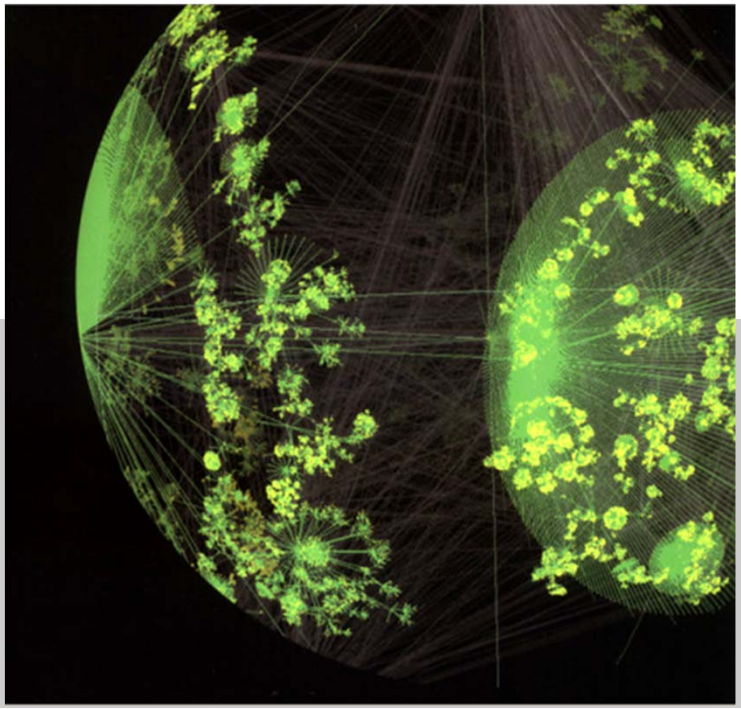


EL5373 Review 1

TCP/IP Essentials

A Lab-Based Approach

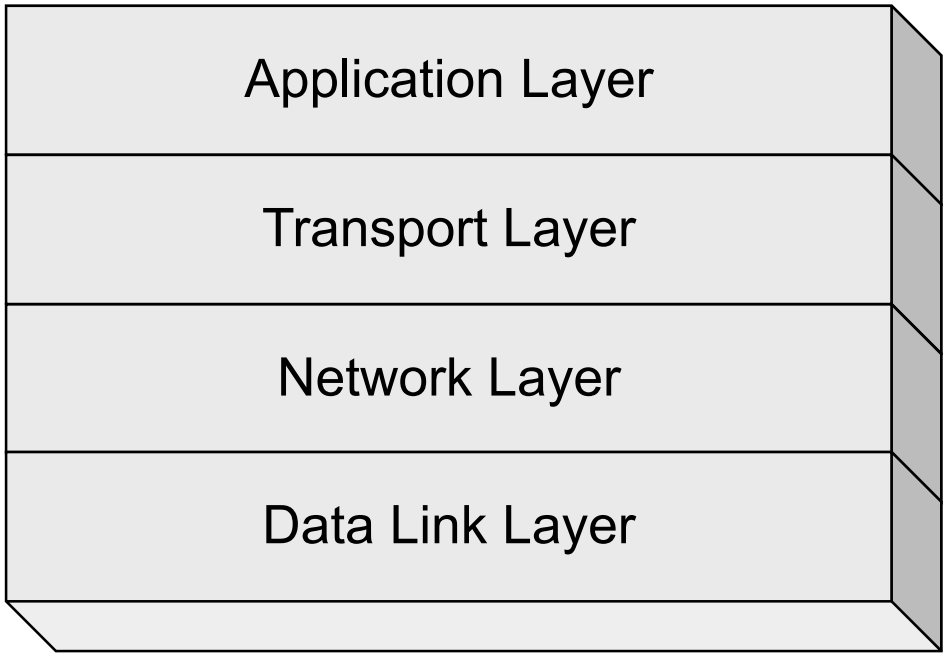
Spring 2017

Hierarchical Communication Architecture

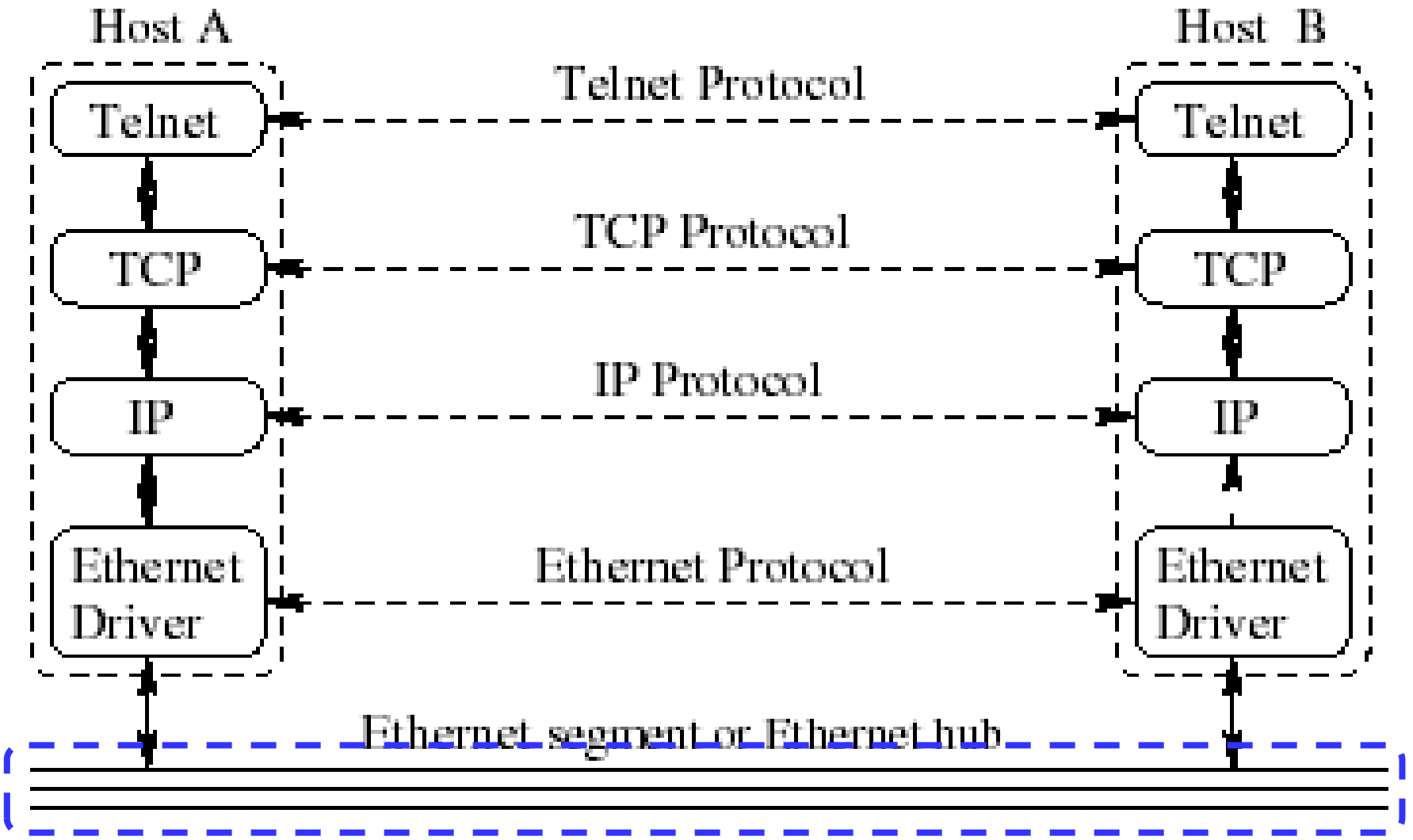
- Networking can be quite complex and requires a high degree of cooperation between the involved parties.
- Cooperation is achieved by forcing parties to adhere to a set of rules and conventions (protocols).
- The complexity of the communication task is reduced by using multiple protocol layers:
  - Each protocol is implemented independently.
  - Each protocol is responsible for a specific subtask.
  - Protocols are grouped in a hierarchy.
- A structured set of protocols is called a communications architecture or protocol suite.

TCP/IP Protocols

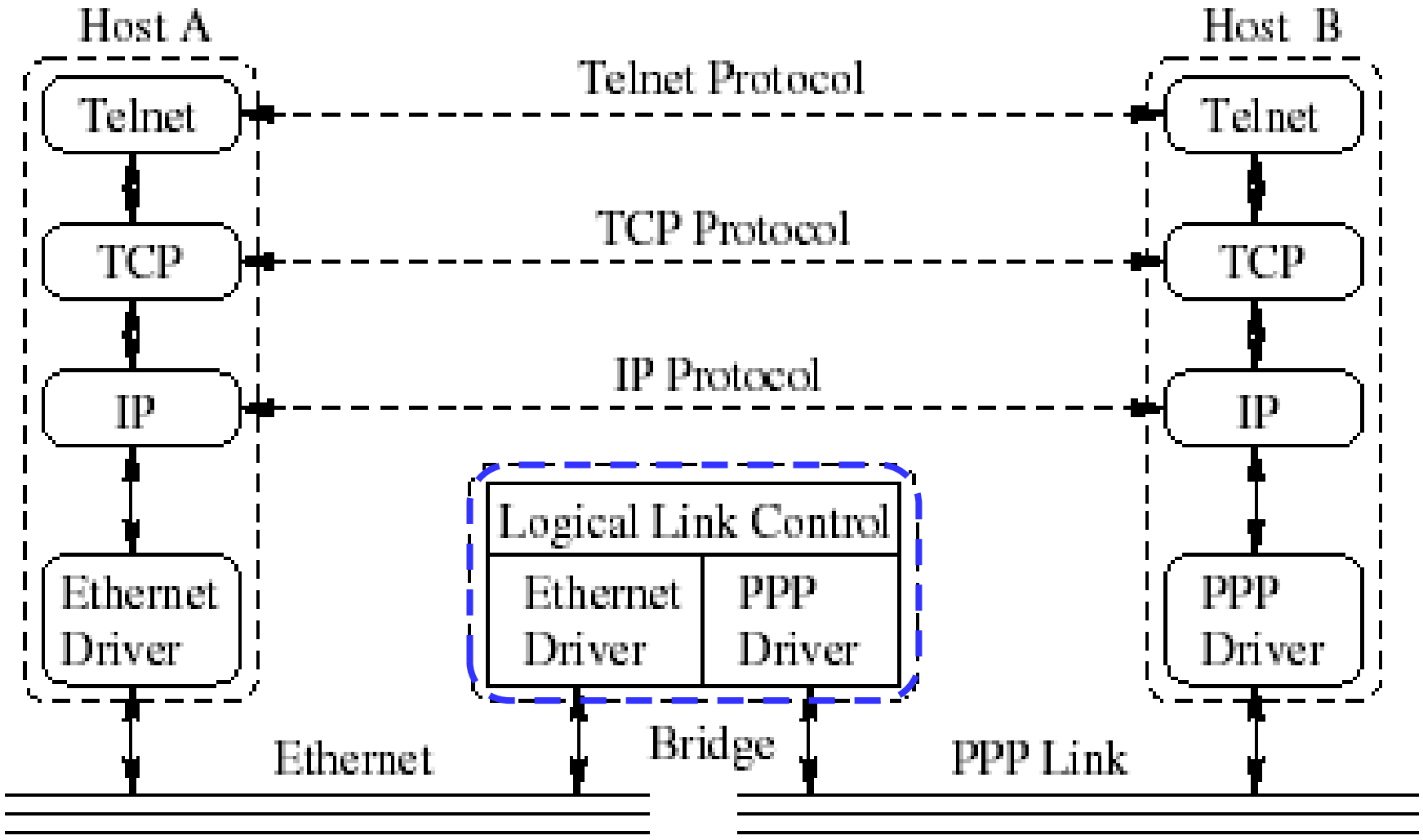
- Internet Protocol Suite
- A combination of different protocols
- Organized into four layers



