Local Area Network

Dr. Farid Farahmand

Revised on: 10/6/12

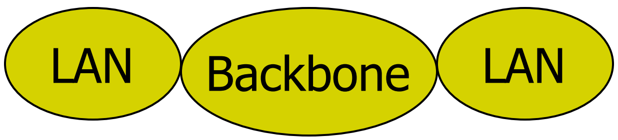
Data Network Areas

- WAN (Wide Area Networks)
- MAN (Metropolitan Area Networks)
- LAN (Local Area Networks)
  - Sharing resources in small but geographically dispersed network

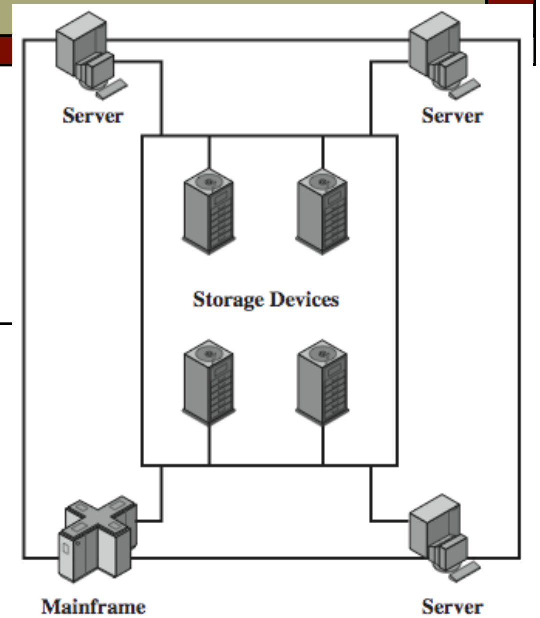
Name	Expansion	Description
LAN	Local Area Network	Least expensive; spans a single room or a single building
MAN	Metropolitan Area Network	Medium expense; spans a major city or a metroplex
WAN	Wide Area Network	Most expensive; spans sites in multiple cities

LAN Applications

- personal computer LANs
  - low cost
  - limited data rate
  - share resources
    - printers, hard drives, etc.
  - Potential issues for a single LAN
    - reliability
    - capacity
    - cost
- High-speed office networks
  - used particularly for desktop image processing
    - a single page with 200 pictures elements (black and white) is about 3 Mbits!
  - high capacity local storage
- backend networks
  - interconnecting large systems (mainframes and large storage devices)
    - high data rate
    - high speed interface
    - distributed access
    - limited distance
    - limited number of devices
- backbone LANs
  - interconnect low-speed LANs
  - Resolve typical drawbacks to LANs



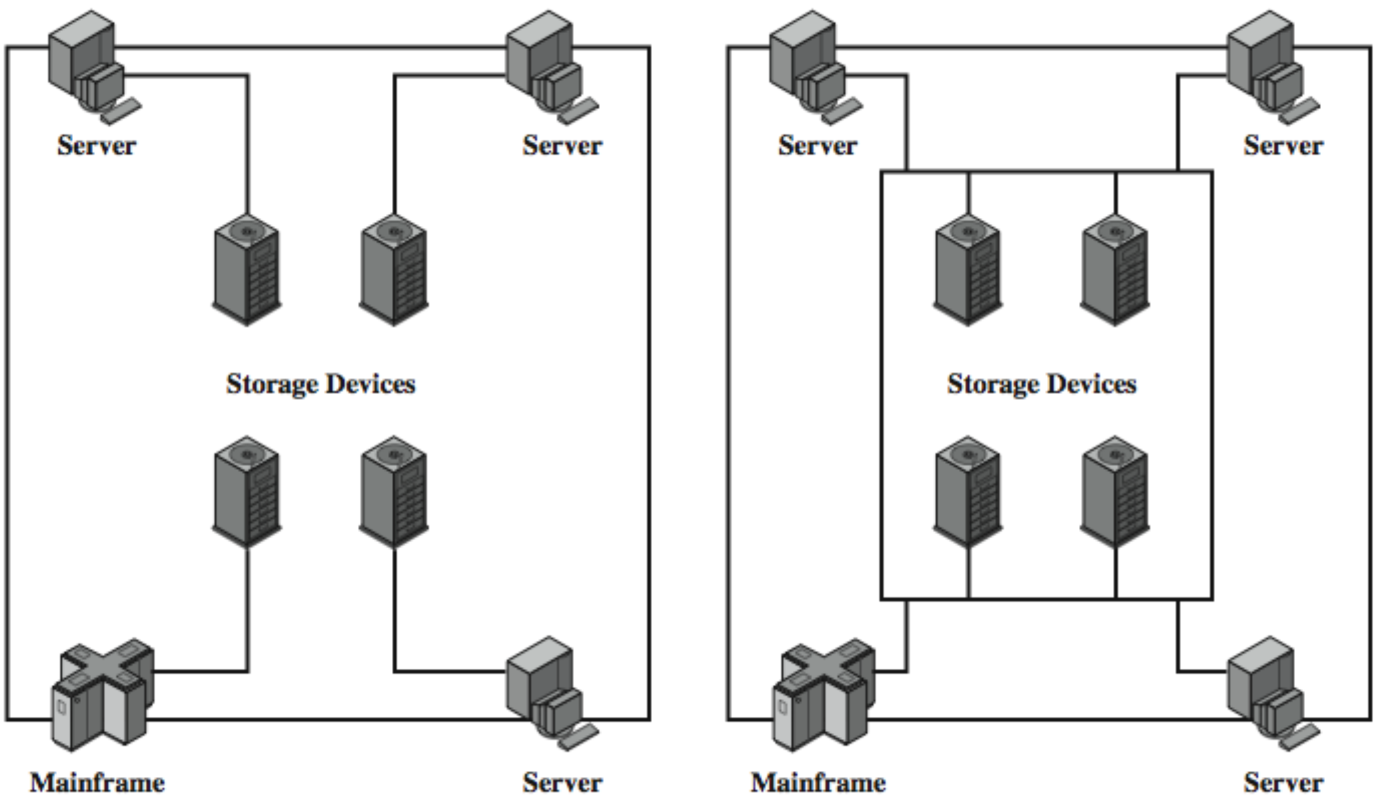
LAN Applications



- storage area networks (SANs)
  - separate network to handle storage needs
    - → shared storage
  - detaches storage tasks from specific servers
  - shared storage facility
    - eg. hard disks, tape libraries, CD arrays
  - accessed using a high-speed network
    - eg. Fibre Channel
  - improved client-server storage access
  - direct storage-to-storage communication for backup

Project: Build a SAN!

Storage Area Networks

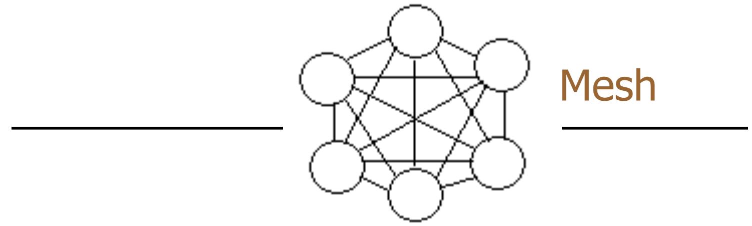


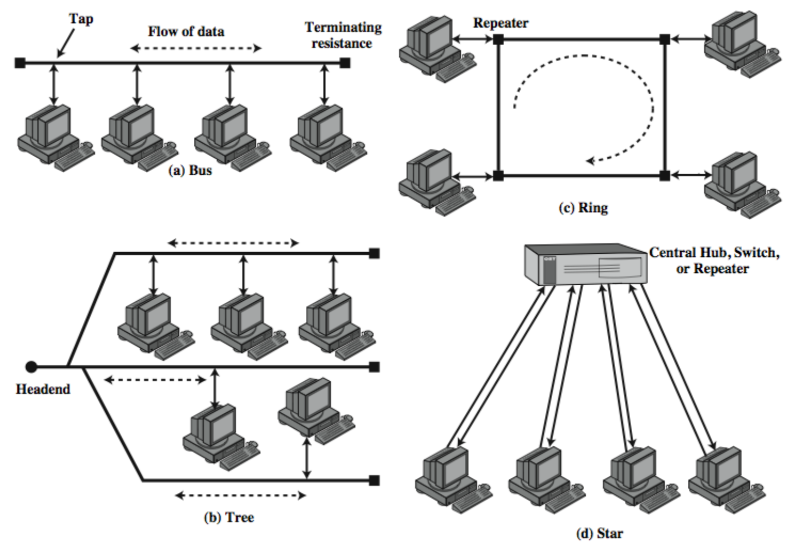
(a) Server-based storage

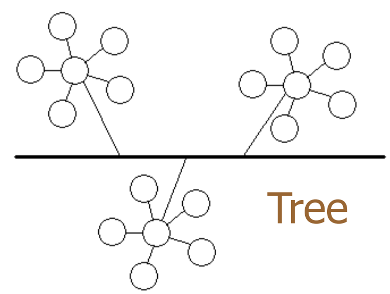
(b) Storage area network

LAN Topologies

- **Mesh Topology**
  - Devices are connected with many redundant interconnections between network nodes.
  - In a full mesh topology every node has a connection to every other node in the network.
- **Star Topology**
  - All devices are connected to a central switch/hub/repeater. Nodes communicate across the network by passing data through the switch/hub
  - Typically has unidirectional links
- **Bus Topology**
  - All devices are connected to a central cable, called the bus or backbone.
  - The bus is often terminated on both ends if not connected to any devices.
  - The bus is typically duplex.
- **Ring Topology**
  - All devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it.
  - Closed loop with unidirectional links (links are point-to-point)
- **Tree Topology**
  - A hybrid topology. Groups of star-configured networks are connected to a linear bus backbone.

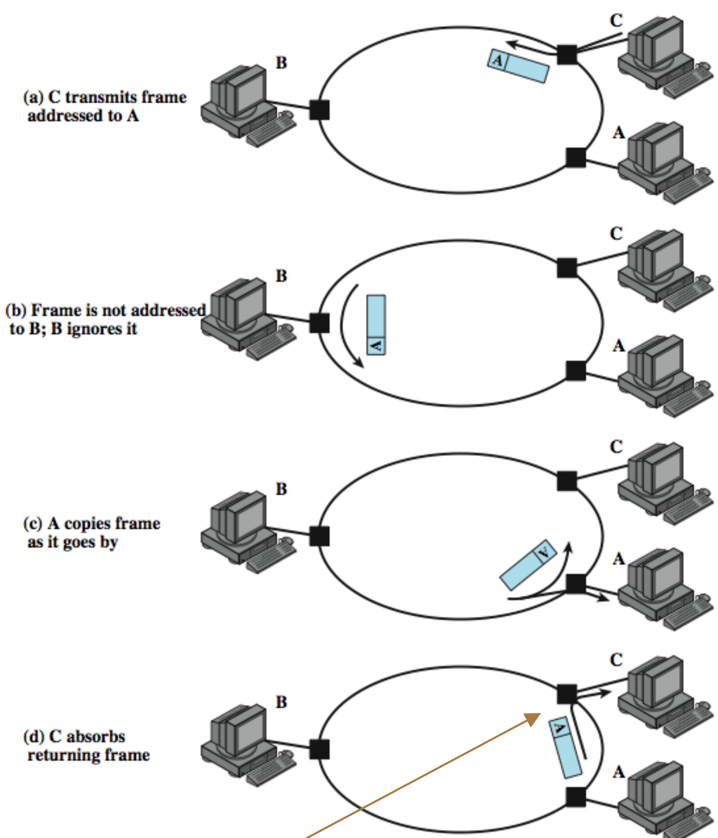




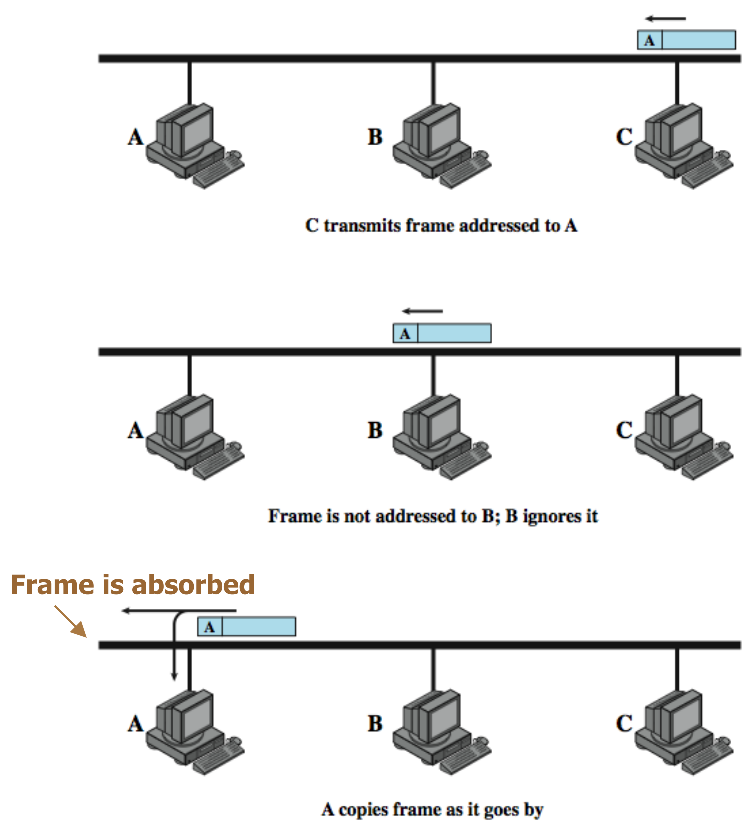


http://www.webopedia.com/quick_ref/topologies.asp

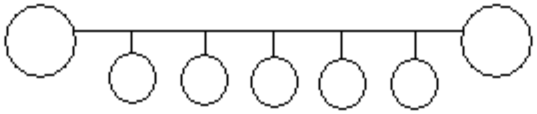
Frame Transmission



Frame is removed when it returns to Its source

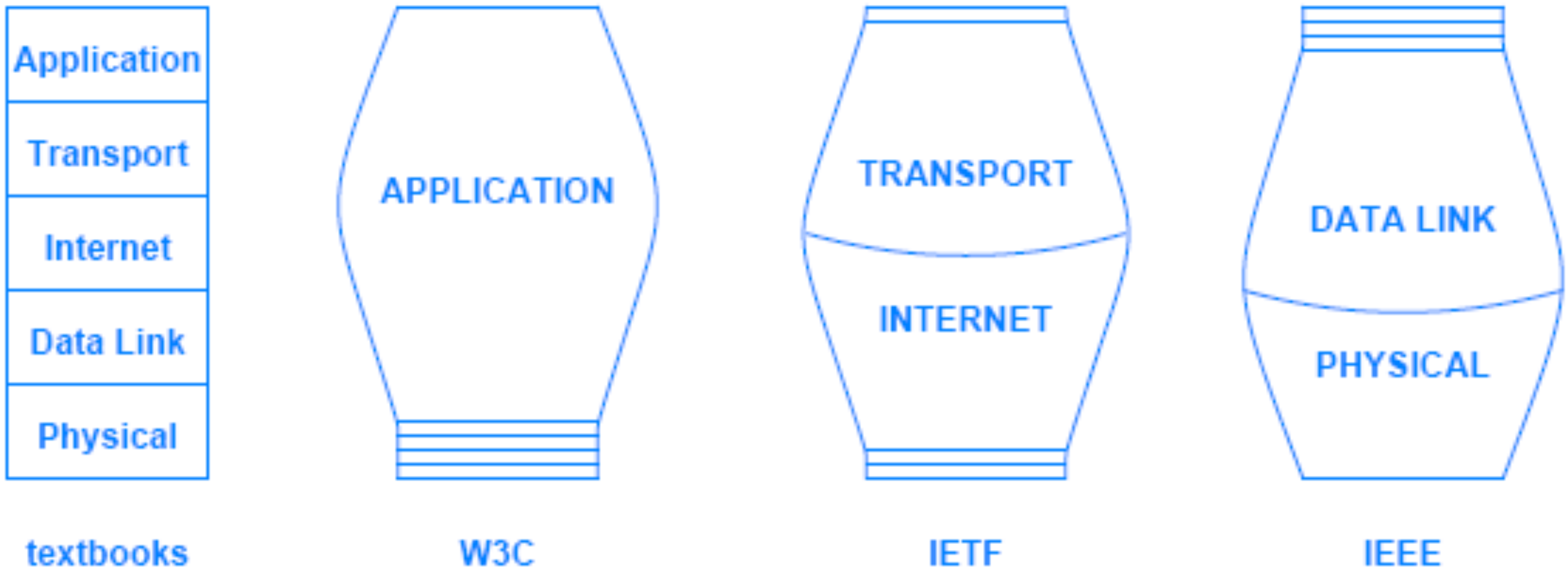


Ethernet – General



- Most common LAN technology allowing multiple devices to connect to each other and share resources
- Developed by Xerox in 1970
- Also known as IEEE 802.3
  - IEEE 802.3 Energy Efficient Ethernet Study Group
- Each standards organization focuses on particular layers of the protocol stack
  - Institute for Electrical and Electronic Engineers (IEEE)
  - World Wide Web Consortium (W3C)
  - Internet Engineering Task Force (IETF)

Various Standard Emphasis



- Institute for Electrical and Electronic Engineers (IEEE)
- World Wide Web Consortium (W3C)
- Internet Engineering Task Force (IETF)

Other Standardization Bodies

- Institute of Electrical and Electronics Engineers (IEEE)
- The European Computer Manufacturers Association (ECMA)
- The International Electrotechnical Commission (IEC)
- The International Organization for Standardization (ISO).

IEEE 802 Model and Standards

- IEEE divides Layer 2 of the protocol stack into two conceptual sub-layers
  - The Logical Link Control (LLC)
    - sublayer specifies addressing and the use of addresses for demultiplexing as described later in the chapter
  - The Media Access Control (MAC)
    - sublayer specifies how multiple computers share underlying medium

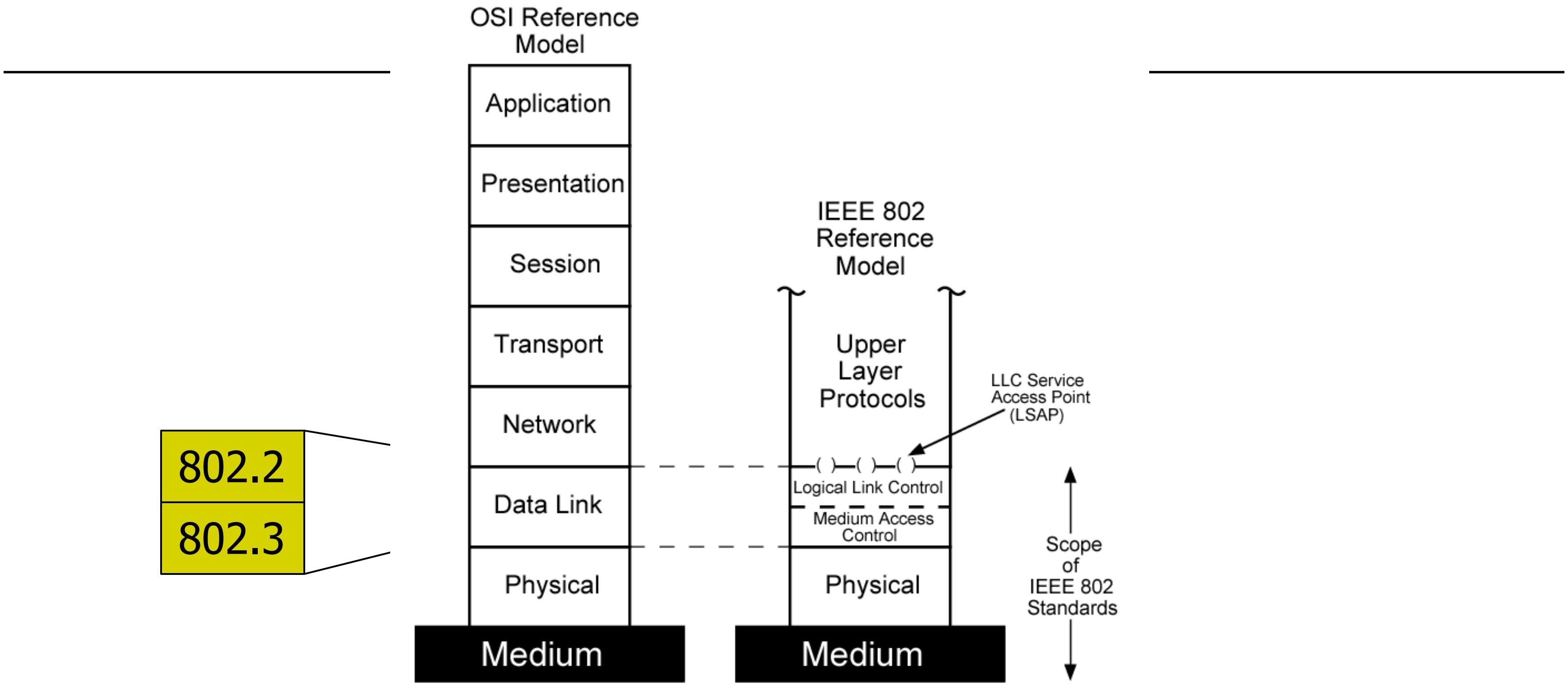
Sub-Layer	Expansion	Purpose
LLC	Logical Link Control	Addressing and demultiplexing
MAC	Media Access Control	Access to shared media

IEEE 802 Model and Standards

- IEEE assigns a multi-part identifier of the form XXX.YYY.ZZZ
  - XXX denotes the category of the standard
  - YYY denotes a subcategory
  - If a subcategory is large enough, a third level can be added

ID	Topic
802.1	Higher layer LAN protocols
802.2	Logical link control
802.3	Ethernet
802.4	Token bus (disbanded)
802.5	Token Ring
802.6	Metropolitan Area Networks (disbanded)
802.7	Broadband LAN using Coaxial Cable (disbanded)
802.9	Integrated Services LAN (disbanded)
802.10	Interoperable LAN Security (disbanded)
802.11	Wireless LAN (Wi-Fi)
802.12	Demand priority
802.13	Category 6 - 10Gb LAN
802.14	Cable modems (disbanded)
802.15	Wireless PAN 802.15.1 (Bluetooth) 802.15.4 (ZigBee)
802.16	Broadband Wireless Access 802.16e (Mobile) Broadband Wireless
802.17	Resilient packet ring
802.18	Radio Regulatory TAG
802.19	Coexistence TAG
802.20	Mobile Broadband Wireless Access
802.21	Media Independent Handoff
802.22	Wireless Regional Area Network

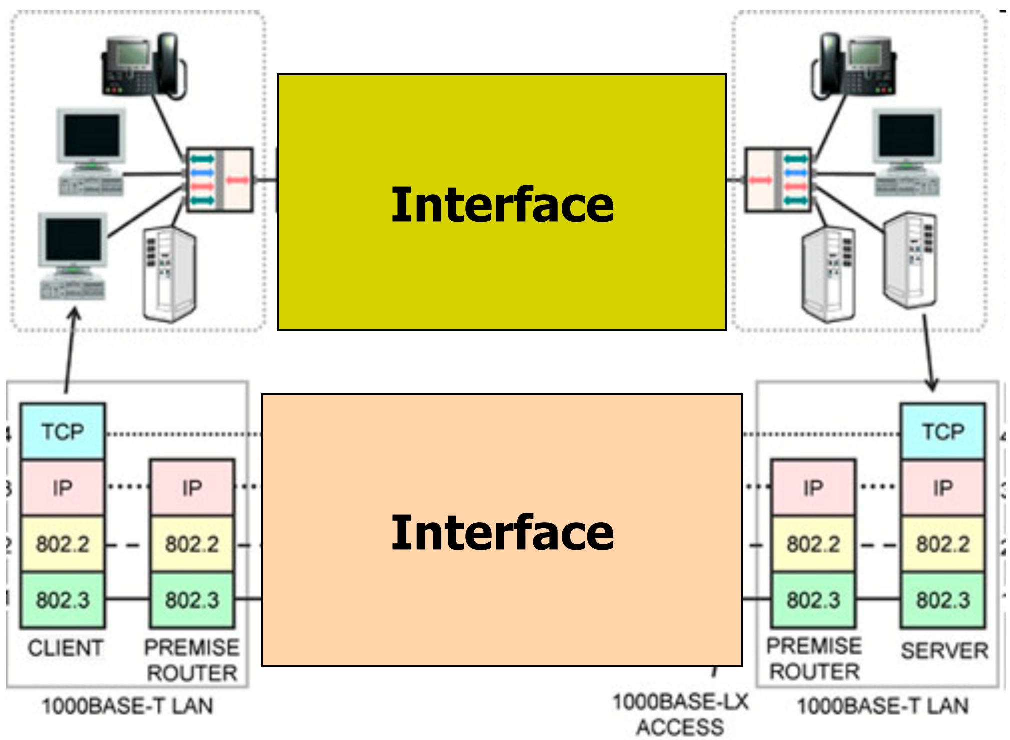
Ethernet Protocol Architecture



EEE 802.2 is the IEEE 802 standard defining Logical Link Control (LLC)

EEE 802.3 is a collection of IEEE standards defining the Physical Layer and Data Link Layer's media access control (MAC) sublayer of wired Ethernet.

Ethernet Protocol Stack

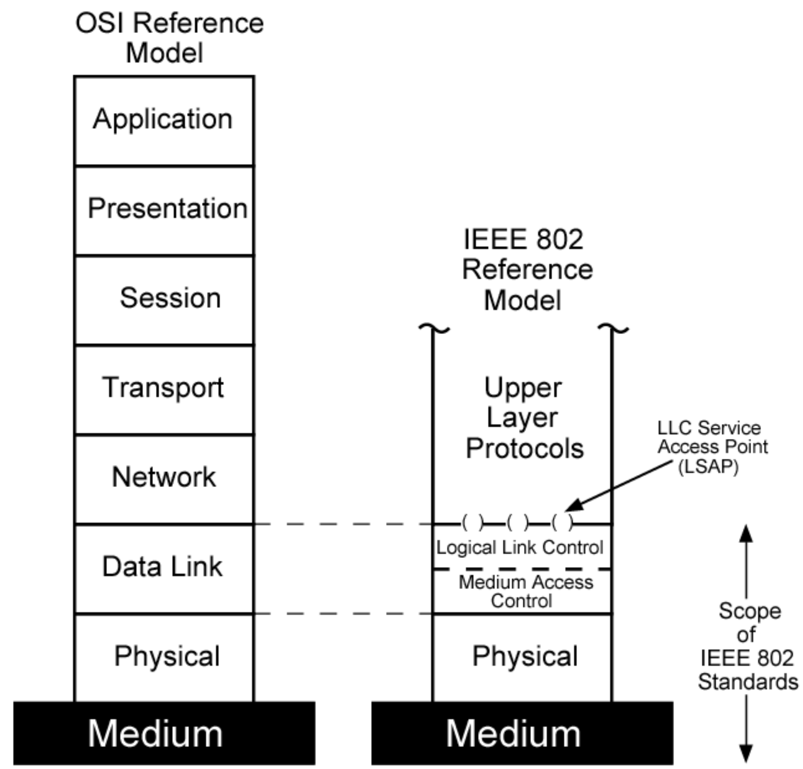


EEE 802.2 is the IEEE 802 standard defining Logical Link Control (LLC)

EEE 802.3 is a collection of IEEE standards defining the Physical Layer and Data Link Layer's media access control (MAC) sublayer of wired Ethernet.

