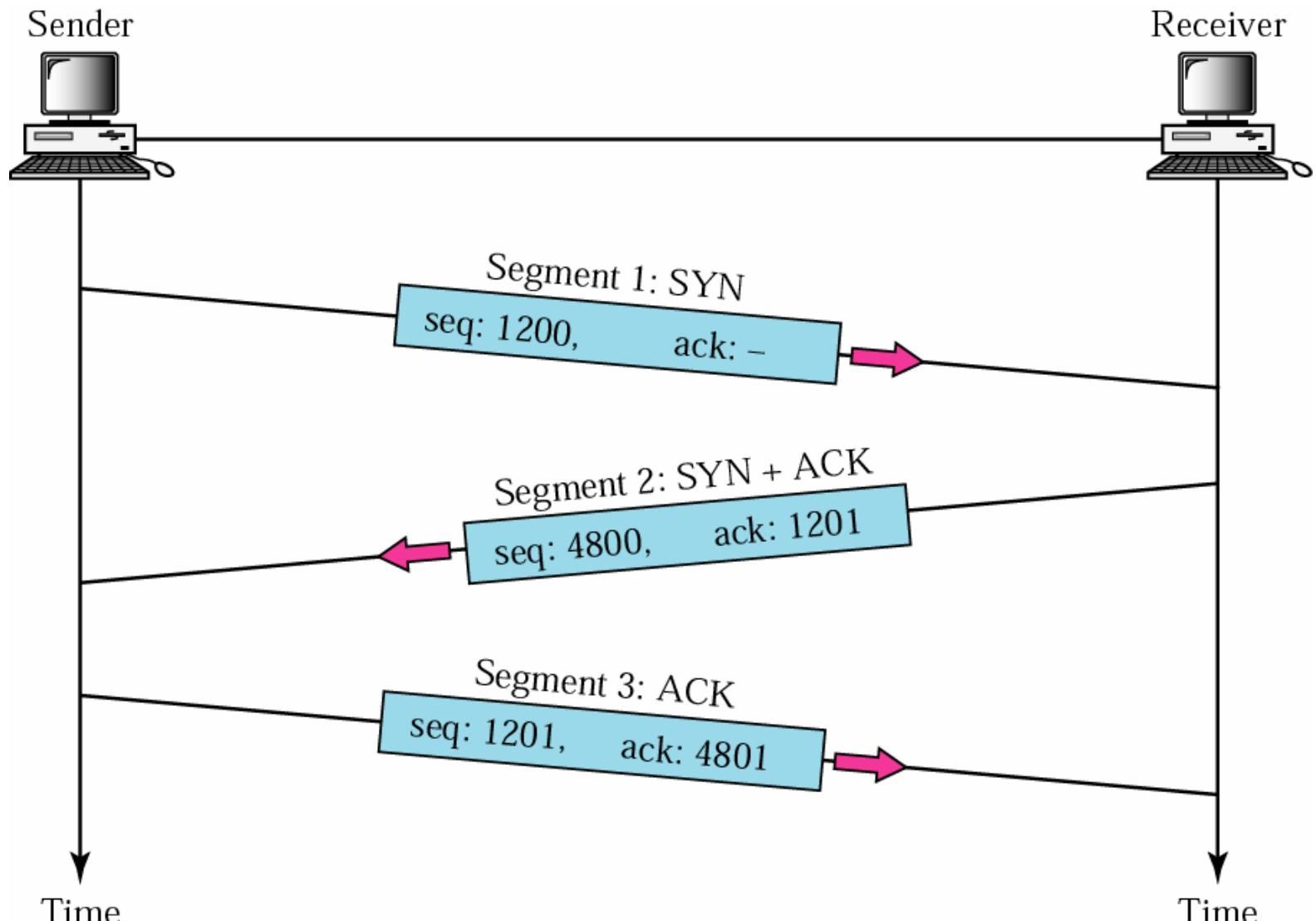


Data and Option

(Padding must be added to make the data a multiple of 16-bits)

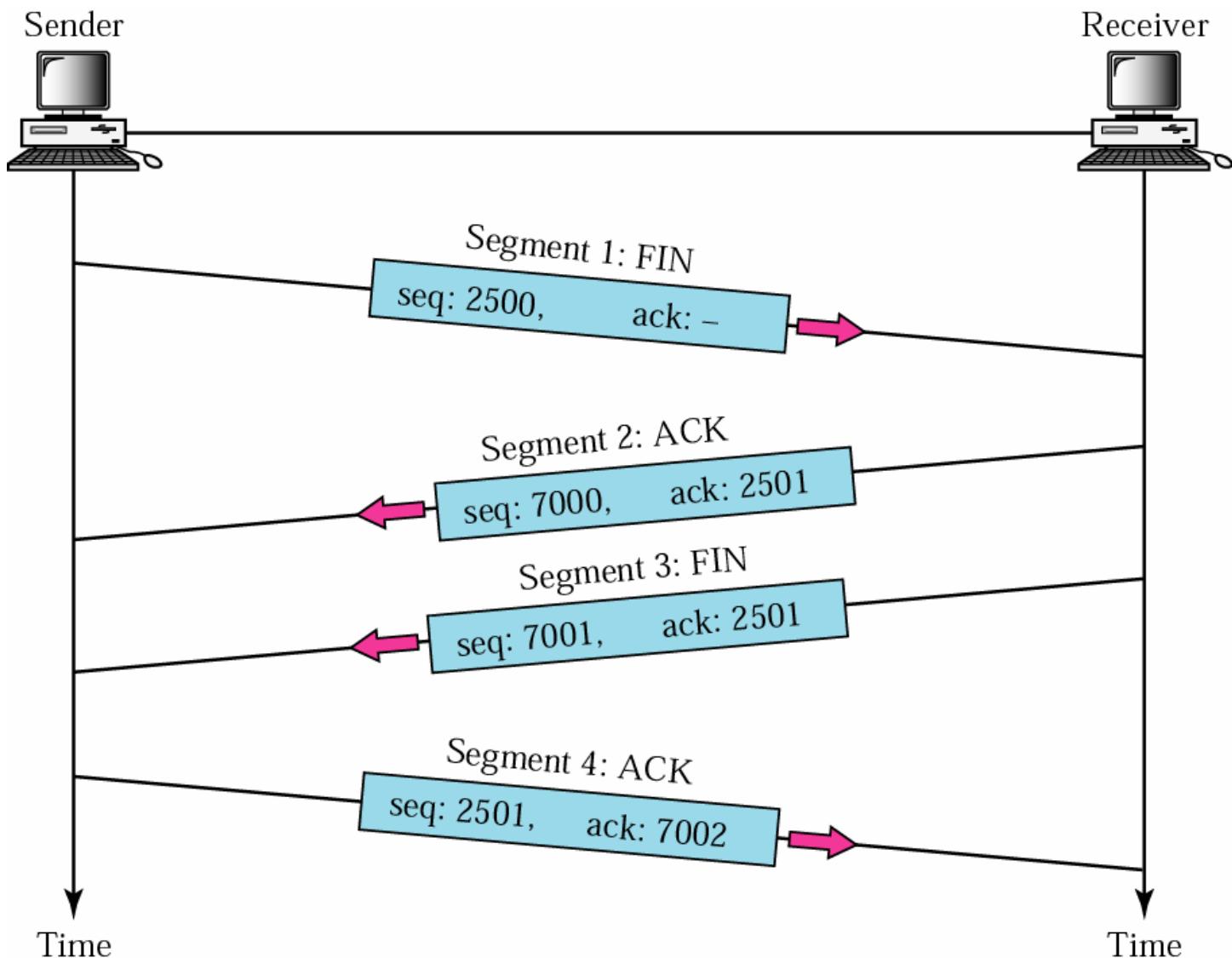


Three-way handshaking



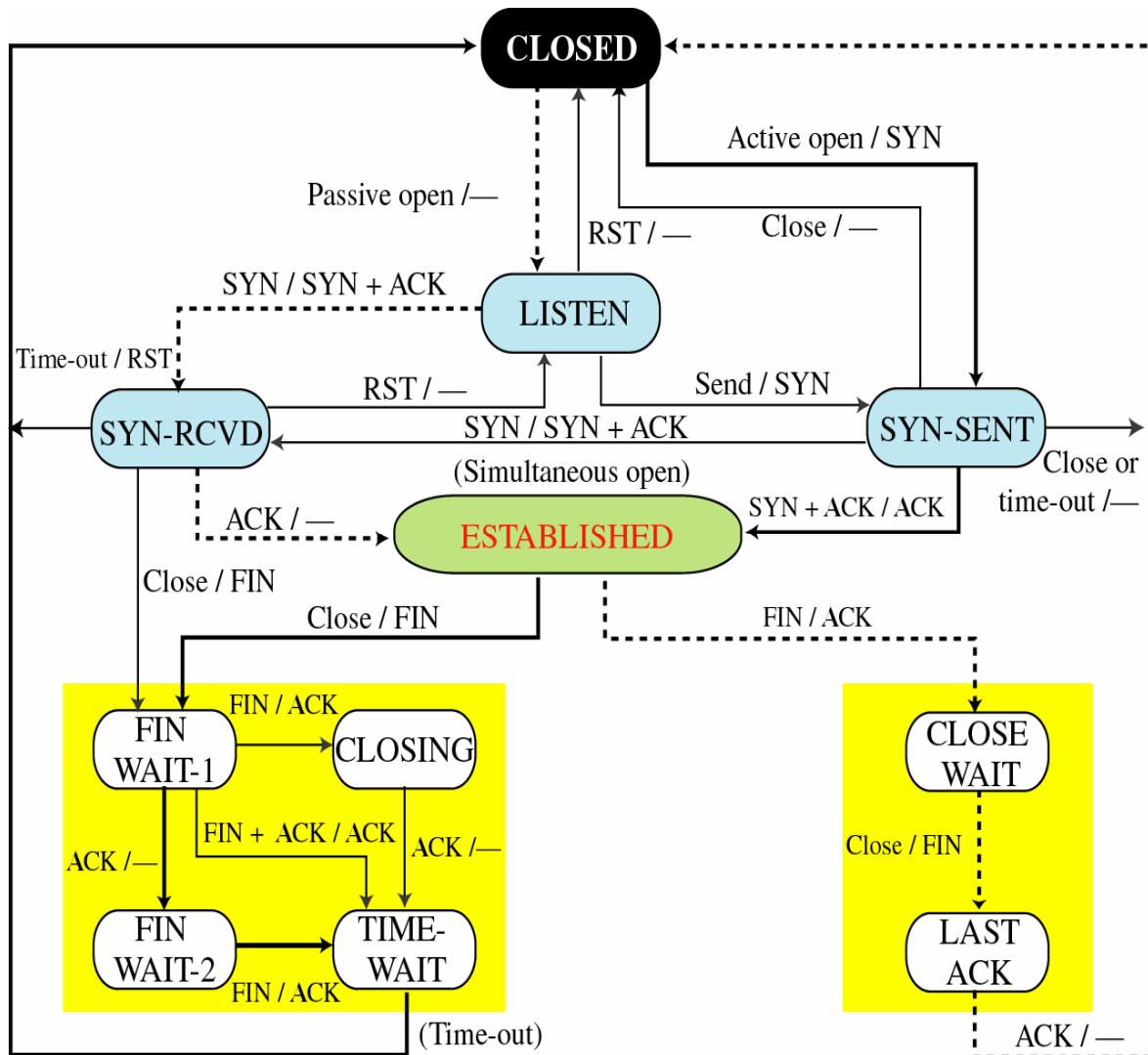


Four-way handshaking





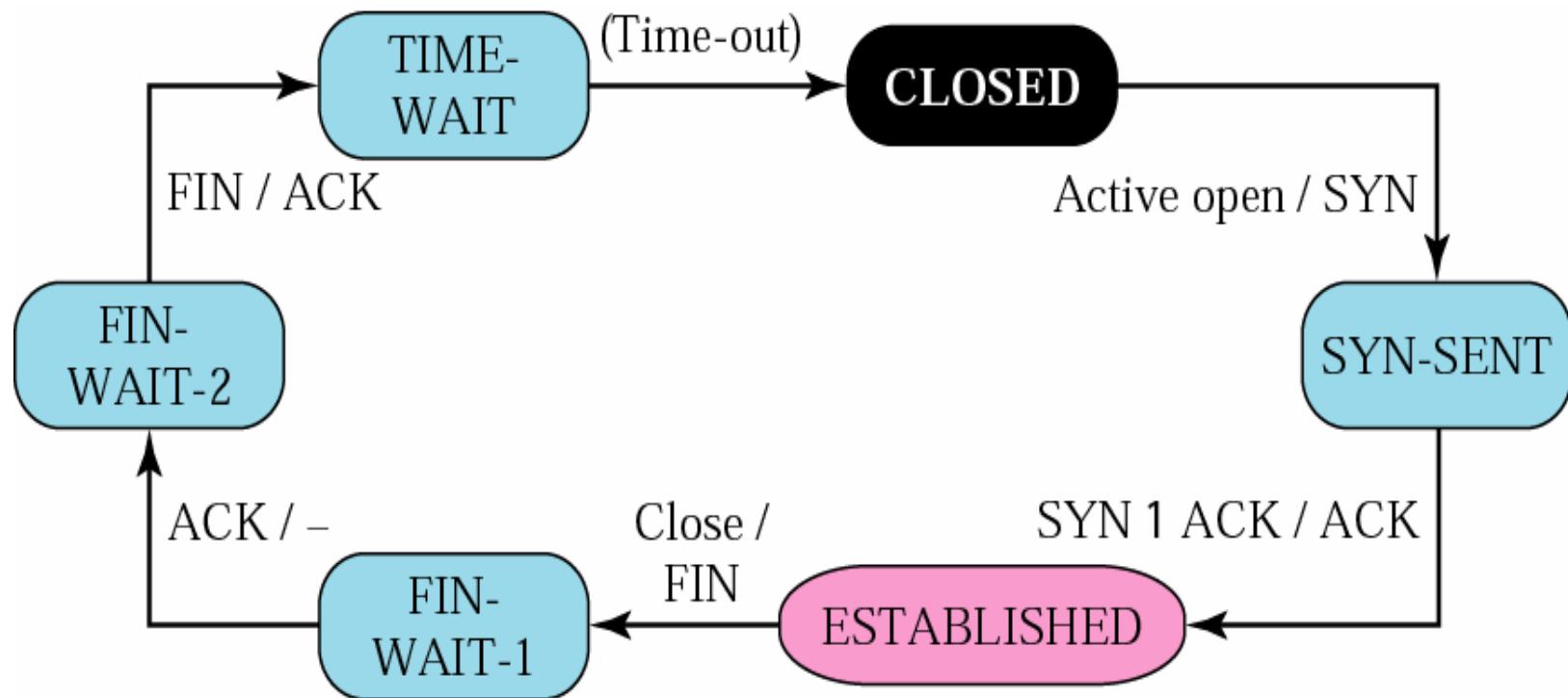
State transition diagram





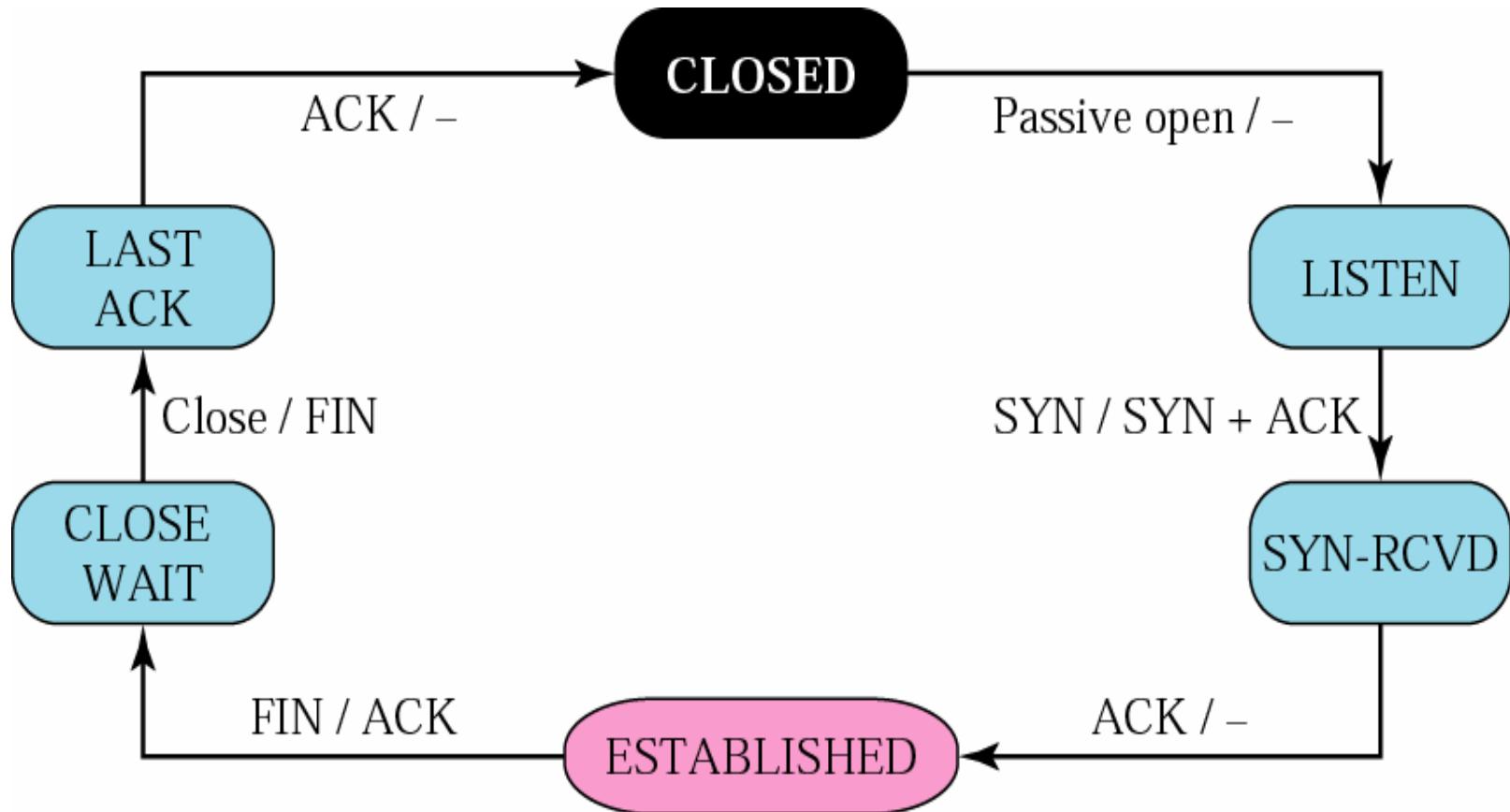
Client States

Global CyberSoft



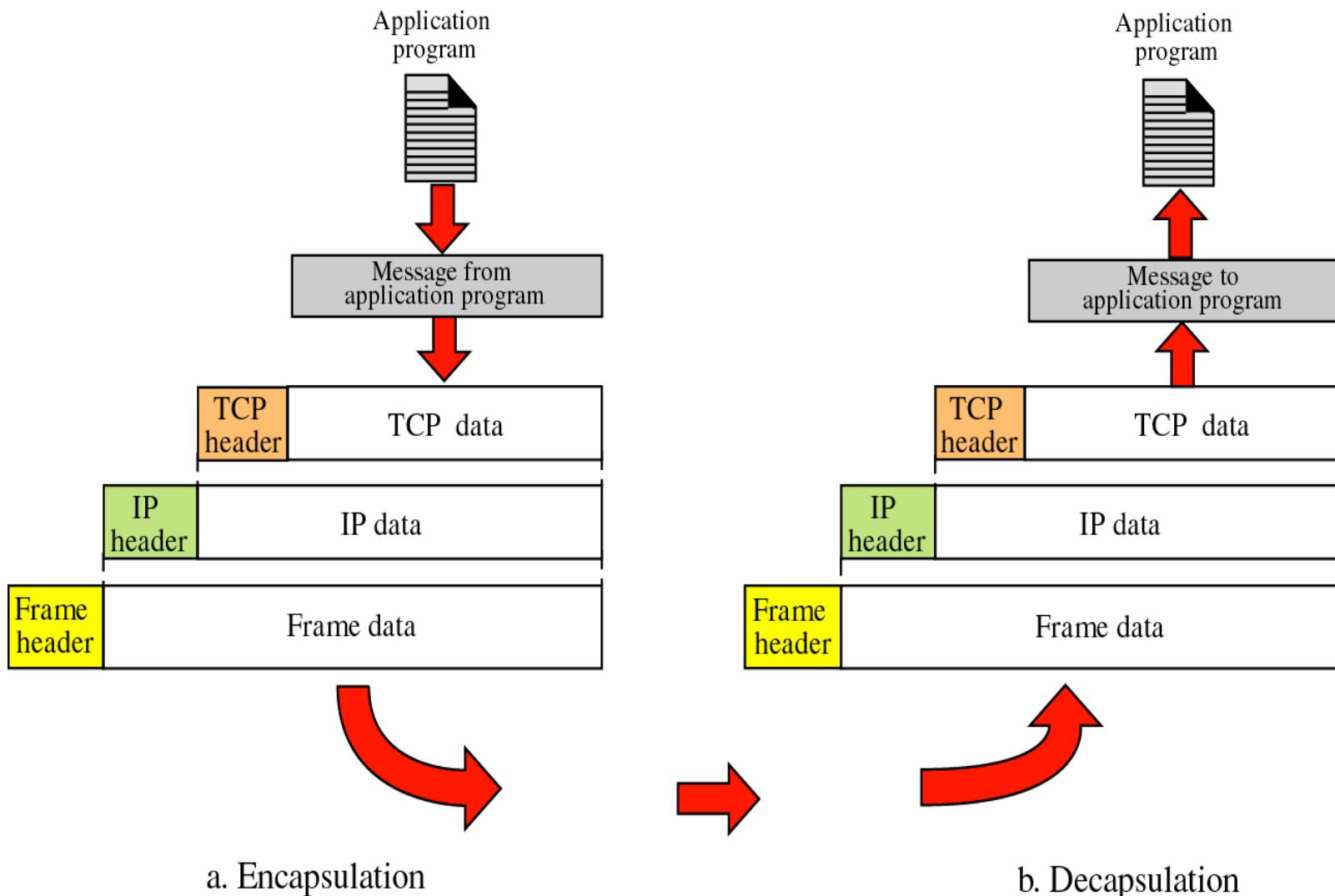


Server States



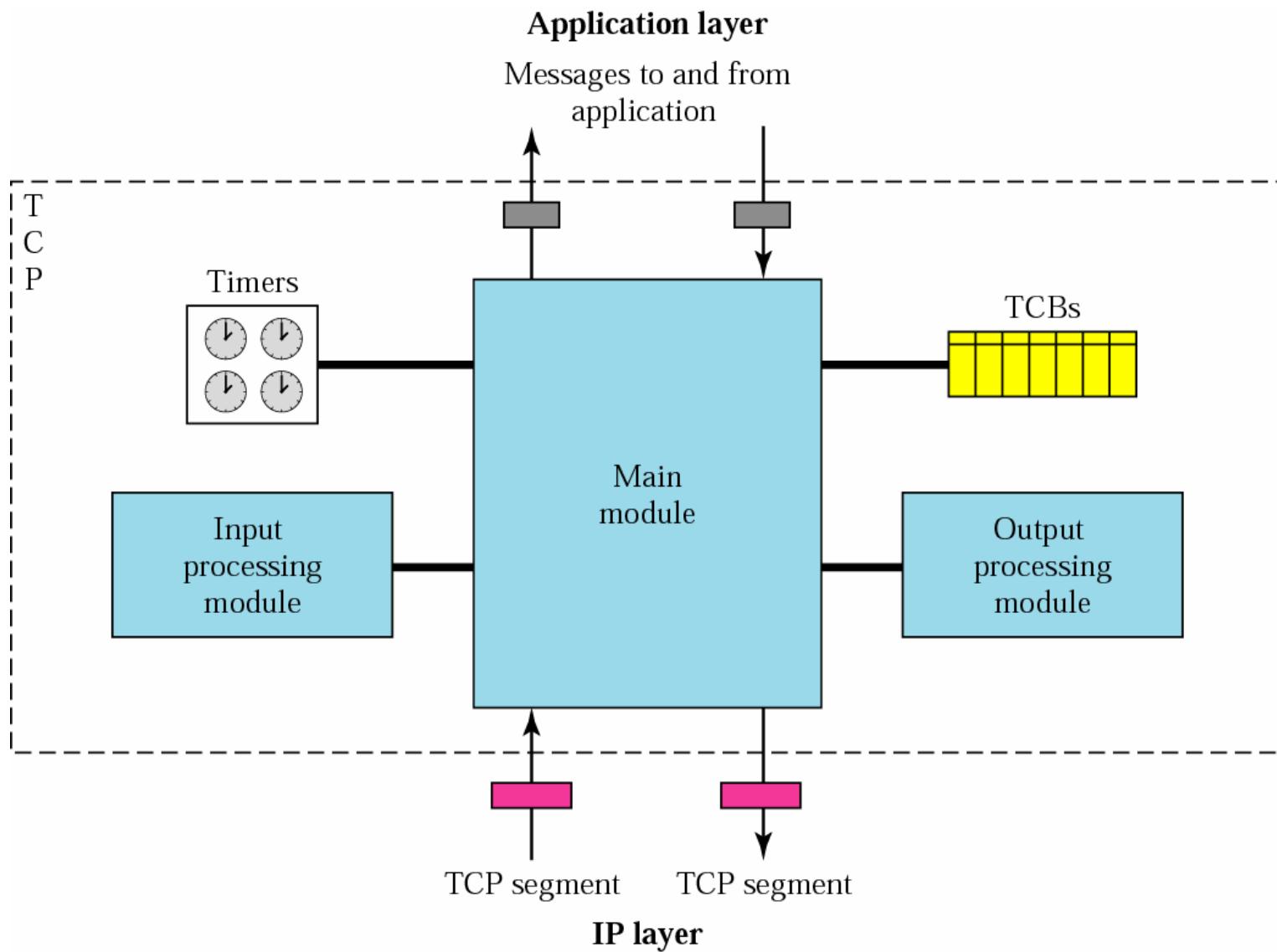


Encapsulation and Decapsulation





TCP Package





Global CyberSoft

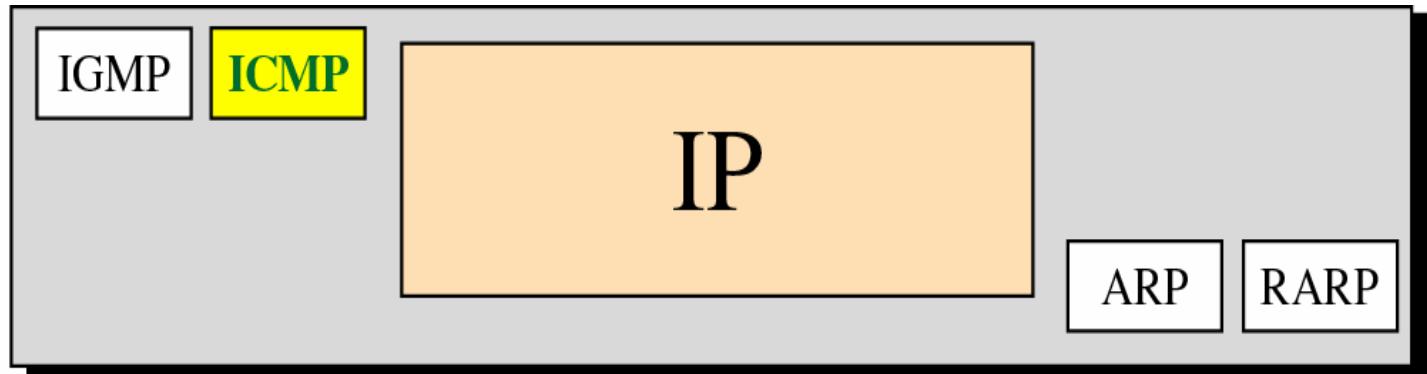
Internet Control Message Protocol

- TYPES OF MESSAGES
- MESSAGE FORMAT
- ERROR REPORTING
- QUERY
- CHECKSUM
- ICMP PACKAGE



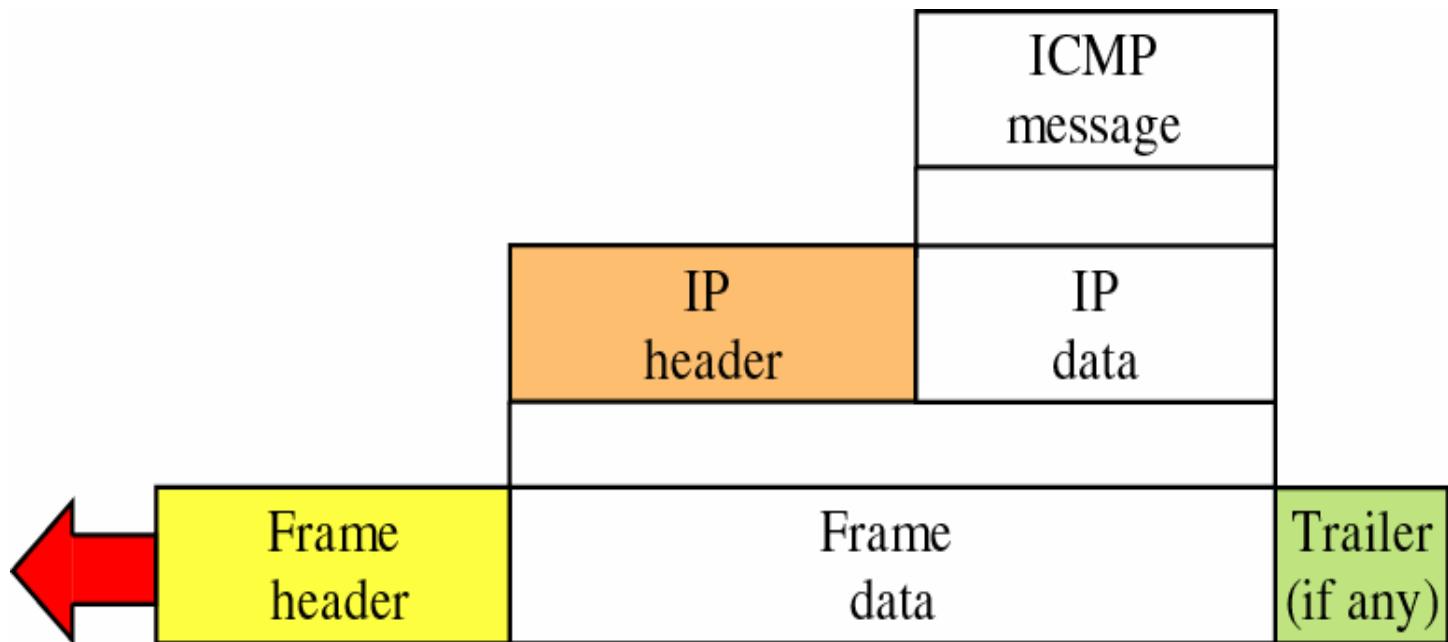
Position in Network layer

Network
layer



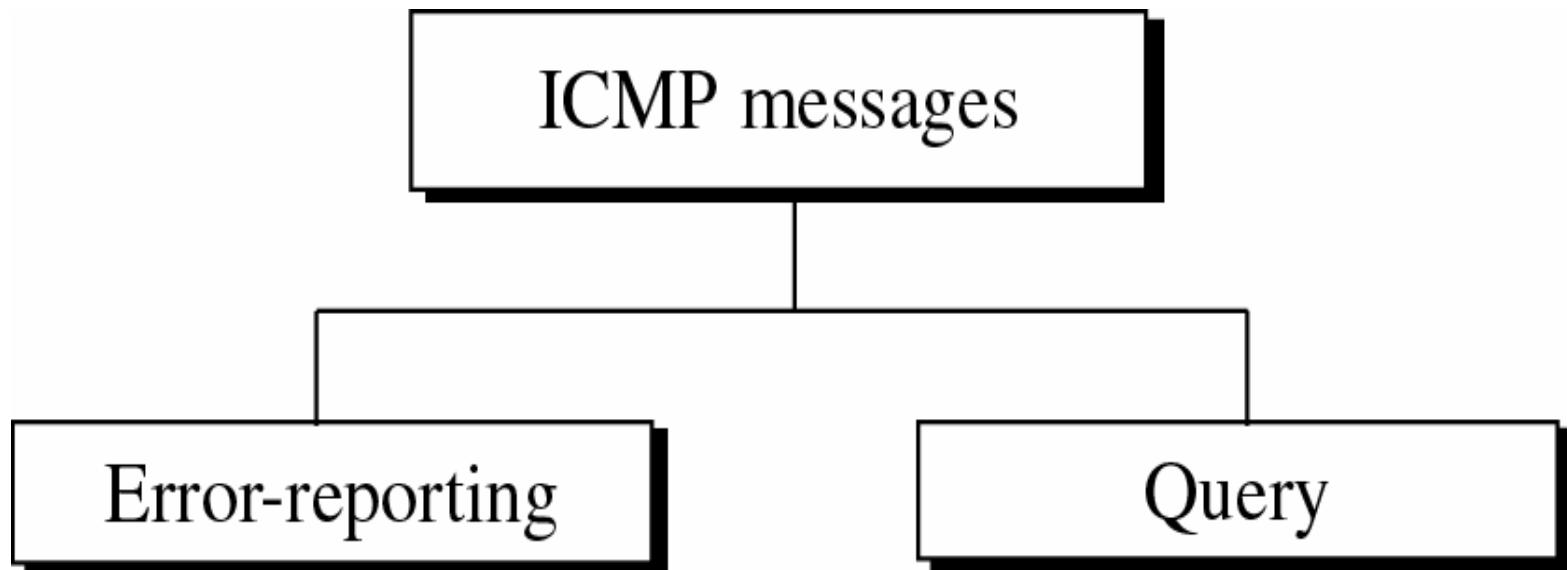


Encapsulation of ICMP Packet



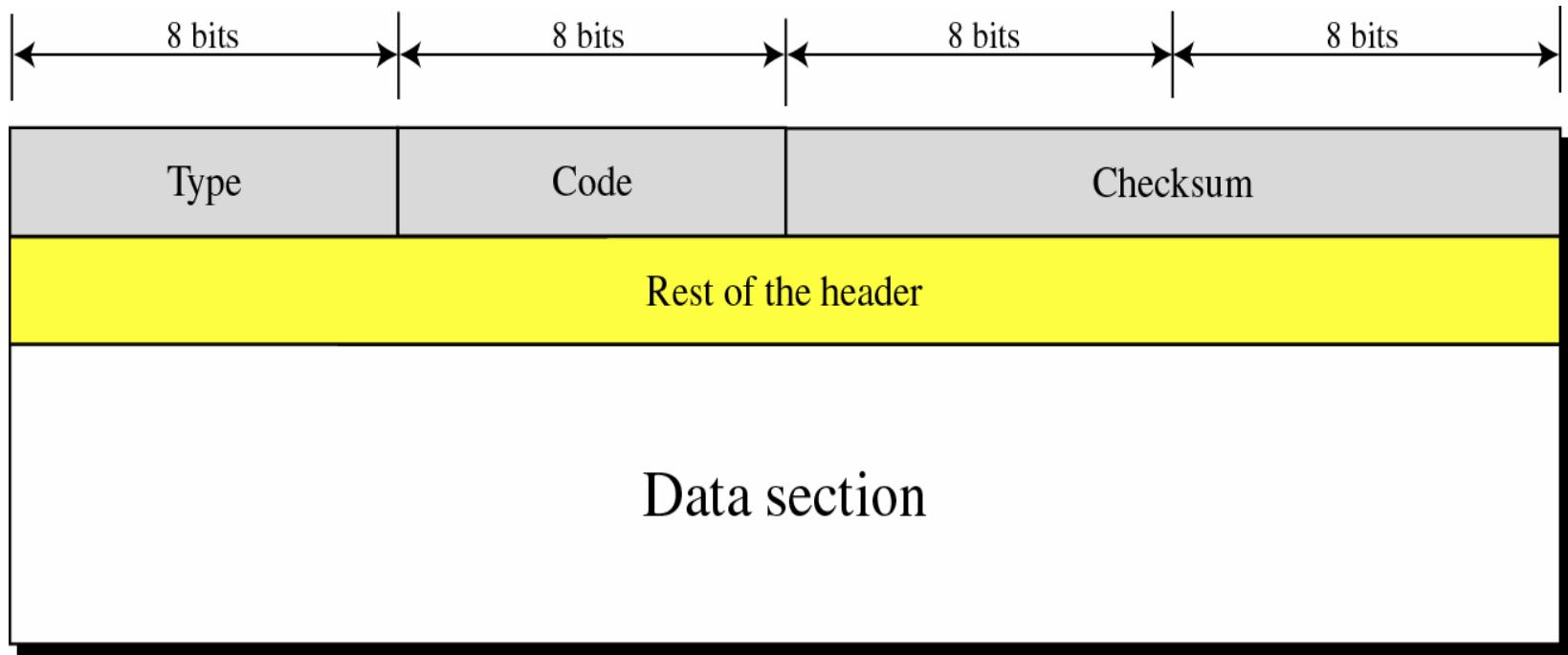


ICMP Messages





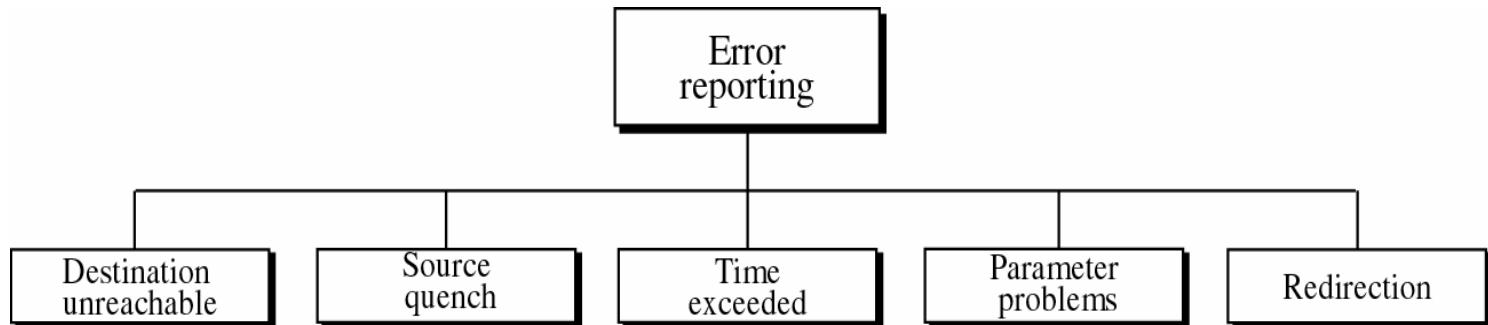
General format of ICMP Messages





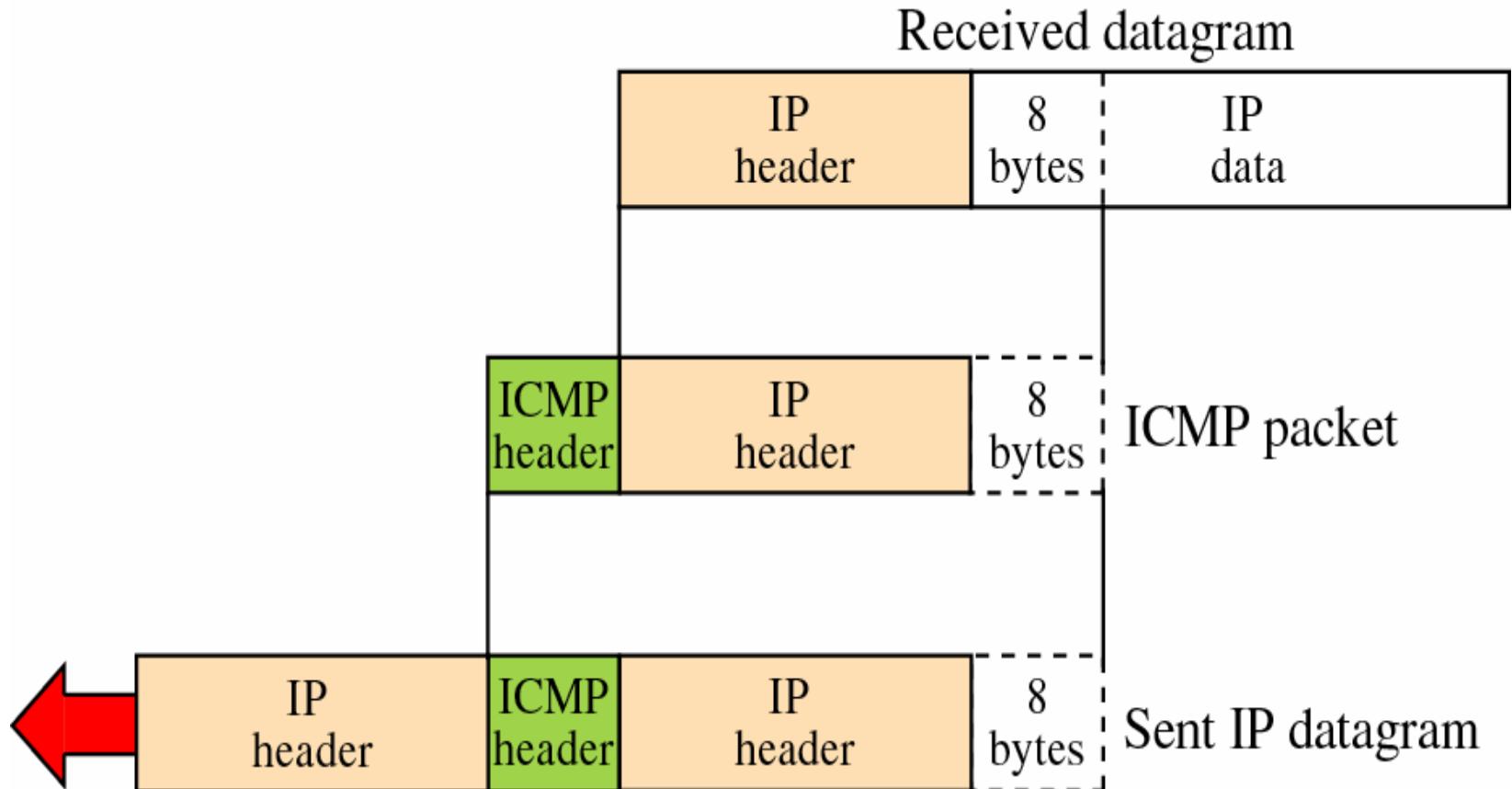
Error Report

- ICMP always reports error messages to the original source.



- No ICMP error message for a datagram carrying an ICMP error message.
- No ICMP error message for a fragmented datagram that is not the first fragment
- No ICMP error message for a datagram having a multicast address
- No ICMP error message for a datagram with a special address such as 127.0.0.0 or 0.0.0.0.

Content of data field for error messages



Destination Unreachable

Type: 3	Code: 0 to 15	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Note: Destination-unreachable messages with codes 2 or 3 can be created only by the destination host. Other destination-unreachable messages can be created only by routers

- There is no flow-control mechanism in the IP protocol
- A router cannot detect all problems that prevent the delivery of a packet.
- Destination-unreachable messages with codes 2 or 3 can be created only by the destination host.
- Other destination-unreachable messages can be created only by routers.