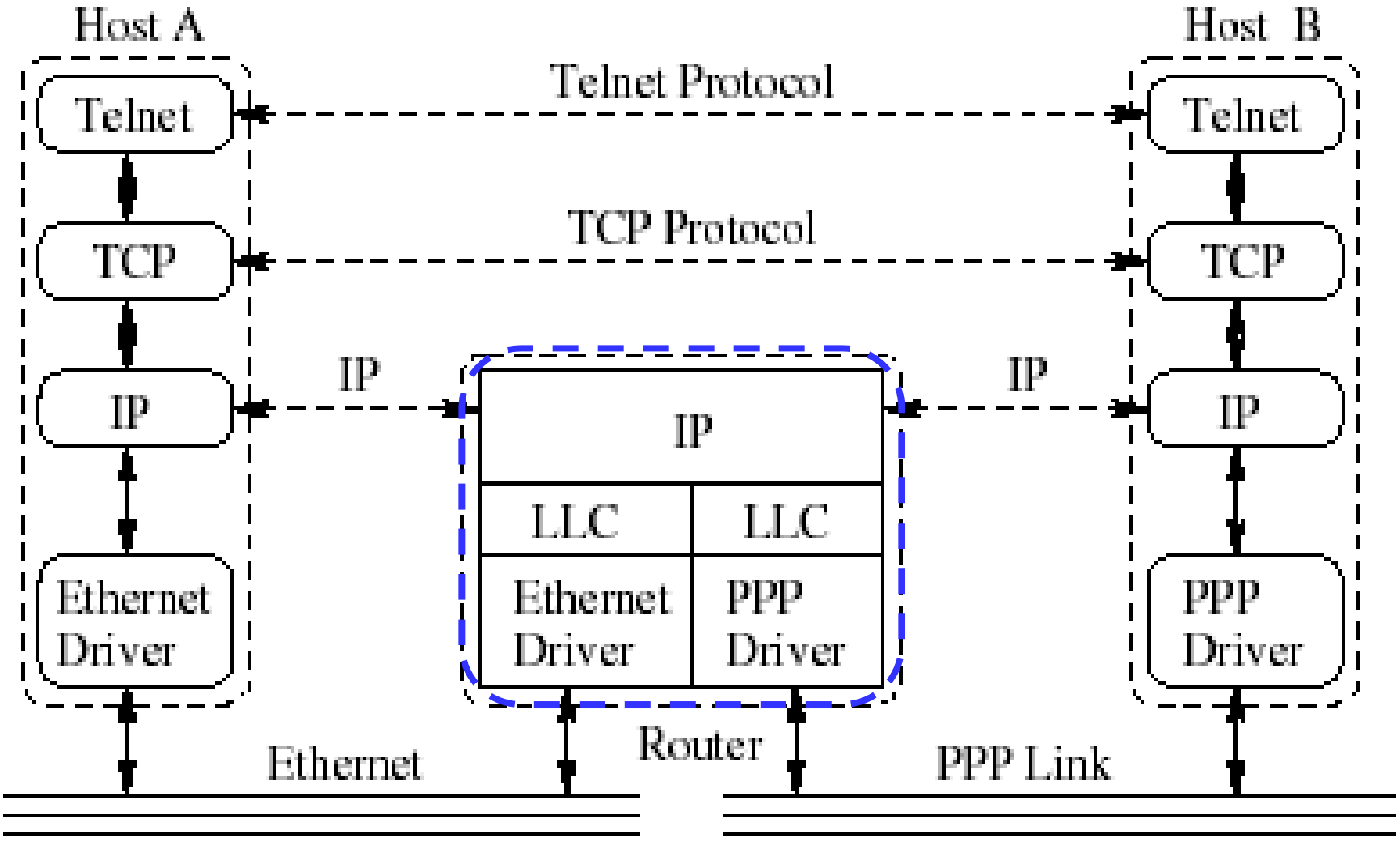
Hosts Communicating over a Hub



Hosts Communicating over a bridge

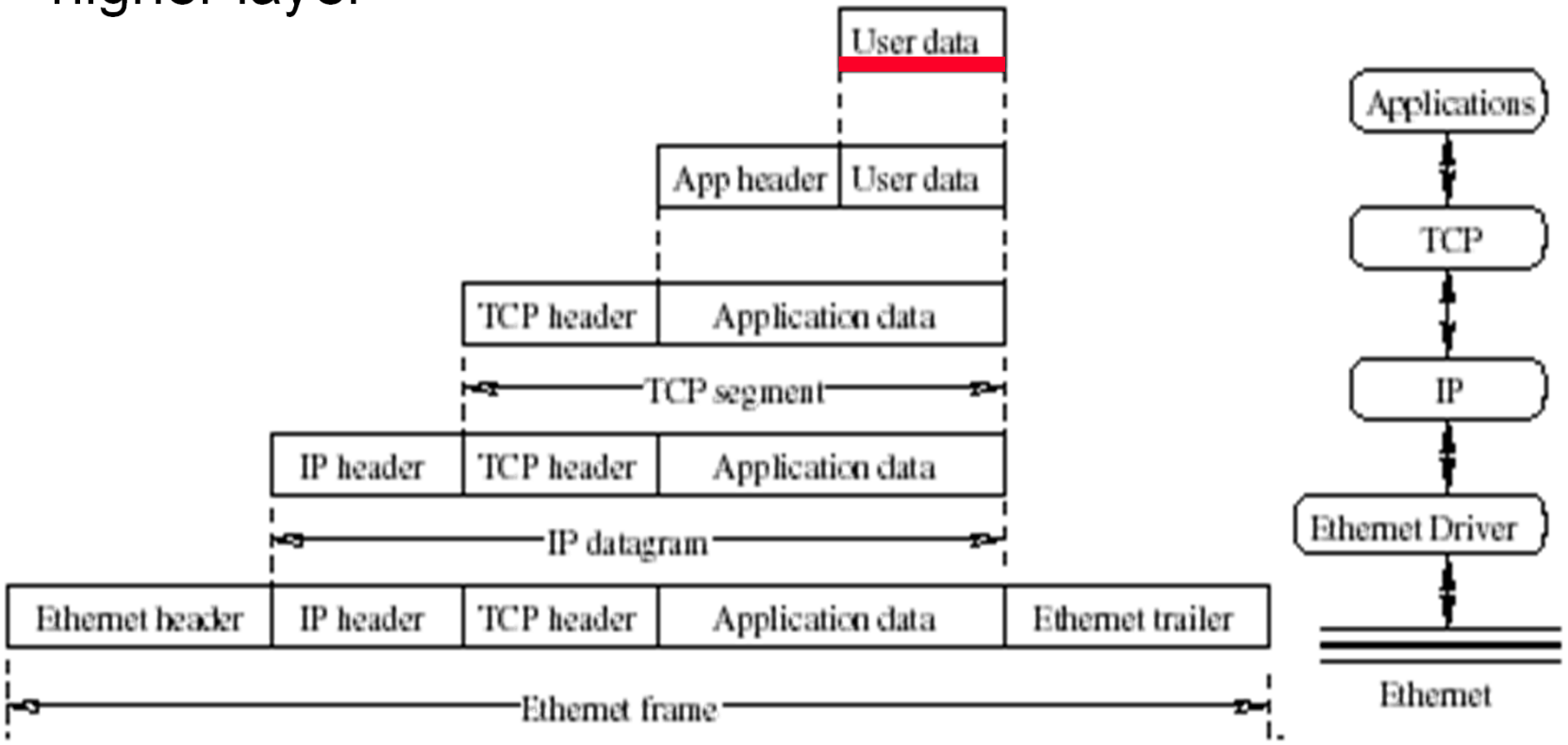


Hosts Communicating over a router



Encapsulation

- The application data is sent down
- Each layer adds a header to the data (PDU) from its higher layer



Naming and Addressing

- Uniquely identify processes in different computers for communications.
  - Domain name
  - MAC address
  - IP address
  - Port number

An Example:
How TCP/IP Protocols Work Together

- Bob, a user, wants to book an air ticket from an online booking website.
- Bob knows the domain name www.expedia.com
- The remote computer with the domain name is a web server.

An Example – the Application

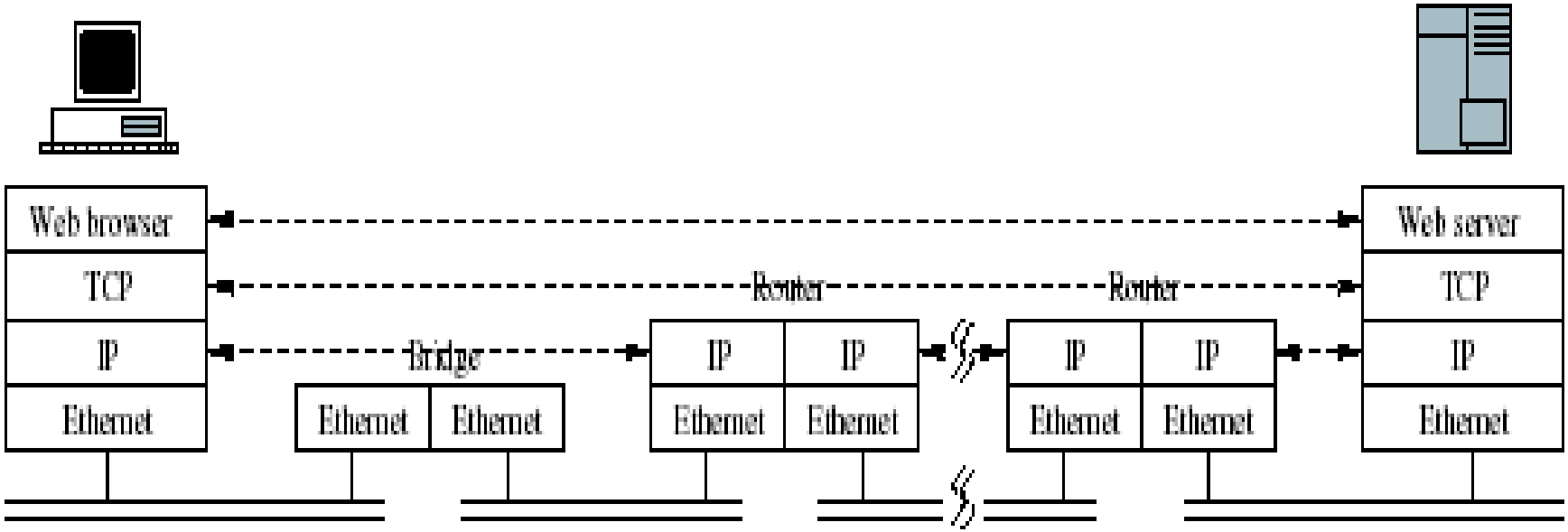
- The web server provides the web service.
- Bob uses a web browser, which is a web client, to request and receive web service.
- The HyperText Transfer Protocol (HTTP), an application layer protocol, is used by the web server and browser.

An Example – DNS

- Bob starts MS Internet Explorer in his computer, and types http://www.expedia.com/index.html.
- The domain name needs to be translated to an IP address.
- A DNS query is sent to a DNS server.
- A DNS reply will return to the client with the IP address.

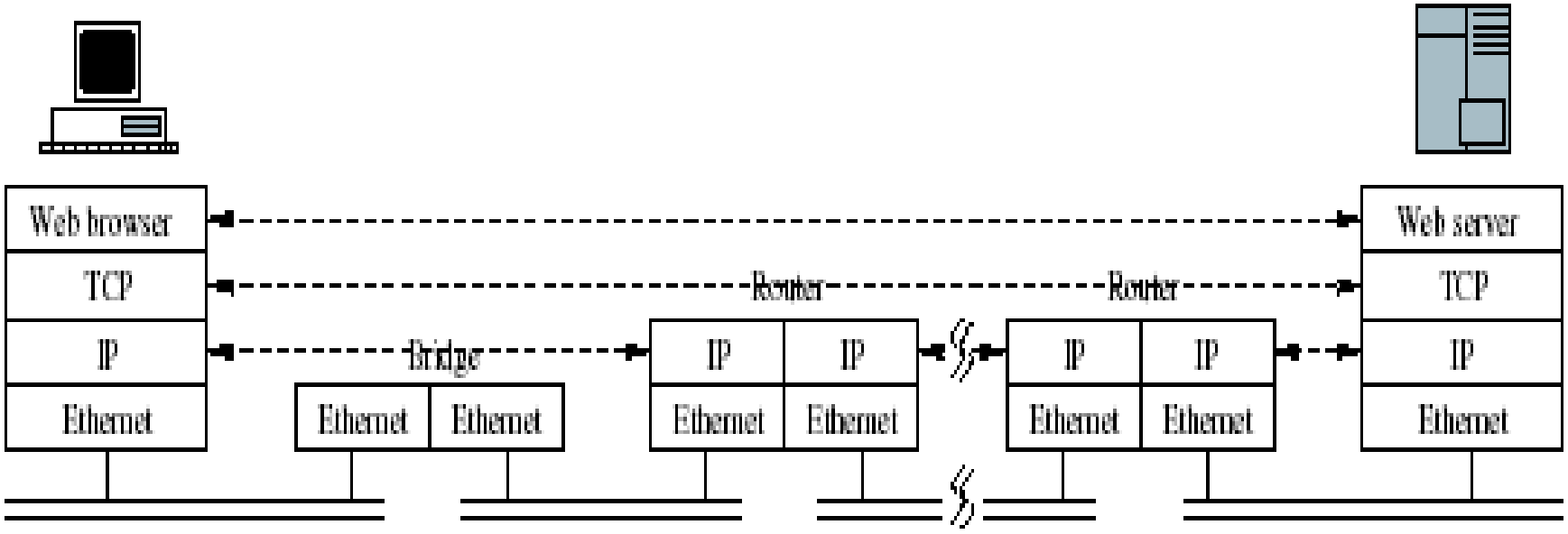
An Example – TCP Connection

- The client establishes a TCP connection to the web server.
- A port number is carried in all packets in this process.
- Application data (an HTTP request message for the index.html file) is sent over the TCP connection, encapsulated in a TCP segment.



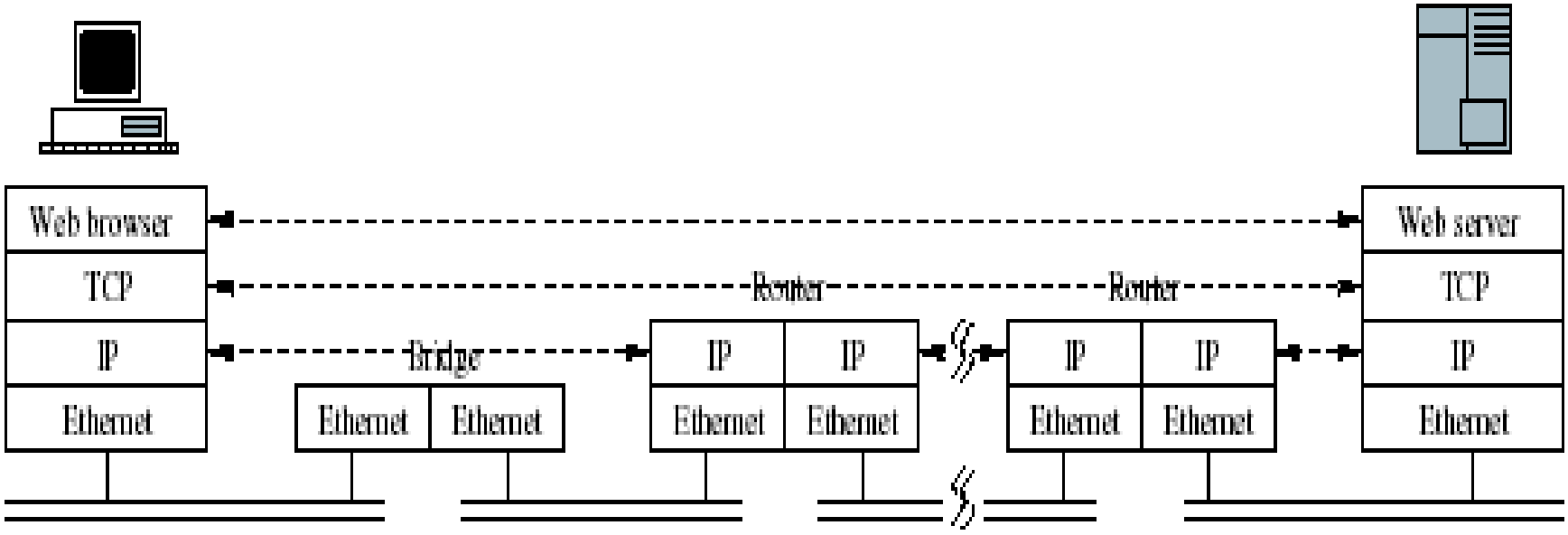
An Example – IP Layer

- The TCP segment is sent down to the IP layer and encapsulated in an IP datagram.
- Routers will forward the IP datagram hop by hop to the web server by checking their routing tables.



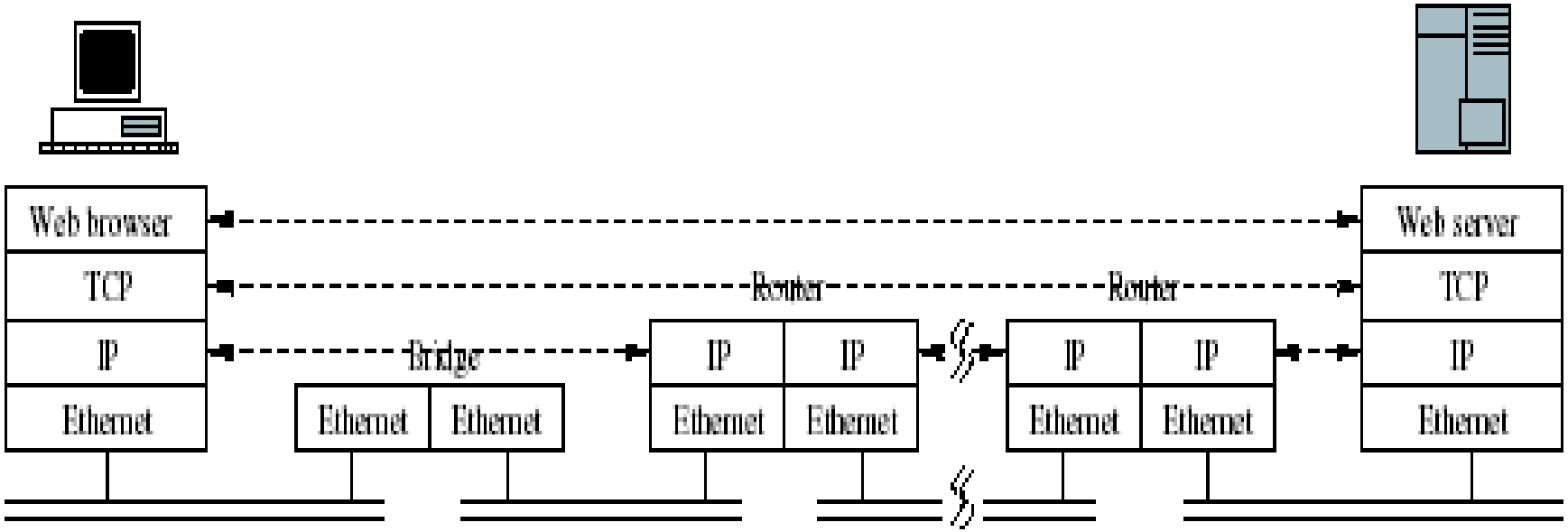
An Example – MAC Layer

- The IP datagram and the next-hop router's IP address down to the MAC layer.
- The IP datagram is encapsulated in an Ethernet frame.