Ethernet Protocol Architecture IEEE 802 Layers

- Physical
  - encoding/decoding of signals
  - preamble generation/removal
  - bit transmission/reception
  - transmission medium and topology



IEEE MAC SUB-LAYER

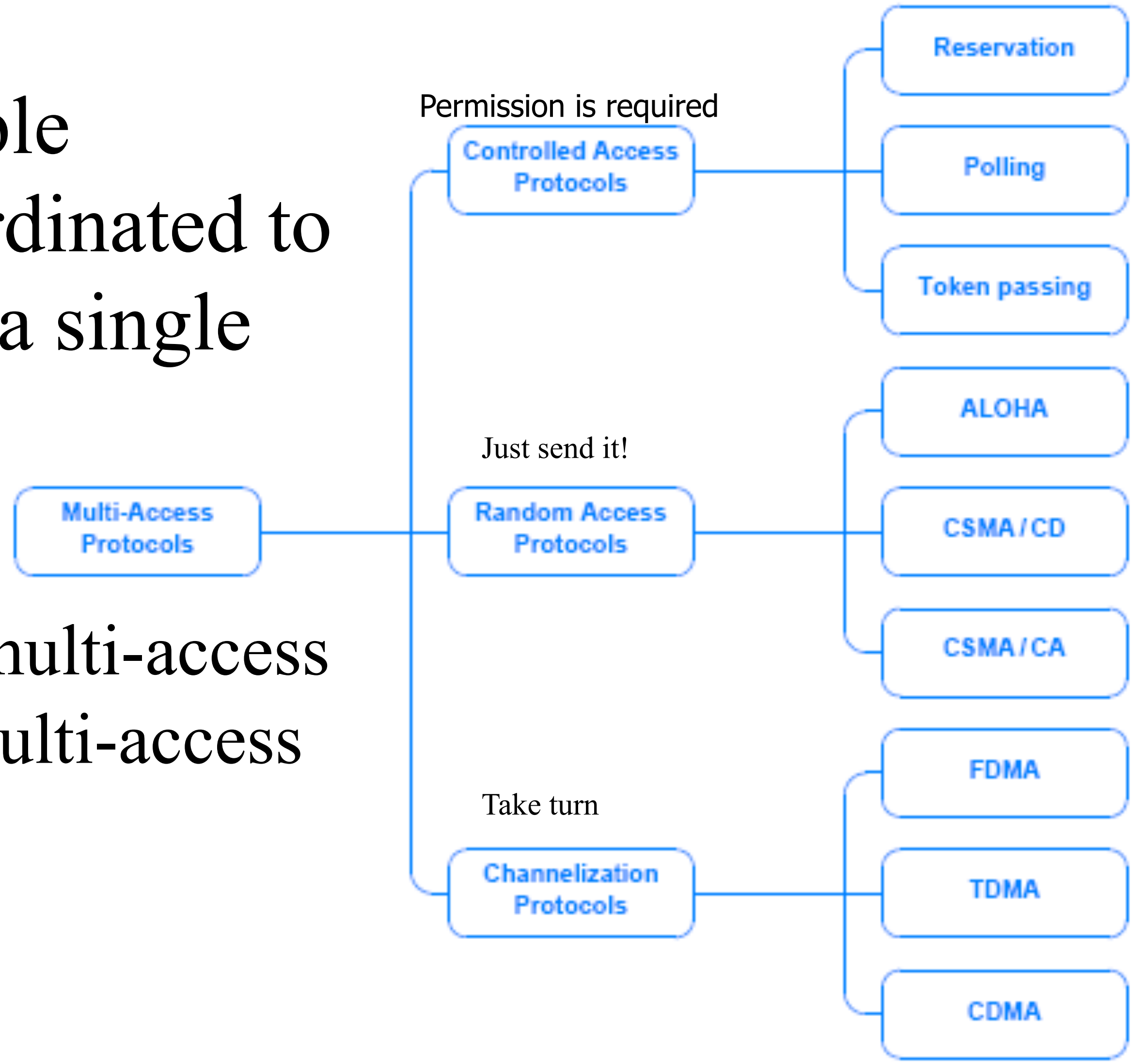
Chapter 14

Multi-Access Protocols & Channel Allocations

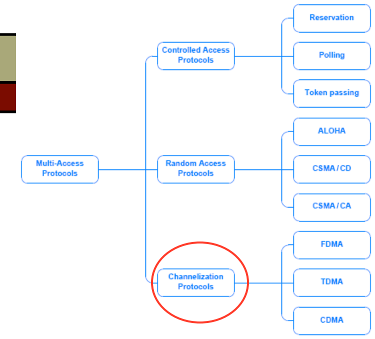
- LAN technologies allow multiple computers to share medium
  - any computer on the LAN can communicate with any other
  - in order to share the medium we have to get access
- We use the term multi-access to describe the way medium access is achieved
- Thus, LAN is considered to be a multi-access network

Channel (medium) Access Control Protocols

- How are multiple computers coordinated to control (share) a single medium?
- In other words:
  - What are the multi-access protocols in multi-access networks?



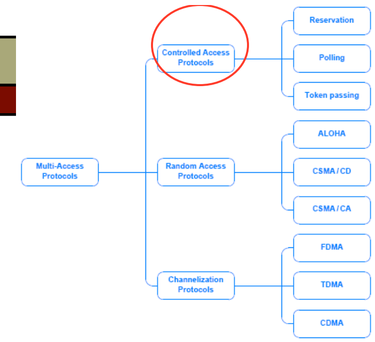
Channelized Access Protocols



- Channelization refers to a mapping between a given communication and a channel in the underlying system
  - There should be a mapping between entities and a channel is referred to as 1-to-1 and static
    - Static channel allocation works well for situations where the set of communicating entities is known in advance and does not change
  - A dynamic channel allocation scheme can be established when a new station appears, and the mapping can be removed when the station disappears

Protocol	Expansion
FDMA	Frequency Division Multi-Access
TDMA	Time Division Multi-Access
CDMA	Code Division Multi-Access

Three main types of channelization
Also referred as
multiplexing techniques



Controlled Access Protocols

- Controlled access protocols provide a distributed version of statistical multiplexing

Type	Description
Polling	Centralized controller repeatedly polls stations and allows each to transmit one packet
Reservation	Stations submit a request for the next round of data transmission
Token Passing	Stations circulate a token; each time it receives the token, a station transmits one packet

Controlled Access Protocols-Polling

- Polling uses a centralized controller cycling through stations on the network and gives each an opportunity to transmit a packet
- The selection step is significant because it means a controller can choose which station to poll at a given time
- There are two general polling policies (how to select):
  - Round robin order
    - Round-robin means each station has an equal opportunity to transmit packets
  - Priority order
    - Priority order means some stations will have more opportunity to send
    - For example, priority order might be used to assign an IP telephone higher priority than a personal computer

Controlled Access Protocols- Reservation

- It is often used with satellite transmission
- Typically, reservation systems have a central controller that follows Algorithm below

Reservation Algorithm

Purpose:

Control transmission of packets through reservation

Method:

```
Controller repeats forever {
    Form a list of stations that have a packet to send;
    Allow stations on the list to transmit;
}
```

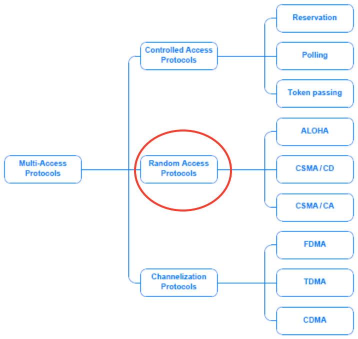
Controlled Access Protocols- Reservation

- It employs a two-step process in which each round of packet transmissions is planned in advance
- In the first step
  - each potential sender specifies whether they have a packet to send during the next round, and the controller transmits a list of the stations that will be transmitting
- In the second step
  - stations use the list to know when they should transmit
- Variations exist
  - where a controller uses an alternate channel to gather reservations for the next round (out-of-band) - while the current round of transmissions proceeds over the main channel

Controlled Access Protocols- Token Passing

- It is most often associated with ring topologies
- Although older LANs used token passing ring technology
  - popularity has decreased, and few token passing networks remain
- Imagine a set of computers connected in a ring
  - and imagine that at any instant, exactly one of the computers has received a special control message called a token
- When no station has any packets to send
  - the token circulates among all stations continuously
- For a ring topology, the order of circulation is defined
  - if messages are sent clockwise, the next station mentioned in the algorithm refers to the next physical station in a clockwise order
- When token passing is applied to other topologies (bus)
  - each station is assigned a position in a logical sequence
  - and the token is passed according to the assigned sequence

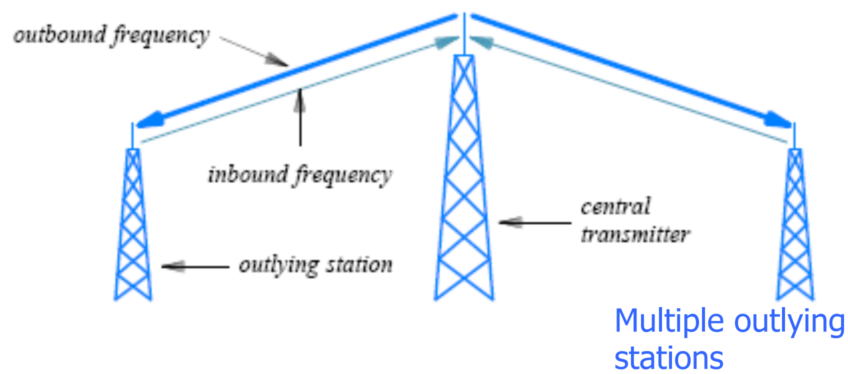
Random Access Protocols



- Some LANs do not employ a controlled access mechanism
  - Instead, a set of computers attached to a shared medium attempt to access the medium without coordination
- The term random is used because access only occurs when a given station has a packet to send
- Three random access methods
  - ALOHA
  - CSMA/CD (Collision Detection)
  - CSMA/CA (Collision Avoidance)

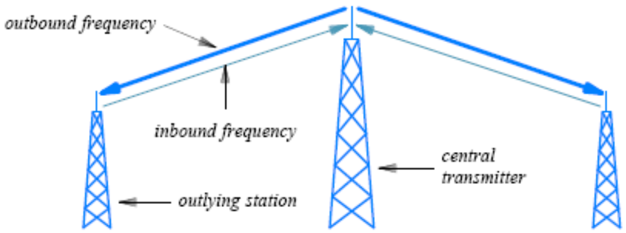
ALOHA

- An early network in Hawaii, known as ALOHAnet, pioneered the concept of random access
  - the network is no longer used, but the ideas have been extended
- The network consisted of a single powerful transmitter in a central geographic location
  - It is surrounded by a set of stations/computer
  - Stations had a transmitter capable of reaching the central transmitter
    - but not powerful enough to reach all the other stations
- ALOHAnet used two (2) carrier frequencies for broadcasting:
  - one for outbound by the central transmitter to all stations
  - and another for inbound by stations to the central transmitter



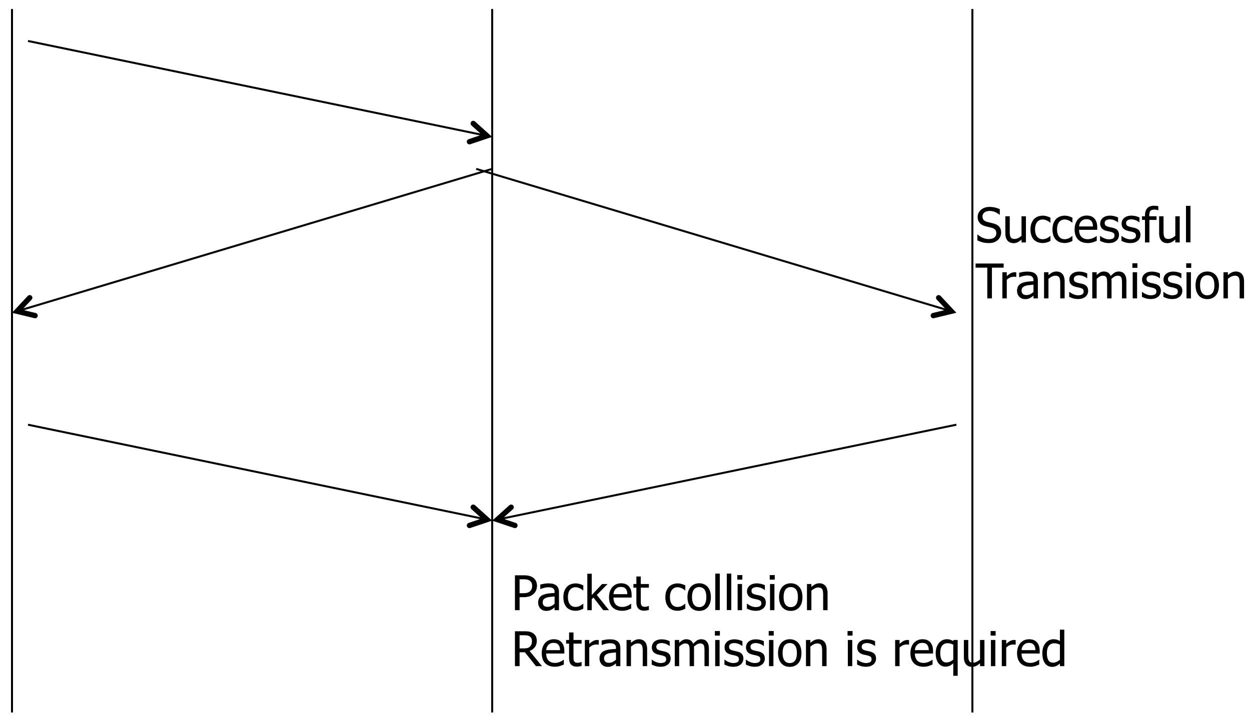
Outbound: 413.475 MHz
Inbound: 407.305 MHz

ALOHA



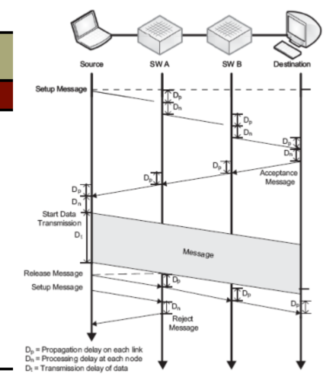
- The ALOHA protocol is straightforward:
  - when a station has a packet to send it transmits the packet on the inbound frequency
  - the central transmitter repeats the transmission on the outbound frequency (which all stations can receive)
- To insure that transmission is successful
  - a sending station listens to the outbound channel
    - if a copy of its packet arrives, the sending station moves to the next packet
    - if no copy arrives, the sending station waits a short time and tries again
- Why might a packet fail to arrive? Interference
  - if two stations simultaneously transmit (on the same frequency)
    - the signals will interfere and the two transmissions will be garbled
    - called a collision, and say that the two transmitted packets collide
- The protocol handles a collision
  - by requiring a sender to retransmit each lost packet

ALOHA


Successful
Transmission
Packet collision
Retransmission is required

CSMA

Three basic features:
Carrier Sense
Collision Detection
Binary Exp. Backoff



Delay Types:
- Node
- Prop.
- Trans.

- Ethernet requires each station to monitor the cable to detect whether another transmission is already in progress
  - this process is known as carrier sense medium access
  - it prevents the most obvious collision problems
  - and substantially improves network utilization
- First listen for clear medium (carrier sense)
  - If medium idle → transmit
  - If two stations start at the same instant → collision
  - Wait for reasonable time
  - If no activity then retransmit
- Max utilization depends on propagation time (medium length) and frame length
  - Longer frame and shorter propagation gives better utilization
- What if the line is busy?
  - Non-persistent
  - 1-persistent
  - P-persistent

Typically, propagation time is much less than transmission time

Non-persistent CSMA

Basic Idea:

1. If medium is idle, transmit; otherwise, go to 2
2. If medium is busy, wait amount of time drawn from probability distribution (retransmission delay) and repeat 1

- Advantage: Random delays reduces probability of collisions
  - Consider two stations become ready to transmit at same time while another transmission is in progress:
    - If both stations delay same time before retrying, both will attempt to transmit at same time
- Disadvantage: Capacity is wasted because medium will remain idle following end of transmission
  - Even if one or more stations waiting – no one is transmitting

1-persistent CSMA

- To avoid idle channel time, 1-persistent protocol is used
- Station wishing to transmit listens and carries out the following:
  1. If medium idle, transmit; otherwise, go to step 2
  2. If medium busy, **listen until idle**; then transmit **immediately**
- 1-persistent stations are selfish
  - If two or more stations waiting, collision guaranteed
- Wasted time is shortened if frame length are long compared to the propagation time

P-persistent CSMA

- Rules:
  - If medium idle, transmit with probability p, and delay one time unit with probability (1 – p)
  - Time unit is typically equal to the maximum propagation delay
  1. If medium busy, listen until idle and repeat step 1
  2. If transmission is delayed one time unit, repeat step 1

What is an effective value of p?

Value of p?

- Avoid instability under heavy load
- Consider that **n** stations are waiting to send, while a transmission is taking place
- End of transmission:
  - Expected number of stations attempting to transmit = number of stations ready * probability of transmitting = **n*p**
- If np > 1 then on average there will be a collision
  - Repeated attempts to transmit almost guaranteeing more collisions
  - Retries compete with new transmissions from other stations
  - Eventually, all stations trying to send
    - Continuous collisions; zero throughput
- If np < 1 then
  - If heavy load expected, p must be small
  - However, as p made smaller, stations wait longer
  - At low loads, this gives very long delays

CSMA/CD – Collision Detection

- With CSMA, collision can occur for the entire duration of transmission
- Using CD stations listen whilst transmitting

1. If medium idle, transmit, otherwise, step 2
2. If busy, listen for idle, then transmit immediately
3. If collision detected, jam (transmit brief jamming signal) then stop transmission – higher level of energy is sensed
4. After jam, wait random time (called backoff) then start from step 1

Three basic features:
Carrier Sense
Collision Detection
Binary Exp. Backoff

Which Persistence Algorithm?

- IEEE 802.3 uses 1-persistent
- Both non-persistent and p-persistent have performance problems
- Issues with 1-persistent (p = 1)
  - Seems more unstable than p-persistent
    - Greed of the stations
  - But wasted time due to collisions is short (if frames long relative to propagation delay)
  - With random backoff, unlikely to collide on next tries
  - To ensure backoff maintains stability, IEEE 802.3 and Ethernet use binary exponential backoff

Binary Exponential Backoff

- A technique used by IEEE 802.3 and Ethernet to ensure that backoff maintains stability
  - As congestion increases, stations back off by larger amounts to reduce the probability of collision.
- How does it work
  - a computer chooses a random delay between 0 - d after one collision
  - a random delay between 0 - 2d after a second collision
  - a random delay between 0 - 4d after a third, and so on
  - After 16 unsuccessful attempts, station gives up and reports error
- **1-persistent algorithm with binary exponential backoff is efficient over wide range of loads**
  - Low loads, 1-persistence guarantees station can seize channel once idle
  - High loads, at least as stable as other techniques
- Backoff algorithm gives last-in, first-out effect
  - Stations with few collisions transmit first

CSMA/CD Algorithm

9.6 usec for 10MMbps → (points to "Delay for the interpacket gap")

Algorithm 14.4

CSMA/CD Algorithm

Purpose:

Use CSMA/CD to send a packet

Method:

```
Wait for a packet to be ready;
Wait for the medium to be idle (carrier sense);
Delay for the interpacket gap;
Set variable  x  to the standard backoff range,  d ;
Attempt to transmit the packet (collision detection);
While  (a collision occurred during previous transmission)  {
    Choose  q  to be a random delay between  0  and  x ;
    Delay for  q  microseconds;
    Double  x  in case needed for the next round;
    Attempt to retransmit the packet (collision detection);
}
```

Collision Detection

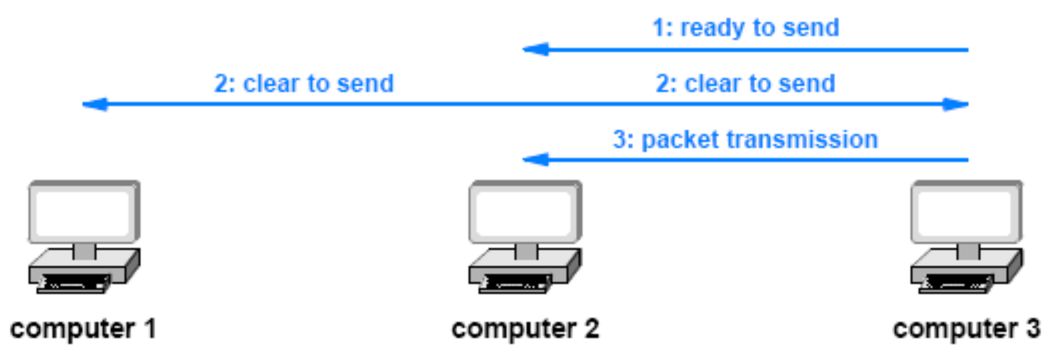
- On baseband bus, collision produces much higher signal voltage than signal
  - Collision detected if cable signal greater than single station signal
  - Signal attenuated over distance
  - Limit distance to 500m (10Base5) or 200m (10Base2)
- For star-topology activity on more than one port is collision

CSMA with Collision Avoidance

- CSMA/CD does not work as well in wireless LANs
  - because a transmitter used in a wireless LAN has a limited range
- A receiver that is more than a few hops away from the transmitter
  - will not receive a signal, and will not be able to detect a carrier
- Wireless LANs use a modified access protocol
  - known as CSMA with Collision Avoidance (CSMA/CA)
- The CSMA/CA triggers a brief transmission from the intended receiver before transmitting a packet

CSMA with Collision Avoidance – Example (1)

- computer3 sends a short message to announce that it is ready to transmit a packet to computer 2
- and computer 2 responds by sending a short message announcing that it is ready to receive the packet
- all computers in range of computer 3 receive the initial announcement
- and all computers in the range of computer 2 receive the response
- as a result, even though it cannot receive the signal or sense a carrier, computer 1 knows that a packet transmission is taking place

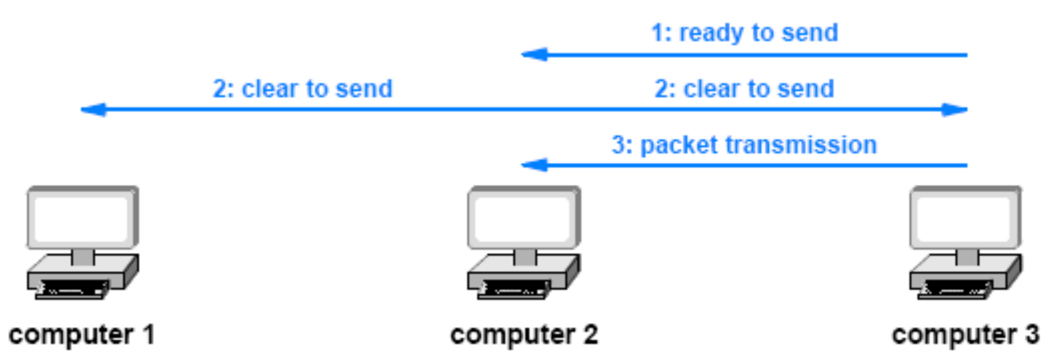


Hidden Station Problem

CSMA with Collision Avoidance – Example (2)

- **Collisions of control messages** can occur when using CSMA/CA, but they can be handled easily
- For example, if computer 1 and computer 3 each attempt to transmit a packet to computer 2 at exactly the same time
  - their control messages will collide
  - When a collision occurs, the sending stations apply random backoff before resending the control messages.
- Because control messages are much shorter than a packet, the probability of a second collision is low

Signal propagation < span distance



Ethernet

- IEEE 802.3 uses CSMA with 1-persistent
- To ensure backoff maintains stability, IEEE 802.3 and Ethernet use binary exponential backoff

<u>Three basic features</u>:
Carrier Sense
Collision Detection
Binary Exp. Backoff

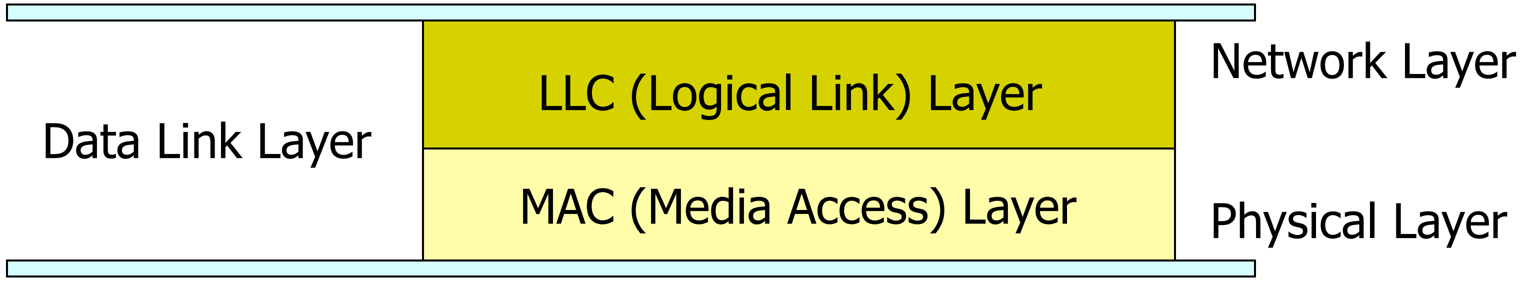
Ethernet Addressing

Ethernet Addressing

- IEEE has created a standard for addressing
- Each packet that travels across the shared medium is intended for a specific recipient
  - and only the intended recipient should process the packet
- The identifier is known as an address
- Each computer is assigned a unique address
  - and each packet contains the address of the intended recipient
- In the IEEE addressing scheme, each address consists of 48 bits; IEEE uses the term Media Access Control address (or simply MAC address)
  - networking professionals often use the term Ethernet address
- IEEE allocates a unique address for each piece of interface
  - Each Network Interface Card (NIC) contains a unique IEEE address assigned when the device was manufactured

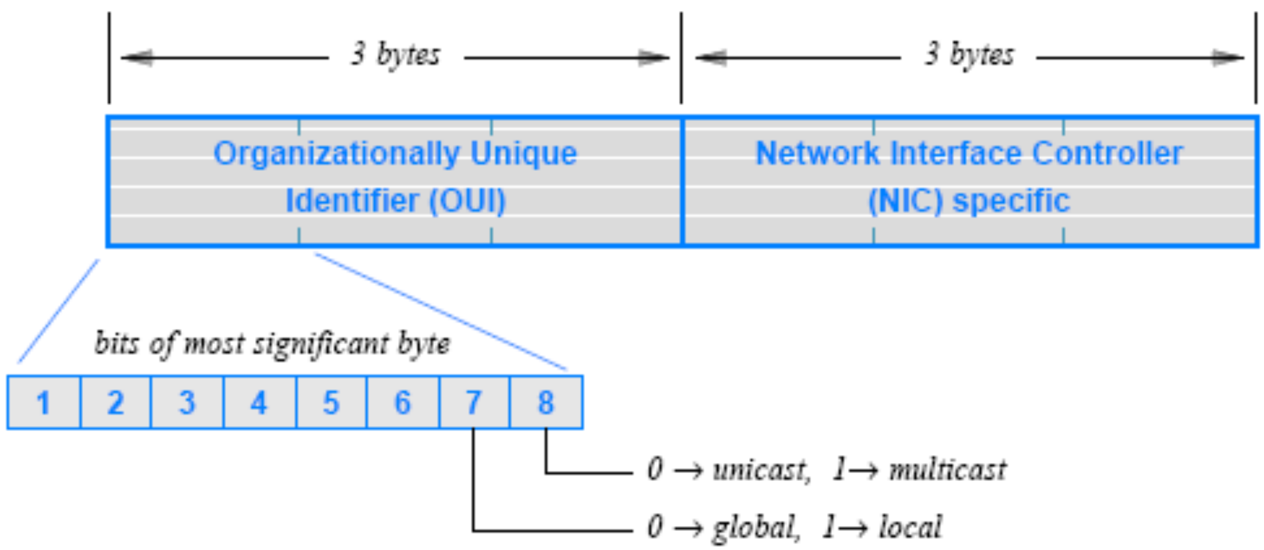
Ethernet Addressing

- Remember: MAC address is a 48 bit flat addressing
  - It is not hierarchical as in IP addressing
- When a device is added its MAC address is announced to others
  - For same LLC, may have several MAC options
- Logical Link Control
  - Interface to higher levels
  - Flow and error control



Ethernet Addressing

- MAC address is 48 bits:
  - 24 bits (OUI – Organizationally unique Identifier
  - 24 bit hardware address – burned in the ROM



