Lecture 5
LAN: Local Area Network

Reading: 4.3 Computer Networks, Tanenbaum

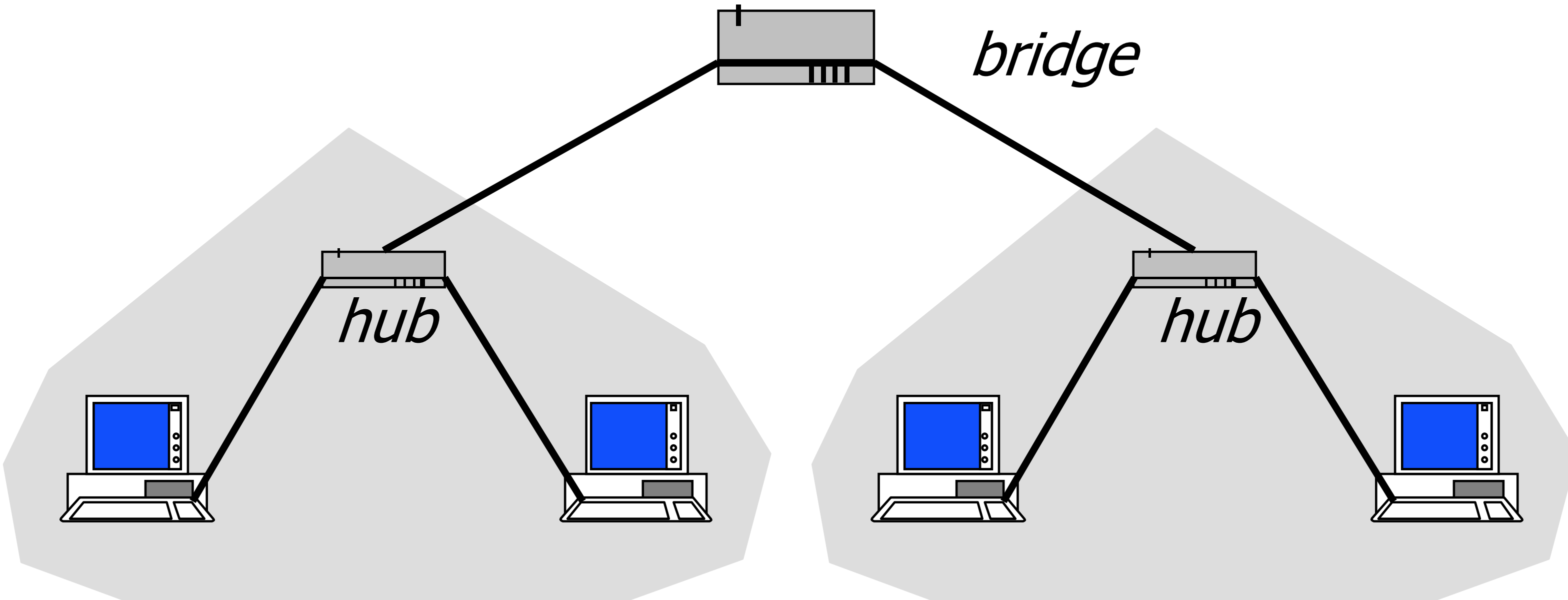
Devices in LAN

Hub, Switch, Bridge, and Router

Devices in LAN

- Repeater (bộ lặp), Hub (bộ chia)
  - Do not offer services of datalink layer
  - Amplify the signal
  - Extend the connection coverage (broadcast zone)
  - <=4 repeaters / 1 network segment (connection between two hosts)
- Bridge (Cầu), Switch (Bộ chuyển mạch)
  - Layer 1 and 2 intermediate system
  - Bridge breaks the network into two collision domains
  - Can store and forward data according to MAC address
    - Receive full frame, check error, forward
- Router (Bộ định tuyến)

Examples



Two ports systems
- Forward MAC frame from one port to the other based on MAC address
- Create two collision domains