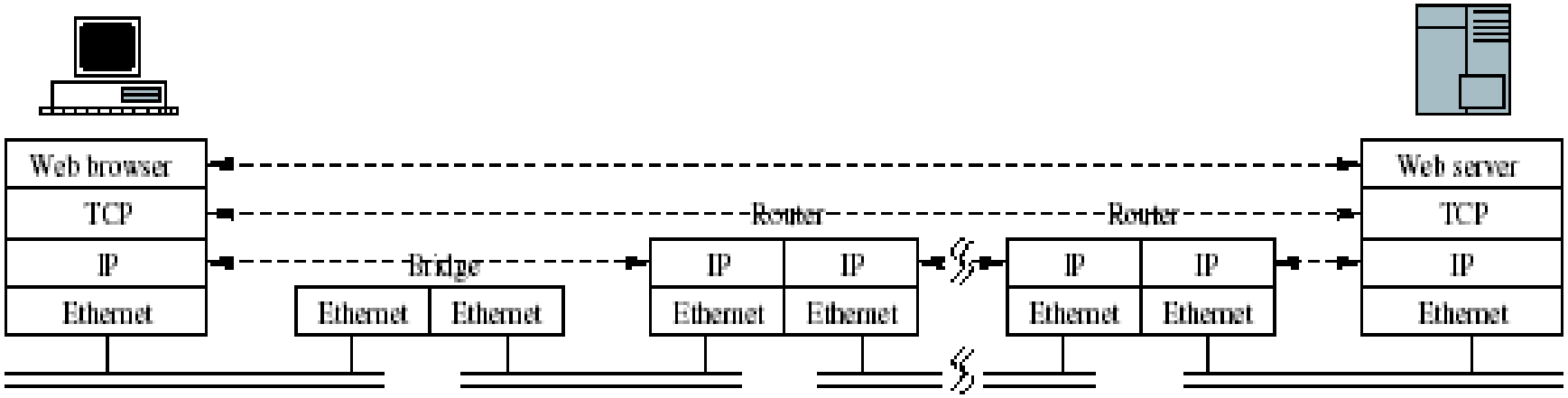
An Example – ARP

- The Ethernet frame needs to be sent to the interface of the next-hop router.
- Only Ethernet MAC address can be recognized.
- ARP request/reply is used to resolve the MAC address.



An Example – On the Other End

- The web server receives the Ethernet frame.
- The packet is delivered to the upper layers.
- When the application layer receives the HTTP request message, it sends an HTTP response message to the client.



Domain Name

- Identify a host
- User friendly
- Hierarchically organized
  - Examples: eeweb.poly.edu, mta.nyc.ny.us
- Domain Name System (DNS): resolves a domain name to the corresponding IP address.
  - DNS servers and the distributed domain name database
  - Name caching
  - DNS query and reply

Ethernet Frame Format

- Source Ethernet (MAC) Address
- Destination Ethernet (MAC) Address
- Frame Type: used to identify the payload
- CRC: used for error control

Dest. Addr.	Src. Addr.	Frame Type	Data	CRC
6 bytes	**6 bytes**	**2 bytes**	**46 – 1500 bytes**	**4 bytes**

Ethernet Frame Format (RFC 894)

Dest. Addr.	Src. Addr.	Length	DSAP AA	SSAP AA	Ctrl.	Org. Code	Frame Type	Data	CRC
6 bytes	**6 bytes**	**2 bytes**	**1 byte**	**1 byte**	**1 byte**	**3 bytes**	**2 bytes**	**38 – 1492 bytes**	**4 bytes**

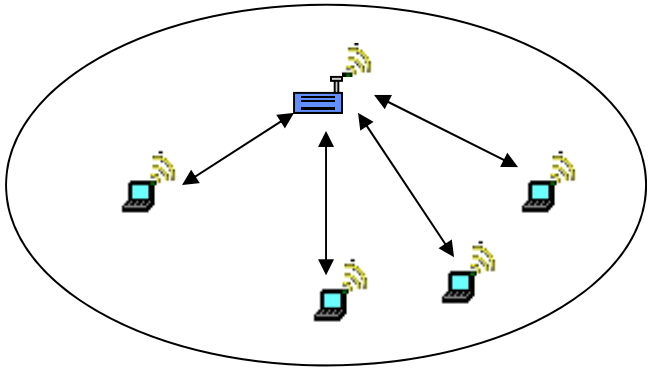
IEEE 802.2/802.3 CSMA/CD Frame Format

Collisions in Ethernet

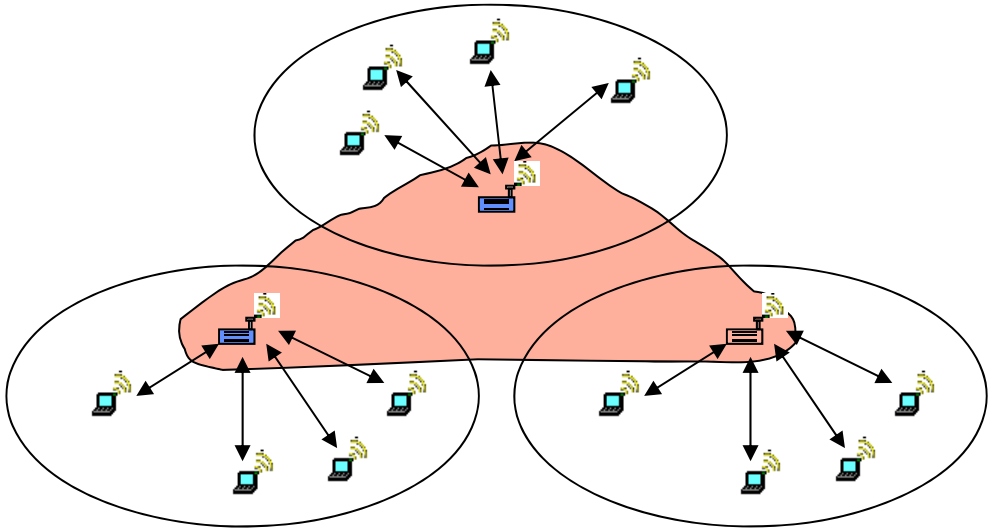
- The collision resolution process of Ethernet requires that a collision is detected while a station is still transmitting.
- Assume the maximum propagation delay on the bus is *a*.
- Restrictions: Each frame should be transmitted at least twice as long as the time to detect a collision (*2a*).

IEEE 802.11 Architecture

Basic Service Set (BSS)



Extended Service Set (ESS)
a.k.a. Infrastructure Mode



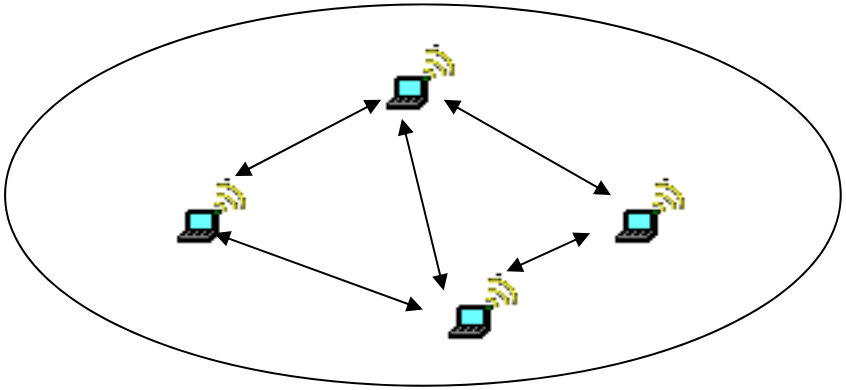
Infrastructure mode

- Fixed Access Point (AP) provides:
  - Connection to wireline network
  - Relay function
- Handoff, an active host moves from one access point to another.

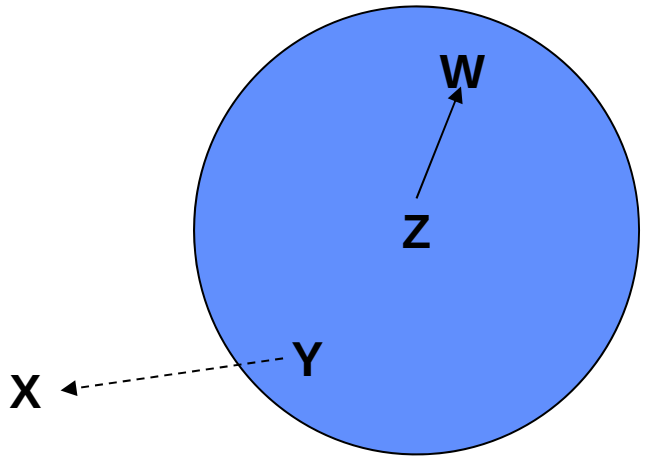
IEEE 802.11 Architecture (cont'd)

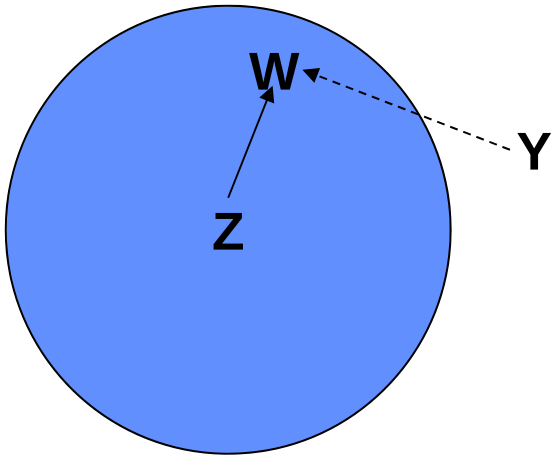
The ad hoc mode, a.k.a. Independent BSS

- No access point.
- Hosts communicate with each other directly.



Exposed & Hidden Terminal Problems





The Exposed Terminal problem

- **Y will not transmit to X even though it can do so**

The Hidden Terminal problem

- **Y finds that medium is free and transmits a packet to W**

IP Address

- Each host “interface” in the Internet has a unique IP address.
- IPv4, 32 bits (4 bytes), written in dotted-decimal notation

  128.238.42.112 means

  10000000 in 1st byte

  11101110 in 2nd byte

  00101010 in 3rd byte

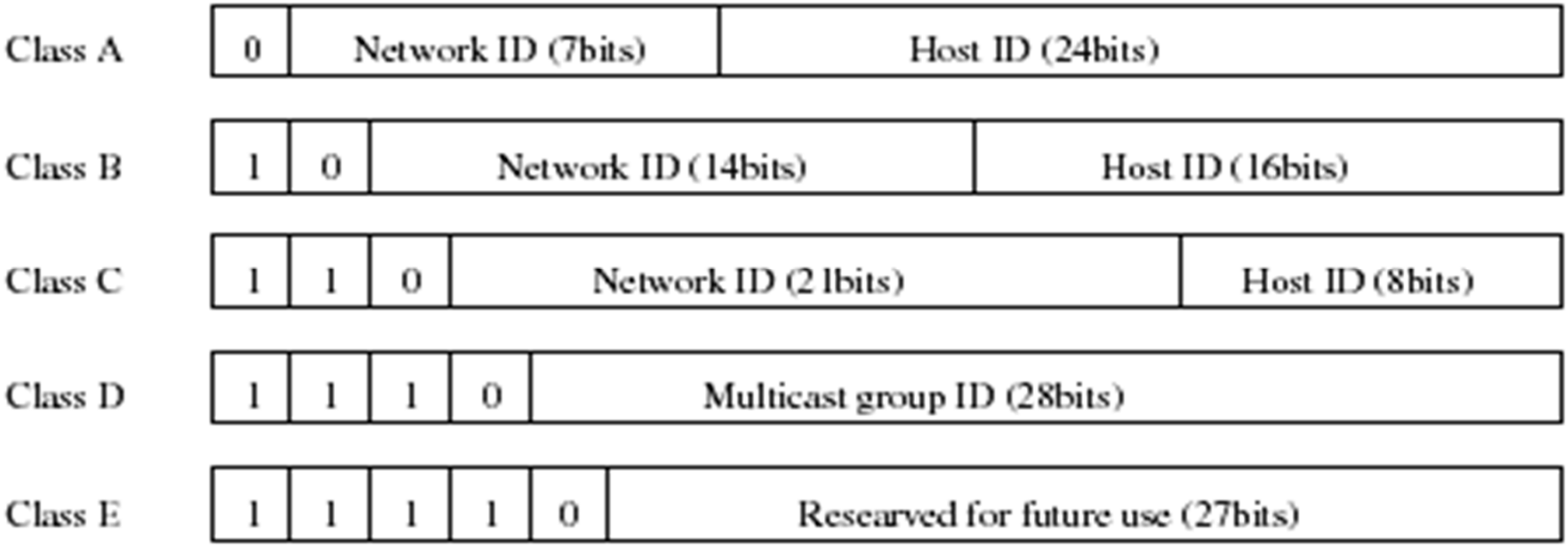
  01110000 in 4th byte

- IPv6, 128-bit address

Five Classes of IP Addresses

Class	From	To
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.255

The end points of each range are not allowed because all zeros and all ones are disallowed for Network ID and Host ID (see later discussion).

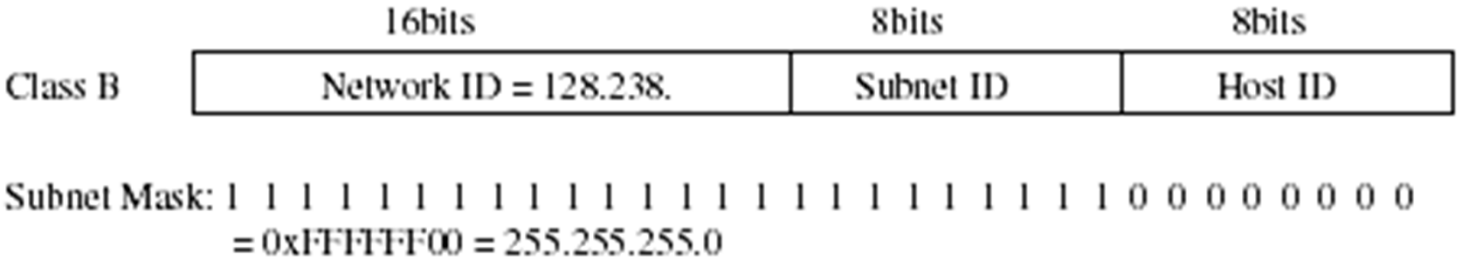


Subnetting

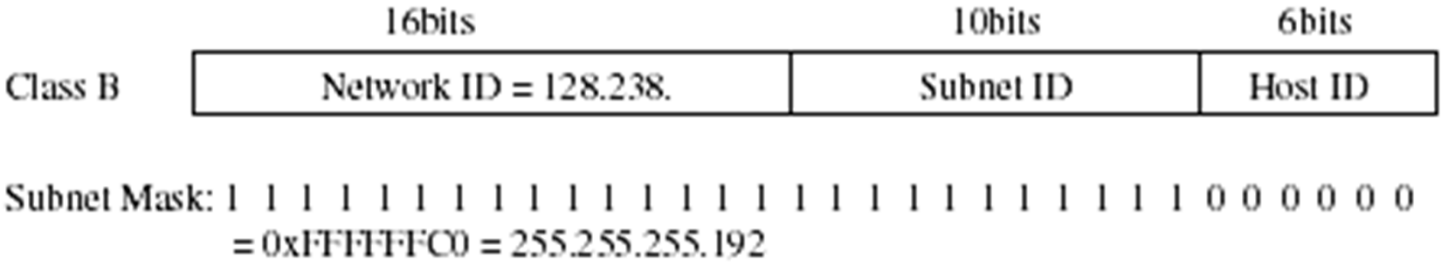
- Use three levels of an IP address:
  - Network ID
  - Subnet ID
  - Host ID
- Subnet mask: separates subnet ID and host ID

Here is another subnetting example with two masks in a design of 640 subnets.