Ethernet Addressing

These MAC addresses are found via:
http://standards.ieee.org/regauth/oui/index.shtml

Enter MAC: [ ] Submit Query

My OUI

Here are the results of your search through the public section of the IEEE Standards OUI database report for **002170**:

```
00-21-70   (hex)           Dell Inc
002170     (base 16)       Dell Inc
                           One Dell Way, MS RR5-45
                           Round Rock Texas 78682
                           UNITED STATES
```

Ethernet Addressing

- The IEEE addressing supports three types of addresses that correspond to three types of packet delivery
  - Unicast, multicast, broadcast
- The standard specifies that a broadcast address consists of 48 bits that are all 1s
  - Thus, a broadcast address has the multicast bit set
- Broadcast can be viewed as a special form of multicast
  - Each multicast address corresponds to a group of computers
  - Broadcast address corresponds to a group that includes all computers on the network

Address Type	Meaning And Packet Delivery
unicast	Uniquely identifies a single computer, and specifies that only the identified computer should receive a copy of the packet
broadcast	Corresponds to all computers, and specifies that each computer on the network should receive a copy of the packet
multicast	Identifies a subset of the computers on a given network, and specifies that each computer in the subset should receive a copy of the packet

Packet Processing and Efficient Multi-Point Delivery

- Recall that a LAN transmits packets over a shared medium
- In a typical LAN
  - each computer on the LAN monitors the shared medium
  - extracts a copy of each packet
  - and then examines the address in the packet
  - determine whether the packet should be processed or ignored

Packet Processing Algorithm in a LAN

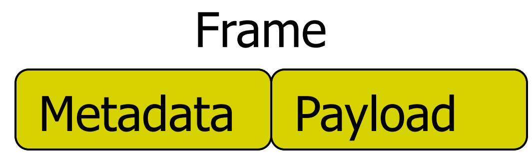
Purpose:

Handle a packet that has arrived over a LAN

Method:

```
Extract destination address, D, from the packet;
if (D matches "my address") {
    accept and process the packet;
} else if (D matches the broadcast address) {
    accept and process the packet;
} else if (D matches one of the multicast addresses for a
  multicast group of which I am a member) {
    accept and process the packet;
} else {
    ignore the packet;
}
```

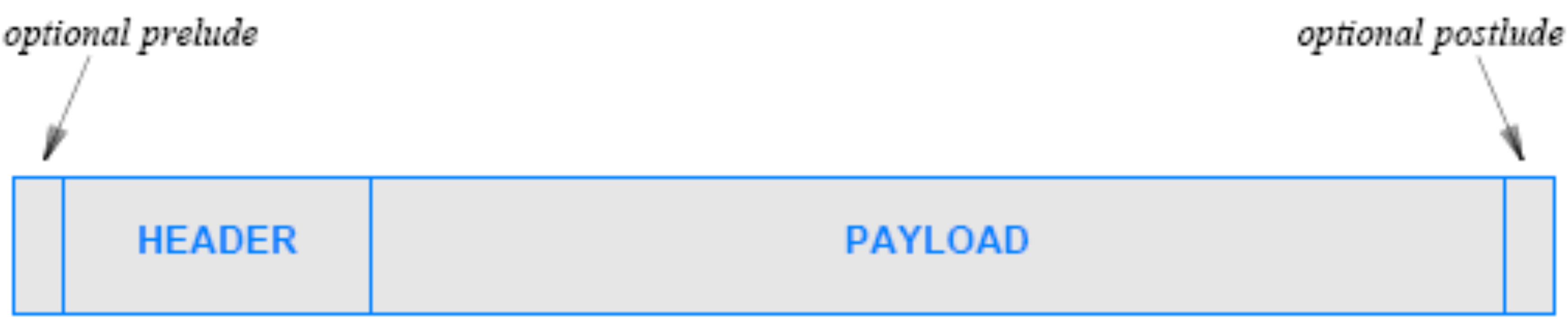
Frames and Framing



- Framing refers to the structure added to a sequence of bits or bytes that allows a sender and receiver to agree on the exact format of the message
- Ethernet is a packet-switched network that transmits and receives Ethernet frames - each frame corresponds to a packet
- A frame consists of two conceptual parts:
  - Header that contains metadata, such as an address
    - contains information used to process the frame
  - Payload that contains the data being sent
    - contains the message being sent
    - and is usually much larger than the frame header

Frames and Framing

- A message is opaque
  - in the sense that the network only examines the frame header
  - the payload can contain an arbitrary sequence of bytes that are only meaningful to the sender and receiver
- Opaque V.s Forwarding
  - Forwarding checks the CRC; Opaque just checks the destination
- Some technologies delineate each frame by sending a short prelude before the frame and a short postlude after it



Frames and Framing

- Assume that a packet header consists of 6 bytes
  - the payload consists of an arbitrary number of bytes
- We can use ASCII character set
  - the Start Of Header (SOH) character marks the beginning of a frame
  - and the End Of Transmission (EOT) character marks the end

Frames and Framing

Byte In Payload	Sequence Sent
SOH	ESC A
EOT	ESC B
ESC	ESC C

- In the ASCII character set
  - SOH has hexadecimal value 201
  - EOT has the hexadecimal value 204
- An important question arises
  - what happens if the payload of a frame includes one or more bytes with value 201 or 204?
- The answer lies in a technique known as byte stuffing
  - that allows transmission of arbitrary data without confusion
- Examples of bit stuffing:
  - the sender replaces each occurrence of SOH by the two characters ESC [1B hex] + A
  - each occurrence of EOT by the characters ESC + B
  - and each occurrence of ESC by the two characters ESC + C

http://www.asciitable.com/

Ethernet Frame Format

Max. Length: 8+6+6+2+1500+4=1526

Min Length: 8+6+6+2+46+4=72

Preamble	Start-of-Frame-Delimiter	MAC destination	MAC source	Ethertype/Length	Payload (Data and padding)	CRC32	Interframe gap
7 octets of 10101010	1 octet of 10101011	6 octets	6 octets	2 octets	46–1500 octets	4 octets	12 octets

8 Bytes of Preamble

Nothing is being Sent!

Ethernet Frame Format

Calculations

Preamble	Start-of-Frame-Delimiter	MAC destination	MAC source	Ethertype/Length	Payload (Data and padding)	CRC32	Interframe gap
7 octets of 10101010	1 octet of 10101011	6 octets	6 octets	2 octets	46–1500 octets	4 octets	12 octets

8 Bytes of Preamble

Nothing is being Sent!

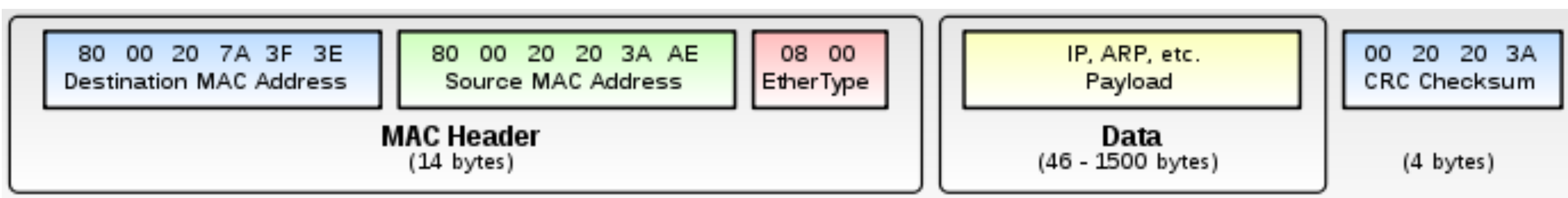
Max. Length: 6+6+2+1500+4=1518 byte excluding the preamble
Min Length: 6+6+2+46+4=64 byte excluding the preamble

When transmitting consecutive Min. Length frames, actually each frame occupies 72+12 = 84 Bytes
Assuming 10 Mbps Ethernet (RJ-45 Cat 5 UTP) → Inter-frame gap will be 9.6 usec
Assuming we have a 100 Mbps Ethernet connection sending minimum size frames,

Overhead Ratio: (Total Bytes Sent – Data Byte) / Total Bytes Sent = (84 B – 64 B)/84 B = 23.8 %
thus, assuming no other traffic and no collision, total BW Efficiency will be only 23.8 %.
But typical Ethernet packet size is about 260 Bytes (lots of TCP ACK packets!)

Framing Structure

```
⊞ Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊟ Ethernet II, Src: Dell_02:94:89 (5c:26:0a:02:94:89), Dst: CameoCom_03:47:56 (00:18:e7:03:47:56)
  ⊟ Destination: CameoCom_03:47:56 (00:18:e7:03:47:56)
      Address: CameoCom_03:47:56 (00:18:e7:03:47:56)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: Dell_02:94:89 (5c:26:0a:02:94:89)
      Address: Dell_02:94:89 (5c:26:0a:02:94:89)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 130.157.5.226 (130.157.5.226)
    Version: 4
```



Exercise: Look at Frame # 9 and Frame 4: Identify all the fields in the frame.

ARP Packet

```
⊟ Ethernet II, Src: Dell_02:94:89 (5c:26:0a:02:94:89), Dst: CameoCom_03:47:56 (00:18:e7:03:47:56)
  ⊟ Destination: CameoCom_03:47:56 (00:18:e7:03:47:56)
      Address: CameoCom_03:47:56 (00:18:e7:03:47:56)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: Dell_02:94:89 (5c:26:0a:02:94:89)
      Address: Dell_02:94:89 (5c:26:0a:02:94:89)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    [Is gratuitous: False]
    Sender MAC address: Dell_02:94:89 (5c:26:0a:02:94:89)
    Sender IP address: 192.168.1.102 (192.168.1.102)
    Target MAC address: CameoCom_03:47:56 (00:18:e7:03:47:56)
    Target IP address: 192.168.1.1 (192.168.1.1)
```

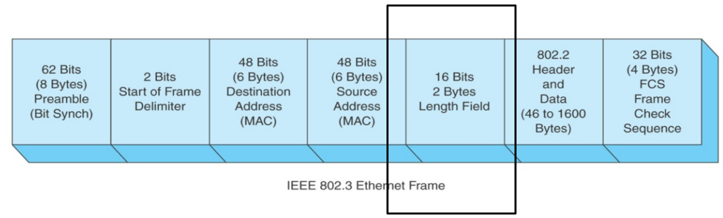
Note that the type is ARP

Given MAC→ what is IP

Ethernet Frame Format

- **Preamble (PRE)**- 7 bytes. The PRE is an alternating pattern of ones and zeros that tells receiving stations that a frame is coming, and that provides a means to synchronize the frame-reception portions of receiving physical layers with the incoming bit stream.
- **Start-of-frame delimiter (SFD)**- 1 byte. The SOF is an alternating pattern of ones and zeros, ending with two consecutive 1-bits indicating that the next bit is the left-most bit in the left-most byte of the destination address.
- **Destination address (DA)**- 6 bytes. The DA field identifies which station(s) should receive the frame..
- **Source addresses (SA)**- 6 bytes. The SA field identifies the sending station.
- **Length/Type**- 2 bytes. This field indicates either the number of MAC-client data bytes that are contained in the data field of the frame, or the frame type ID if the frame is assembled using an optional format.
- **Data**- Is a sequence of n bytes (46=< n =<1500) of any value. (The total frame minimum is 64bytes.)
- **Frame check sequence (FCS)**- 4 bytes. This sequence contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames.
- **Inter-Frame Gap**: Used to ensure that a single node does not utilize the link at all the time.

Ethernet Type Field



- The type field in an Ethernet frame provides multiplexing and demultiplexing (2 bytes long)
  - Allows a given computer to have multiple protocols operating simultaneously
- The protocols used on the Internet send IP datagrams and ARP (Address Resolution Protocol) messages over Ethernet
  - Each is assigned a unique Ethernet type (hexadecimal 0800 for IP datagrams and hexadecimal 0806 for ARP messages)
  - When transmitting a IP datagram in an Ethernet frame, the sender assigns a type 0800
- When a frame arrives at its destination
  - the receiver examines the type field, and it uses the value to determine which software module should process the frame

Ethernet Types:

0600	Xerox NS IDP
0800	Internetworking Protocol (IP)
0801	X.75
0802	NBS
0803	ECMA
0804	Chaosnet
0805	X.25 Packet (Level 3)
0806	Address Resolution Protocol (ARP)
0807	XNS Compatibility
1000	Berkeley Trailer
5208	BBN Simnet
6001	DEC MOP (Dump/Load)
6002	DEC MOP (Remote Console)
6003	DECNET Phase 4
6004	DEC LAT
6005	DEC
6006	DEC
8005	HP Probe
8010	Excelan
8035	Reverse ARP
8038	DEC LANBridge
809B	AppleTalk
80F3	AppleTalk ARP
8137	NetWare IPX/SPX

Versions of Ethernet

- IEEE developed a standard for Ethernet (1983) and attempted to redefine the Ethernet frame format
- The IEEE working group that produced the standard is numbered 802.3
  - professionals often refer to it as 802.3 Ethernet
- The major difference between conventional Ethernet and 802.3 Ethernet arises from the interpretation of the type field
  - The 802.3 standard interprets the original type field as a packet length, and adds 8-byte header that contains the packet type
  - The extra header is known as a Logical Link Control / Sub-Network Attachment Point (LLC/SNAP) header; (next slides)

http://standards.ieee.org/getieee802/download/802-2001.pdf

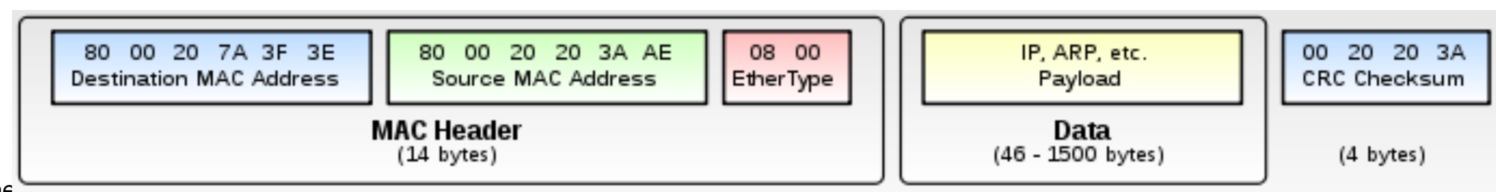
Ethernet Types

How to distinguish

- Novell's non-standard variation of IEEE 802.3 ("raw 802.3 frame") without an IEEE 802.2 LLC header.
  - If the IPX header (0xFF-FF) - the data field
  - Length Field is used (Max. 1500=05DC Hex)
- The Ethernet Version 2 or Ethernet II frame, the so-called DIX frame (named after DEC, Intel, and Xerox)
  - often used directly by the Internet Protocol.
  - Uses Ethernet Type -Larger than 05DC Hex →
- IEEE 802.2 LLC frame
  - Uses Length Field + LLC
- IEEE 802.2 LLC/SNAP frame
  - Uses Length Field + LLC + SNAP
  - If SSAP value is 0xAA, the frame is interpreted as a SNAP frame otherwise LLC only
- Example of Ethernet Version 2:

Ethernet Types:

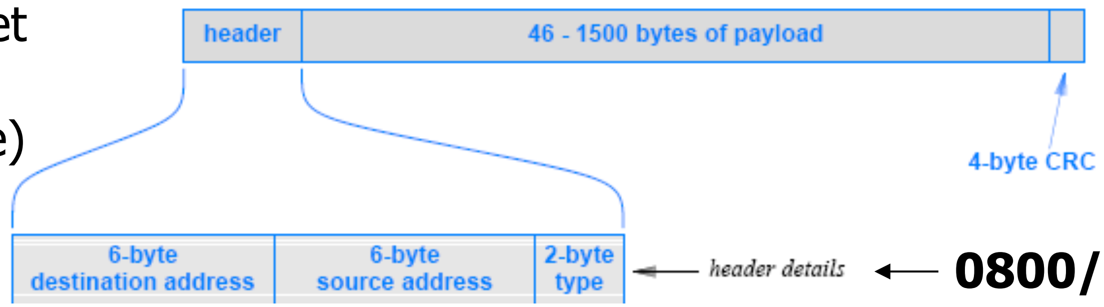
Hexadecimal Assignment	Description
0600	Xerox NS IDP
0800	Internetworking Protocol (IP)
0801	X.75
0802	NBS
0803	ECMA
0804	Chaosnet
0805	X.25 Packet (Level 3)
0806	Address Resolution Protocol (ARP)
0807	XNS Compatibility
1000	Berkeley Trailer
5208	BBN Simnet
6001	DEC MOP (Dump/Load)
6002	DEC MOP (Remote Console)
6003	DECNET Phase 4
6004	DEC LAT
6005	DEC
6006	DEC
8005	HP Probe
8010	Excelan
8035	Reverse ARP
8038	DEC LANBridge
809B	AppleTalk
80F3	AppleTalk ARP
8137	NetWare IPX/SPX



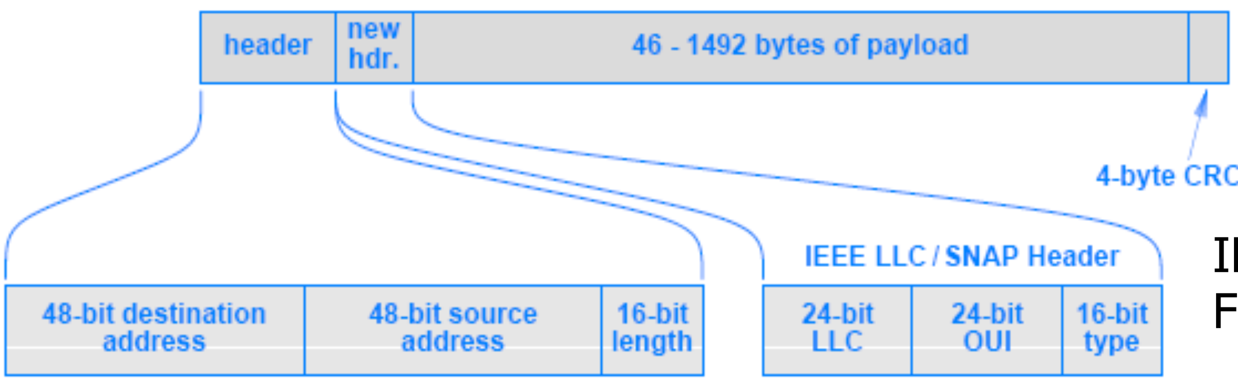
http://en.wikipedia.org/wiki/Etherne

Comparing IEEE802.3

conventional Ethernet
(Ethernet Version II
or Ethernet II frame)
Max. 1518 byte



0800/0806 hex



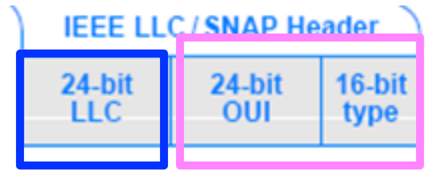
IEEE 802.2 LLC/SNAP Frame (Max. 1518 byte)

Added 8 bytes by 802.3

IEEE 802.3 Frame Format

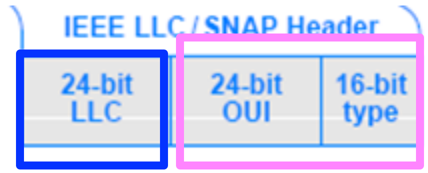
LLC/SNAP

Destination SAP
Source SAP
Control (Type I: Connectionless
Type II: Connection Oriented)



- Remember: the upper sublayer of the Data Link Layer is LLC (layer 2)
  - HDLC (High Level Link Control Protocol) is a general purpose data link layer
  - HDLC uses the services of a physical layer:
  - It offers **best effort** or **reliable** communications path between the TX & RX
- LLC provides multiplexing and flow control mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network (different SAP) and to be transported over the same network media
  - **LLC field is divided into DSAP, SSAP, & Control**
  - **Service Access Point (SAP):** 8-bit 802.2 fields are typically used in data link layers (LLC sublayer) for addressing purpose –
  - SAP is the label used for the equipment
  - E.g., ATP SONET/SDH have their own SAP

LLC/SNAP



- There are different Service Access Points (SAPs): Transport SAP, Session SAP, Network SAP (NSAP)
- Note that NSAP in OSI model is similar (broadly speaking) to IP Address in TCP/IP Layered Model
- TSAP in OSI model serves similar task as TCP Port Address

- The **Subnetwork Access Protocol** (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by SAP
  - SNAP supports vendor-private protocol identifier spaces (OUI – organizationally unique identifier) .
  - Identifies protocols by Ethernet type field values;
    - IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

Ethernet Advantages and Disadvantages

- Advantages
  - Easy to setup; Requires no configurations; Robust to noise
- Disadvantages
  - High collision rate, hence it must operate under low load conditions
    - As the load increases the throughput decreases to zero (that is amount f traffic shifted from one node to another in unit of time)
    - Ethernet loads rarely exceed 30%, so this is not a major problem
  - Providing non-deterministic service
    - Packets may experience indefinite delay due to high collision rate
    - Ethernet may not be suitable for applications demanding a bound on worst-case delay
  - Ethernet, and in general CSMA, does not support priority
    - Each station has equal chance to transmit
    - In case of client-server we may actually want the server to have greater priority
  - Requiring minimum packet length of 64 Bytes
    - This can increase the overhead on applications sending only 1-5 bytes!

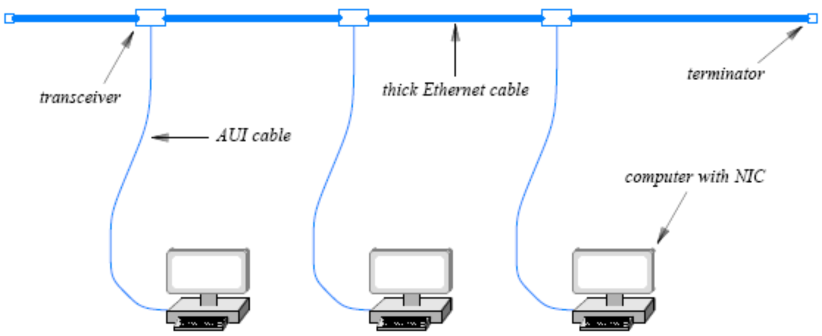
Ethernet Evolution

Ethernet Evolution - Thicknet

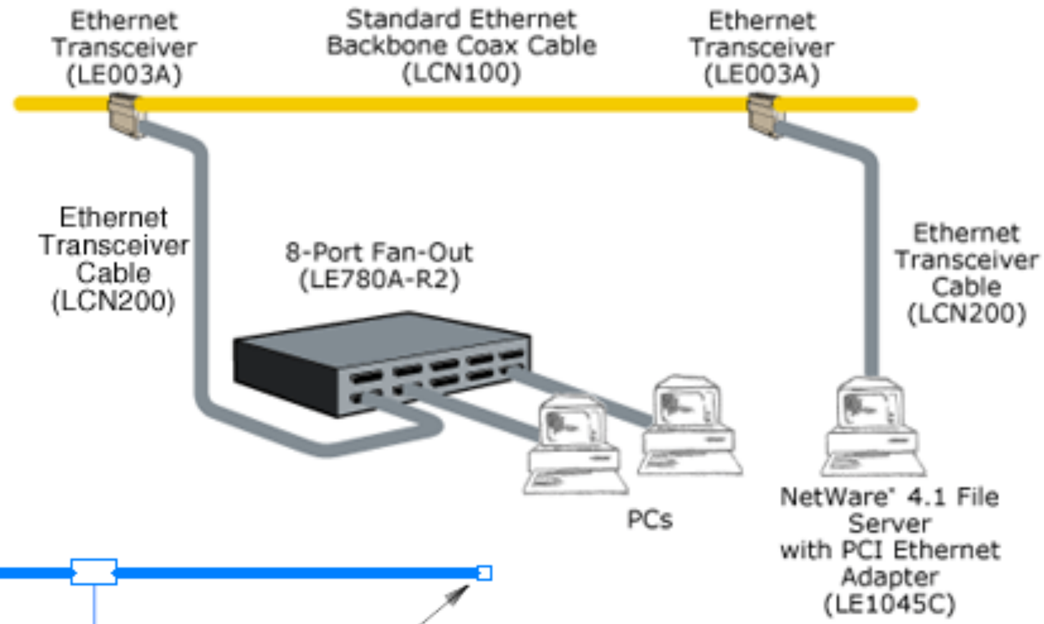
- Ethernet has undergone several major changes
  - with the most significant changes in media and wiring
- The original Ethernet wiring scheme was informally called thick wire Ethernet or Thicknet
  - because the medium consisted of a heavy coaxial cable
  - the formal term for the wiring is 10Base5
- Hardware used with Thicknet was divided into two major parts
  - A NIC handled the digital aspects of communication
  - A separate electronic device called a transceiver connected to the Ethernet cable
    - It handles carrier detection, conversion of bits into appropriate voltages for transmission, and conversion of incoming signals to bits
- A physical cable known as an Attachment Unit Interface (AUI) connected a transceiver to a NIC in a computer
- A transceiver was usually remote from a computer

Ethernet Evolution - Thicknet

- Hardware used with Thicknet was divided into two major parts
  - A NIC handled the digital aspects of communication
  - A separate electronic device called a transceiver connected to the Ethernet cable
    - It handles carrier detection, conversion of bits into appropriate voltages for transmission, and conversion of incoming signals to bits
- A physical cable known as an Attachment Unit Interface (AUI) connected a transceiver to a NIC in a computer
- A transceiver was usually remote from a computer



ThickNet



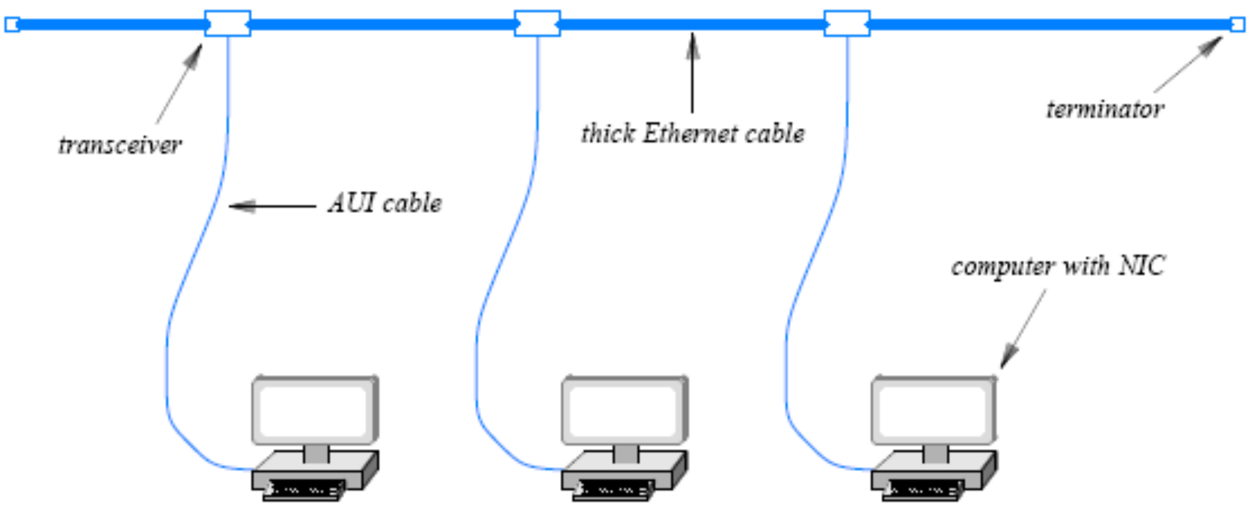
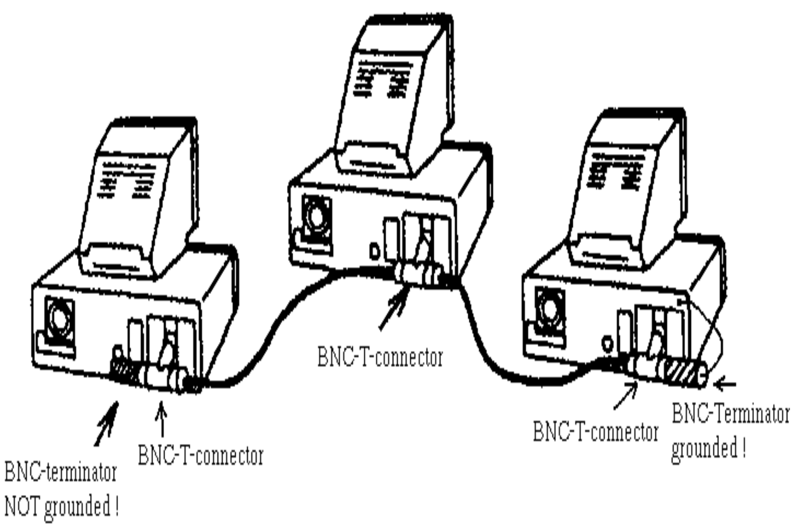
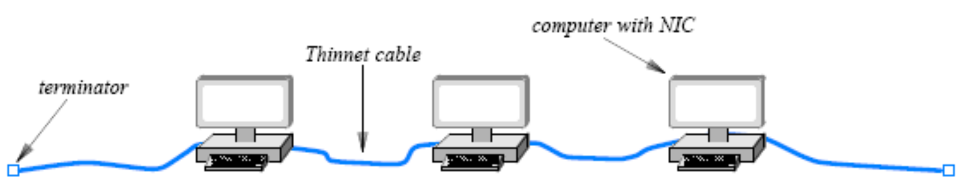


Figure 15.4 Illustration of the original Thicknet Ethernet wiring.

