Computer Networks and Communication

Lecture 11-12

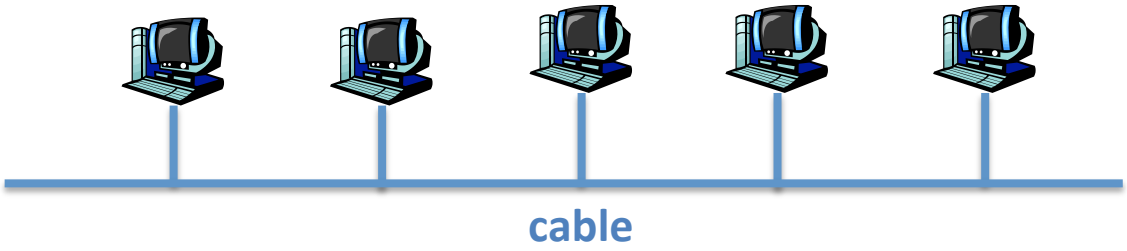
Link Layer II

Local Area Network

- Local Area Network (LAN)
- Networks within a single building or campus
- Transmission speed: 10Mbps – 10Gbps
- Most of them use **Ethernet** protocol (IEEE 802.3) to transport data
- Different LAN can be categorized based on e.g.,
  - **Topologies**: How they are physically connected
  - **Communication medium**: Which cables are employed (or is it a wireless LAN?)

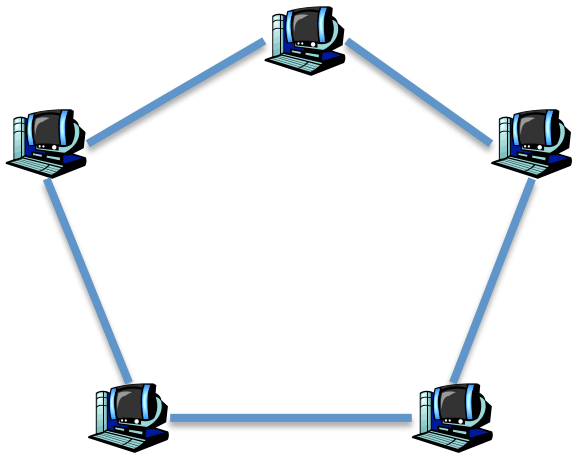
LAN Topology: Bus

- Bus topology
- Nodes are connected using one cable
- Only one node can transmit at a time
- **Terminators** are usually placed at both ends of the bus to prevent transferred signal to reflect back into the channel
- Original version of Ethernet uses this topology

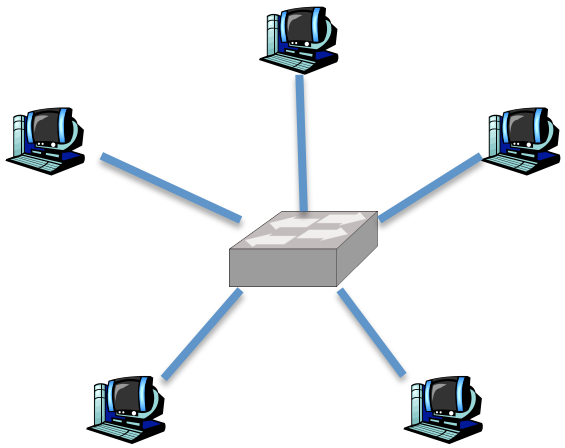


LAN Topology: Ring

- Ring topology
- Nodes are connected using one cable
- Only one node can transmit at a time
- Some protocols such as FDDI uses token to organize medium access
- It is possible to transfer data bidirectional



LAN Topology: Star



- Star topology
- Central node could be a **hub** or **switch**
- Unlike other topologies, each node in star topology has a dedicated medium
- Widely used now (especially in Ethernet)
  - Simple to maintain