- Use a /24 mask to define 128 subnets, say with subnet address from 128.238.0.0 to 128.238.127.0
- Use a /26 mask to define another 512 subnets, say in this same example with subnet address, from 128.238.128.0 to 128.238.255.192



128.238.0.0/24 net then contains: 2^8 = 256 subnets with 2^8-2 = 254 hosts in each subnet



128.238.0.0/26 net then contains: 2^{10} = 1024 subnets with 2^6-2 = 62 hosts in each subnet

CIDR – Type Address

- IP address in CIDR (Classless Inter-Domain Routing)
  - Not classified into classes
  - Two components of an IP address
    - > Network prefix ranging from 13 to 27 bits – a Variable Length Subnet Mask (VLSM)
    - > Host ID using the remaining bits
  - Slashed-notation

  A dotted-decimal IP address + */* + *Number of bits used for the network prefix*
- Network address are assigned in a hierarchical manner.
- In the core network, routing entries for networks with the same higher level prefix, a CIDR block, can be summarized into one entry – i.e. supernetting for route aggregation
- The longest-prefix-matching rule is still used in table lookups.

Private IP Address

- A Private Network is designed to be used mainly inside an organization
  - Intranet is a private network (LAN) that its access is limited to the users inside the organization
  - Extranet is also a private network (LAN) like the intranet but it allows some users outside the organization to access the network
- Blocks of IP addresses are assigned for private use
- Private IP addressed are not recognized globally
- Private IP addresses are used either in isolation or in connection with Network Address Translation (NAT) technique

Class	NetID	Block
A	10.0.0	1
B	172.16 to 172.31	16
C	192.168.0 to 192.168.255	256

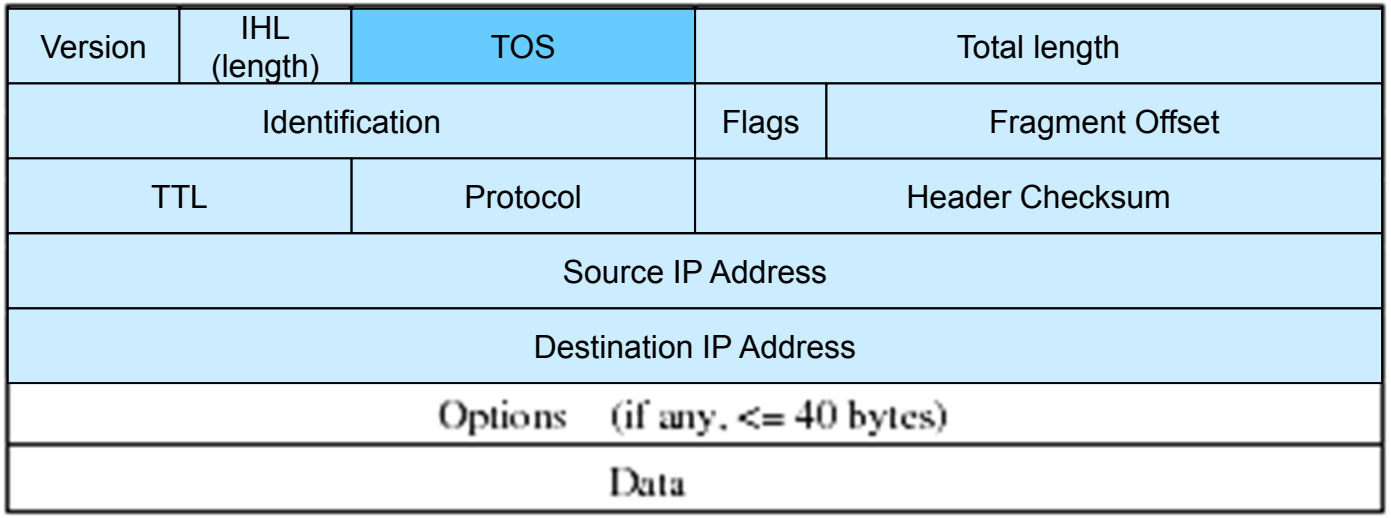
RFC1812 on Special IP Address

Network ID	Host ID	Special Address
Specific	All 0's	Network address
Specific	All 1's (-1)	Direct broadcast address
All 0's	Specific	Specified host on this network
All 0's	All 0's	This host on this network
All 1's (-1)	All 1's (-1)	Limited broadcast address
127	Any	Loopback address

- IP addresses are not permitted to have the value 0 or -1 for the <Host-number> or <Network-prefix> fields except in the special cases listed above. This implies that each of these fields will be at least two bits long.
- Use1's to mean "ALL"
- Use0's to mean "THIS"

IPv4 Header Format … …

- Version: 4 – the currently used IP version.
- 5 32 bit-words (without options) ≤ Header Size ≤ 2^4 * 32 bit-words = 60 bytes
- 20 bytes ≤ Total Length ≤ 2^{16} bytes = 65536 bytes
- Differentiated Services (TOS bits) – for assignment of Precedence, Delay, Throughput and Reliability.
- Time To Live (TTL) - a counter that gradually decrements down to zero, at which point the datagram is discarded.



IP Layer Service

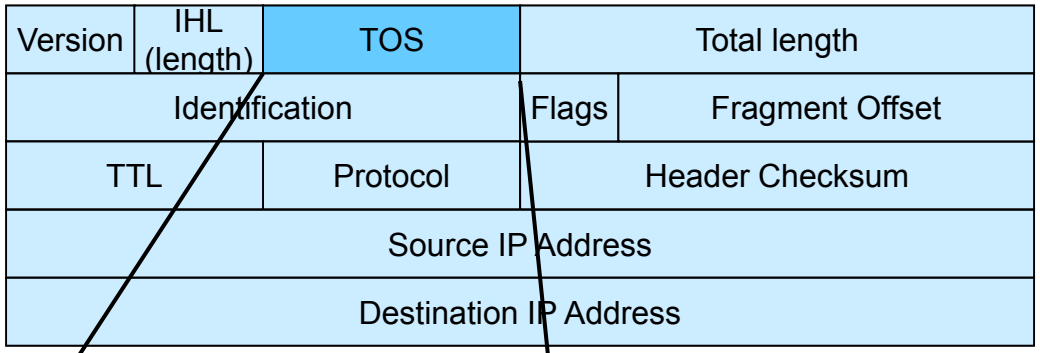
- IP layer provides an unreliable and connectionless service ("datagram service").
  - Unreliable: IP does not guarantee that a transmitted packet will be delivered.
  - Connectionless: Each packet ("datagram") is handled independently. IP is not aware that packets between hosts may be sent in a logical sequence.
- Consequences of an unreliable, connectionless service.
  - Lost Packets
  - Packets are delivered out-of-sequence
  - Duplicated Packets

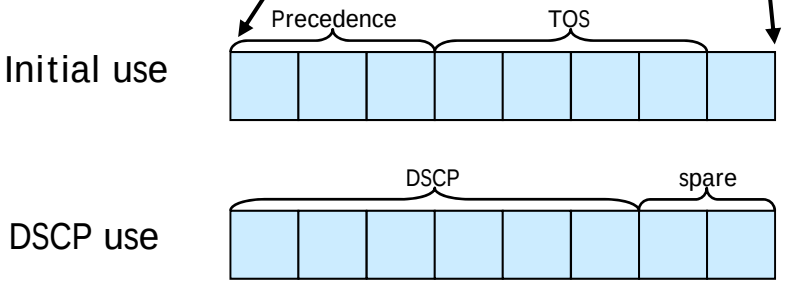
IP Service (cont'd)

- IP offers a Best Effort* service by default;
  i.e., IP does NOT make performance guarantees on:
  - the packet loss rate
  - the time until a packet is delivered
  - the delay variation between selected packets in a flow to support a given application
  - the throughput of traffic between two hosts
- Performance guarantees are also called Quality-of-Service (QoS) guarantees
  - Quality of Expectation (QoE) often refers to the service quality experienced by end users

* "Best effort" may mean different things to different people.

IP Header TOS Field



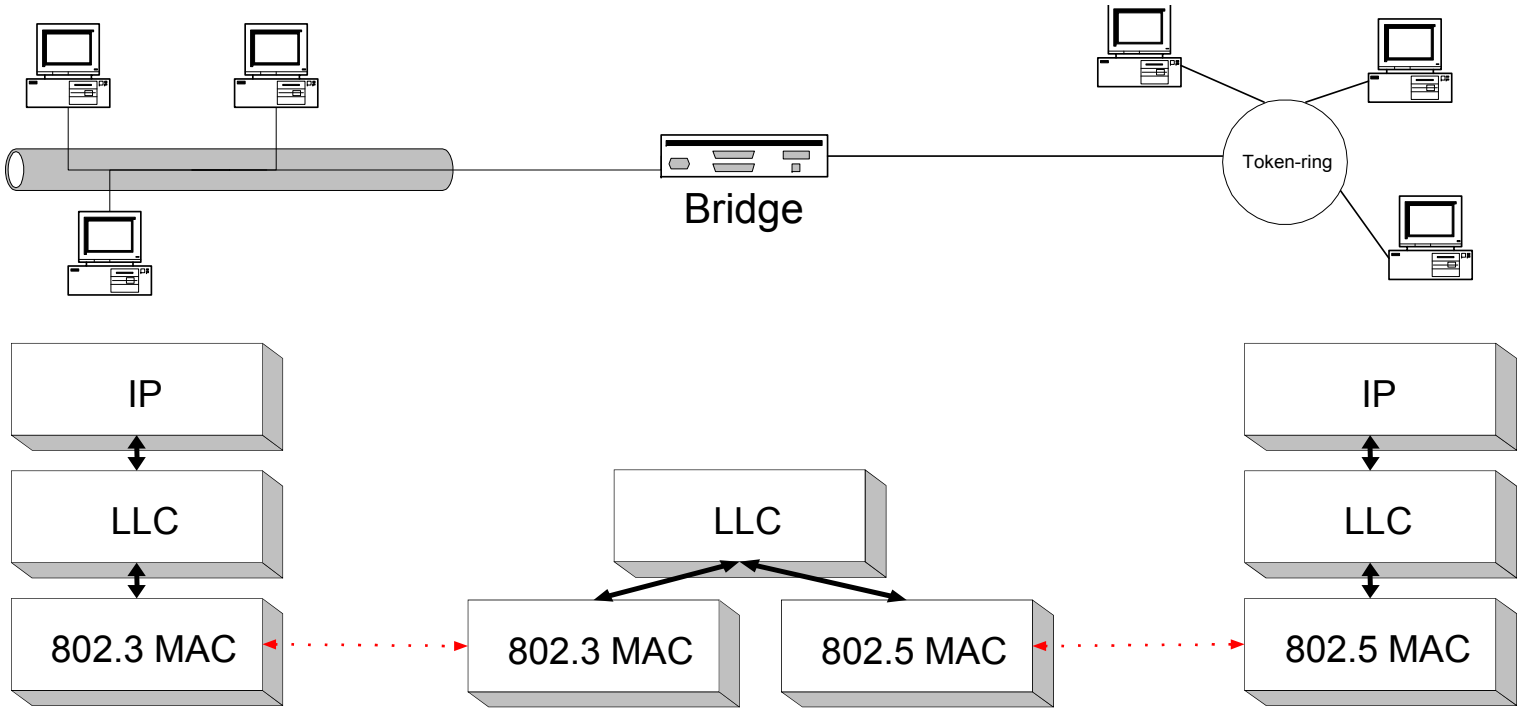


DSCP: Differentiated Services Code Point

DSCP	Precedence	Purpose
0	0	Best effort
8	1	Class 1
16	2	Class 2
24	3	Class 3
32	4	Class 4
40	5	Express forwarding
48	6	Control
56	7	Control

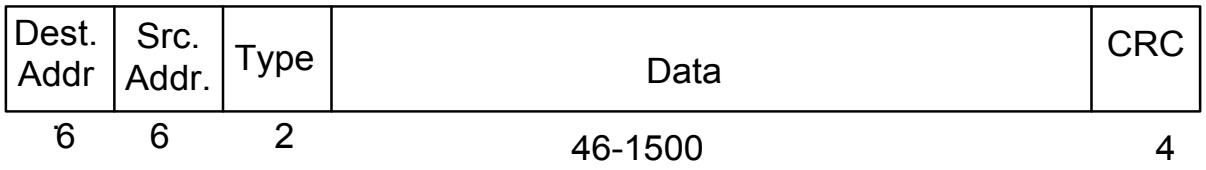
Interconnection of LANs

- LANs can be interconnected by data link bridges.
- Basic functions of a Bridge (simplified):
  - Pass frames to a different LAN if the destination is not on the local LAN.
  - No modification of header, format, and no encapsulation
- A single bridge may connect to more than two LANs



Maximum Transmission Unit

- There is a limit on the data packet size of each data link layer protocol.
- This limit is called Maximum Transmission Unit (MTU).
- MTUs for various data link layers:
  - Ethernet, PPP: 1500 bytes
  - FDDI: 4352 bytes
  - PPP (low delay): 296 bytes
- MTU does not count its own header and trailer bytes of the data link protocol. e.g. Ethernet's MTU is 1500 bytes.