Thinnet Ethernet Wiring

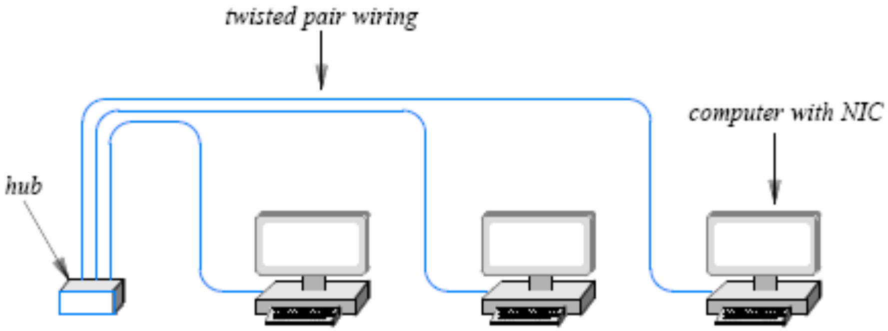
- A second generation of Ethernet used a thinner coaxial cable that was more flexible than Thicknet
  - Formally named 10Base2 and informally known as Thinwire Ethernet or Thinnet
- Thinnet integrates a transceiver directly on the NIC
  - runs a coaxial cable from one computer to another





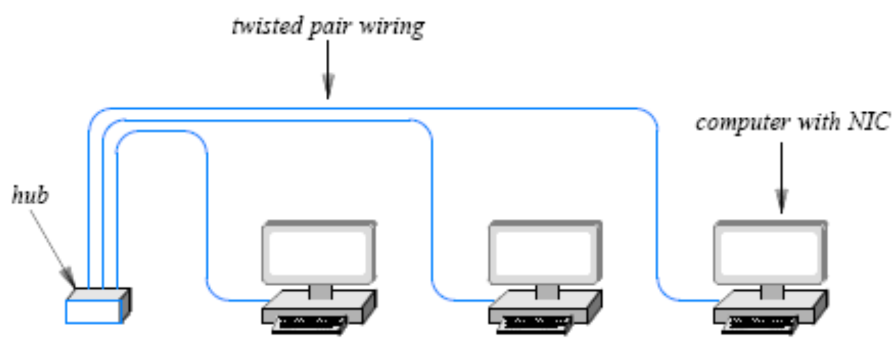
Twisted Pair Ethernet Wiring and Hubs

- A third generation of Ethernet wiring made a dramatic shift:
  - In place of coaxial cable
    - it uses a central electronic device separate from the computers attached to the network
  - Instead of heavy, shielded cabling
    - it uses twisted pair wiring
- The technology is informally known as twisted pair Ethernet, and has replaced other versions
  - Thus, when someone now refers to Ethernet, they are referring to twisted pair Ethernet
- The electronic device that served as the central interconnection was known as a hub
  - Hubs were available in a variety of sizes, with the cost proportional to size, but recently replaced with switches



Logical and Physical Topologies

- To understand Ethernet topology
  - we must distinguish between logical and physical topologies
  - Logically
    - twisted pair Ethernet employs a bus topology
  - Physically
    - twisted pair Ethernet forms a star-shaped topology



Compatibility

Twisted pair Ethernet Technologies

Designation	Name	Data Rate	Cable Used
10BaseT	Twisted Pair Ethernet	10 Mbps	Category 5
100BaseT	Fast Ethernet	100 Mbps	Category 5E
1000BaseT	Gigabit Ethernet	1 Gbps	Category 6

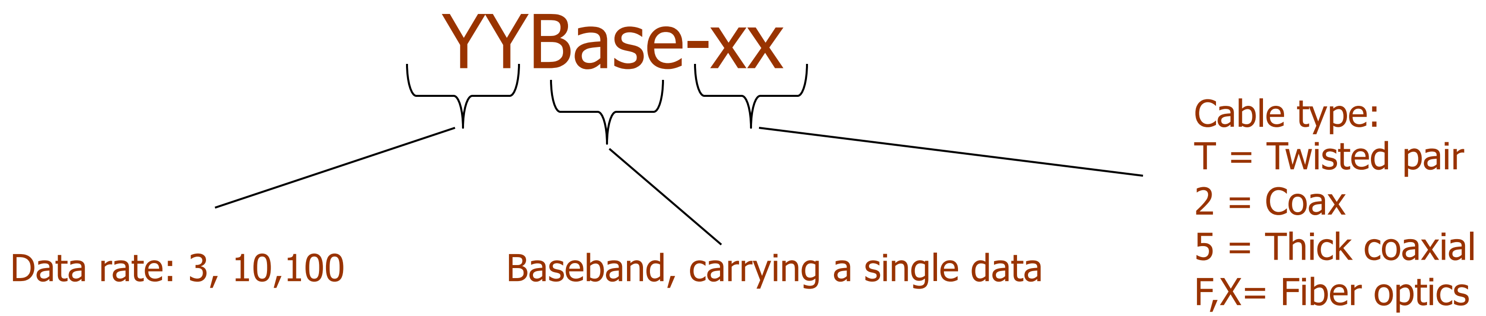
- Significant improvements have been made in the quality and shielding available in twisted pair cables
  - the data rate used on twisted pair Ethernet has increased (three types – above)
- Higher-speed Ethernet technologies use an electronic device known as a switch rather than a hub
- To remain backward compatible
  - standards for the higher-speed versions specify that interfaces automatically sense the speed at which a connection can operate
  - and slow down to accommodate older devices
  - For example, if one plugs an Ethernet cable between an old device that uses 10BaseT and a new device that uses 1000BaseT
    - the new device will autosense

Ethernet Specifications

- Ethernet classification

  < Speed> <Baseband/Broadband> <Physical>

- Speed: 3,10,100 Mbps depending on the cable type:
  - Baseband is typically used for small building
  - Broadband is used for larger networks such as Cable TV
- Cable Standards



10BASE-T

http://www.comptechdoc.org/independent/networking/cert/netphysical.html

Physical Interfaces

- Twisted Pair
  - Unshielded Twisted Pair (UTP). Normally UTP
  - Shielded twisted pair (STP) – e.g., Cat5E Shielded Twisted Pair
- Coaxial
  - RG-62 - 93 ohm, primarily used for ArcNet.
  - RG-59 - 75 ohm, for broadband transmission such as cable TV.
  - RG-58 /U - 50 ohm, with a solid copper wire core for thin Ethernet.
  - RG-58 A/U* - 50 ohm, with a stranded wire core.
  - RG-58 C/U* - Military version of RG-58 A/U.
  - RG-11 - 75 ohm thick Ethernet.
  - RG-8 - 50 ohm thick Ethernet.
  - RG-6 - Used for satellite cable (if you want to run a cable to a satellite!).
- Fiber-optic
  - expensive taps / better alternatives available / not used in bus LANs
  - Single mode cables for use with lasers and offer greater bandwidth and costs more
  - Multimode cables for use with Light Emitting Diode (LED) drivers

50 Ohms Cable - **RG58/U--50 Ohm**

"RG" was originally a unit indicator for bulk RF cable in the U.S. military

http://www.ciscopress.com/articles/article.asp?p=31276&seqNum=2

AWG Standards

American wire gauge (AWG)

Quantity of resistance

$$R = \rho \cdot \frac{l}{A}$$

R	= resistance	Ω
ρ	= specific resistance	Ω·m
l	= length of the cable	m
A	= cross section	m^2

metal	Electrical conductivity Electrical conductance	Electrical resistivity Specific resistance
copper	$\sigma = 58$	$\rho = 0.0172$
aluminium	$\sigma = 36$	$\rho = 0.0277$
Silver	$\sigma = 62$	$\rho = 0.0161$

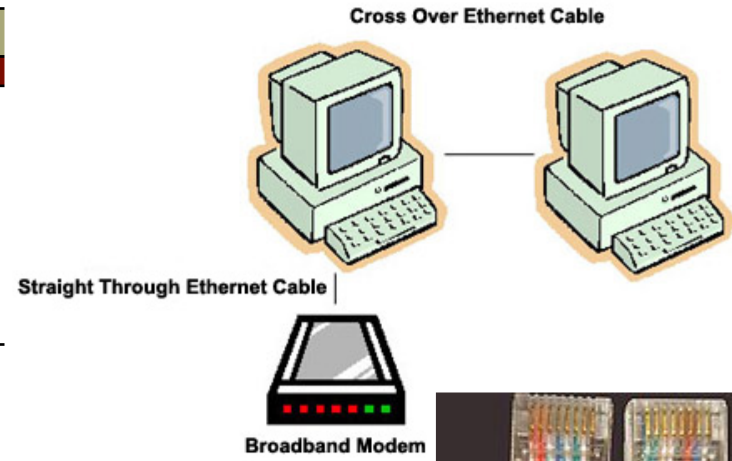
AWG Copper Wire Table

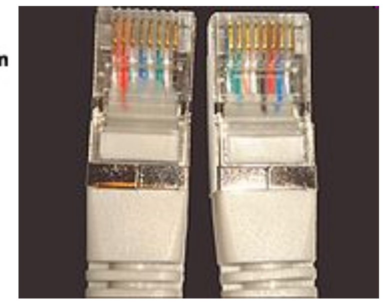
AWG	Diam. (mils)	Circular mils	Ohms/1000ft	Current Carrying	Fusing Current	Feet per Pound
0000	460	212000	0.050	-	-	1.56
000	410	168000	0.063	-	-	1.96
00	365	133000	0.077	-	-	2.4826
0	324.8	105531	0.096	-	-	3.1305
1	289.3	83694	0.126	119.6	-	3.947
2	257.6	66358	0.159	94.8	-	4.977
3	229.4	52624	0.200	75.2	-	6.276
4	204.3	41738	0.253	59.6	-	7.914
5	181.9	33088	0.391	47.3	-	9.980

Smaller

Higher
(less signal goes through)

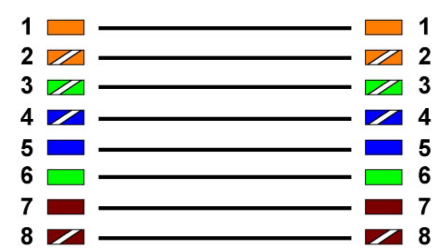
Ethernet Cables



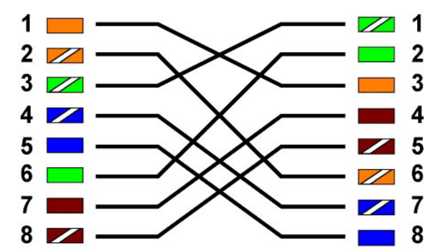


- Ethernet *Crossover* cable
  - Used to connect computing devices (PCs, two routers, or two hubs) together directly
  - Used to connect PC and router
  - Example: connecting two personal computers via their network adapters
- Ethernet Standard *straight through* cable
  - Each pin of the connector on one end is connected to the corresponding pin on the other connector.
  - used to connect a PC or Router or an Ethernet hub (connecting different equipments)
  - Exception: Connecting an uplink port of a hub to a regular port of another regular port of hub

EIA/TIA T568B Straight Through Diagram

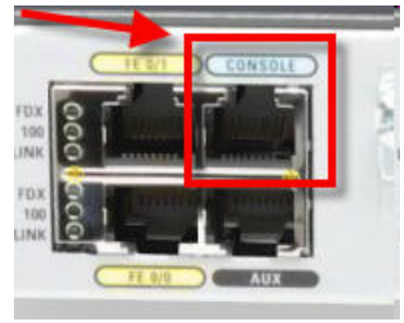


EIA/TIA T568B Crossover Diagram



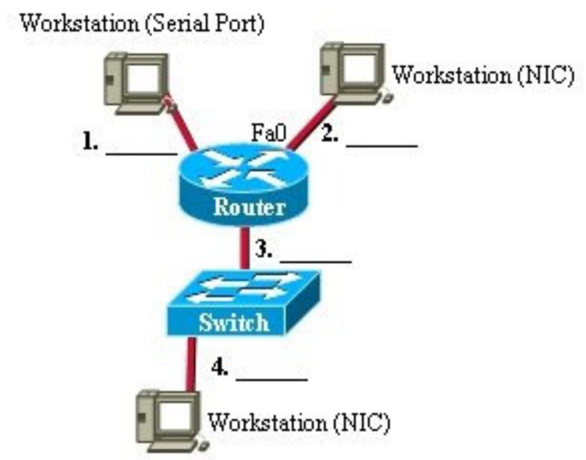
Wiring Serial Connection

- Asynchronous Serial Ports are used to access the console port of a router a PC– used to send ASCII characters
- The serial port is connected to a PC via RS-232 (DB-25 connector with 25 pins or DB-9 connector with 9 pins or RJ-45 with 8 pins – similar to the Ethernet cable)
- Rolled cable (rollover) is used to access the console port
  - Pin 1 → 8 and so on (all pins are rolled)



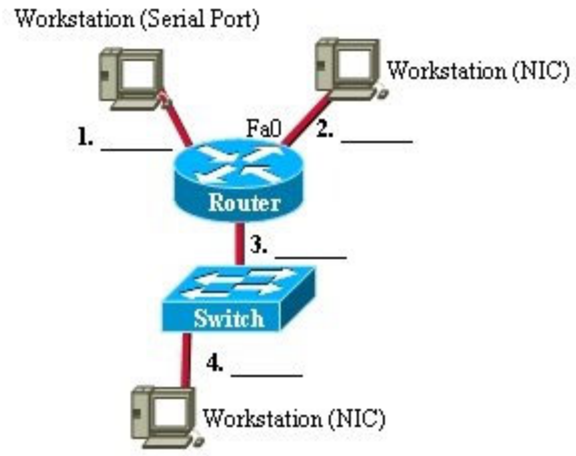
Example

- Which interface uses a crossover cable?
  - 1-?
  - 2-?
  - 3-?
  - 4-?



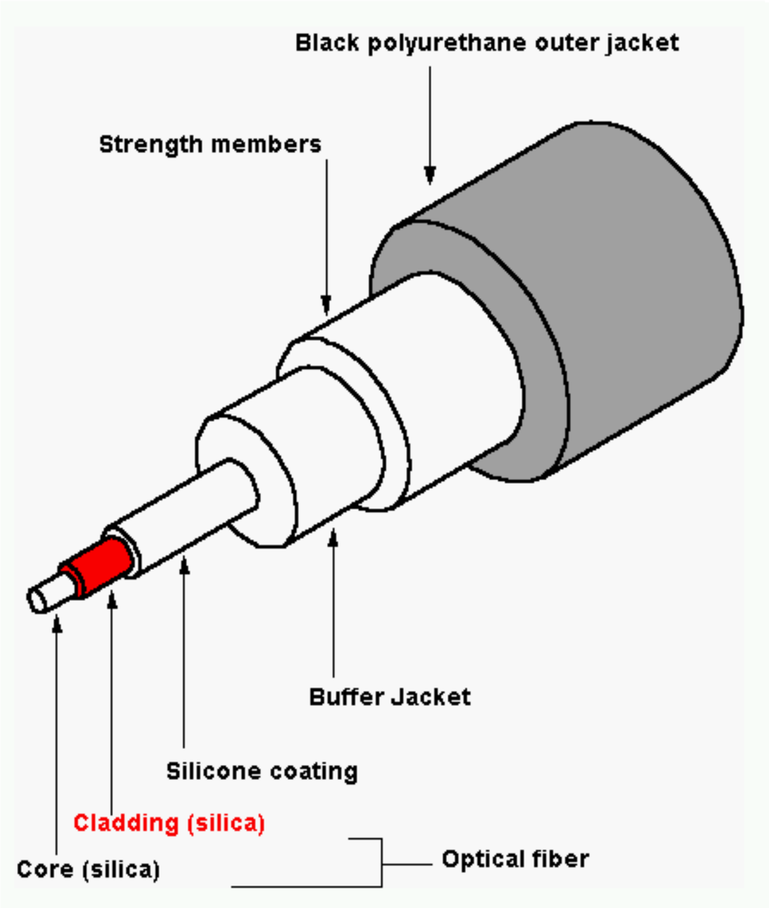
Example

- Which interface uses a crossover cable?
  - 1-Rolled cable
  - 2-Crossover cable
  - 3-Straight-through cable
  - 4-Straight-through cable



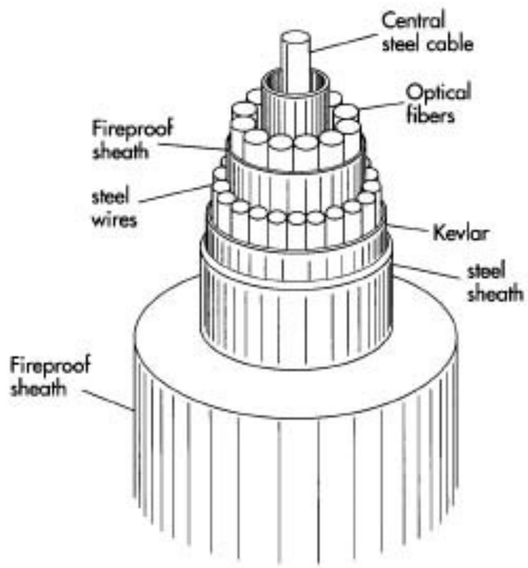
Fiber Optics Cable

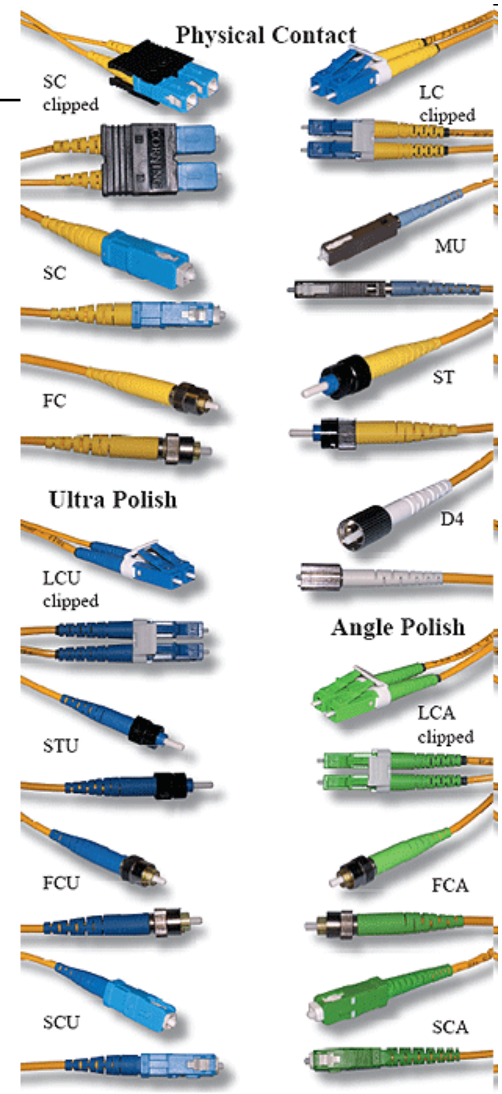
From Computer Desktop Encyclopedia



Optical Connections

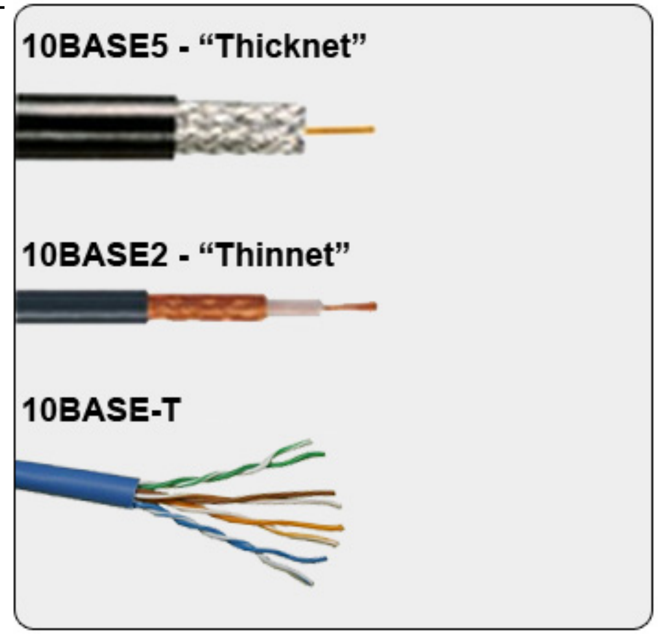
- Different physical contacts are used for optical fiber cables
- A typical optical fiber cable usually includes several optical fibers around a central steel cable.
- Various protective layers are applied, depending on the harshness of the environment where the cable will be situated.





Ethernet Cable Types (Examples)

- **10BASE-2**
  - Also known as "Thin Ethernet" or Thinnet, 10BASE-2 is an IEEE standard for baseband Ethernet at 10MBps over thick coaxial cable. 10Base2 has a maximum distance of 185 meters.
- **10BASE-5**
  - Also known as "Thick Ethernet" or Thicknet, 10BASE-5 is an IEEE standard for baseband Ethernet at 10MBps over thick coaxial cable. 10BASE-5 has a maximum distance of 500 meters.
- **10BASE-T**
  - Similar to the standard telephone cabling, 10BASE-T is a 10MBps CSMA/CD Ethernet LAN that works on Category 3 or better twisted-pair cables capable of being 100 meters long.
- **100BASE-T / Fast Ethernet / 100BASE-TX (or 802.3u)**
  - Fast Ethernet is also referred to as 100BASE-T or 802.3u and is a communications protocol that enables computers on a local-area network to share information with one another at rates of 100 million bits per second instead of the standard 10 million BPS. Fast Ethernet works over Category 5 twisted-pair wiring.

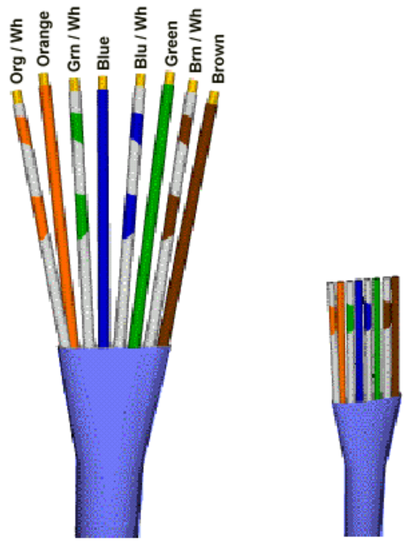


Cable type:
T = Twisted pair
2 = Coax
5 = Thick coaxial
F,X= Fiber optics

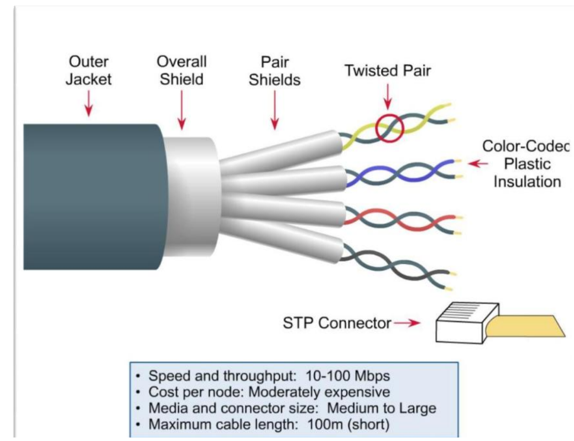
100BASE-TX is the predominant form of Fast Ethernet, and runs over two wire-pairs inside a category 5 or above cable (a typical category 5 cable contains 4 pairs and can therefore support two 100BASE-TX links)

Common Ethernet Speeds: 10BaseT Ethernet; Fast Ethernet; GigE

STP vs UTP



Cat 5 (UTP) Un-Shielded Twisted Pair



Shielded Twisted Pair

Fast Ethernet - IEEE 802.3u

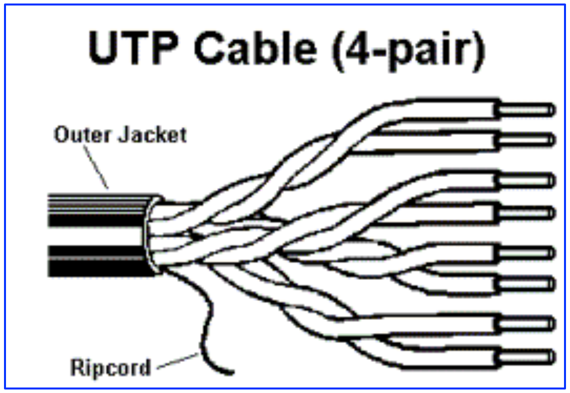
- In 1995 a committee was established to develop standards for faster LAN
  - Backward compatible
  - 10 nsec bit time (100 Mbit/sec)
- Interesting properties
- Three signal levels : +V, 0, -V
- Codewords are selected such that line is d.c.balanced
  ➔ all codewords have a combined weight of 0 or 1.

