CSCD 330
Network Programming
Spring 2017

Who is this?

Lecture 18
Link Layer Protocols Continued

Reading: Chapter 5

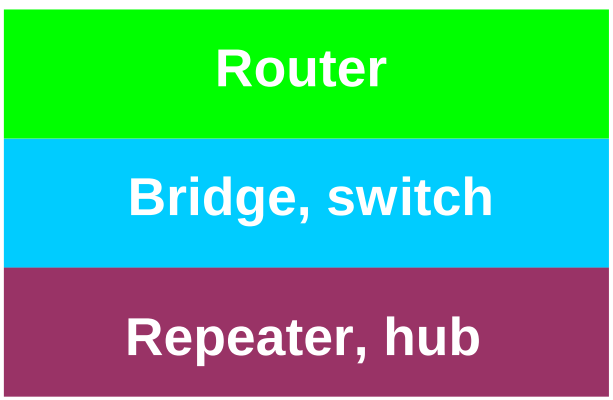
Overview

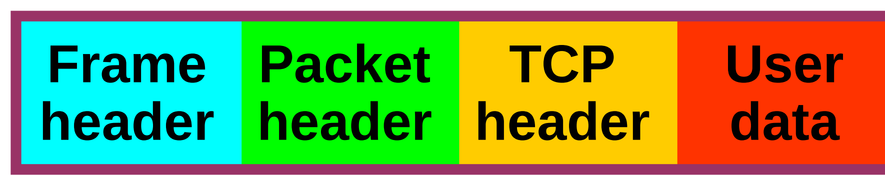
- Link Layer Hardware
  - Hubs vs Switches vs Routers
- Ethernet
- ARP and MAC Addressing

LAN and Network Hardware

Shuttling Data at Different Layers

- Different devices switch different things
  - Physical Layer: Electrical signals (repeaters and hubs)
  - Link layer: Frames (bridges and switches)
  - Network layer: Packets (routers)





Unicast, Multicast, Broadcast Defined

- **Unicast**
  - **Unicast separate transmission stream from source to destination for each recipient, example - HTTP**
- **Multicast**
  - **Traffic is sent to multiple recipients at same time using one transmission stream, data then distributed to end users on separate lines, example – IPTV**
- **Broadcast**
  - **Traffic sent out to every node on network or a portion of the network (LAN segment)**
  - **Broadcasts are issued for address resolution when location of user or server is not known, example – DHCP uses broadcast for IP management**

Key Distinction

(Smart) Routers

- Forward based on IP headers 192.168.0.1

(Dumber) Switches/Bridges

00:13:02:BA:43:56

- Forward based on MAC addresses

(Dumbest) Repeaters/Hubs

- Broadcast all bits 010101010101

Concept of devices being "smart" or "stupid"

- Smart means they can detect addresses
- Stupid means they can't make decisions – too dumb

Repeaters

- Length of cable used influence quality of communication

- Repeaters repeat signals
  - Clean and boost digital transmission
  - Analog networks use amplifiers to boost signal
- Repeaters only work with the physical signal
  - Cannot reformat, resize, or manipulate the data
- Physical layer, **Layer 1 device**

Repeaters (continued)

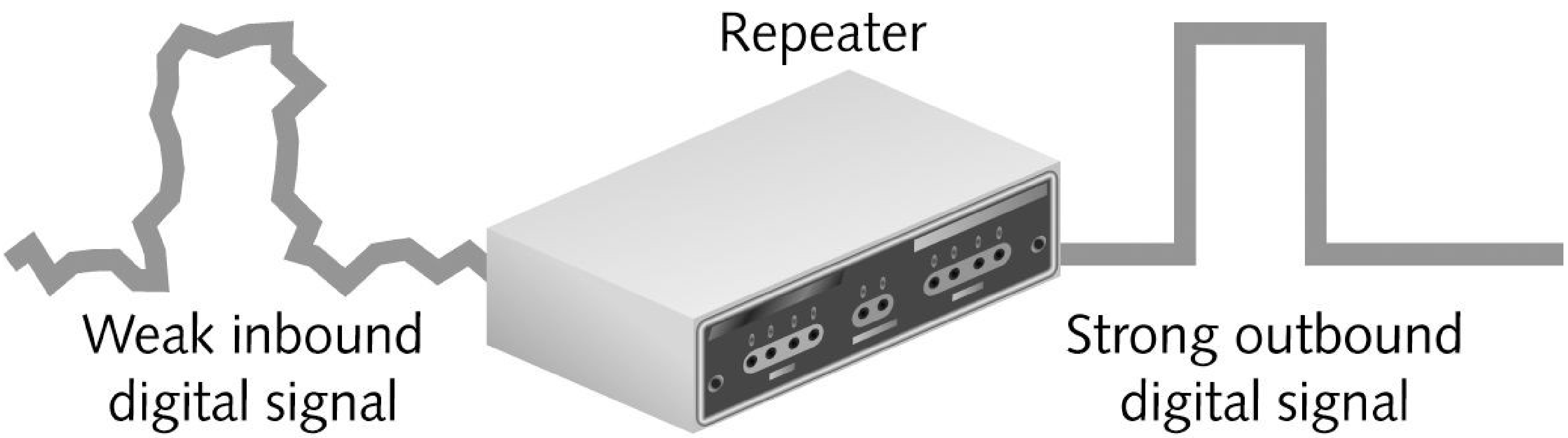


Figure 2-1 Repeater

Repeaters (continued)

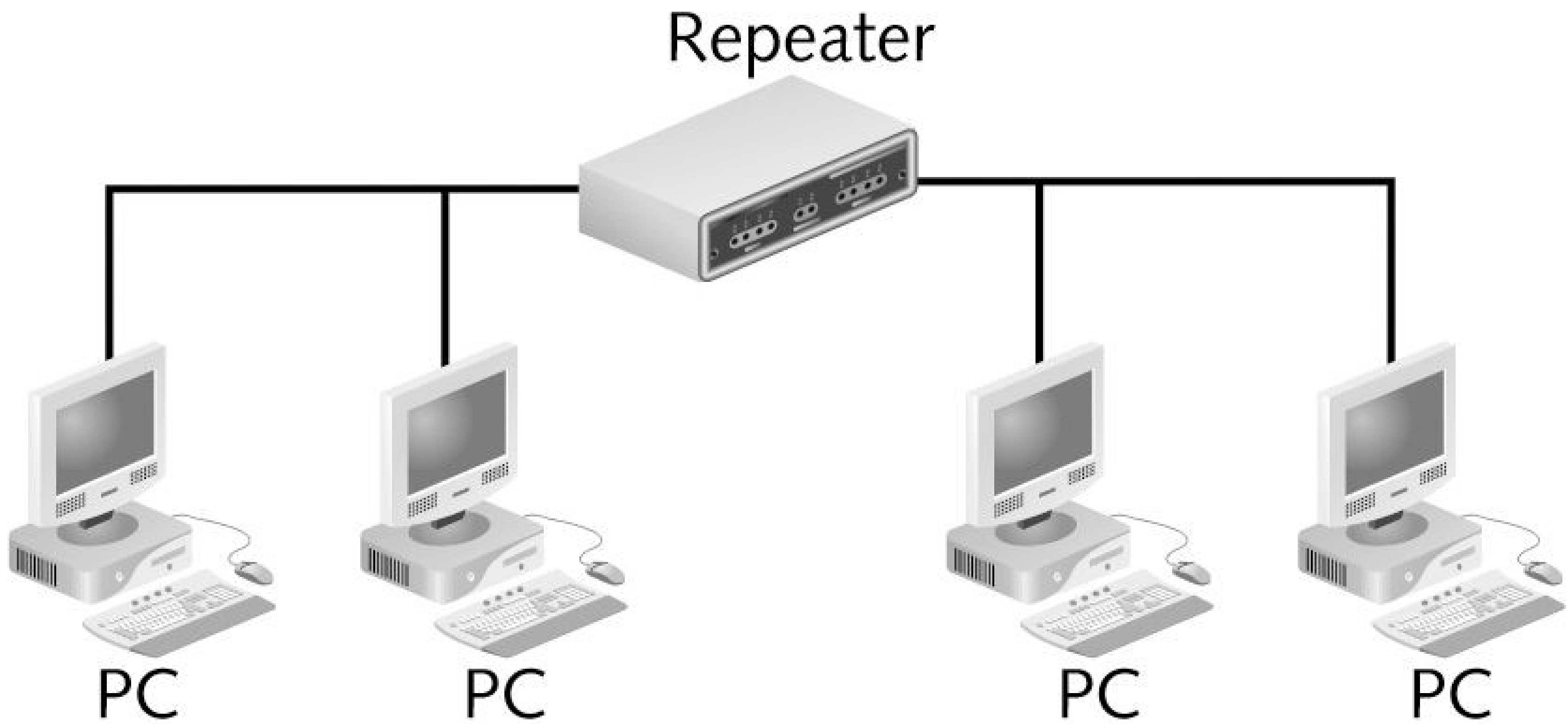


Figure 2-2 Repeater in the network

Hubs

- Generic connection device
  - Operates at the **Physical Layer**
- Connect several networking cables together

- Active hubs
  - Known as ... Multiport repeaters
- Passive hubs
  - Something that does not boost signal, just connects the wires

Hubs (continued)