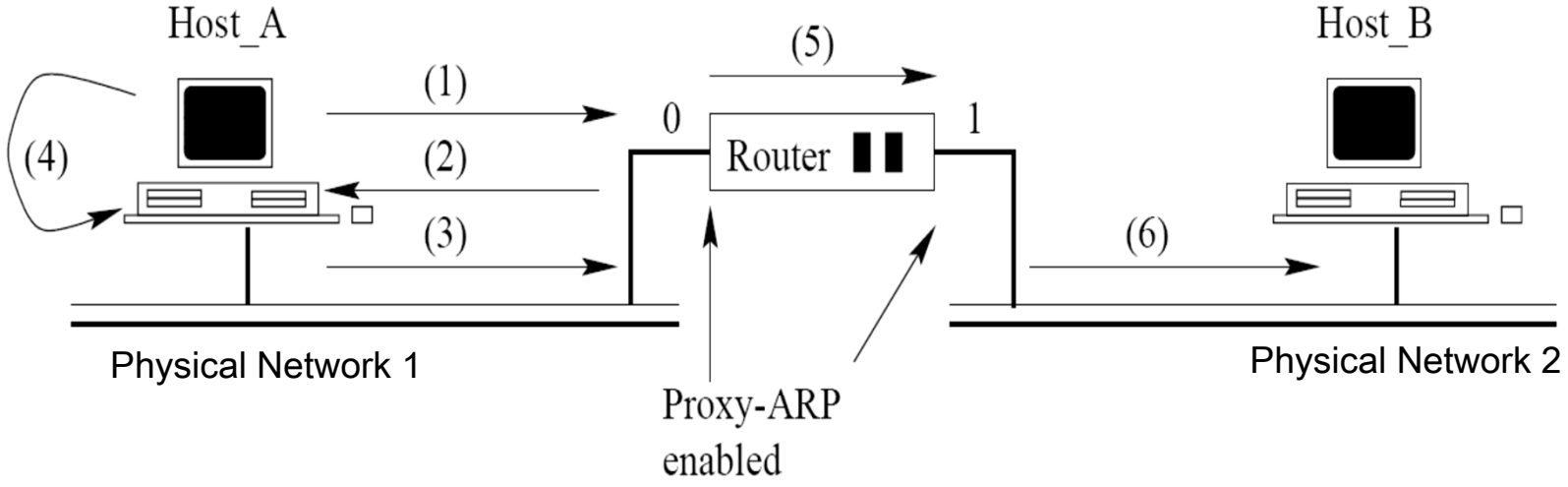


ARP Process

- IP addresses are not recognizable in the interface layer where physical addresses, i.e. MAC addresses, are used.
- When a source host wants to send an IP packet to a destination, it's network interface first *broadcasts* an *ARP request* asking for the MAC address corresponding to the target IP address.
- The target host will return an *ARP reply* in *unicast* with its MAC address.
- Each host maintains an ARP cache containing the recent resolved IP addresses.

Proxy ARP (RFC 1027)

- **Hide the two physical networks from each other.**
- **A router answers ARP requests targeted for a host.**



(1): Host_A sends ARP request for Host_B's MAC

(2): Router Port 0 replies for Host_B

(3): Host_A sends the frame to Router Port 0

(4): Host_A inserts a new entry in its ARP cache: {(Host_B's IP) at (Router Port 0's MAC)}

(5): Router forwards the frame to port 1

(6): Router port 1 sends the frame to Host_B

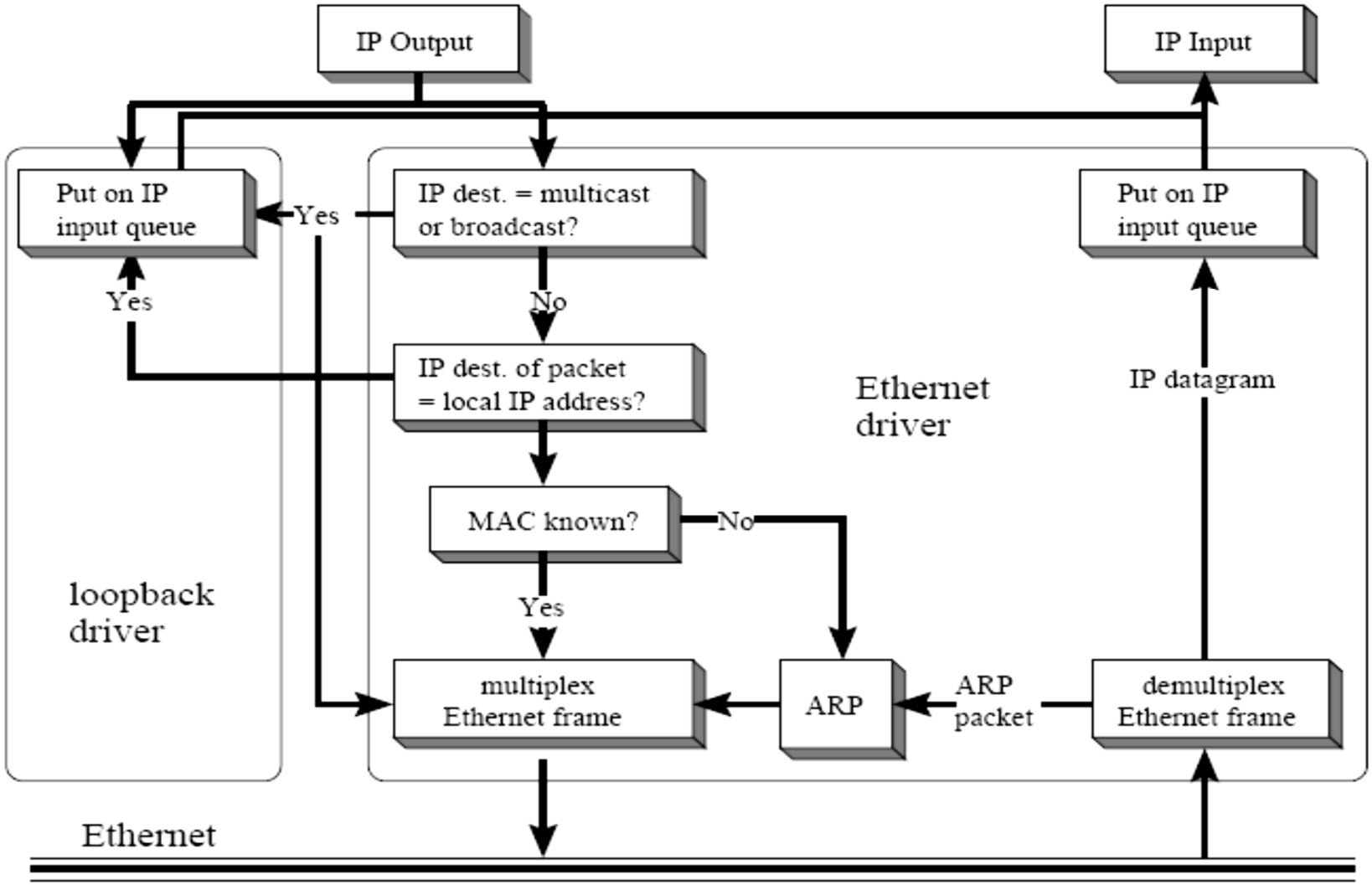
Note

- Two networks are logically in the same subnet (at least from Host A's point of view ...)
- Often used by a router connected with a serial link, ex. PPP to Host B

Gratuitous ARP

- Occurs when a host sends an ARP request resolving its own IP address.
- Usually happens when the interface is configured at bootstrap time.
- The interface uses gratuitous ARP to determine if there are other hosts using the same IP address.
- The sender's IP and MAC address are broadcast, and other hosts will insert this mapping into their ARP tables.

Network Interface Operations

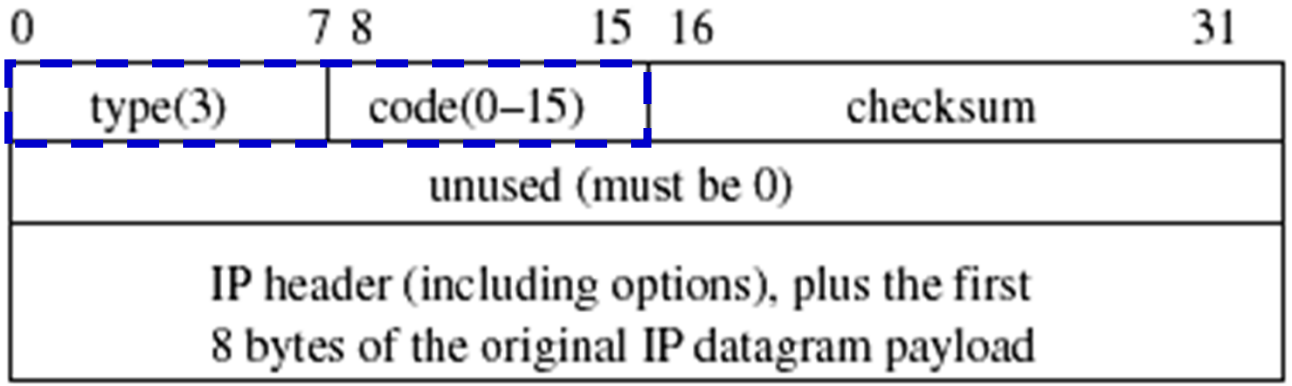


Functional Diagram of an Ethernet Interface Card

Internet Control Message Protocol

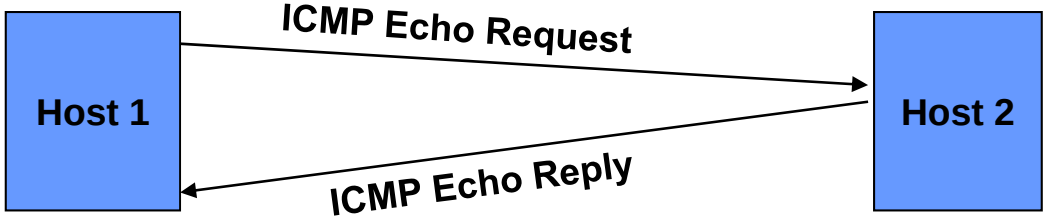
- The Internet Control Message Protocol (ICMP) is the protocol used for error and control messages in Internet.
- ICMP provides an error reporting mechanism of routers to the sources.
- All ICMP packets are encapsulated as IP datagrams (IP protocol type 1)
- The packet format is simple:

  Shown destination unreachable error message



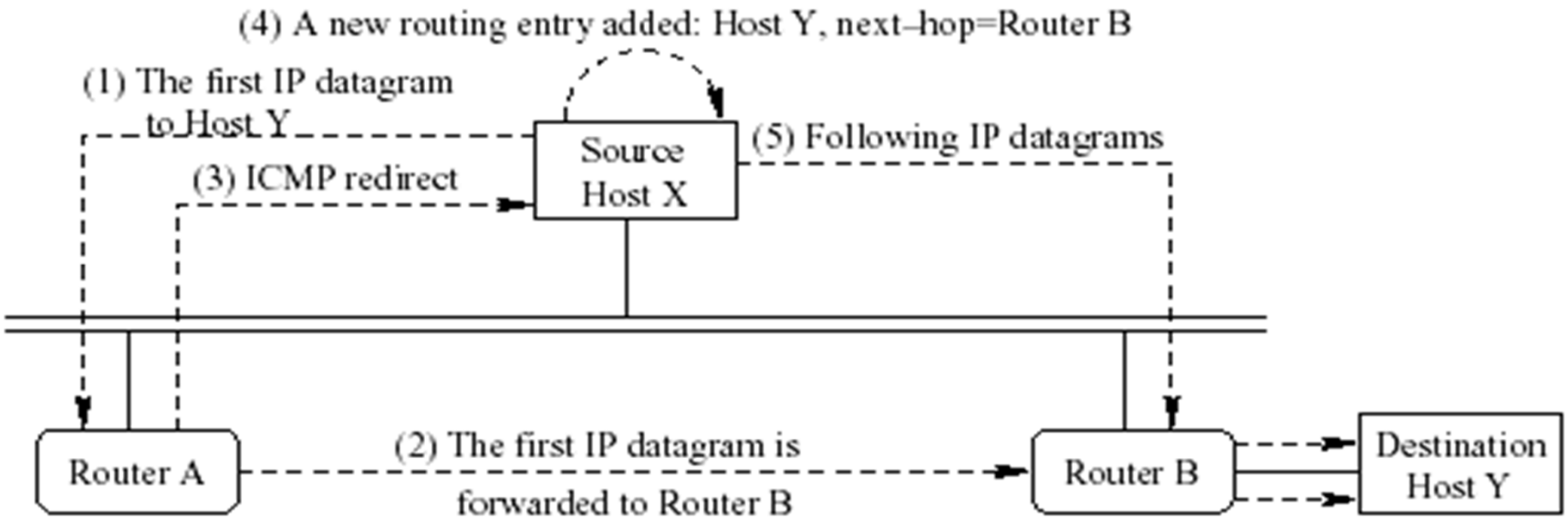
Packet InterNet Gopher (PING)

- **PING is used to verify if a certain host is up and running. It is used extensively for fault isolation in IP networks.**
- **PING is a program that utilizes the ICMP echo request and echo reply messages.**
  - **Each Ping is translated into an ICMP Echo Request.**
  - **The Ping'ed host responds with an ICMP Echo Reply.**



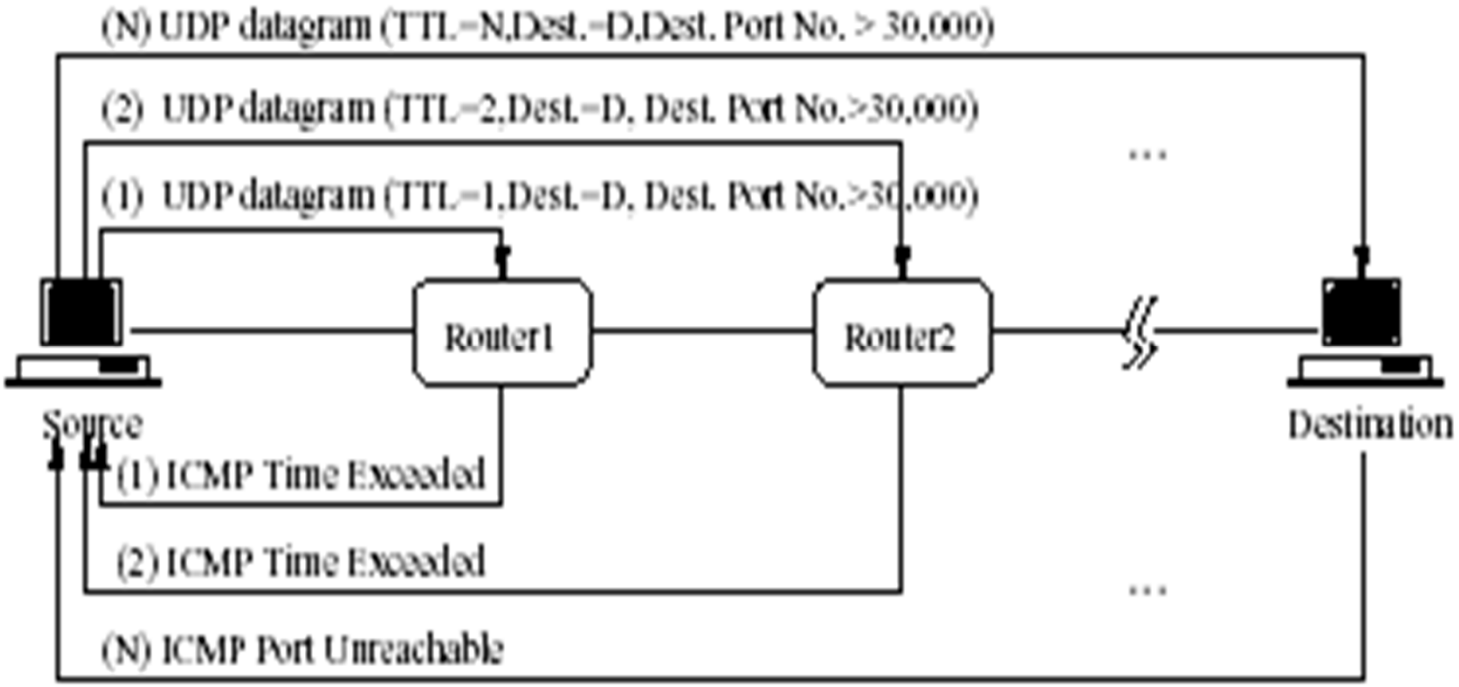
ICMP Redirect Example

- Host X uses Router A as its default router
- Host X sends a datagram destined to Host Y
- Router A looks up it routing table
  - Router B is the next-hop router
  - The datagram is sent out on the same interface it was received on
- Router A sends a ICMP redirect message to Host X
- Host X update the routing entry for Host Y, with a D flag