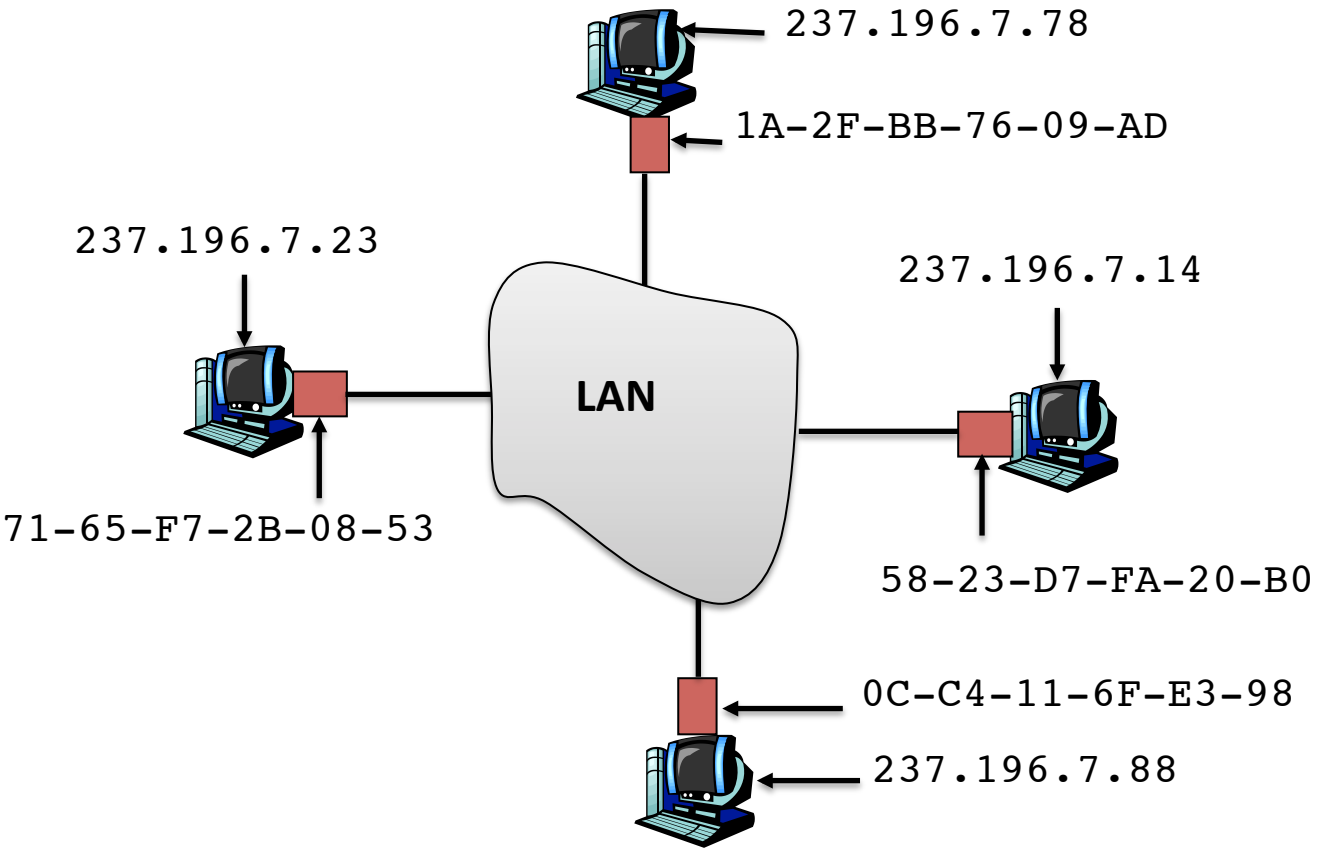
Link-Layer Addressing

- Link layer address is generally called **MAC (Medium-Access Control) address**
- Most LAN and WLAN technologies (e.g. Ethernet and 802.11 a/b/g/n) share the same MAC addressing
  - 48 bit address
  - Each network card in the world has unique address
  - The addresses will not be exhausted until the year 2100 or later

ARP

- **ARP: Address Resolution Protocol**
- Maps the IP address to MAC address
- The mapping is stored in ARP table:
  - Each node has an ARP table
  - Each table contains IP/MAC address mappings
  - The table might not have the mapping of every node in the network
  - Each mapping in the table has a time-to-live, after which the mapping will be discarded

ARP (2)



ARP at Work

1. A wants to send datagram to B, and B's MAC address not in A's ARP table.
2. A **broadcasts** ARP query packet, containing B's IP address
   - Destination MAC address = FF-FF-FF-FF-FF-FF
   - all machines on LAN receive ARP query
3. B receives ARP packet, replies to A with its (B's) MAC address
   - frame sent to A's MAC address (unicast)
4. A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
   - soft state: information that times out (goes away) unless refreshed
5. ARP is "plug-and-play":
   - nodes create their ARP tables without intervention from net administrator

Reverse ARP

- In some cases, the host only knows its MAC address but not its IP
  - Diskless network terminal
- **Before** DHCP, such host can request an IP using **RARP (Reverse ARP)**
- RARP is used when a host asks for its IP address
- A host that stores a list or IP-to-MAC mappings would respond to such queries
- RARP is now obsolete
- Another similar protocol: **BOOTP**

Link Layer

- Objectives:

✔ – Error detection and correction

✔ – Multiple access
  - ALOHA, Slotted ALOHA
  - CSMA
  - CSMA/CD

✔ – Link-layer addressing: MAC address

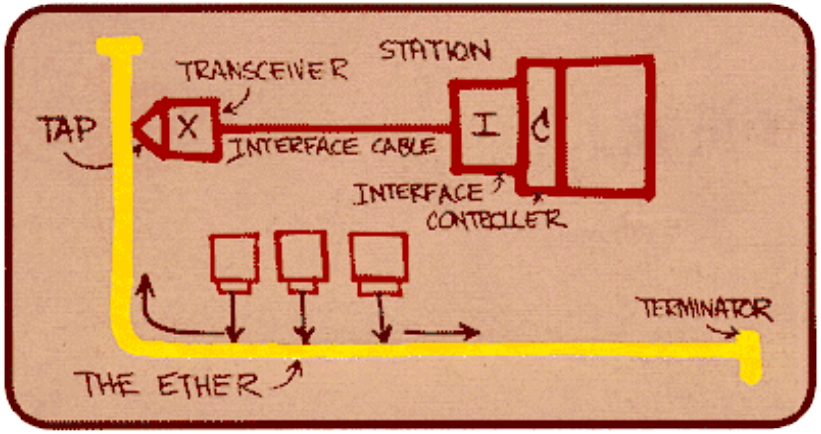
✔ – Flow control

✔ – Reliable data transfer

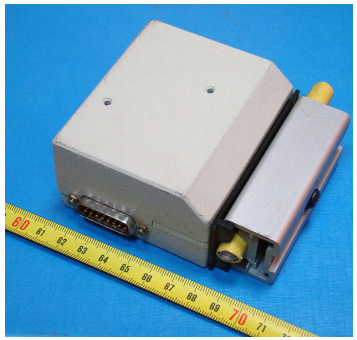
– A number of link layer technologies and protocols

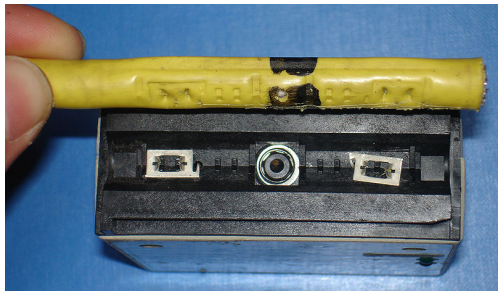
Ethernet

- The most popular LAN protocol
- The name **ether** is taken from the words *luminiferous aether*
  - In the 19th century, we though the electrical signals propagate through this thing
- Original Ethernet networks employ
  - Coaxial cable: **Thick Ethernet**
  - Bus topology
  - Shared cable in bus topology: the ether
  - Connections are made by plugging a pin called **vampire taps** directly into the cable