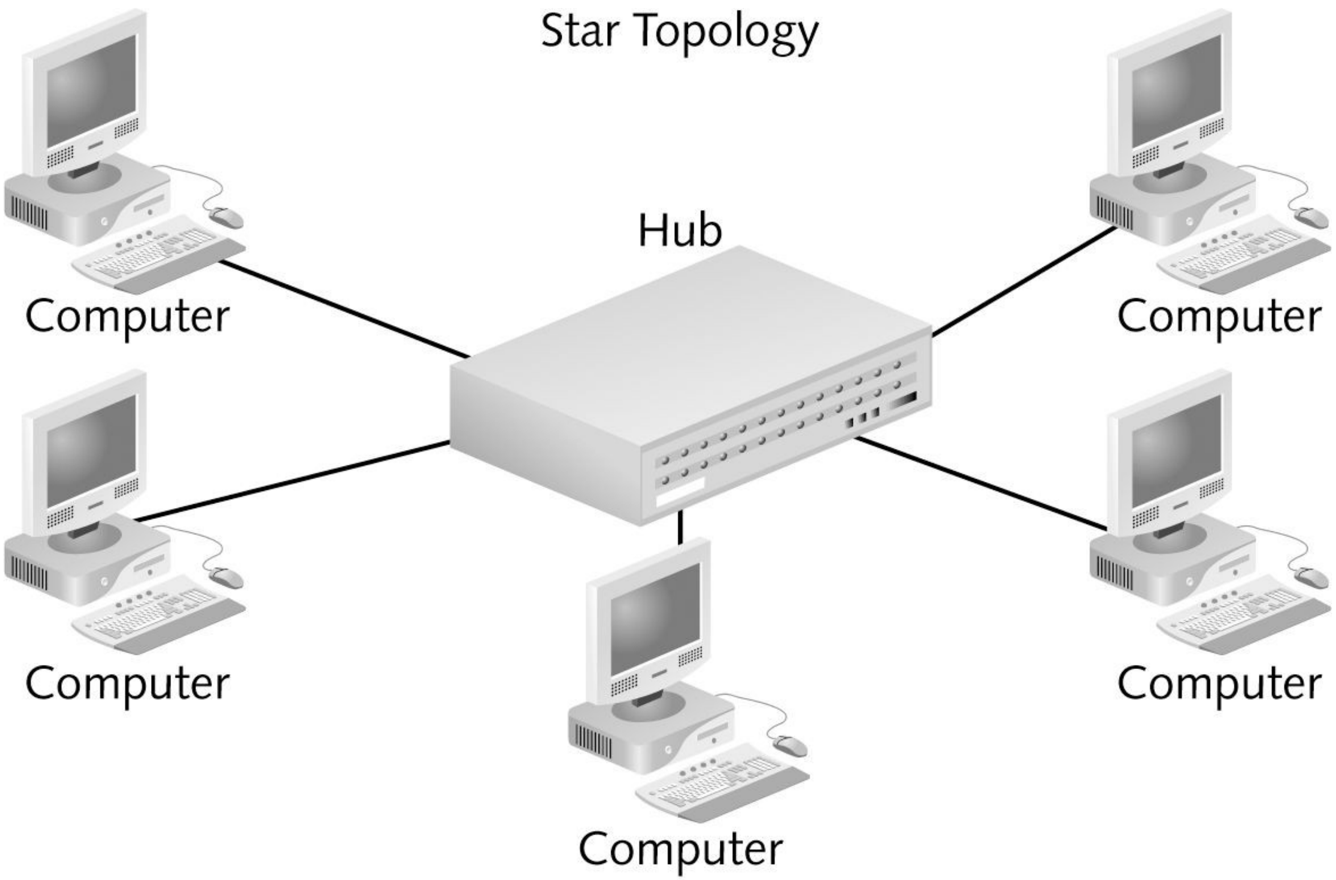
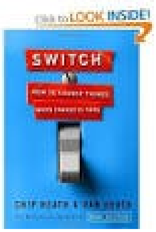


Figure 2-3 Star topology

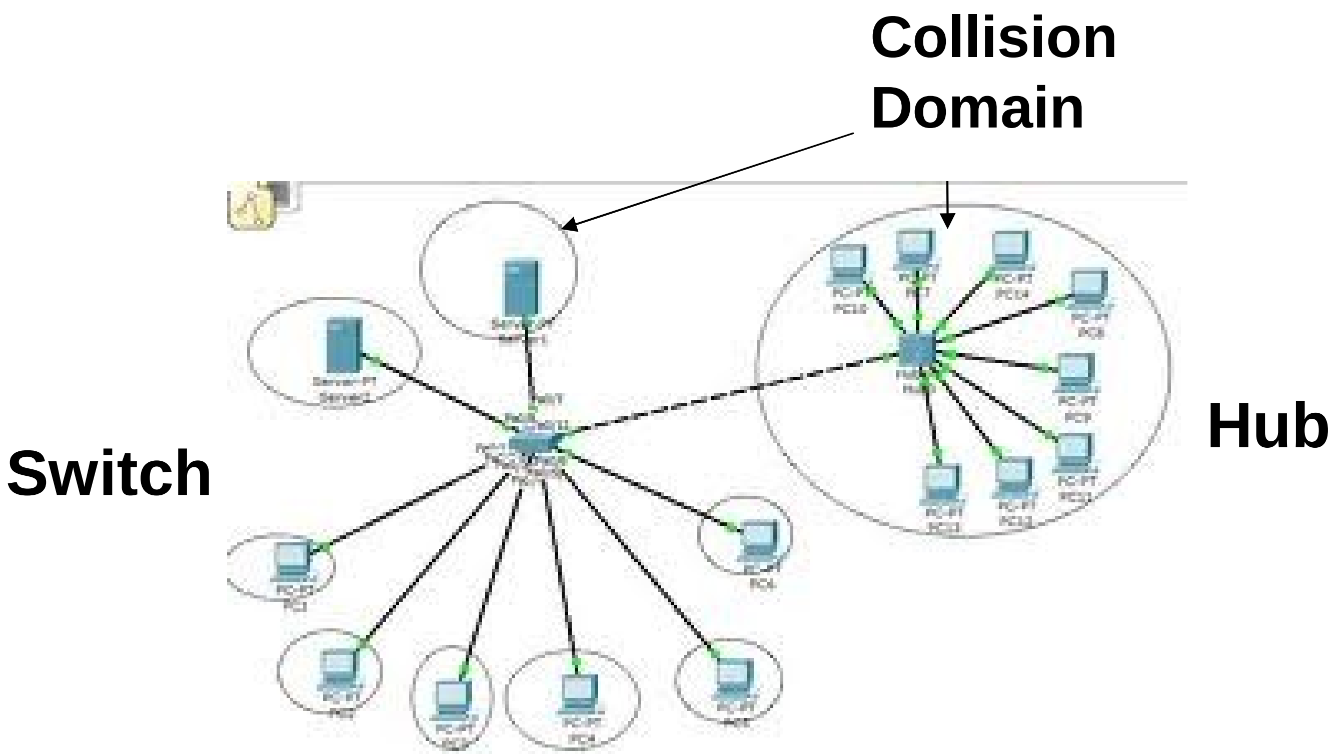
Switches



- Operate at the **Data Link layer**
  - Increases network performance
- Virtual circuits between source and destination
- Segmentation at the physical port level
- Is the norm now in LAN, replaced hubs

Switches

- Switch
  - Filter based on MAC addresses
  - Build tables in memory of host locations
  - Creates singular collision domains