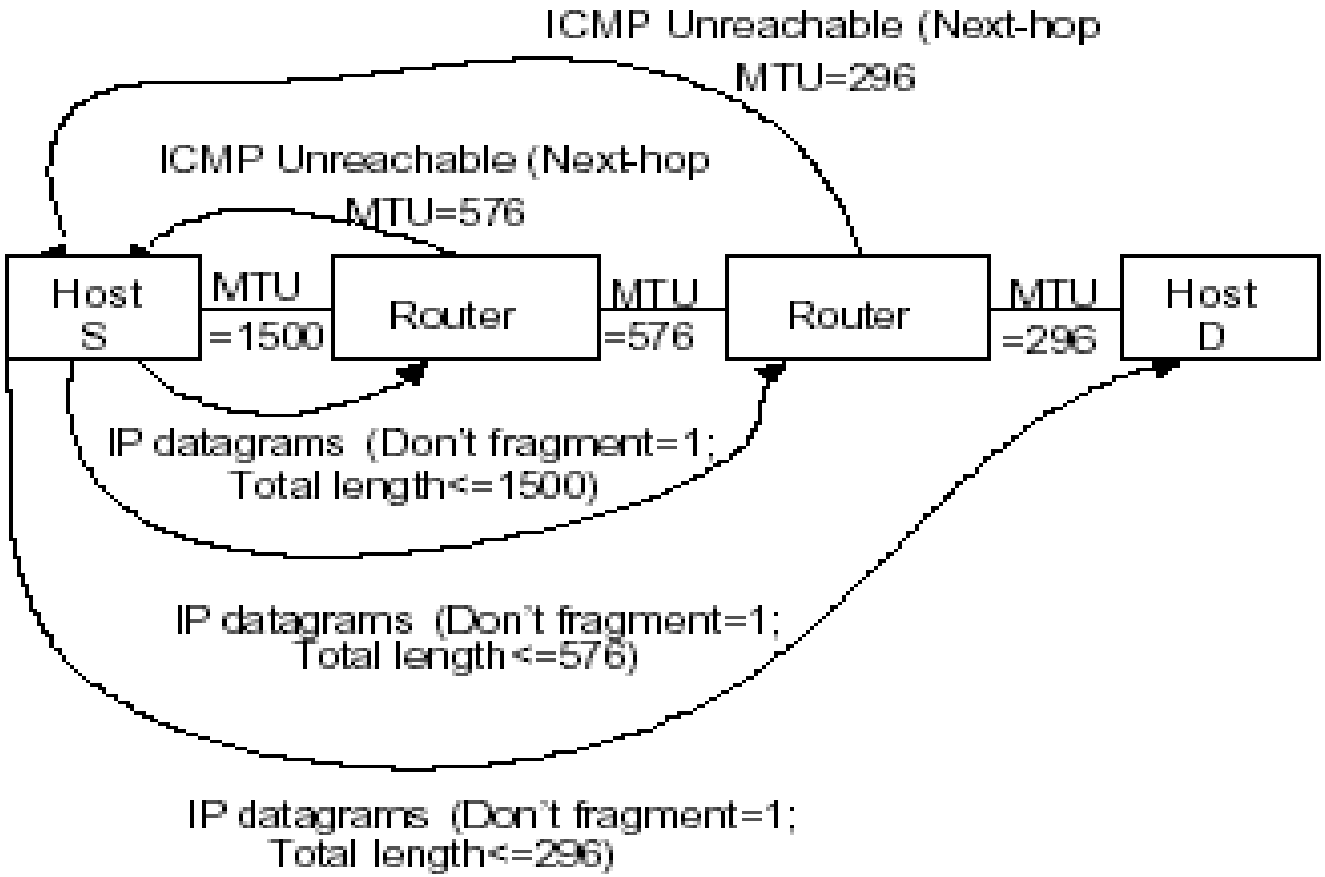
Traceroute

- **Help determine all the routers in an end-to-end path**
- **Use the Time-to-Live (TTL) field in the IP header and the ICMP protocol.**
- **Traceroute operation:**



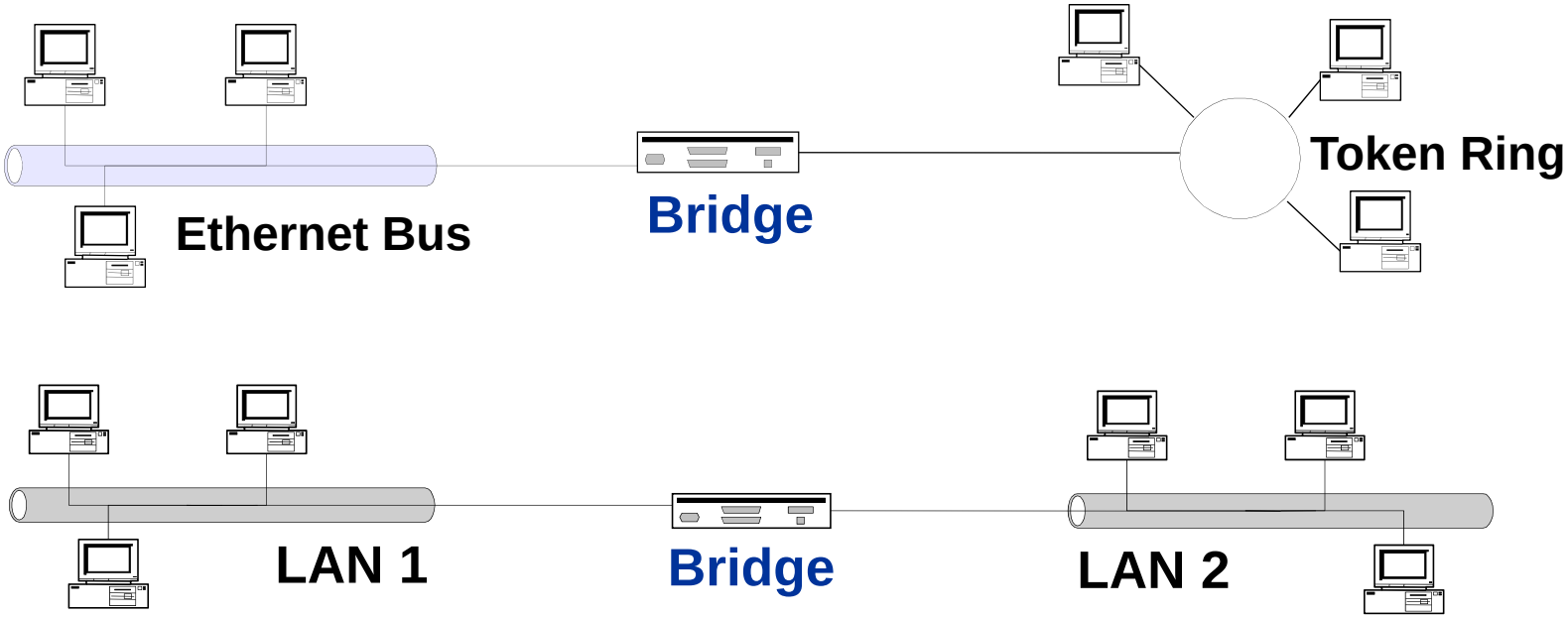
Path MTU Discovery

A host sends a set of IP datagrams with various lengths and the "don't fragment" bit set



Bridges

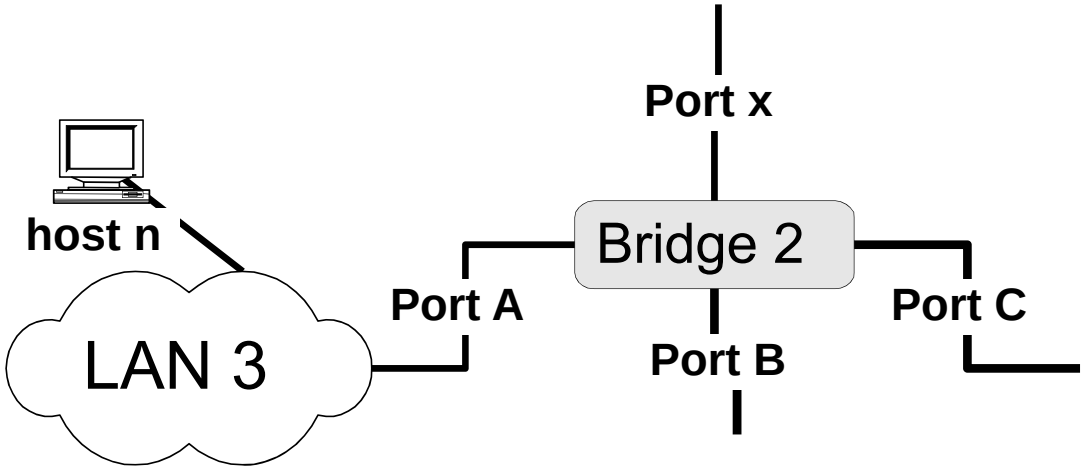
- Interconnect multiple LANs, possibly of different types
- Bridges operate at the Data Link Layer (Layer 2)
- Pass frames to a different LAN if the destination is not on the local LAN.



Bridge MAC Address Learning

Algorithm:

- For each frame received, the bridge stores the source field in the filtering database together with the port where the frame was received.
- All entries are deleted after some time (default is 300 seconds).



Bridge Operations

- A bridge makes forwarding decisions by filtering database lookups.
  - If an entry is found, the bridge forwards the frame to the network segment indicated by the entry.
  - Otherwise, Flooding is used. The frame is copied to all active ports except the incoming port.

Frame Forwarding Conditions

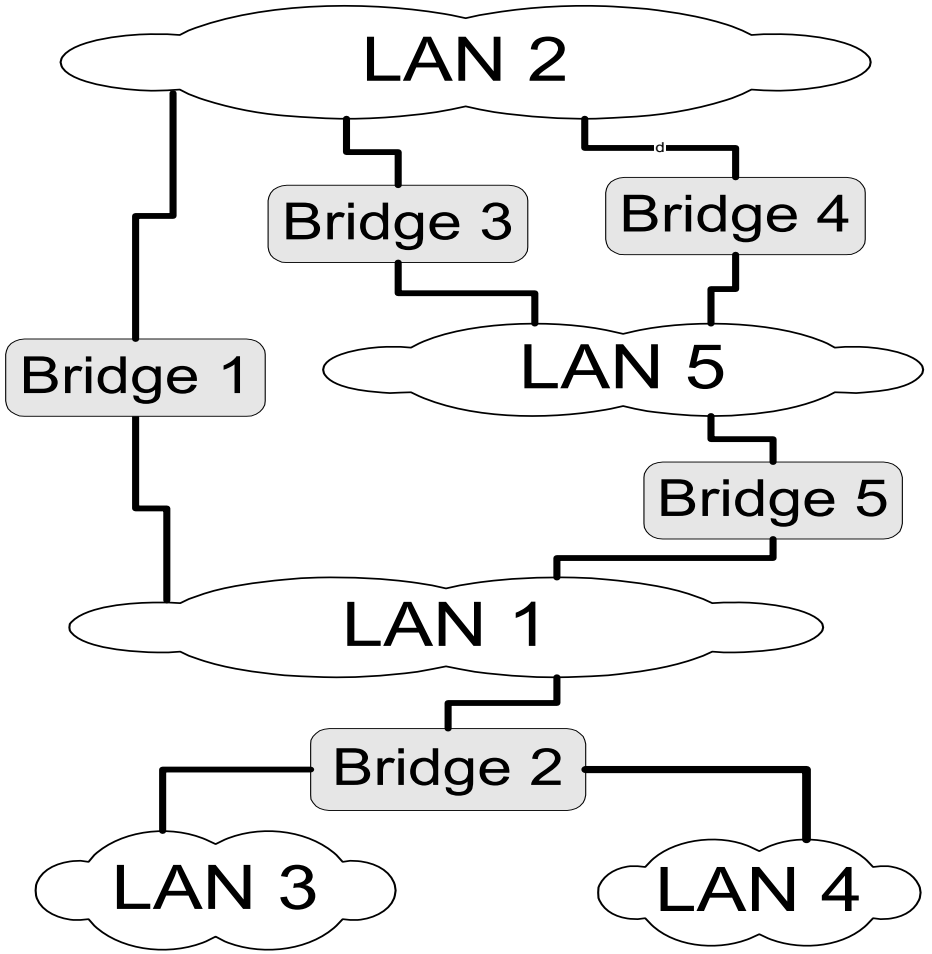
A MAC frame can be forwarded within a bridge from a receiving port to a transmitting port if and only if

- The receiving port is in a Forwarding State,
- The transmitting port is in a forwarding state,
- Either the Filtering Database indicates the port number for the destination MAC address or no such entry is present (in which case all ports are eligible transmission ports), or the values of the source and destination MAC addresses are the same and the bridge is configured to not filter such frames, and
- The maximum service data unit (MTU) size supported by the LAN to which the transmitting port is connected is not exceeded.

Need for Bridge Forwarding

What do bridges do if some LANs are reachable only in multiple hops ?

What do bridges do if the path between two LANs is not unique ?

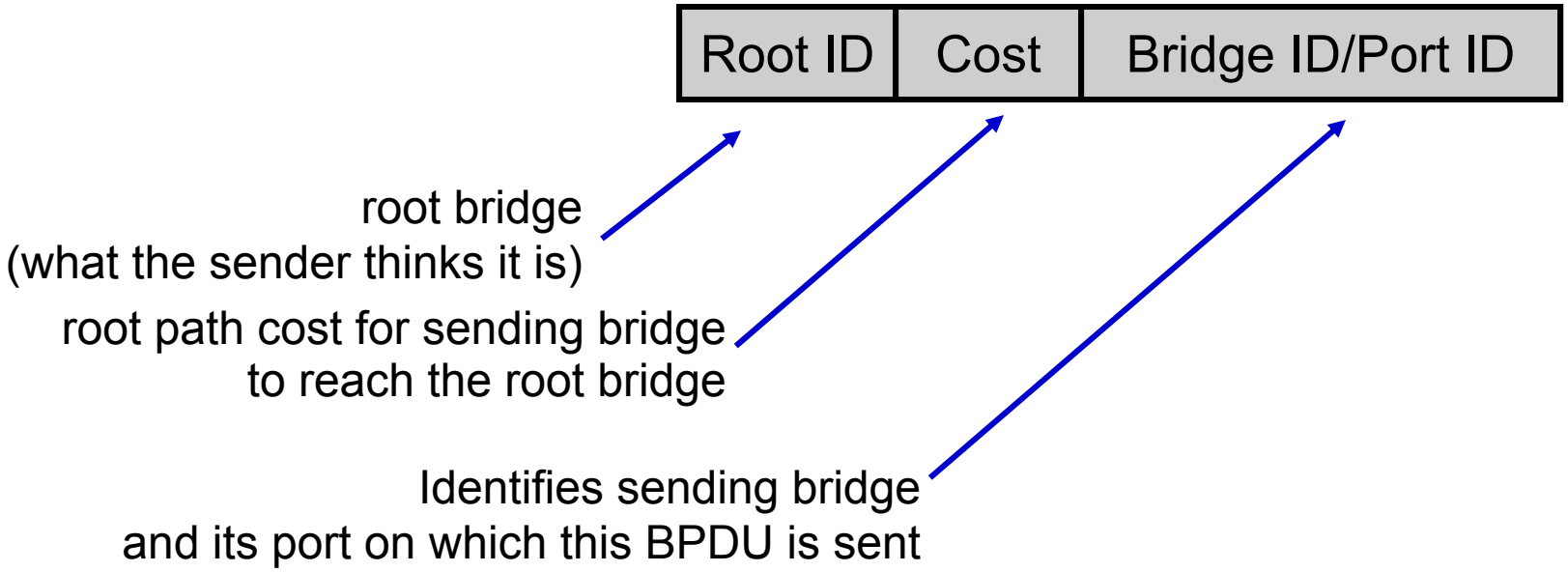


Spanning Trees

- The solution to the loop problem is to not have loops in the topology
- IEEE 802.1 has an algorithm (Spanning Tree Protocol – STP) that builds and maintains a spanning tree in a dynamic environment.
- Bridges exchange messages (Bridge Protocol Data Units, BPDUs) to configure the bridge and build the tree.