Original Ethernet Design Sketch





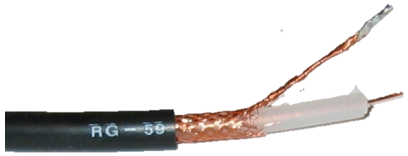
Ethernet Mediums

- Vampire taps are hard to use
- Thick Ethernet is also hard to deploy
- Cables and connectors are thus improved
  - Smaller coaxial cables
  - Use BNC connectors instead of vampire taps
  - **Unshielded twisted pairs (UTP)** cables
  - Fiber optics

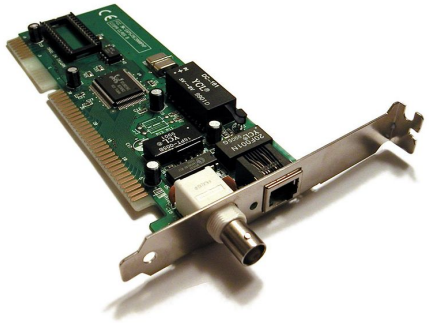
Thick Ethernet

terminator

BNC T-Connector



coaxial cable



Ethernet Cables

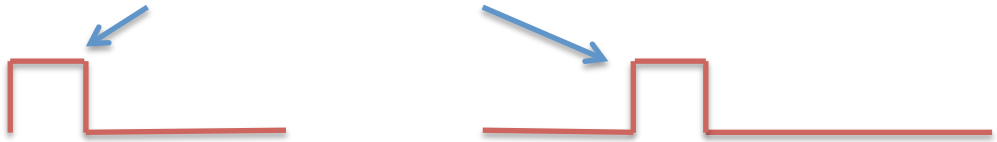
- Ethernet cables are categorized in classes
- The name of each class indicates the capability of the cable
- 10Base5: 10Mbps / Baseband transmission / 500 meters

Name	Cable	Max Segment	# Nodes / Segment	Notes
10Base5	Thick coax	500 m	100	Original; Obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheap
100Base-T	Twisted pair	100 m	1024	Fast Ethernet
1000Base-T	Twisted pair	100 m	1024	Gigabit Ethernet. Currently the most popular
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Example of Ethernet cables

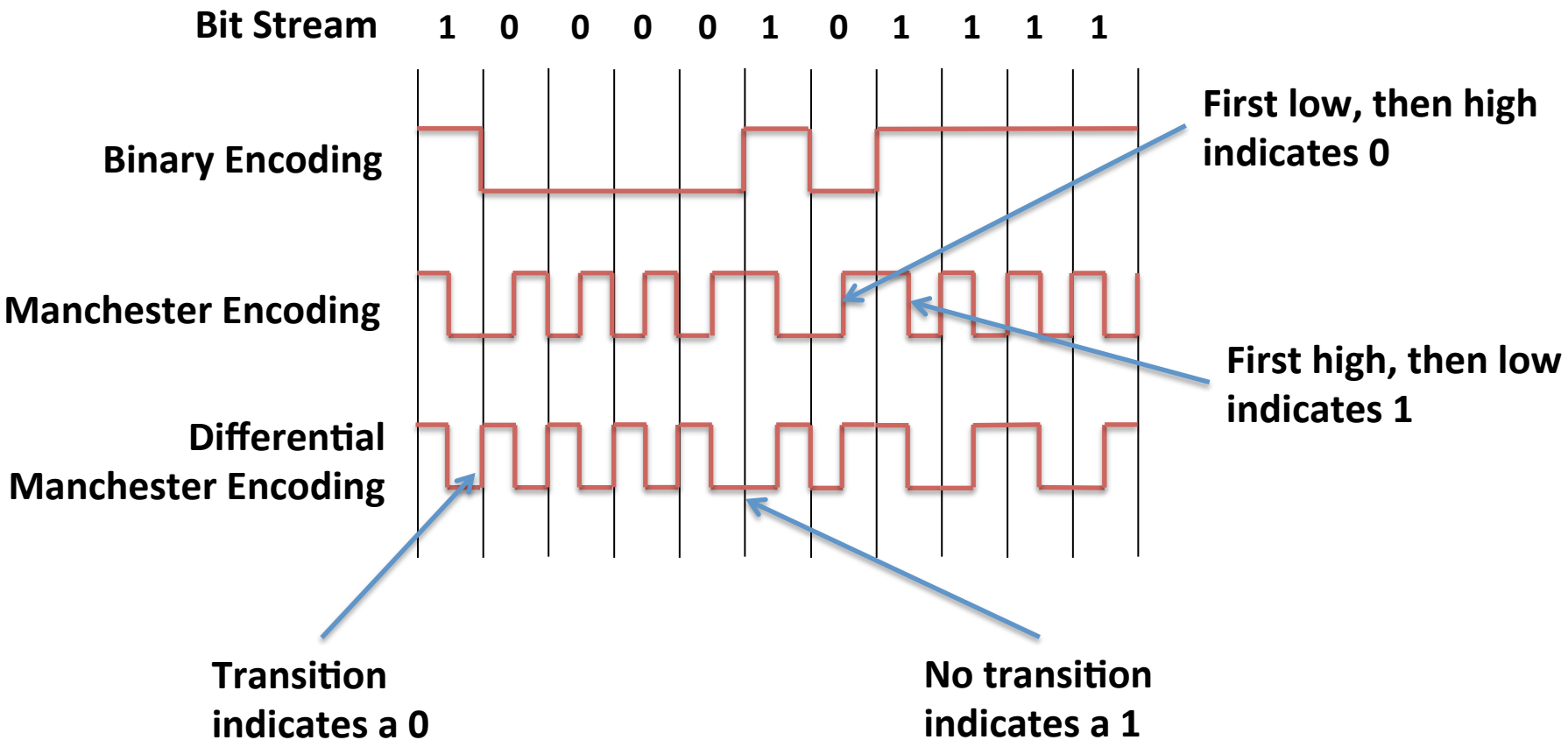
Manchester Encoding

- The Ethernet network sends bit streams through cable using high and low voltages
  - +0.85V for high (one)
  - -0.85V for low (zero)
- However, one cannot just send high and low signals directly
  - It is ambiguous: We don't know when the signal pulses start or stop
  - For example: 100000 and 0010000