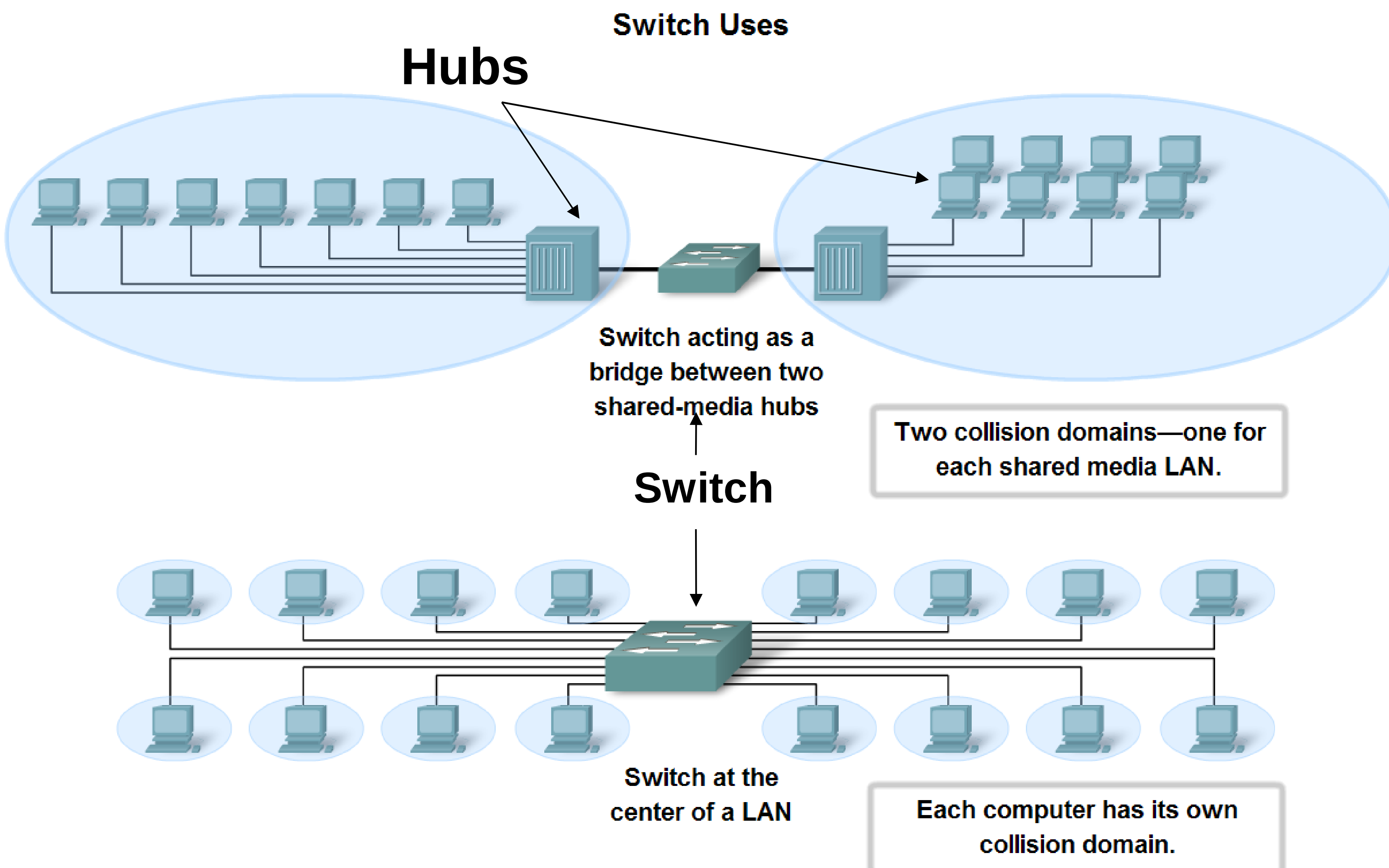
Collision Domain

- What is a Collision Domain?
  - Group of nodes in Ethernet network that compete with each other for access
  - If two or more devices try to access network at exact same time, collision will occur
  - In switched Ethernet environment, each transmitting-receiving pair of nodes is essentially its own collision domain, except that no collisions can occur, because there is no sharing of bandwidth

Broadcast Domain - Definition

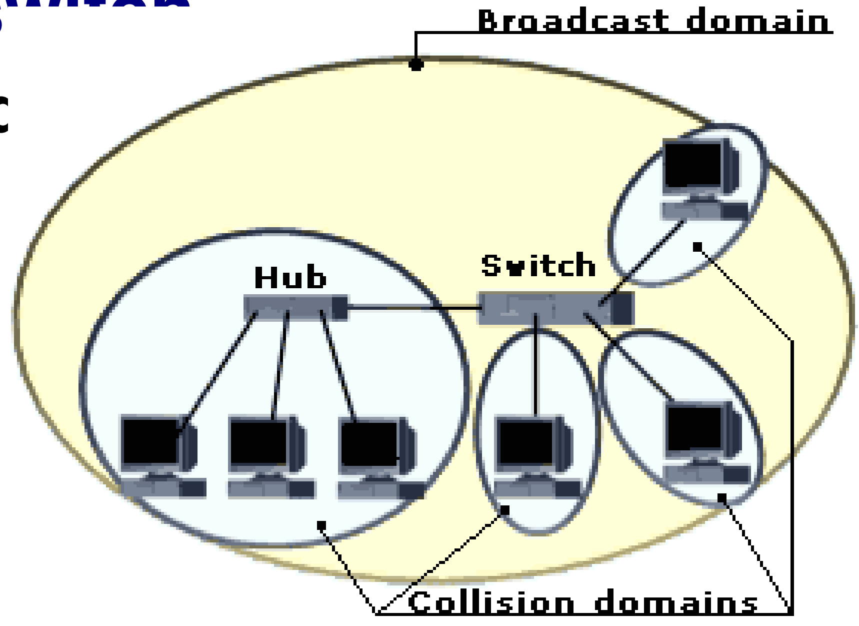
- All devices in same broadcast domain will receive broadcast frames originating from any other device within the domain
  - Broadcast frames are explicitly directed to all nodes in same network
  - Broadcast domains are typically bounded by routers because routers do not forward broadcast frames
  - Broadcast domains are Layer 2 segments, which can be extended or separated by using appropriate network components

Use of Ethernet Switches Versus Hubs in a LAN



Ethernet LAN with Switch and Hub

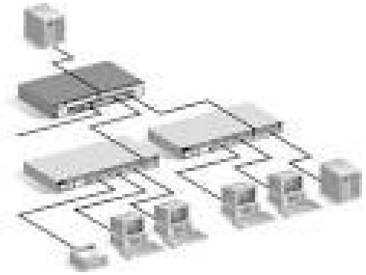
- Switches separate individual computers into their own collision domain
- Broadcast domain all computers connected via a switch
  - Unless configured otherwise



Switch

- Link-layer device, “Layer 2” Switch
  - Store, forward Ethernet frames
  - Examine incoming frame’s MAC address, selectively forward frame outgoing link when frame is to be forwarded on segment
- Transparent
  - Important !!!!! Note that
  - Hosts are unaware of presence of switches
  - Operate at lower levels of protocol stack
- Plug-and-play, self-learning
  - Switches do not need to be manually set

Switches



- Advantages of Switches
  - Increase available network bandwidth
  - Reduced workload, computers only receive packets intended for them specifically
  - Increase network performance
    - Each host gets full speed use of link
  - Smaller collision domains

Switches

- Disadvantages of Switches
  - More expensive than hubs and bridges
  - Difficult to trace network connectivity problems through a switch
  - Does not filter broadcast traffic
  - Are the norm in networks or combination with routers

Switches (continued)

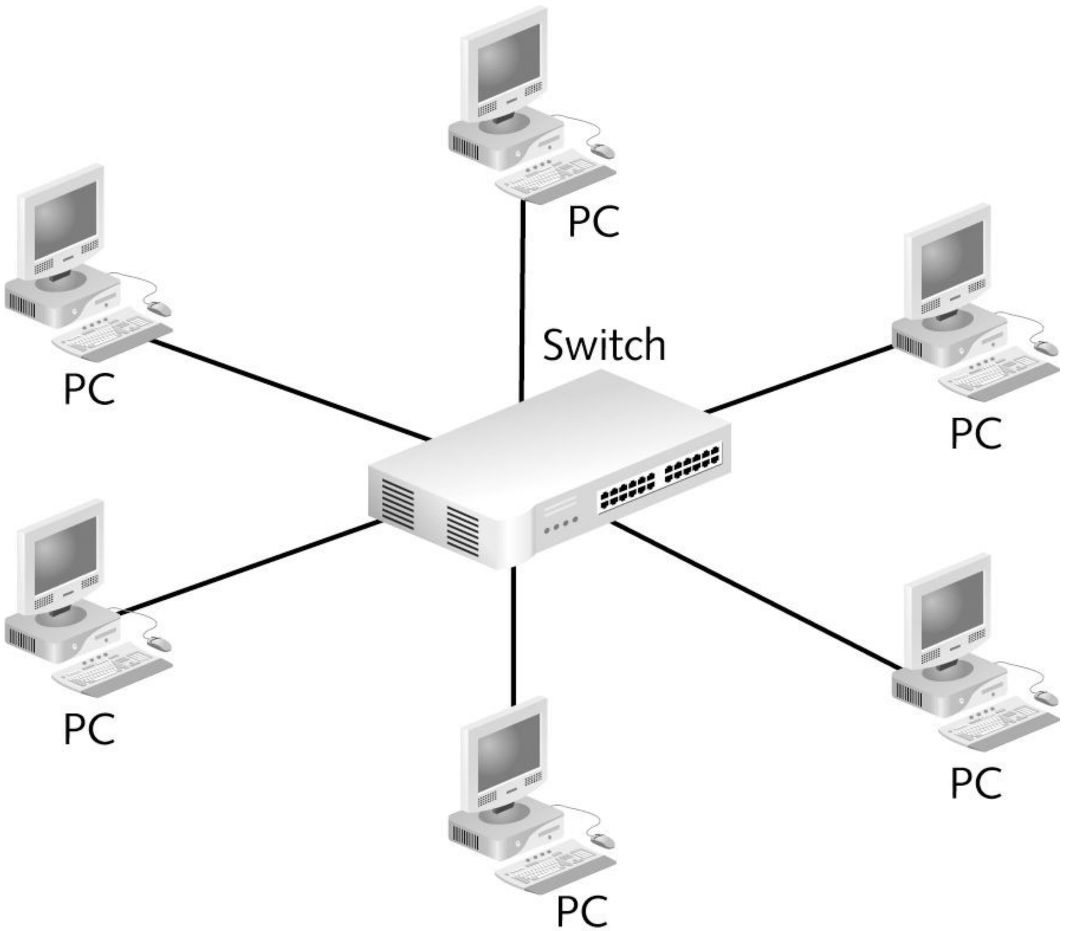


Figure 2-7 Star topology using a switch

Routers

- What does a router do?
  - Provides filtering and network traffic control
  - Used for LANs to connect segments and WANs
  - Connect multiple segments and networks
  - Routers have multiple NIC cards and create separate networks
  - Multiple routers create an “internetwork”
  - Operates at Network layer
  - Layer 3 device

Routers

- Creates a table to determine how to forward packets
- Filtering and traffic control base on logical addresses, IP addresses

Differences Logical vs. Physical

- Look at the Differences Between Logical and Physical Addresses ...