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Common Ethernet Speeds: 10BaseT Ethernet; Fast Ethernet; GigE

Gigabit Ethernet – 802.3z

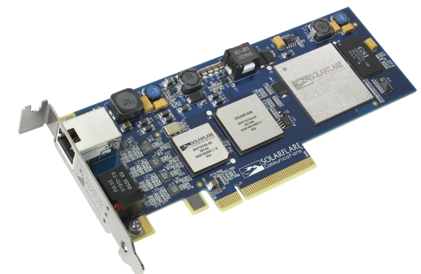
- Started in 1998 following formation of a High-Speed Study Group to study convening packets in Ethernet format at Gbps speed
  - Used to interface lower-speed Ethernets (LANs)
  - Suitable for streaming HD and multimedia
  - Backward compatible
- Compatible with Fast Ethernet
  - Using similar CDMA/CD frame format and MAC protocol
  - Point-to-point only (not multipoint)
  - Supports Full duplex & half duplex



Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

Good Summary: http://www.infocellar.com/networks/standards/ethernet.htm

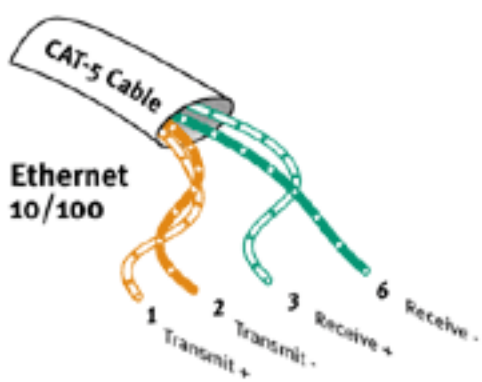
10G Ethernet



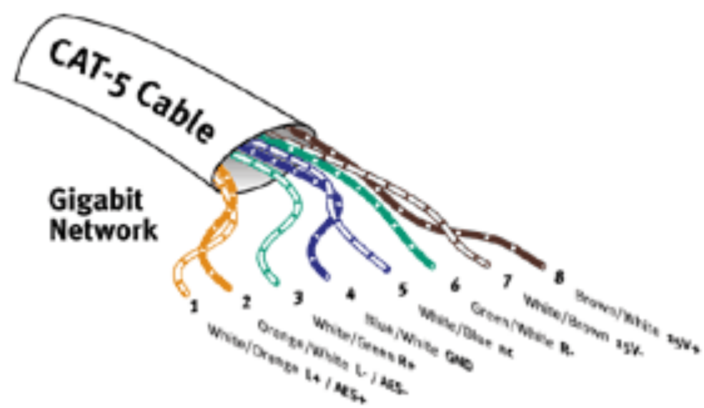
- Operates at 10G
- Several IEEE standards, including:
  - 802.3ae-2002 (fiber -SR, -LR, -ER, etc.)
    - SR: Short Reach; LR: Long Reach; ER: Extended Reach; LX: Fiber;
  - 802.3ak-2004 (-CX4 copper cable)
  - 802.3an-2006 (10GBASE-T copper twisted pair),

2-Pair & 4-Pair CAT 5

- Ethernet 10Base-T uses pairs 2 and 3 (pins 1-2, 3-6)
- Ethernet 100Base-T4 uses pairs 2 and 3 (pins 1-2, 3-6) – using 4 wires
- Ethernet 100Base-T8 uses pairs 1,2,3 and 4 (pins 4-5, 1-2, 3-6, 7-8) – using 8 wires
- GigE 1000Base-TX uses pairs 1,2,3 and 4 (pins 4-5, 1-2, 3-6, 7-8) – using 8 wires



Differential TX & RX



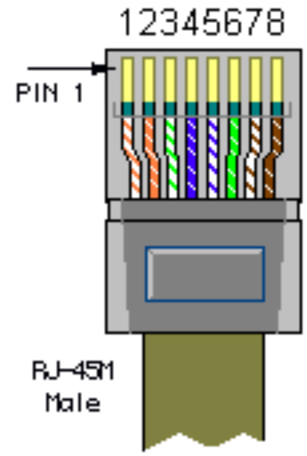
Differential TX & RX
Including +/- 15V and GND

RJ-45 Pinout

Crossover Cable	
RJ-45 PIN	**RJ-45 PIN**
1 Rx+	3 Tx+
2 Rc-	6 Tx-
3 Tx+	1 Rc+
6 Tx-	2 Rc-

1-orange/white
2-orange
3-green/white
4-blue
5-blue/white
6-green
7-brown/white
8-brown

Straight Through Cable	
RJ-45 PIN	**RJ-45 PIN**
1 Tx+	1 Rc+
2 Tx-	2 Rc-
3 Rc+	3 Tx+
6 Rc-	6 Tx-



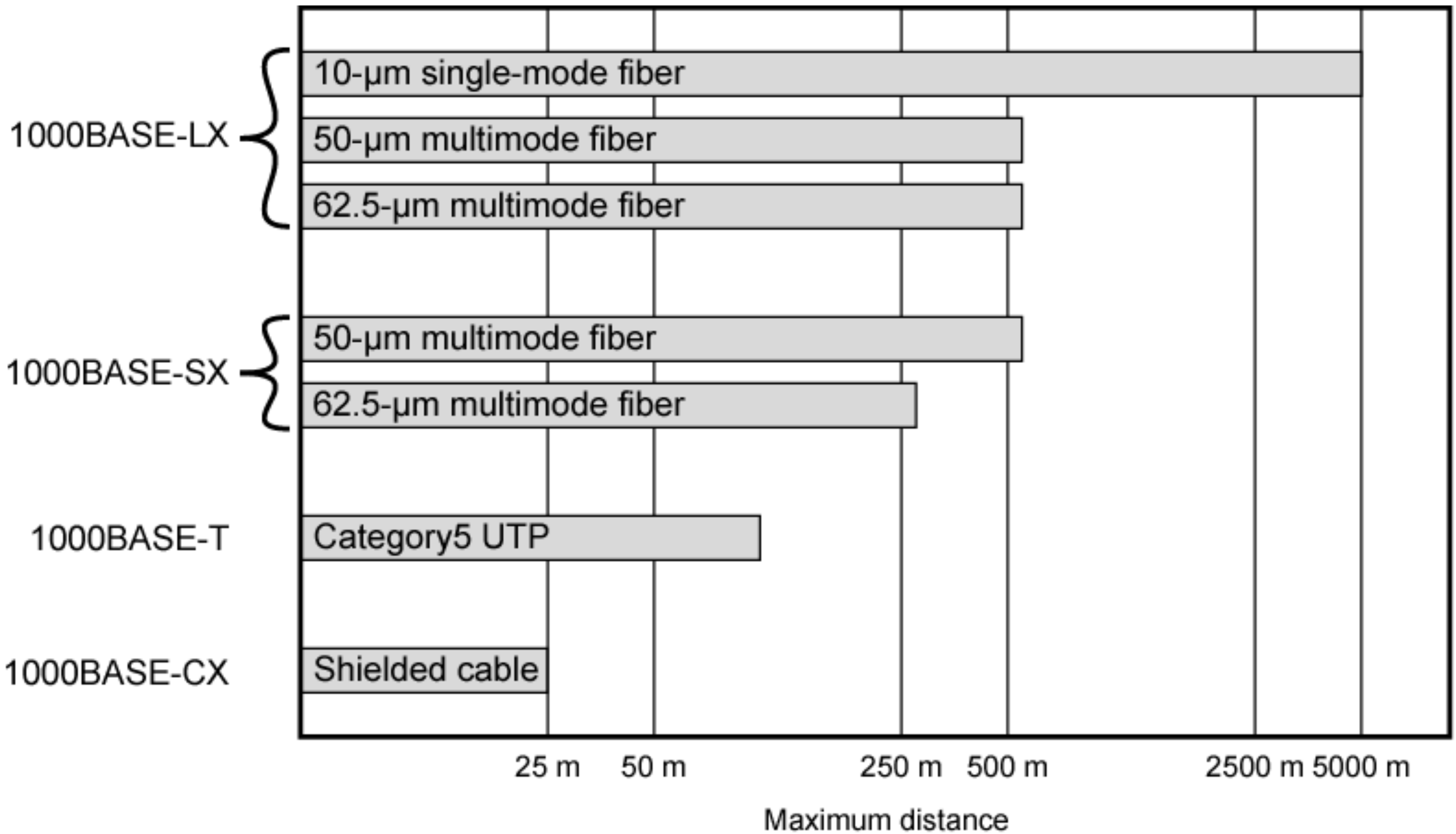
Physical Media Comparisons

Cable Category	Speed	Notes
1	None	Used for old telephone systems
2	4Mps	
3	10Mps	The minimum category for data networks
4	16Mps	
5	100Mps	Cat 5 network cable, used by most networks today
6		Data patch, Two pair with foil and braided shield
7		Undefined
8		Flat cable for under carpets with two twisted pair
9		Plenum cable with two twisted pair. It is safe if you're having a fire.

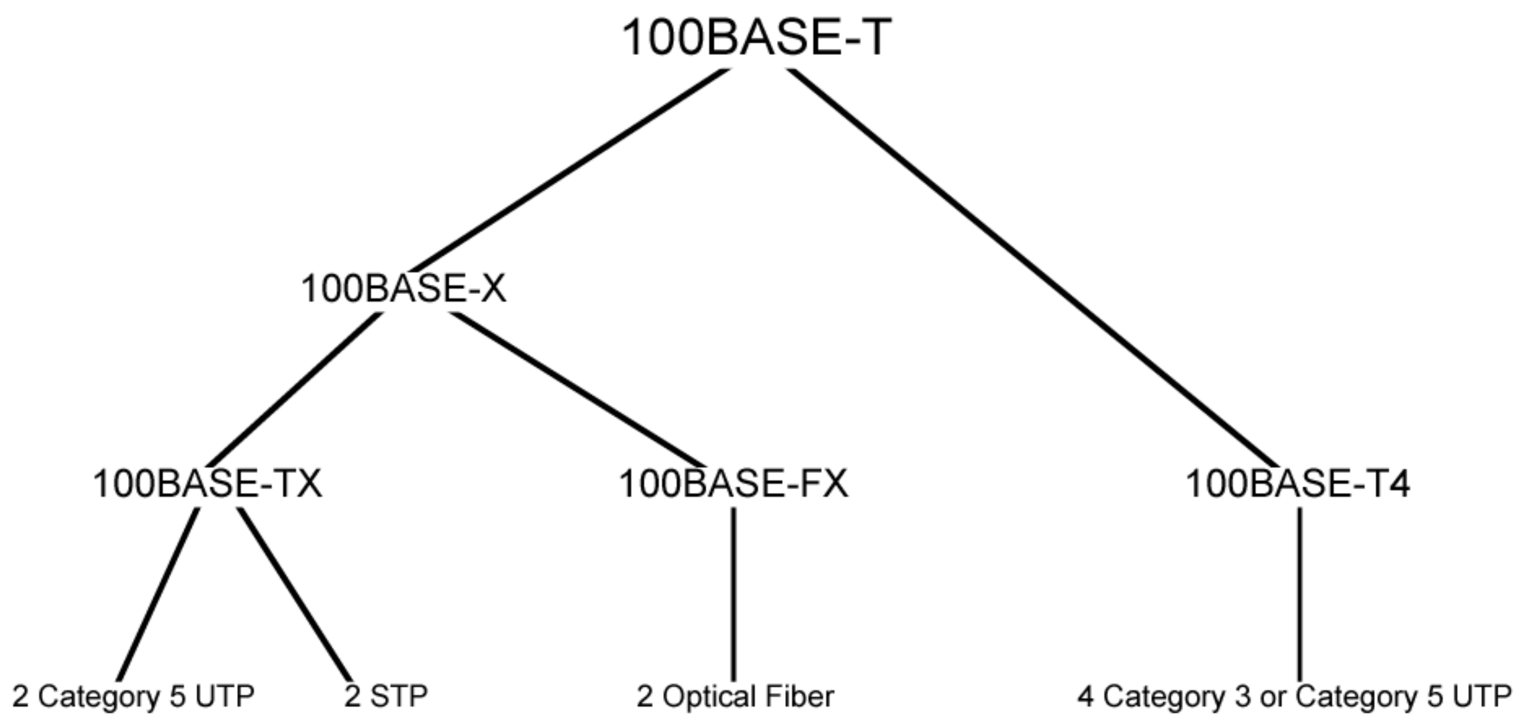
Media	Distance (meters)	Speed
UTP	100	4-100Mbps
STP	100	16-155Mbps
Thinnet	185	10Mbps
Thicknet	500	10Mbps
Fiber	2000	100Mbps-2Gbps

The Electronic Industries Association and Telecommunications Industries Association (EIA/TIA) defined a standard called EIA/TIA 568 which is a commercial building wiring standard. It defines transmission speed and twists per foot.

Gbit Ethernet Medium Options (log scale)



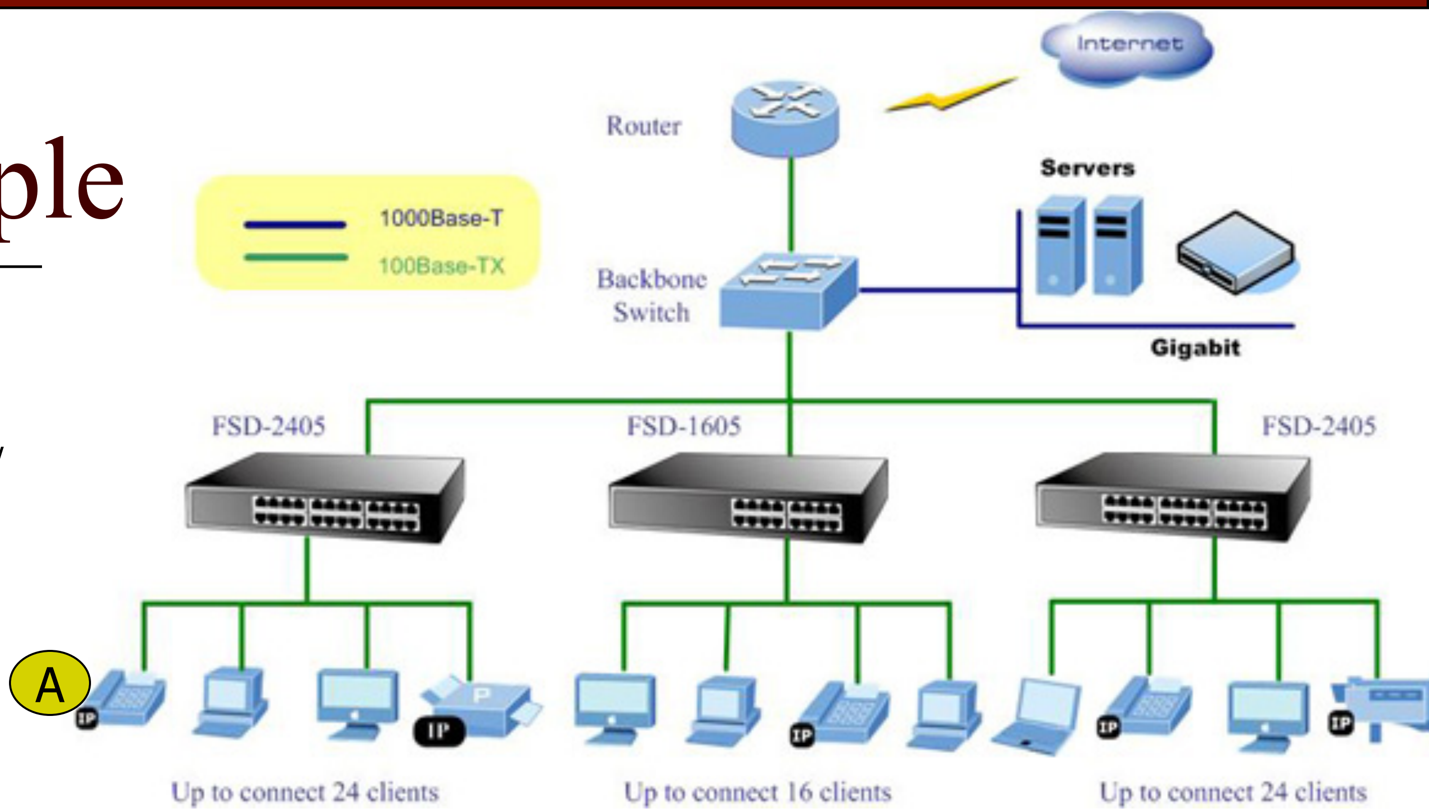
100BASE-T Options



100BASE-TX: two pairs of high-quality twisted-pair wires
100BASE-T4: four pairs of normal-quality twisted-pair wires
100BASE-FX: fiber optic cables

Example

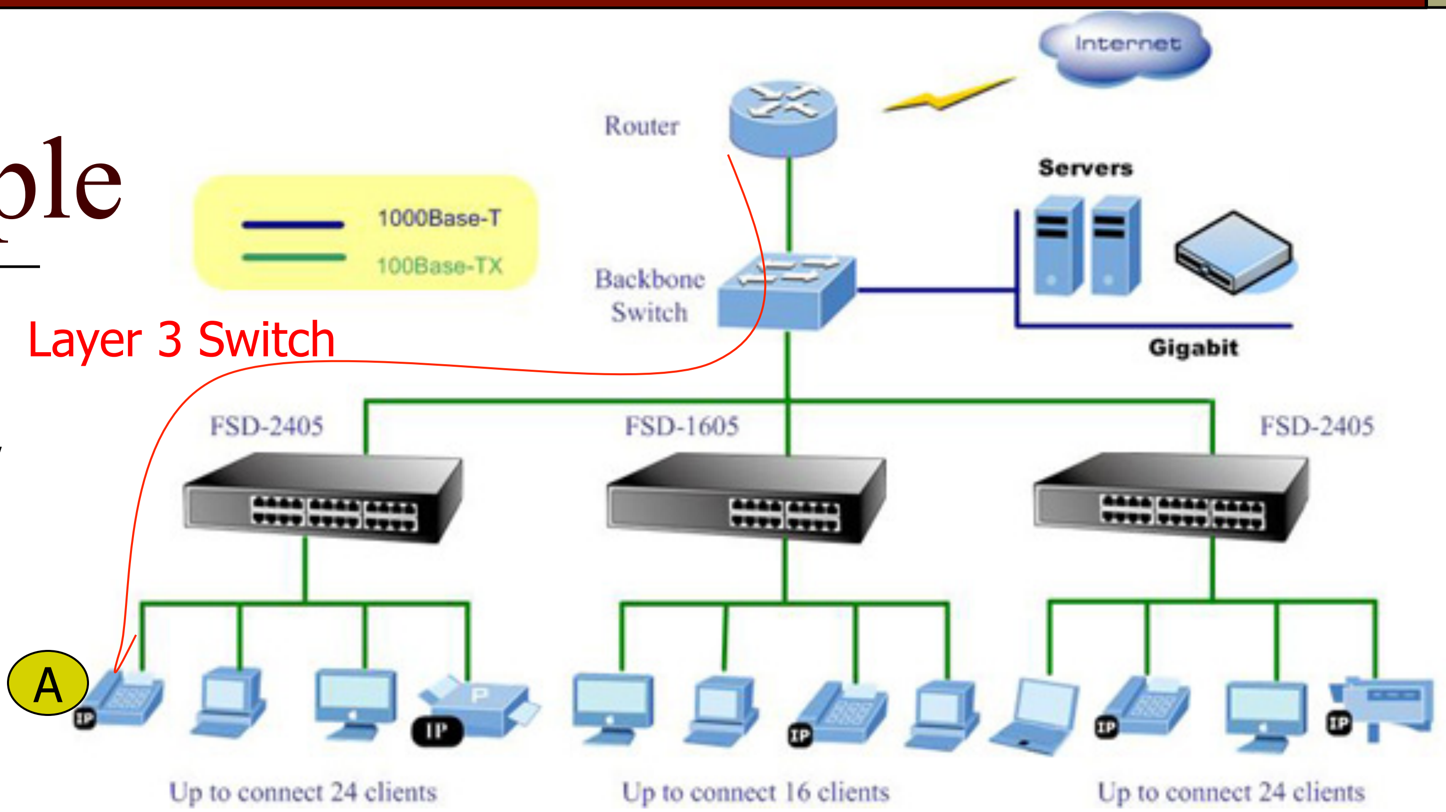
High-Speed 10/100Mbps Workgroup Switch
The PLANET FSD-1605 / FSD-2405 is a 10/100Mbps Fast Ethernet Switch with 16 / 24 ports



Questions:
What rate can 1000Base-T handle?
What type of an Ethernet Switch is the Backbone Switch?
What type of cable will you use to connect to clients?
What type of cable would you use to connect to the servers?
How many total number of clients can be supported?
Show the route for a packet entering the router with destination A
Assuming no more FSDs can be added, can you support 100 clients? Explain!

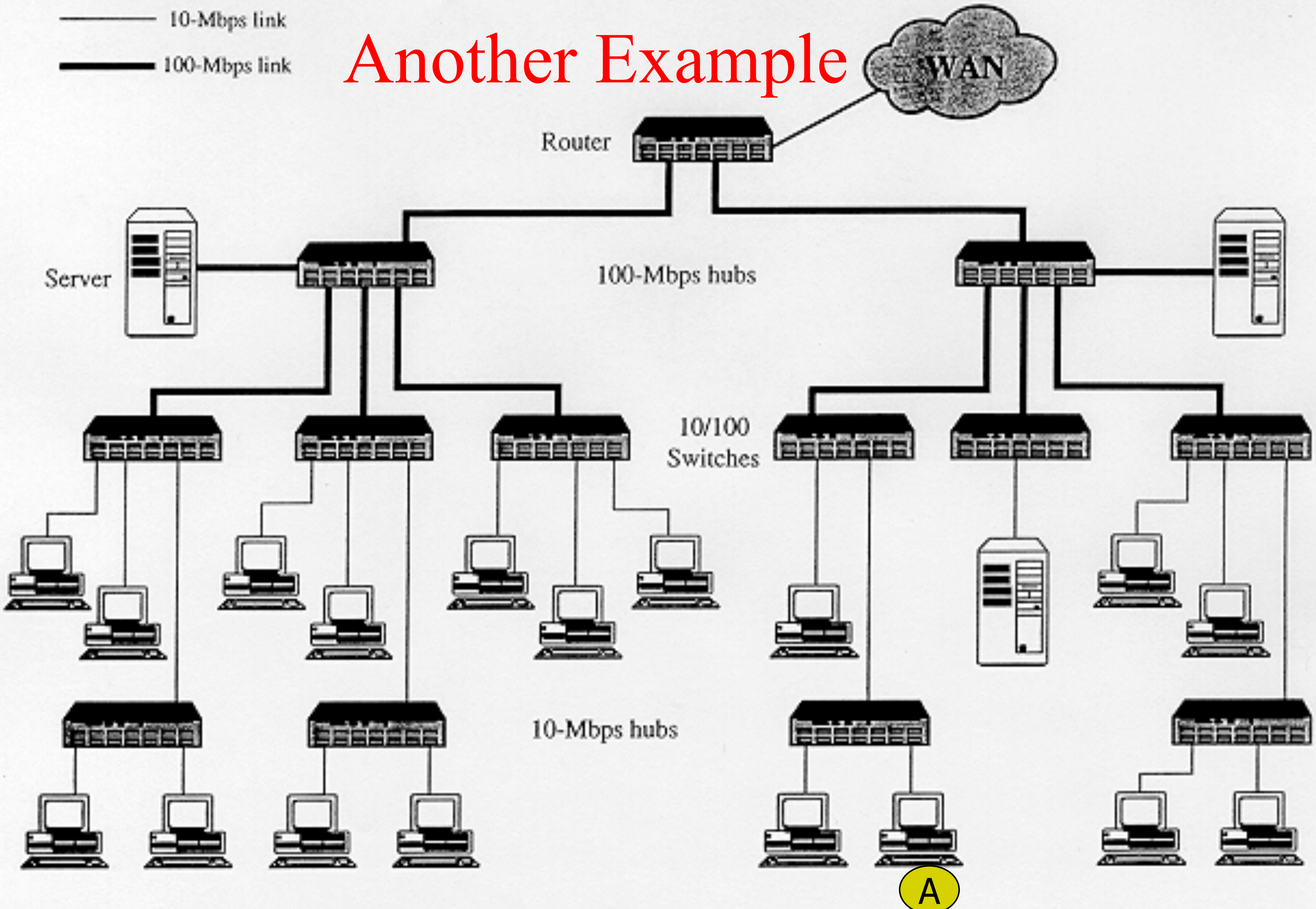
Example

High-Speed 10/100Mbps Workgroup Switch
The PLANET FSD-1605 / FSD-2405 is a 10/100Mbps Fast Ethernet Switch with 16 / 24 ports



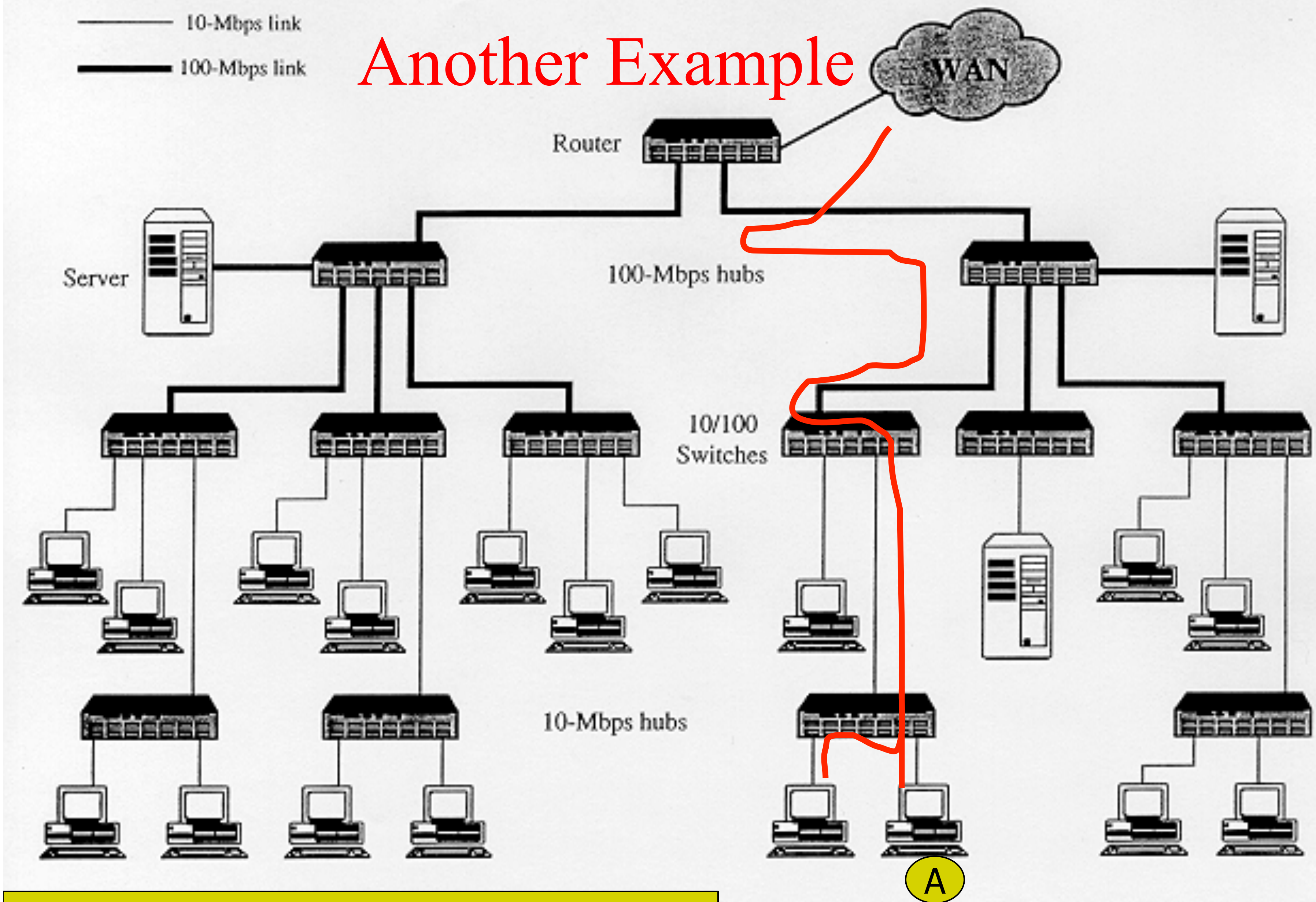
Questions:
What rate can 1000Base-T handle? – 1 Gig bits per sec
What type of an Ethernet Switch is the Backbone Switch? – Fast Ethernet
What type of cable will you use to connect to clients? – Two Cat 5 UTP or 2 STP (100Base-TX)
What type of cable would you use to connect to the servers? – 2 Cat 5 / UTP
How many total number of clients can be supported? - 64
Show the route for a packet entering the router with destination A – shown above
Assuming no more FSDs can be added, can you support 100 clients? Explain! → Fairness and system utilizations must be considered as we add more new hubs to support more clients.

Another Example



Backbone Example

Another Example



Backbone Example

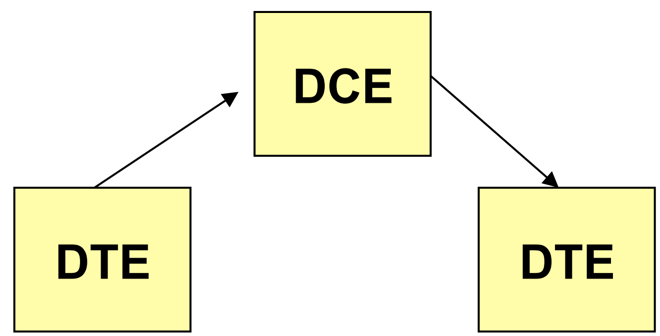
Layer 2 hub

Devices

Data Communication Equipments

- Used to transport information over the network
- Perform data formatting, routing, transporting, and ensure to maintain data integrity
- Examples: Routers, Switches, Bridges
- Differ in terms of cost, size, carries class (reliability or uptime requirement)

A generic Point-to-point system



DTE (Data Terminating Equipment)
-e.g., PC, Mainframe,
where signal ends
DCE (Data Communications Equipment)
-T1, POTS, ISDN

Switching Equipment

- Network Switching
  - Different/same networks
  - Example: Routers, Gateways, etc.
- LAN Switching
  - Different/same Segments (collision domains)
  - Layer 2 switch, Repeater), Hub, etc.