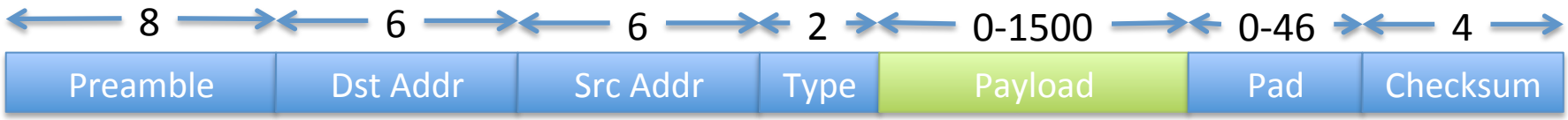


- Ethernet employs **Manchester encoding** to solve this problem
  - Dividing bits into two intervals
  - Changing voltage in the two intervals
  - High to low: bit value = 1
  - Low to high: bit value = 0

Manchester Encoding (2)



Ethernet Frame



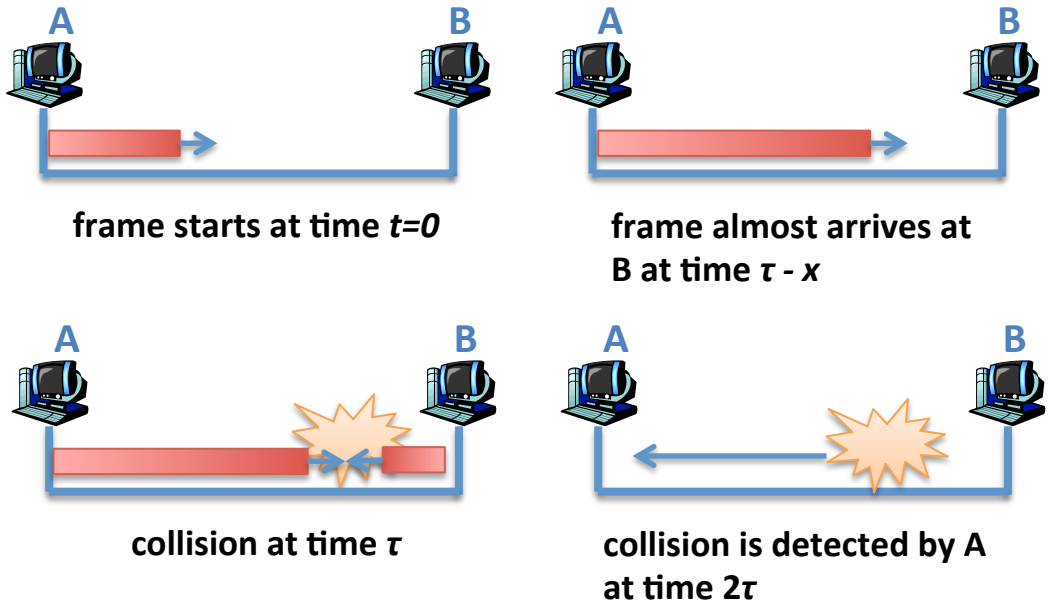
- Ethernet network adaptors encapsulate the datagrams in **frame**
- **Preamble**:
  - Indicates the beginning of the frame
  - 7 bytes pattern of 10101010, followed by
  - 1 byte pattern of 10101011
- **dstAddr** and **srcAddr**: MAC addresses of the sender and receiver, respectively
- **Type**: Indicates higher-layer protocol (usually IP)
- **Padding**: If the frame is too short, the padding is used to fill up the missing bits
- **Checksum**: CRC checksum (**Which CRC scheme is used?**)

Minimum Frame Size

- The Ethernet specifies minimum frame size based on the transportation speed
- This is to ensure that the frame reaches the destination **before** the sender finishes sending the frame
- Otherwise, the sender will not be able to detect collision

τ = propagation time to reach another end

If the frame is too short, A might thought that the frame is correctly sent and the collision belongs to other's frame

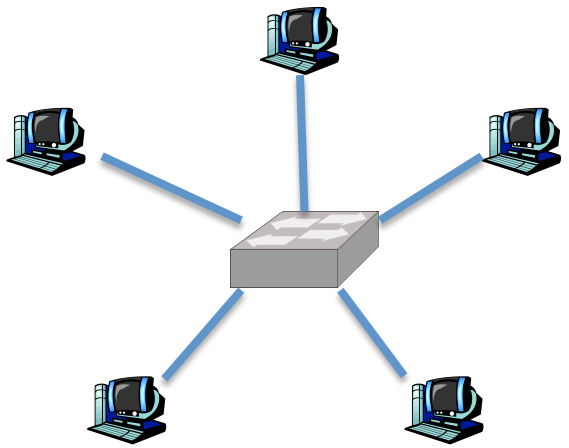


Ethernet Data Transfer Service

- Data transfer service provided by Ethernet is
  - Connectionless
  - Unreliable:
    - CRC check is done only for each frame
    - No ACKs or NACKs are exchanged between sender and receiver
- Ethernet uses CSMA/CD
  - Network interface does not transmit if it senses that the carrier is in use (**carrier sense**)
  - Transmission is aborted if the sending interface sensed that another interface is also sending data (**collision detection**)
  - Before retransmission, the interface backs off and waits for a random period of time