Source-quence format

Type: 4	Code: 0	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Source-quench format

- A source-quench message informs the source that a datagram has been discarded due to congestion in a router or the destination host. The source must slow down the sending of datagrams until the congestion is relieved
- One source-quench message should be sent for each datagram that is discarded due to congestion.
- Whenever a router receives a datagram with a time-to-live value of zero, it discards the datagram and sends a time-exceeded message to the original source
- When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source.
- In a time-exceeded message, code 0 is used only by routers to show that the value of the time-to-live field is zero.
Code 1 is used only by the destination host to show that not all of the fragments have arrived within a set time



Time-exceed Format

Type: 11	Code: 0 or 1	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Code 0: Time to live

Code 1: Fragmentation

Parameter-problem message format

Type: 12	Code: 0 or 1	Checksum
Pointer		Unused (All 0s)

Part of the received IP datagram including IP header
plus the first 8 bytes of datagram data

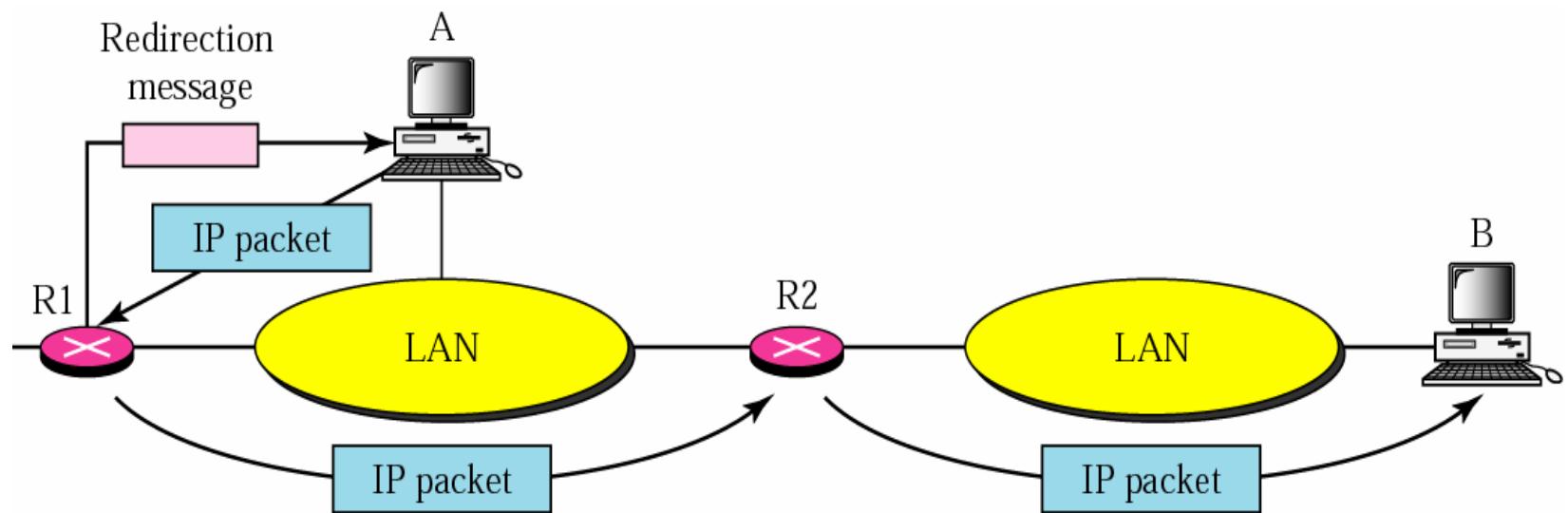
Code 0: Main header problem

Code 1: Problem in the option field

A parameter-problem message can be created by a router or the destination host

Redirection concept

A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is the redirection message



Redirection message format

Type: 5	Code: 0 to 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Code 0: Network specific

Code 1: Host specific

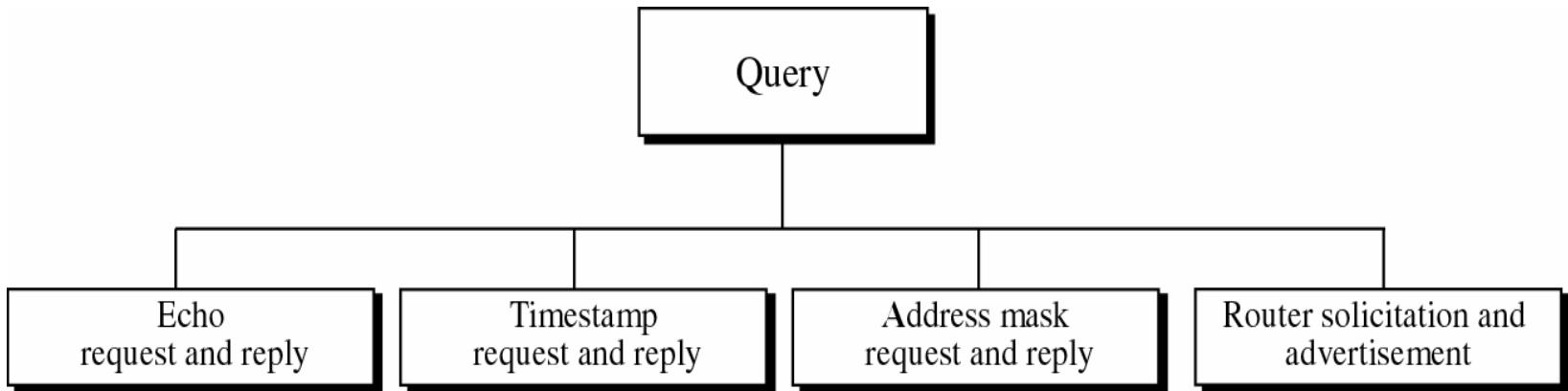
Code 2: Network specific (specified service)

Code 3: Host specific (specified service)

A redirection message is sent from a router to a host on the same local network



Query message



Query message

- An echo-request message can be sent by a host or router.
An echo-reply message is sent by the host or router which receives an echo-request message
- Echo-request and echo-reply messages can be used by network managers to check the operation of the IP protocol
- Echo-request and echo-reply messages can test the reachability of a host. This is usually done by invoking the **ping** command



Echo request and echo reply

8: Echo request
0: Echo reply

Type: 8 or 0	Code: 0	Checksum
Identifier		Sequence number
Optional data Sent by the request message; repeated by the reply message		



Timestamp request and reply

13: request
14: reply

Type: 13 or 14	Code: 0	Checksum
Identifier		Sequence number
Original timestamp		
Receive timestamp		
Transmit timestamp		



Mask request and reply

17: Request
18: Reply

Type: 17 or 18	Code: 0	Checksum
Identifier		Sequence number
Address mask		



Router solicitation

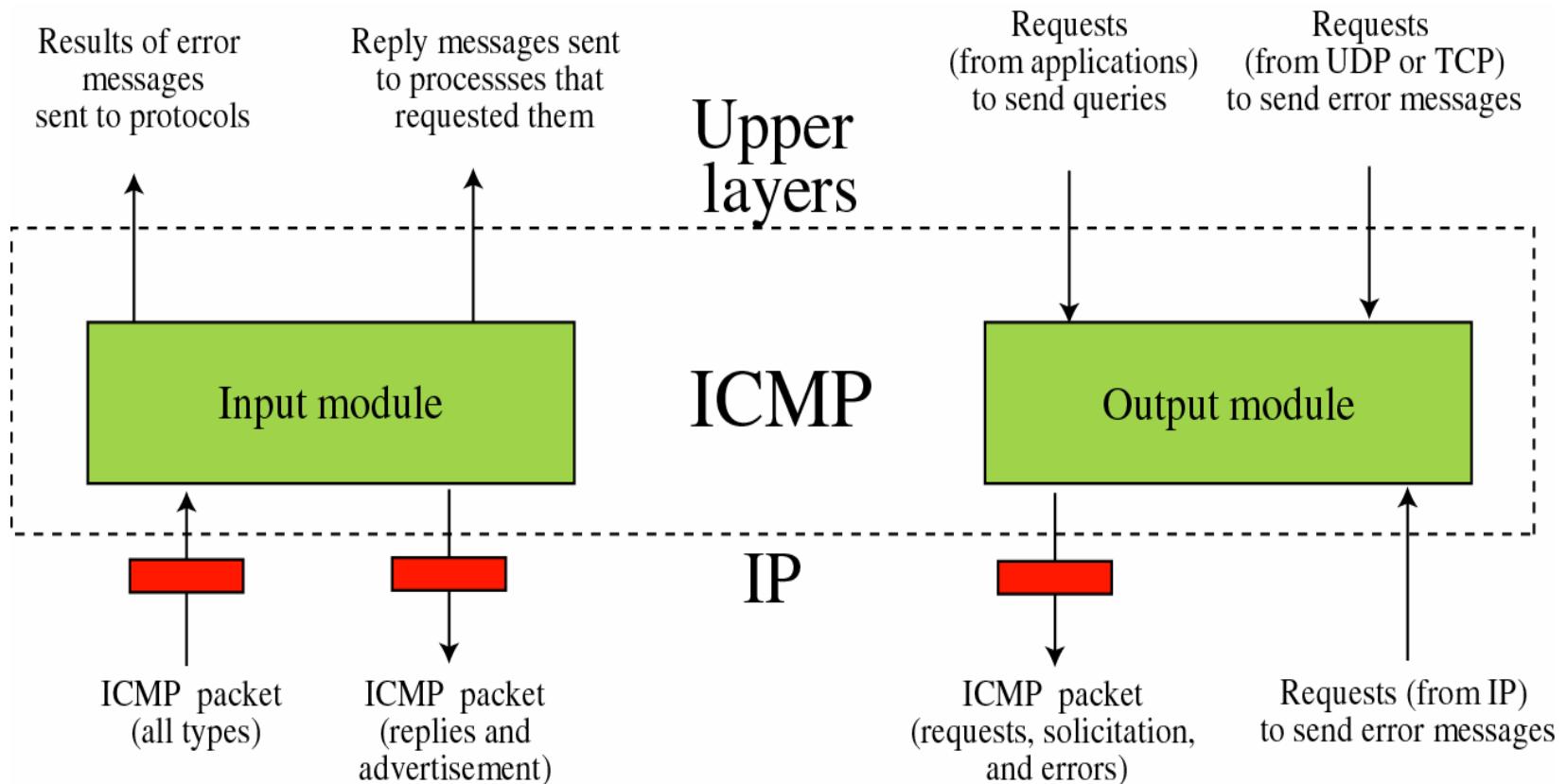
Type: 10	Code: 0	Checksum
Identifier		Sequence number

Router advertisement

Type: 9	Code: 0	Checksum
Number of addresses	Address entry size	Lifetime
Router address 1		
Address preference 1		
Router address 2		
Address preference 2		
• • •		



ICMP Package





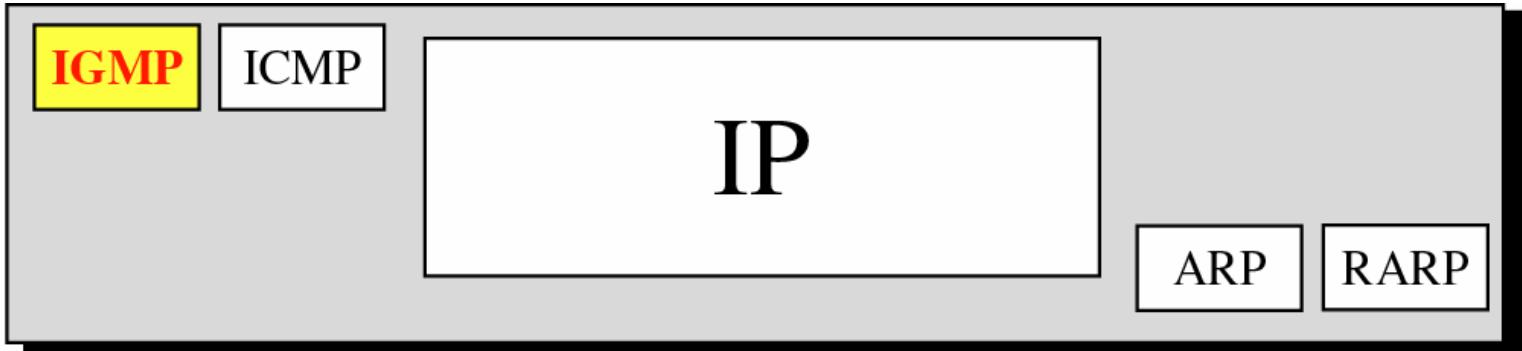
Global CyberSoft

Internet Group Management Protocol

- GROUP MANAGEMENT
- IGMP MESSAGES
- IGMP OPERATION
- ENCAPSULATION
- IGMP PACKAGE

Position in Network layer

Network
layer



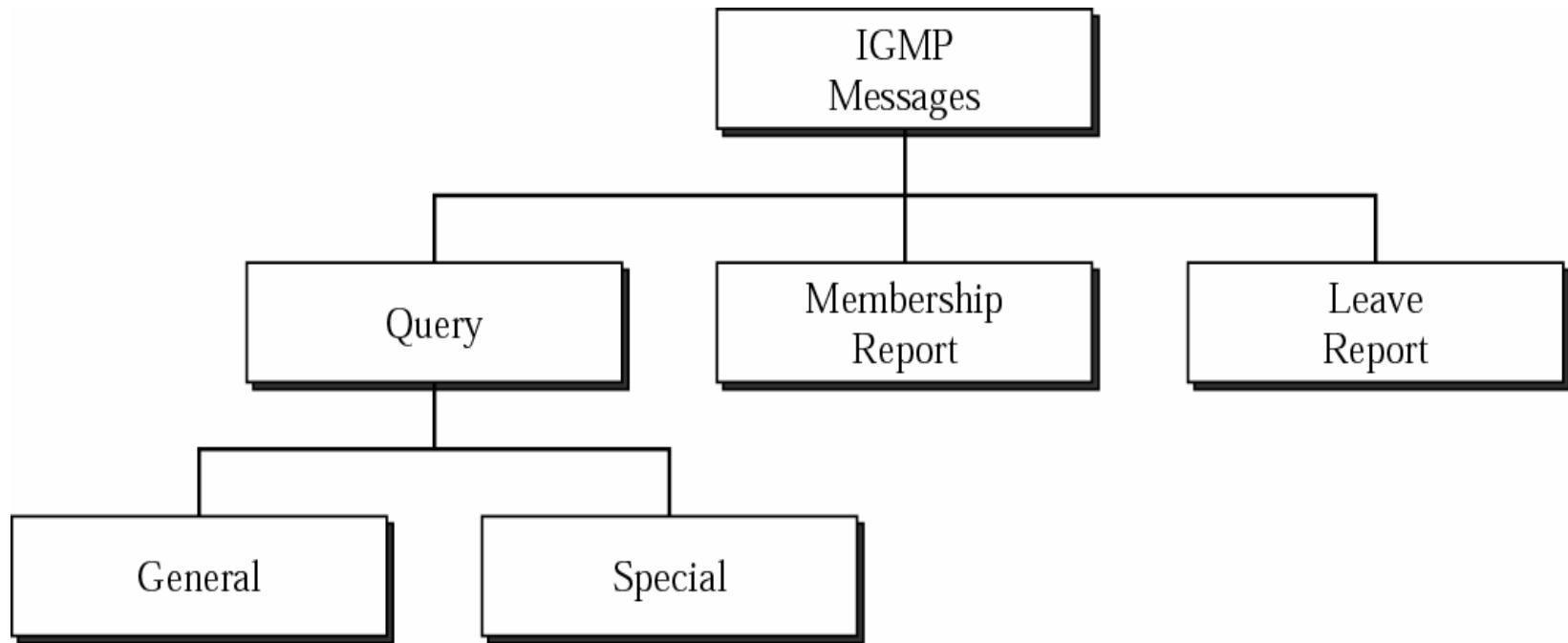


What is IGMP

- IGMP is a group management protocol. It helps a multicast router create and update a list of loyal members related to each router interface

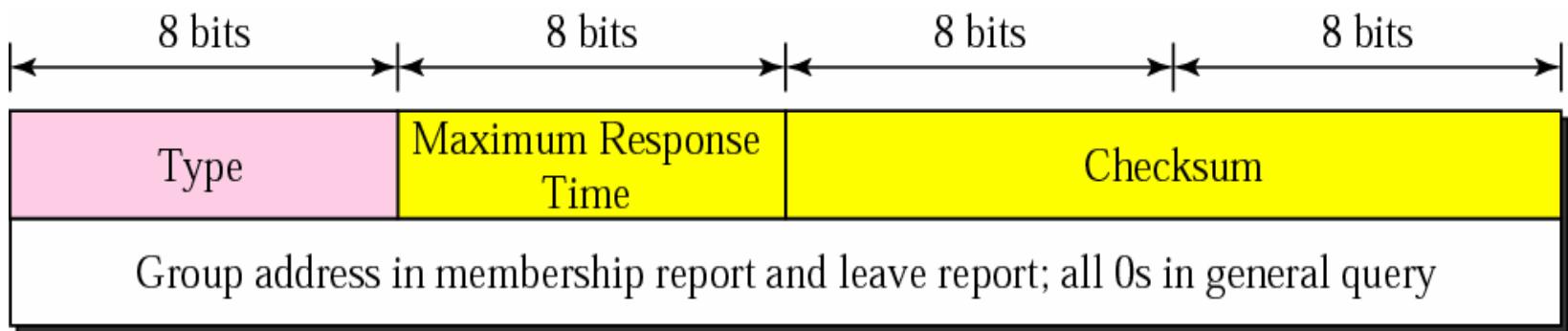


IGMP Message Type



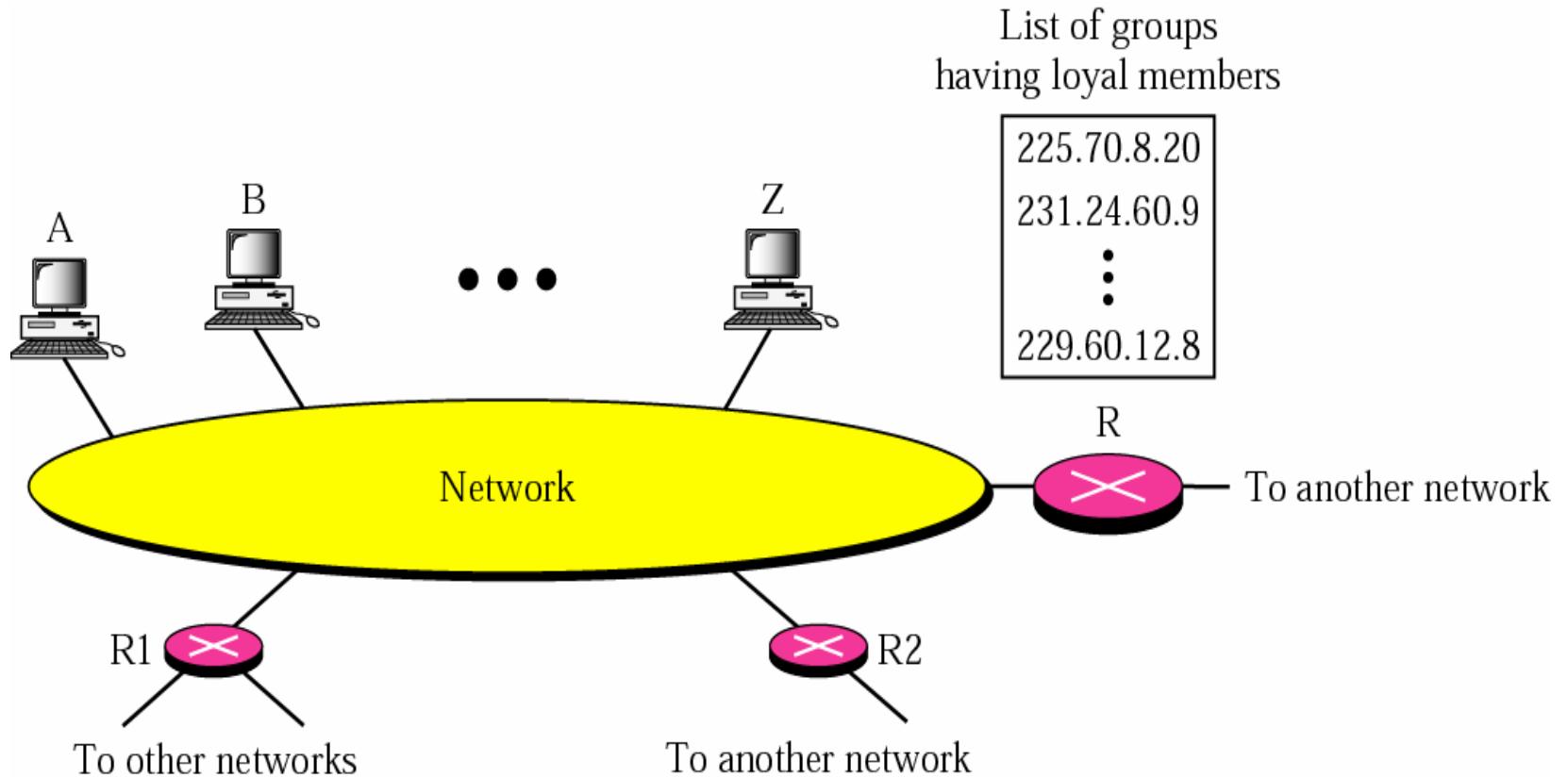


IGMP Message Format





IGMP Operation

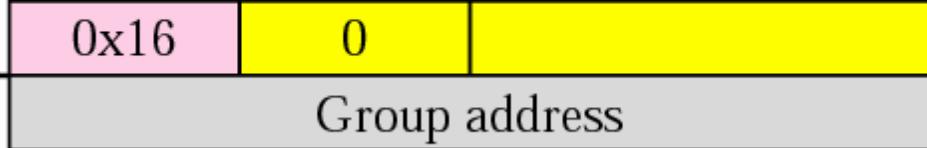


Membership Report

Host or Router



Membership Report



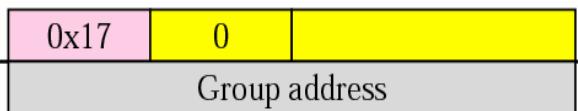
In IGMP, a membership report is sent twice, one after the other

Leave Report

Host or Router



Leave Report



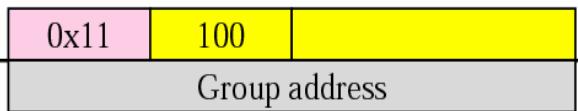
Router



Host or Router



Special Query



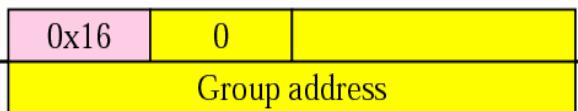
Router



Host or Router



Membership Report



Router



Or

Host or Router



Router



General query message

Host or Router



General Query



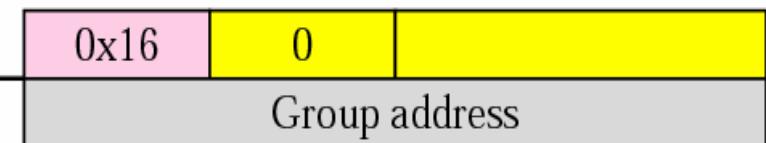
Router



Host or Router



Membership Report



Router



Or

Host or Router

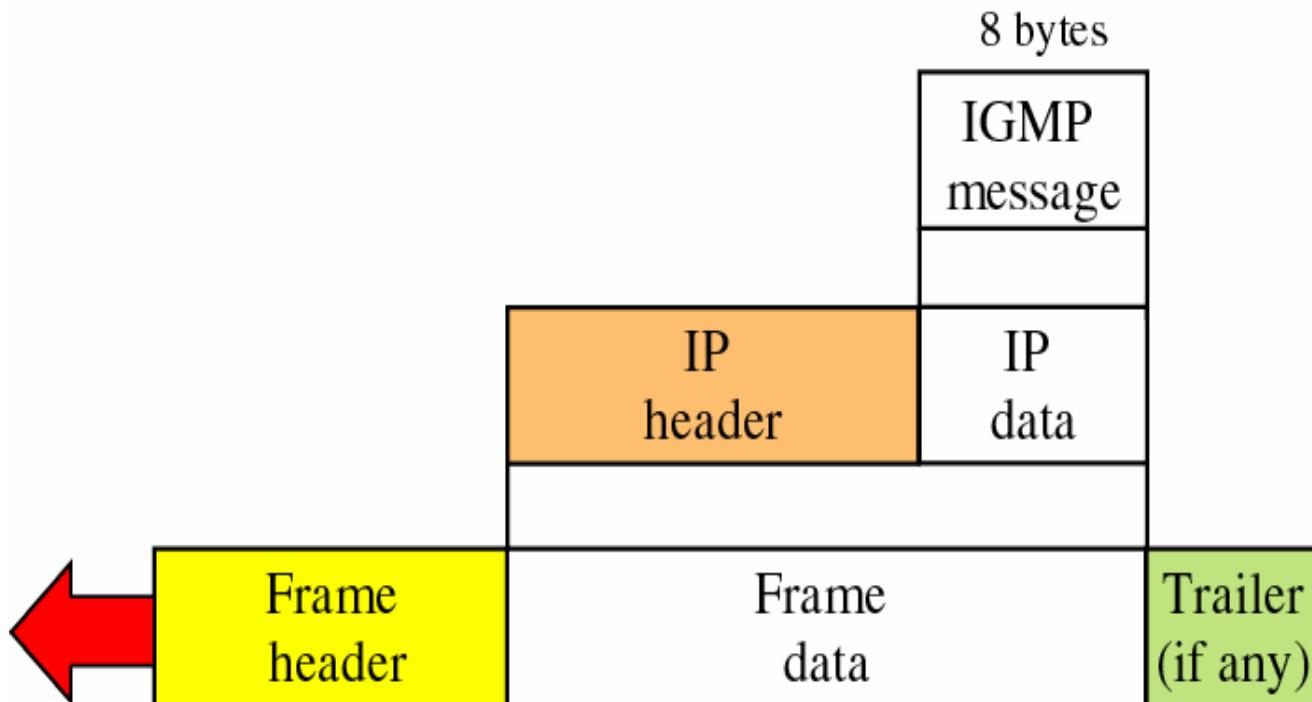


Router



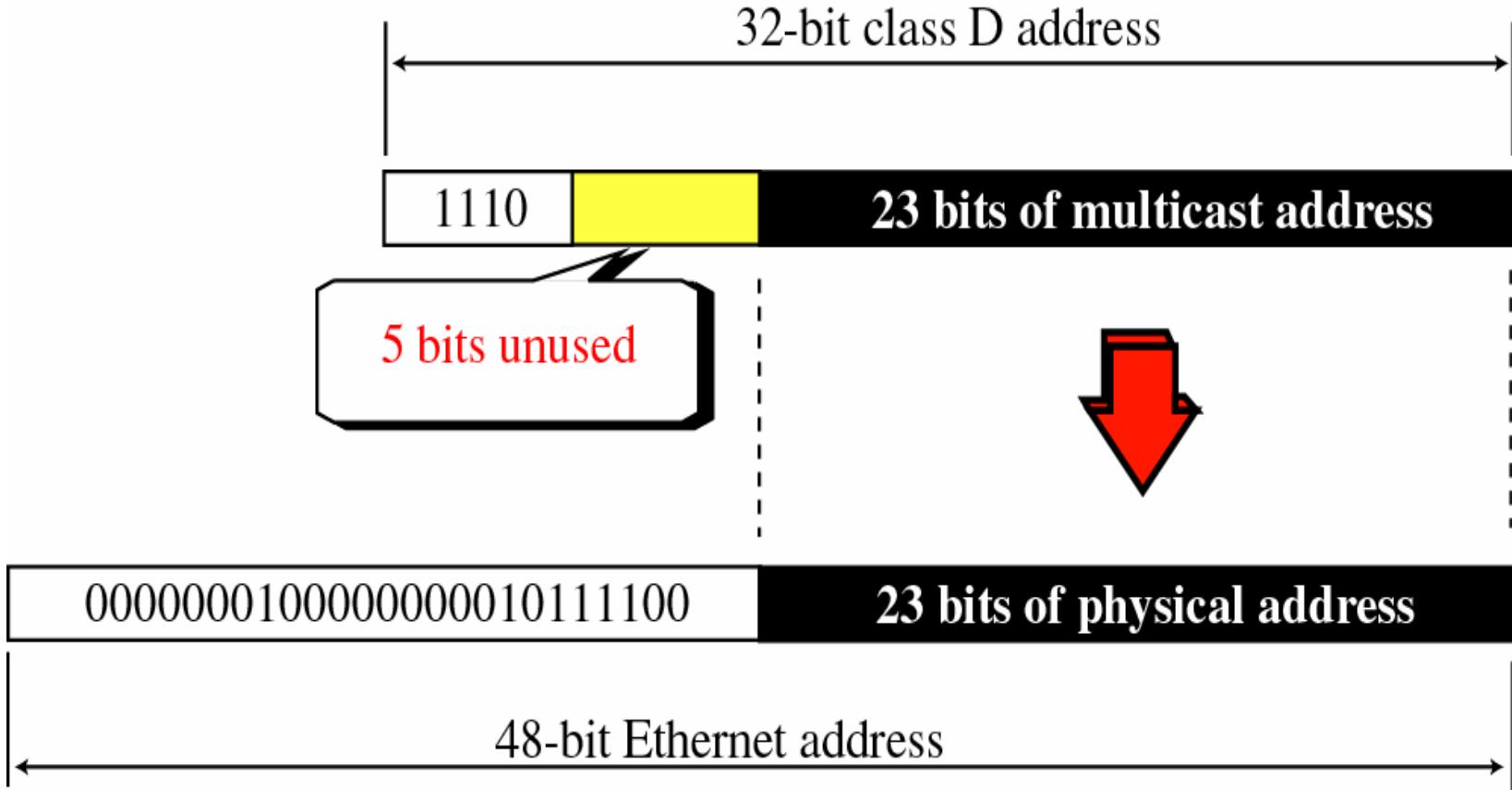


Encapsulation of IGMP packet





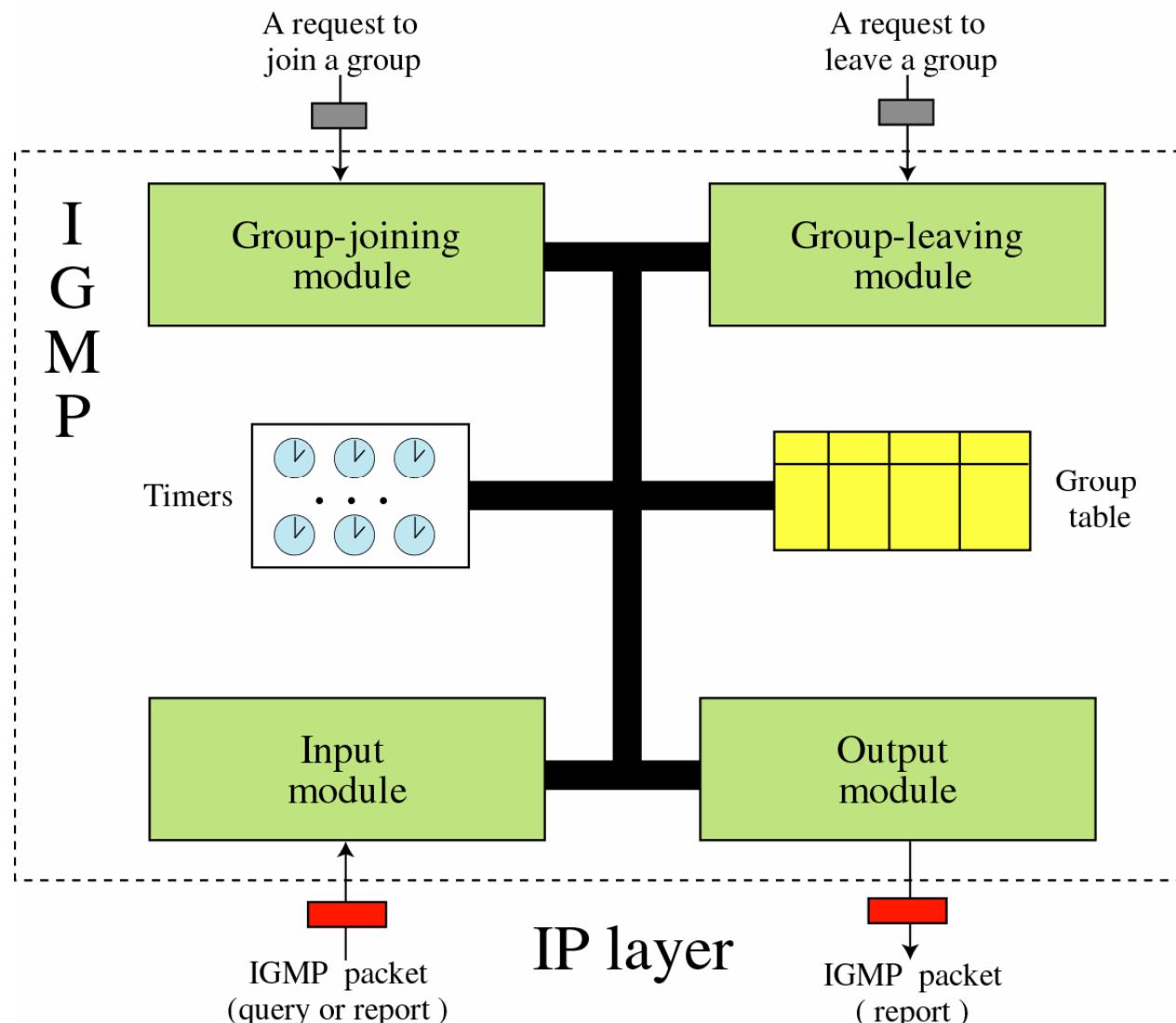
Mapping Class D to Ethernet physical address





IGMP Package

Application layer





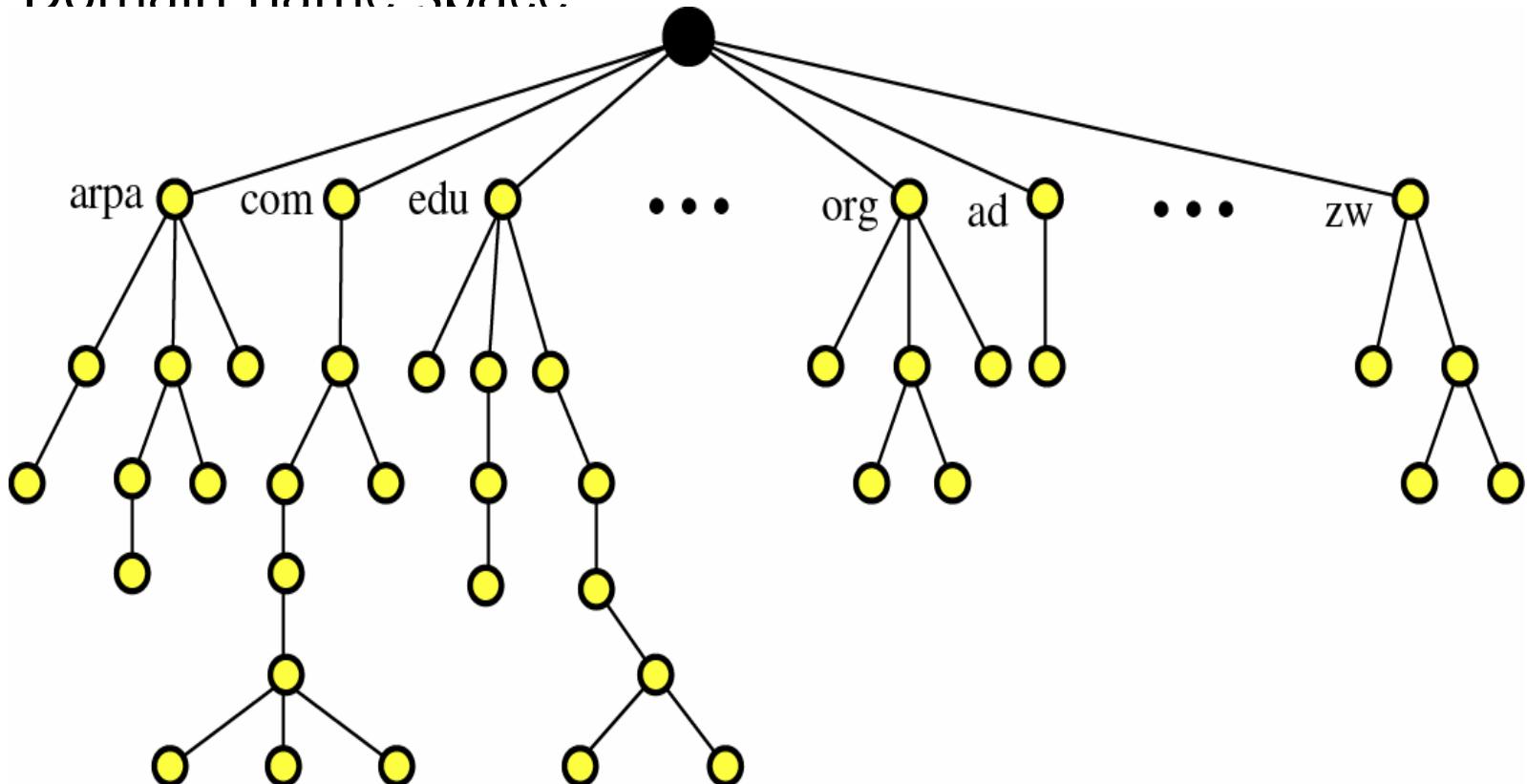
Global CyberSoft

Upper layer Protocol

- DNS
- FTP
- TELNET

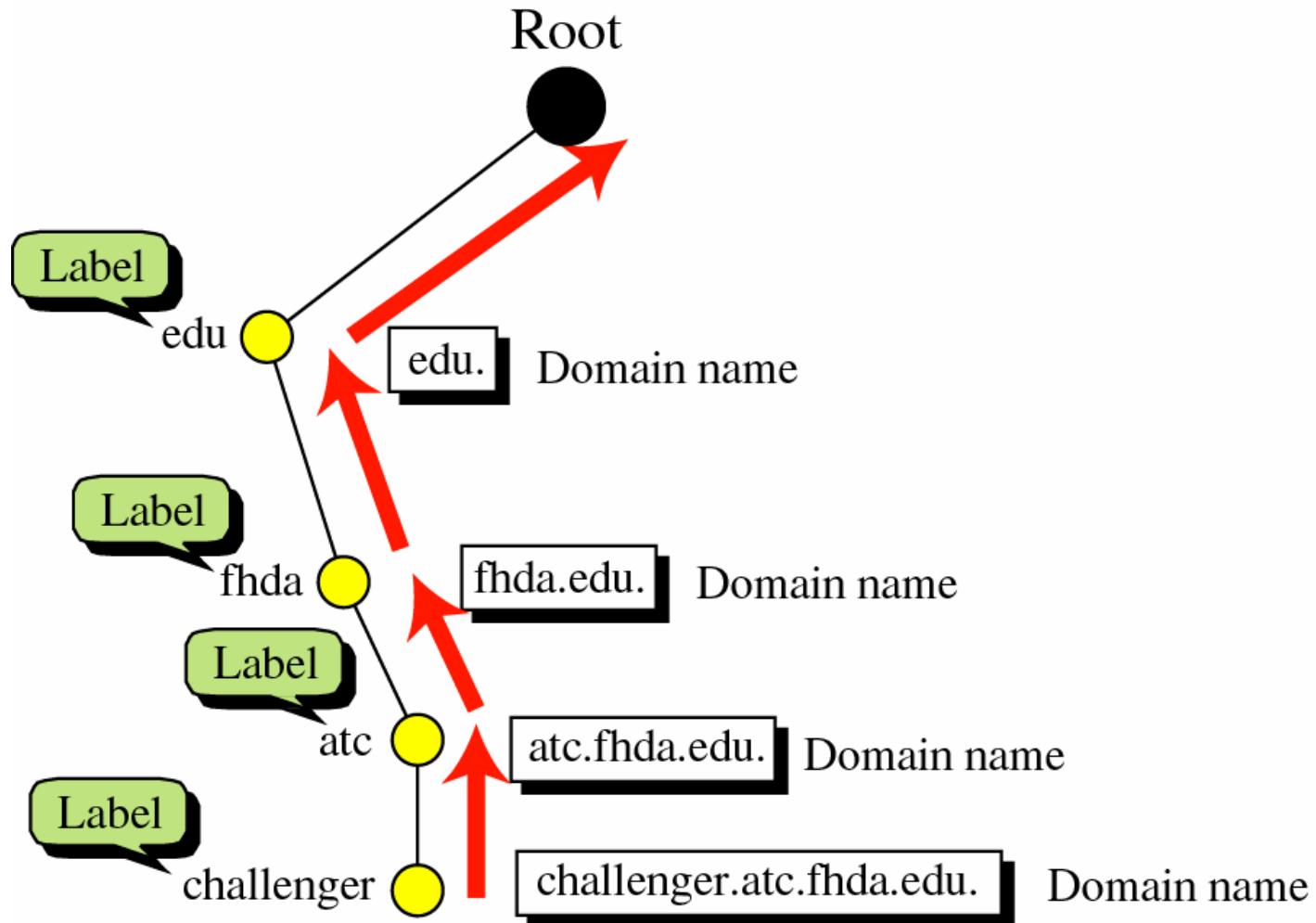
Domain Name System - DNS

- Domain name space





- Domain name and label





FQDN and PQND

FQDN

challenger.atc.fhda.edu.

cs.hmme.com.

www.funny.int.