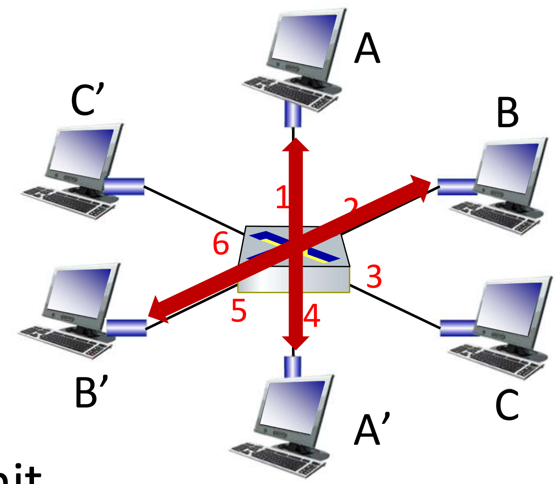
Data forwarding

Switch

- Switch is a link-layer device: takes an *active* role
  - store, forward datalink frames
  - examine incoming frame's MAC address, *selectively* forward frame to one-or-more outgoing links when frame is to be forwarded on segment, uses CSMA/CD to access segment
- transparent: hosts *unaware* of presence of switches
- plug-and-play, self-learning
  - switches do not need to be configured

Switch: multiple simultaneous transmissions

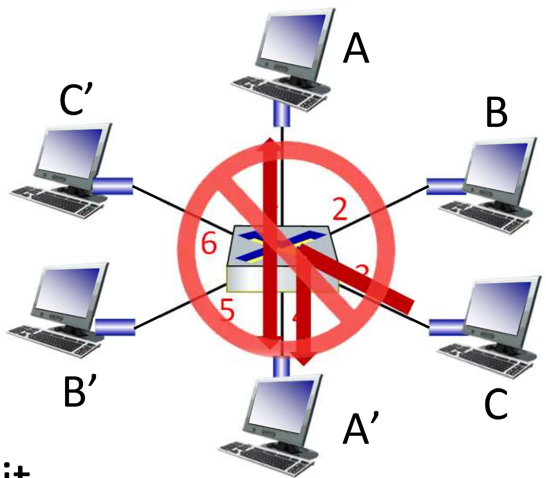
- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, so:
  - no collisions; full duplex
  - each link is its own collision domain
- switching: A-to-A' and B-to-B' can transmit simultaneously, without collisions



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

Switch: multiple simultaneous transmissions

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, so:
  - no collisions; full duplex
  - each link is its own collision domain
- switching: A-to-A' and B-to-B' can transmit simultaneously, without collisions
  - but A-to-A' and C to A' can *not* happen simultaneously



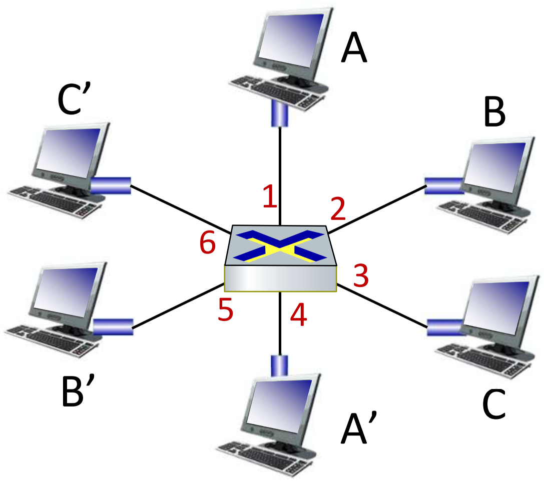
switch with six interfaces (1,2,3,4,5,6)

Switch forwarding table

Q: how does switch know A' reachable via interface 4, B' reachable via interface 5?

A: each switch has a switch table, each entry:

- (MAC address of host, interface to reach host, time stamp)
- looks like a routing table!