Physical Versus Logical Addresses

- MAC addresses
  - Data Link layer
  - Used by switches
  - Used for directly connected devices
  - Mostly encoded in firmware, does not change
- Logical addresses, IP
  - Network layer
  - Use by routers
  - Changes with network segment
  - IP addresses are assigned manually or by software

Physical Versus Logical Addresses (continued)

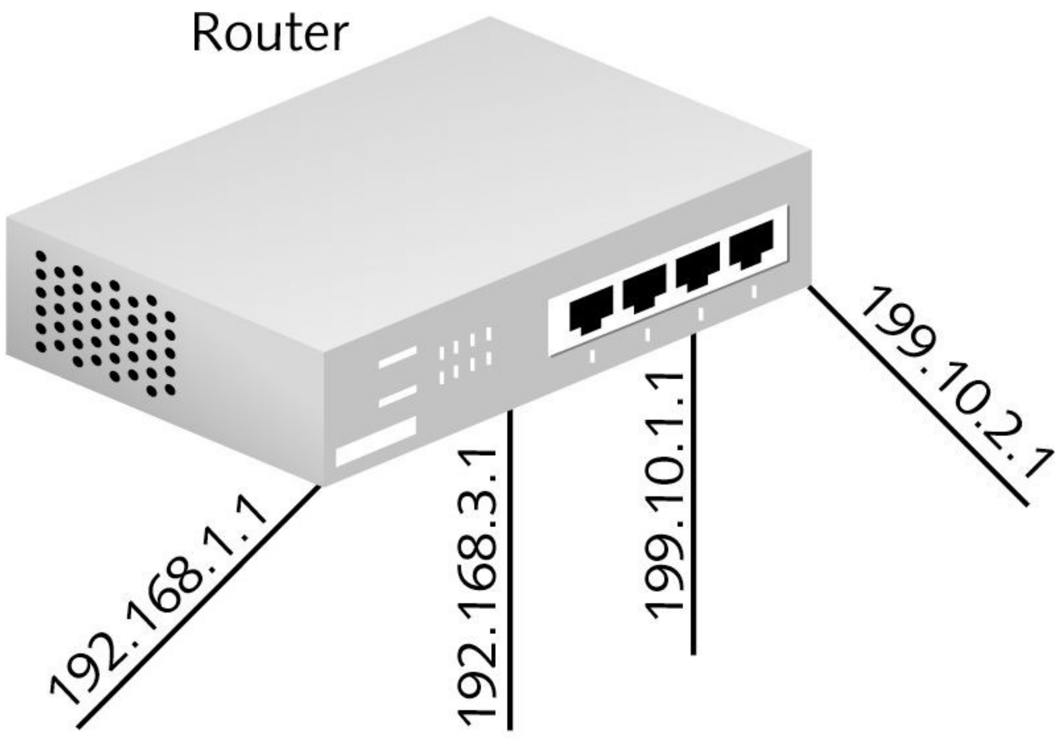
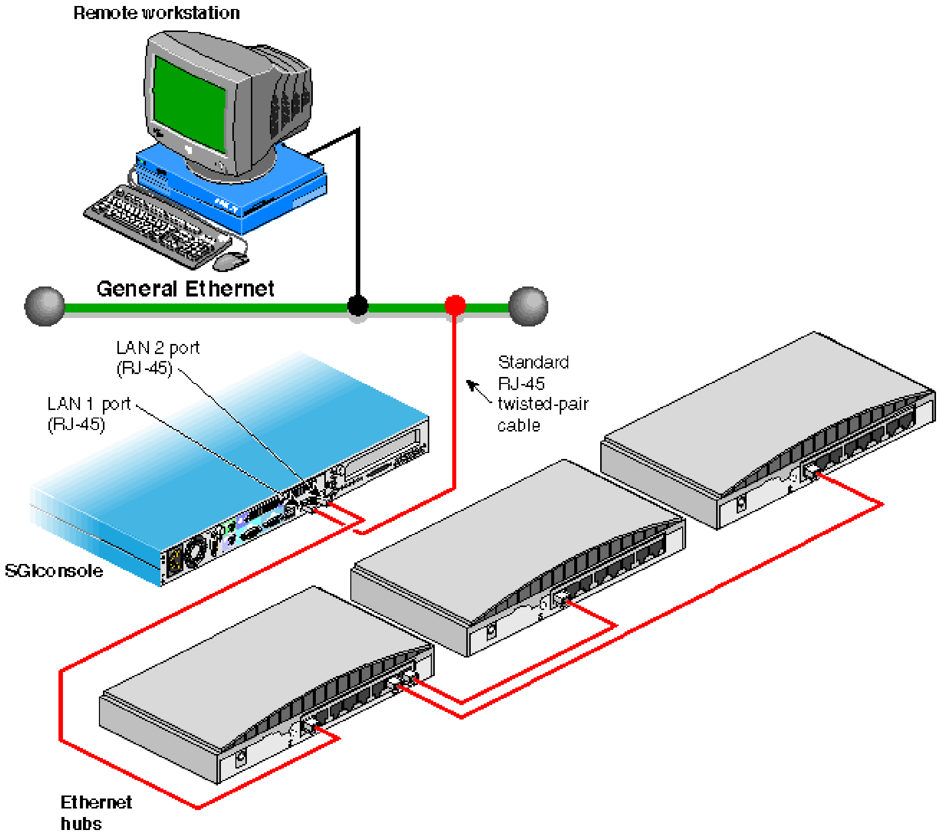


Figure 2-8 Router


Remote workstation
General Ethernet
LAN 2 port
(RJ-45)
LAN 1 port
(RJ-45)
Standard
RJ-45
twisted-pair
cable
SGIconsole
Ethernet
hubs

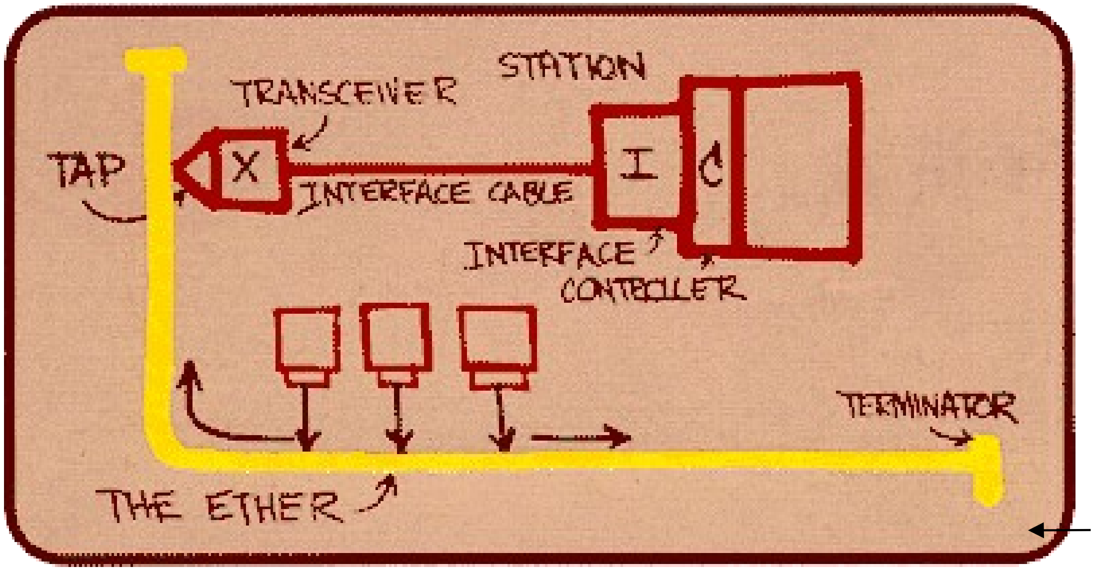
Ethernet

Ethernet History

- 1973 Xerox Corporation's Palo Alto Research Center developed bus topology Local Area Network (LAN)
- 1976, carrier sensing added,
  - Xerox built 2.94 Mbps network to connect over 100 personal workstations on 1 km cable
- Network called Ethernet, named after ether, single coaxial cable used to connect machines
- "Ethernet" refers to product which predates IEEE 802.3 Standard
- But, nowadays any 802.3 compliant network is referred to as an Ethernet

Ethernet

Bob Metcalf



Metcalfe's Ethernet sketch

Original Paper published in 1976

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.87.1052&rep=rep1&type=pdf

802.3 Standard Project

- In 1980, (IEEE) started project 802 to standardize local area networks (LAN)
- IEEE wanted to put forward one standard
  - IBM Token Ring,
  - Token Bus and
  - Ethernet were all contenders
- Eventually, Ethernet won and it became a standard in **1985 … 28 years ago!**
- First standard was for 10 Mbps
- Entire list of Ethernet Standards