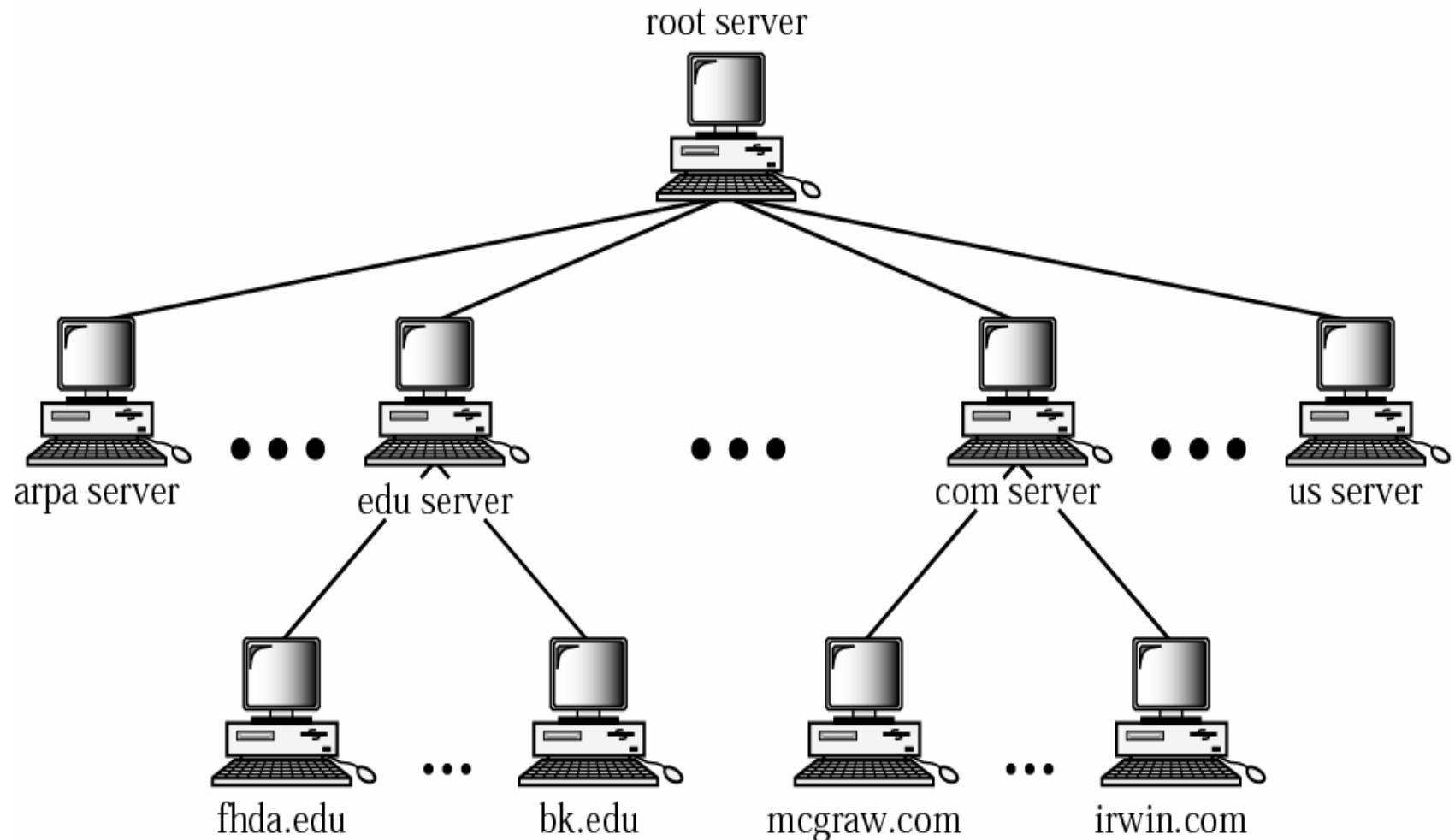
PQDN

challenger.atc.fhda.edu

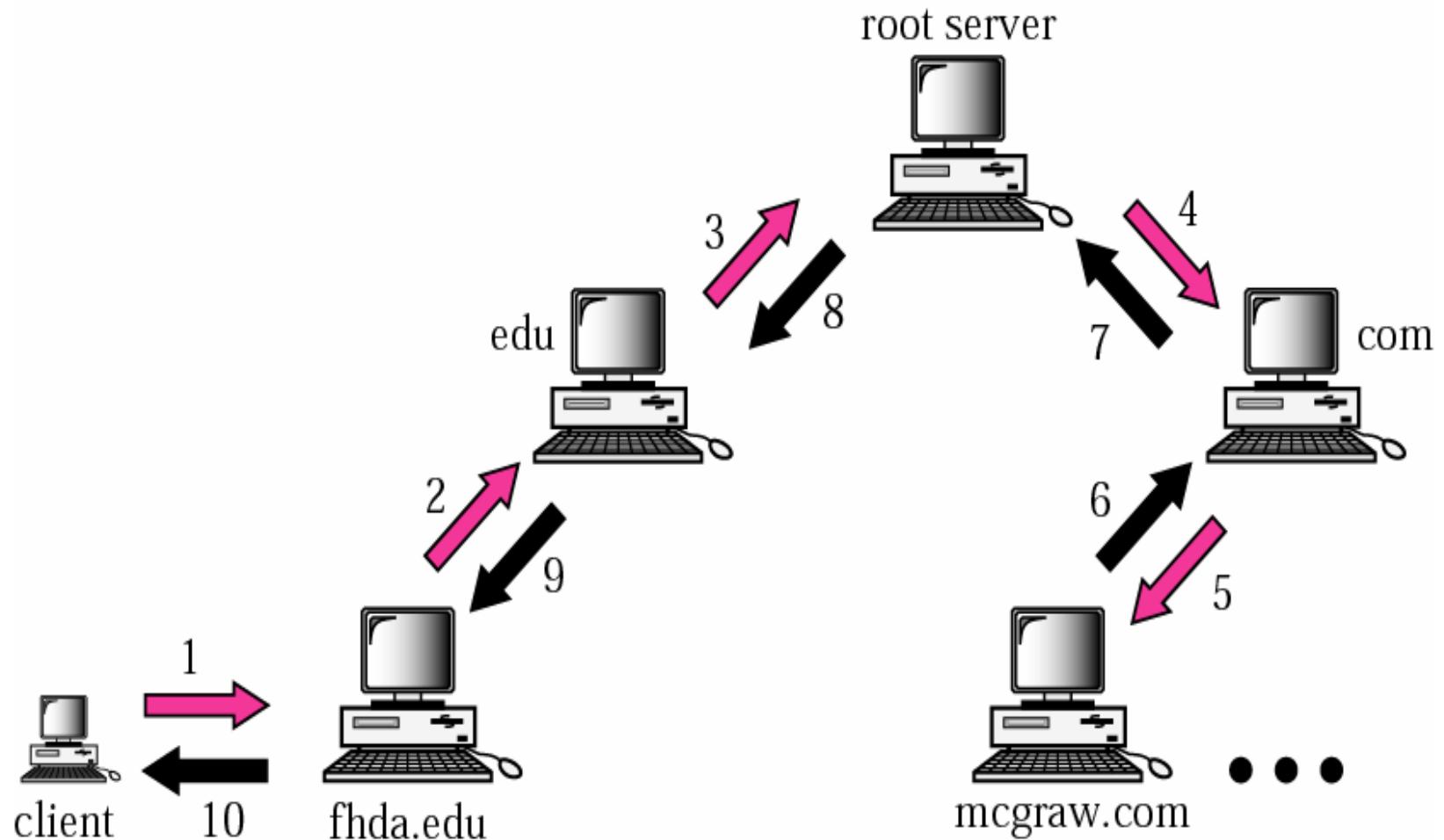
cs.hmme

www

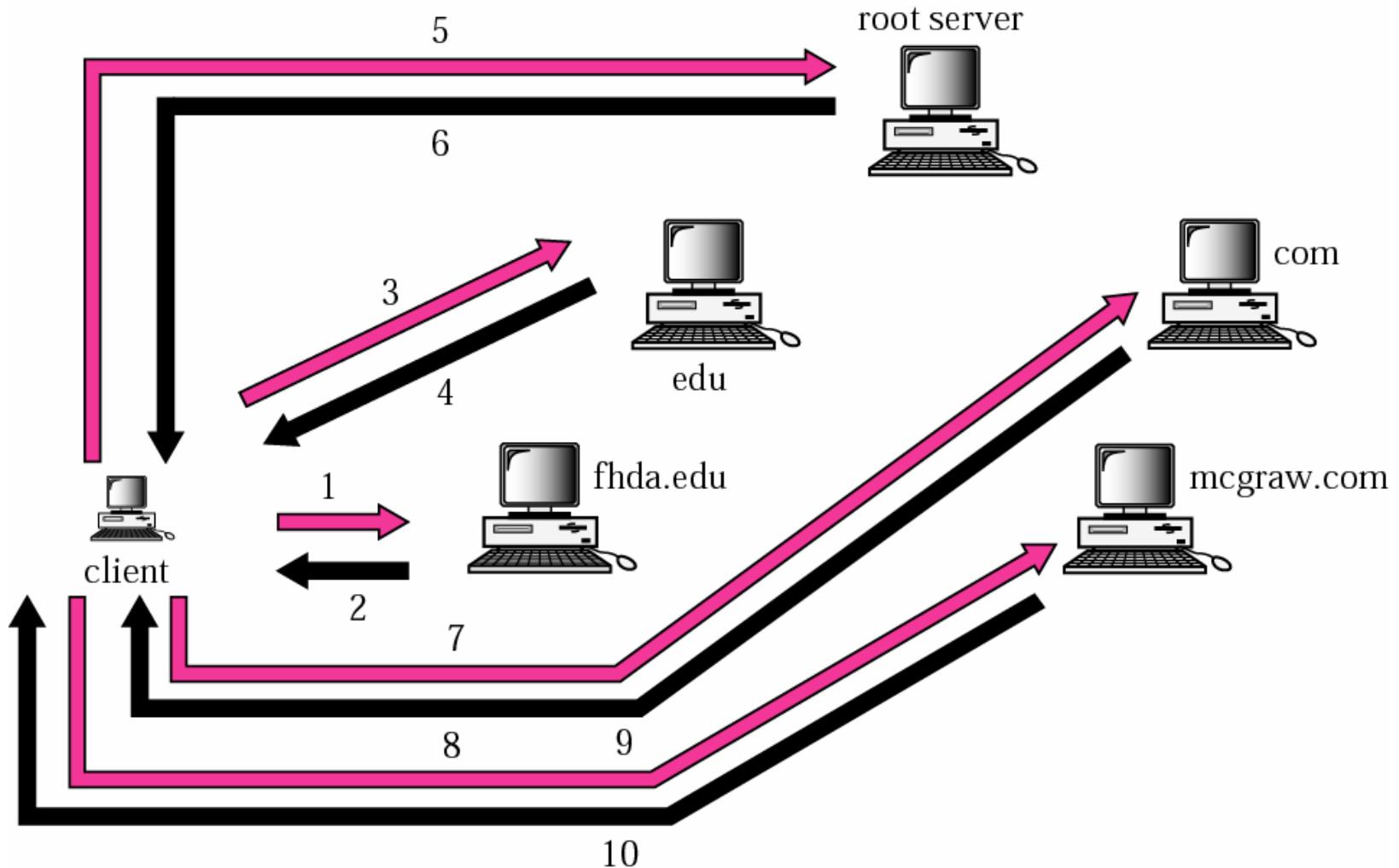
Hierarchy of Name server



Recursive resolution



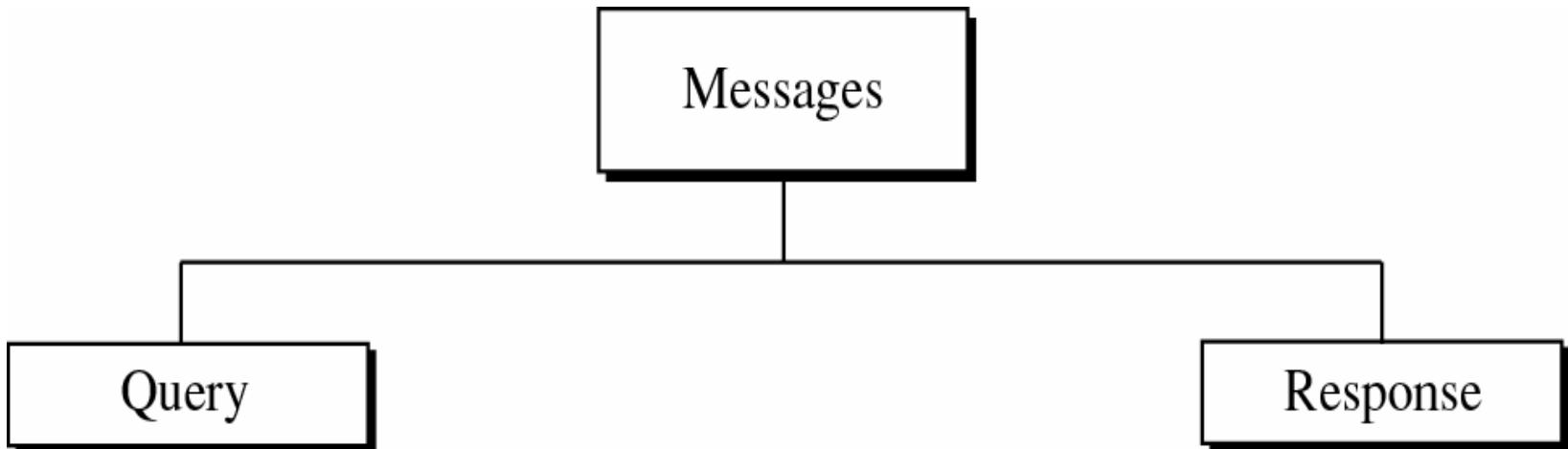
Interactive resolution





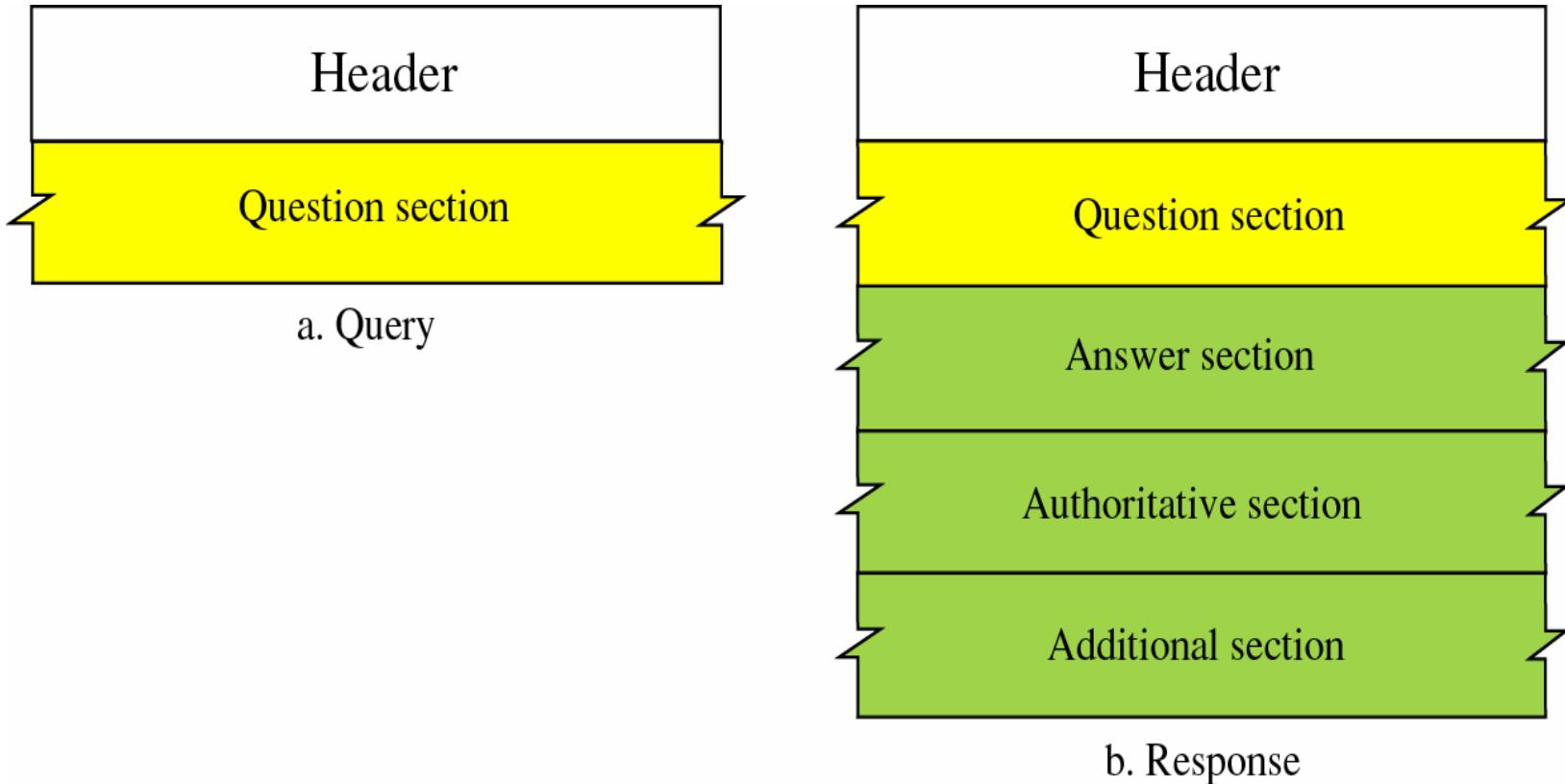
DNS Message

Global CyberSoft





DNS Message Format





Header Format

Global CyberSoft

Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

Flags Field



QR: Query/Response

OpCode: 0 standard, 1 inverse, 2 server status

AA: Authoritative

TC: Truncated

RD: Recursion Desired

RA: Recursion Available

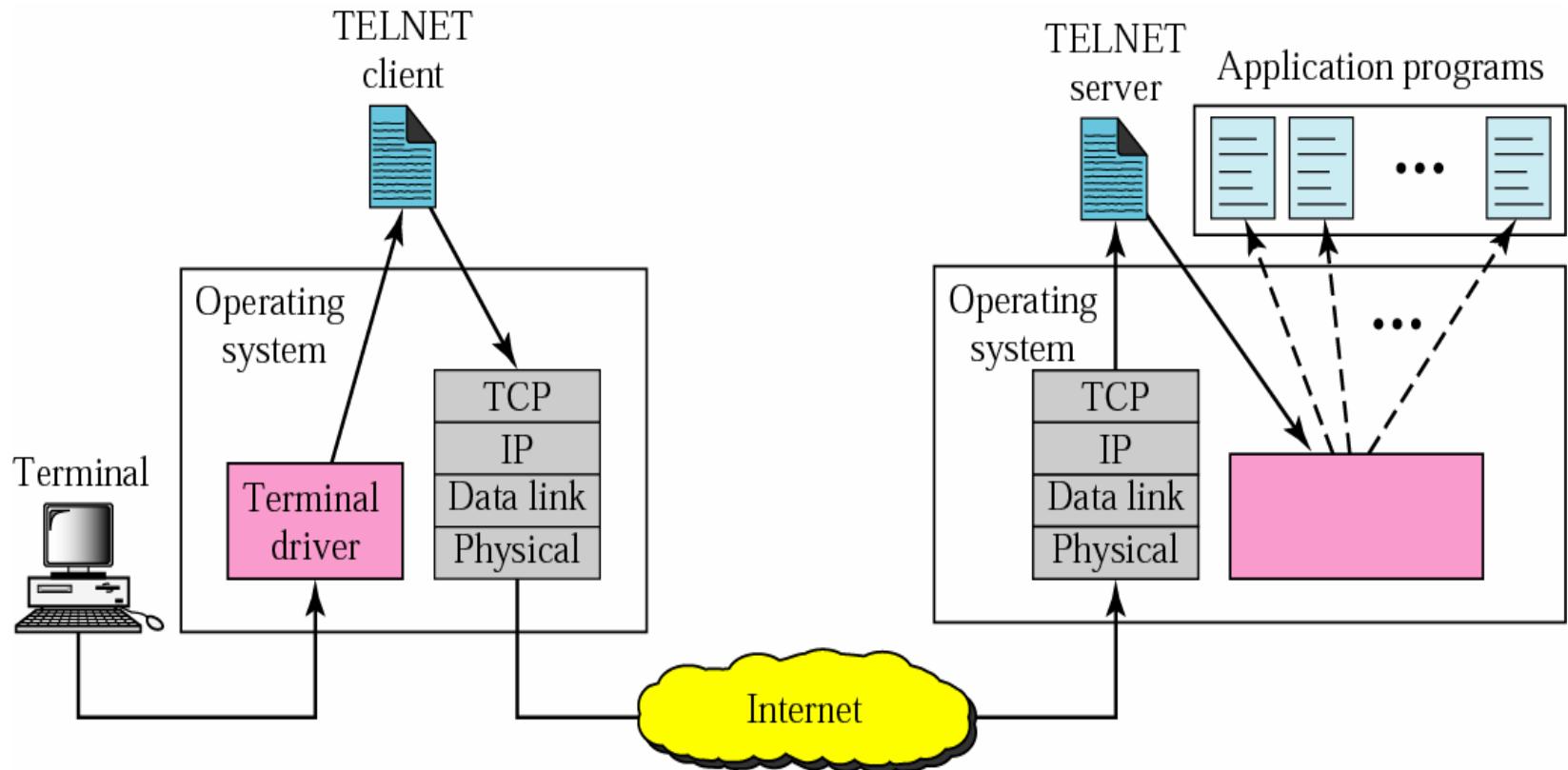
rCode: Status of the error



- Use the service of UDP or TCP, well-known port 53.
- Some DNS server:
 - Window DNS, built in Windows Server version.
 - Unix/Linux: bind.



Telnet



- Telnet is a standard application that almost every TCP/IP implementation provides. It works between hosts that use different operating systems.
- Telnet uses option negotiation between the client and server to determine what features each end can provide
- network virtual terminal (NVT): imaginary device from which both ends of the connection, the client and server, map their real terminal to and from.

- NVT ASCII:

- refers to the 7-bit U.S. variant of the ASCII character set used throughout the Internet protocol suite. Each 7-bit character is sent as an 8-bit byte, with the high-order bit set to 0
- An end-of-line is transmitted as the 2-character sequence CR (carriage return) followed by an LF (linefeed). (\r\n)
- A carriage return is transmitted as the 2-character sequence CR followed by a NUL (byte of 0). We show this as (\r\0).

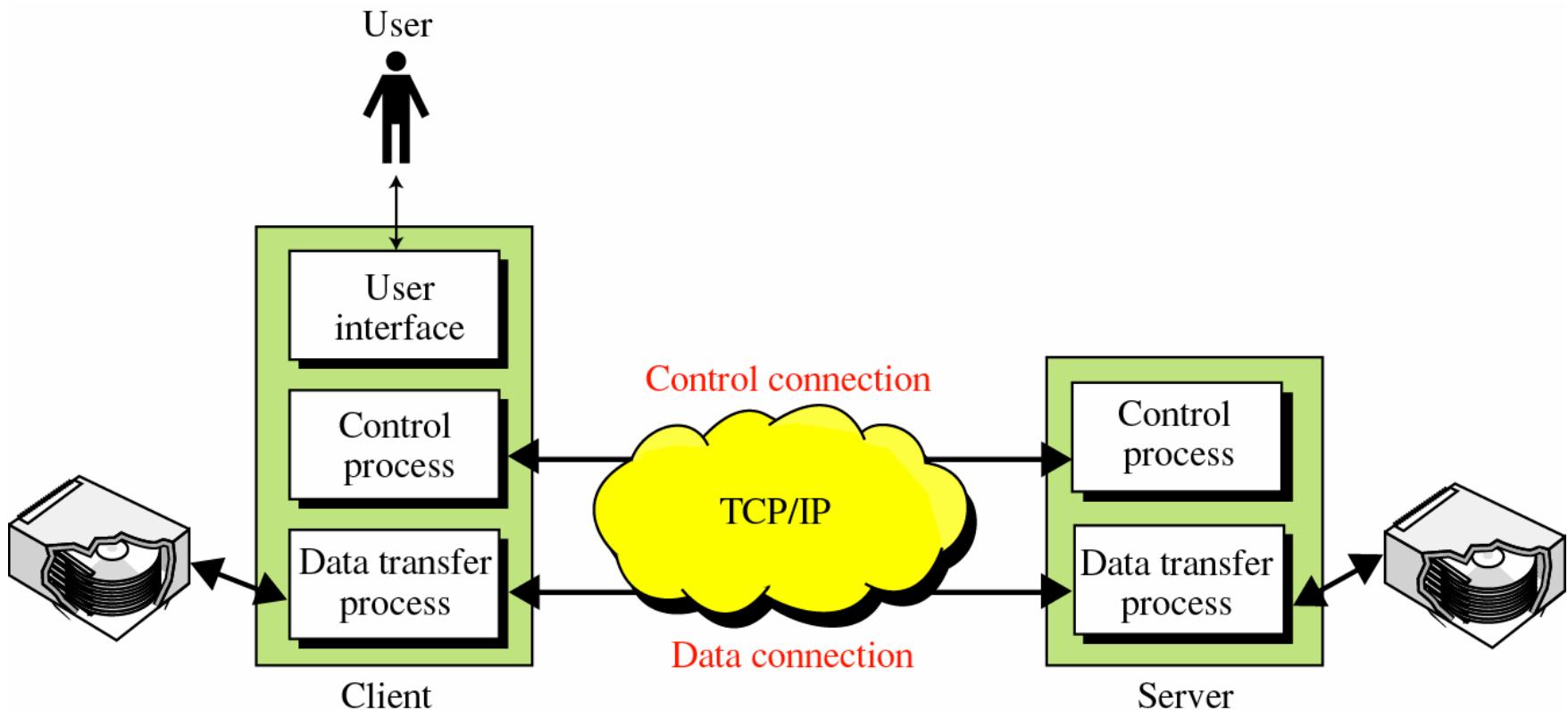
- Telnet Server: default port 23.
- Specification in RFC 854

File Transfer Protocol - FTP

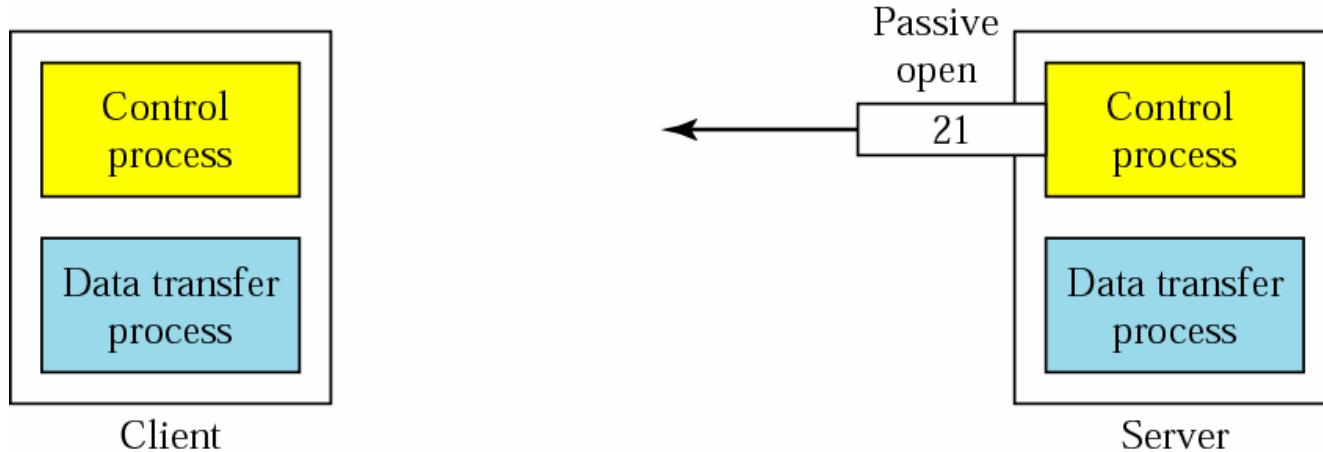
- FTP uses service of TCP
- 2 well-known ports:
 - 21: control connection
 - 20: data connection
- Ftp client.



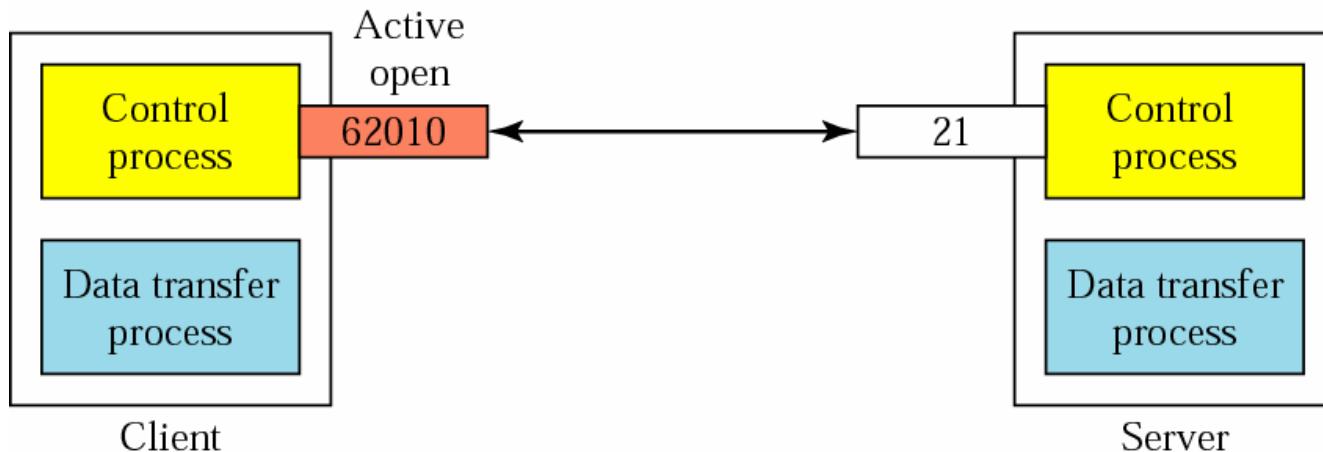
FTP



Opening the control connection

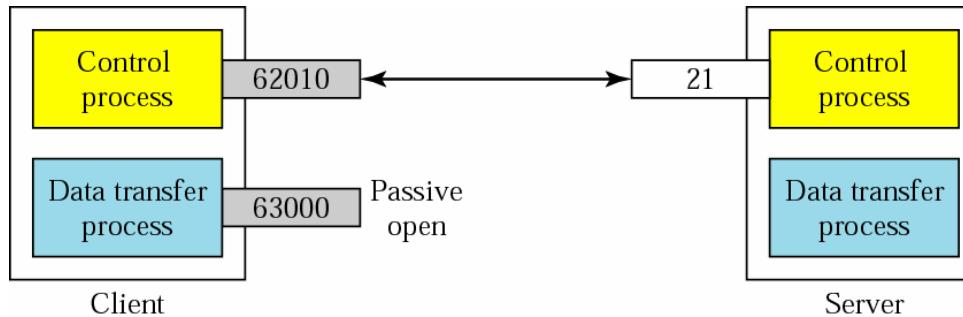


a. Passive open by server

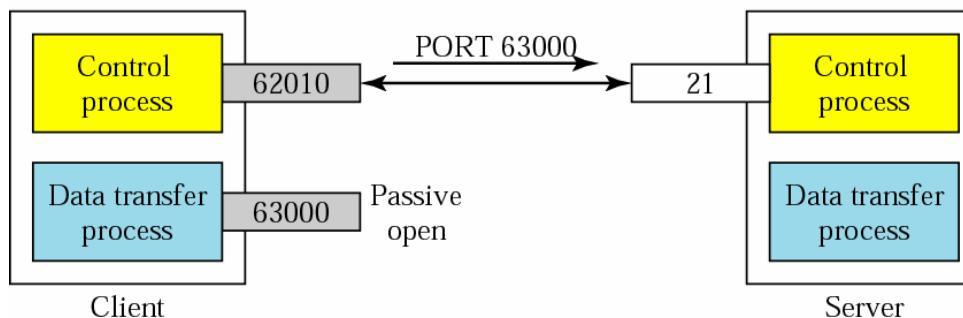


b. Active open by client

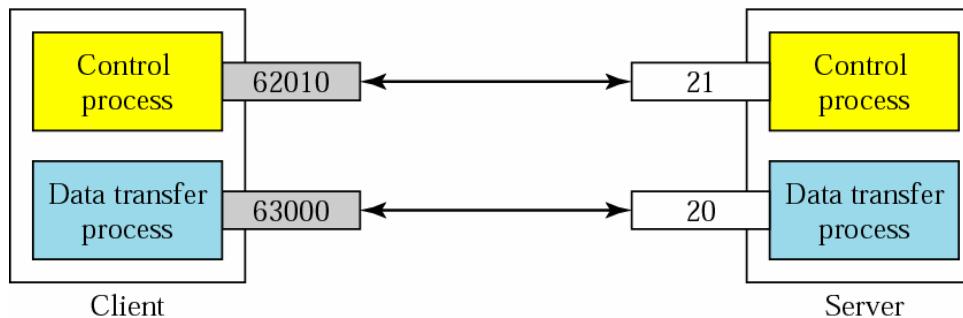
Creating data connection



a. Passive open by client



b. Sending ephemeral port number to server

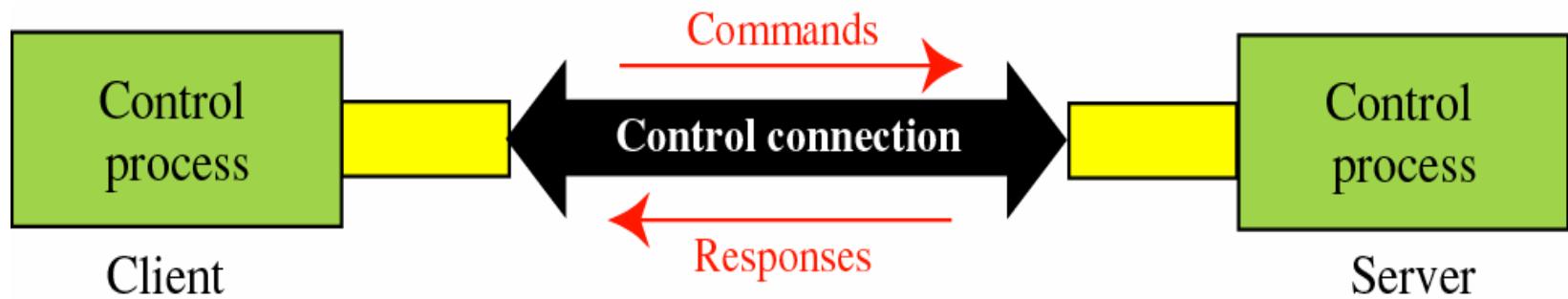


c. Active open by server



Command Processing

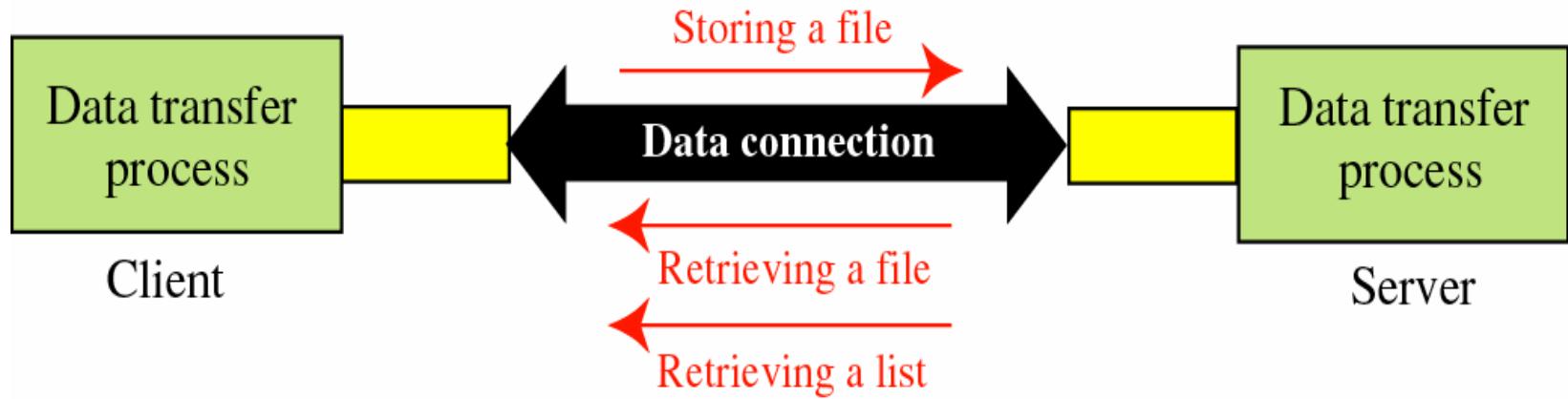
Global CyberSoft



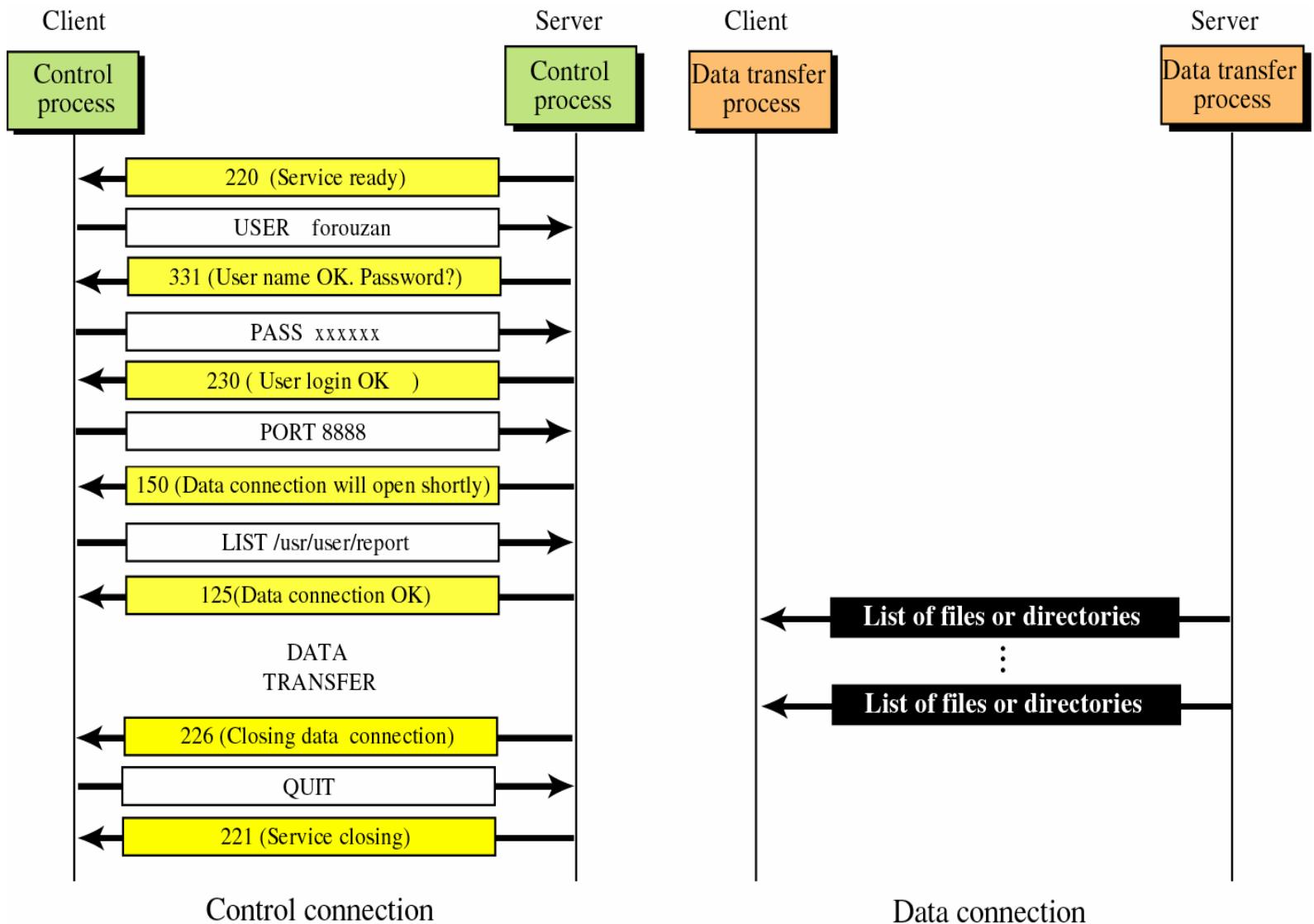


File Transfer

Global CyberSoft



Example



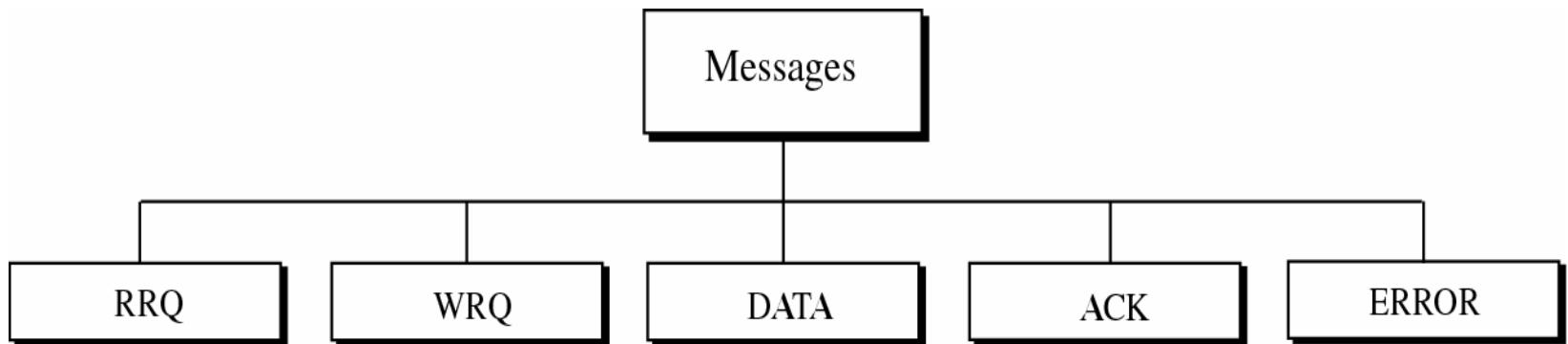


Trivial File Transfer Protocol

- Use service of UDP
- Well-known port 69



Message categories





RRQ: Read Request

OpCode = 1	File name	All 0s	Mode	All 0s
2 bytes	Variable	1 byte	Variable	1 byte

Mode: netascii or octet

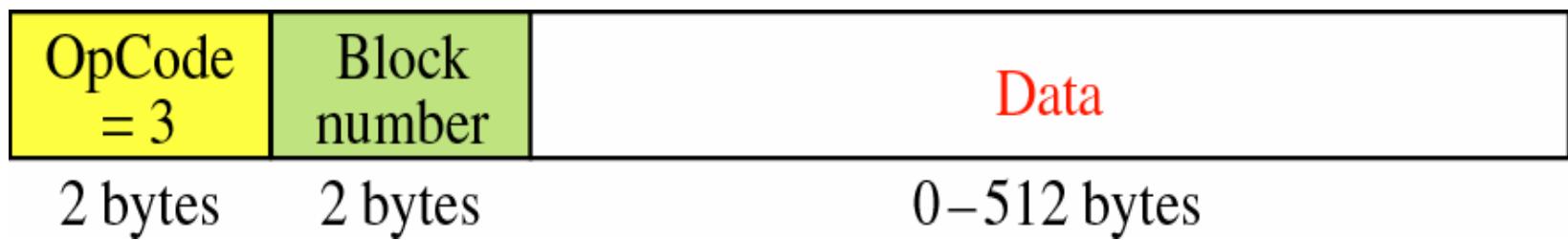


WRQ: Write Request





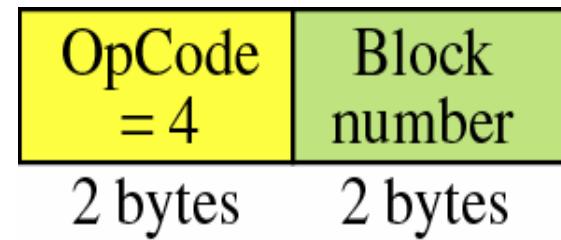
DATA Format





ACK Format

Global CyberSoft

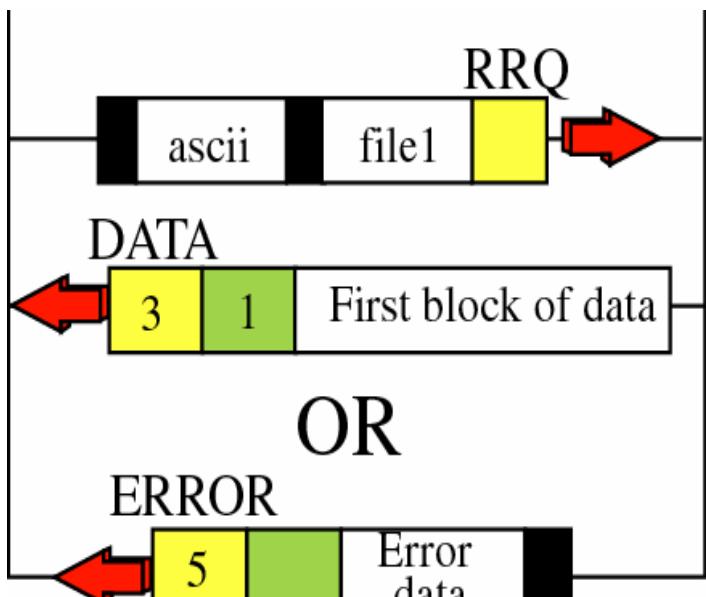




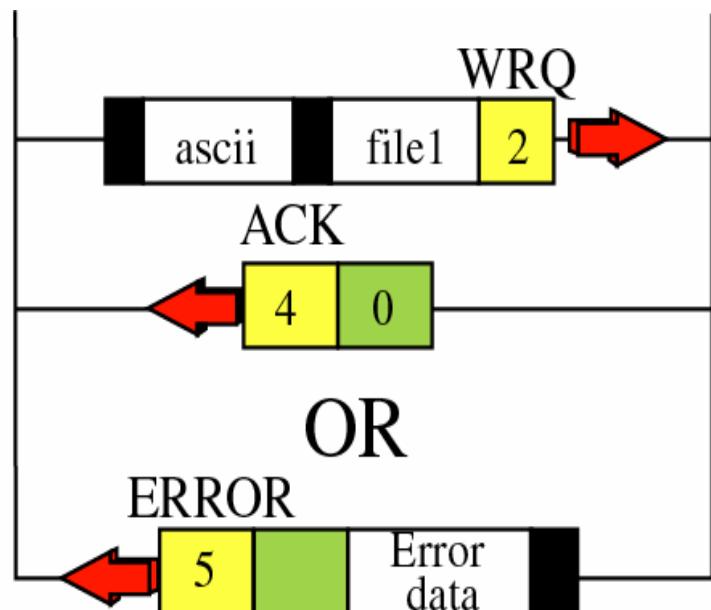
ERROR Format



Connection Establish



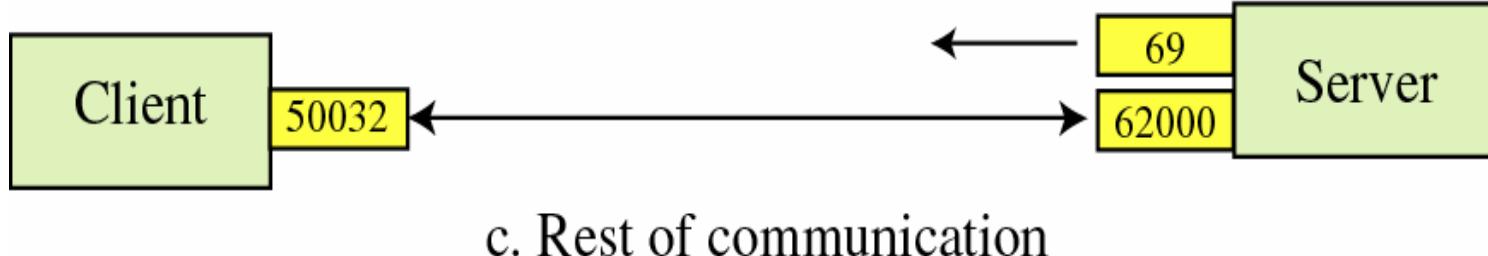
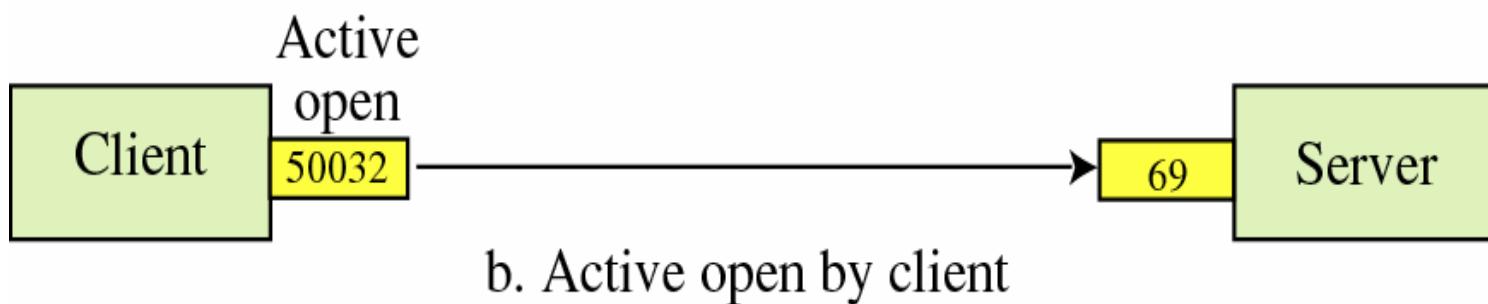
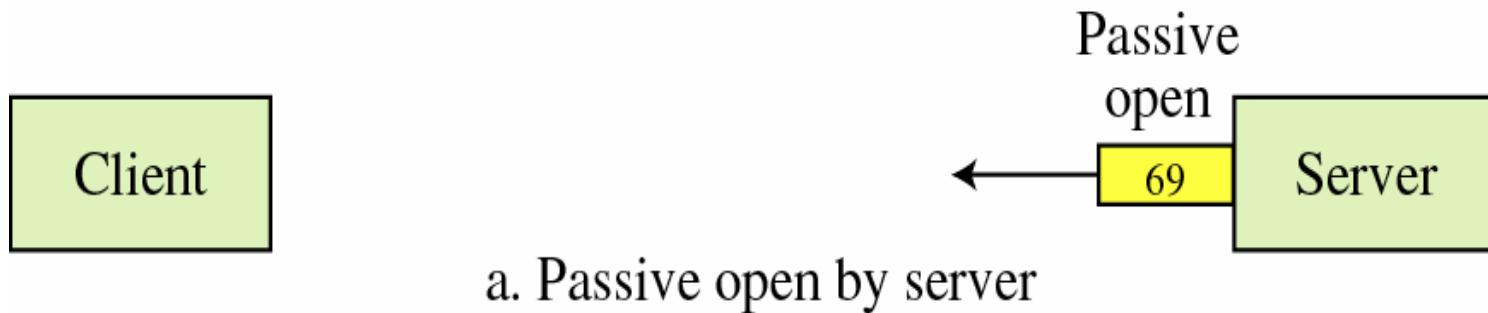
a. Connection for reading