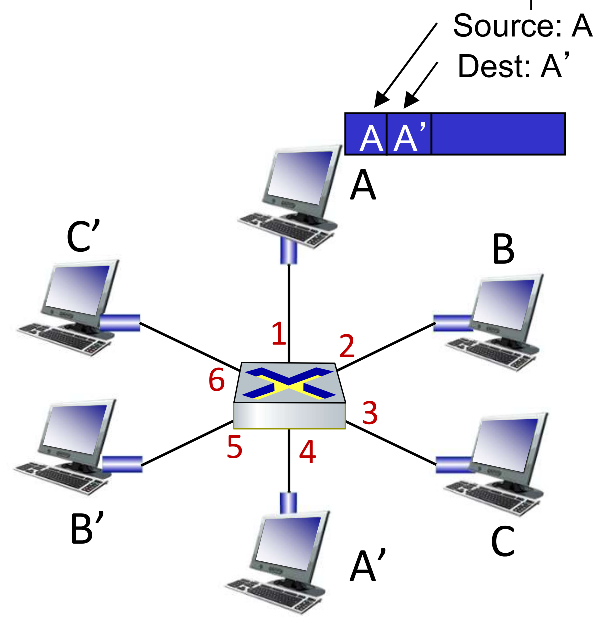


Q: how are entries created, maintained in switch table?

- something like a routing protocol?

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 in switch table



MAC addr	interface	TTL
A	*1*	*60*

Switch table (initially empty)

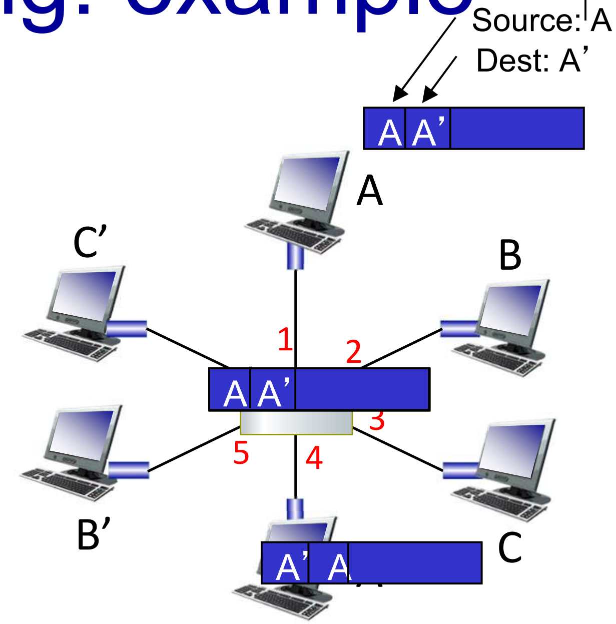
Switch: frame filtering/forwarding

when frame received at switch:

1. record incoming link, MAC address of sending host
2. index switch table using MAC destination address
3. if entry found for destination
   then {
   if destination on segment from which frame arrived
      then drop frame
      else forward frame on interface indicated by entry
   }
   else flood /* forward on all interfaces except arriving interface */

Self-learning, forwarding: example

- frame destination, A', location unknown: flood
- destination A location known: selectively send on just one link

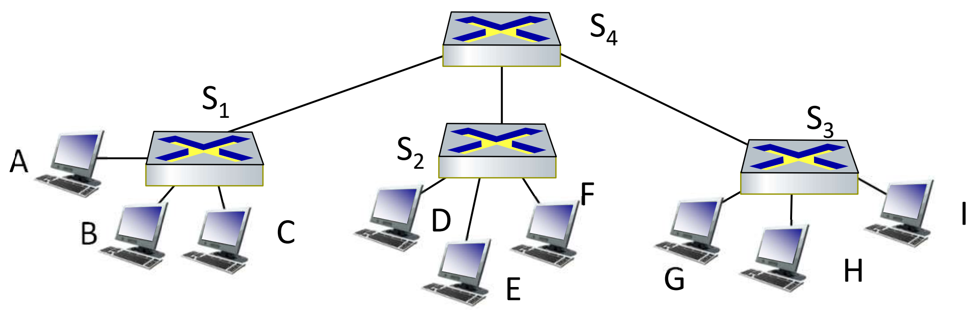


MAC addr	interface	TTL
A	*1*	*60*
A'	*4*	*60*

switch table (initially empty)