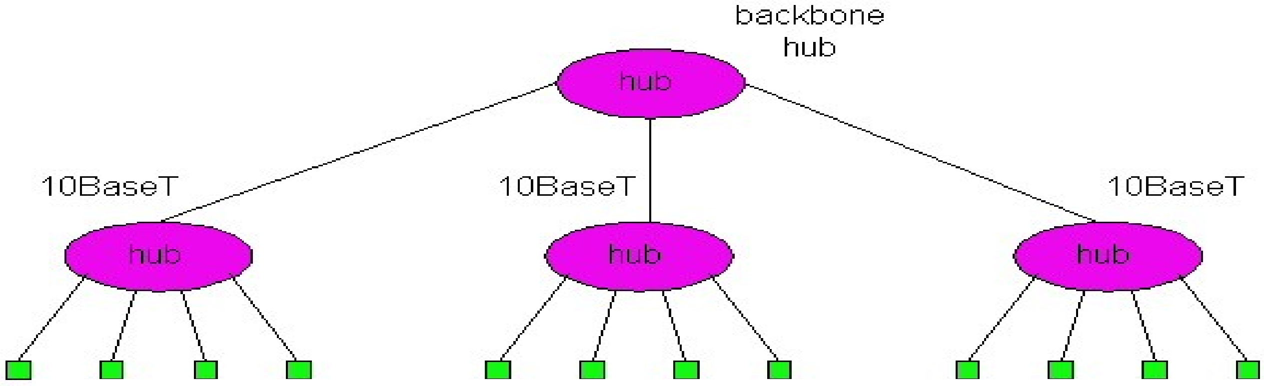
  http://en.wikipedia.org/wiki/IEEE_802.3

Classical Ethernet Broadcast

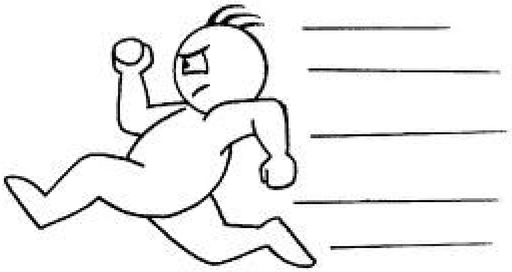
- Classical Ethernet, is Broadcast Network
- Hosts connected to network through single shared medium
- If two nodes try to send at same time,
  - Called **collision** and prevents any information passed along network
  - Multiple messages would collide and corrupt each other

Ethernet Technologies: 10BaseT and 100BaseT

- Hub(s) connected by twisted pair in "star topology"
  - Distance of any node to hub < 326 ft



802.3u Fast Ethernet



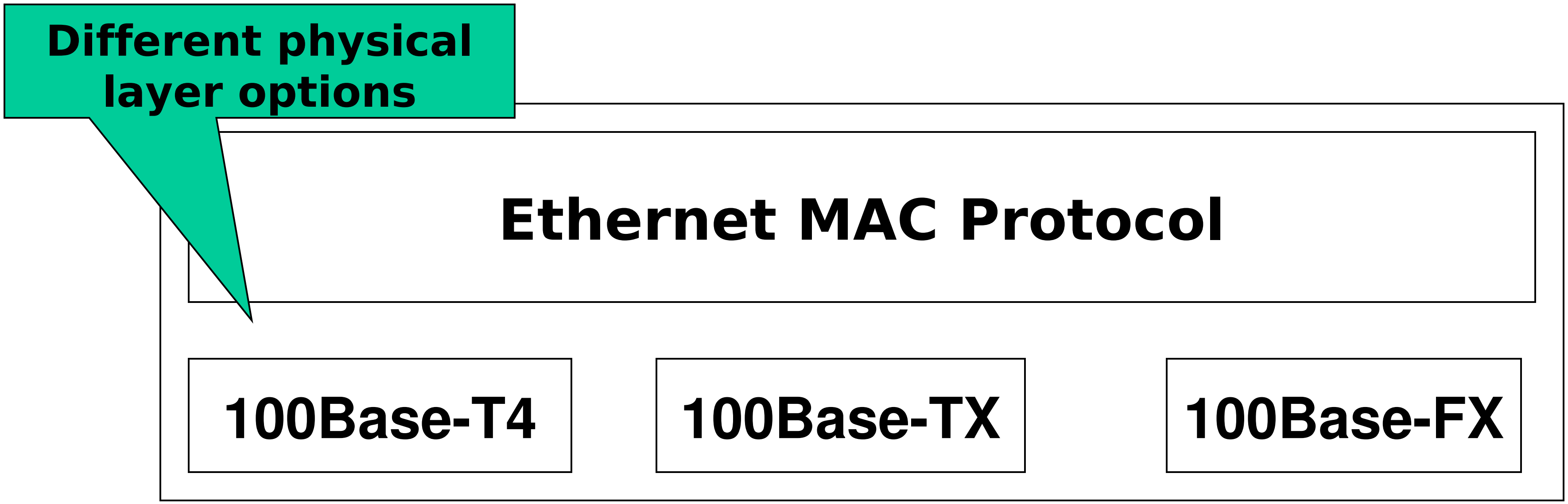
- In **1995**, IEEE adopted
  802.3u Fast Ethernet standard

- Fast Ethernet is 100 Mbps Ethernet standard
- With Fast Ethernet came **full-duplex Ethernet**
  Two stations could transmit at the same time!

- Previously, Ethernets worked in half-duplex mode

The 100Mb/s Ethernet Standard

"Fast Ethernet"



Up to 100m of cable per segment.

100Base-T4: Uses four pairs of voice grade Category-3 cable .
100Base-TX: Uses two pairs of data grade Category-5 cable.
100Base-FX: Uses two optical fibers.

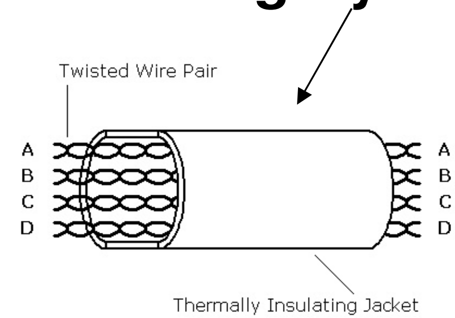
The 1Gb/s Ethernet Standard

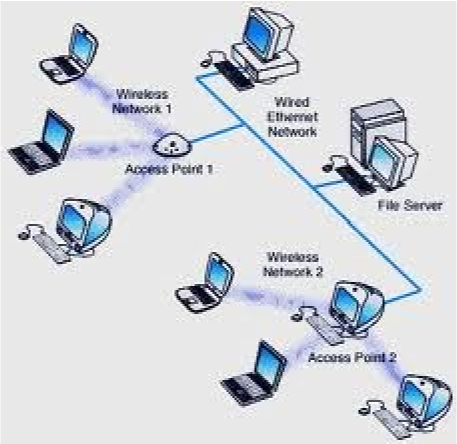
“Gigabit Ethernet”

Ethernet MAC Protocol

1000Base-TX | **1000Base-FX**

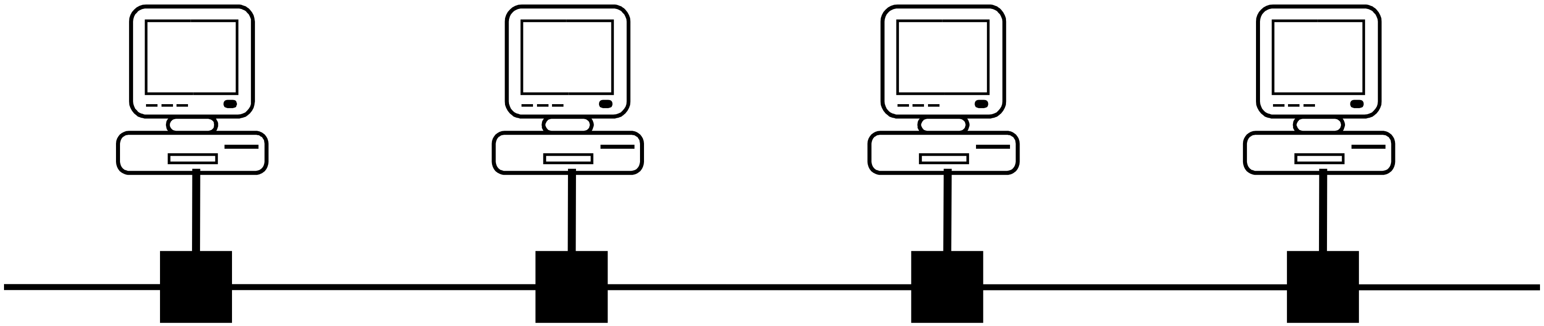
1000Base-TX: Uses four pairs of data grade Category-5 cable.
1000Base-FX: Uses two optical fibers.





CSMA/CD in Ethernet

CSMA/CD Protocol



All hosts transmit & receive on one channel
Packets are of variable size.

When a host has a packet to transmit:

1. **Carrier Sense:** **Check that the line is quiet before transmitting.**
2. **Collision Detection:** **Detect collision as soon as possible. If a collision is detected, stop transmitting; wait a random time, then return to step 1.**

↑ **binary exponential backoff**

Ethernet CSMA/CD algorithm
Carrier Sense Multiple Access/ Collision Detection

Algorithm

1. NIC receives datagram from network layer, creates frame
2. If NIC senses channel idle, starts frame transmission
   If NIC senses channel busy, waits until channel idle, then transmits
3. If NIC transmits entire frame without detecting another transmission, NIC is done with frame !