b. Connection for writing

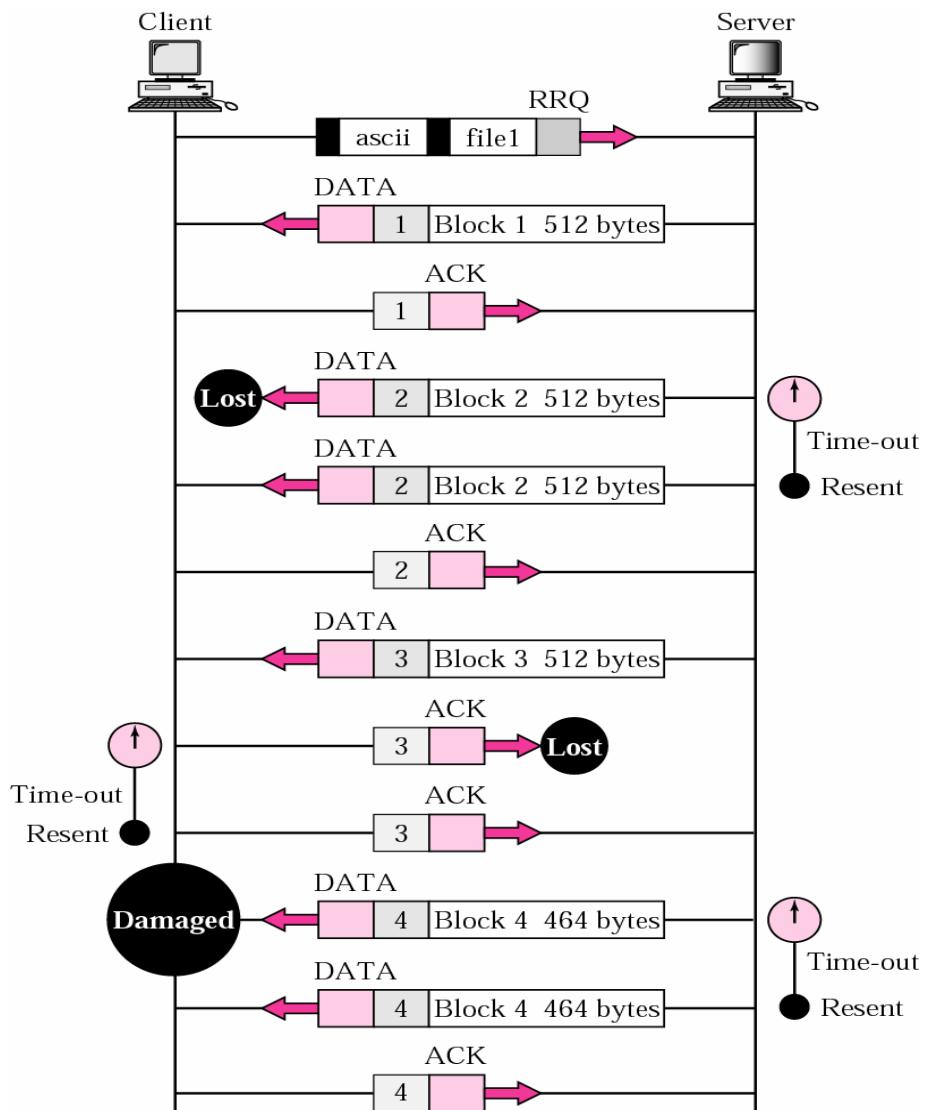


UDP Port Number used by TFTP



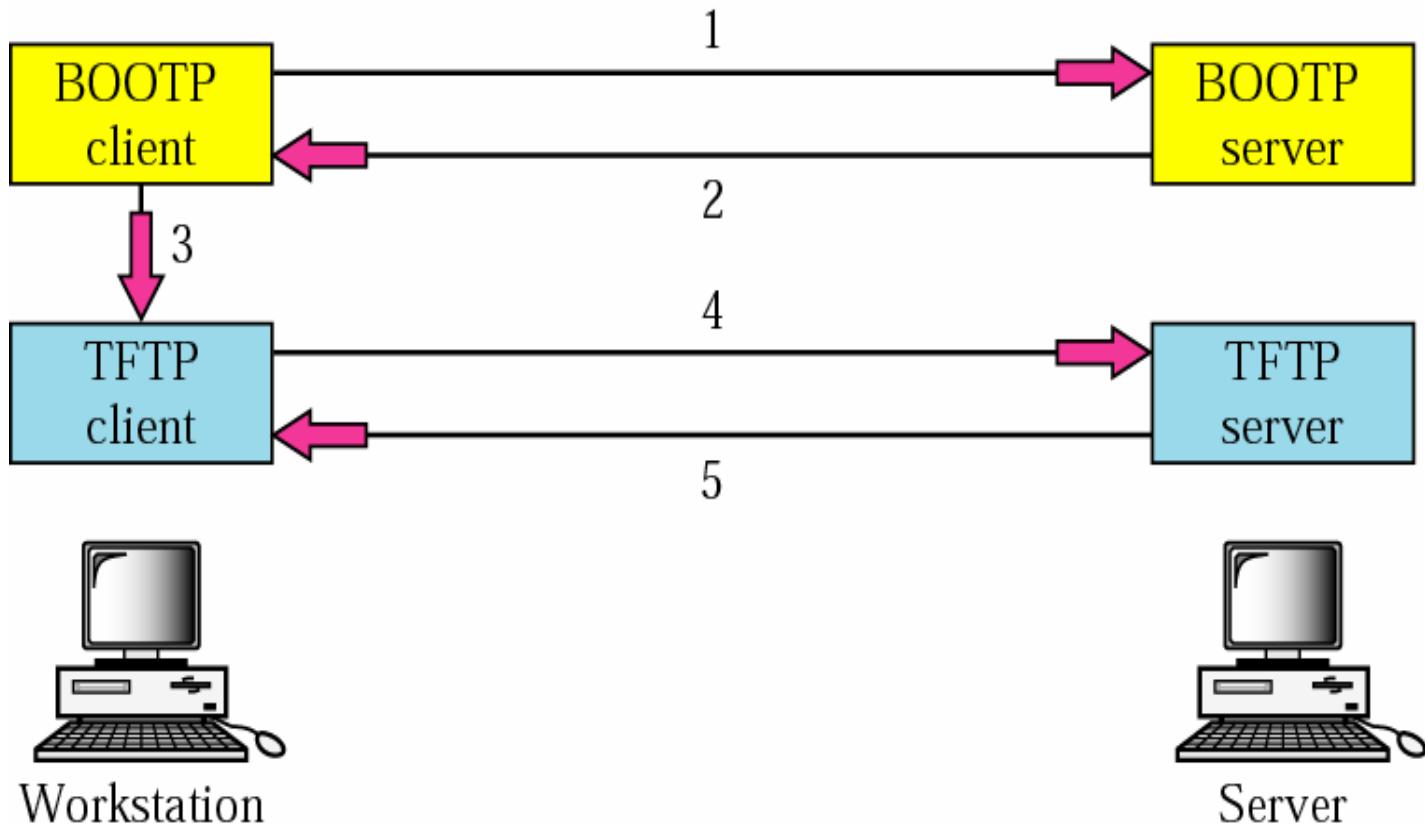


Example





Application: TFTP and BOOTP





Global CyberSoft

TCP/IP Utilities

- Ping
- Traceroute
- Telnet, rlogin
- Ssh
- Ftp
- Tcpdump/ethereal



Routing Basic

- Routing basic
- Static Routing
- Dynamic Routing
 - Routing Protocol
 - RIP v1/v2
 - OSPF
 - BGP

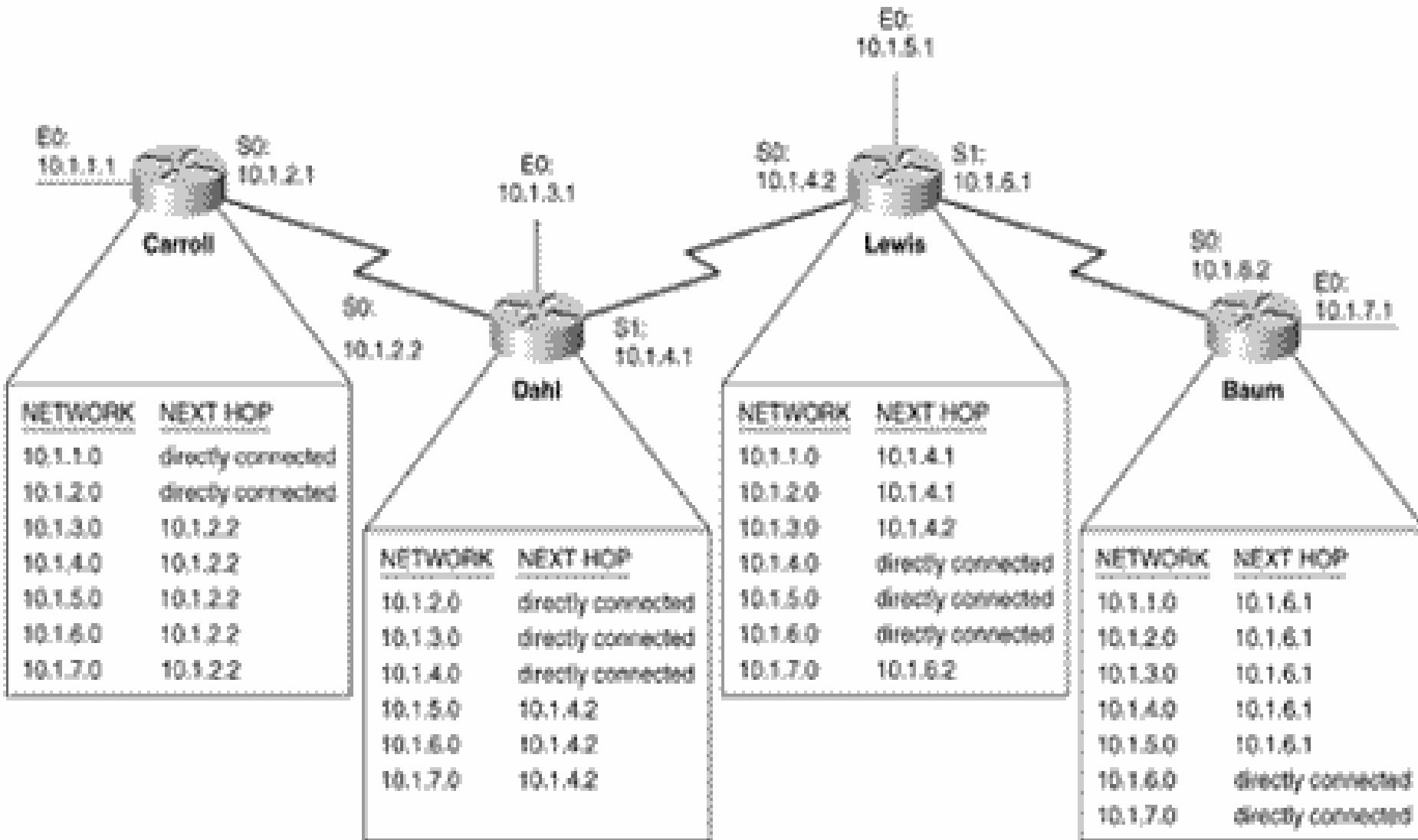
- Routing is the act of moving information across an internetwork from a source to a destination.
- Routing occurs at Layer 3 (the network layer).
- Two basic activities:
 - Determining optimal routing paths
 - Transporting information groups
- Lookup order:
 - Search for a matching host address.
 - Search for a matching network address.
 - Search for a default entry. (The default entry is normally specified in the routing table as a network entry, with a network ID of 0.)

Static Routing

- Static routing table contains information entered manually.
- Route entry:
 - A destination address.
 - A pointer to the destination.
- For each change in the network, administrator must manually change the static route as necessary.
- Static routes is used in:
 - Network with low bandwidth.
 - Network firewall architectures.
 - Connections with external partners.



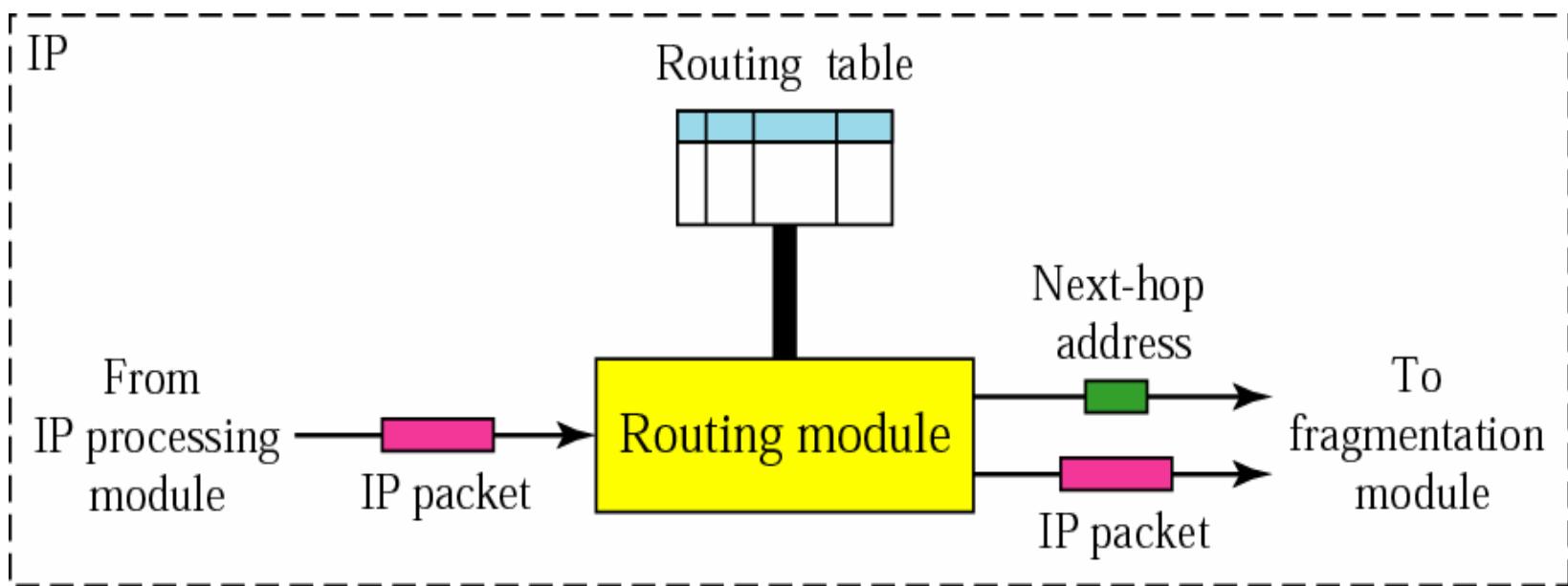
Static Routing





Routing Module

Global CyberSoft



Routing Table

Mask	Destination address	Next-hop address	Flags	Reference count	Use	Interface
255.0.0.0	124.0.0.0	145.6.7.23	UG	4	20	m2
.....
.....

Flags

- U** The router is up and running.
- G** The destination is in another network.
- H** Host-specific address.
- D** Added by redirection.
- M** Modified by redirection.

- A **dynamic routing table** is updated periodically using one of the dynamic routing protocols such as RIP, OSPF, or BGP.
- Dynamic routing protocol is the language a router speaks with other in order to share information about reachability and status of networks.
- Dynamic routing protocol not only perform the path determination and route table update functions but also determine the next-best path if the path to a destination becomes unusable

Dynamic Routing Protocol

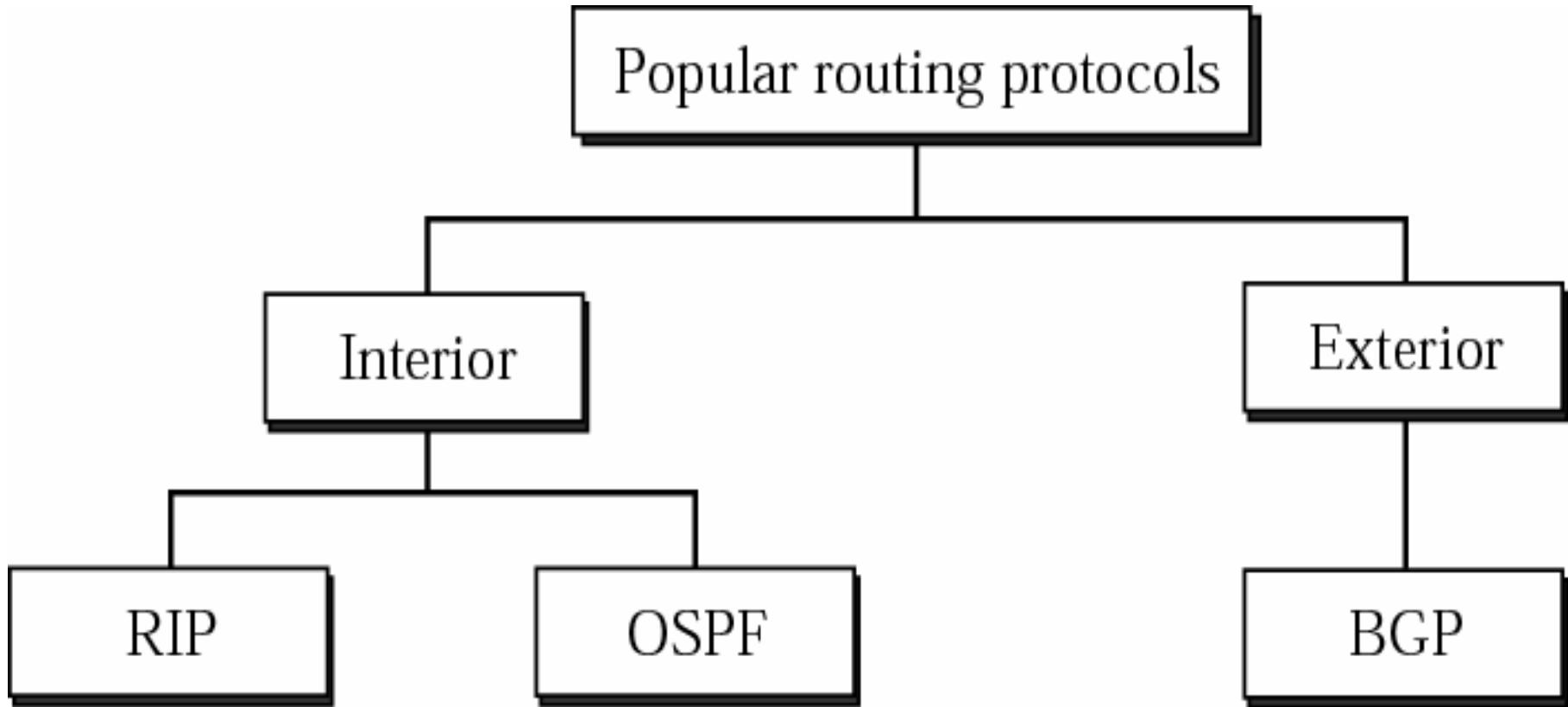
- A procedure for passing reachability information about networks to other routers.
- A procedure for receiving reachability information from other routers
- A procedure for determining optimal routes based on the reachability information it has and for recording this information in a route table
- A procedure for reacting to, compensating for, and advertising topology changes in an internetwork

Dynamic Routing Protocol

- Distance Vector Routing Protocols: RIP
- Link State Routing Protocols: OSPF
- Interior and Exterior Gateway Protocol: BGP



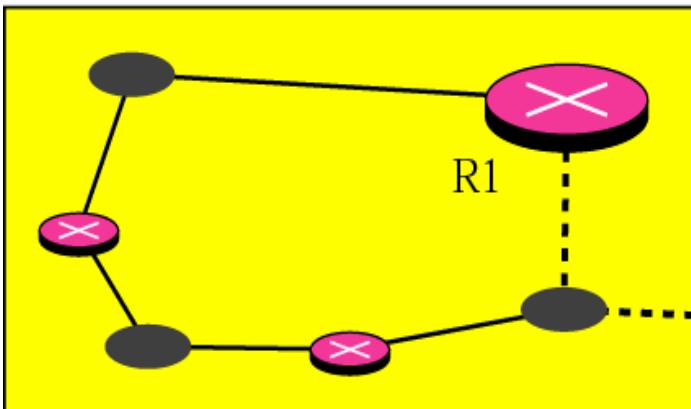
Interior and exterior routing



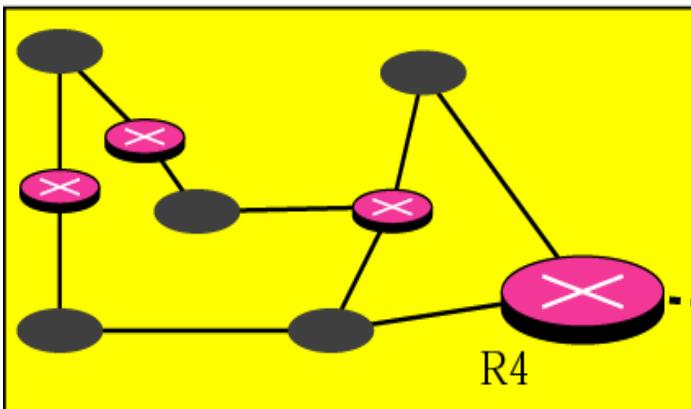
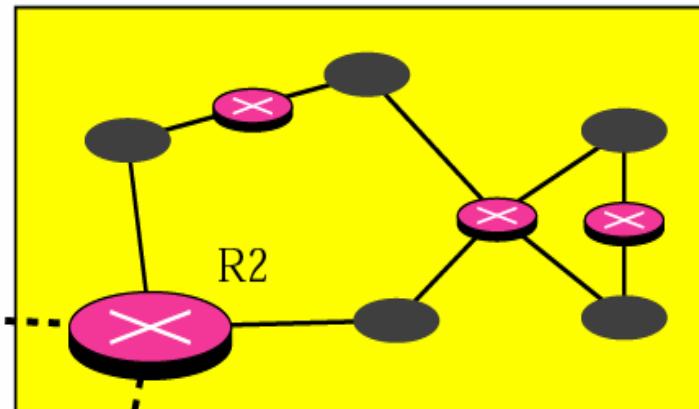


Autonomous System

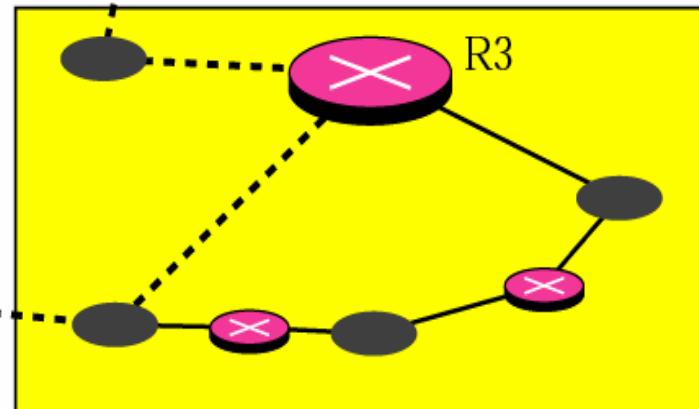
Autonomous system



Autonomous system



Autonomous system



Autonomous system

Routing Information Protocol (RIP)

- One of the most enduring of all routing protocols
- Use distance vectors to mathematically compare routes to identify the best path to any given destination address
- Request For Comments (RFC): 1058, 1388, 1723 (RIPv2)

Routing Update

- RIP sends routing-update messages at regular intervals and when the network topology changes.
- When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop.
- RIP routers maintain only the best route (the route with the lowest metric value) to a destination.
- After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change.
- These updates are sent independently of the regularly scheduled updates that RIP routers send

RIP Routing Metric

- RIP uses a single routing metric (hop count) to measure the distance between the source and a destination network.
- Each hop in a path from source to destination is assigned a hop count value, which is typically 1.
- When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop

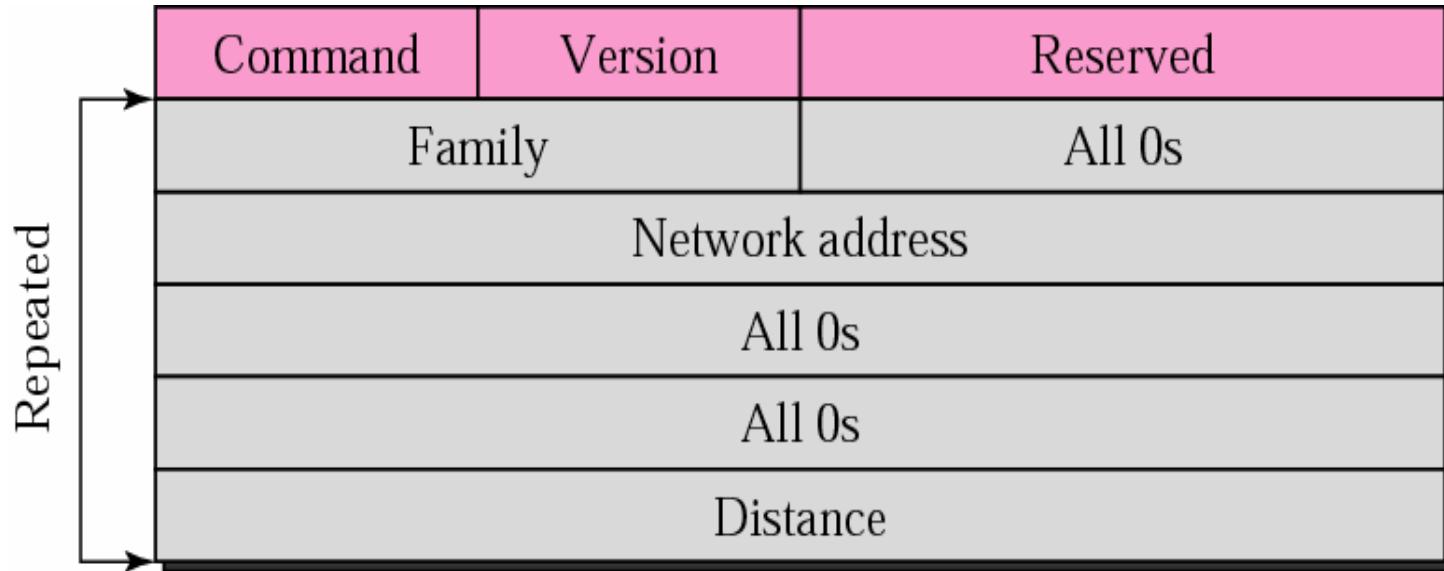
RIP Stability Feature

- RIP prevents routing loops from continuing indefinitely by implementing a limit on the number of hops allowed in a path from the source to a destination.
- The maximum number of hops in a path is 15.
- If a router receives a routing update that contains a new or changed entry, and if increasing the metric value by 1 causes the metric to be infinity (that is, 16), the network destination is considered unreachable.
- The downside of this stability feature is that it limits the maximum diameter of a RIP network to less than 16 hops.

- RIP uses numerous timers to regulate its performance. These include a routing-update timer, a route-timeout timer, and a route-flush timer.
- The routing-update timer clocks the interval between periodic routing updates. Generally, it is set to 30 seconds, with a small random amount of time added whenever the timer is reset. This is done to help prevent congestion, which could result from all routers simultaneously attempting to update their neighbors.
- Each routing table entry has a route-timeout timer associated with it. When the route-timeout timer expires, the route is marked invalid but is retained in the table until the route-flush timer expires.

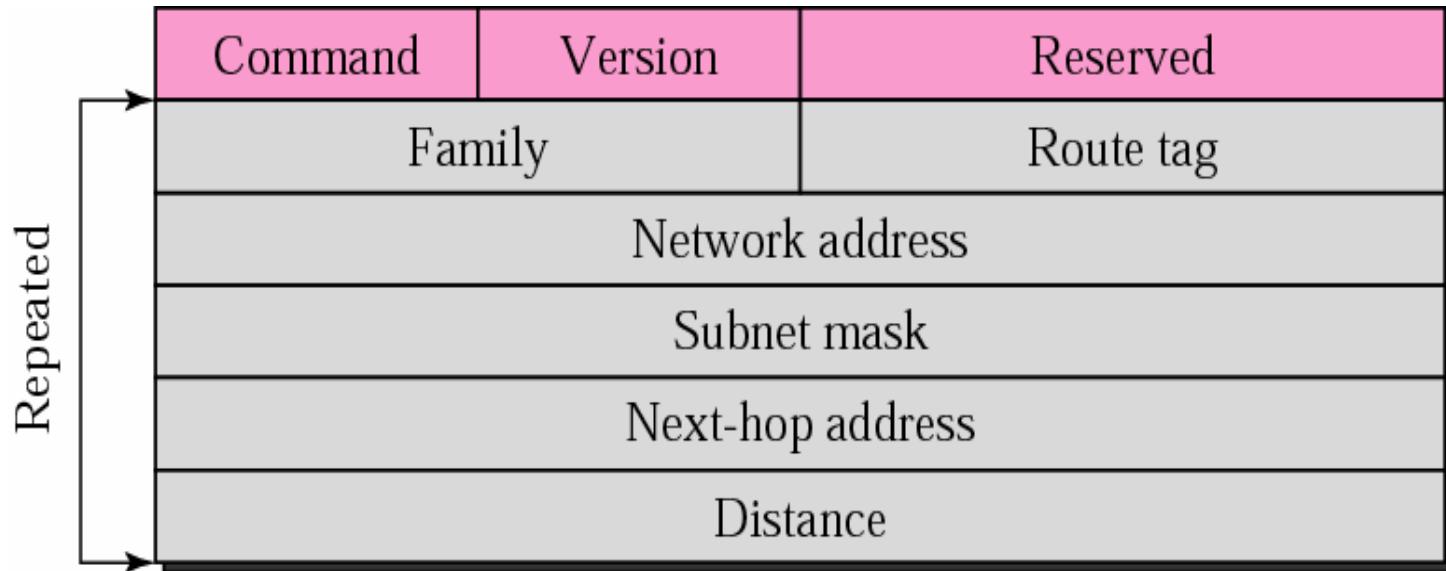


RIP Message Format





RIP v2 Message Format

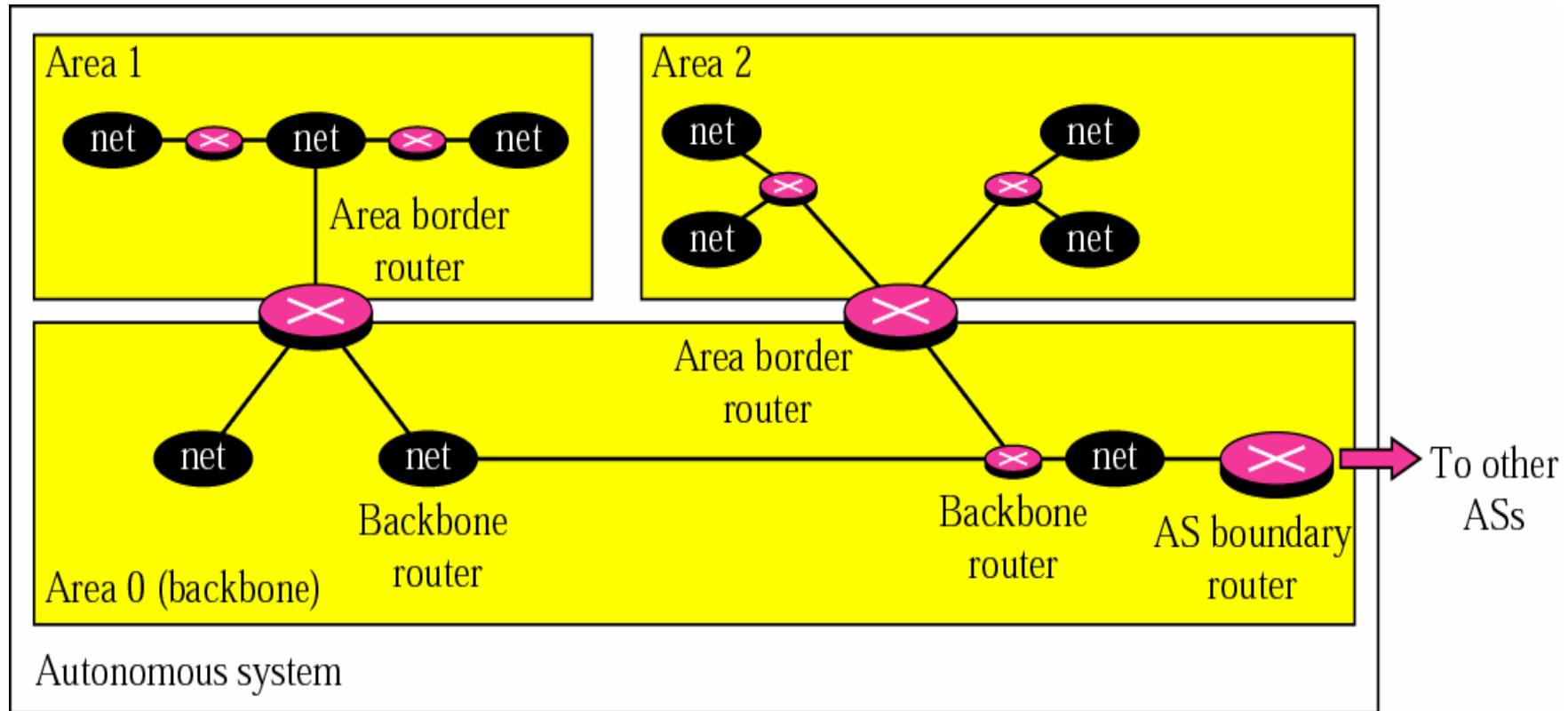




RIP v2

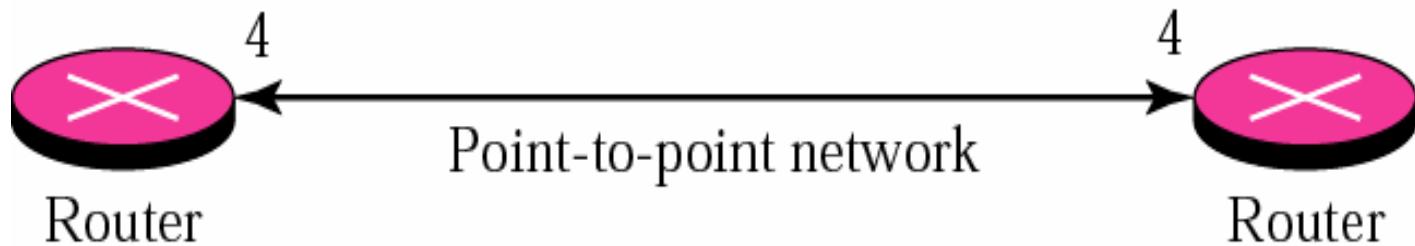
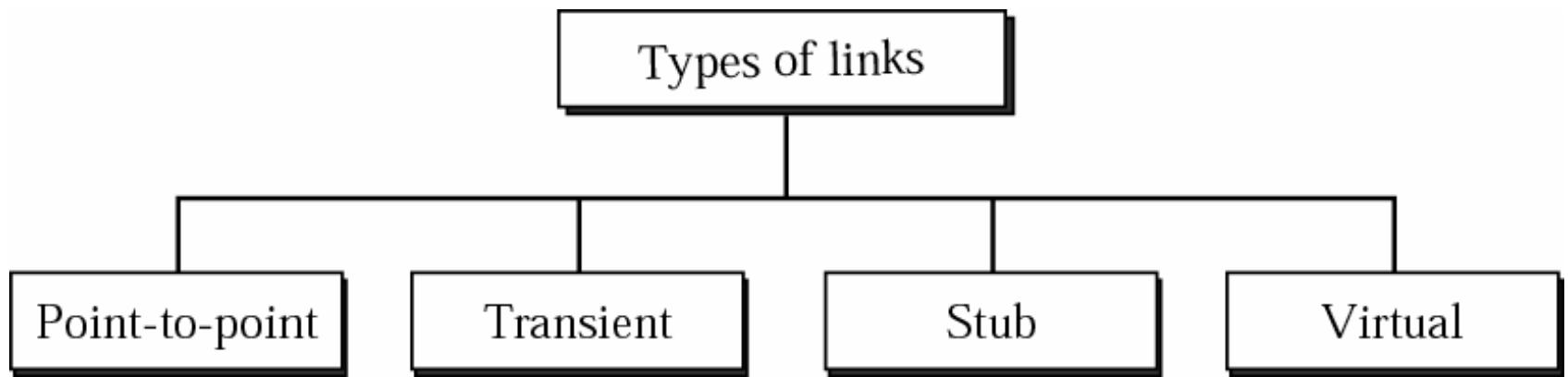
- RIPv2 support CIDR
- RIP uses the services of UDP on well-known port 520