Interconnecting switches

self-learning switches can be connected together:

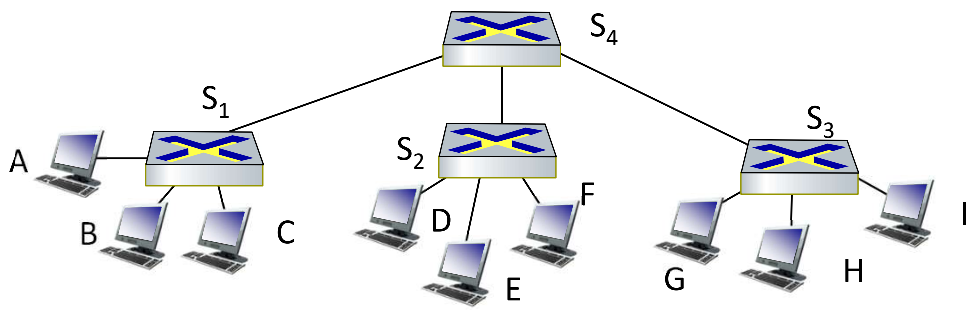


Q: sending from A to G - how does S_1 know to forward frame destined to G via S_4 and S_3?

- *A:* self learning! (works exactly the same as in single-switch case!)

Self-learning multi-switch example

Suppose C sends frame to I, I responds to C



Q: show switch tables and packet forwarding in S_1, S_2, S_3, S_4

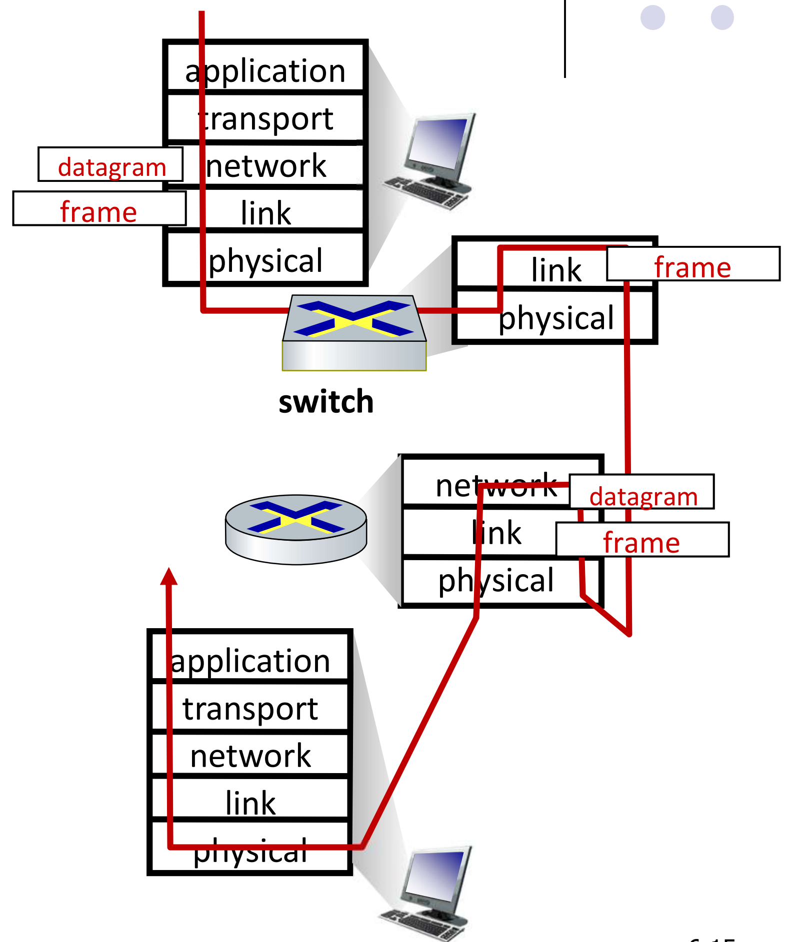
Switches vs. routers

both are store-and-forward:

- *routers*: network-layer devices (examine network-layer headers)
- *switches:* link-layer devices (examine link-layer headers)

both have forwarding tables:

- *routers:* compute tables using routing algorithms, IP addresses
- *switches:* learn forwarding table using flooding, learning, MAC addresses

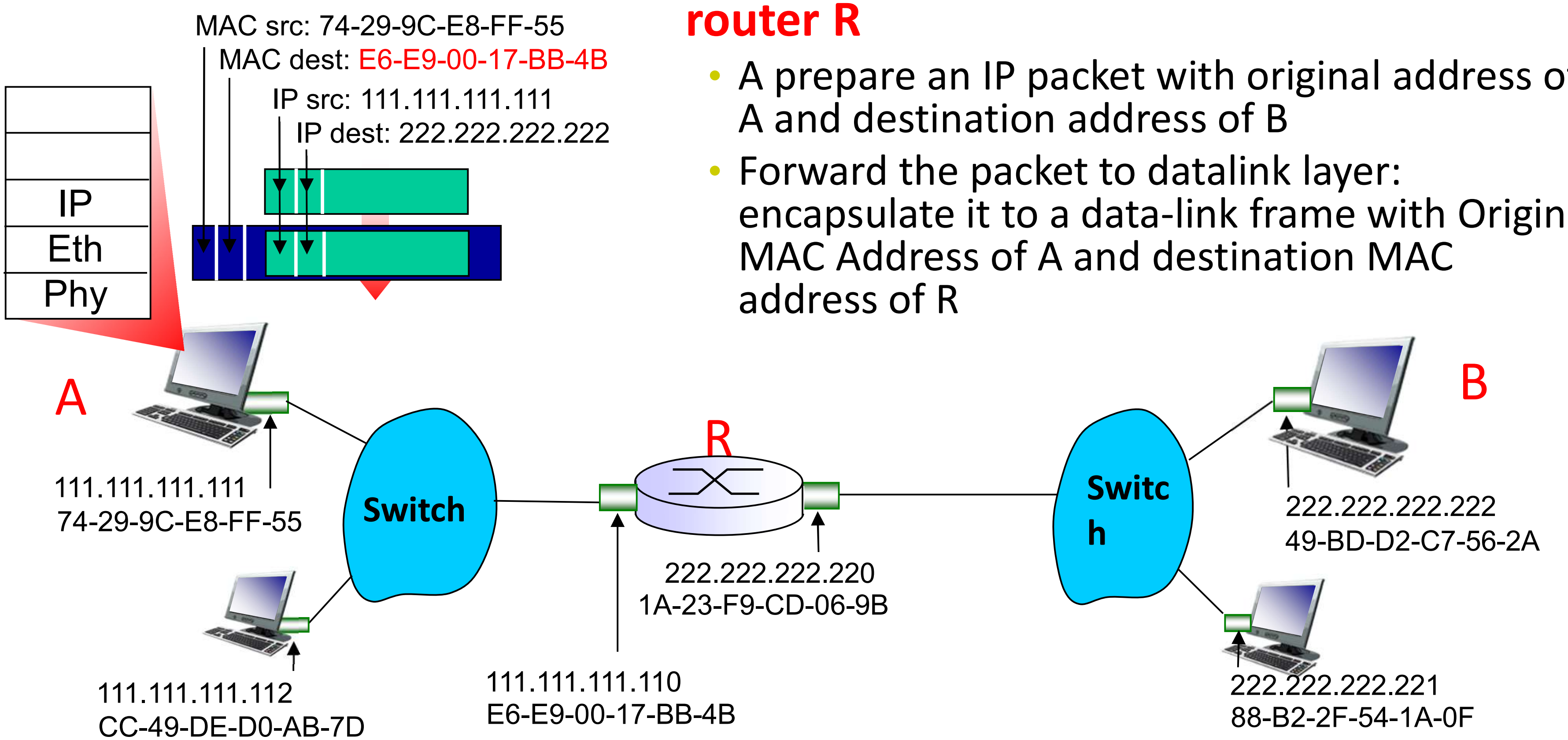


6-15

Router connects LANs

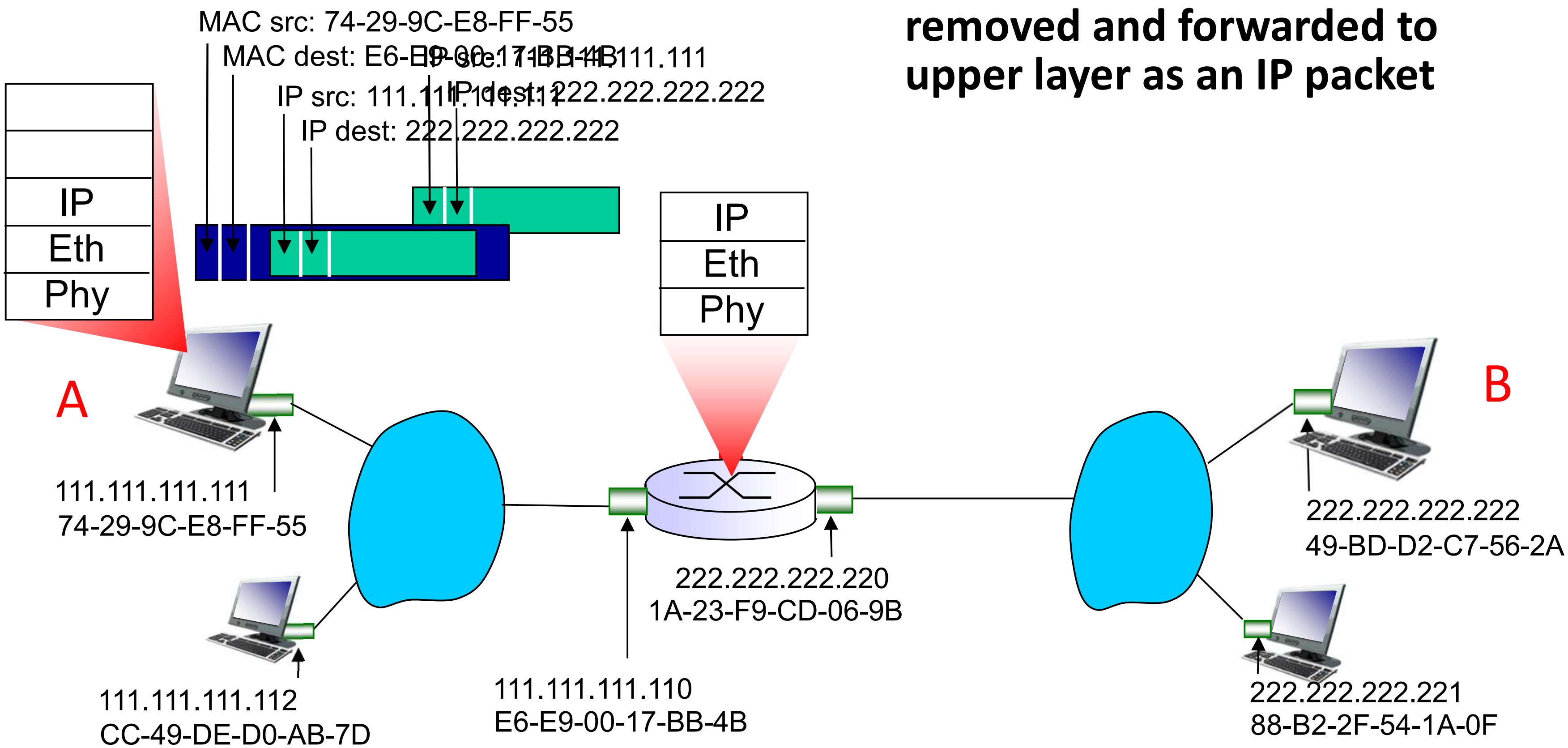
Example: **Send data from A to B through router R**