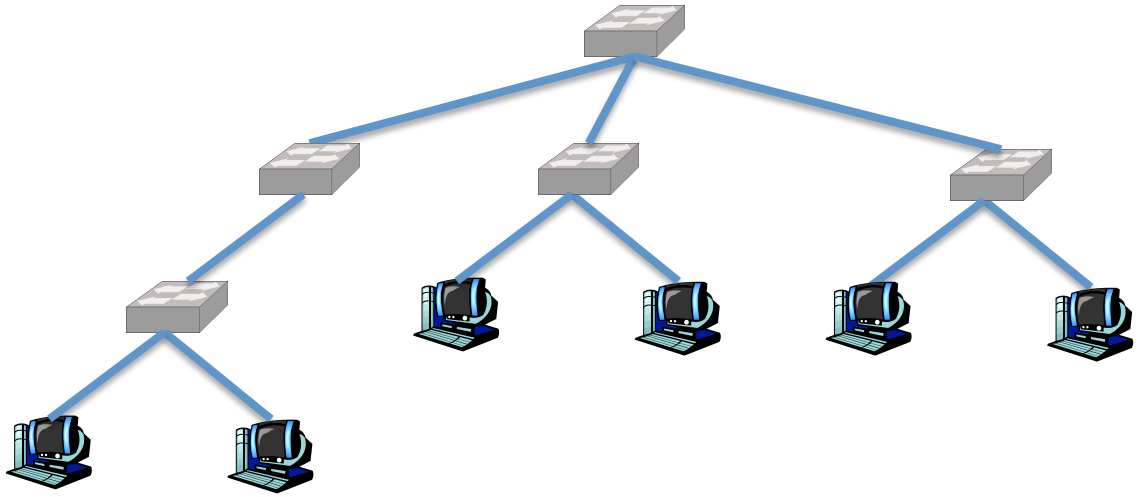
Hubs

- Hubs are essentially physical-layer repeaters:
  - bits coming from one link go out **all** other links
  - at the same rate
  - no frame buffering
  - no CSMA/CD at hub: adapters detect collisions



Interconnecting Hubs

- Backbone hub interconnects LAN segments
- Extends max distance between nodes
- But individual segment collision domains become one large collision domain



Switch

- Like hub, a **switch** is a link-layer devices which forwards incoming frames to appropriate links
  - But smarter
- Switch functionalities and properties:
  - Stores and forwards Ethernet frame
  - **Selectively** forwards frames only to appropriate destination based on MAC destination address
    - Does not broadcast the frame (unlike hubs)
    - MAC address–interface mappings are stored in a **switch table**

Filtering and Forwarding

- When a switch receives a frame:

  index switch table using MAC destination address

  if entry found for destination

  then {

  if dest on segment from which frame arrived

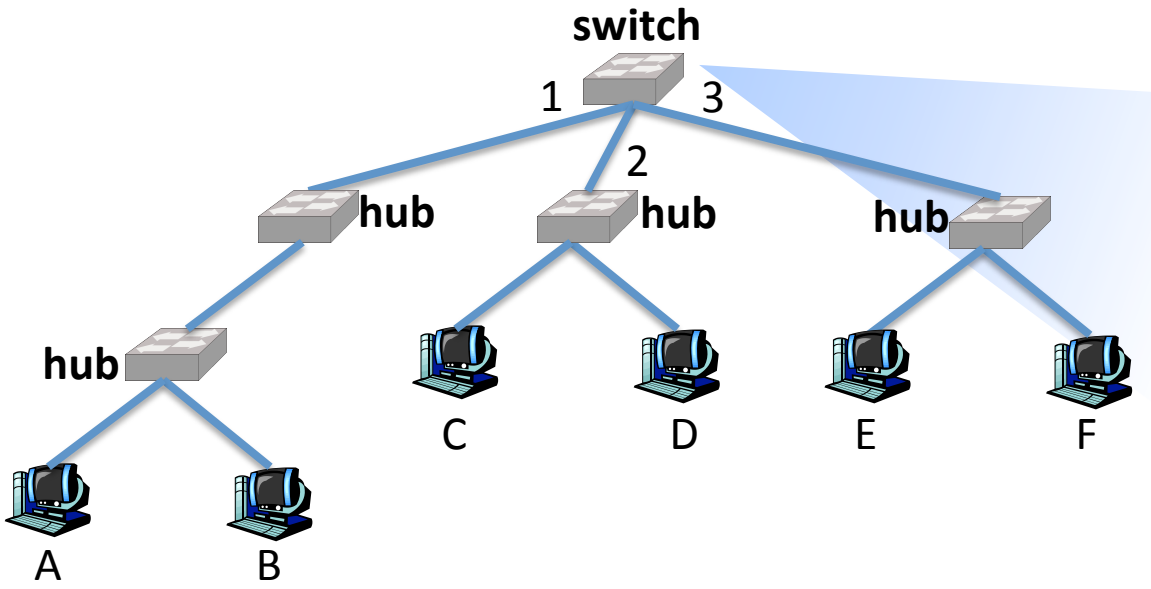
  then drop the frame

  else forward the frame on interface indicated

  }

  else flood (forward frame to all interfaces except the one from which the frame arrived)