A Different View: LAN Switching Technologies

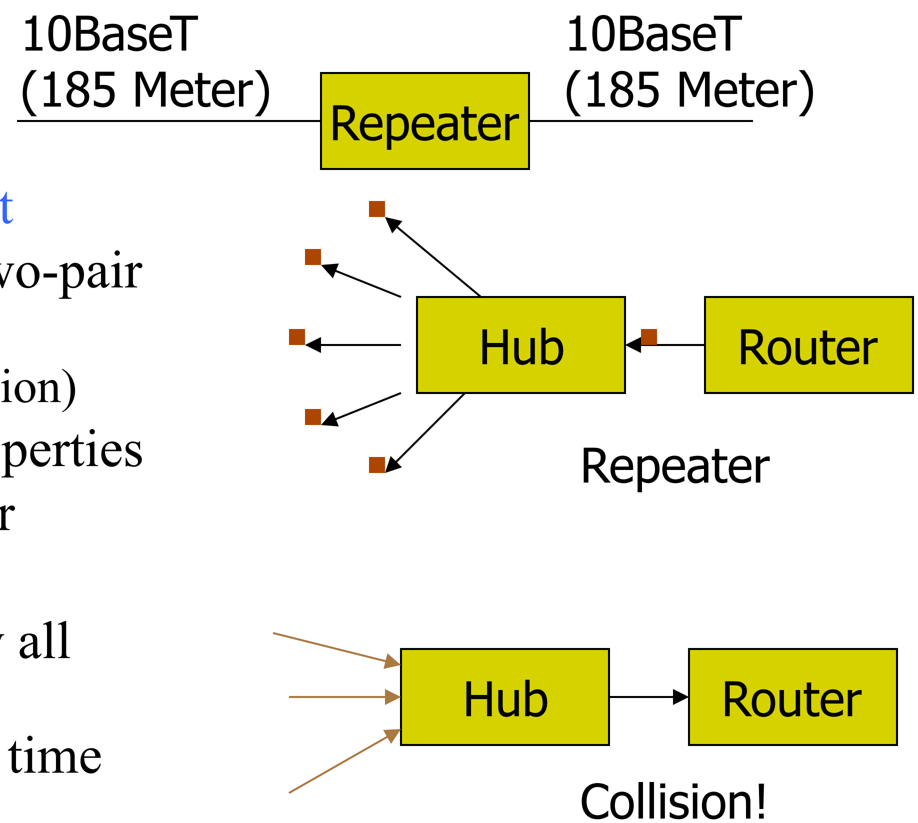
- LAN Switching involves packet switching in LAN
- Different technologies
  - Speed, Addressing, Utilization, etc.
- Layer 1 switching – just blindly copying the packet
  - Pass-through devices
  - Considered to be analog
  - Example is a hub or repeater
- Layer 2 switching is hardware-based switching
  - Uses the media access control address (MAC address) from the host's network interface cards (NICs) to decide where to forward
  - Allows dividing the LAN into multiple Segments
  - Typically uses 80/20 rule (80 percent of the traffic is local)
  - Not all bridges support multicasting and broadcasting
  - Example: Multiport Bridge (Layer 2 Switch)

Interconnecting LANs

- In many scenarios we need larger LANs
  - Connecting similar LANs
  - Creating longer LANs
- Interconnecting using repeaters, bridges, or routers

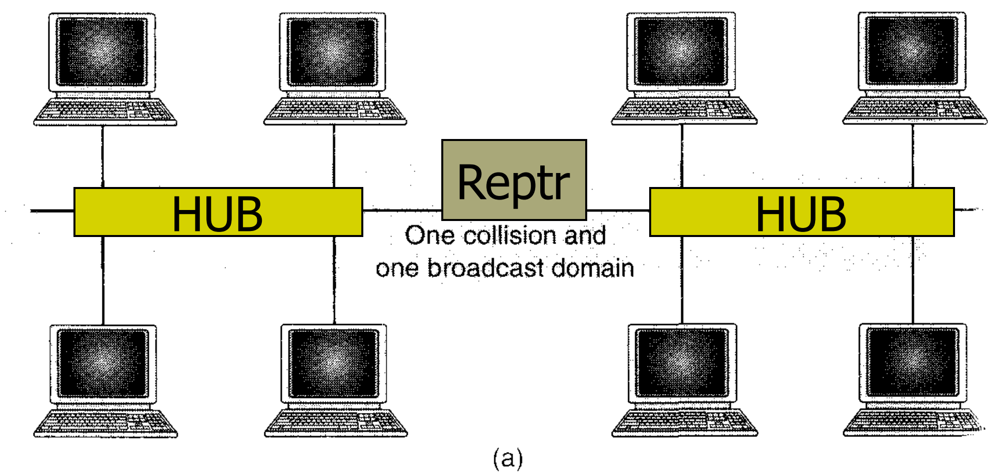
Layer 1 LAN Devices

- Repeaters
  - Boosts the signal (layer 1 operation)
  - Transparent to the signal
- Hub
  - active central element of star layout
  - each station connected to hub by two-pair UTP lines
  - hub acts as a repeater (layer 1 operation)
  - limited to about 100 m by UTP properties
  - optical fiber may be used for longer
  - physically star, logically bus
  - transmission from a station seen by all others
  - if two stations transmit at the same time have a collision

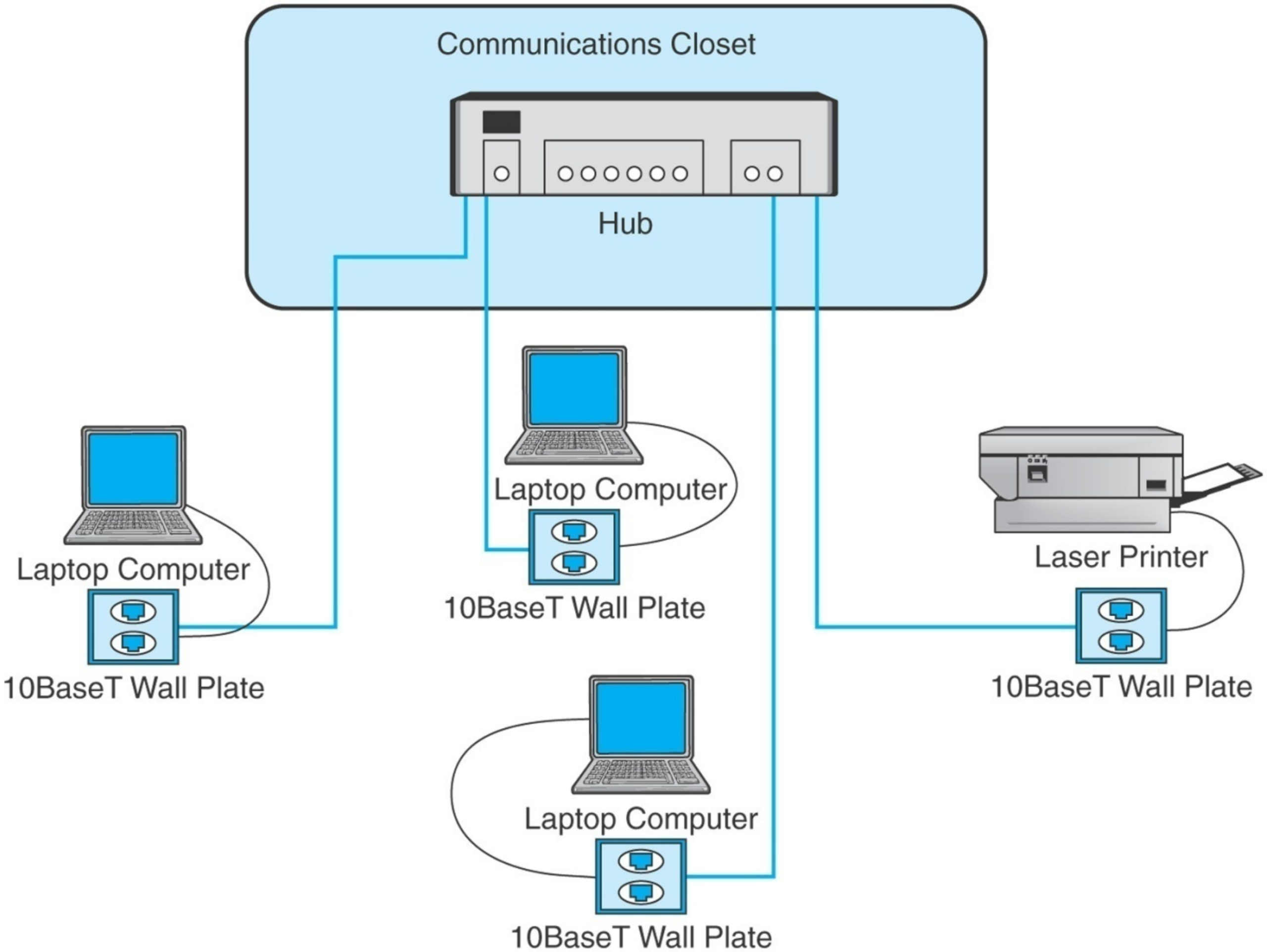


Hub and Repeaters

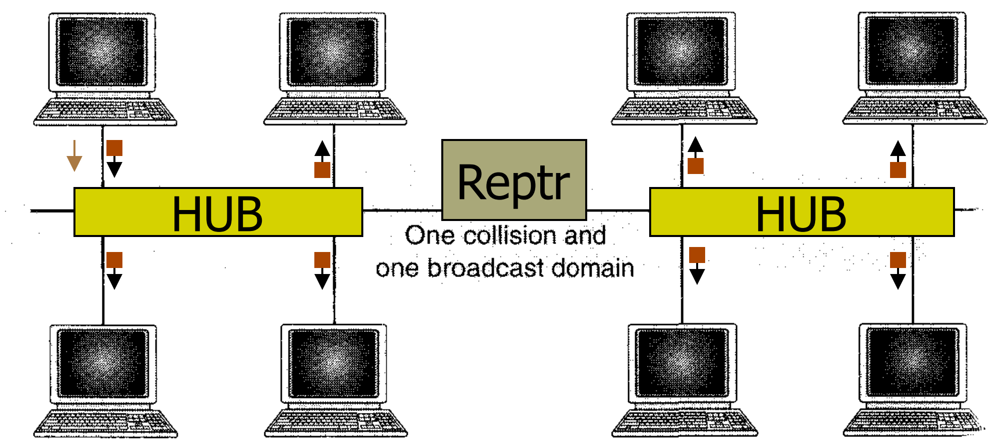
Single Collision/Broadcast Domain



Hub Stack Configuration


Communications Closet
Hub
Laptop Computer
10BaseT Wall Plate
Laptop Computer
10BaseT Wall Plate
Laser Printer
10BaseT Wall Plate
Laptop Computer
10BaseT Wall Plate

Hub and Repeaters

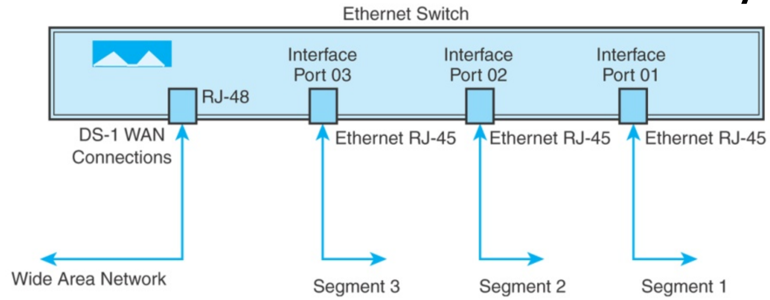


(a)

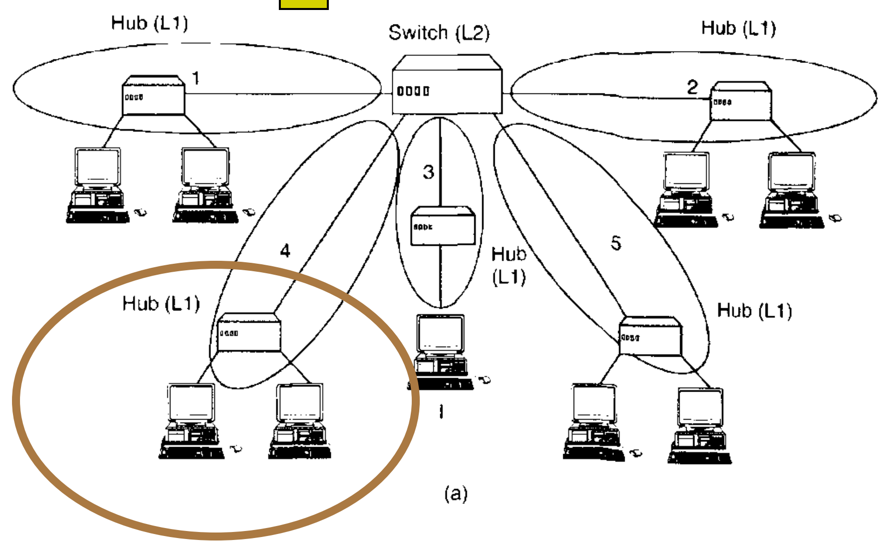
Hub Stack Configuration

Layer 2 Switch

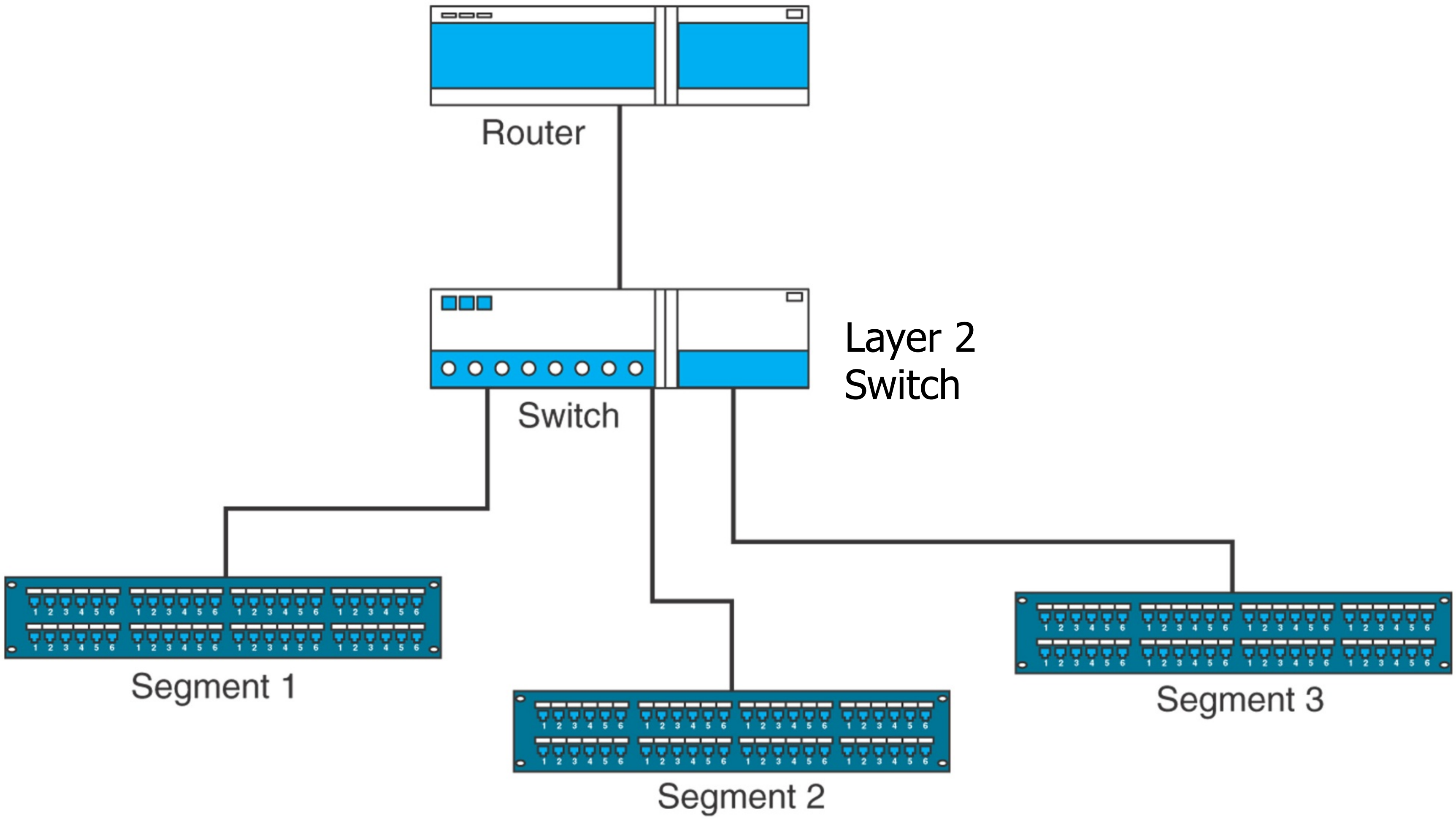
Cisco's Catalyst Switch



- An Ethernet switch, sometimes called a Layer 2 switch is an electronic device that resembles a hub
  - a switch provides multiple ports that each attach to a single computer
  - and a switch allows computers to send frames to one another
- The difference between a hub and a switch arises from the way the devices operate:
  - a hub operates as an analog device that forwards signals among computers
  - while a switch is a digital device that forwards packets
  - We can think of a hub as simulating a shared transmission medium
  - We think of a switch as simulating a **bridged** network that has one computer per LAN segment



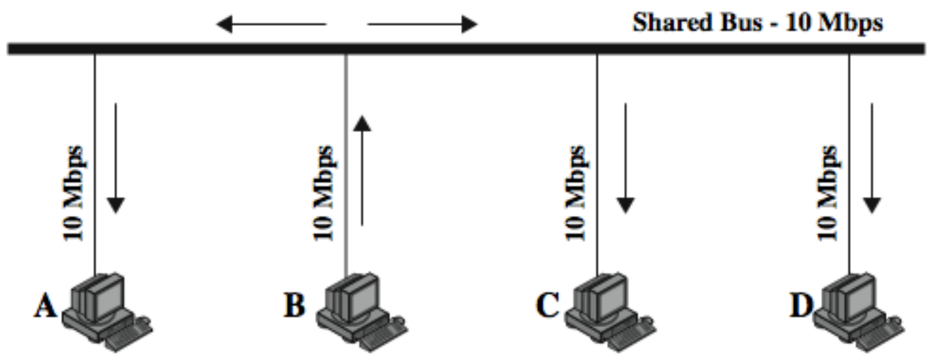
As before



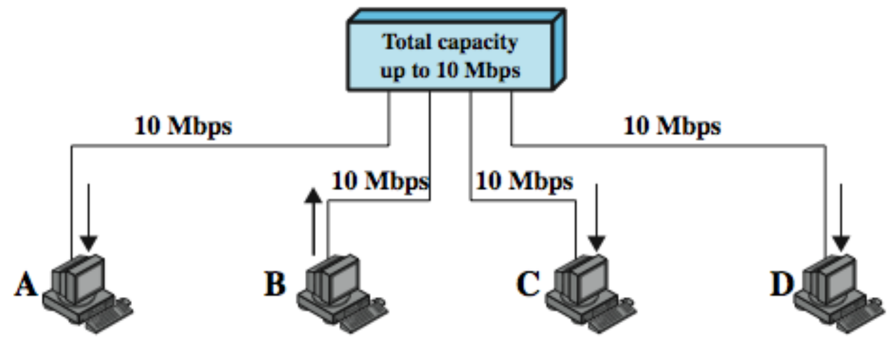
Router
Switch
Layer 2
Switch
Segment 1
Segment 2
Segment 3

Capacity

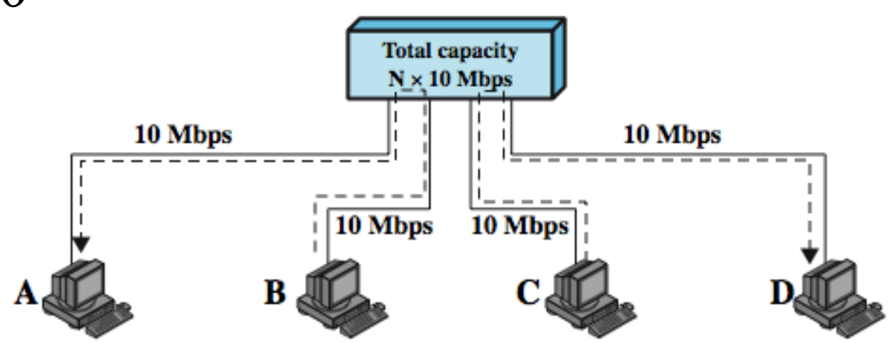
- HUB uses star wiring to attach stations
  - transmission from any station received by hub and retransmitted on all outgoing lines
  - only one station can transmit at a time
  - total capacity of LAN is 10 Mbps



(a) Shared medium bus



(b) Shared medium hub

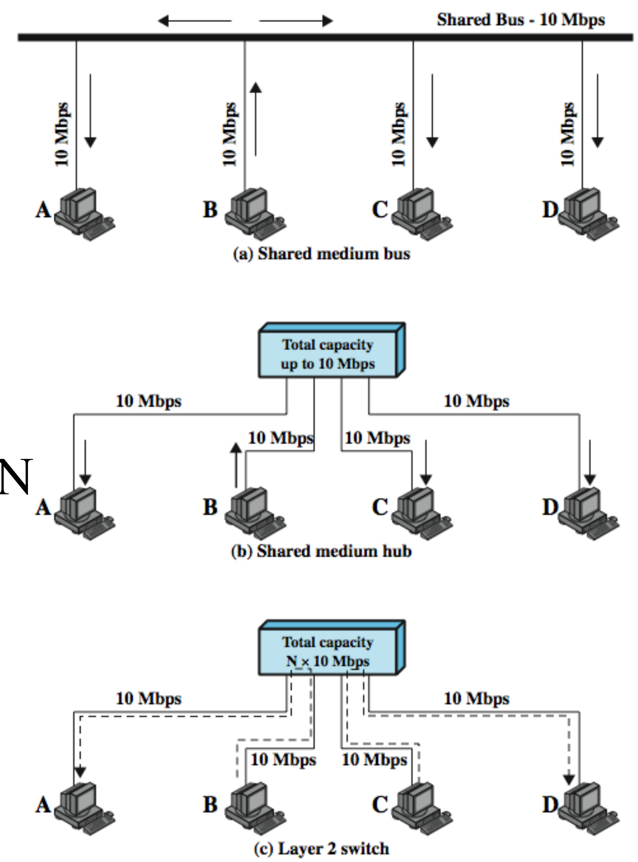


(c) Layer 2 switch

Compare the traffic capacity of a hub and a switch

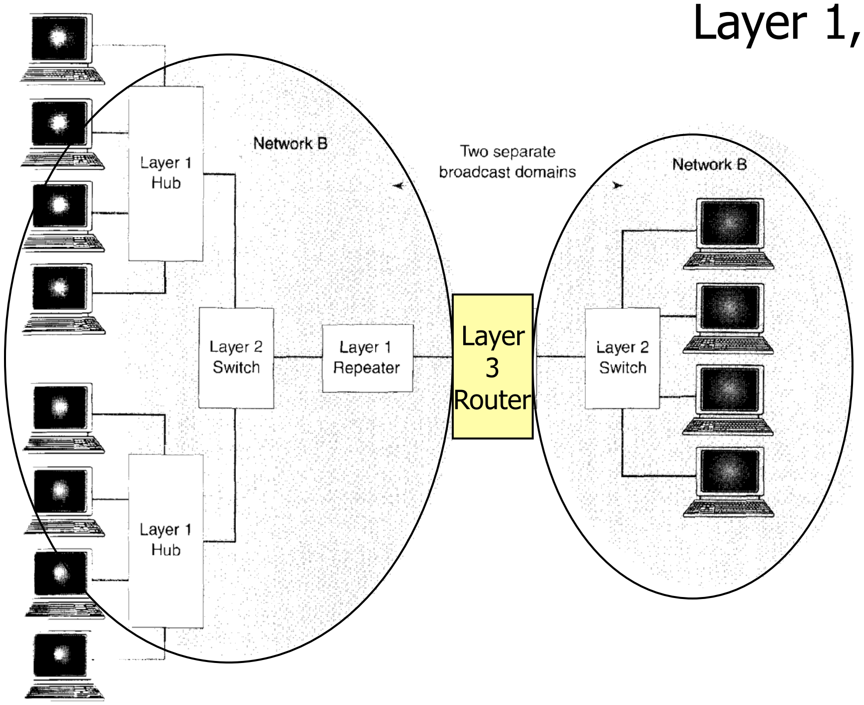
Capacity of Layer 2 Switch

- HUB can improve performance using a layer 2 switch
  - can switch multiple frames between separate ports
  - multiplying capacity of LAN
  - Hardware-based addressing
- Layer 2 switches can convert bus LAN or hub LAN to switched LAN
  - e.g. Ethernet LANs use Ethernet MAC protocol
- Layer 2 switches have dedicated capacity equal to original LAN
  - assuming switch has sufficient capacity to keep up with all devices
- Layer 2 switches scale easily
  - additional devices attached to switch by increasing capacity of layer 2

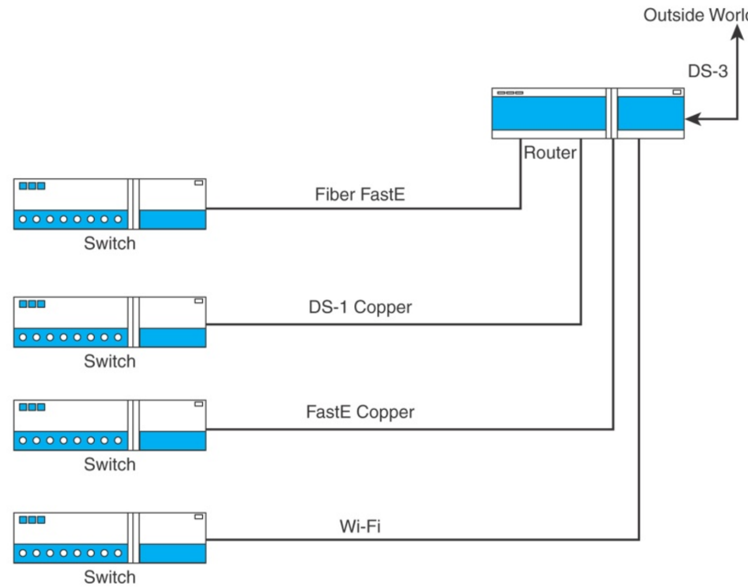


Interconnection Between Different Networks

Layer 1, 2, and 3



Routers



- Handles layer 2 and 3 operations (complex)
- Cracks packets to check their destinations
- Performs load balancing
- Detects failure and performs dynamic routing
- Provided traffic statistics
- Support different interfaces: OC, 56 Kbps, Ethernet, DS3, etc.
- Exchanges routing information
- Routers have their own address
- Require lots of memory
- Uses discovery protocols to find all neighboring nodes
- Types
  - Intermediate routers: Connecting two LANS - Translating packet from one LAN to another (Ethernet Frame to Token Ring Frame)
  - Gateway Routers: Connecting a LAN to the Internet