Ethernet CSMA/CD algorithm

4. If NIC detects another transmission while transmitting, aborts and sends jam signal
5. After aborting

NIC enters exponential backoff

after mth collision, NIC chooses a *K,* small

integer, at random from $\{0,1,2,\ldots,2^m-1\}$

NIC then waits K·512 bit time,

Returns to Step 2

More details follow …

Ethernet CSMA/CD algorithm

Features

- **Transmitting station intentionally transmits a "jam sequence" to ensure all stations are notified the frame transmission failed due to a collision**
- **Station then remains silent for a random period of time before attempting to transmit again**
- **Repeats: Until frame is eventually transmitted successfully**

Ethernet's CSMA/CD (more)

Exponential Backoff

- Goal Adapt retransmission attempts to estimated current load
  - Heavy load -> random wait will be longer and more varied

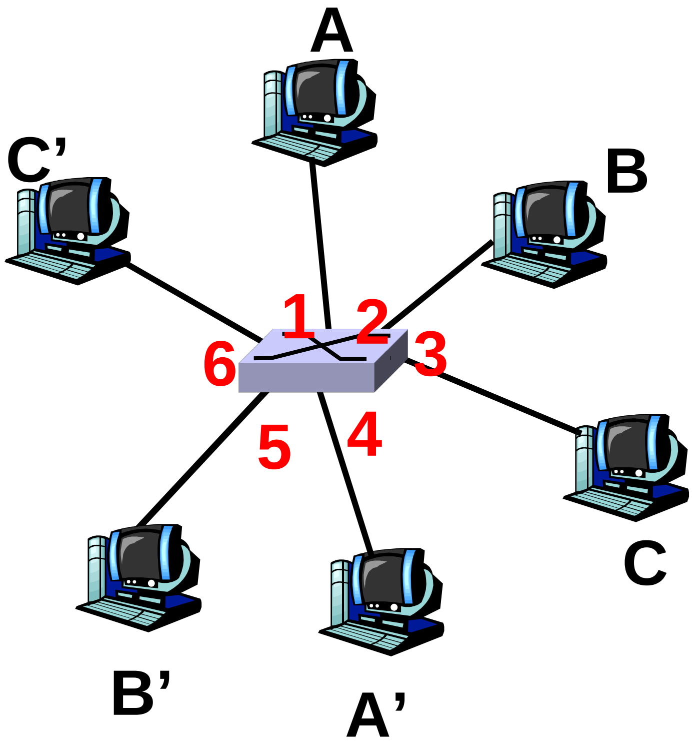
- First collision: Choose K from {0,1};

  Delay is K· 512 bit transmission times
- After second collision: Choose K from {0,1,2,3}…
- After ten collisions, Choose K from {0,1,2,3,4,…,1023}
- Set size grows Exponentially

Ethernet and Switches

Switch: Allows *multiple* simultaneous transmissions

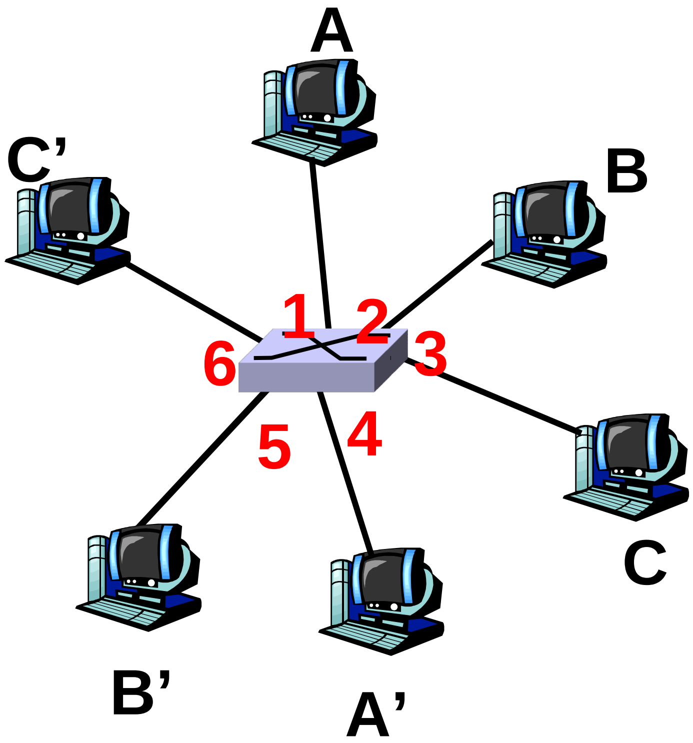
- Hosts have dedicated, direct connection to switch
- Switches "buffer" packets
- Ethernet protocol used on each incoming link, no collisions AND full duplex
  - Each link is its own collision domain
- Switching: A-to-A' and B-to-B' simultaneously, without collisions
  - Not possible with "dumb" hub



switch with six interfaces (1,2,3,4,5,6)

Switch Table

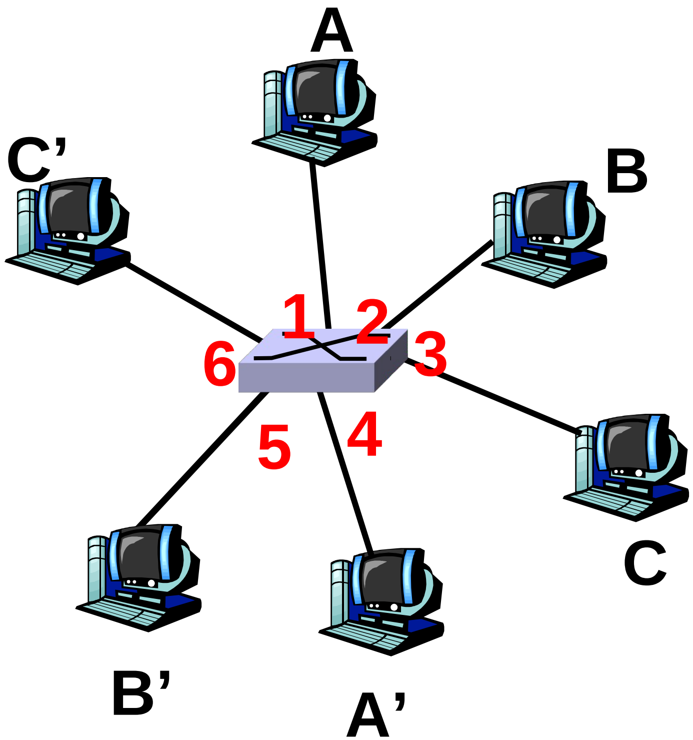
- ***Q:*** how does switch know that A' reachable via interface 4, B' reachable via interface 5?
- ***A:*** Each switch has **switch table,** each entry:
  - MAC address of host, interface to reach host, time stamp
- Looks like a routing table!
- ***Q:*** How are entries created, maintained in switch table?
  - Self-Learning



Switch with six interfaces (1,2,3,4,5,6)

Switch: self-learning

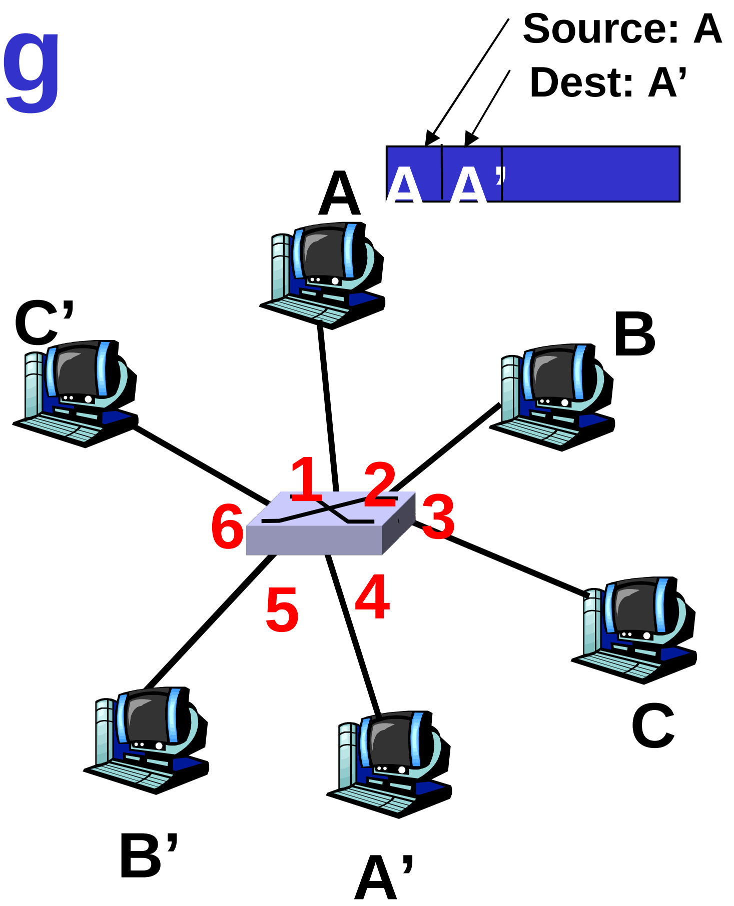
- Switch *learns* which hosts can be reached through which interfaces
  - When frame received, switch "learns" location of sender: incoming LAN segment
  - Records sender/location pair