- A prepare an IP packet with original address of A and destination address of B
- Forward the packet to datalink layer: encapsulate it to a data-link frame with Original MAC Address of A and destination MAC address of R



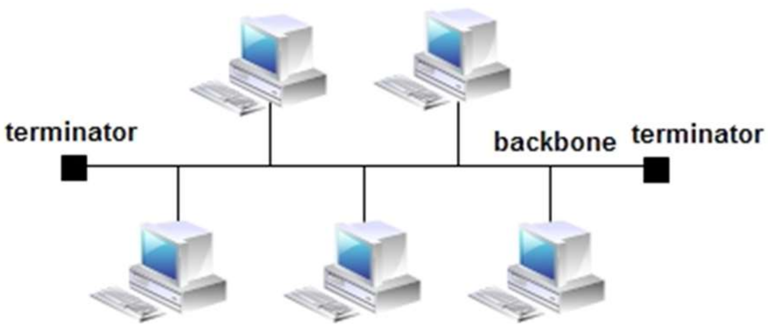
Forward data to other LANs

- **The frame is forwarded from A to R**
- **At R: the frame header is removed and forwarded to upper layer as an IP packet**

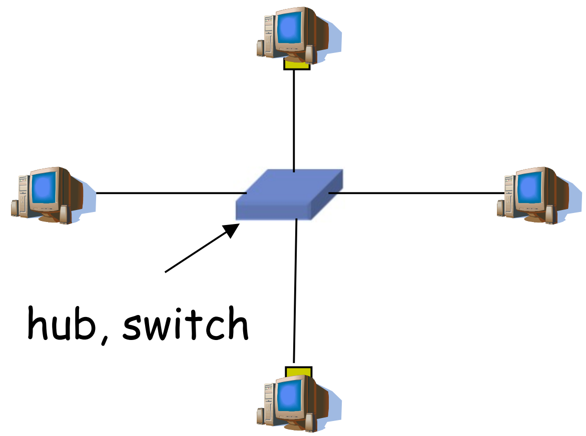


LAN topology and standards

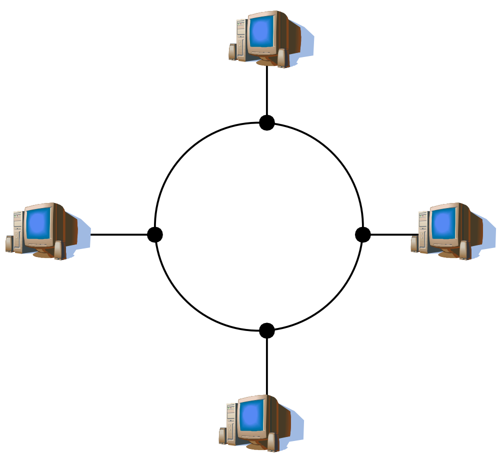
LAN topology



Traditional bus topo



Star

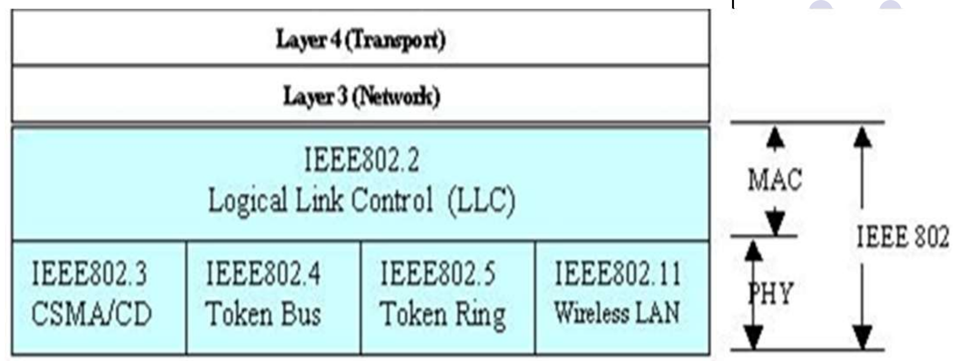


Ring

WLAN

LAN standards: IEEE 802.x

- IEEE 802.1 Network Management
- IEEE 802.2 Logical link control
- IEEE 802.3 Ethernet (CSMA/CD)
- IEEE 802.4 Token bus
- IEEE 802.5 Token Ring
- IEEE 802.6 Metropolitan Area Networks
- IEEE 802.7 Broadband LAN using Coaxial Cable
- IEEE 802.8 Fiber Optic TAG
- IEEE 802.9 Integrated Services LAN
- IEEE 802.10 Interoperable LAN Security
- IEEE 802.11 Wireless LAN



- **IEEE 802.12 demand priority**