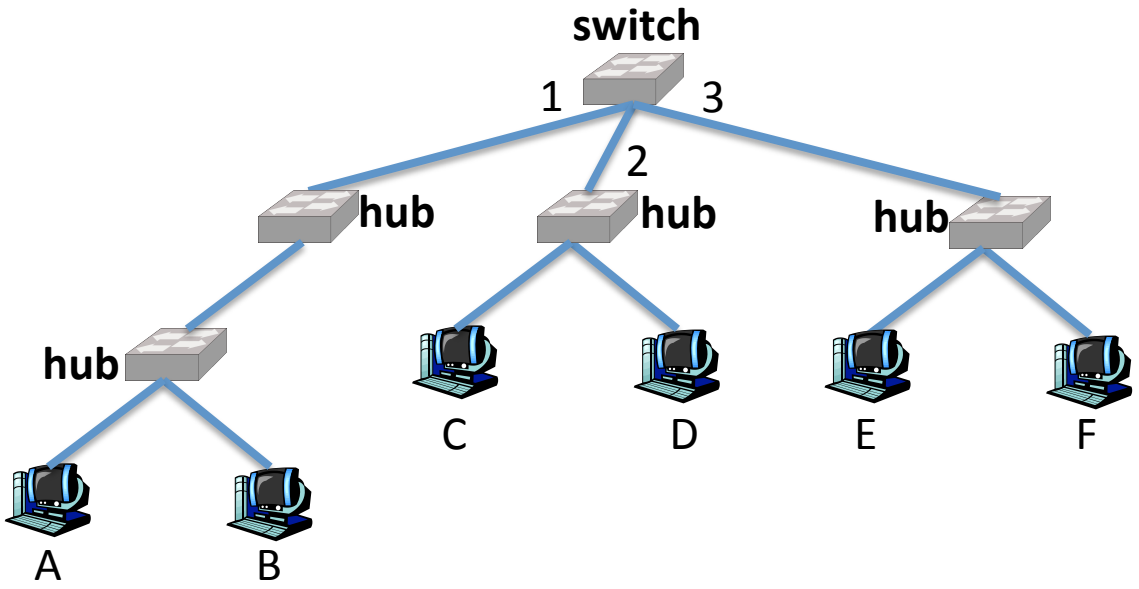
Switch in Action



Address	Interface
A	1
C	2
E	3
F	3
B	1

- Scenario 1: B sends a frame to D
  1. Switch receives frame from B
  2. It records that B is on interface 1
  3. D is not in the switch table, the switch forwards frame into interfaces 2 and 3 (and not 1)
  4. D finally receives the frame

Switch in Action (2)

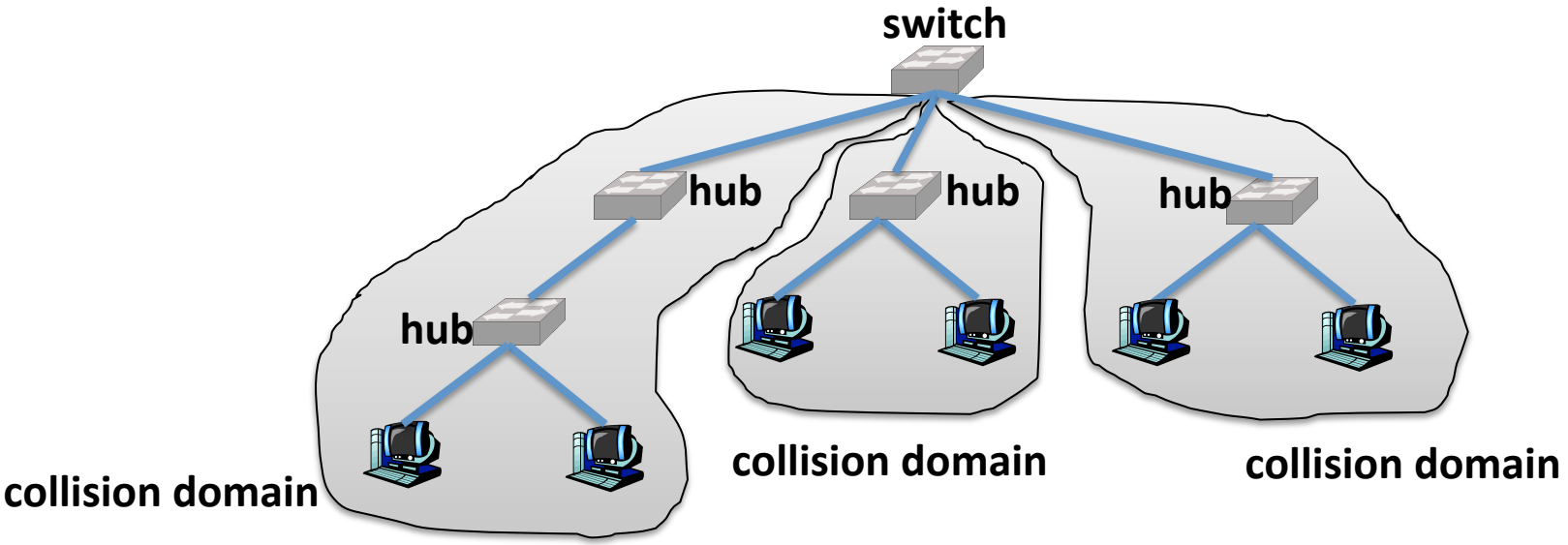


Address	Interface
A	1
C	2
E	3
F	3
B	1
D	2

- Scenario 2: D replies back to B
  1. Switch receives frame from D
  2. It records that D is on interface 2
  3. Because B is in the table, switch forwards frame only to interface 1
  4. B receives the frame

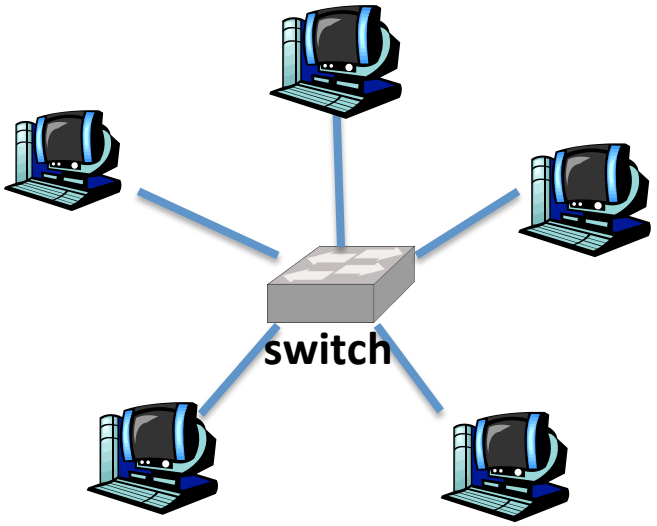
Traffic Isolation

- With selective forwarding, switch effectively breaks subnet into LAN segments
- Switch filters packets:
  - Same LAN-segment frames are not forwarded onto other LAN segments
  - Segments become separated **collision domain**



Dedicated Access

- Hosts may have direct connection to switch
- No collision and full duplex
- This is what you normally have at home