MAC addr	interface	TTL
A	1	60

Switch table
(initially empty)

Switch: self-learning



- **Frame with Destination A' arrives at switch from interface 1**

Two possibilities:

1. No entry in table, for A', switch forwards frame to all interfaces except 1

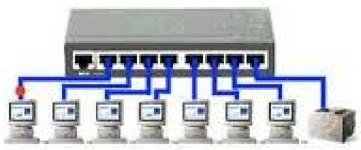
- Entry for A' added when A' answers

2. Entry in table, for A' interface of 4, frame would get forwarded only to A'

MAC addr	interface	TTL
A	1	60
A'	4	60

Switch table (initially empty)

Switches and CSMA/CD



- Do we need to use CSMA/CD on today's switched network?
  - Ethernet Collision domain has pretty much been relegated to history
  - Hubs still use CSMA/CD, but if network uses switches, in full-duplex mode, then CSMA/CD no longer comes into play

  - Full-duplex switches use separate wire pairs so switch port can send data to attached computer, while receiving data from that computer on another wire pair

Link Layer

- 5.1 Introduction and services
- 5.2 Error detection and correction
- 5.3Multiple access protocols
- 5.4 Link-Layer Addressing
- 5.6 Link-layer switches

MAC Addresses

Network Layer

32-bit IP address

Network-layer address, dotted decimal

Ex.: 146.187.130.76

To route datagram to destination machine

MAC (or LAN or physical or Ethernet) Address

MAC stands for Media Access Control

48 bit MAC address (for most LANs)

Burned in NIC ROM, also sometimes software settable

24 bits set for manufacturer, 24 bits for NIC adapter

Ex.: 00:E0:B8:9C:A6:60

Change Your MAC Address

- How to change your MAC address
  - Windows XP/2000/Vista
    - Use regedit to edit registry or use a utility
    - Mac Makeup,

    http://www.gorlani.com/publicprj/macmakeup/macmakeup.asp
    - MadMACs

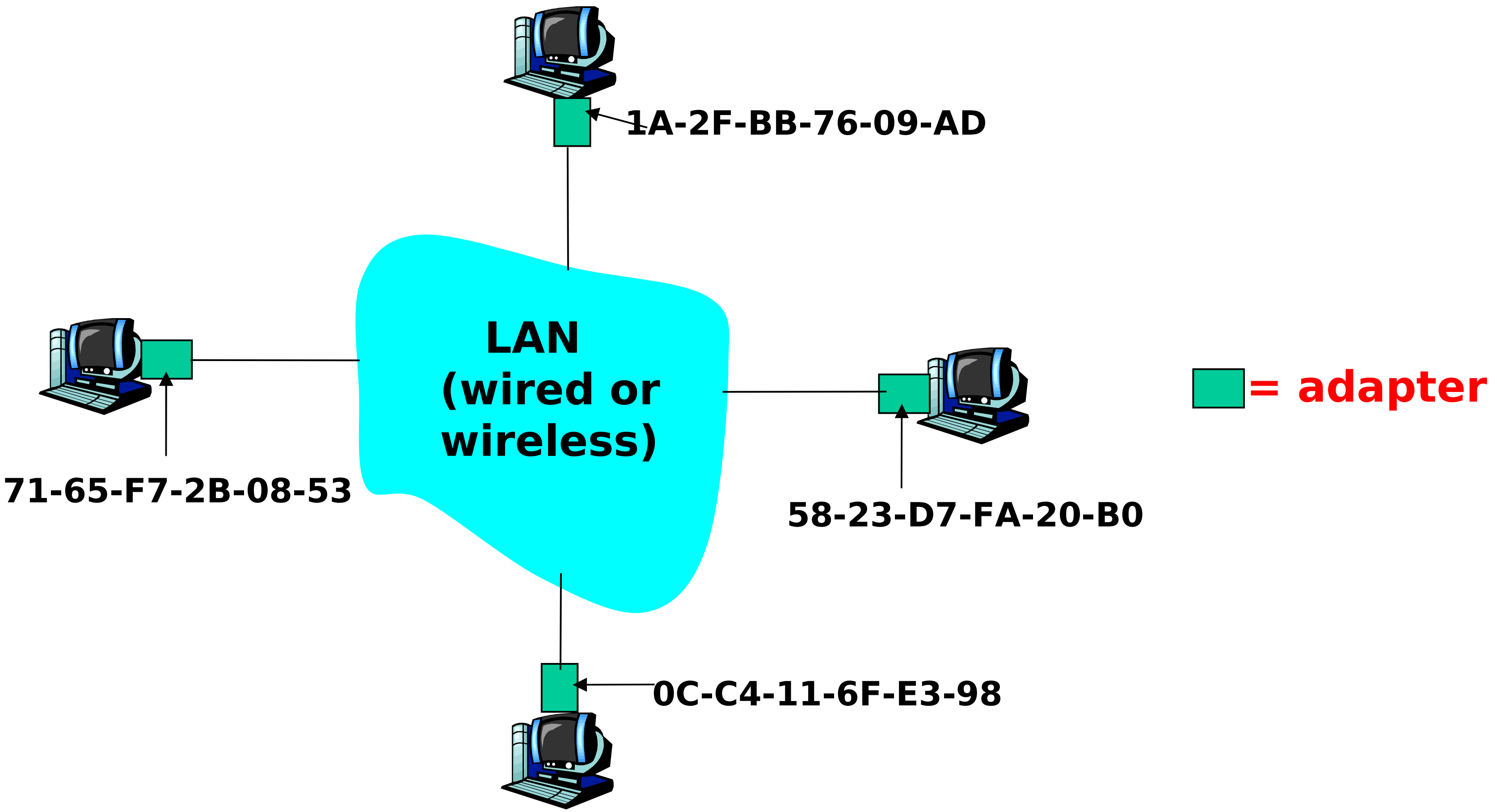
    http://www.irongeek.com/i.php?page=security/madmacs-mac-spoofer
    - Smac - http://www.klcconsulting.net/smac/
    - Etherchange - http://ntsecurity.nu/toolbox/etherchange/
  - Linux

```
$  ifconfig eth0 down hw ether 00:00:00:00:00:01
$  ifconfig eth0 up
```

http://www.irongeek.com/i.php?page=security/changemac

MAC Addresses

Each adapter on LAN has unique MAC address except for Broadcast address which is FF-FF-FF-FF-FF-FF



MAC Address

- MAC address allocation administered by IEEE
- Manufacturer buys portion of MAC address space (to assure uniqueness)

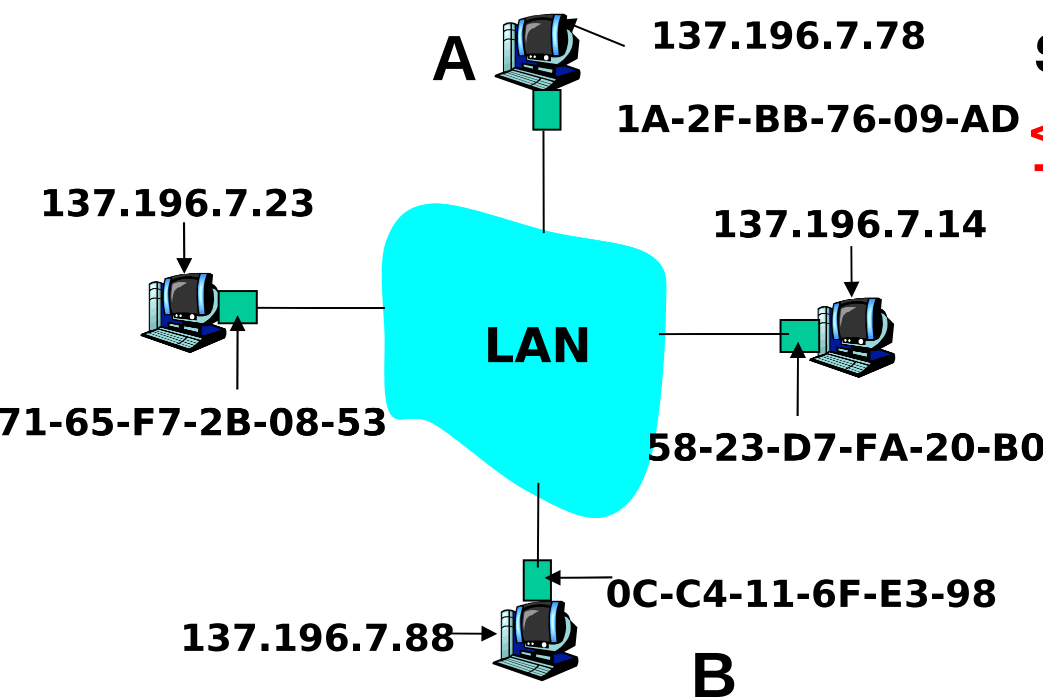
  Table: http://standards.ieee.org/regauth/oui/oui.txt

- Analogy:
  - (a) MAC address … like Social Security Number
    Take it with you
  - (b) IP address … like postal address,
    Changes when you move

- Flat MAC address increases Portability
  - Can move LAN card from one LAN to another
- IP hierarchical address NOT portable
  - Address depends on IP subnet to which node is attached
  - Must change IP address if move to a different subnet

ARP: Address Resolution Protocol

Question: How to determine MAC address of B knowing B's IP address?