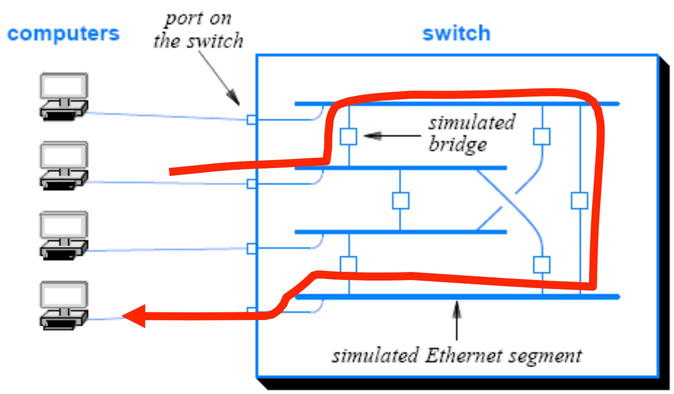
Bridging Devices

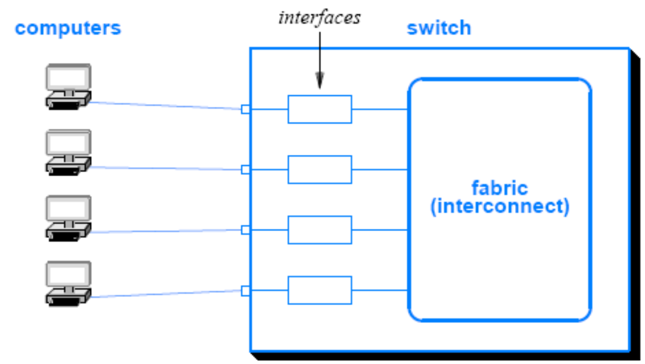
- Bridging allows connecting identical physical / link layer protocols
  - minimal processing
  - can map between MAC formats
  - reasons for use
    - Reliability – partitioning the network
    - Performance – smaller LANs perform better
    - Security – supporting different traffic types by each LAN
    - Geography – separated

In order to handle layer 2 routing, bridging must include ways to discover which devices are connected together & and how to forward

- Bridge operation
  - Used to connect two/more LANS
  - Less sophisticated than routers
  - Separates different segments
  - Its routing protocol architecture is based on 802.1D
  - More intelligent than repeaters (operates digitally)
  - Connect layer 2 segments
    - Handles layer 2 functionalities only
    - Transparent to layer 3
  - Uses polling and discovery packets
    - What is your MAC address again?
    - Establishes a tree-system

Conceptual use of bridges in a switch



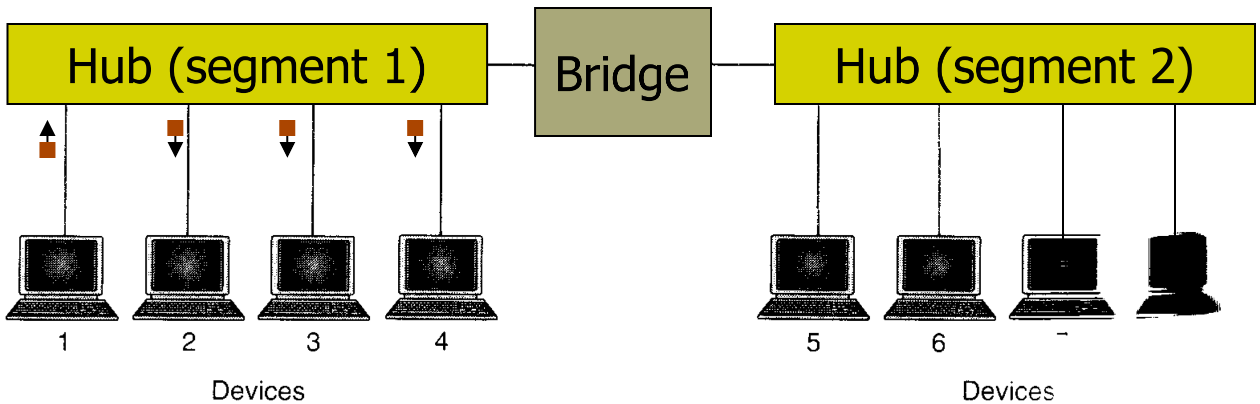


A switch consists of an intelligent interface attached to each port and a central fabric that provides simultaneous transfers

An interface contains a processor, memory, and other hardware needed to accept a packet consult a forwarding table and send the packet across the fabric to the correct output port

An interface can buffer arriving packets when an output port is busy

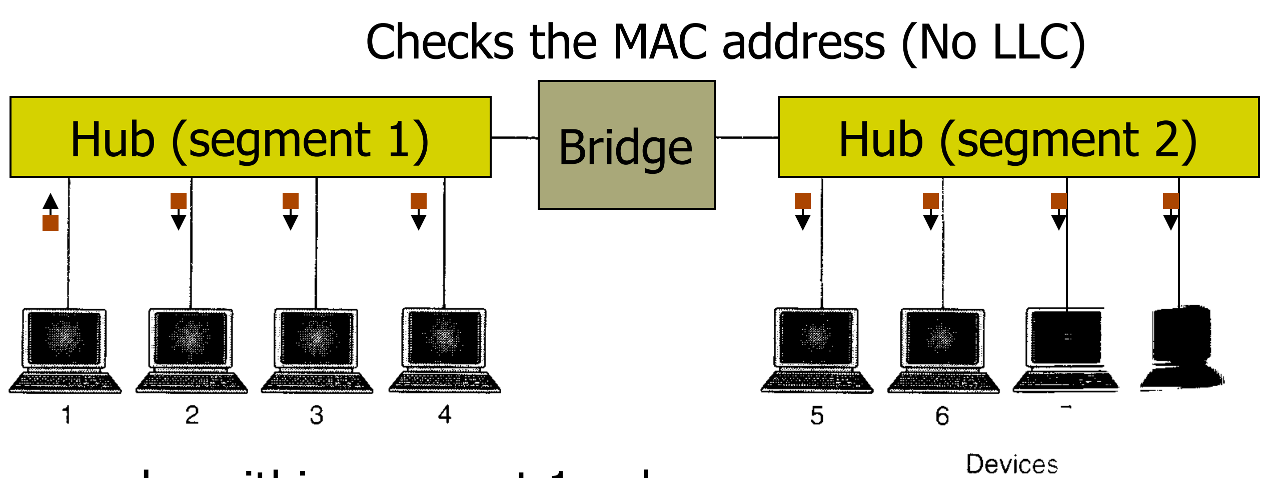
Bridge Operation



(a)

The transmission can be within segment 1 only
Or flooded between segment 1 and 2

Bridge Operation



The transmission can be within segment 1 only
Or flooded between segment 1 and 2

Remember: bridge uses MAC addresses to perform filtering – layer 2 switch

Bridge Design

- the bridge listens in promiscuous mode on each segment
  - i.e., receives all packets sent on the segment
- no modification to frame content or format
- no encapsulation
- exact bitwise copy of frame
- minimal buffering to meet peak demand
- contains routing and address intelligence
- may connect more than two LANs
- bridging is transparent to stations (Cut-through)

Bridges and Frame Filtering

- Bridges do not blindly forward a copy of each frame from one LAN to another
  - Instead, a bridge uses MAC addresses to perform filtering – layer 2 switch
- A bridge examines the destination address in a frame
  - and does not forward the frame onto the other LAN segment unless necessary
- If the LAN supports broadcast or multicast
  - the bridge must forward a copy of each broadcast or multicast frame
    - to make the bridged LAN operate like a single LAN

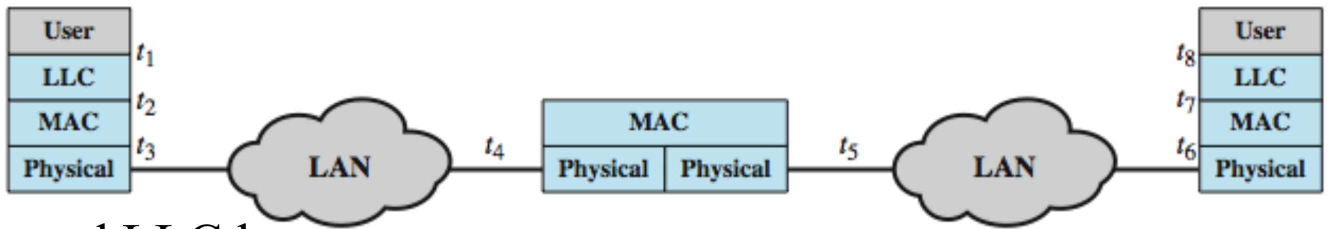
About Routing Protocols

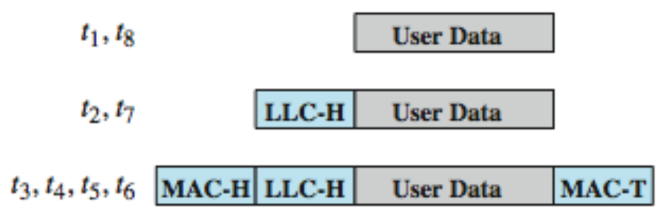
- How can a bridge know which computers are attached to which segments?
  - Most bridges are called adaptive or learning bridges
    - because they learn the locations of computers automatically
  - To do so, a bridge uses source addresses

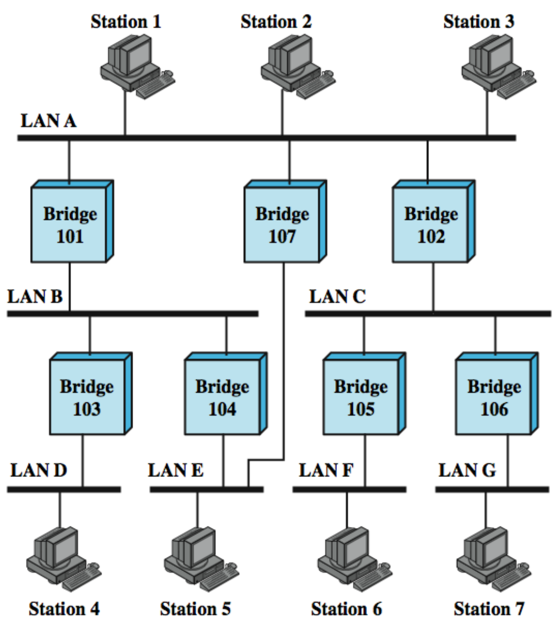
Here is how….

Bridge Protocol Architecture

- IEEE 802.1D
- MAC level
- Bridge does not need LLC layer







Bridges and LANs with Alternative Routes

Bridge Protocol Architecture

- Bridges must have some routing capacity
  - Must know the topology
  - Capable of changing the routing when changes occur
  - Route based on the MAC address
- Routing
  - Fixed routing (for small and stable networks)
  - Spanning Tree (802.1)
  - Source routing (802.5 – Token Ring)

Remember: 802.1D is the IEEE MAC Bridges standard which includes Bridging, Spanning Tree and others.

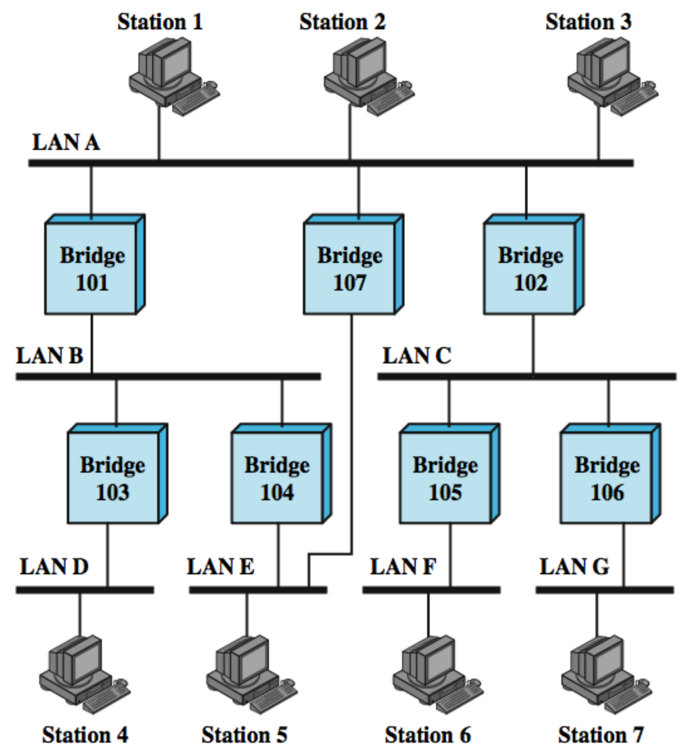
Fixed Routing

- Used for each source-destination pair of LANs
  - done in configuration
  - usually least hop route
  - only changed when topology changes
  - widely used but limited flexibility

Example of Fixed Routing

- Create a routing matrix – stored in the bridge
- Shortest route is based on least cost function
- Note that A→B = B→A

	A	B	C	D	E	F
A	NONE	101	102			
B	101	NONE		103	104	
C	102		NONE			105
D		103		NONE		
E	107	104			NONE	
F			105			NONE



- Find routing from E→ F

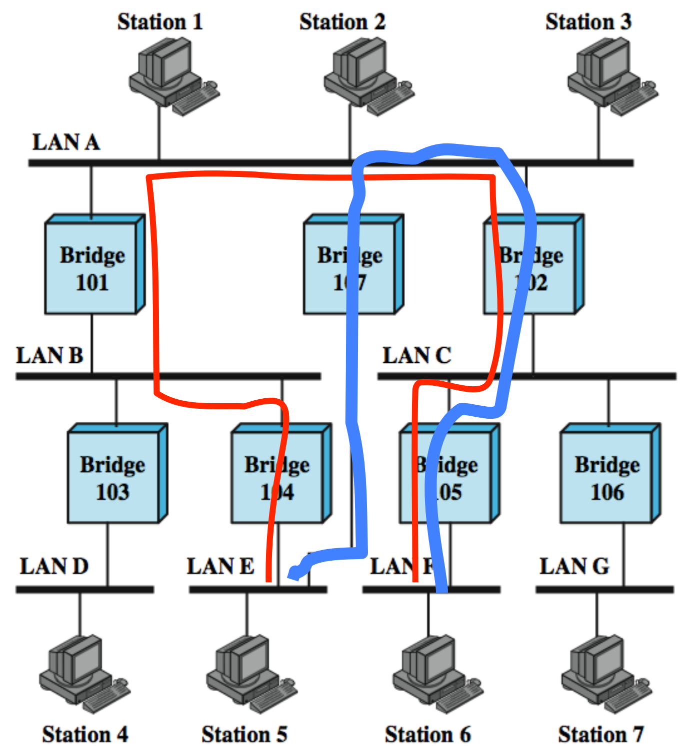
The table is manually created for each bridge!

Example of Fixed Routing

- Create a routing matrix – stored in the bridge

	A	B	C	D	E	F
A	NONE	101	102			
B	101	NONE		103	104	
C	102		NONE			105
D		103		NONE		
E	107	104			NONE	
F			105			NONE

- Find routing from E→ F
- E→B→A→C→F
- E→A→C→F (lower hop count)



The table is manually created for each bridge!

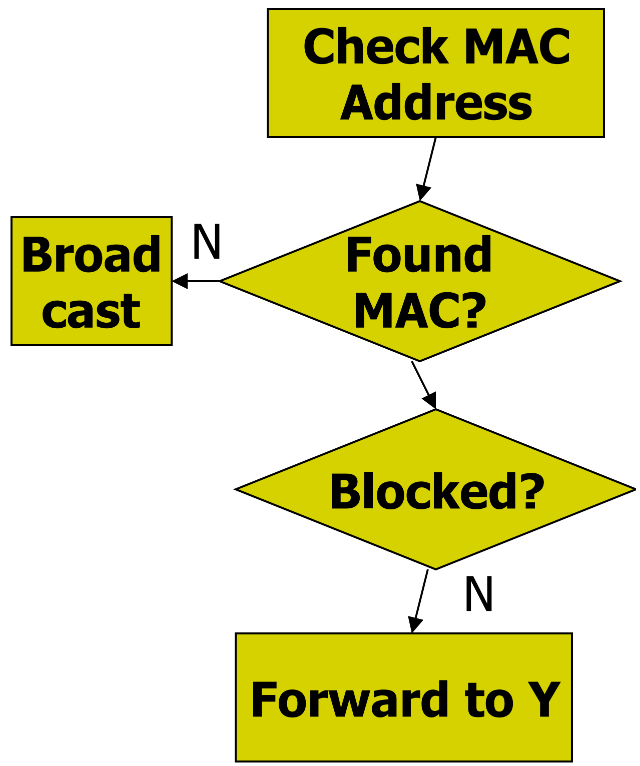
Use Shortest Path Routing

Spanning Tree

- bridge automatically develops routing table
- automatically updates routing table in response to changes
- three mechanisms:
  - frame forwarding
  - address learning
  - loop resolution (distributed spanning tree)

Frame Forwarding-
Forward a request or block?

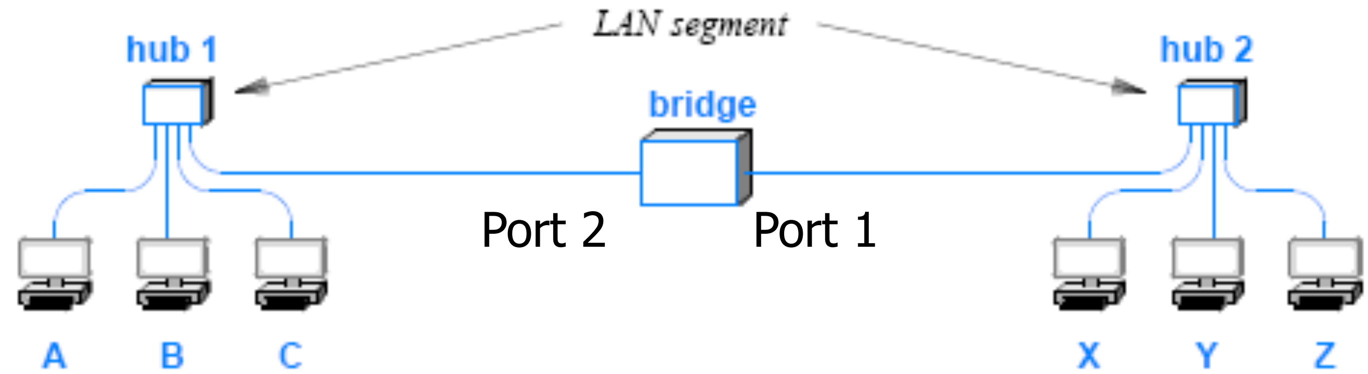
- When a frame arrives, the bridge must extract the MAC address from the frame
  - use the address to determine whether to forward the frame
- The bridge must maintain forwarding database for each port
  - lists station addresses reached through each port
- For a frame arriving on port X:
  - search forwarding database to see if MAC address is listed for any port except X
  - if address not found, forward to all ports except X
  - if address listed for port Y, check port Y for blocking or forwarding state
  - if not blocked, transmit frame through port Y



Address Learning –
Who is connected to the bridge

- A bridge learns that a computer is present on a segment as soon as the computer transmits a frame
- When a frame arrives from a given segment
  - the bridge extracts the source address from the header and adds the address to a list of computers attached to the segment

Address Learning (No looping)



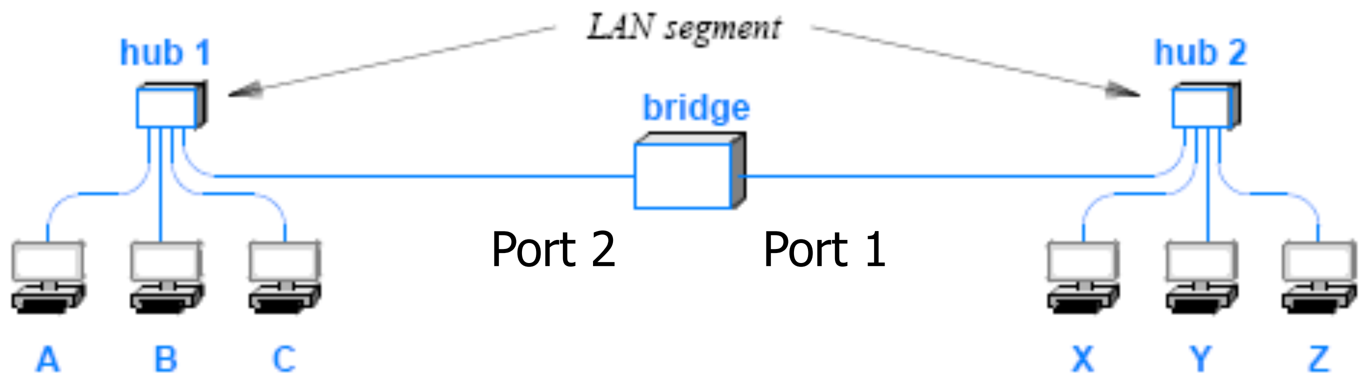
Only src addresses are detected

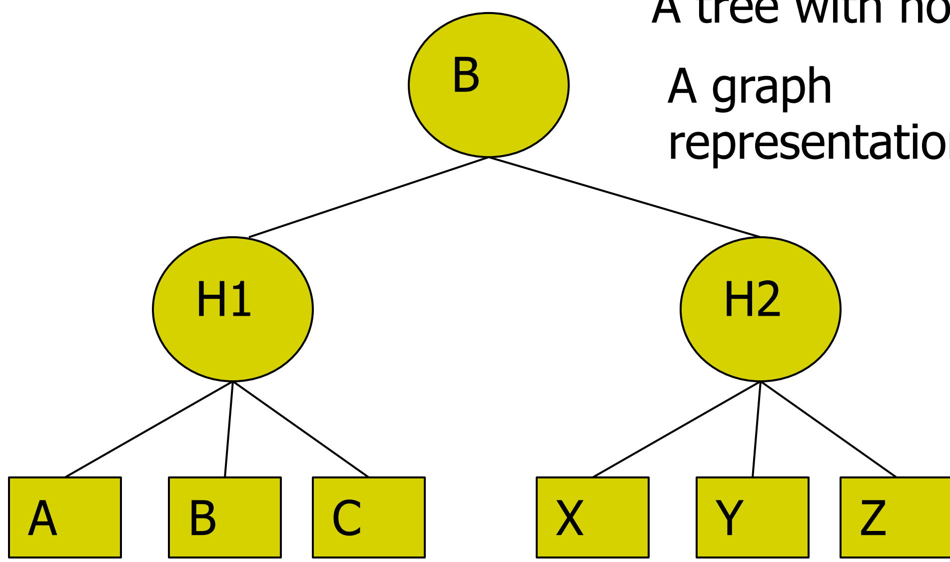
Initially, the Bridge looks at both Segments to forward the frame

Event	Segment 1	Segment 2	Frame Sent
Bridge boots	–	–	–
A sends to B	A	–	Both Segments
B sends to A	A, B	–	Segment 1 only
X broadcasts	A, B	X	Both Segments
Y sends to A	A, B	X, Y	Both Segments
Y sends to X	A, B	X, Y	Segment 2 only
X sends to Z	A, B	X, Y	Both Segments
Z sends to X	A, B, C	X, Y, Z	Segment 2 only

At this point the bridge Knows all the connected nodes to its two segments

Address Learning (No looping)



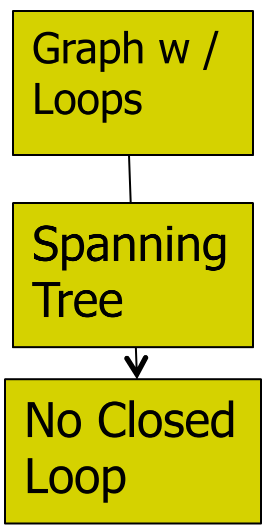


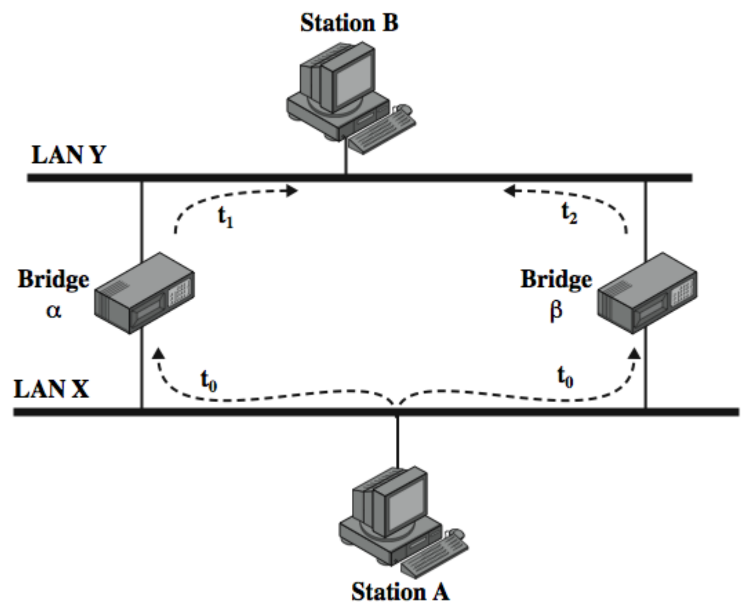
A tree with no loop!

A graph representation of the topology!

Distributed Spanning Tree Algorithm (Loop Resolution)

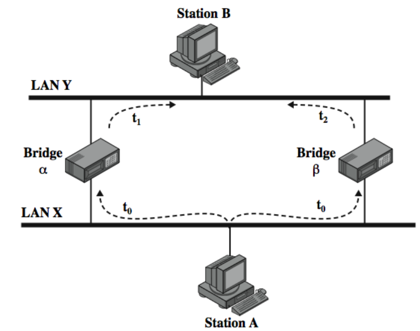
- address learning works for tree layout
- however, in general graph have loops
- for any connected graph there is a spanning tree maintaining connectivity with no closed loops
- IEEE 802.1 Spanning Tree Algorithm





-Address learning does not work when there is a loop!
- In the case above, bridges get confused!
    - Both bridges want to send packet from A to B!