Open Shortest Path First: OSPF

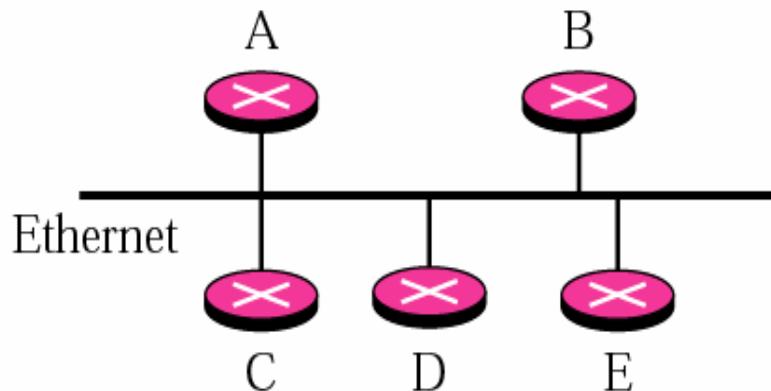




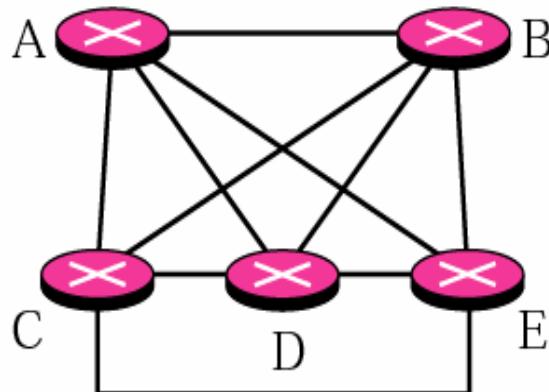
OSPF: Type of links



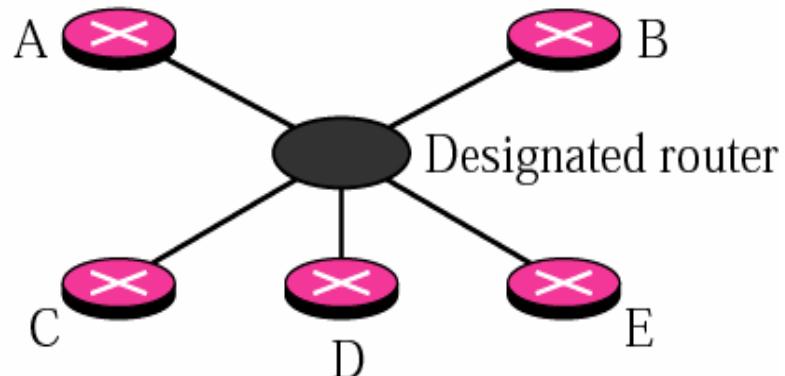
Type of link



a. Transient network



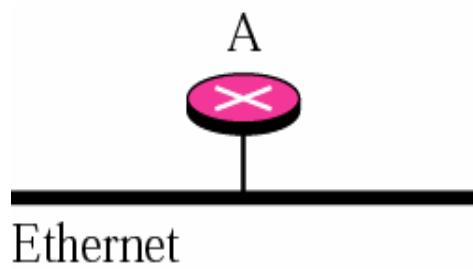
b. Unrealistic representation



c. Realistic representation



Stub link

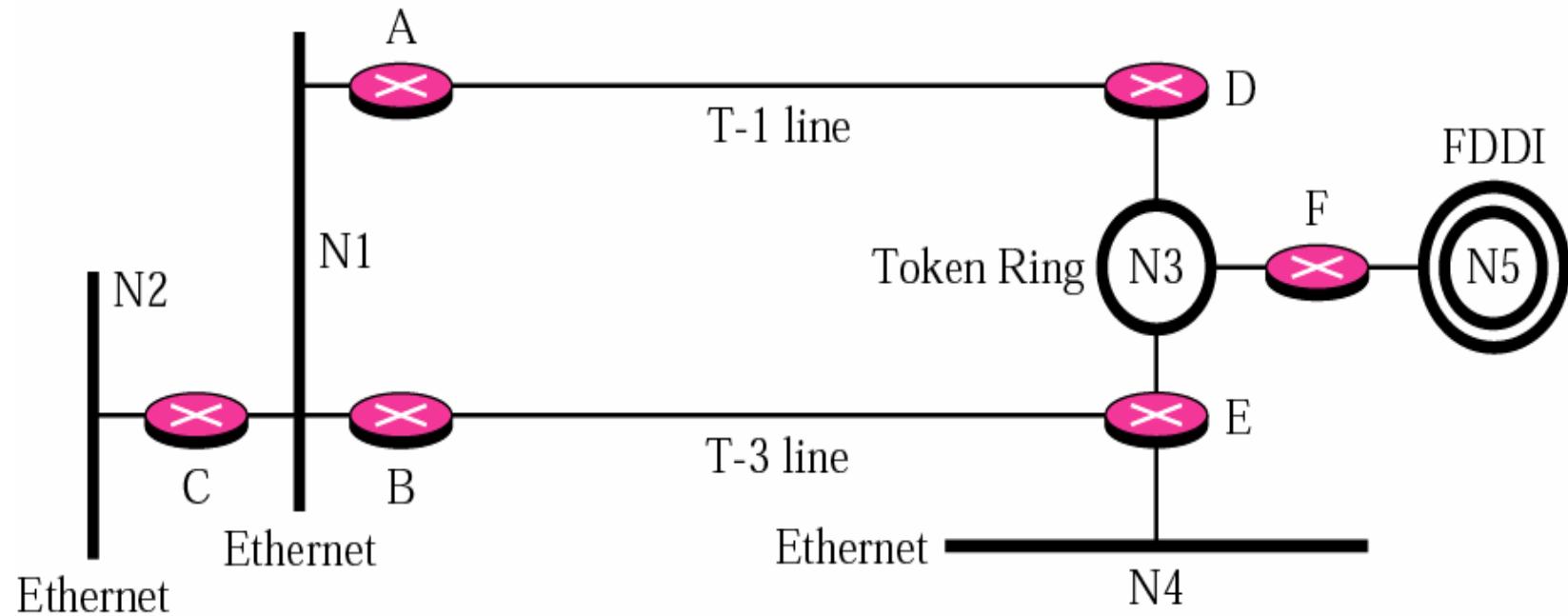


a. Stub network



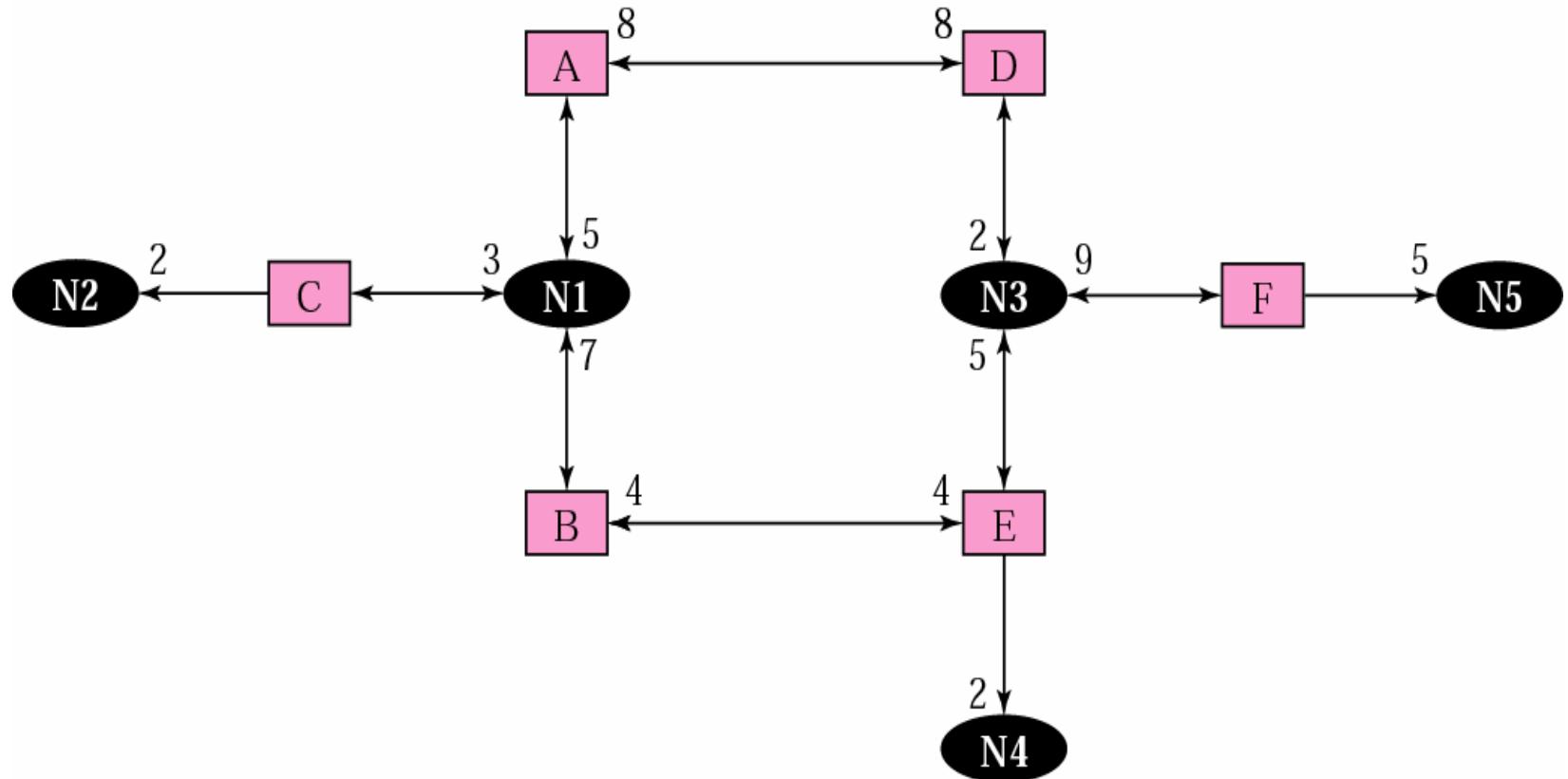
b. Representation

An example of Internet



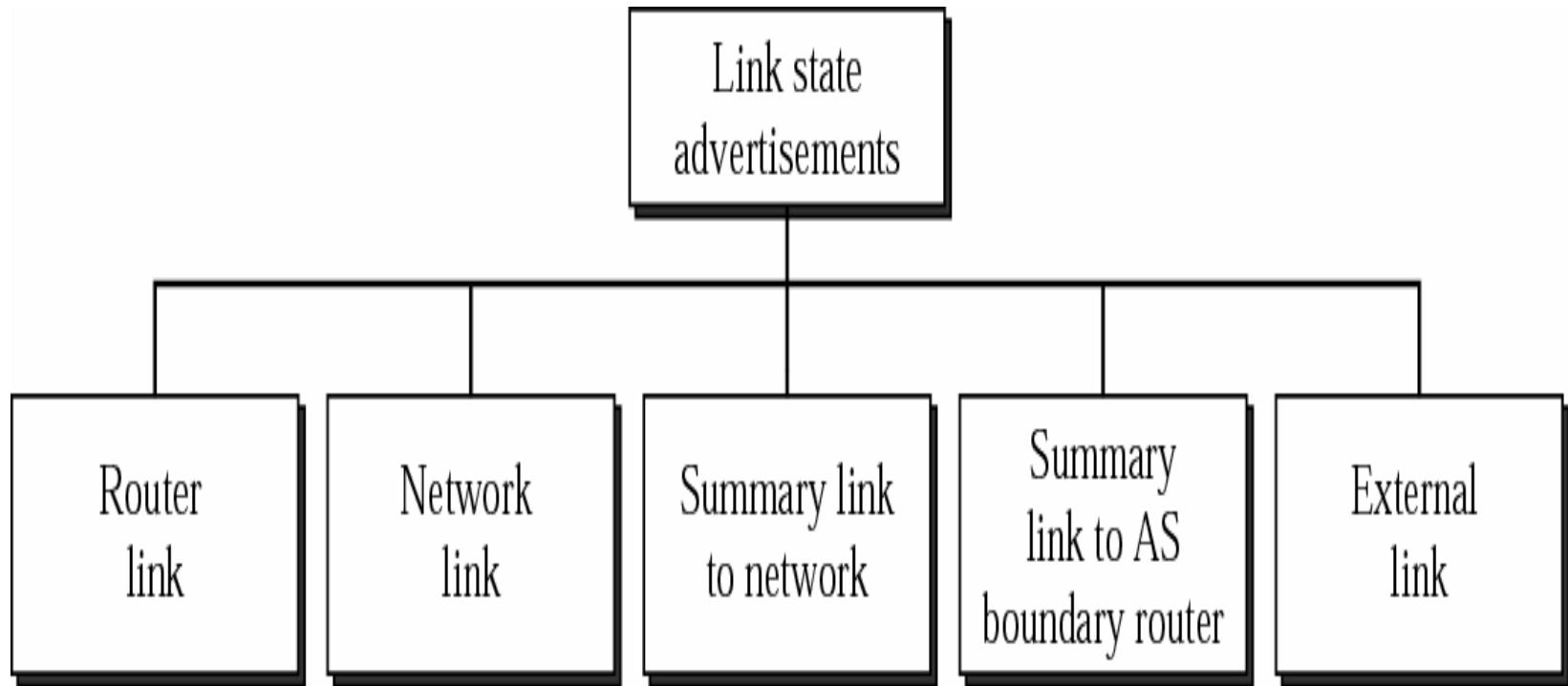


Graphic presentation of an Internet



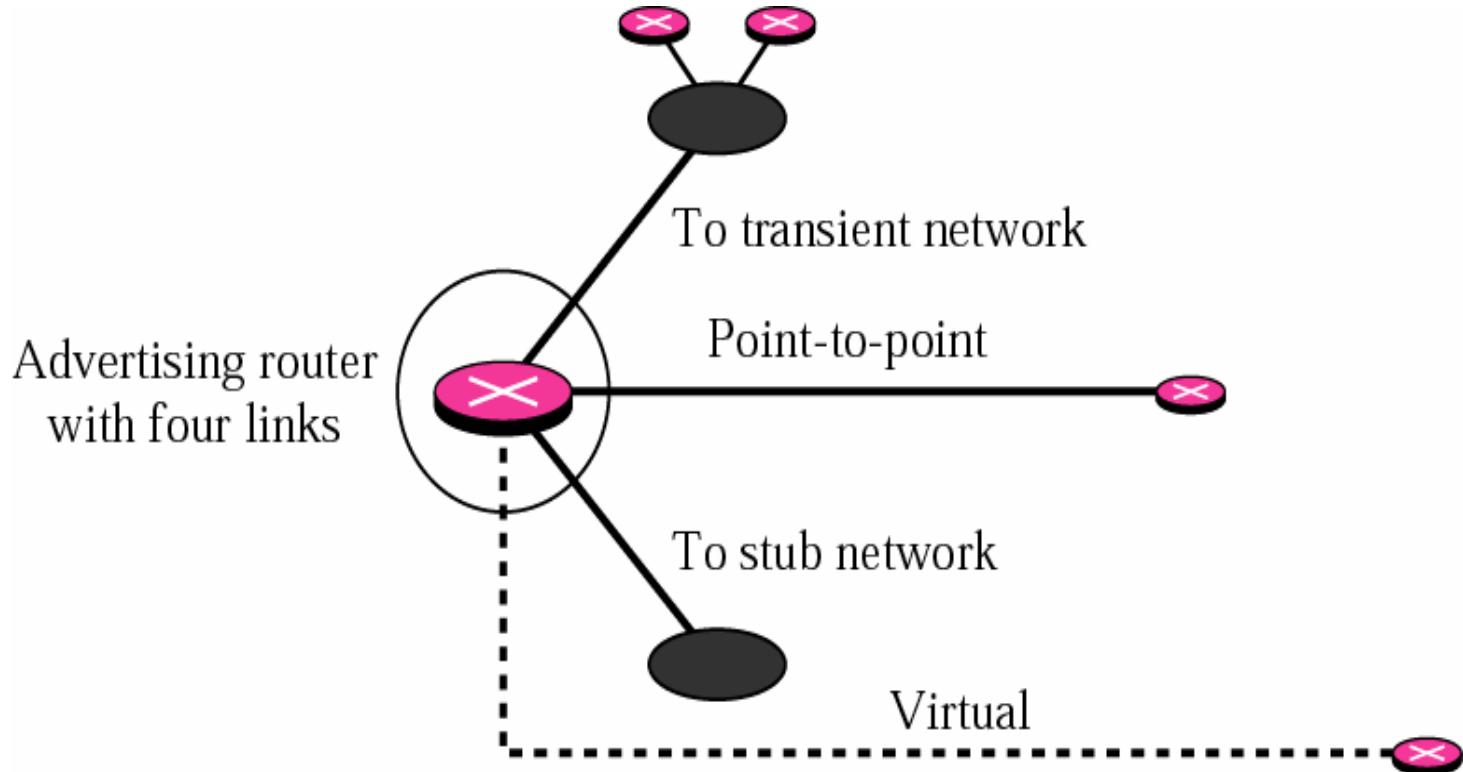


Type of LSA



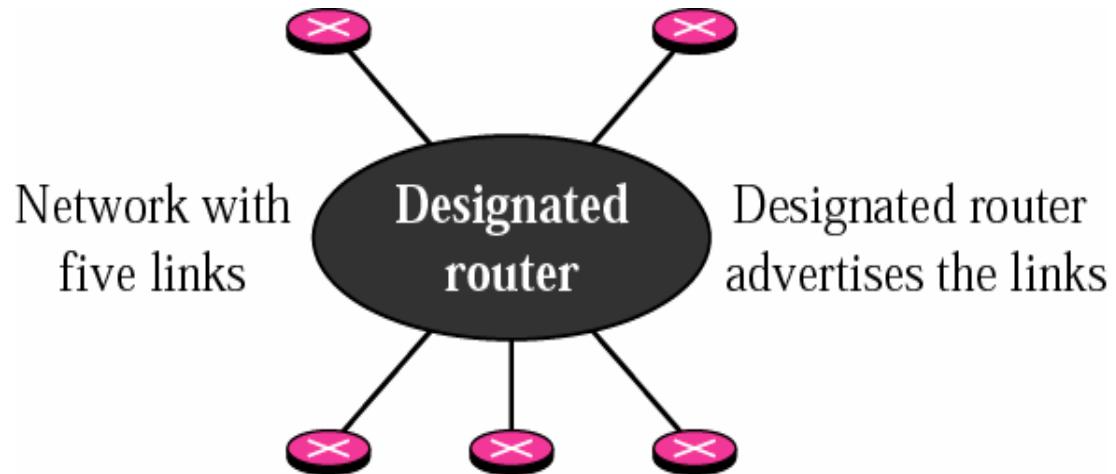


Router Link



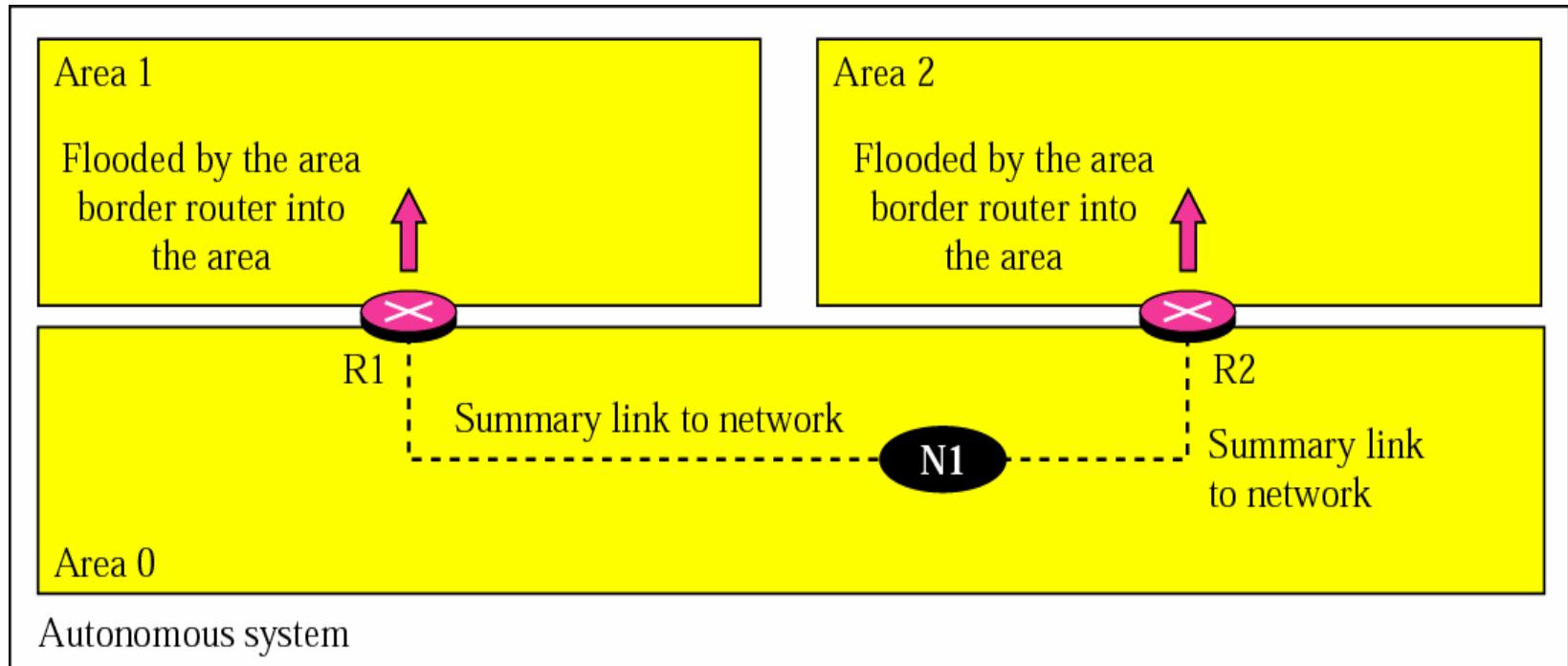


Network Link



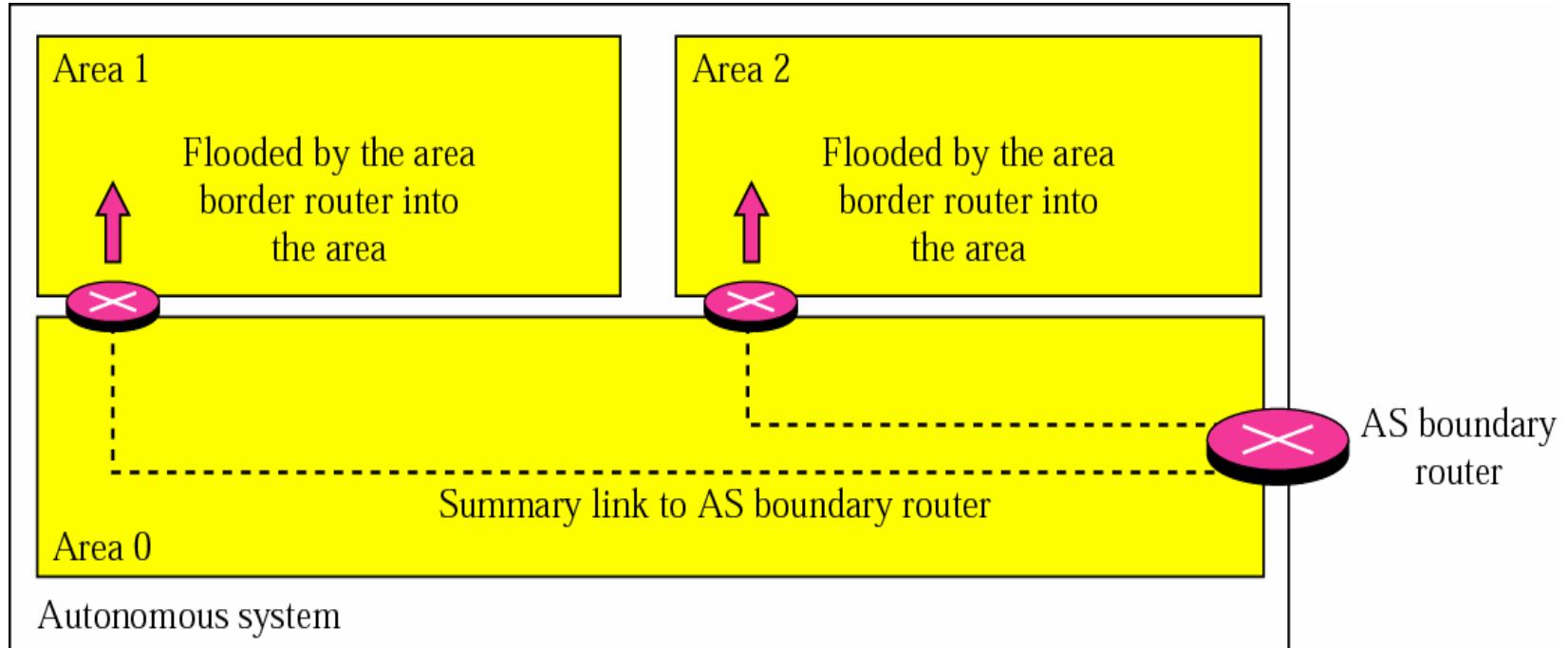


Summary link to network





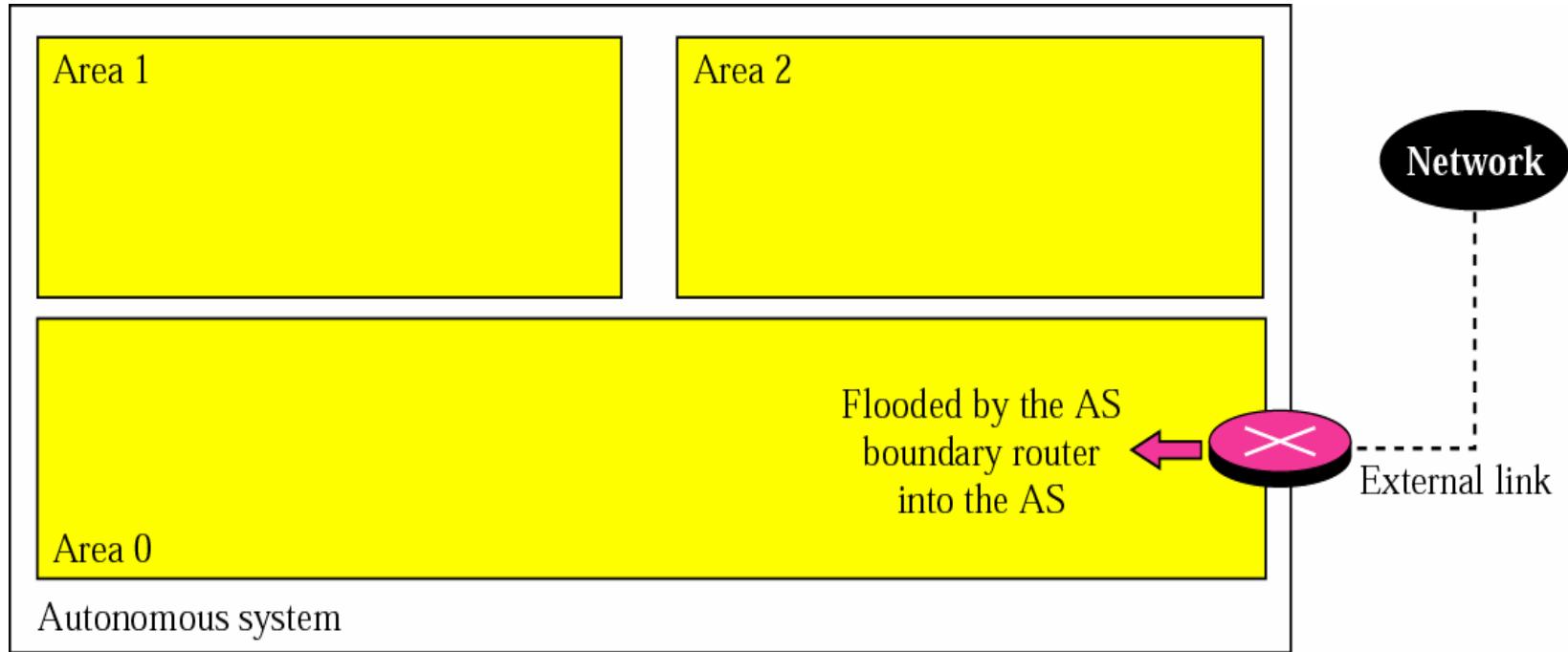
Summary link to AS boundary router





External link

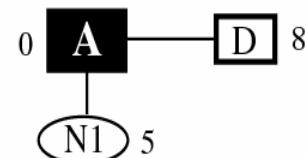
Global CyberSoft



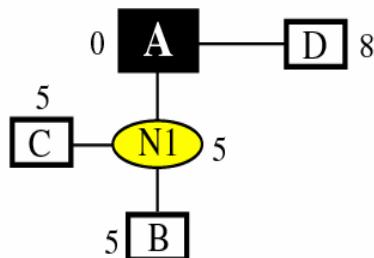
Shortest Path Calculation



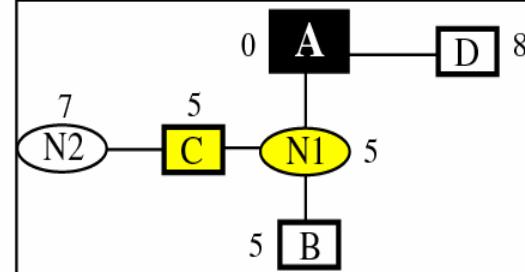
a. Start with A



b. Make A permanent, add its neighbors

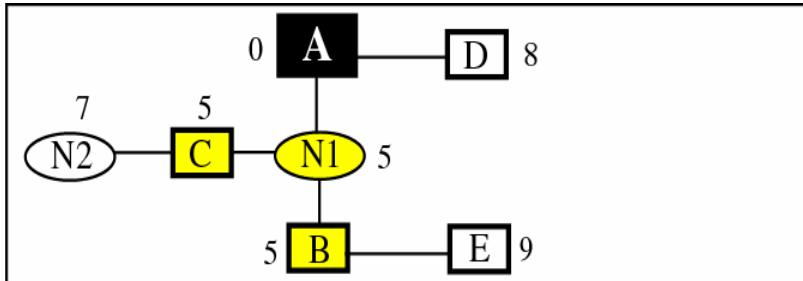


c. Make N1 permanent, add its neighbors

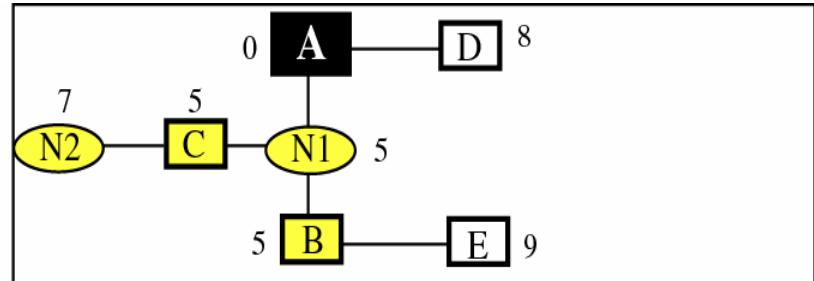


d. Make C permanent, add its neighbors

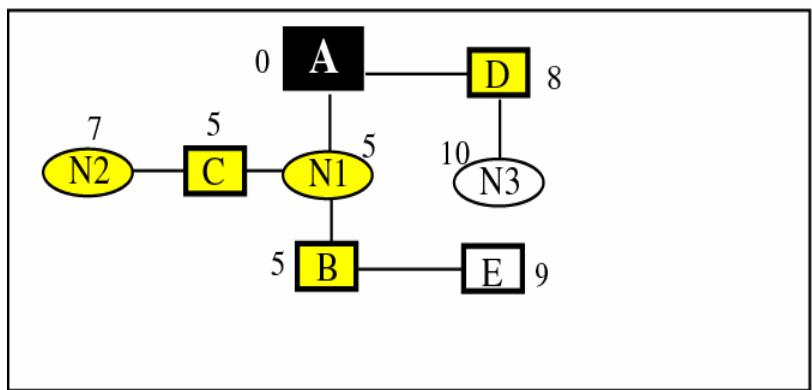
Shortest Path Calculation



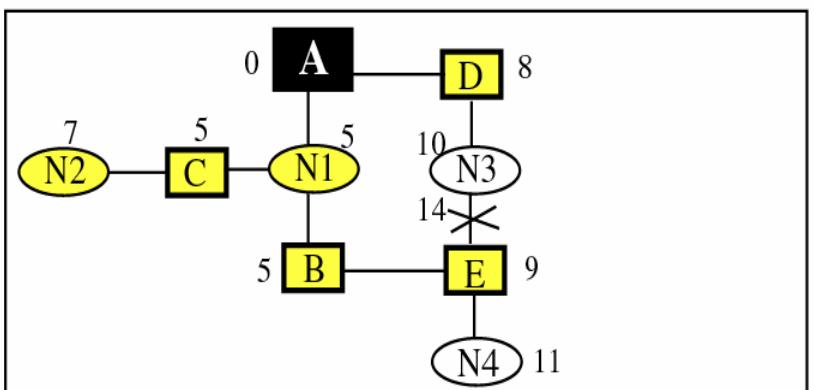
e. Make B permanent, add its neighbors



f. Make N2 permanent



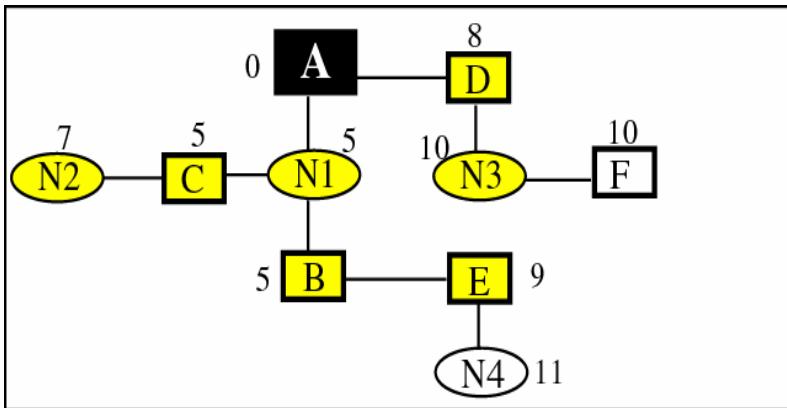
g. Make D permanent, add its neighbors



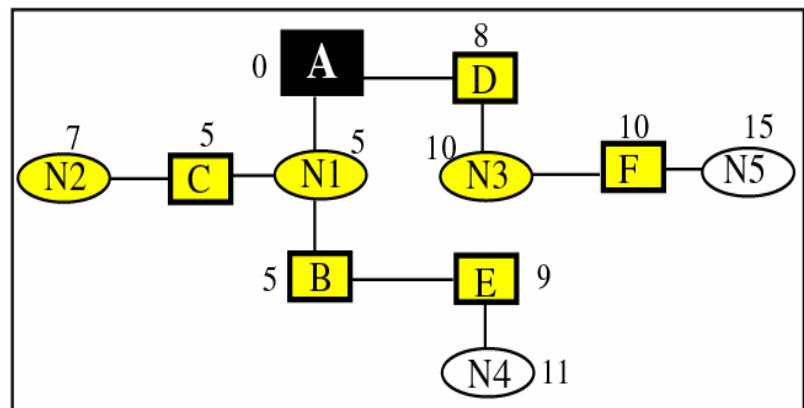
h. Make E permanent, add its neighbors



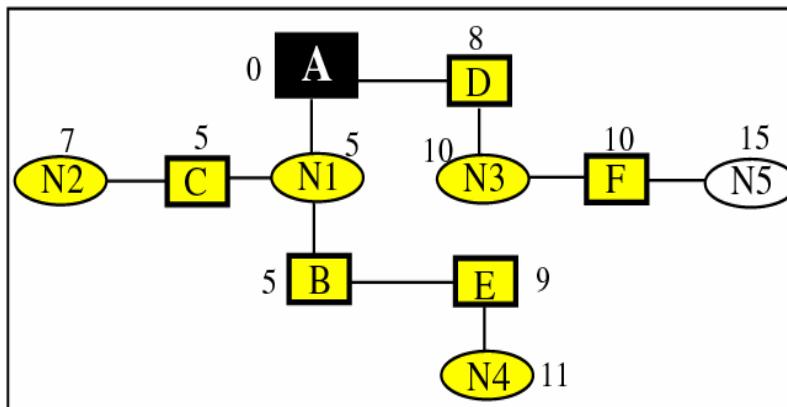
Shortest Path Calculation



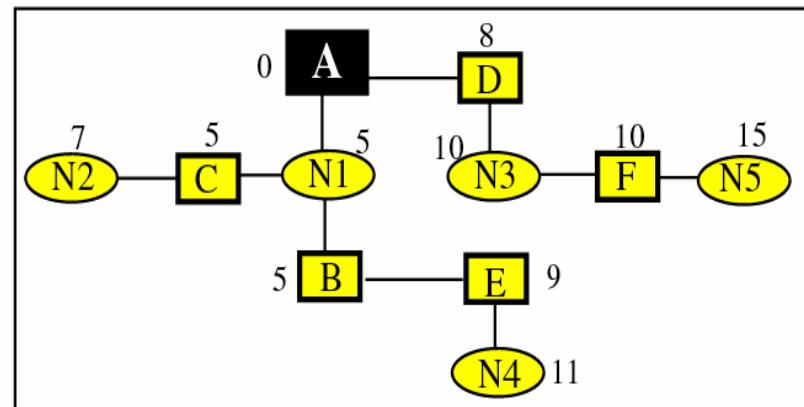
i. Make N3 permanent, add its neighbors



j. Make F permanent, add its neighbors



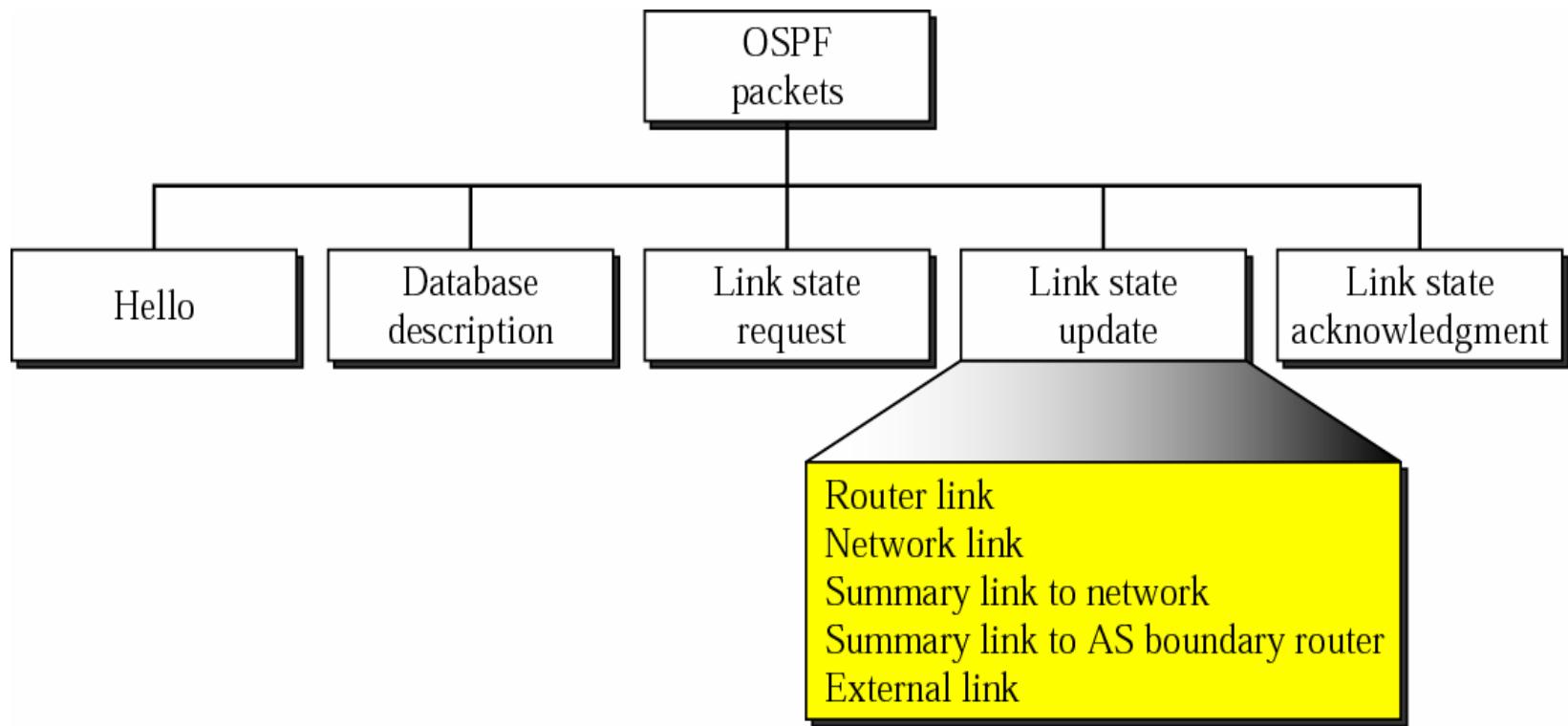
k. Make N4 permanent



l. Make N5 permanent



Type of OSPF packet





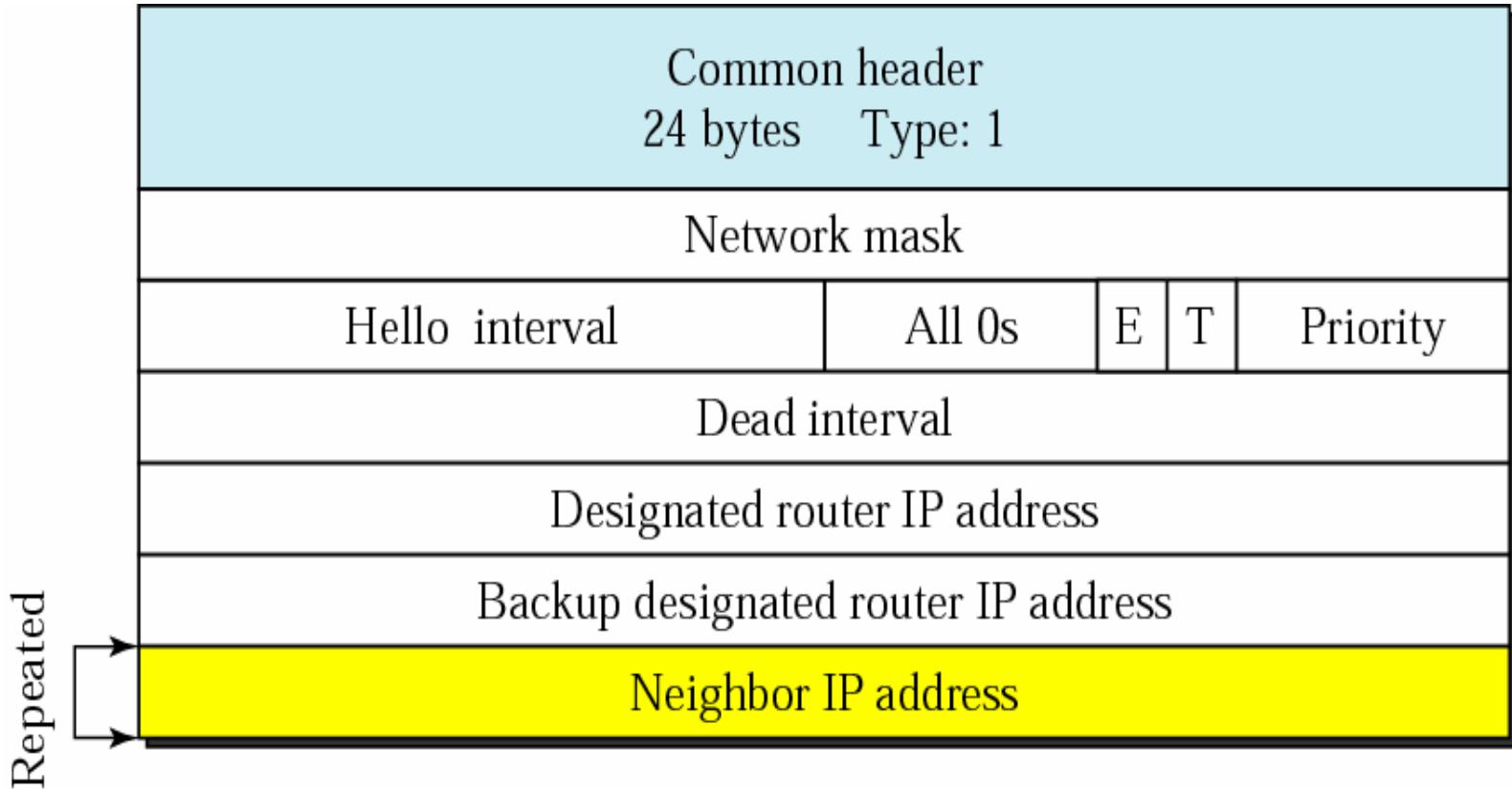
OSPF Packet header

Version	Type	Message length
Source router IP address		
Checksum	Authentication type	
Authentication		



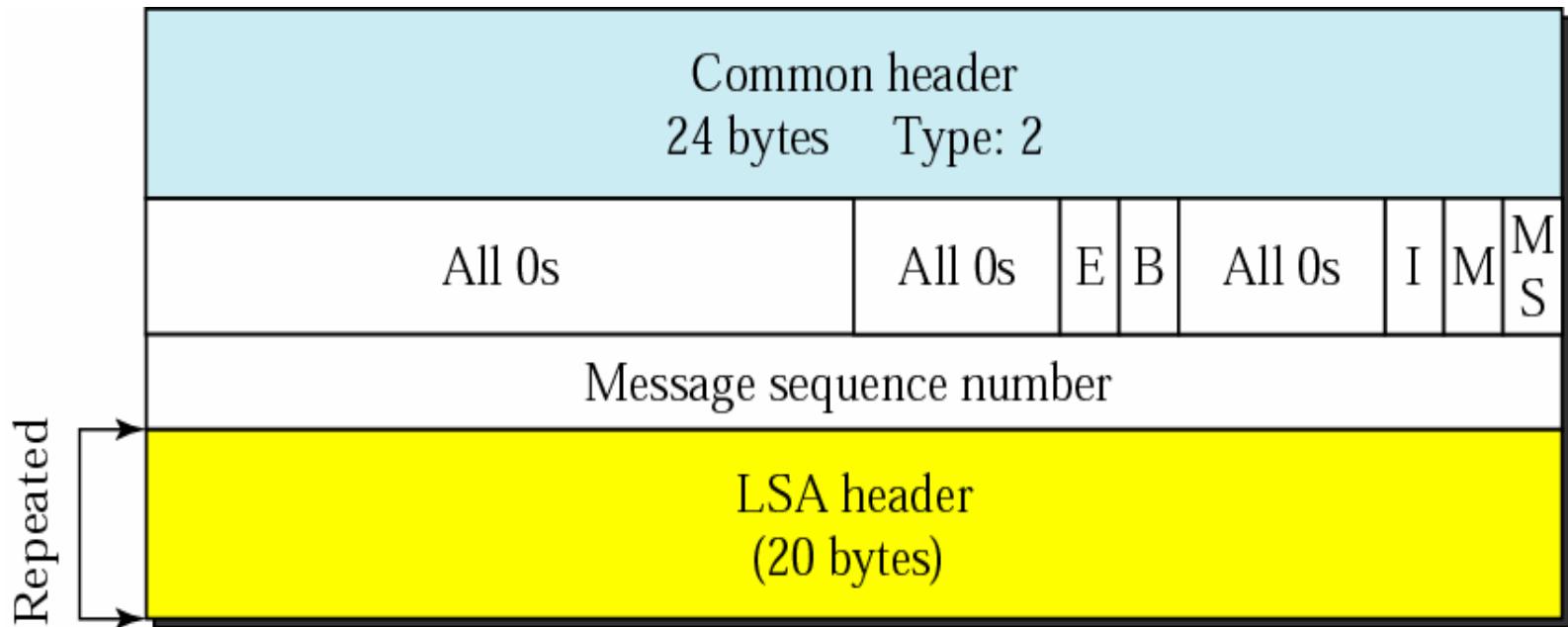
Hello Packet

Global CyberSoft



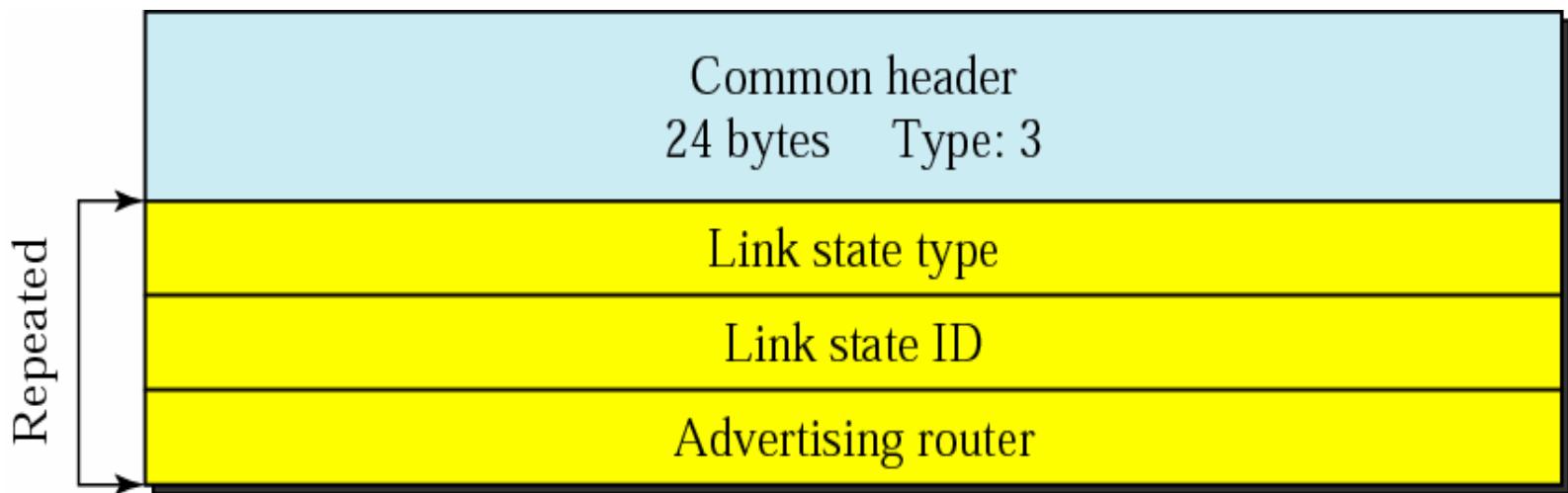


Database description packet



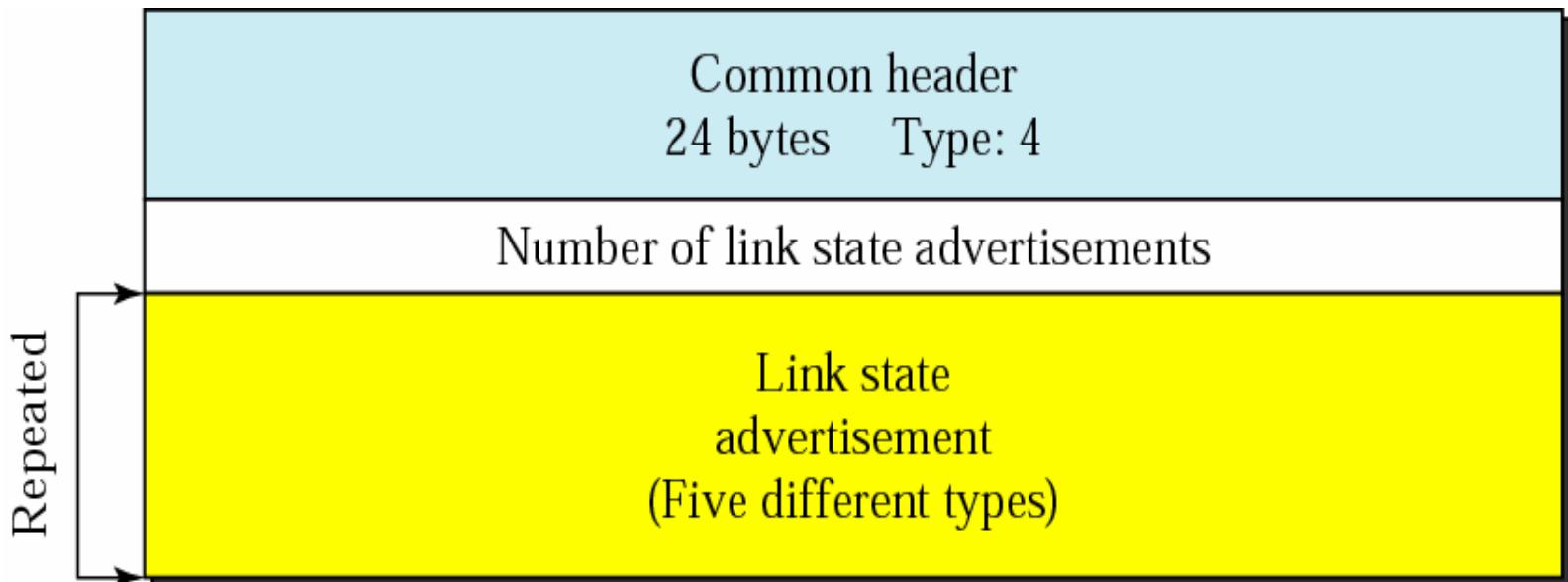


Link state request packet





Link state update packet



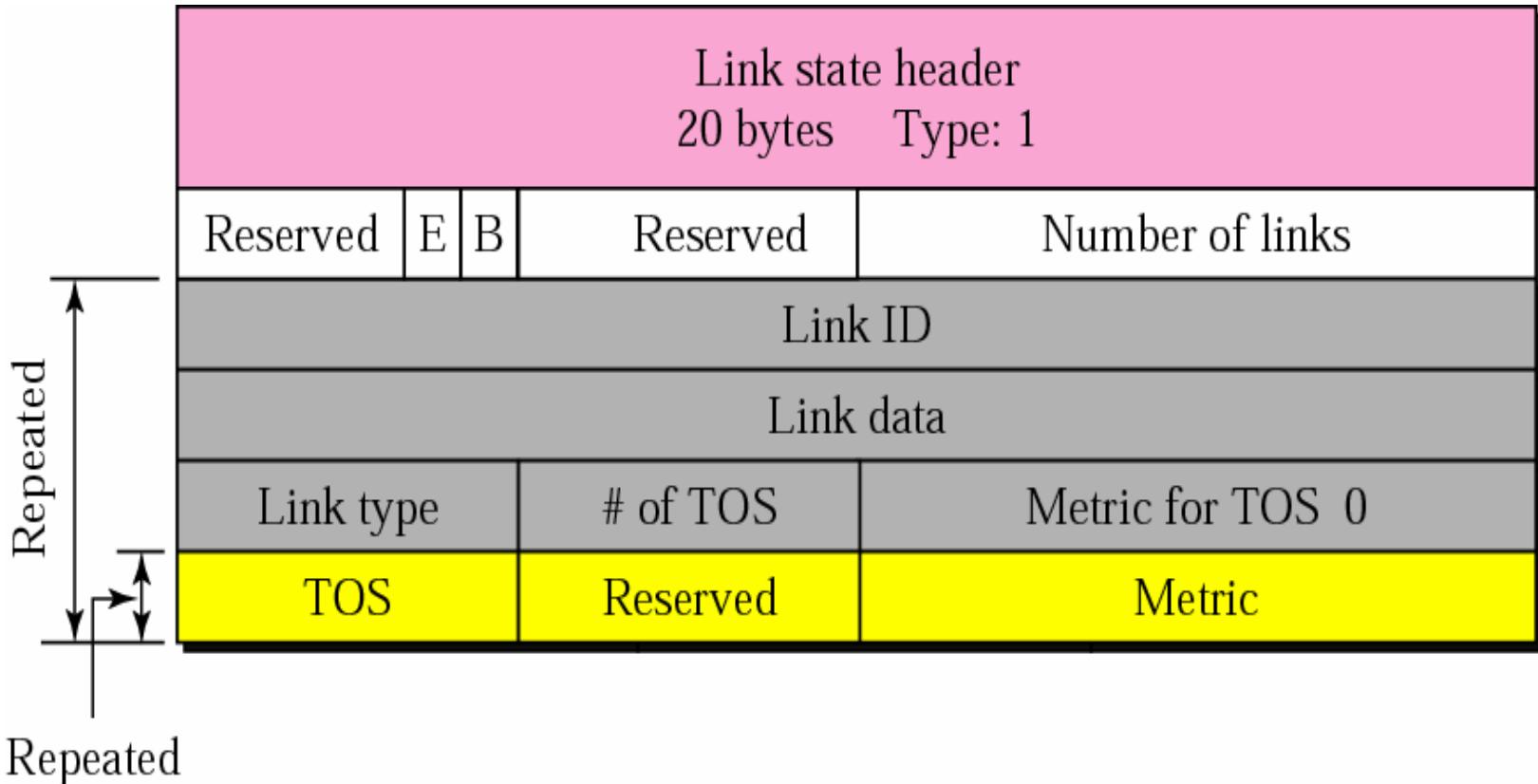


LSA Header

Link state age	Reserved	E	T	Link state type
Link state ID				
Advertising router				
Link state sequence number				
Link state checksum	Length			