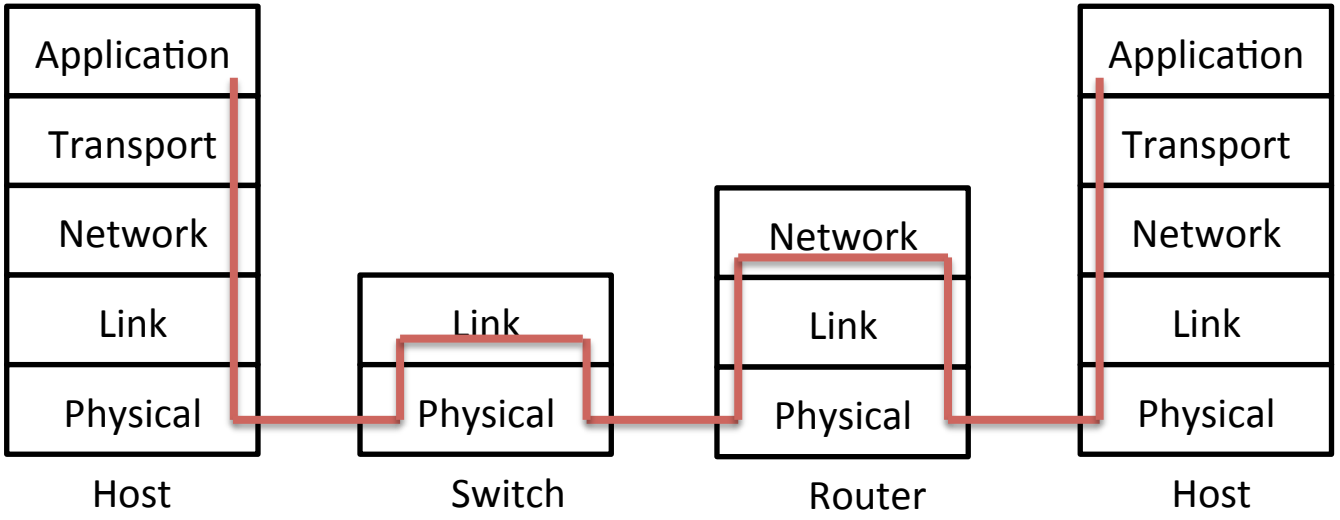


Switch Types

- **Store-and-Forward switch**
  - Buffer the entire incoming frames before they are sent away
  - Perform CRC check on the stored frames
- **Cut-Through switch**
  - The frames are forwarded to the destination without buffering
  - Reduce delay
  - More prone to error

Switches and Routers

- Both store-and-forward devices
  - Routers: network layer devices (examine network layer headers)
  - Switches: link layer devices
- Routers maintain routing tables, implement routing algorithms
- Switches maintain switch tables, implement filtering, learning algorithms



Switch: Conclusion

- Instead of simply sending frames into the medium, switch selectively sends frames directly to the receivers
  - Multiple data transfer are carried out in parallel
  - Switch automatically learns which nodes are connected to which interface
- With switch, Ethernet is advanced from **shared medium** to **switched medium**
  - No collision at all!

Other Link Layer Technologies

- We have discussed link-layer technologies which are:
  - Broadcasting
  - Connectionless
- Now, let's take a look into other technologies:
  - Point-to-point protocol: **PPP**
  - Connection oriented protocols: **ATM**, **MPLS**

PPP

- **PPP**: **Point-to-Point protocol**
- Designed to be used in point-to-point links
  - Example: Dialup, DSL, ISDN, serial cable
  - Connect only two peers
  - No media access control
  - No MAC addressing
  - Works with any network-layer protocol
- PPP functionalities
  - Link establishment
  - Authentication
  - Link termination
  - Error detection

PPP Variations

- **PPP over Ethernet (PPPoE)**
  - Encapsulate PPP frame within Ethernet frame
  - Widely used in DSL (Digital Subscriber Line)
  - Ethernet is connectionless and does not recognize "connection"
  - PPP is used to establish virtual point-to-point link between two hosts
- **PPP over ATM (PPPoA)**
  - Encapsulate PPP frame within ATM cell

ATM

- **ATM: Asynchronous Transfer Mode**
- Designed in early 1990 to be used as the ultimate protocol
  - Integrated, end-to-end transportation of voice, video and data
  - Quality-of-service can be guaranteed
- It was one of the competitors of Ethernet
- Now, it is used only in Internet backbones and telephone systems
- It is much more complex and difficult to maintain than the Ethernet

ATM (2)

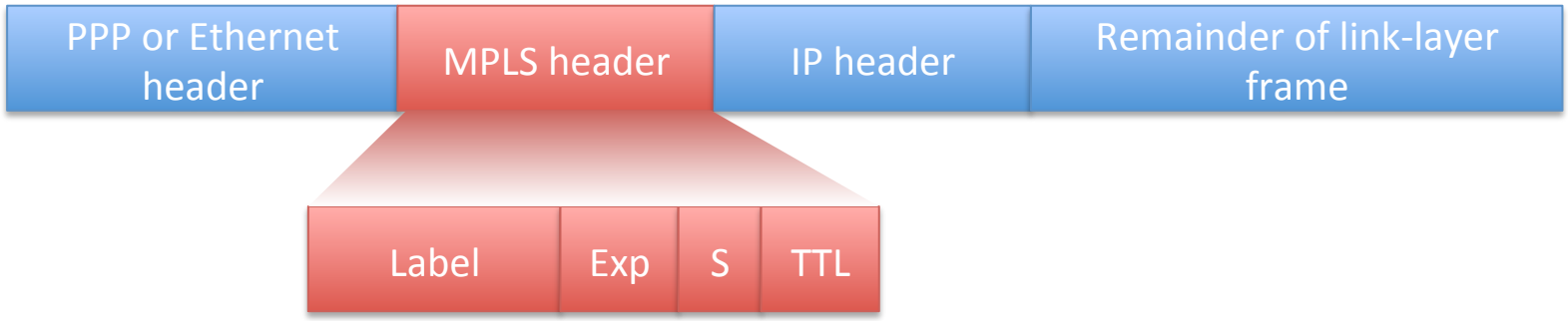
- ATM is a **connection-oriented** protocol
- A **virtual circuit** must be established before two hosts can communicate to each other
  - Network resources must be reserved beforehand
  - A circuit can be **switched** or **permanent**
  - Each circuit has a virtual circuit identifier (VCI)
- ATM transfer data in **cells**
  - Small, fixed-size packet
  - Cell size 53 bytes: 5 bytes header, 48 bytes payload
  - Fixed-size cell allows shorter processing time
- Common speed: 155-622 Mbps