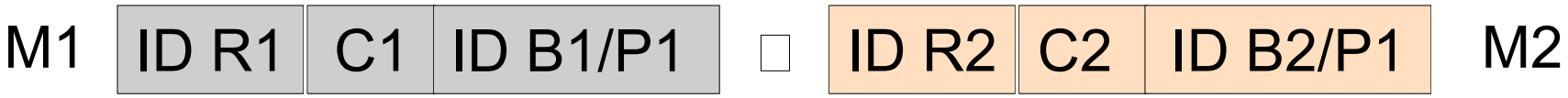
Short Form Notation for BPDUs

- Each bridge sends out BPDUs
  - With Bridge Group Address starting like 01:80:C2:00:00:00
  - Containing the following information:



Ordering of BPDU Messages

We can order BPDU messages with the following ordering relation "□":



If (R1 < R2)

M1 □ M2

elseif ((R1 == R2) and (C1 < C2))

M1 □ M2

elseif ((R1 == R2) and (C1 == C2) and (B1 < B2))

M1 □ M2

elseif ((R1 == R2) and (C1 == C2) and (B1 == B2) and (P1<P2))

M1 □ M2

How do the bridges determine a spanning tree?

With the help of the BPDUs:

- Bridges can elect a single bridge as the Root Bridge.
- Each bridge can determine:
  - a Root Port, the port that gives the best path to the root.
  - and the corresponding Root Path Cost
- Each bridge determines whether it is a Designated Bridge, for the LANs connected to each of its ports. The designated bridge will forward packets towards the root bridge.
- Each bridge selects ports to be included in the Spanning Tree.
  - Root ports and designated ports
- Bridge ports that are in the spanning tree will forward packets (Forwarding State); ports that are not in the spanning tree will not forward packets (Blocking State).

Example: Building Spanning Trees for two VLANs

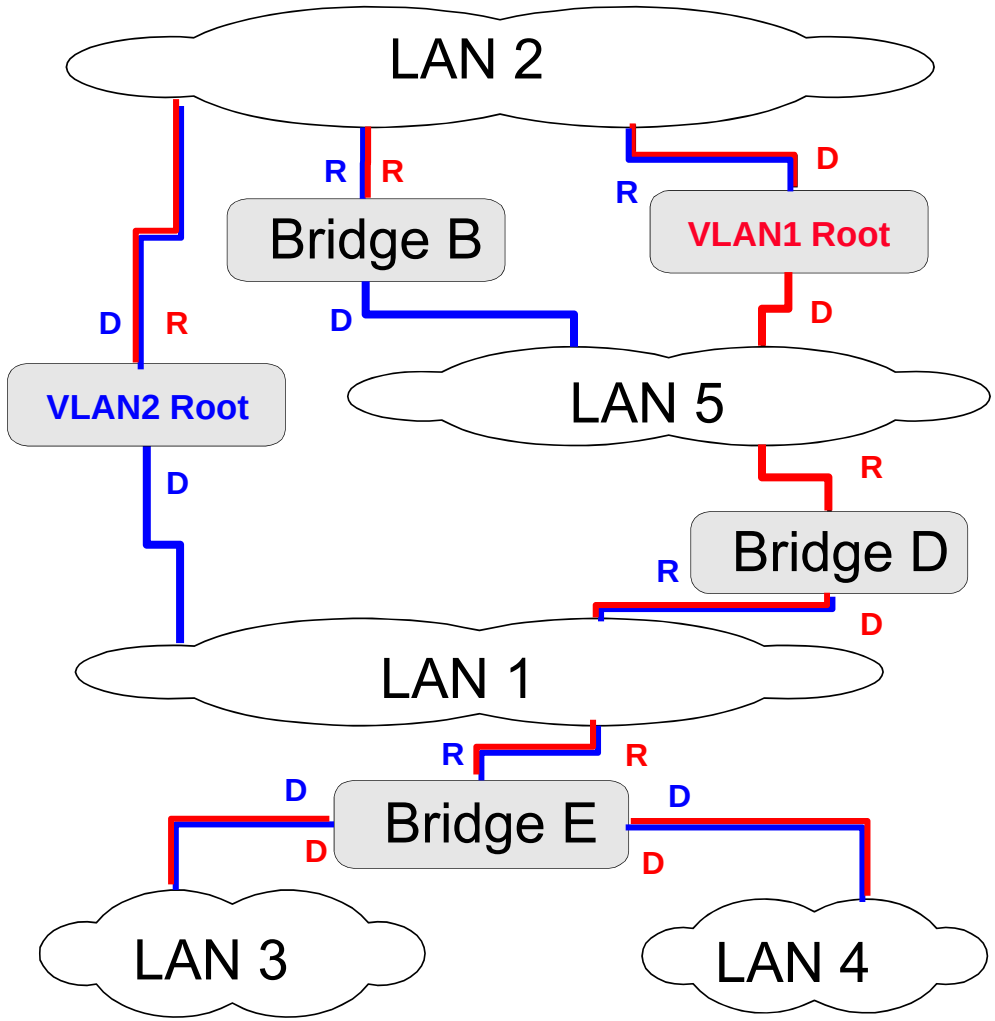
Design two VLANs, VLAN1 and VLAN2 in a bridged network

Each bridge has two distinct Bridge IDs, one for each VLAN

- Configured with different priority levels

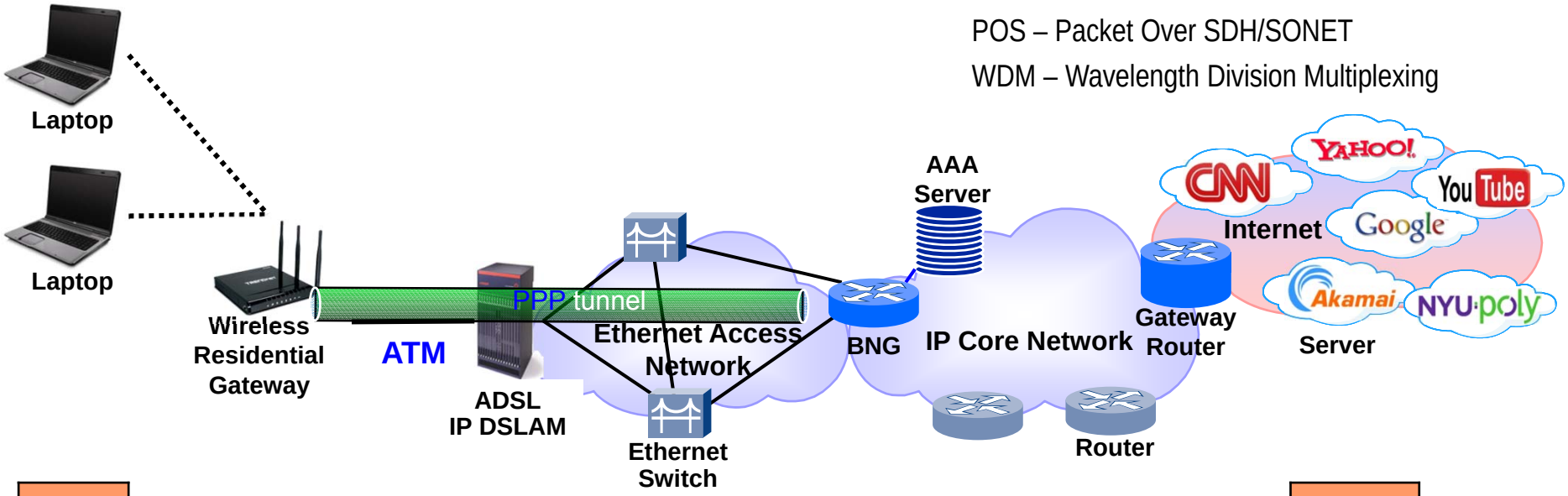
Each bridge port is configured with two port IDs

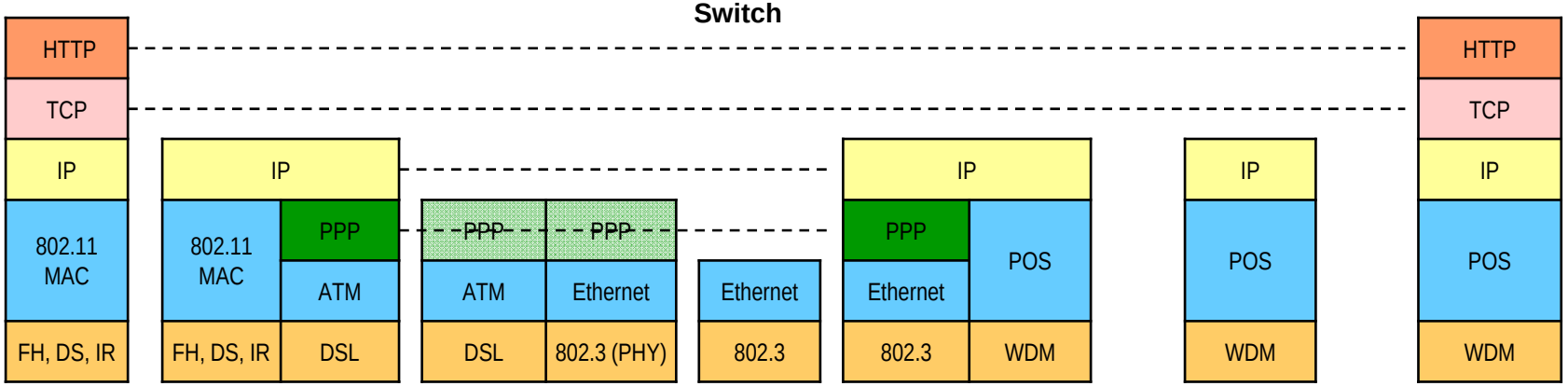
Multiple Spanning Tree Protocol (MSTP) forms two spanning trees, one for each VALN



IP Networking Example – High Speed Internet Web Browsing

AAA – Authentication, Authorization, Accounting
BNG – Broadband Network Gateway
DSL – Digital Subscriber Line
DSLAM – DSL Access Multiplexer
DSSS – Direct Sequencing Spread Spectrum
FHSS – Frequency Hopping Spread Spectrum
IR – Infrared
POS – Packet Over SDH/SONET
WDM – Wavelength Division Multiplexing





Routing

Routing is to transfer packets from a source to a destination using network layer protocol information.

Two activities:

- Determine optimal routing paths
- Transport packets through an internetwork

Routing table

- Records optimal routes.
- Gets consulted when a forwarding decision is to be made.
- Can be set manually, updated by some ICMP messages, or by using dynamic routing protocols.

Next-Hop Routing

- Direct delivery: send datagram directly through Layer 2 (Ethernet, …) when the source and the destination are on the same (sub)network.
- Indirect delivery: when the source and the destination are NOT on the same network
  - Need to send datagram through a router.
  - Consult the routing table to determine the next hop router.
  - Only ONE hop on the path is listed in the routing table.

Routing Table Lookup

To route each IP packet, the destination IP address is first extracted and then

- The network prefix gets calculated to determine whether the network prefix matches any directly connected network address so the packet can be delivered directly.
- If not direct delivery, a routing table lookup takes place in the following order named as the Longest-prefix-matching rule
  - Find matching host address
  - Find matching network address
  - Find default entry
- To keep the routing table small, network-specific entries and default router are often used

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
128.238.4.0	0.0.0.0	255.255.255.0	U	40	0	0	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	40	0	0	lo
0.0.0.0	128.238.4.4	0.0.0.0	UG	40	0	0	eth0

Routing Algorithm Overview

Distance Vector

- Each node knows the distance (="cost") to its directly connected neighbors.
- Each node sends its neighbors a list of the current distances to all nodes in network.
- If all nodes eventually update their distances (including to those not directly connected), the routing tables get converged.

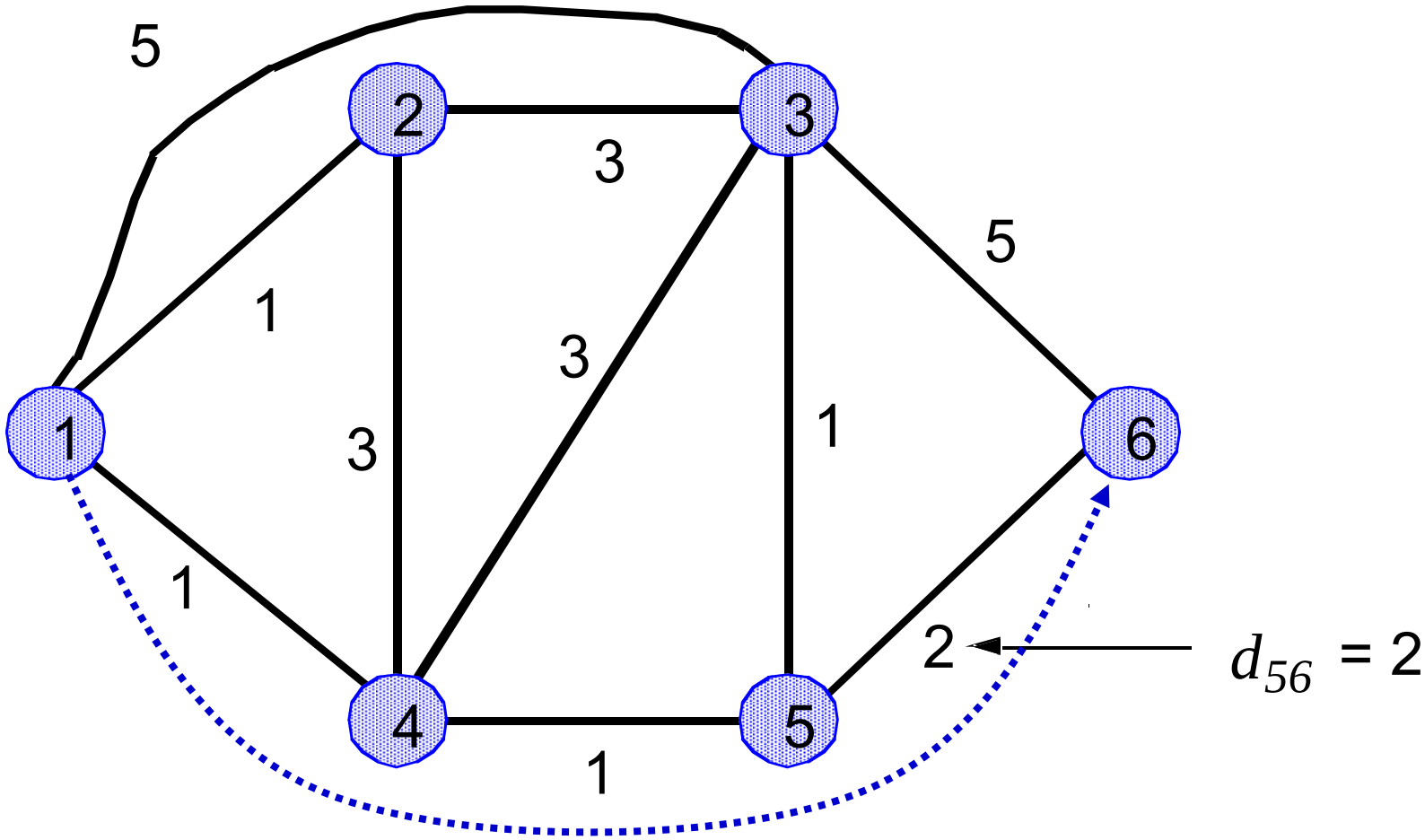
Link State

- Each node broadcasts distance information (i.e. link state) to ALL other nodes in the network
- All nodes in the same network have an identical database for the status of all links.
- Each router calculates the shortest path to all other destinations independently

Distance Vector

- Each node maintains two tables:
  - Distance Table: Cost to each node via each outgoing link.
  - Routing Table: Minimum cost to each node and next hop node.
- Nodes exchange messages that contain information on the cost of a route
- Reception of messages triggers recalculation of routing table

Example



How does node 1 find the optimal path to node 6?