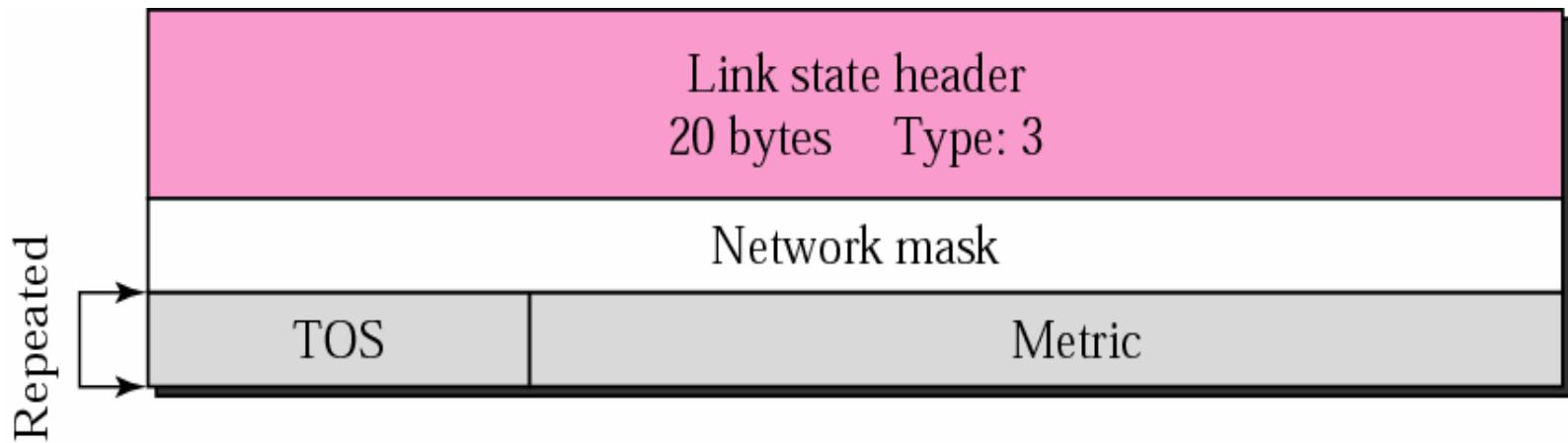


Router Link LSA



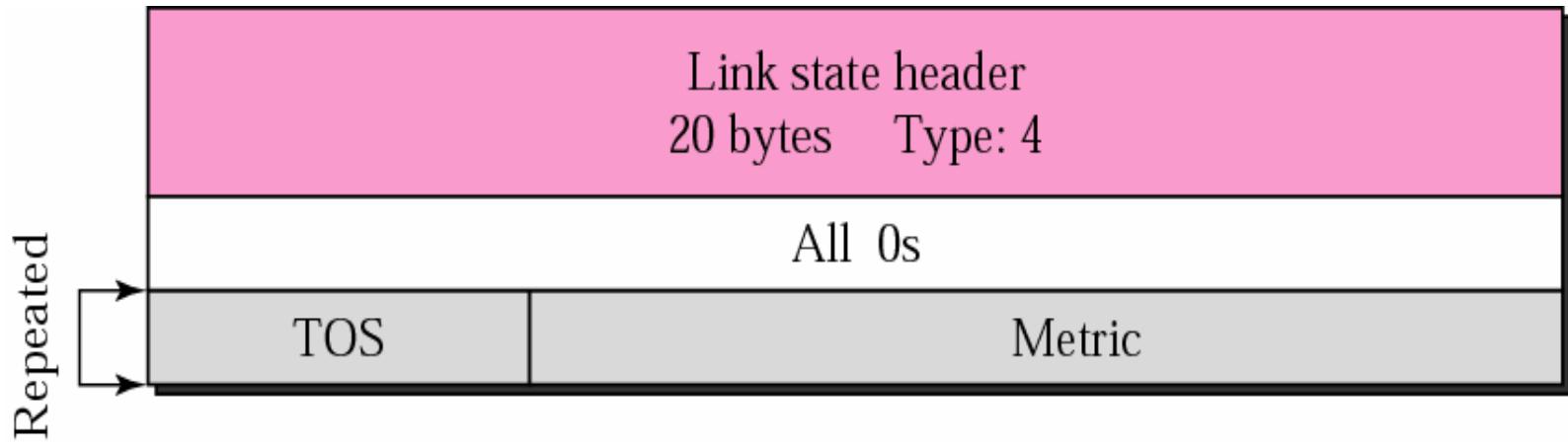


Summary link to network LSA

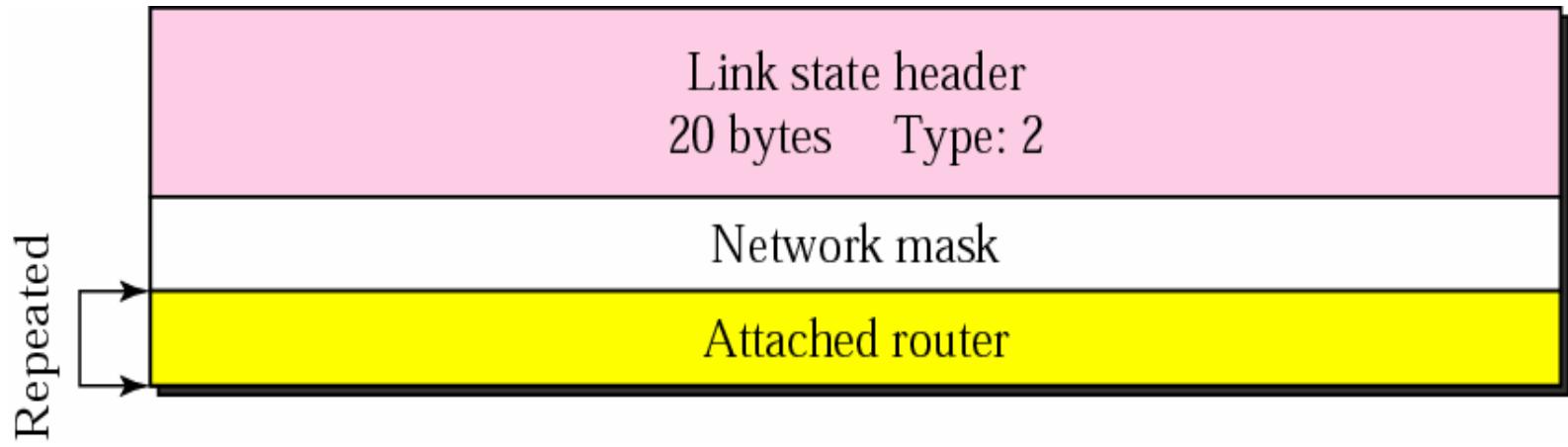




Summary link to AS boundary LSA

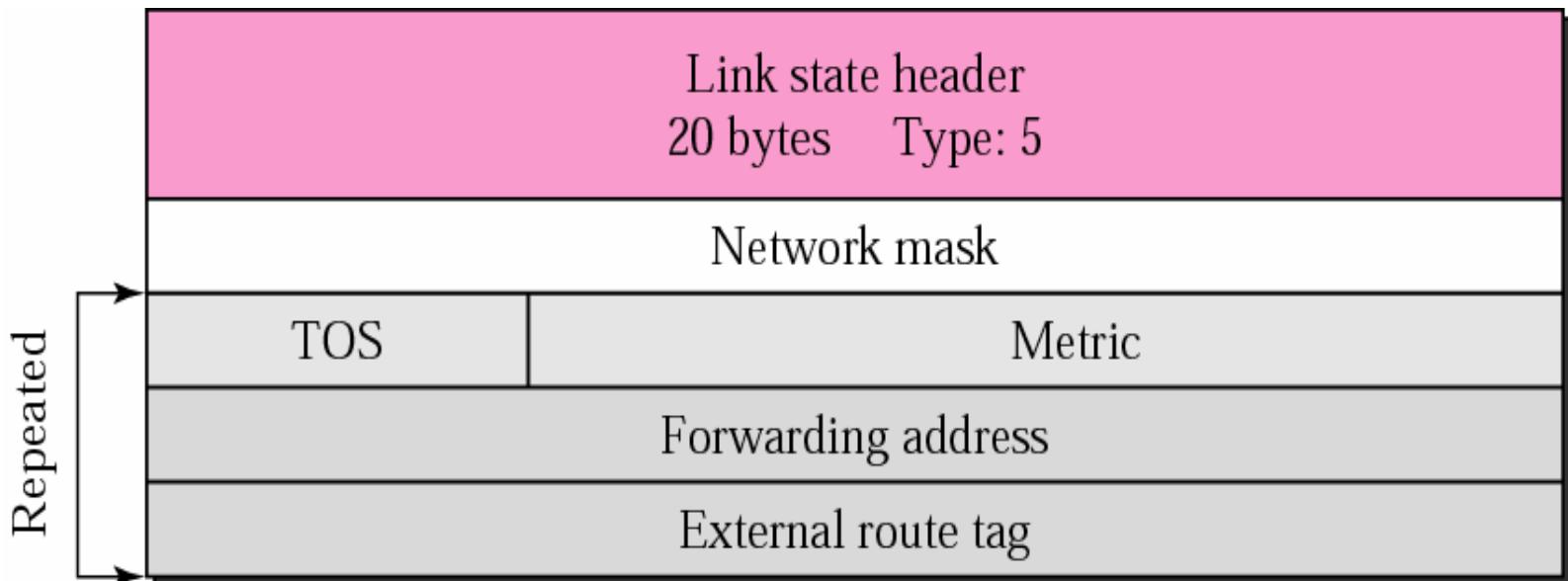


Network link advertisement format



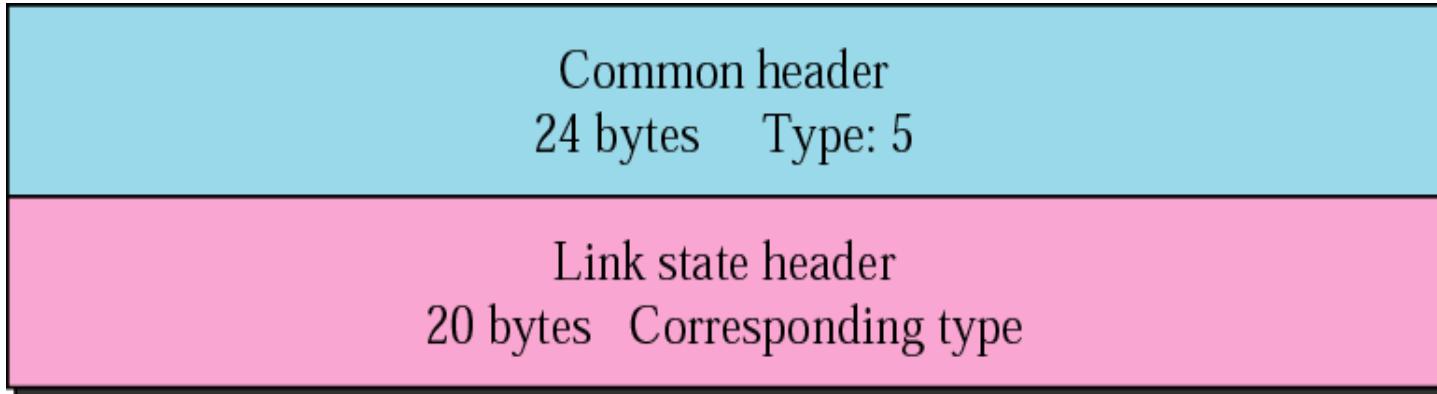


External link LSA



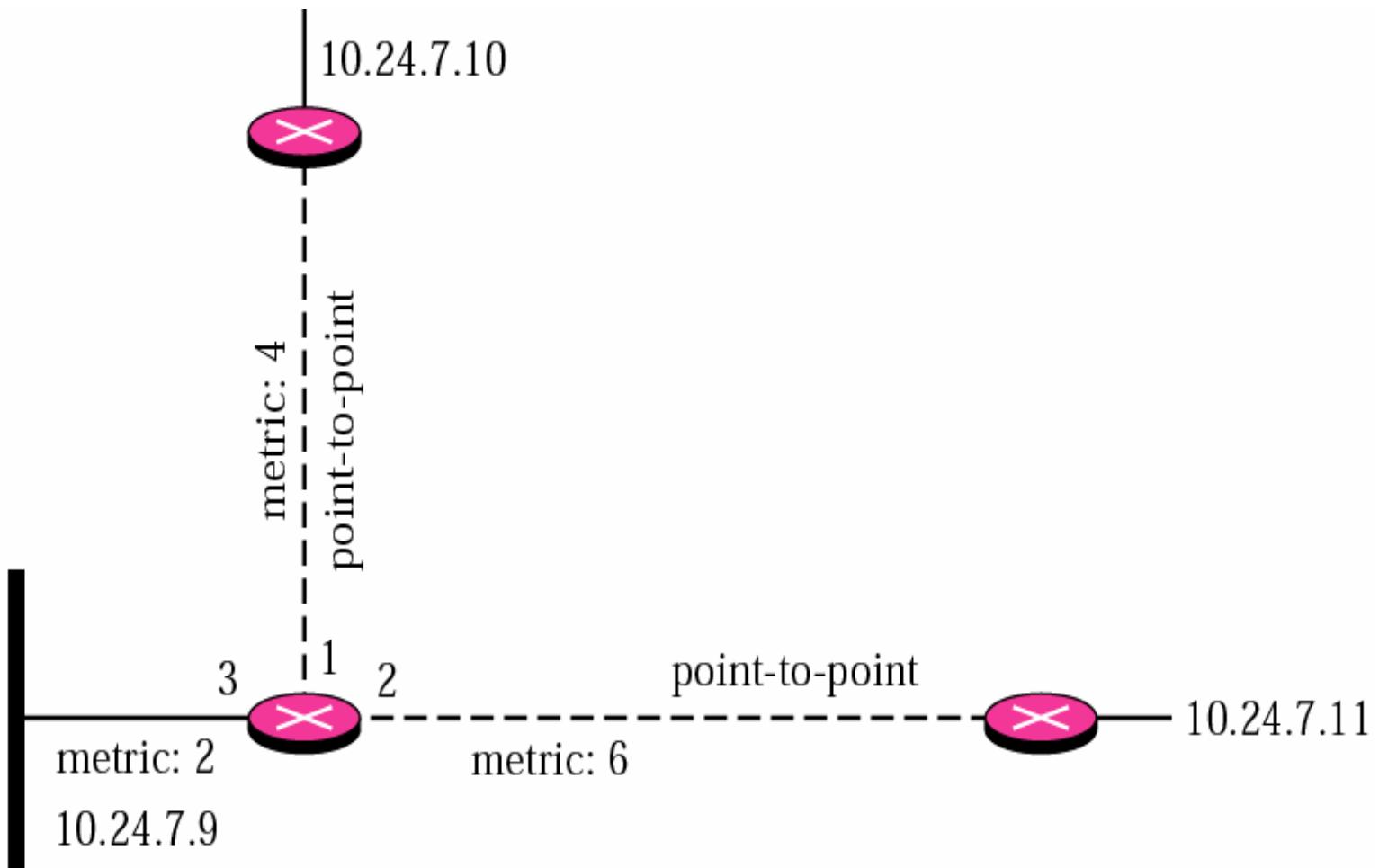


Link state acknowledgment packet





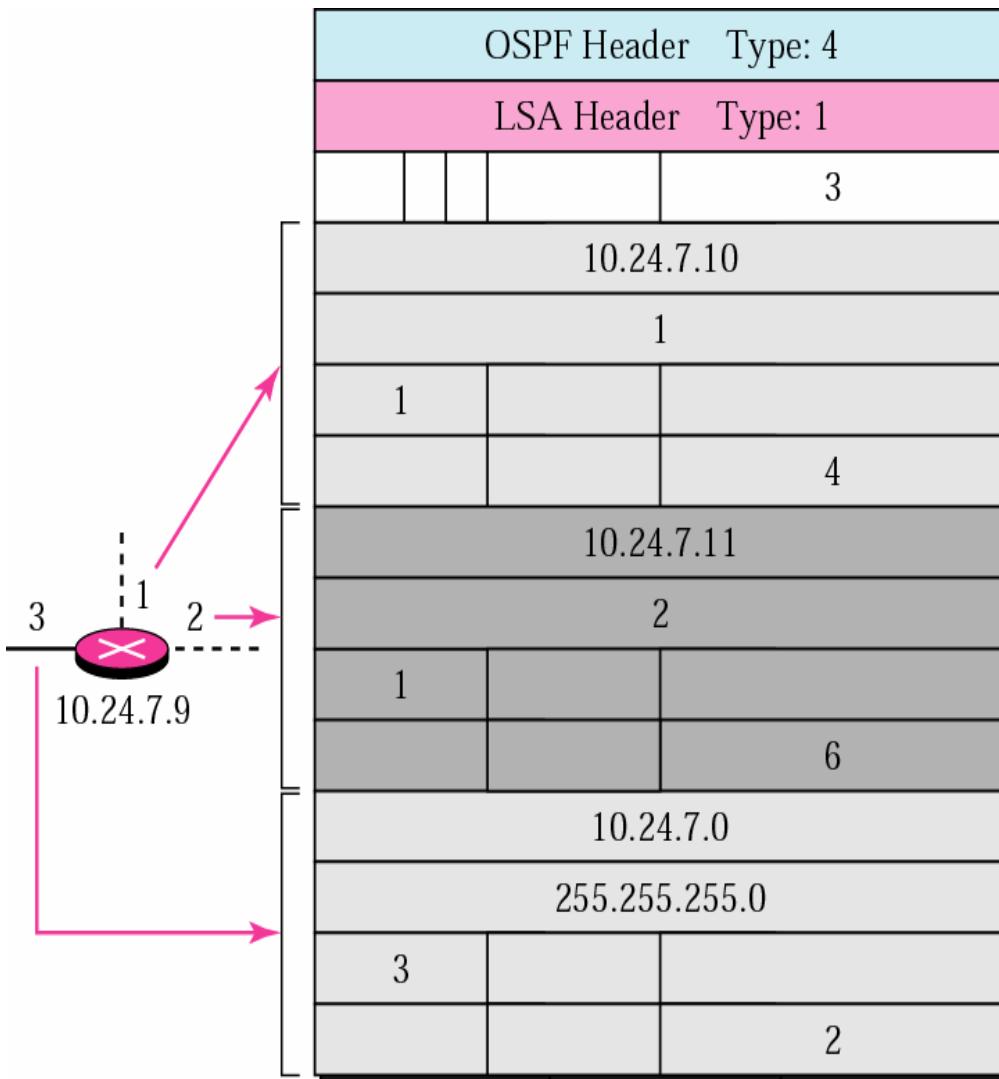
Example



10.24.7.0/24

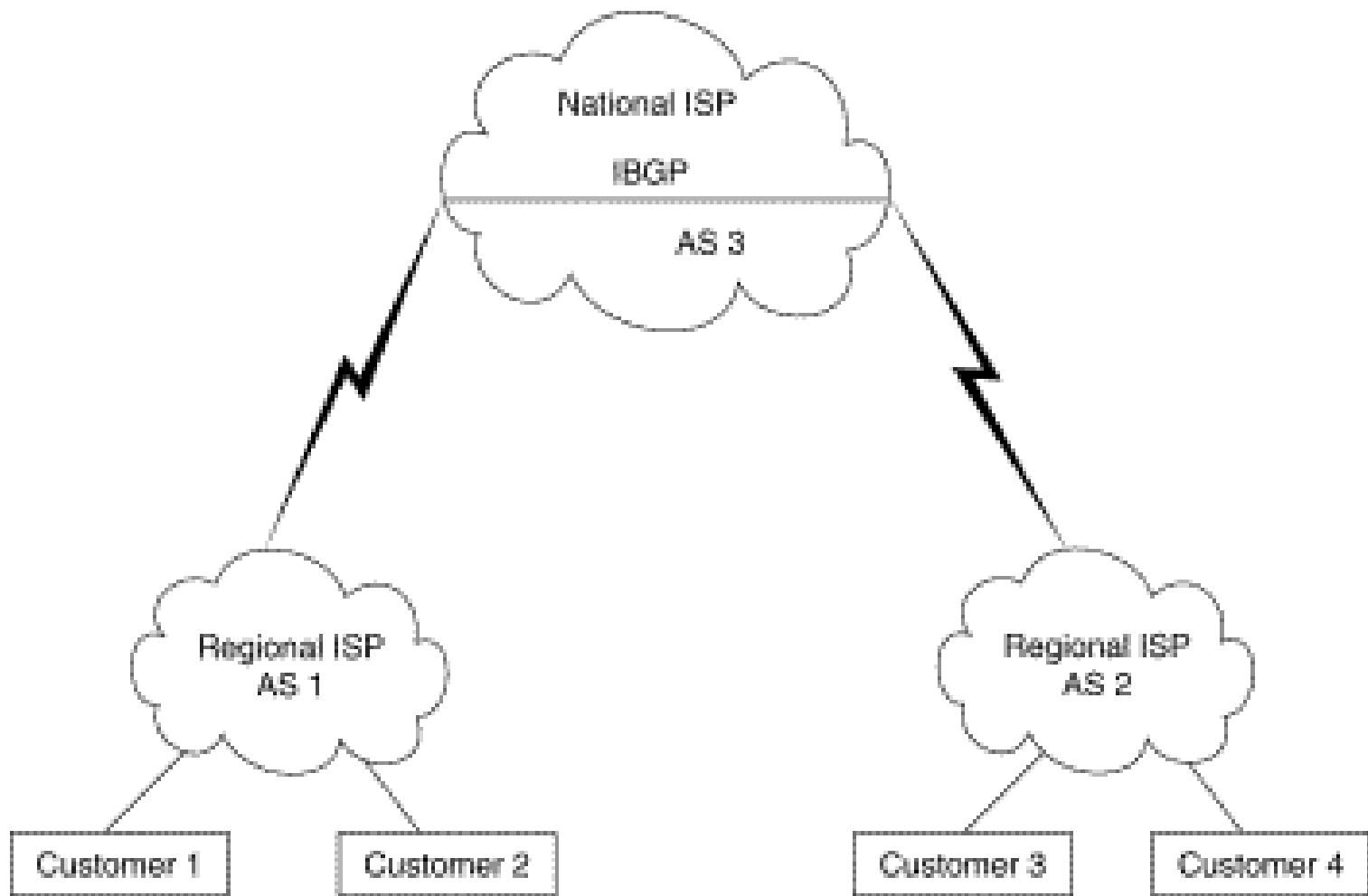


Solution



Border Gateway Protocol

- is an interautonomous system routing protocol.
- is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).
- Customer networks, such as universities and corporations, usually employ an Interior Gateway Protocol (IGP) such as RIP or OSPF for the exchange of routing information within their networks.
- Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Interior BGP (IBGP).

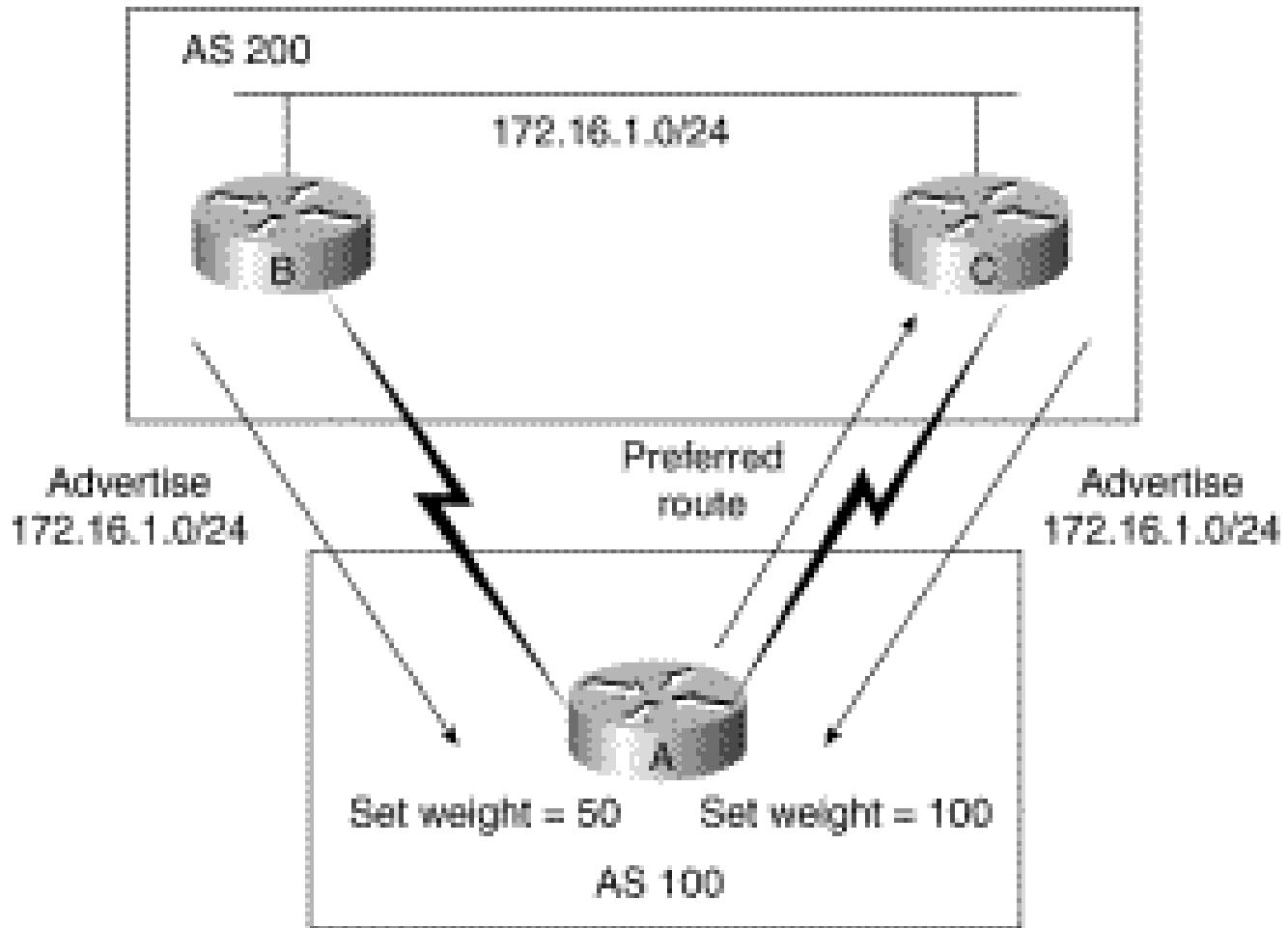


BGP Attributes

- Routes learned via BGP have associated properties that are used to determine the best route to a destination when multiple paths exist to a particular destination. These properties are referred to as BGP attributes, and an understanding of how BGP attributes influence route selection is required for the design of robust networks. This section describes the attributes that BGP uses in the route selection process:
 - Weight
 - Local preference
 - Multi-exit discriminator
 - Origin
 - AS_path
 - Next hop
 - Community

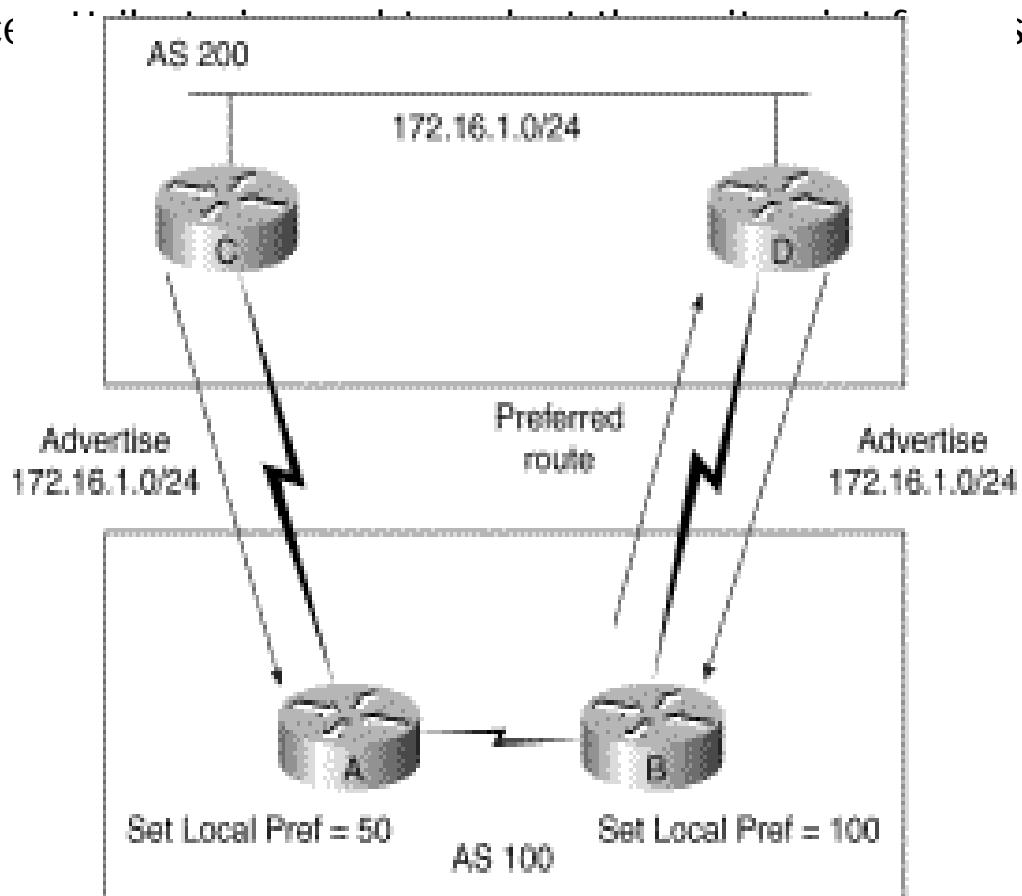


Weight Attribute



Local Preference Attribute

- used to prefer an exit point from the local autonomous system (AS). Unlike the weight attribute, the local preference attribute is propagated throughout the local AS. If there are multiple exit points from the AS, the local preference value is compared at the border routers to determine the preferred route.



Multi-Exit Discriminator Attribute

- The *multi-exit discriminator (MED)* or *metric attribute* is used as a suggestion to an external AS regarding the preferred route into the AS that is advertising the metric.
- The term *suggestion* is used because the external AS that is receiving the MEDs may be using other BGP attributes for route selection

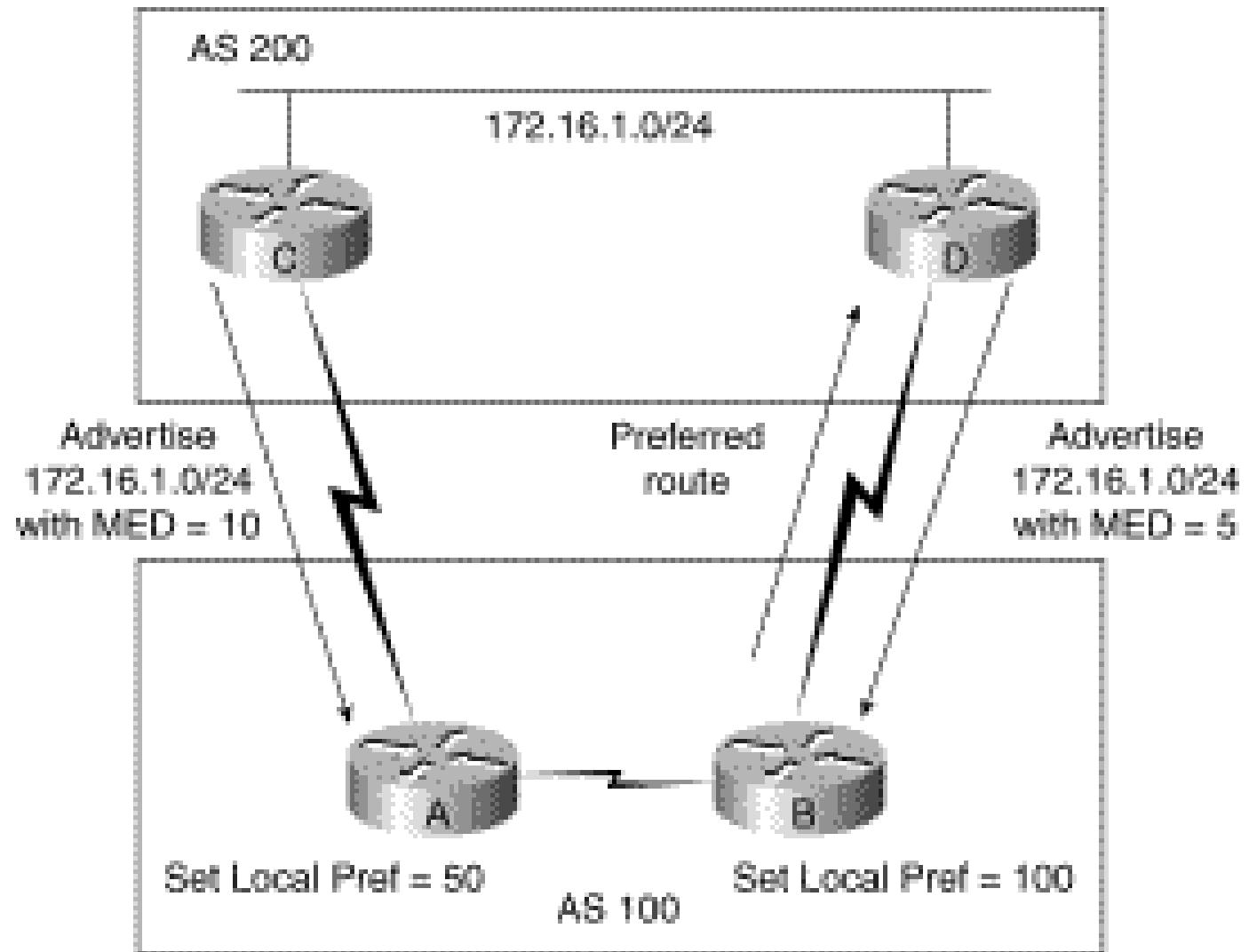
Origin Attribute

The *origin attribute* indicates how BGP learned about a particular route. The origin attribute can have one of three possible values:

- **IGP**—The route is interior to the originating AS. This value is set when the network router configuration command is used to inject the route into BGP.
- **EGP**—The route is learned via the Exterior Border Gateway Protocol (EBGP).
- **Incomplete**—The origin of the route is unknown or learned in some other way. An origin of incomplete occurs when a route is redistributed into BGP



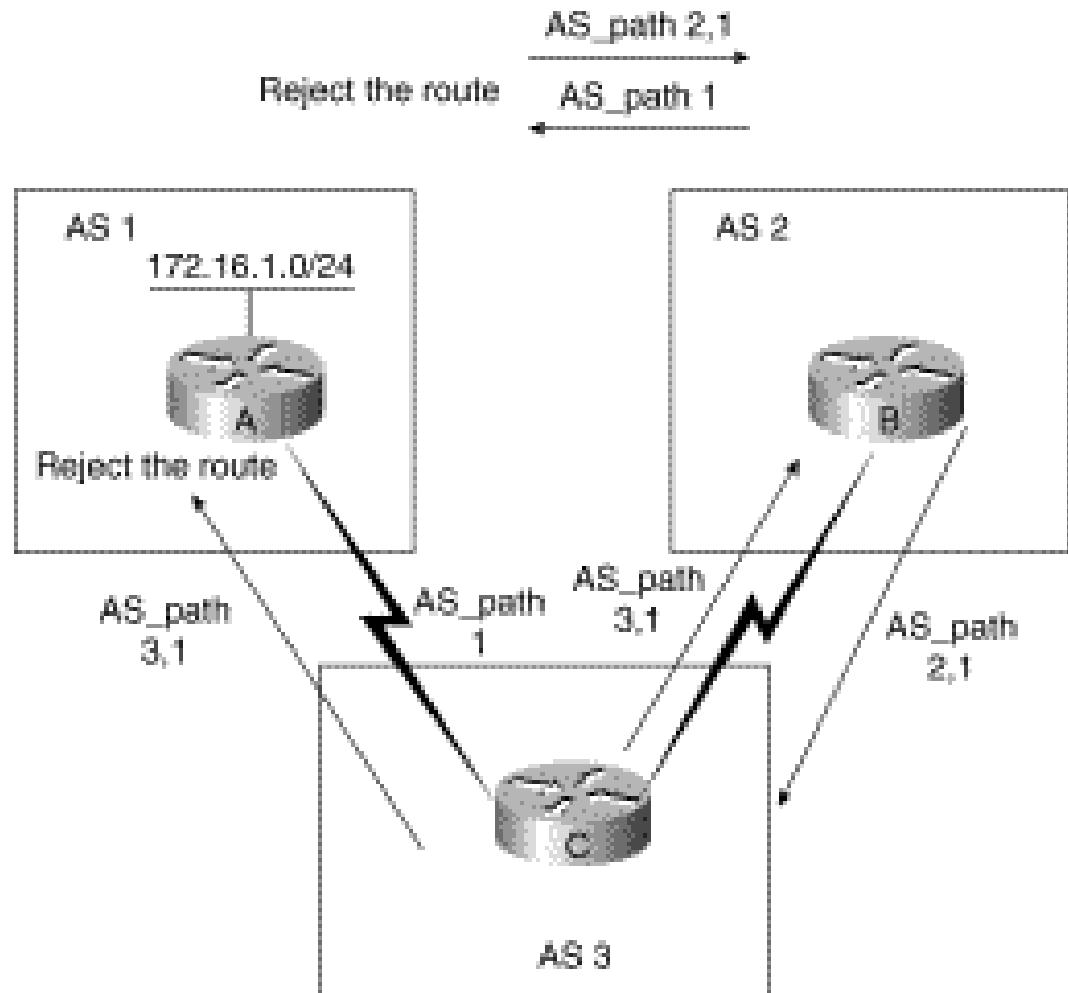
Origin Attribute





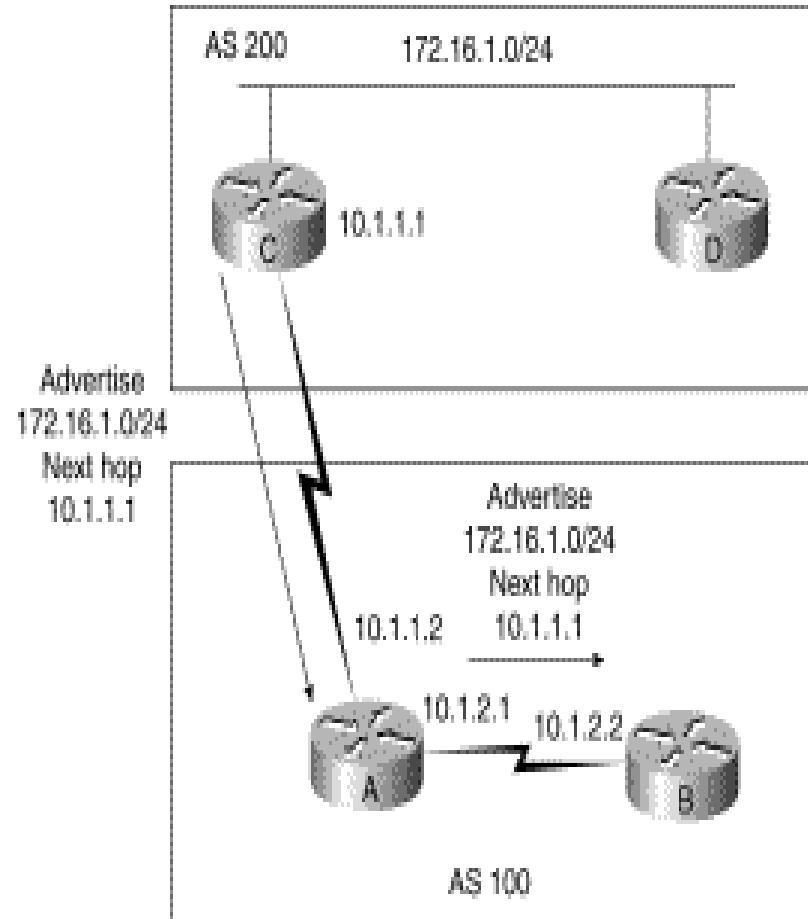
AS_path Attribute

- When a route advertisement passes through an autonomous system, the AS number is added to an ordered list of AS numbers that the route advertisement has traversed