- Each IP node on LAN has ARP table
- ARP table: IP/MAC address mappings for some LAN nodes

< IP address; MAC address; TTL>

- TTL (Time To Live): time after which address mapping discarded
- Varies 1 to 20 minutes on average

ARP Cache

- For every outgoing packet sending ARP request and wait for response is inefficient
  - Requires more bandwidth
  - Consumes Time
- So, ARP cache maintained at each node
- Size limit = 512 entries

ARP Protocol: Same LAN

- A wants to send datagram to B, and B’s MAC address not in A’s ARP table
  - A broadcasts ARP query packet, containing B's IP address
  - Shouts to everyone on LAN!!!
  - Destination MAC address = FF-FF-FF-FF-FF-FF
    - This is the MAC broadcast address
  - All machines on LAN receive ARP query

- B receives ARP packet, replies to A with its (B's) MAC address
  - Frame sent to A’s MAC address (unicast)

Types of ARP Messages

- ARP request
  - Who is IP addr X.X.X.X tell IP addr Y.Y.Y.Y
- ARP reply
  - IP addr X.X.X.X is Ethernet Address hh:hh:hh:hh:hh:hh

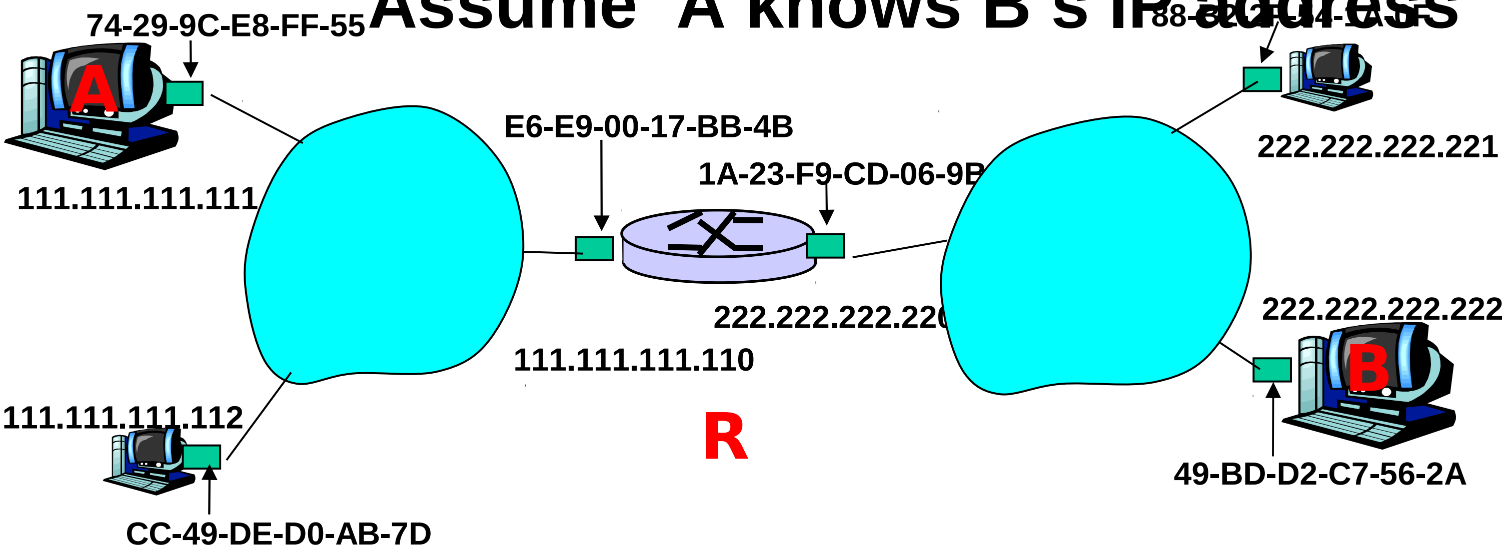
ARP Protocol: Same LAN

- A caches (saves) IP-to-MAC address pair
- Called: ARP table until information becomes old
- Eventually
  - Times out
  - ARP table keeps Soft state information that times out unless refreshed
- ARP is "plug-and-play"
- Nodes create their ARP tables *without intervention from, you, the network administrator*
- **Look at example within one LAN … in class**

ARP Protocol: Routing to another LAN

Walkthrough: Send datagram from A to B via router, R

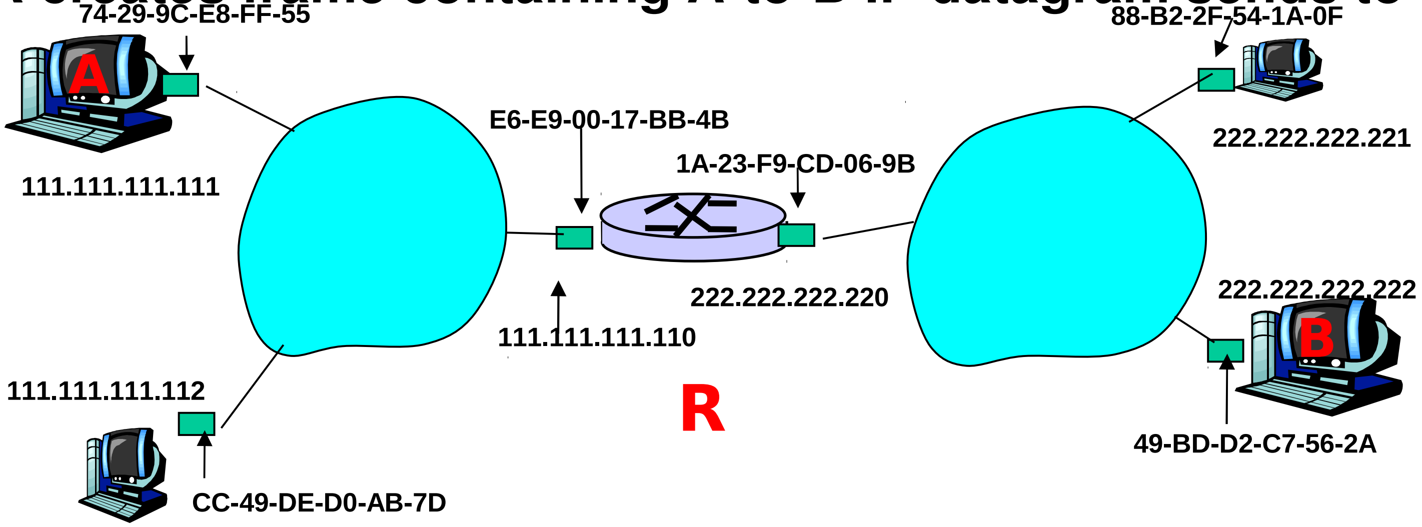
Assume A knows B's IP address



- **Two ARP tables in router R, one for each IP network (LAN)**

ARP Protocol example continued

- A creates IP datagram with source A, destination B
- A uses ARP to get R’s MAC address for 111.111.111.110
- A creates link-layer frame with R's MAC address as destination, frame contains A-to-B IP datagram
  - A’s NIC sends frame
  - R’s NIC receives frame
- R removes IP datagram from Ethernet frame, sees its destined to B
- R uses ARP to get B’s MAC address
- R creates frame containing A-to-B IP datagram sends to B



Summary

- Ethernet highly successful LAN technology
  - Simple, cheap and adaptable
  - Can adapt to new faster underlying medium

- Hubs, Switches and Routers
  - Good to know what each does
  - Hubs and switches at Link Layer
  - Router at higher layer

End

4

Unicast, Multicast, Broadcast Defined

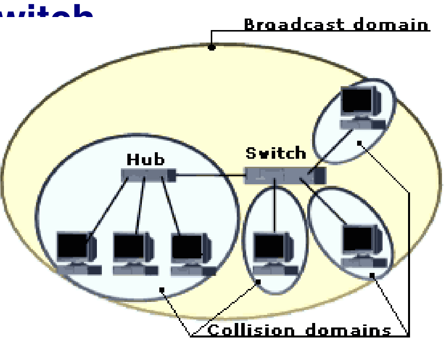
- **Unicast**
  - **Unicast separate transmission stream from source to destination for each recipient, example - HTTP**
- **Multicast**
  - **Traffic is sent to multiple recipients at same time using one transmission stream, data then distributed to end users on separate lines, example – IPTV**
- **Broadcast**
  - **Traffic sent out to every node on network or a portion of the network (LAN segment)**
  - **Broadcasts are issued for address resolution when location of user or server is not known, example – DHCP uses broadcast for IP management**

Broadcast Domain - Definition

- All devices in same broadcast domain will receive broadcast frames originating from any other device within the domain
  - Broadcast frames are explicitly directed to all nodes in same network
  - Broadcast domains are typically bounded by routers because routers do not forward broadcast frames
  - Broadcast domains are Layer 2 segments, which can be extended or separated by using appropriate network components

Ethernet LAN with Switch and Hub

- Switches separate individual computers into their own collision domain
- Broadcast domain all computers connected via a switch
  - Unless configured otherwise



Differences Logical vs. Physical

- Look at the Differences Between Logical and Physical Addresses ...