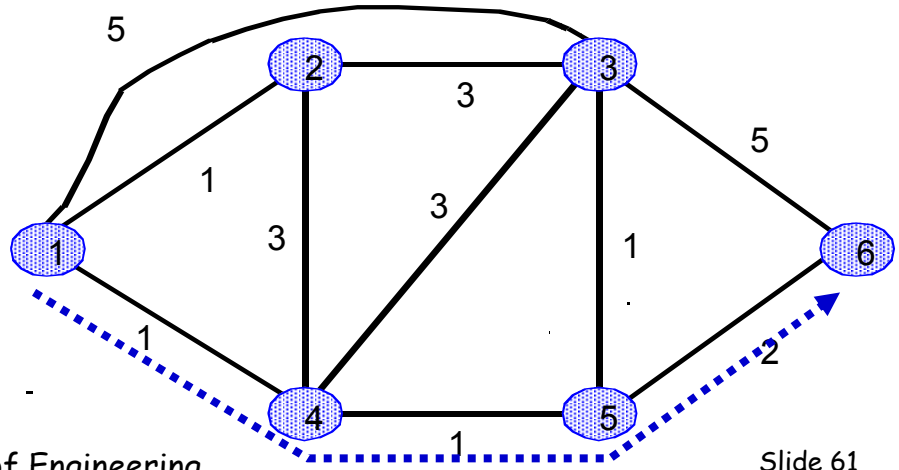
Distance Vector Solution Example

Show how the entries at node 1 change for node 6:

Time	Messages received about the dist. to node 6	Distance via			Routing	
		2	3	4	via	Cost
T = 0	**No message received. Node 1 is not aware of Node 6.**					
T = 1	**Node 3 says the dist. is 5. Node 2 and 4 are not aware of Node 6.**	∞	**10**	∞	**3**	**10**
T = 2	**Node 2 says the dist. is 8; Node 3 and 4 both say the dist. is 3.**	**9**	**8**	**4**	**4**	**4**
T = 3	**Node 2 says the dist. is 6; Node 3 and 4 say the dist. is 3**	**7**	**8**	**4**	**4**	**4**
T = 4	**Node 2 says the dist. is 5; no change in the messages from Node 3 and 4**	**6**	**8**	**4**	**4**	**4**

A routing table can be formed at node 1:

Destination	Next Hop	Cost
2	2	1
3	4	3
4	4	1
5	4	2
6	4	4



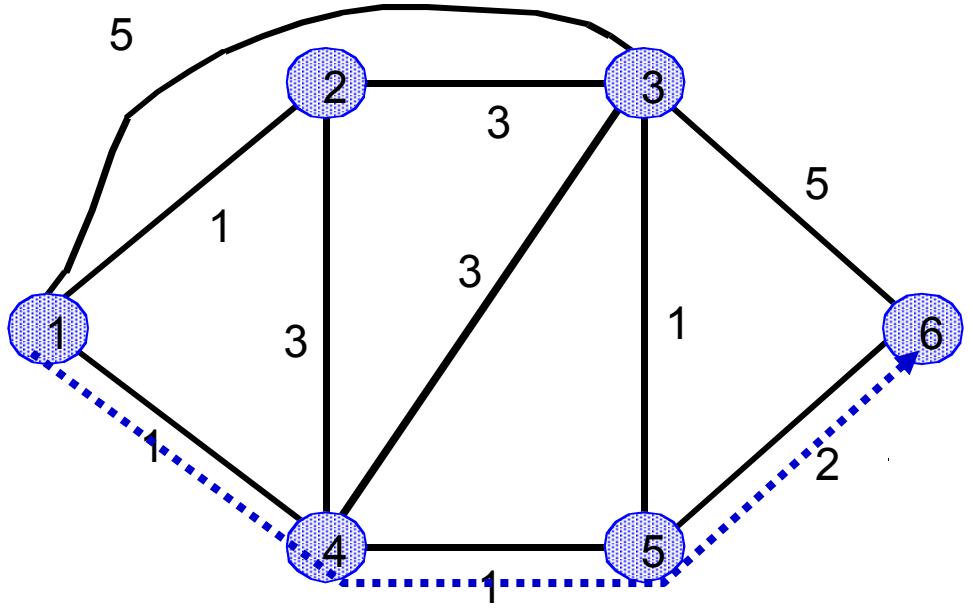
Link State Routing Algorithm

- Use a routing protocol to collect the whole network topology
- Obtain destination reachability information as well as link weights/states
- Compute shortest paths using Dijkstra's algorithm from a node to all other nodes
- Construct routing tables that show the destination addresses and the next hop addresses
- Note that while Dijkstra's algorithm gives you end-to-end routes, the routing tables may only store the next hop address.

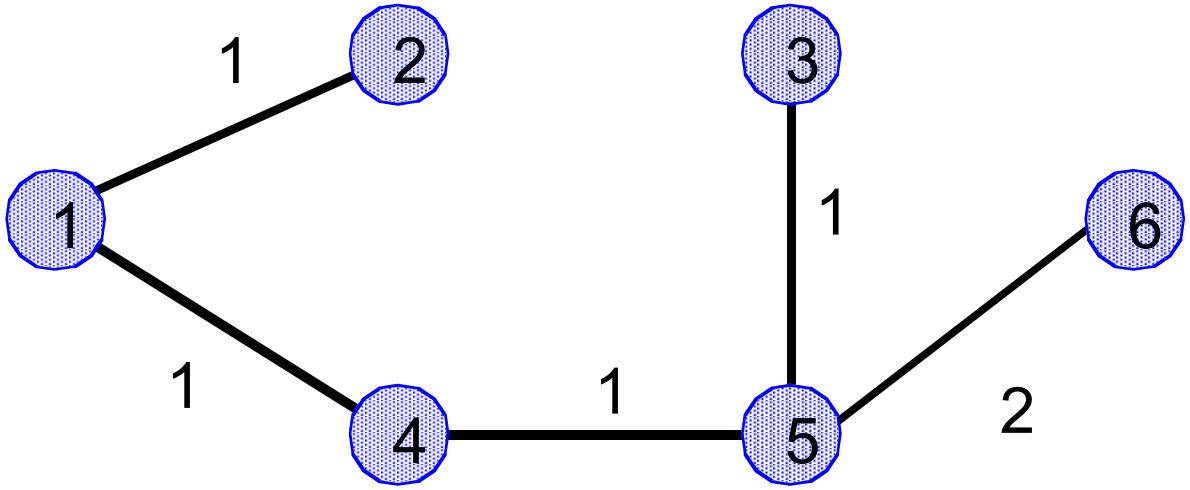
Example (at node 1)

Dijkstra's algorithm

	M	D1	D2	D3	D4	D5	D6
0	{1}	0	1	5	1	∞	∞
1	{1, 2}	0	1	4	1	∞	∞
2	{1, 2, 4}	0	1	4	1	2	∞
3	{1,2, 4, 5}	0	1	3	1	2	4
4	{1,2, 4, 5, 3}	0	1	3	1	2	4



Resulting Routing Tree (at node 1)



The tree is translated into a routing table at node 1:

Destination	Next Hop
2	2
3	4
4	4
5	4
6	4

Distance Vector Routing vs. Link State Routing

- Both work well in most circumstances
- Link state routing
  - Each node requires complete topology information.
  - Link state information must be flooded to all nodes.
  - Convergence is guaranteed and faster.
  - Less prone to routing loops.
- Distance vector routing
  - Requires less resources
  - Less cost to implement and support
  - Some datagrams may experience looping if routing tables get change while a packet is being transmitted

IP Packet Forwarding from Source to Destination

- Find out the IP address by DNS query for a given domain name of the destination
- If the destination is
  - in the same network (or subnet), send the packet directly to the destination
  - in a different network, a router is needed to forward the datagram
    - > If no router available, drop the packet
- IP packets have to be encapsulated in a link layer frame (e.g., Ethernet frame)
  - A link layer frame can only be sent within the same network (or subnet)
  - The link layer frame has to be sent with the MAC address of the other end
    - > ARP

Communications in the Same Network/Subnet

What is "the Same Network/Subnet"?

- Host X wants to send IP packets to host Y
- What does the X know
  - X's IP address
  - X's subnet mask
  - Y's IP address
- Computation by X
  - X's network/subnet ID: (X's IP add) & (X's subnet mask)
  - Y's network/subnet ID: (Y's IP add) & (X's subnet mask)
  - If the above two results are the same, X believes that Y is in the same network/subnet
- If X and Y have different subnet masks, they may have different calculation results
  - Each calculates network/subnet ID by using its own subnet mask

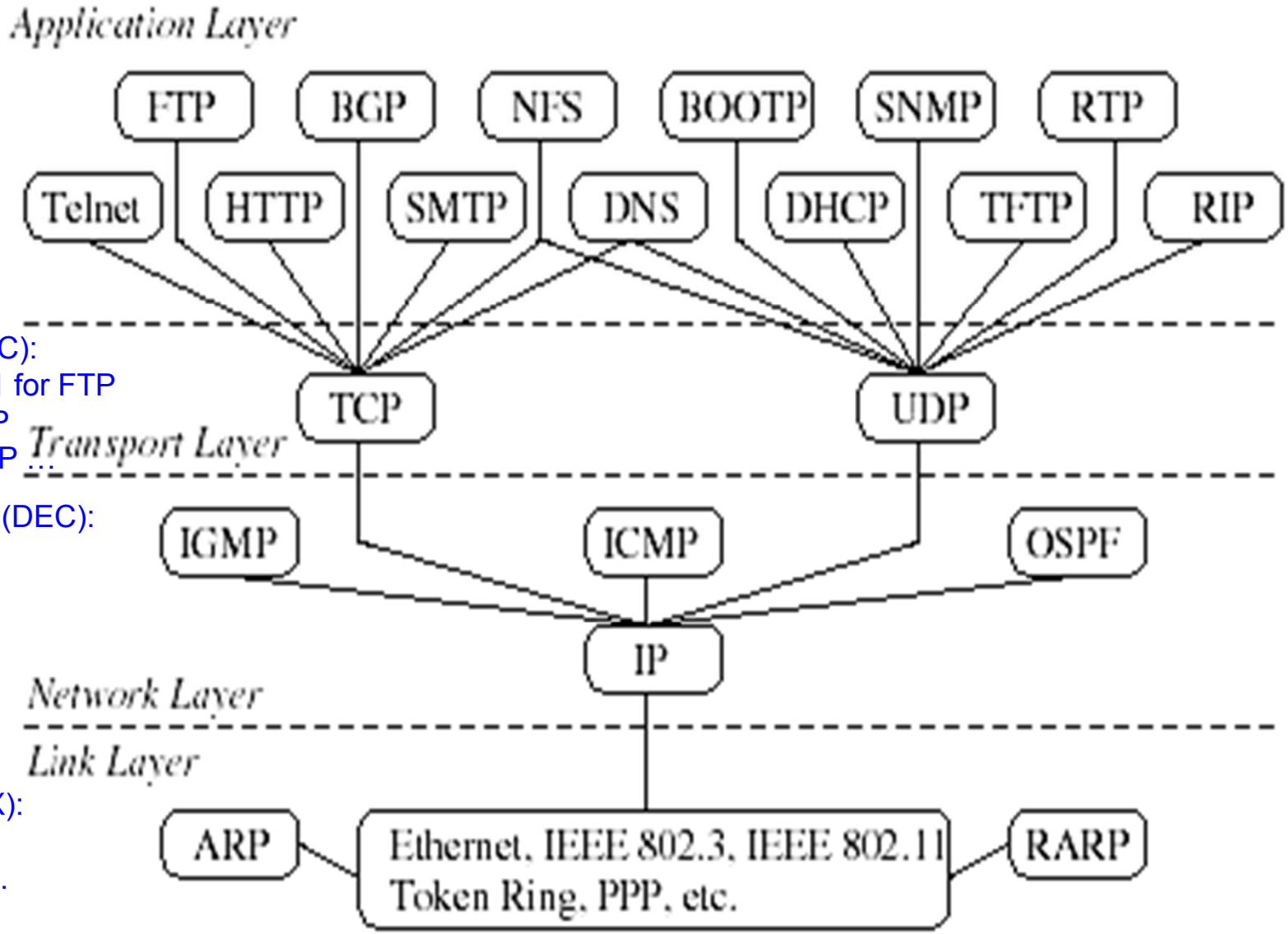
Communications between Two Network Segments (in the Same Network)

- Two segments connected by a bridge, host X in segment 1 and host Y in segment 2
- Assume that at the beginning,
  - the ARP tables of X and Y are empty
  - the bridge has correct entries for X and Y in its filtering database
- X tries to send an IP packet to Y
  - X broadcasts an ARP request to resolve Y's MAC address
  - The bridge forwards the ARP request to segment 2
  - Y sends an ARP reply destined to X
  - The bridge forwards the ARP reply to segment 1
  - X sends out an Ethernet frame containing the IP packet
  - The bridge forward the frame to segment 2 for Y
- In each packet, what are the values in the following fields?
  - IP: source IP address, destination IP address
  - ARP: sender IP address, target IP address
  - Ethernet for ARP: source Ethernet address, destination Ethernet address
  - Ethernet for IP: source Ethernet address, destination Ethernet address

Communications between Two Networks

- Two networks connected by a router, host X in network 1 and host Y in network 2
- Assume that at the beginning,
  - the ARP tables of X, Y and the router are empty
  - the router has entries for X and Y in its routing table
- X tries to send an IP packet to Y
  - X broadcast an ARP request (in network 1) to resolve the router's MAC
  - The router sends an ARP reply to X
  - X sends the IP packet to the router
  - The router broadcasts an ARP request (in network 2) to resolve Y's MAC
  - Y sends an ARP reply to the router
  - The router forwards the IP packet to Y
- A router NEVER forwards an ARP message. (Why?)
- In each packet, (how many?) what is the value in the following fields?
  - Source/sender IP address, Destination/target IP address
  - Source/sender Ethernet address, destination/target Ethernet address

Protocols in Different Layers



Port Number (DEC):
- TCP/20, TCP/21 for FTP
- UDP/520 for RIP
- TCP/80 for HTTP …

Protocol Number (DEC):
- 1 for ICMP
- 2 for IGMP
- 6 for TCP
- 17 for UDP
- 47 for GRE
- 89 for OSFP …

Frame Type (HEX):
- 08:00 for IP
- 08:06 for ARP …