Next-Hop Attribute

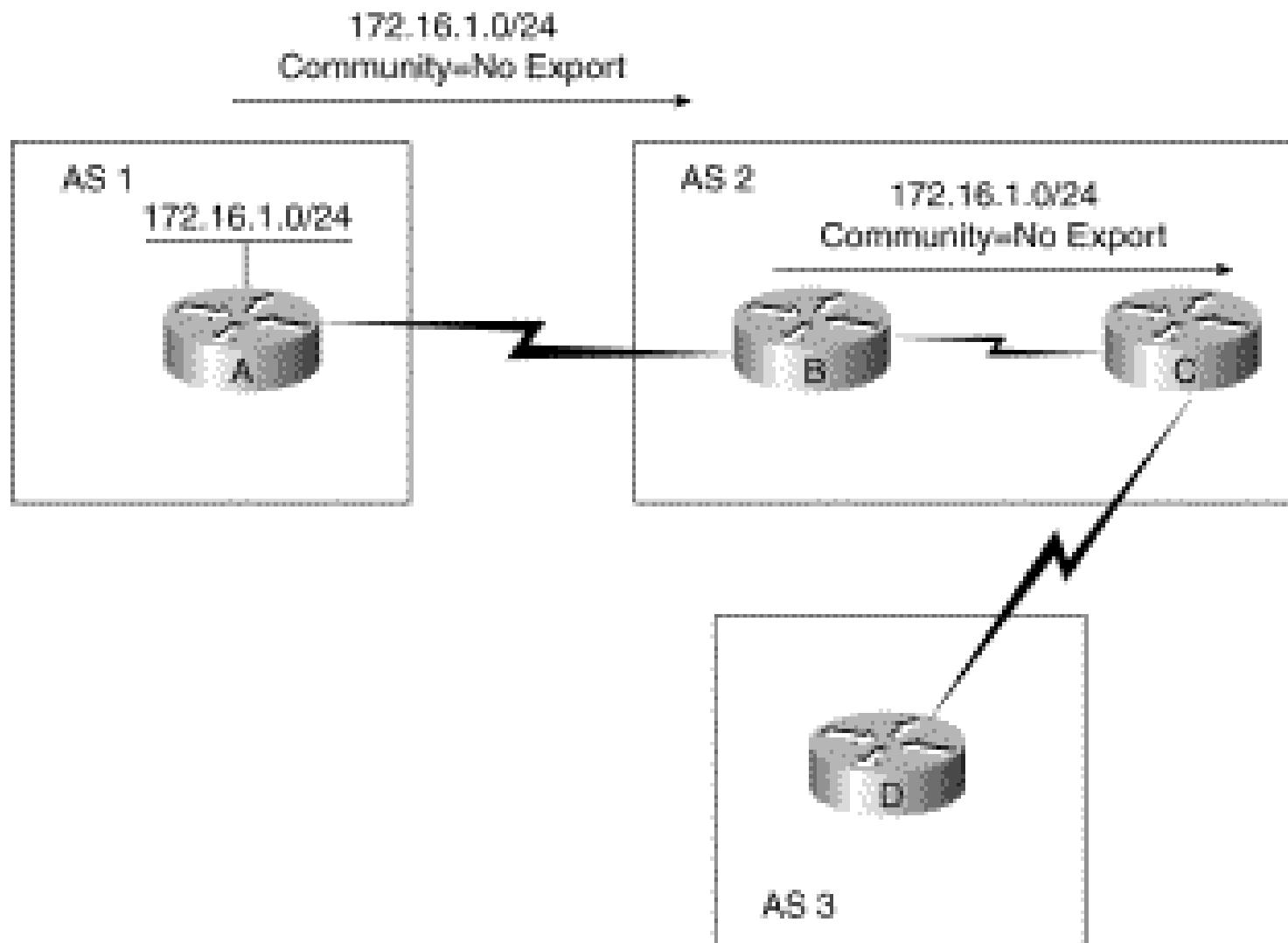
- The EBGP *next-hop* attribute is the IP address that is used to reach the advertising router. For EBGP peers, the next-hop address is the IP address of the connection between the peers. For IBGP, the EBGP next-hop address is carried into the local AS



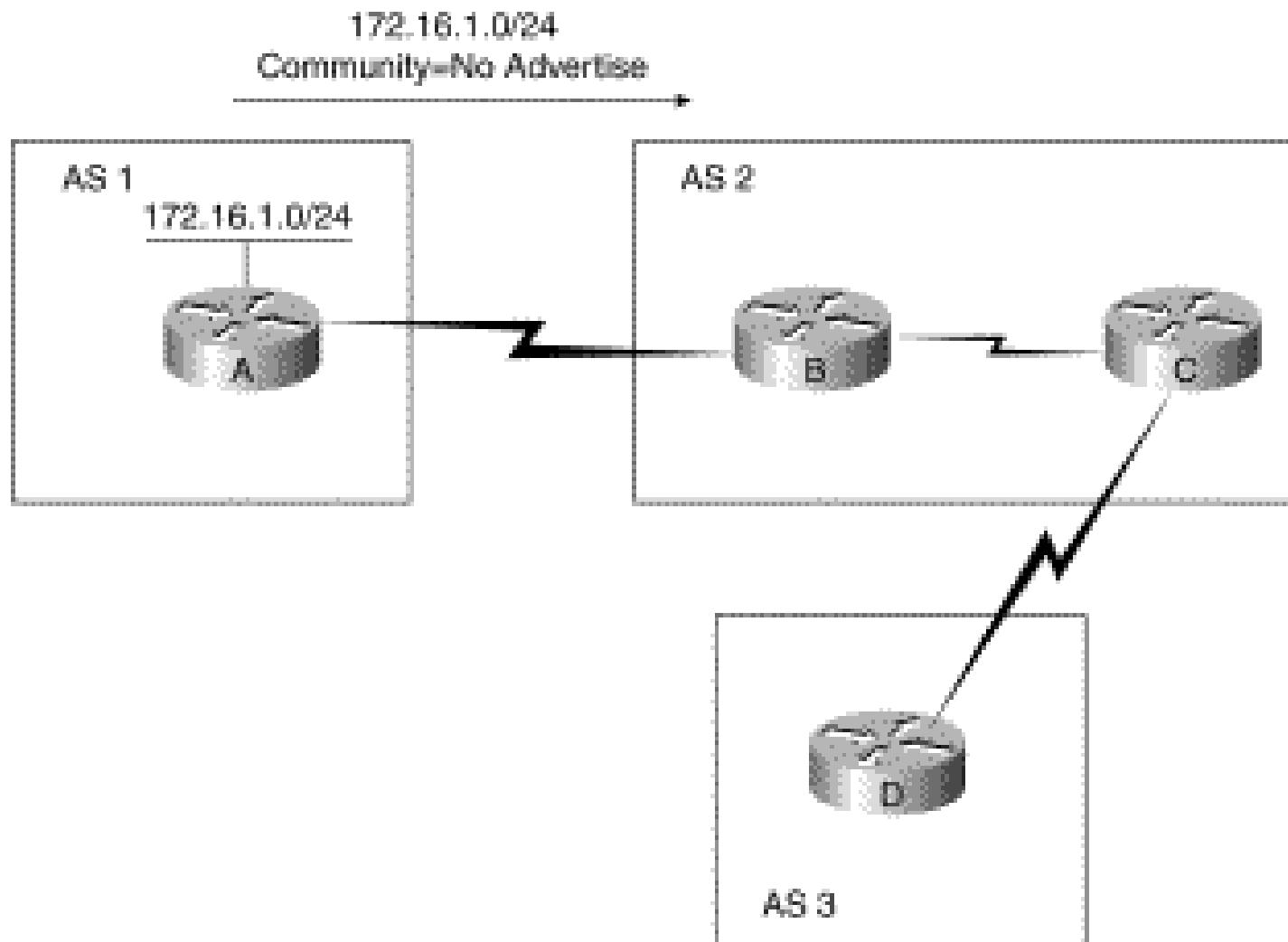
Community Attribute

- The community attribute provides a way of grouping destinations, called communities, to which routing decisions (such as acceptance, preference, and redistribution) can be applied. Route maps are used to set the community attribute. Predefined community attributes are listed here:
 - **no-export**—Do not advertise this route to EBGP peers.
 - **no-advertise**—Do not advertise this route to any peer.
 - **internet**—Advertise this route to the Internet community; all routers in the network belong to it

Community-No export

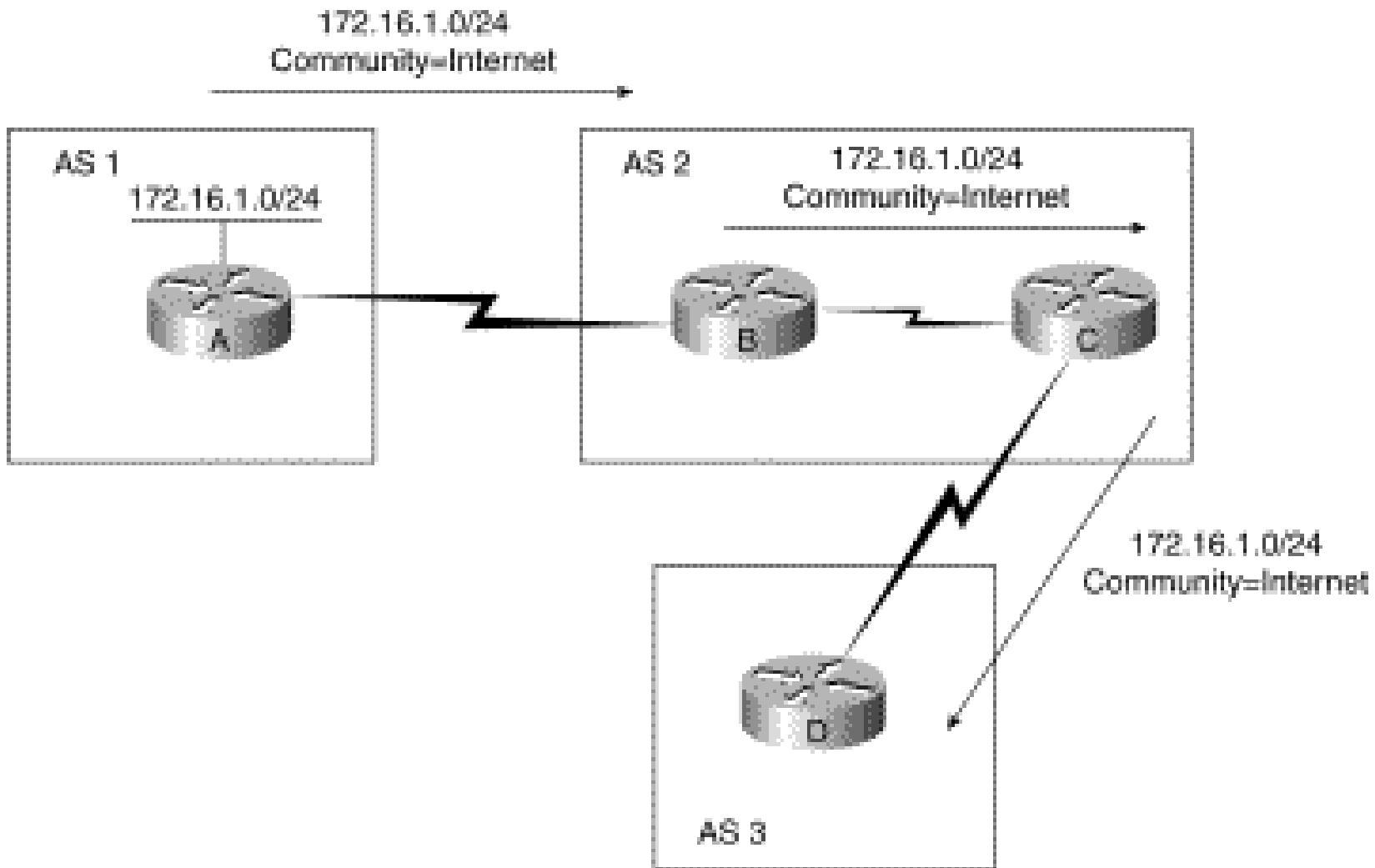


Community-No Advertise





Community-Internet



BGP Path Selection

- If the path specifies a next hop that is inaccessible, drop the update.
- Prefer the path with the largest weight.
- If the weights are the same, prefer the path with the largest local preference.
- If the local preferences are the same, prefer the path that was originated by BGP running on this router.
- If no route was originated, prefer the route that has the shortest AS_path
- If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP, and EGP is lower than incomplete).

BGP Path Selection

- If the origin codes are the same, prefer the path with the lowest MED attribute.
- If the paths have the same MED, prefer the external path over the internal path.
- If the paths are still the same, prefer the path through the closest IGP neighbor.
- Prefer the path with the lowest IP address, as specified by the BGP router ID.

Broadcast and Multicast

- Broadcasting and multicasting only apply to UDP, where it makes sense for an application to send a single message to multiple recipients
- when a host wants to send a frame to every other host on the cable-called a *broadcast*. We saw this with ARP and RARP. Multicasting fits between unicasting and broadcasting: the frame should be delivered to a set of hosts that belong to a multicast group.

Broadcast and Multicast

- The problem with broadcasting is the processing load that it places on hosts that aren't interested in the broadcasts
- The intent of multicasting is to reduce this load on hosts with no interest in the application. With multicasting a host specifically joins one or more multicast groups. If possible, the interface card is told which multicast groups the host belongs to, and only those multicast frames are received

- Limited Broadcast:
 - The *limited broadcast address* is 255.255.255.255
 - A datagram destined for the limited broadcast address is *never* forwarded by a router under any circumstance. It only appears on the local cable
- Net-directed Broadcast:
 - The *net-directed broadcast address* has a host ID of all one bits. A class A net-directed broadcast address is netid.255.255.255, where *netid* is the class A network ID.
 - A router must forward a net-directed broadcast, but it must also have an option to disable this forwarding
- Subnet-directed Broadcast:
 - The *subnet-directed broadcast address* has a host ID of all one bits but a specific subnet ID. Classification of an IP address as a subnet-directed broadcast address requires knowledge of the subnet mask

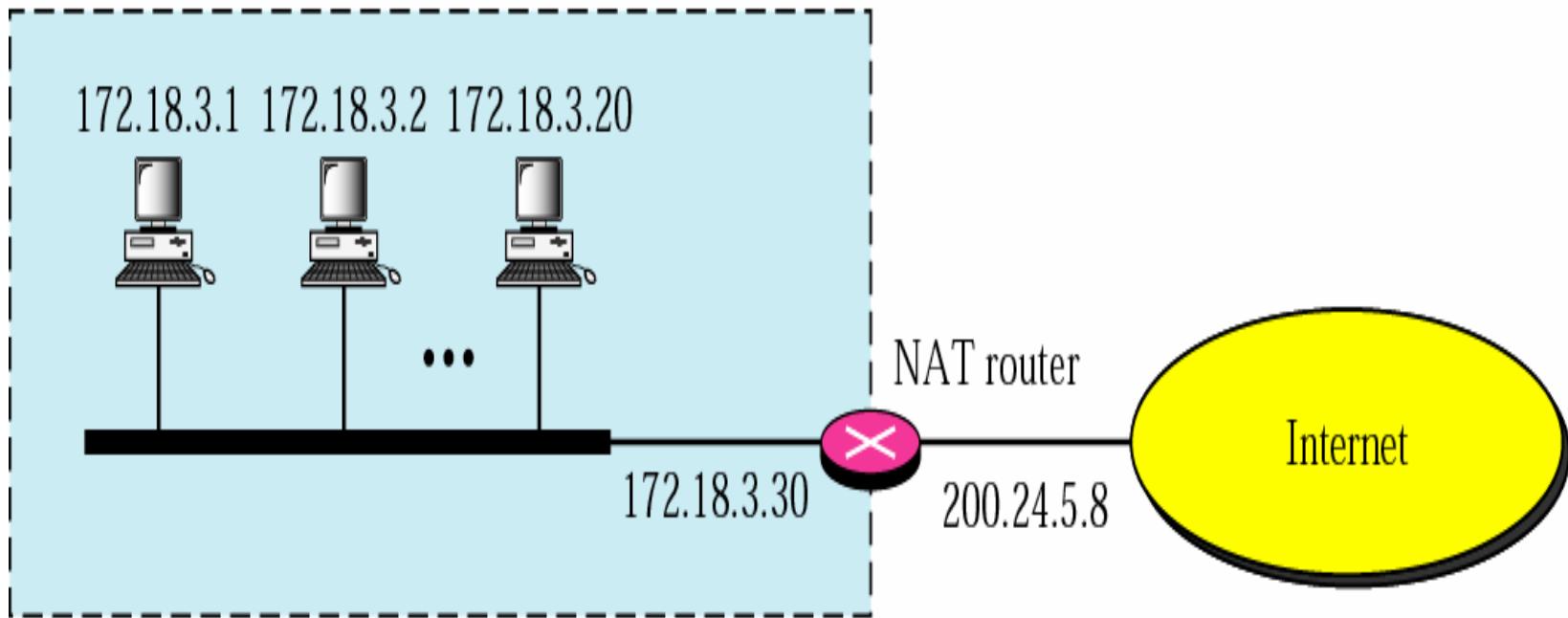
● All-subnets-directed Broadcast:

- An *all-subnets-directed broadcast address* also requires knowledge of the destination network's subnet mask, to differentiate this broadcast address from a net-directed broadcast address. Both the subnet ID and the host ID are all one bits.
- For example, if the destination's subnet mask is 255.255.255.0, then the IP address 128.1.255.255 is an all-subnets-directed broadcast. But if the network is not subnetted, then this is a net-directed broadcast

- IP multicasting provides service for an application:
 - Delivery to multiple destinations
- Multicast Group Addresses
 - A *multicast group address* is the combination of the high-order 4 bits of 1110 and the multicast group ID. These are normally written as dotted-decimal numbers and are in the range 224.0.0.0 through 239.255.255.255
 - The set of hosts listening to a particular IP multicast address is called a *host group*
- Converting Multicast Group Addresses to Ethernet Addresses
 - first byte of any Ethernet address must be 01 to specify a multicast address, this means the Ethernet addresses corresponding to IP multicasting are in the range 01:00:5e:00:00:00 through 01:00:5e:7f:ff:ff

Network Address Translation

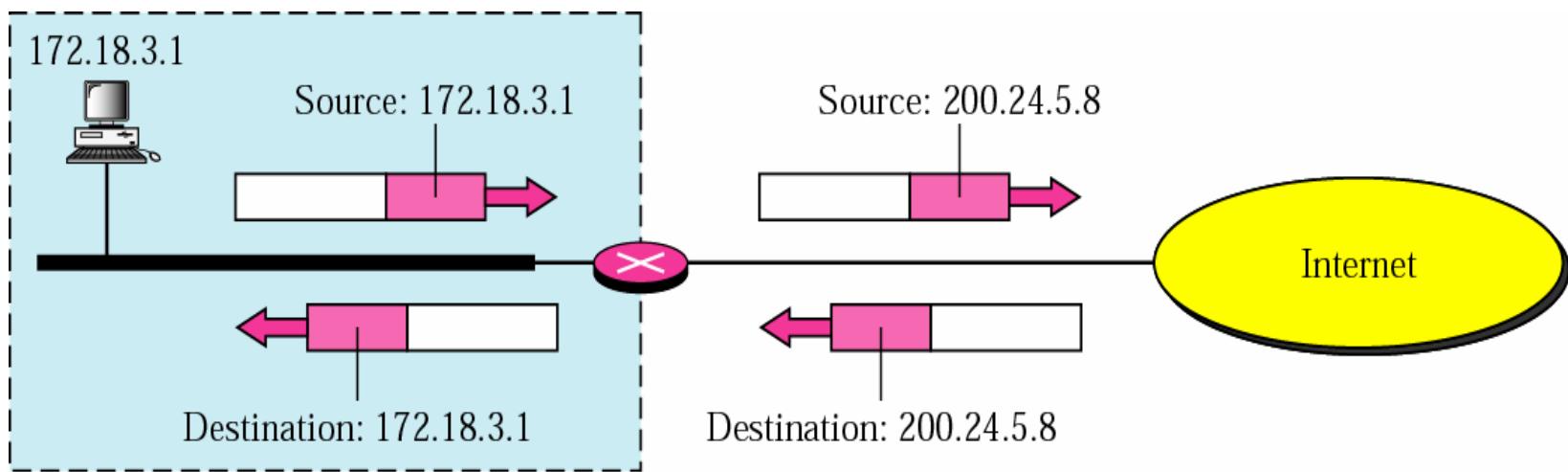
Site using private addresses





Address Translation

Global CyberSoft



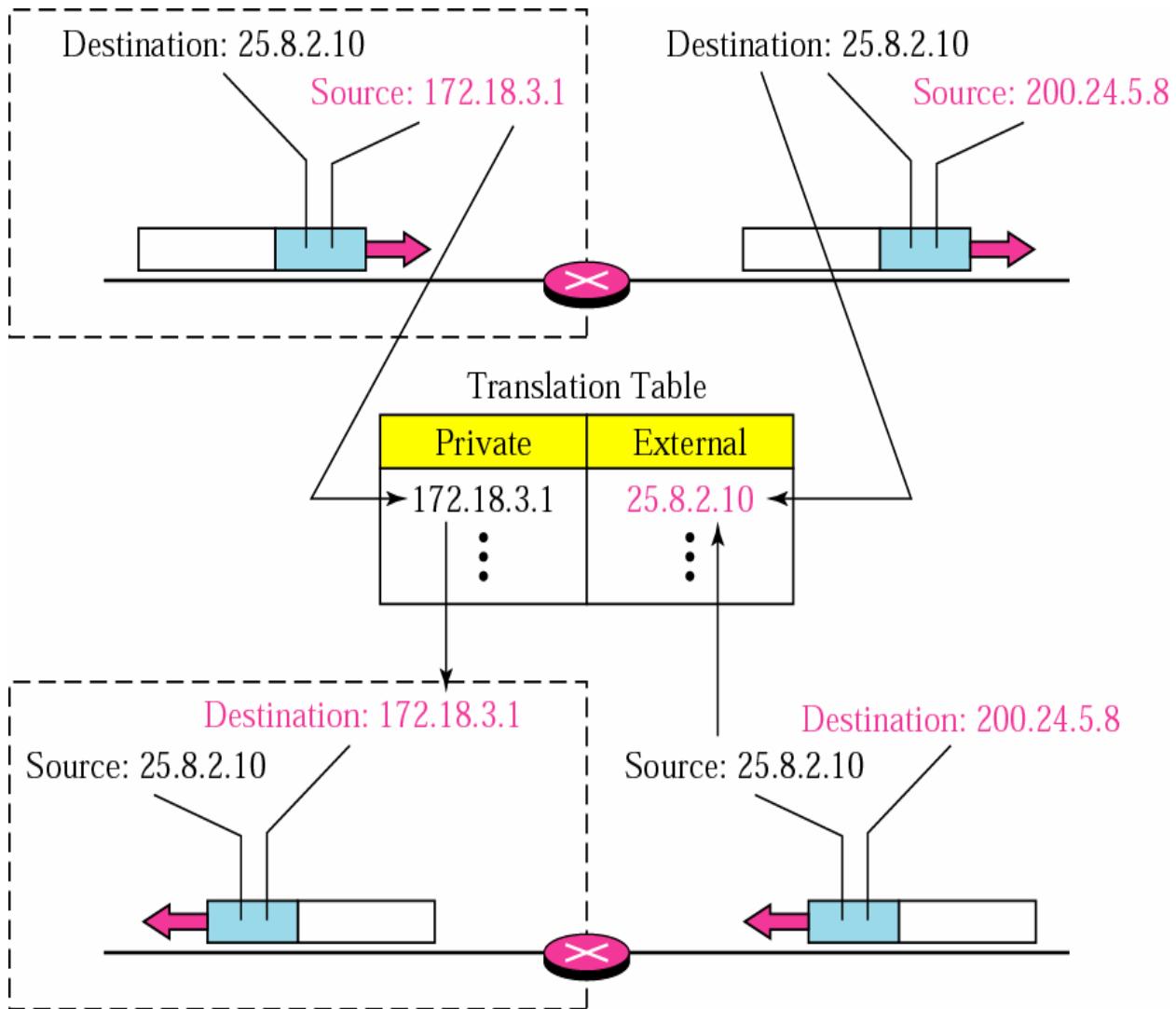


Global CyberSoft

Type of NAT

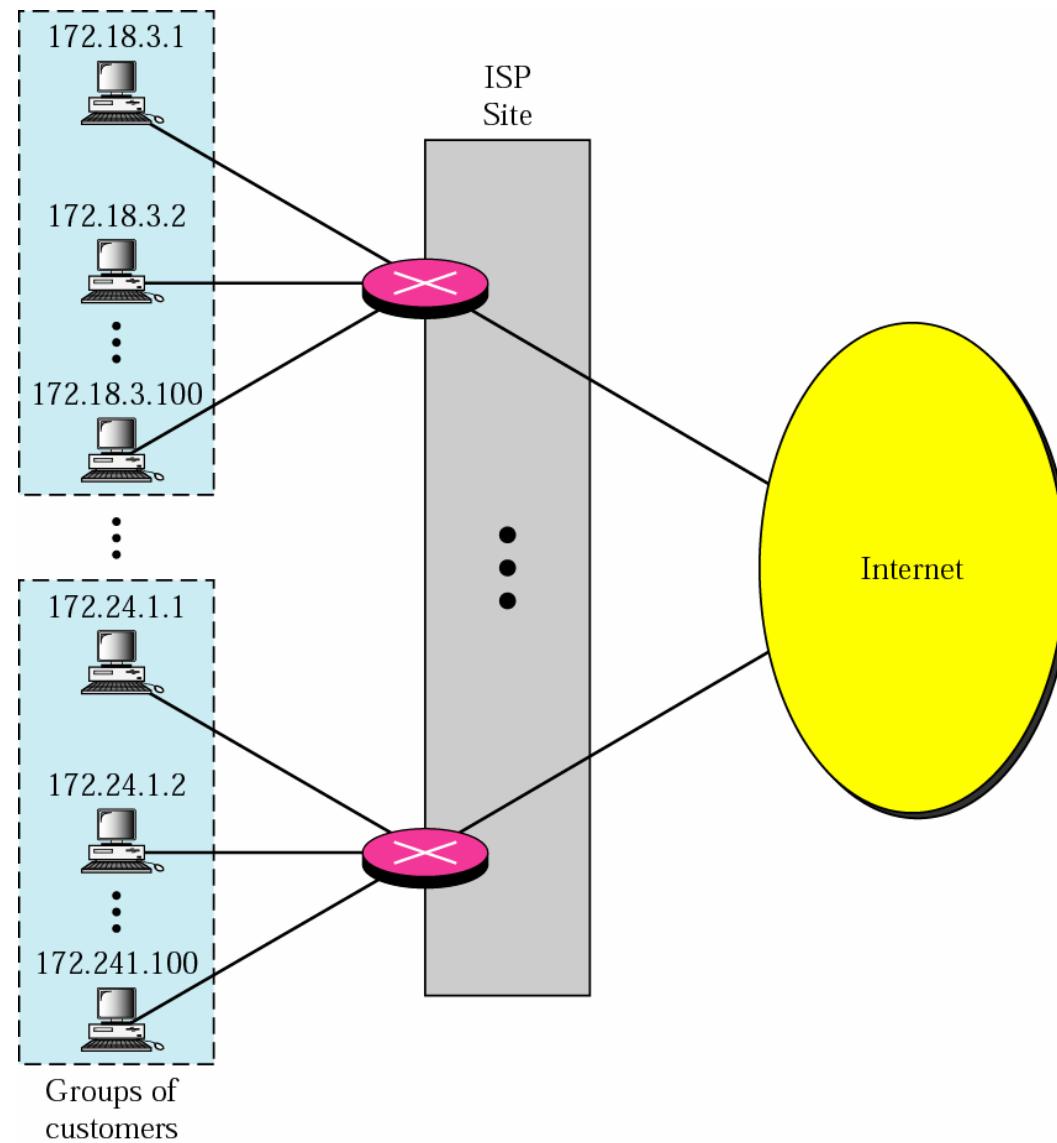
- SNAT: Static NAT
- DNAT: Dynamic NAT

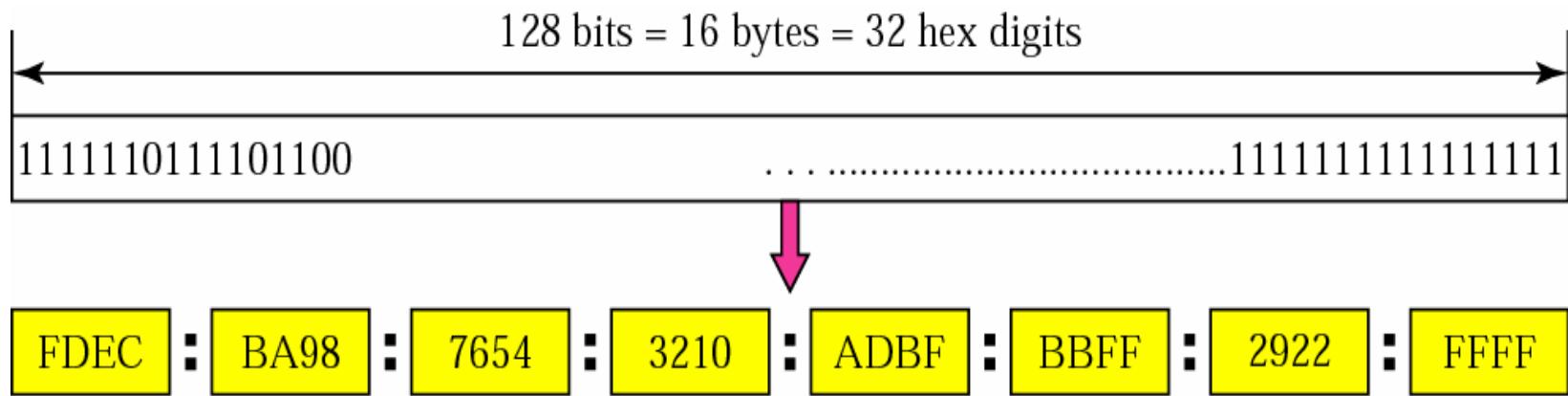
Translation





ISP and NAT







Abbreviated Address

Unabbreviated

```
FDEC : BA98 : 0074 : 3210 : 000F : BBFF : 0000 : FFFF
```



```
FDEC : BA98 : 74 : 3210 : F : BBFF : 0 : FFFF
```