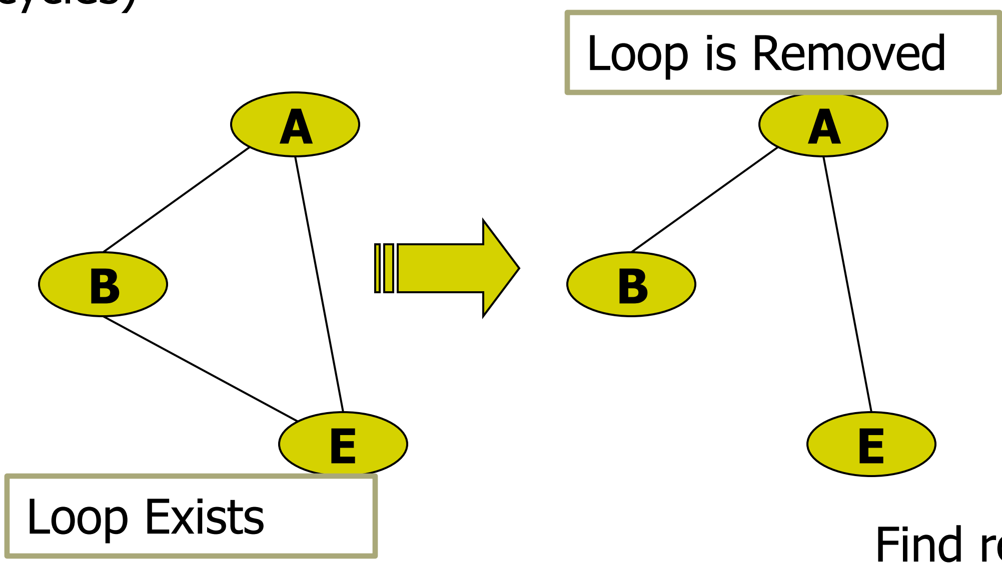
Spanning Tree Protocol

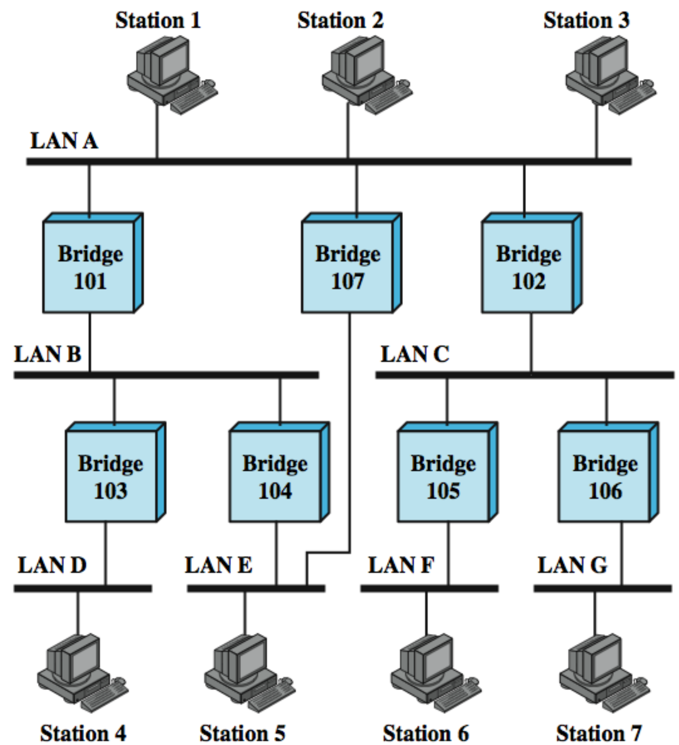


- STP consists of three steps:
  1. Root election
     - To permit a manager to control the election a bridge ID is used; it consists of two parts: a 16-bit configurable priority number and a 48-bit MAC address
     - bridges multicast a packet that contains their bridge ID, and the bridge with the smallest ID is chosen (sometimes only priority number is picked) See http://www.cisco.com/warp/public/473/spanning_tree1.swf
  2. Shortest path computation
     - Each bridge computes a shortest path to the root bridge.
     - Links included in the shortest paths of all bridges form the spanning tree
  3. Frame Forwarding
     - An interface that connects to the shortest path is enabled for forwarding packets; an interface that does not lie on the shortest path is blocked,
- In STP, Ethernet bridges communicate amongst themselves using a multicast address that is reserved for STP

Example:
Resolving the Loop of Bridges

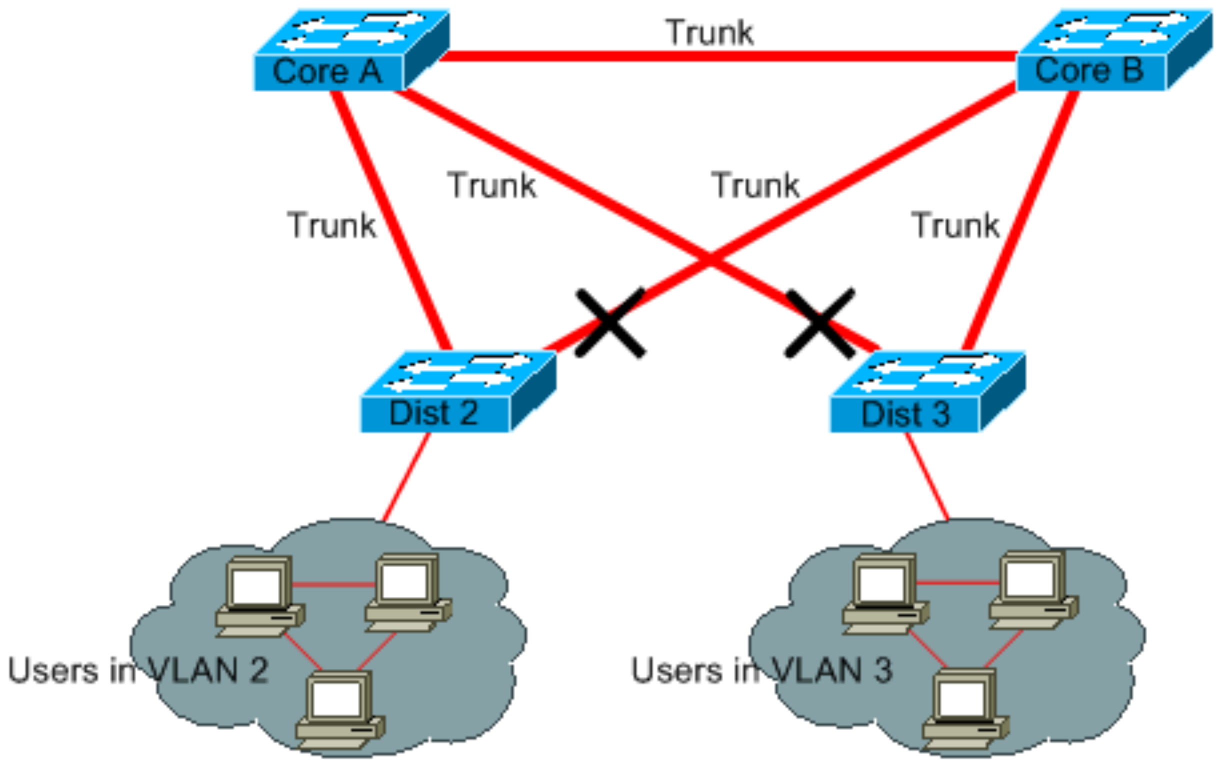
- To prevent cycles, a Distributed Spanning Tree (DST) is used
- This algorithm views bridges as nodes in a graph and imposes a tree on the graph (a tree is a graph that does not contain cycles)



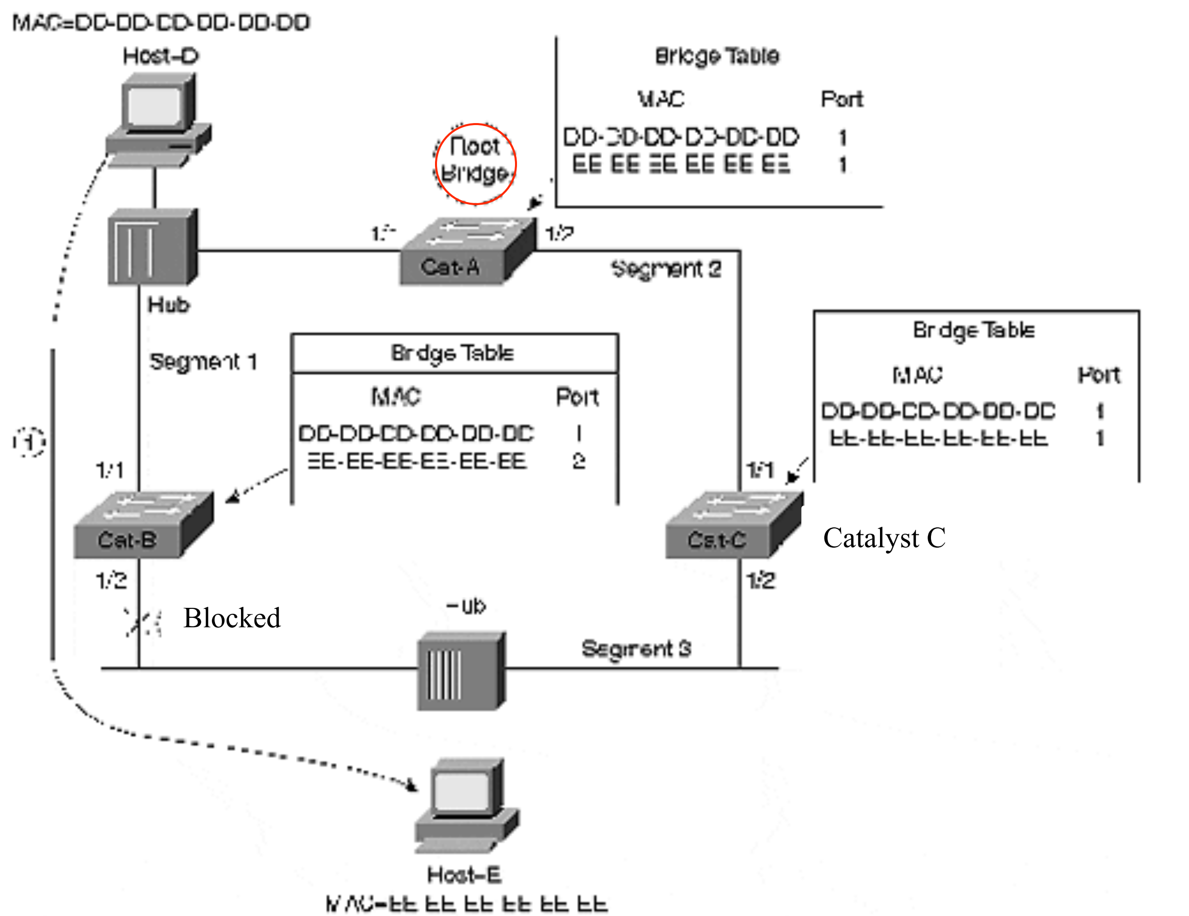


Find routing from E→ F
E→B→A→C→F
E→A→C→F (lower hop count)

Another Example of Spanning Tree



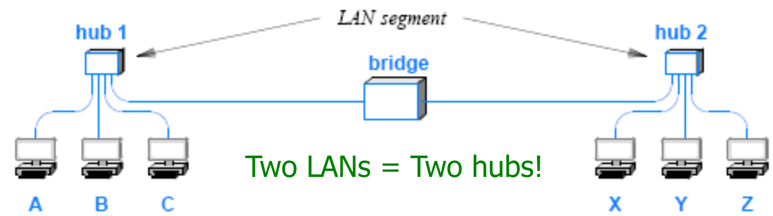
Creating Bridge Table



Spanning Tree Protocol Variations

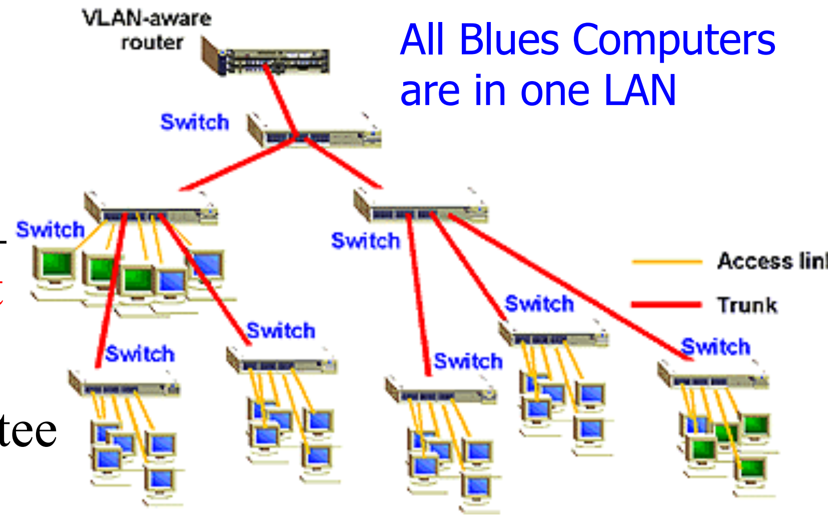
- Different variations of STP have been standardized
  - IEEE created a standard named 802.1D (in 1990)
  - the standard was updated in 1998
- IEEE standard 802.1Q provides a way to run STP on a set of logically independent networks (VLAN)
  - that share a physical medium without any confusion or interference
- Cisco created a proprietary version of STP, Per-VLAN Spanning Tree (PVST) for use on a VLAN switch
- IEEE standard 802.1W introduced the Rapid STP (RSTP) has been incorporated in 801.1d-2004 (in 1998), and now replaces STP, some versions are
  - Multiple Instance STP (MISTP)
  - Multiple STP (MSTP)

VLAN Switches



- Thus far, k LANs requires k hubs
  - This can cause low efficiency; no load balancing
  - What if users are dispersed
- One solution is to establish Virtual Local Area Network (VLAN)
  - Use VLAN switches; Make is flexible to add/remove users to each LAN
- The concept of VLAN is straightforward:
  - Allow a manager to configure a single switch to emulate multiple independent switches
  - A manager can specify a set of ports on the switch and designates them to be on virtual LAN 1, then designates another set of ports to be on virtual LAN 2, and so on
  - When a computer on virtual LAN 2 broadcasts a packet only those computers on the same virtual LAN receive a copy (i.e., once configured, a VLAN switch makes it appear that there are multiple switches)

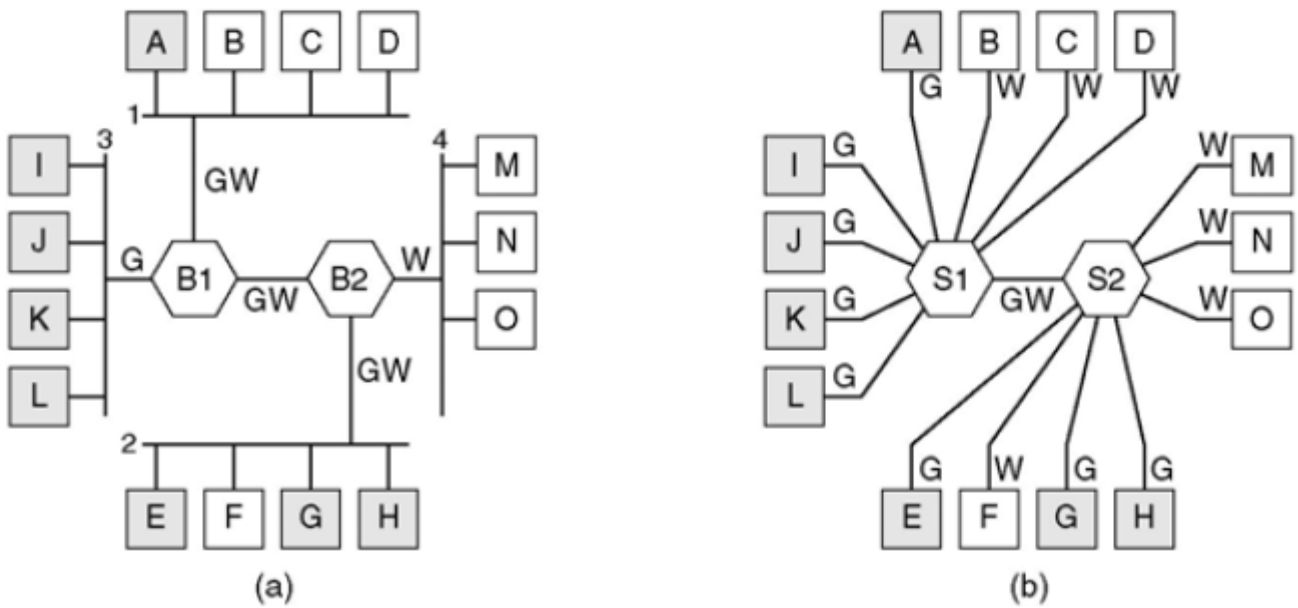
VLAN Switches



All Blues Computers are in one LAN

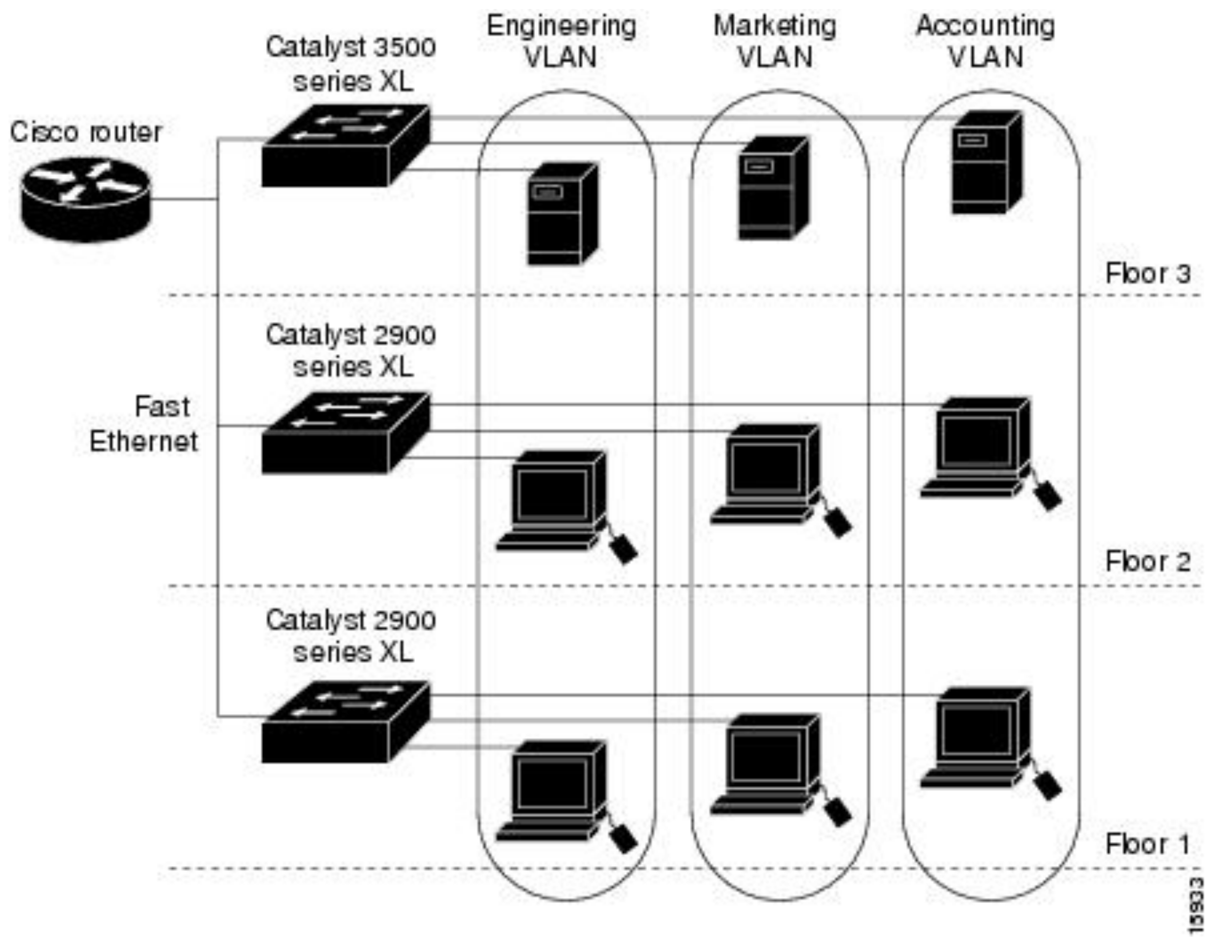
- Dividing computers into separate broadcast domains is important
- In each case, it may be important to guarantee that a set of computers can communicate without others receiving the packets and without receiving packets from outsiders
- In such cases, packets from each domain (LAN segment) has a separate *color*
- Frame Colors can be determined different ways
  - Each port of the Bridge (switch) is dedicated to a particular color → all domains must be connected to the same VLAN
  - Each MAC address is recognized as a particular color → all domains must be within the same organization
  - Each IP address is recognized as a particular color → the switch must act as level 3 device; mixing level 2 and 3 operations!

VLAN Example
Using Switches or Bridge Devices



(a) Four physical LANs organized into two VLANs, gray and white, by two bridges. (b) The same 15 machines organized into two VLANs by switches.

A Practical VLAN Setup

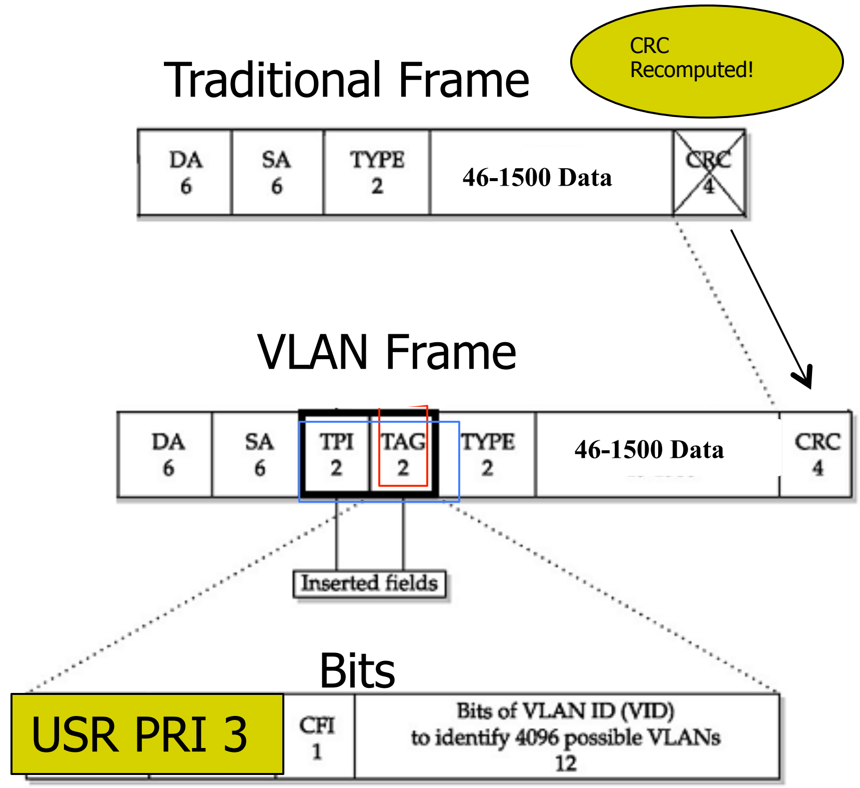


Preamble	Start-of-Frame-Delimiter	MAC destination	MAC source	Ethertype/Length	Payload (Data and padding)	CRC32	Interframe gap
7 octets of 10101010	1 octet of 10101011	6 octets	6 octets	2 octets	46–1500 octets	4 octets	12 octets

VLAN Frame

Max Total Bytes = 1518

- In 1988 802.1Q was established
  - VLAN compliant Ethernet → changing the frame max. length of Ethernet from 1518 to 1522 bytes
  - Adding VLAN tag to each frame
- **PRI** bits are used for QoS and supporting real-time applications
- **CFI** is Canonical Format Indicator (Corporate Ego Indicator!) – nothing to do with Ethernet
- In case 802.1Q compliant switches are connected to the traditional,
  - 802.1Q encapsulation inserts a 4-byte tag field into the original Ethernet frame between the source address and type/length fields and re-computes the frame check sequence (FCS) on the modified frame.
  - The added 4 bytes are removed when the frame is sent to a non-802.1Q node → next slide

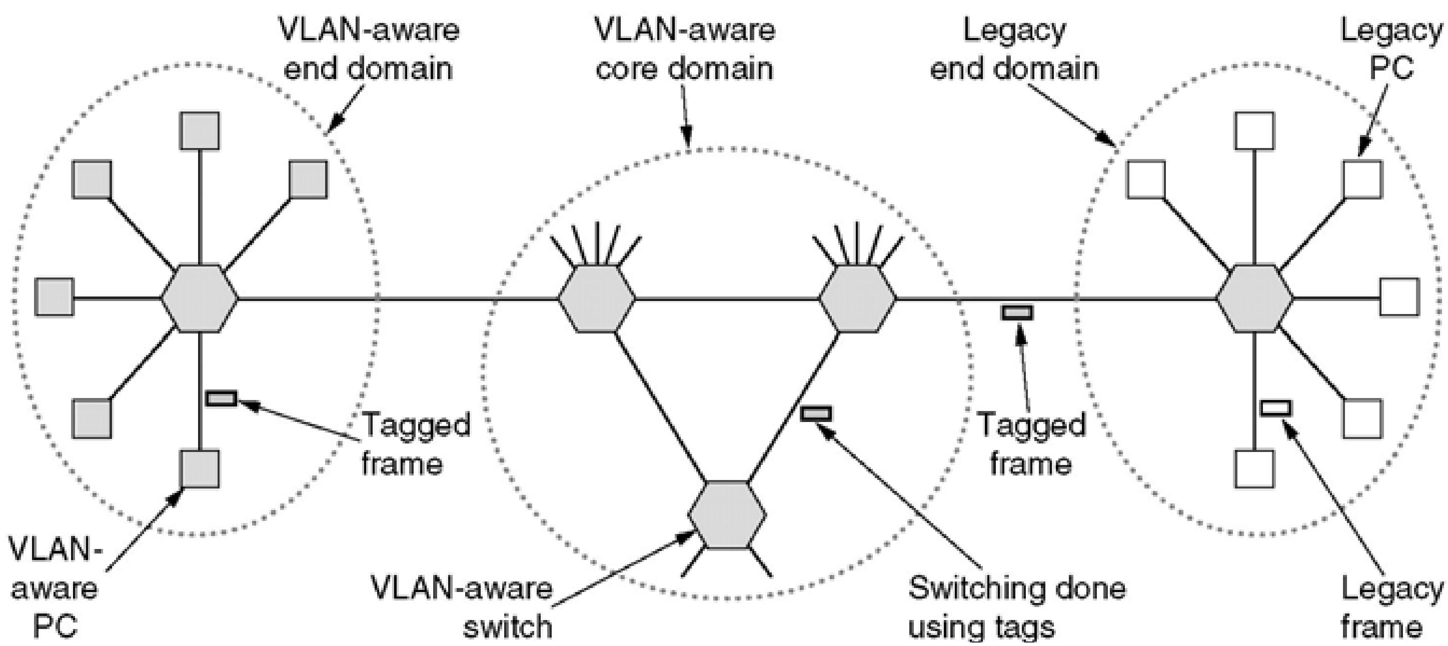


We can always add the VLAN field! (but not supported by current 802.3 devices!

SNAP: Sub-Network Attachment Point

http://routemyworld.com/2009/04/22/bcmsn-vlan-configuration-and-implementation/

The IEEE 802.1Q Standard



802.1Q bridges Plug & Pay!

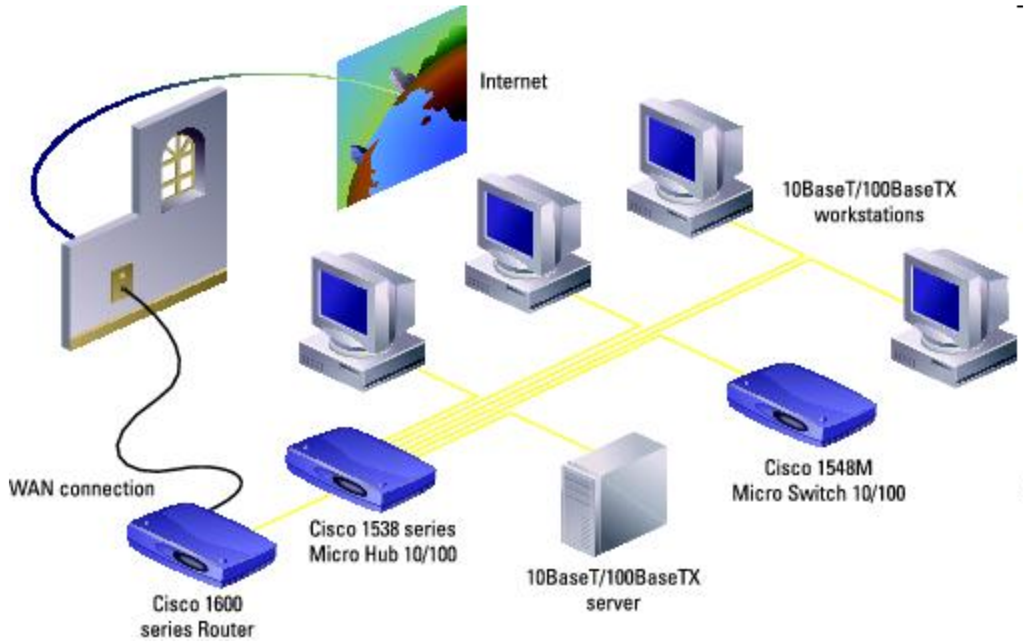
Sources

- Tomasi Text Book
- Wireless lan
  http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.htm
- LAN Design : http://module42k5.tripod.com/toyota.htm
- Read about VLAN http://www.3com.com/other/pdfs/solutions/en_US/20037401.pdf
- Tanenbaum Web resources
  http://authors.phptr.com/tanenbaumcn4/webResources/coverPageWebResources.html#VLAN
- Network Efficiency
  - http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/enet-calc.html

Projects

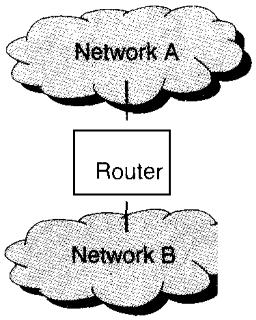
- Creating VLAN using Linux
  - http://www.candelatech.com/~greear/vlan.html
  - http://vimeo.com/6828914

Extra



Internet
10BaseT/100BaseTX
workstations
WAN connection
Cisco 1538 series
Micro Hub 10/100
Cisco 1548M
Micro Switch 10/100
10BaseT/100BaseTX
server
Cisco 1600
series Router

Interconnection Between Devices



(a)