ATM (3)

- Advantages of ATM VC approach:
  - QoS performance guarantee for connection mapped to VC (bandwidth, delay, delay jitter)
- Drawbacks of ATM VC approach:
  - Inefficient support of datagram traffic
  - One permanent VC between each source-destination pair does not scale
  - Switched VC introduces call setup latency, processing overhead for short lived connections

MPLS

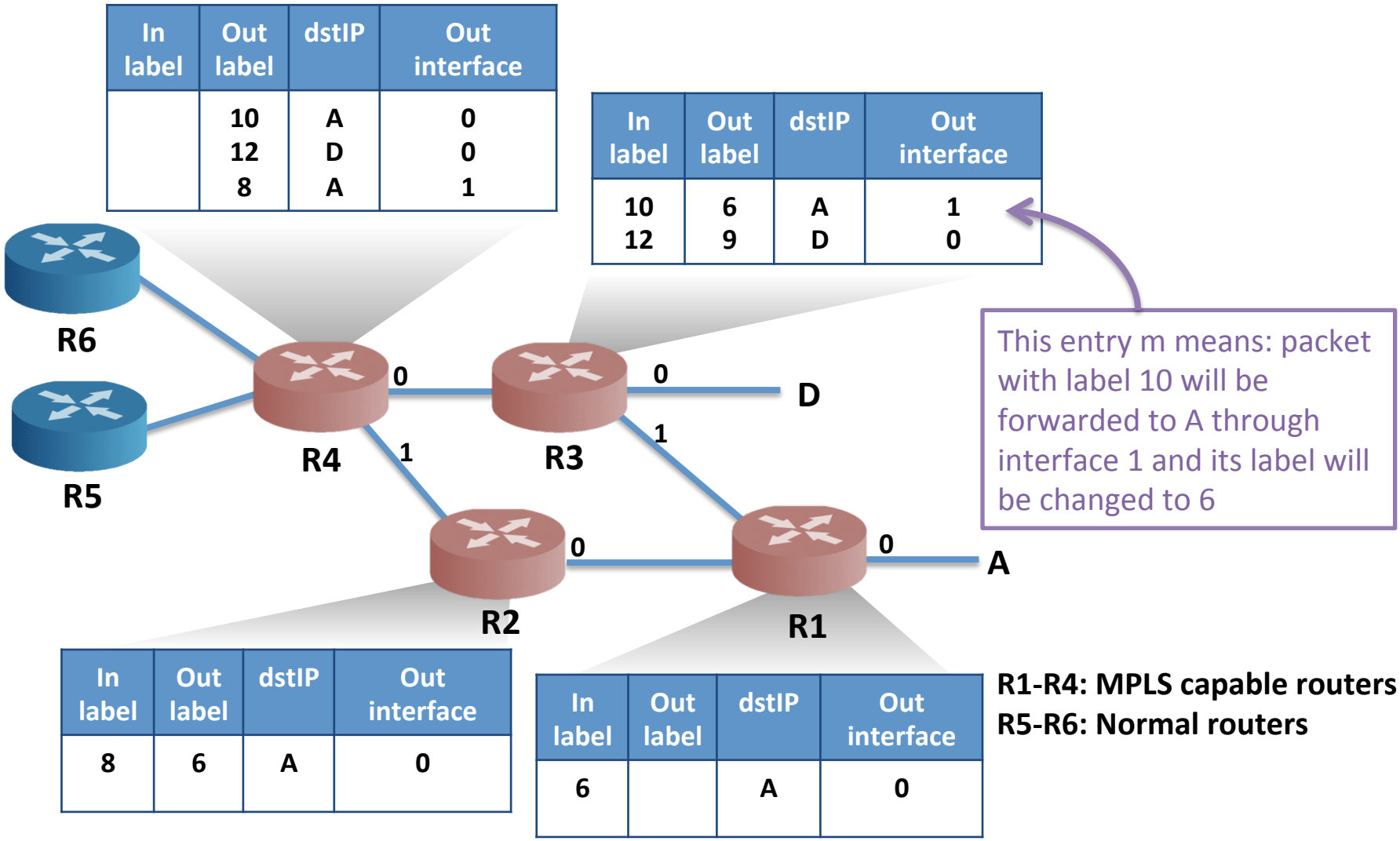
- **MPLS: Multiprotocol Label Switching**
- Designed to speed up IP forwarding
  - Using fixed length label (instead of IP address) to do forwarding
  - Borrowing ideas from Virtual Circuit (VC) approach
  - But IP datagram still keeps IP address
  - Adding extra header between link and network layers



MPLS (2)

- **MPLS-capable routers** forward packets based on MPLS label
  - Since MPLS is not part of link-layer protocols, it can be used to forward both IP and ATM packets
  - This is where the name "**multiple** protocol" comes from
- MPLS can be used in **traffic engineering**
  - Forwarding packets through **specific path**, with respect to labels
  - Different labels, different path
  - This cannot be done with IP alone
  - Advantage: Performance, QoS, virtual private networks (VPNs)
- A signaling protocol needed to set up forwarding tables
  - **Resource Reservation Protocol** - Traffic Engineering protocol (RSVP-TE)

MPLS Forwarding Table



What we have learned so far

- Principles behind data link layer services:
  - error detection, correction
  - sharing a broadcast channel: multiple access
  - link layer addressing
- Instantiation and implementation of various link layer technologies
  - Ethernet
  - Switched Ethernet
  - PPP
  - Virtualized networks as a link layer: ATM, MPLS
- What's left:
  - Wireless networks
  - Network security