Abbreviated



Abbreviated address with consecutive zero

Abbreviated

FDEC :: 0 :: 0 :: 0 :: 0 :: BBFF :: 0 :: FFFF



FDEC :: BBFF :: 0 :: FFFF

More Abbreviated

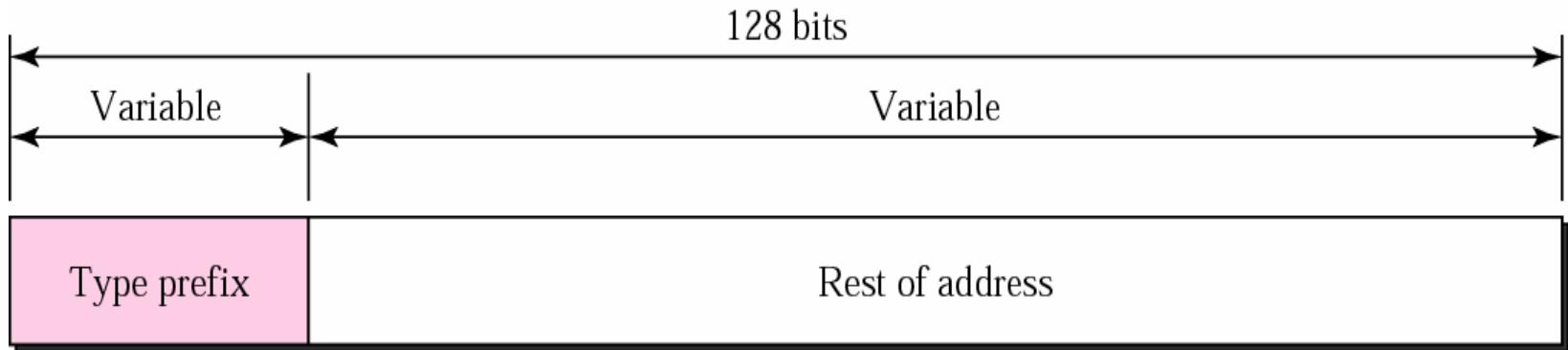


CIDR Address

FDEC : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF/60



Address Structure





8 bits

00000000

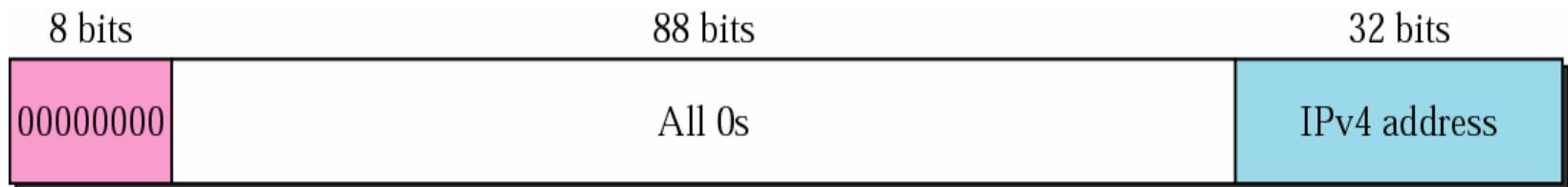
120 bits

0000000000000000.....0000000001



Compatible Address

Global CyberSoft



a. Compatible address

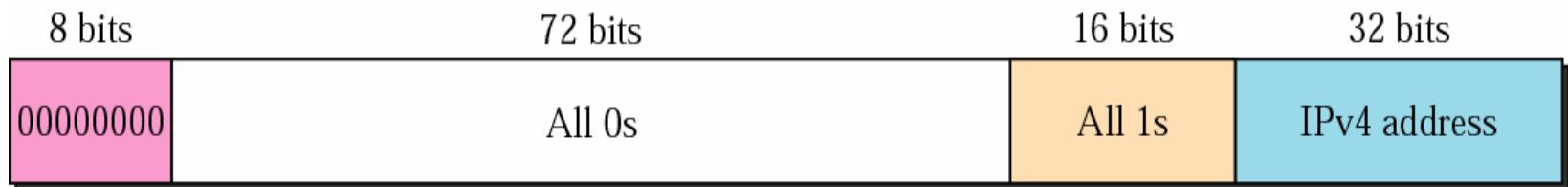


b. An example of address transformation



Mapped Address

Global CyberSoft



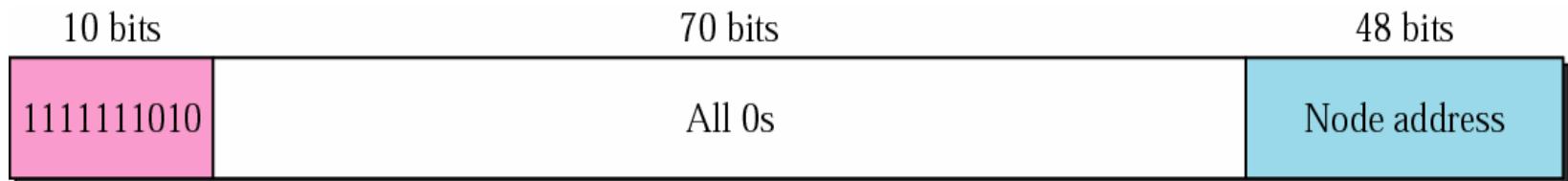
a. Mapped address



b. An example of address transformation

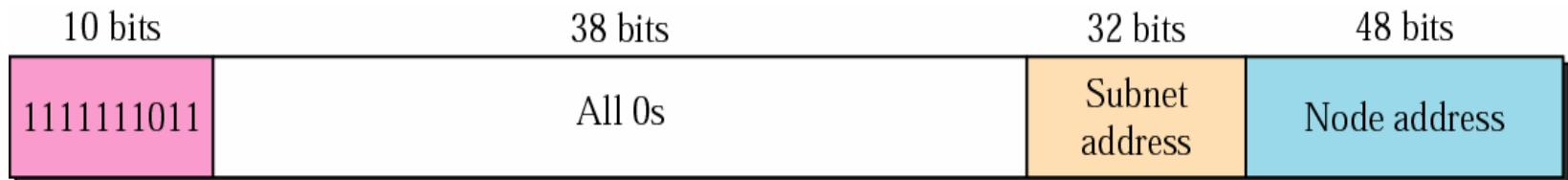


Link local Address





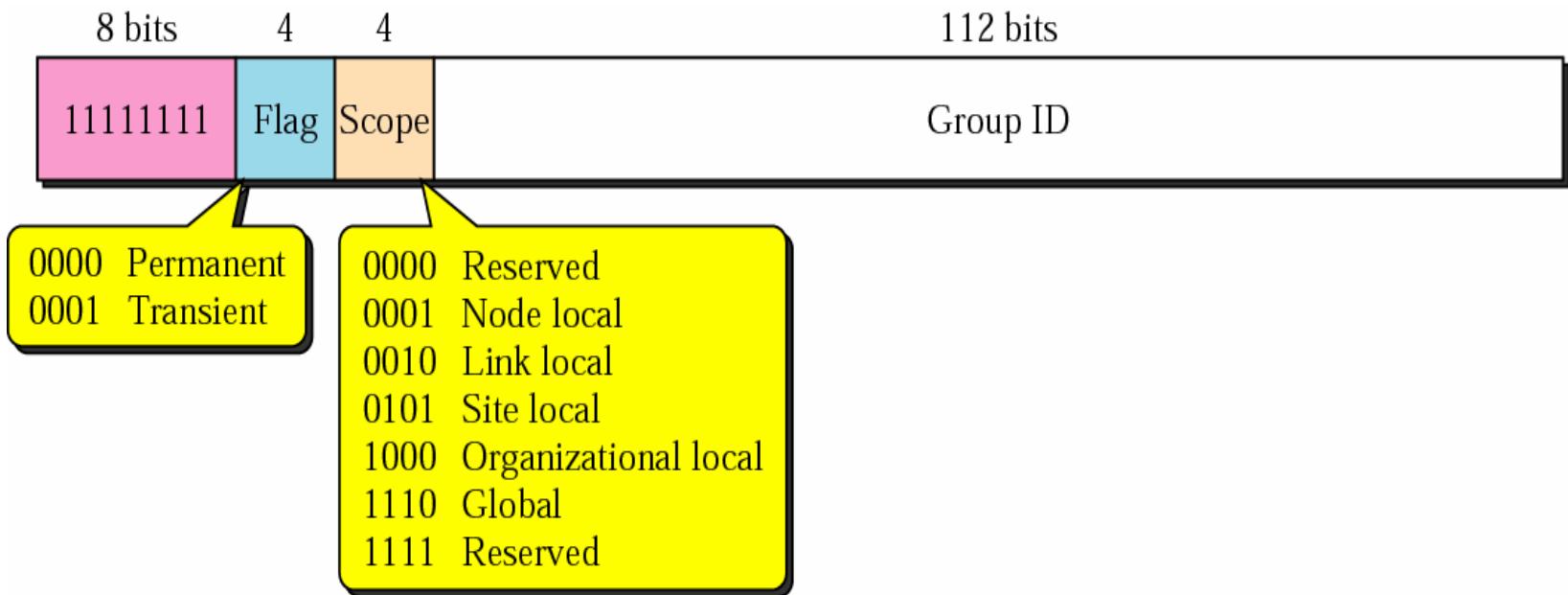
Site Local Address





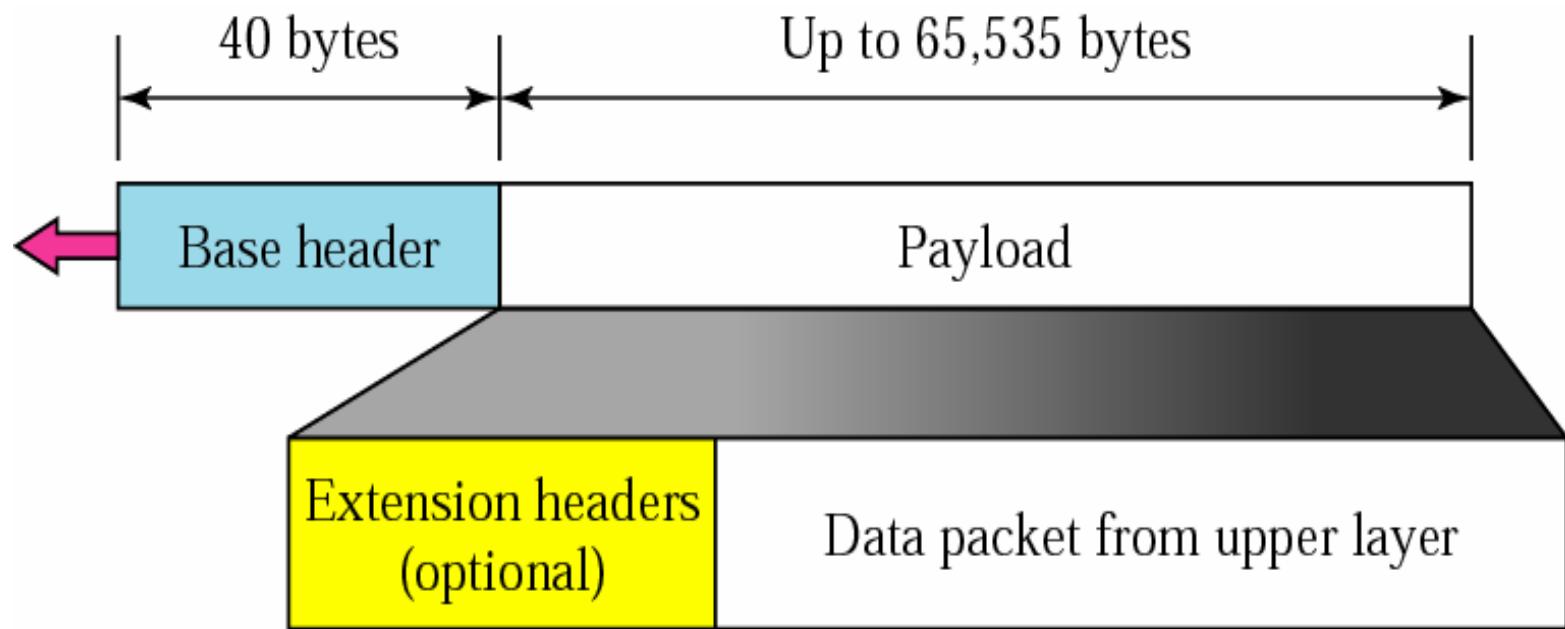
Multicast Address

Global CyberSoft



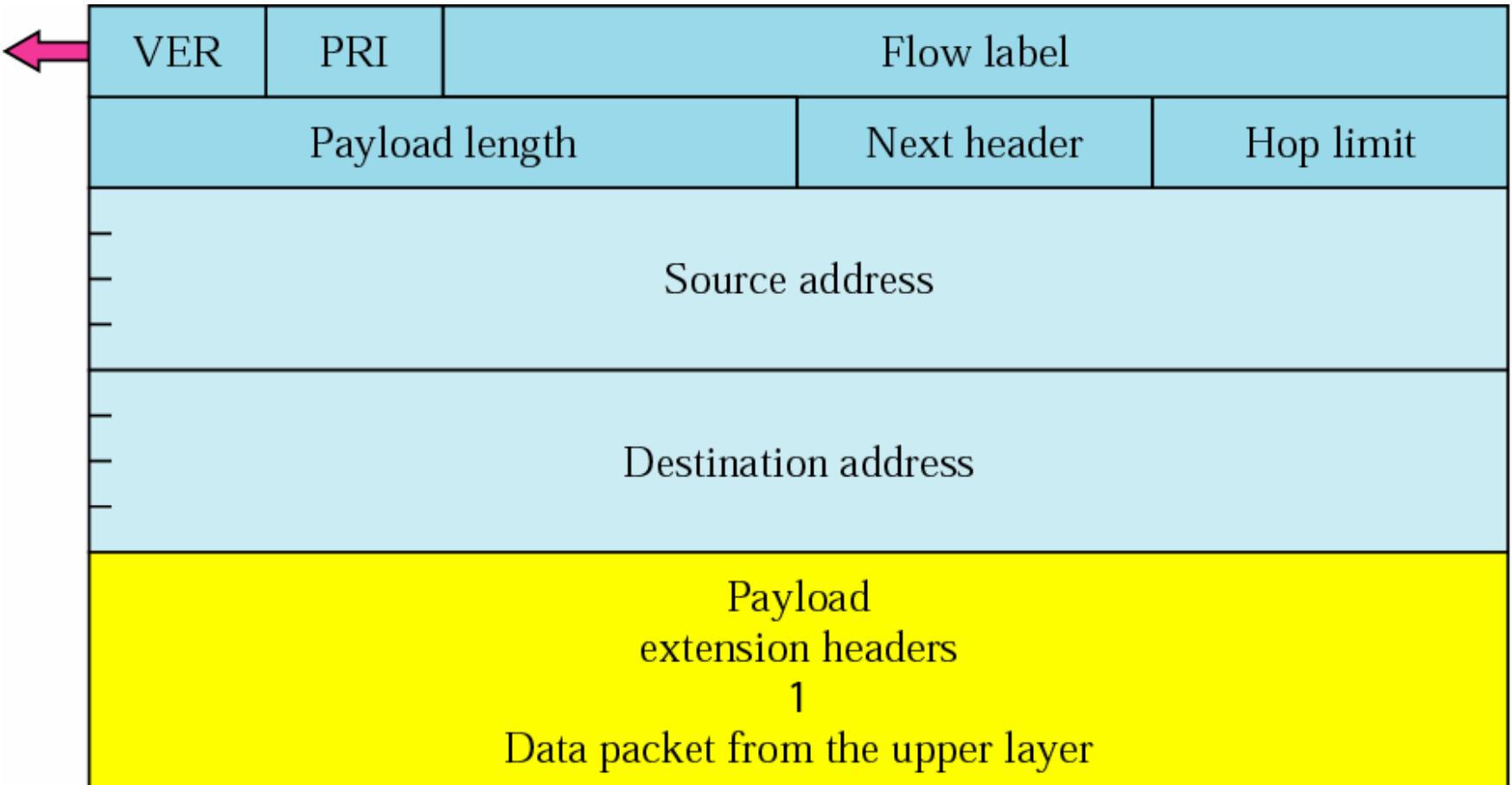


IPv6 Datagram



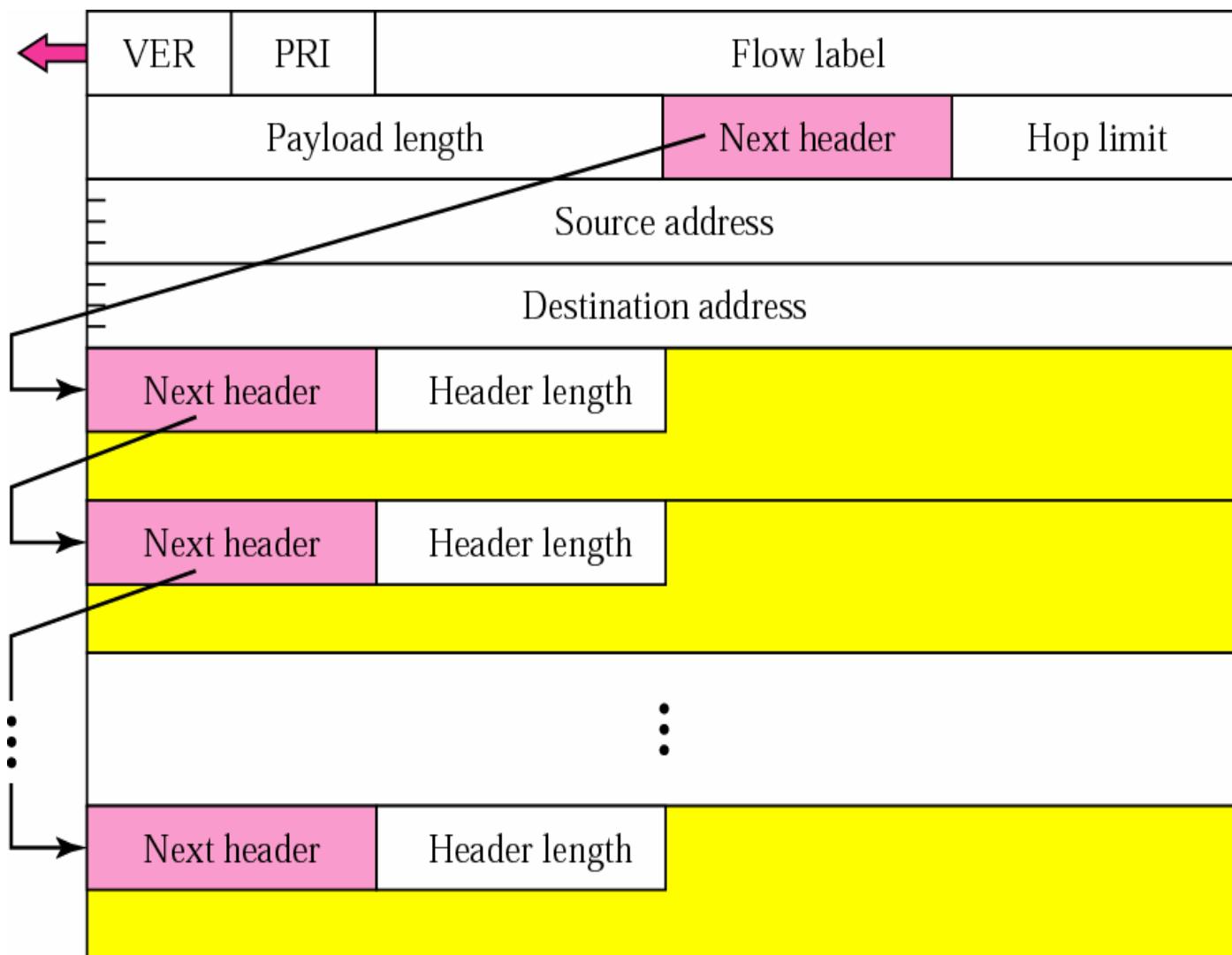


IPv6 Datagram Format



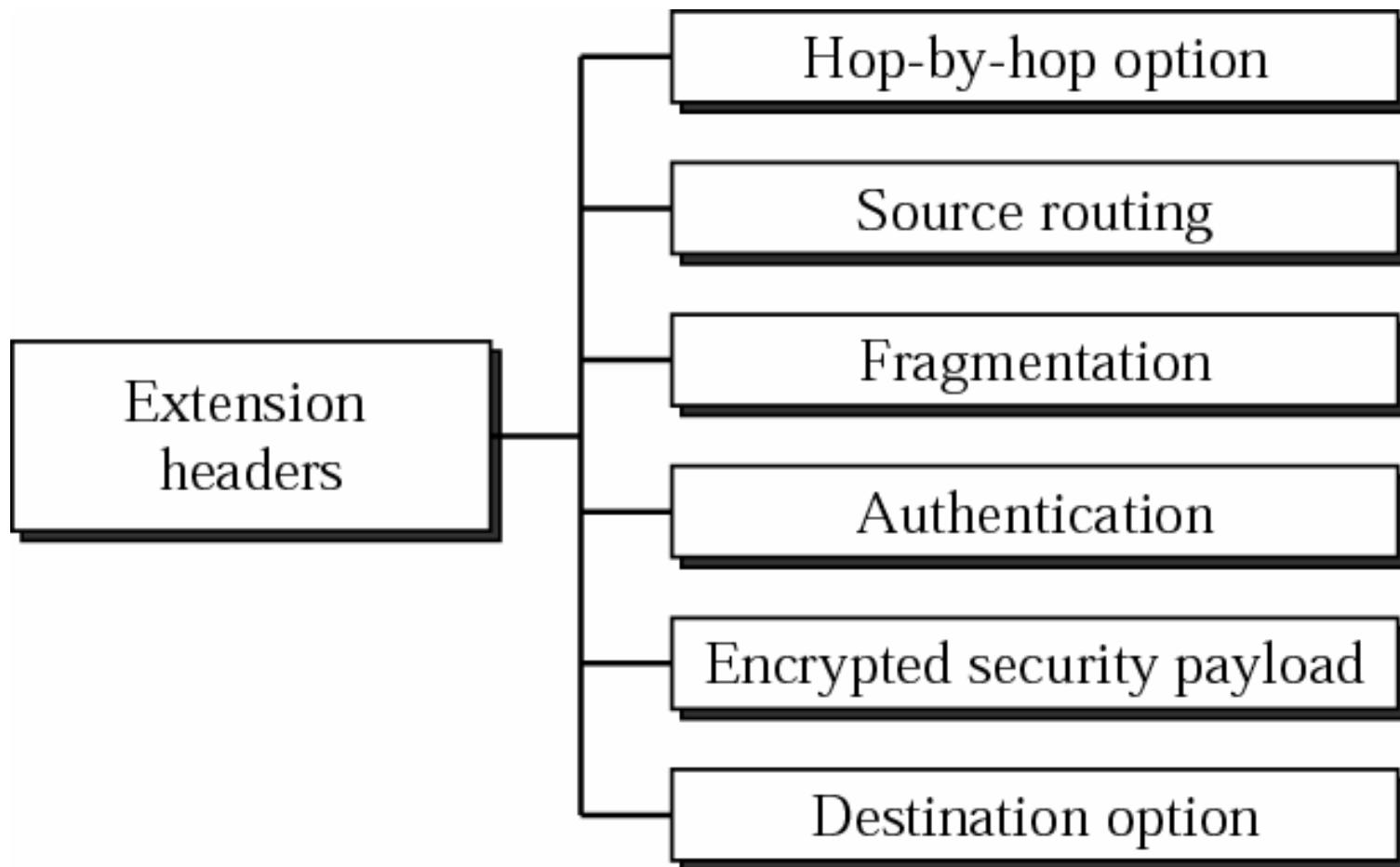


Extension Header Format





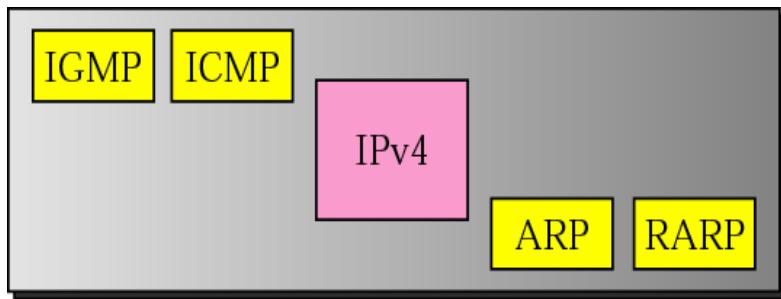
Extension Header Type



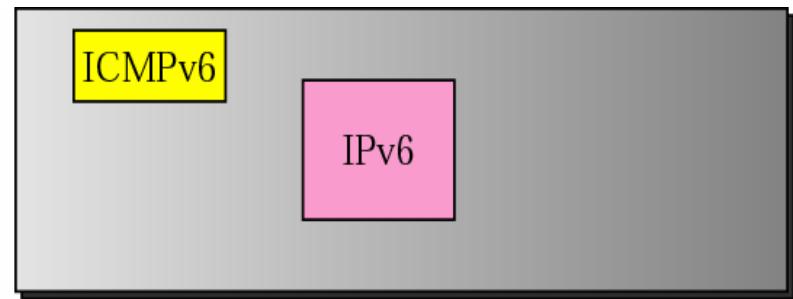


ICMPv6

Global CyberSoft



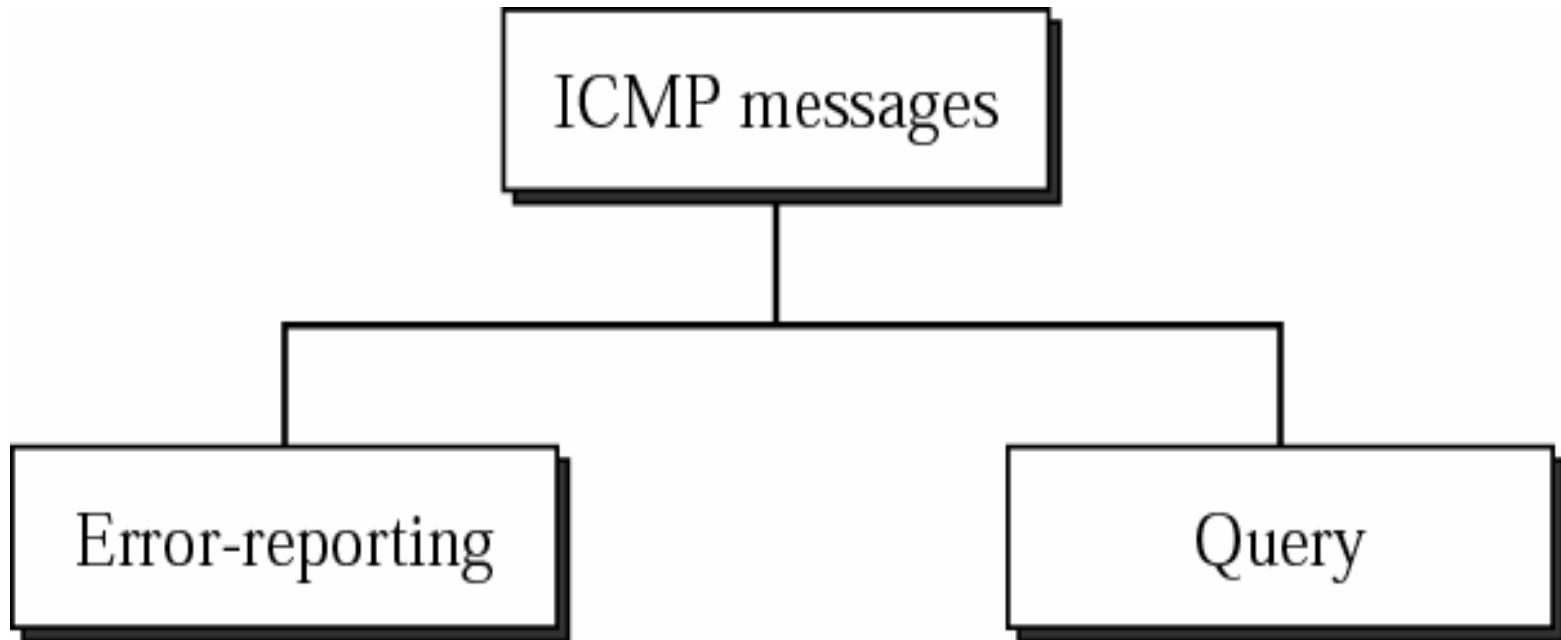
Network layer in version 4



Network layer in version 6

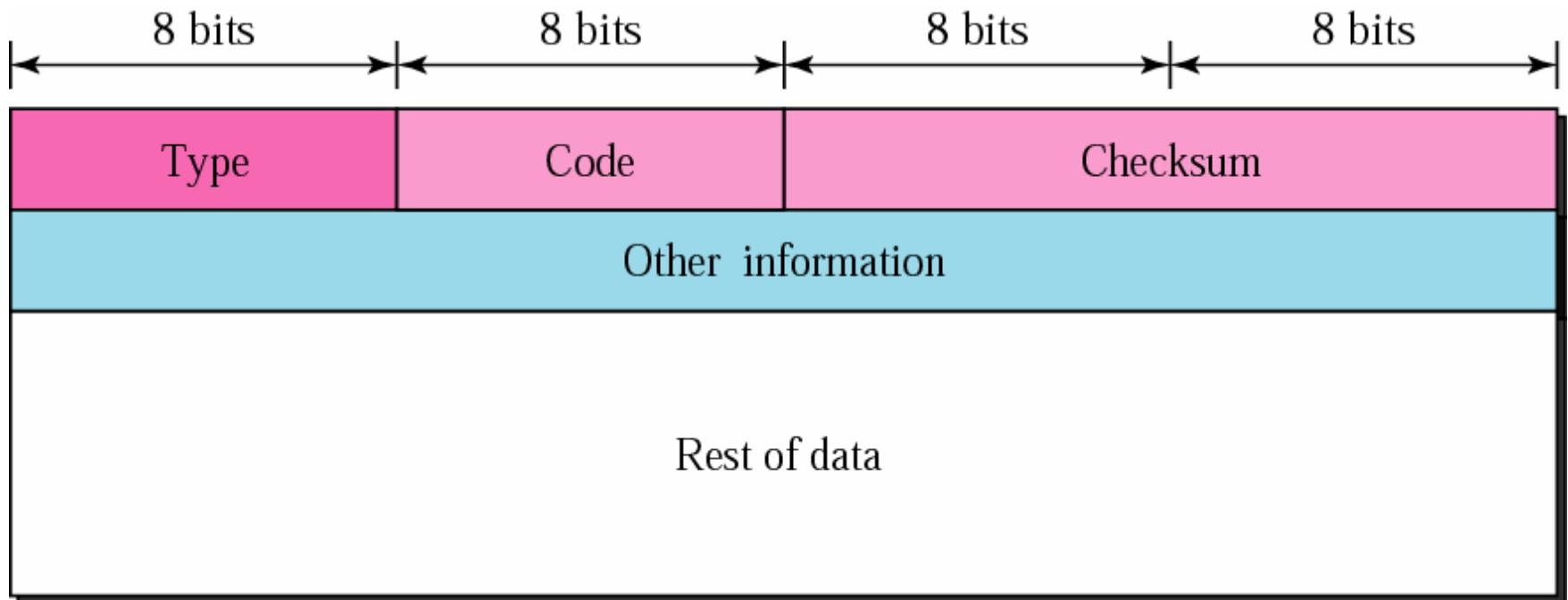


Categories of ICMPv6 messages



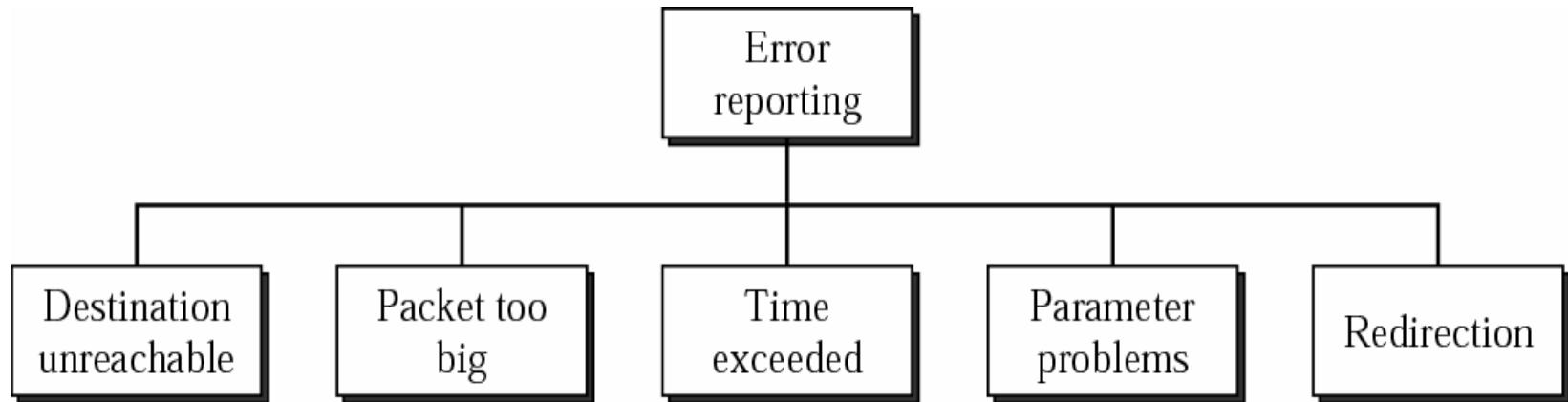


General format of ICMPv6 message





Error reporting Message





Destination Unreachable Message

Type: 1

Code: 0 to 4

Checksum

Unused (All 0s)

Part of the received IP datagram including IP header
plus the first 8 bytes of datagram data



Packet-too-big Message

Type: 2

Code: 0

Checksum

MTU

Part of the received IP datagram including IP header
plus the first 8 bytes of datagram data



Time-exceeded message

Type: 3

Code: 0 or 1

Checksum

Unused (All 0s)

Part of the received IP datagram including IP header
plus the first 8 bytes of datagram data



Parameter problem message

Type: 4	Code: 0, 1, 2	Checksum
Offset pointer		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

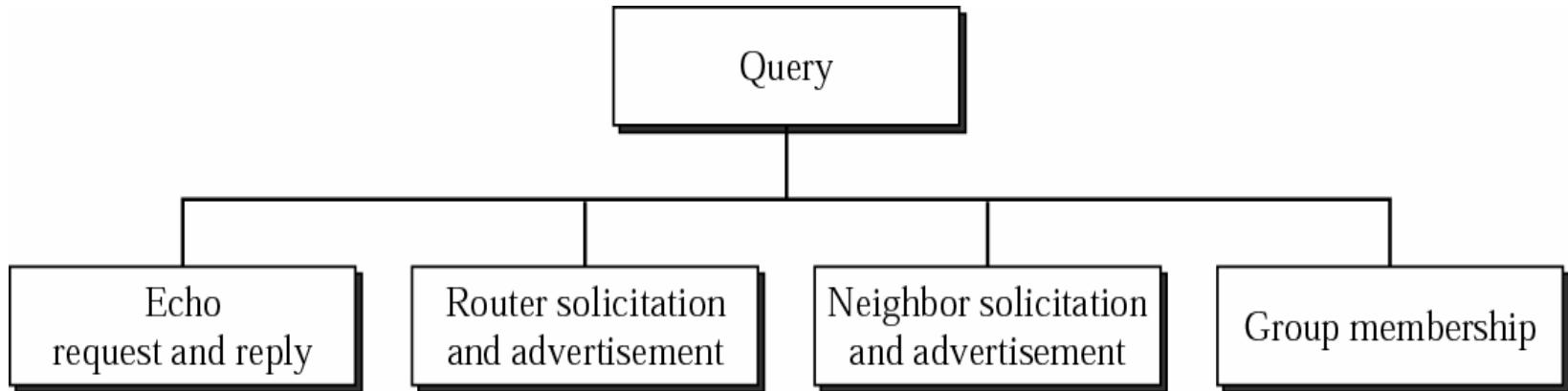
Redirection Message

Type: 137	Code: 0	Checksum
Reserved		
Target (router) IP address		
Destination IP address		
OPT. code	OPT. length	
Target (router) physical address		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		



Query Message

Global CyberSoft



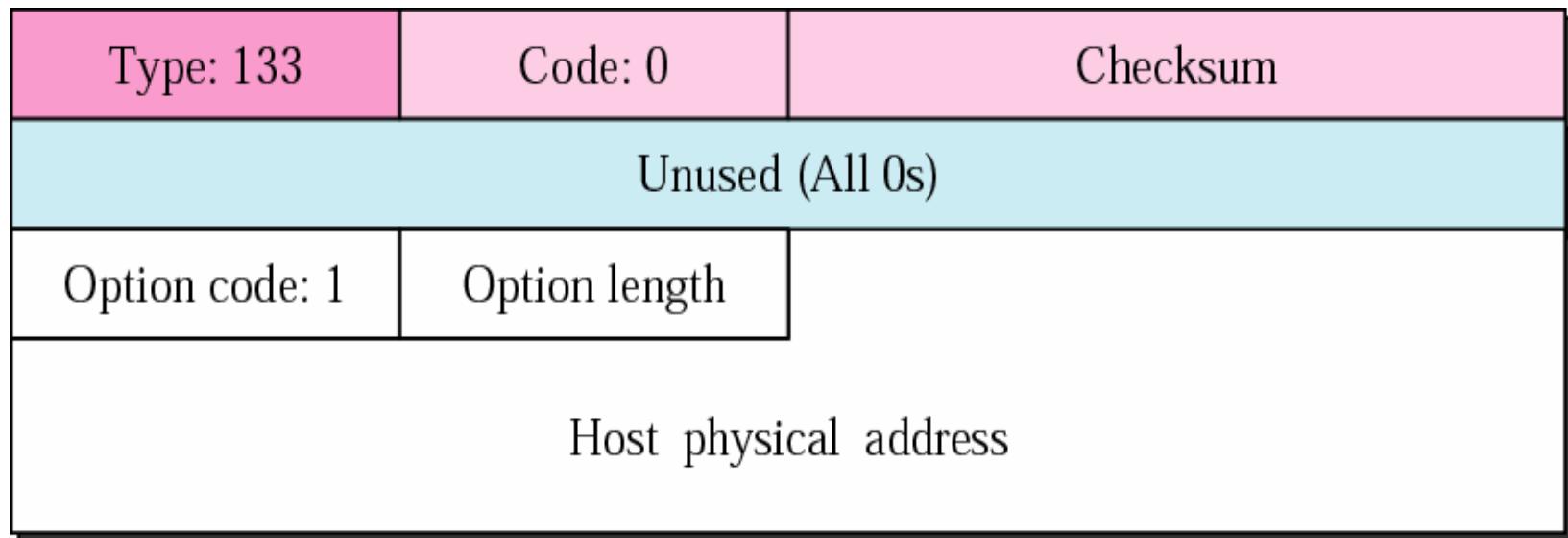


Echo Request and Reply

Type: 128 or 129	Code: 0	Checksum
Identifier		Sequence number
Optional data Sent by the request message; repeated by the reply message		



Router solicitation message



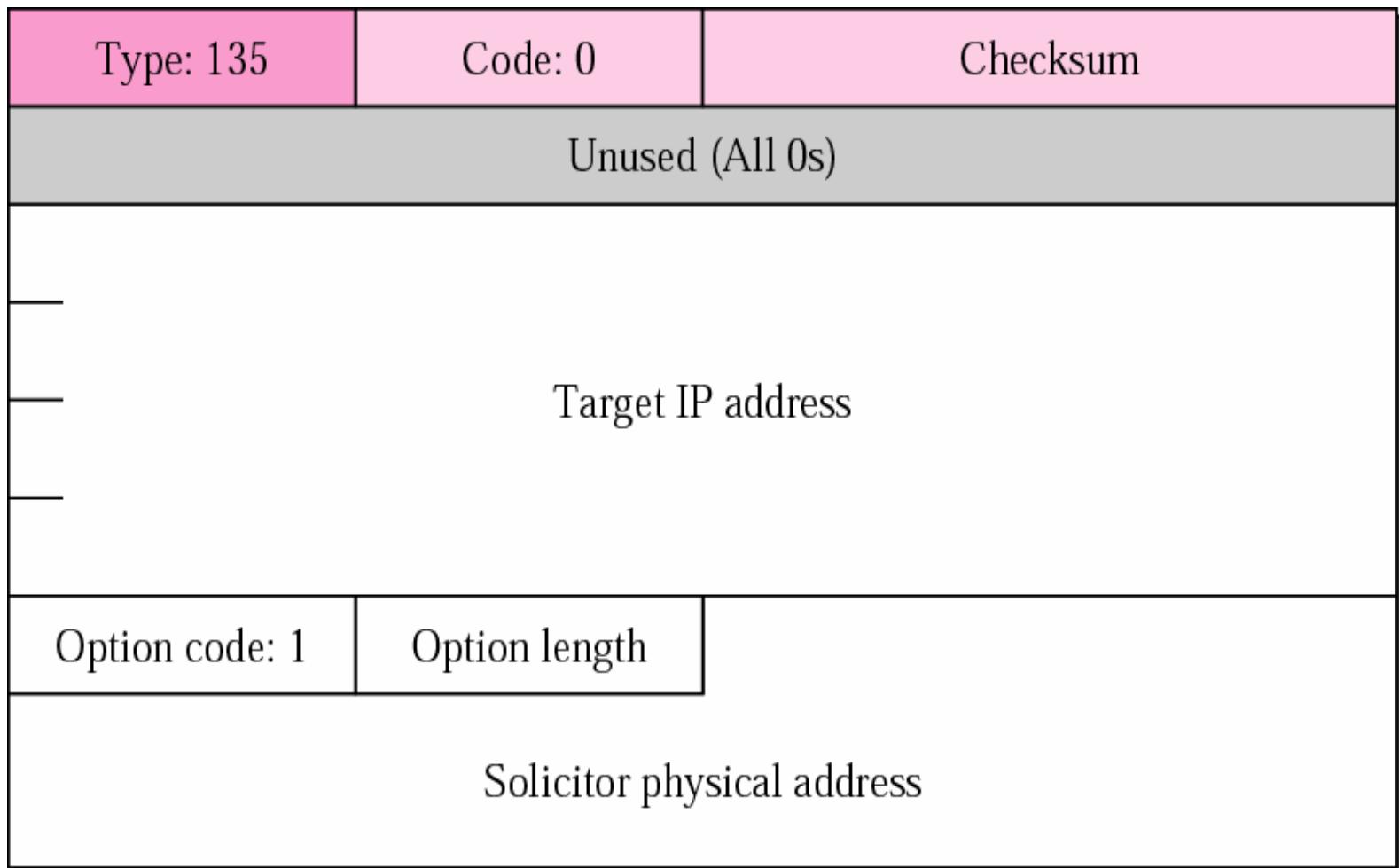
- a. Router solicitation format

Router advertisement message

Type: 134	Code: 0	Checksum
Max hop	M O Unused(All 0s)	Router lifetime
Reachability lifetime		
Reachability transmission interval		
Option code: 1	Option length	
Router physical address		
Option code: 5	Option length	Unused (All 0s)
MTU size		

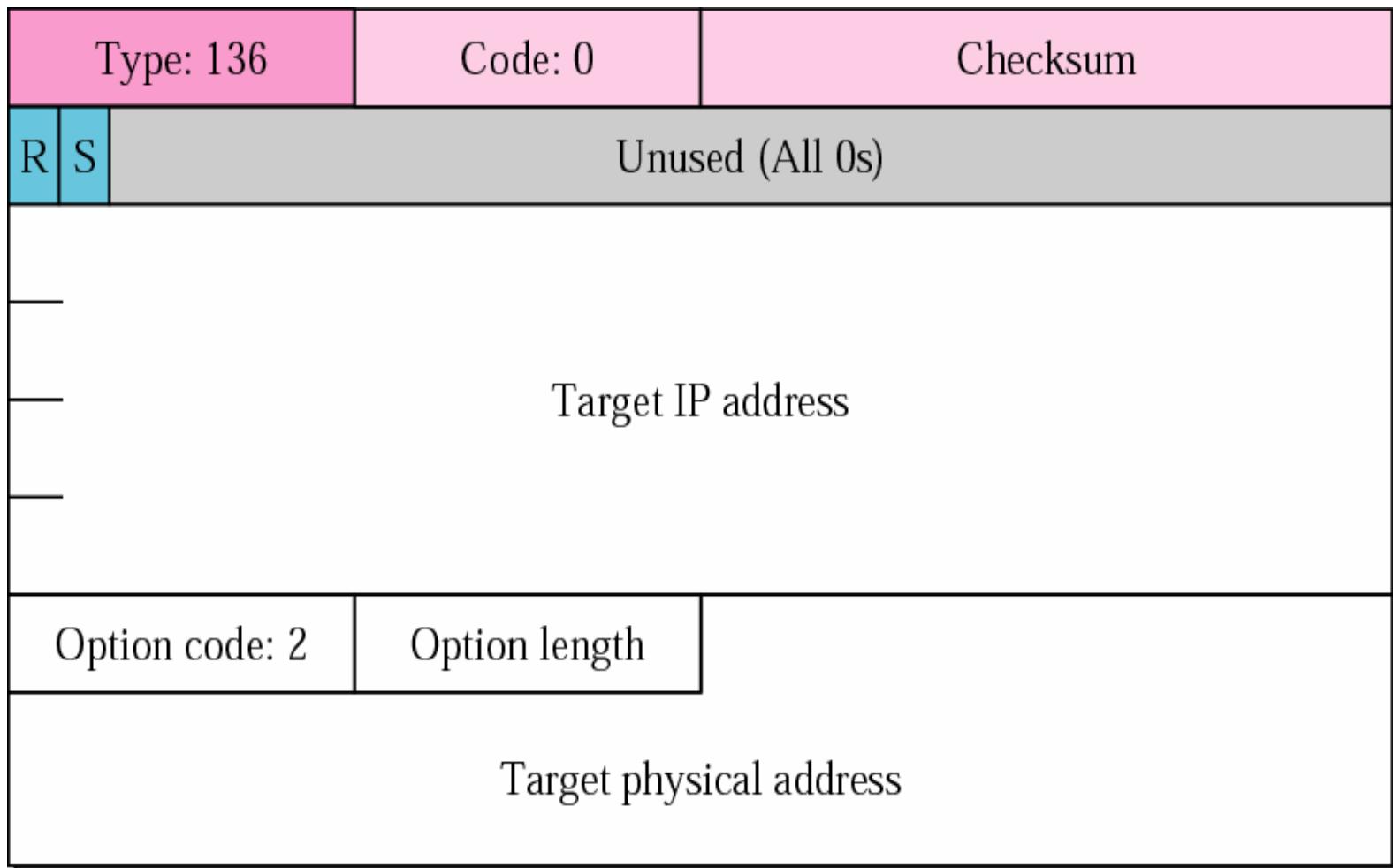
b. Router advertisement format

Neighbor solicitation message



a. Neighbor solicitation

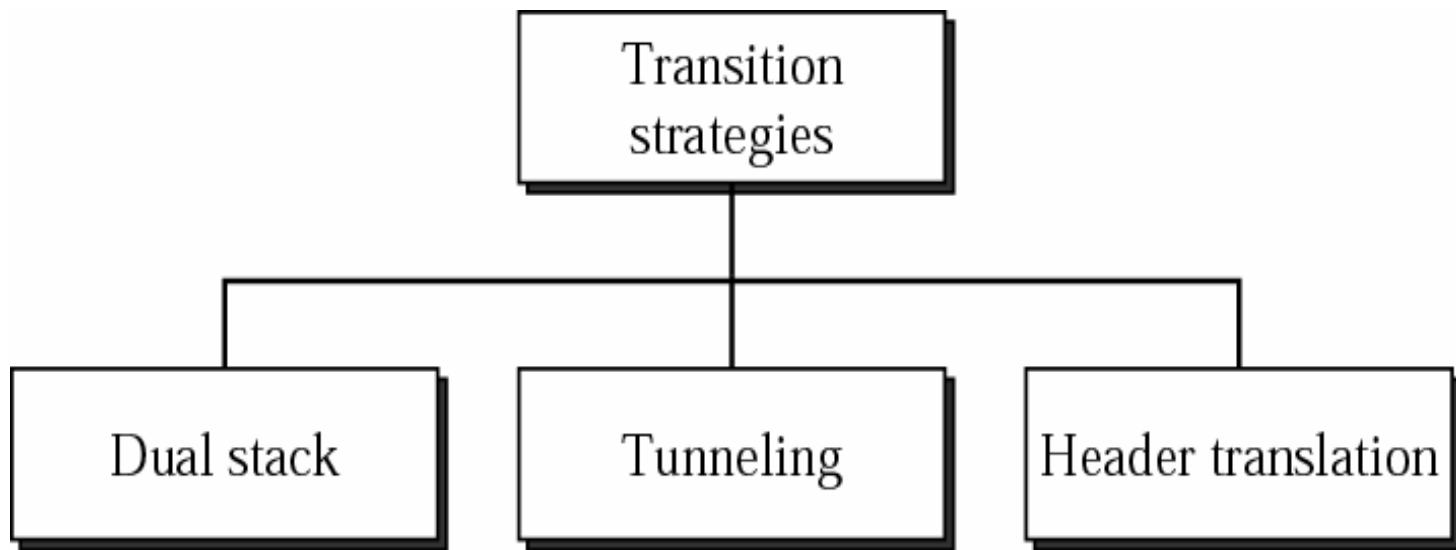
Neighbor advertisement message



b. Neighbor advertisement

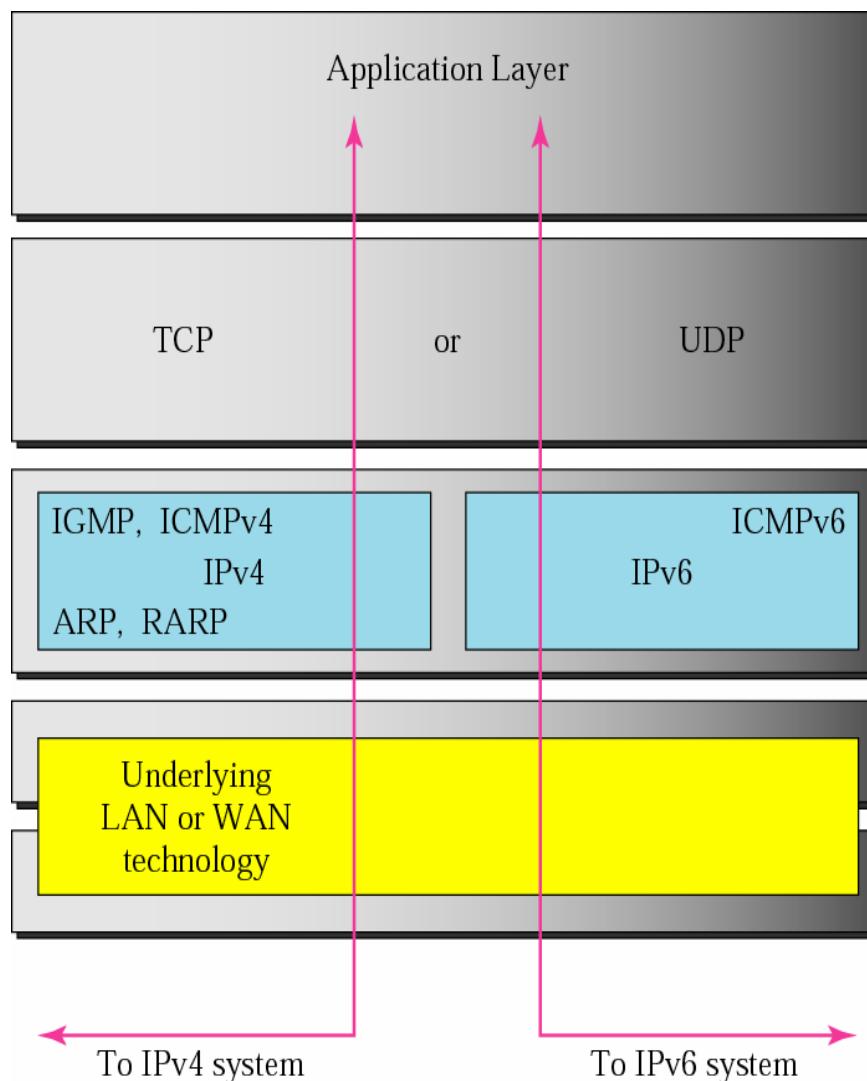


Transition from IPv4 to IPv6



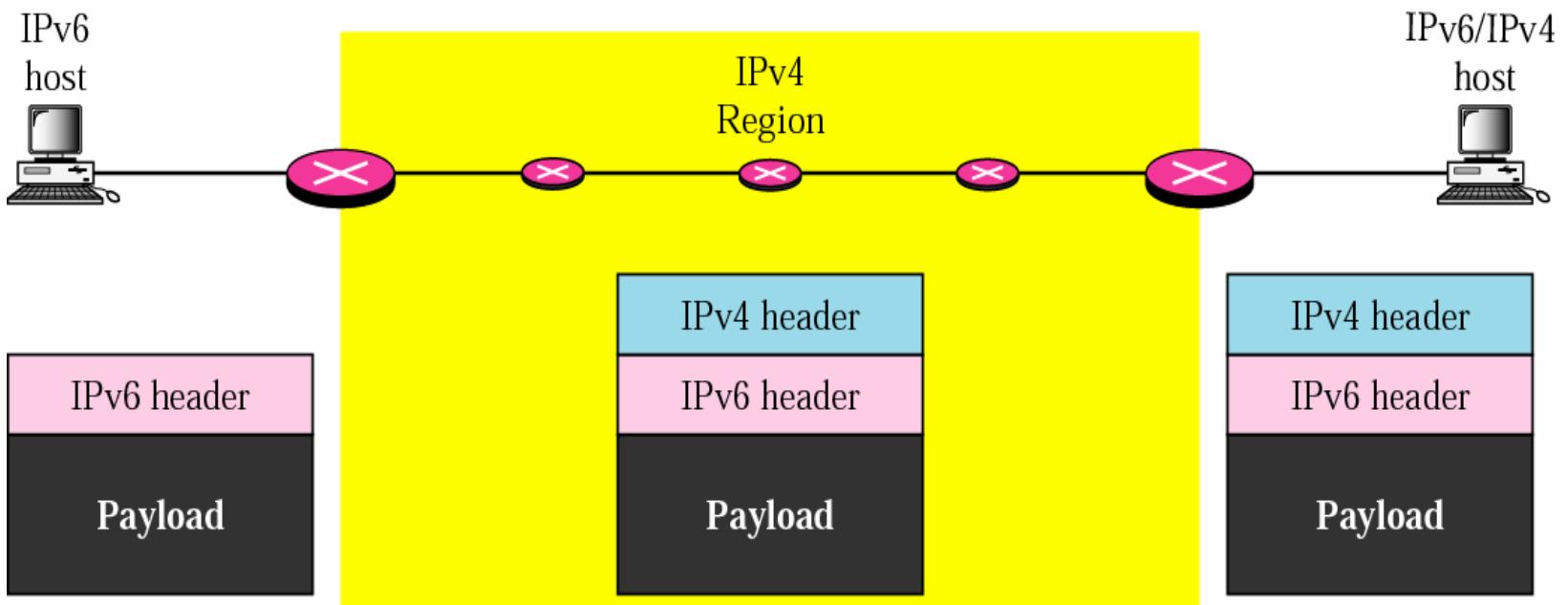


Dual Stack



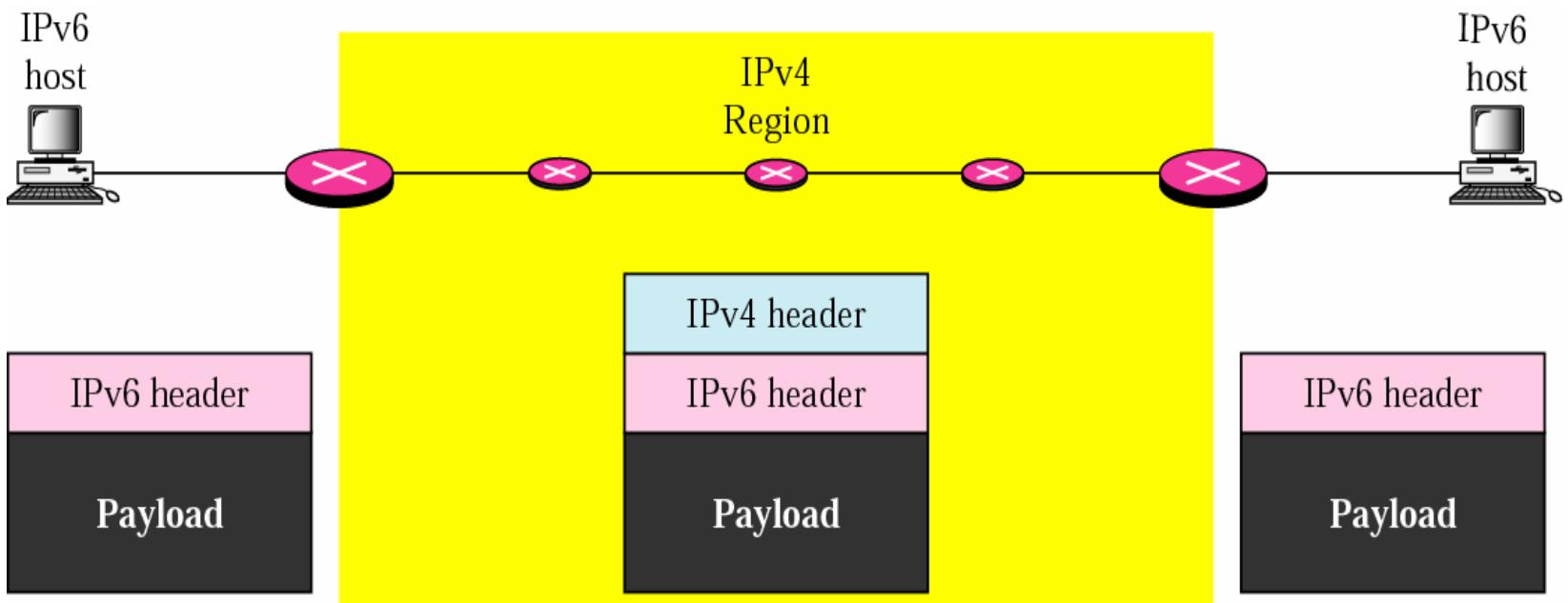


Automatic Tunneling



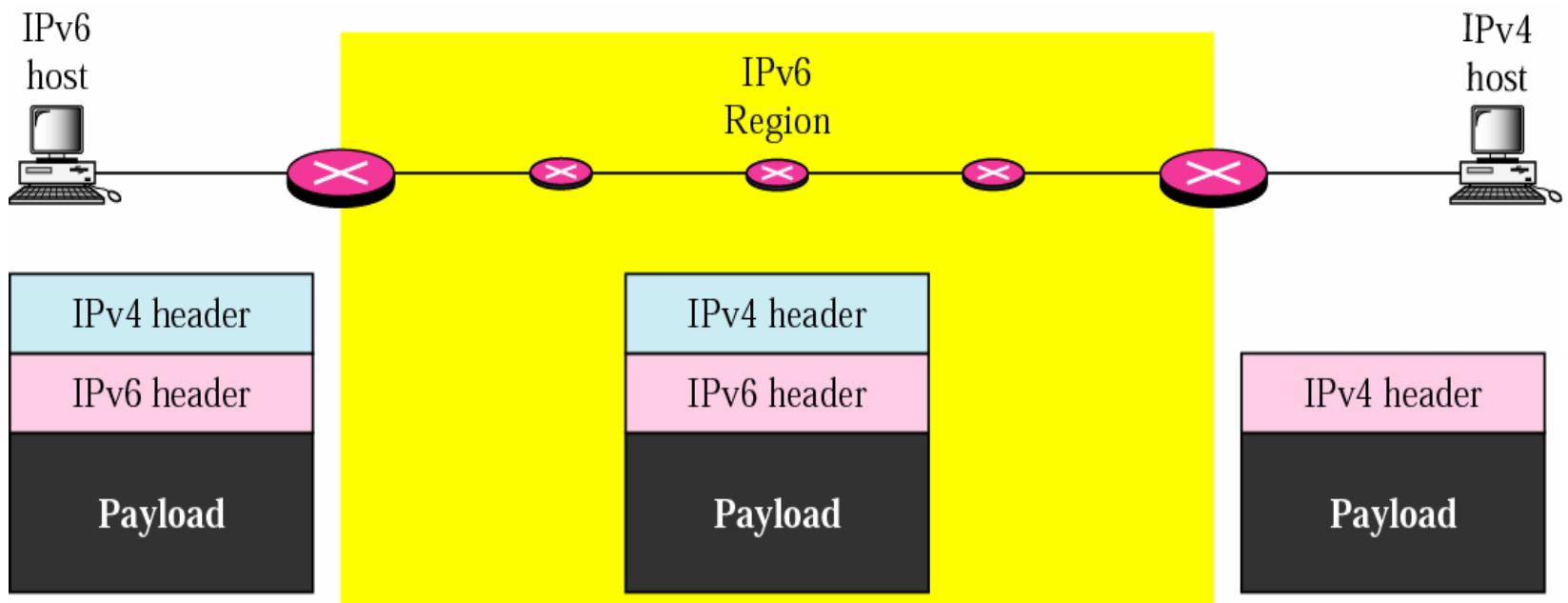


Configured Tunneling





Header Translation





Thanks

Global CyberSoft

Thanks for your attention!