- **IEEE 802.14 Cable modems**
- **IEEE 802.15 Wireless PAN**
- **IEEE 802.15.1 (Bluetooth)**
- **IEEE 802.15.4 (ZigBee)**
- **IEEE 802.16 WiMAX**
- **V.v…**

LLC: IEEE802.2

802.2 LLC Header			Information
DSAP address	SSAP address	Control	
8 bits	8 bits	8 or 16 bits	multiple of 8 bits

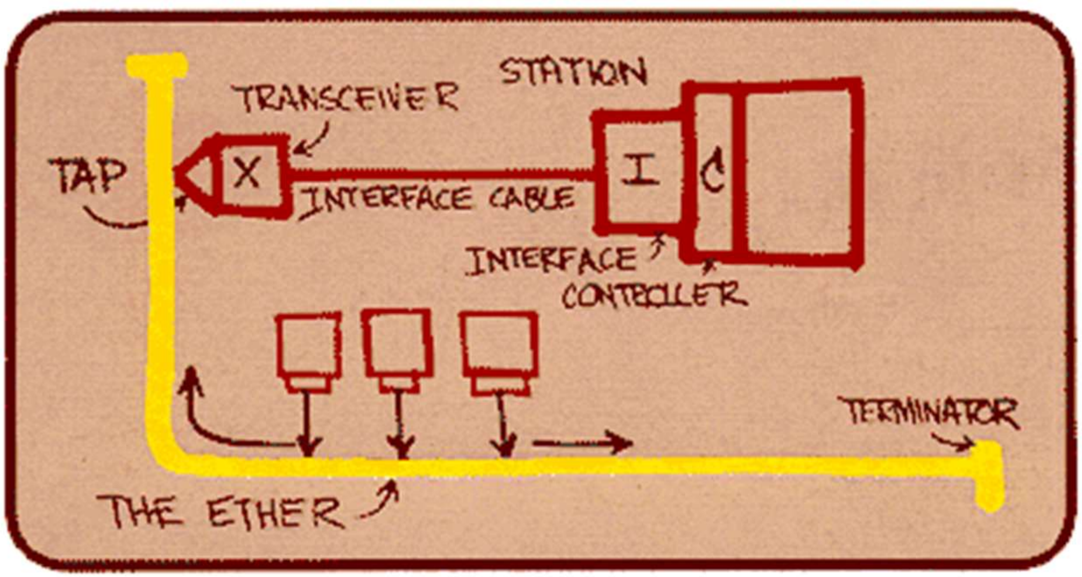
- Roles:
  - Connect with protocols of Network Layer: IPX, DCE, **IP**, v.v..
  - With different physical layers: cable, wireless, optical
- Functionalities:
  - Multiplexing/ Demultiplexing
  - Flow control with 3 different modes:
    - Unacknowledged connectionless
    - Acknowledged connectionless
    - Connection mode
- Frame structure:
  - DSAP & SSAP: Destination/Source SAP, for Multiplexing/ Demultiplexing of the upper layer (which entity of the Network Layer is sending/ receiving LLC frames)
  - Control: define PDU to transfer and control:
    - U-frame: send/receive in connectionless mode (U: Unnumbered)
    - I-frame: frame with information (I: Information), used in acknowledged mode
    - S-frame: for controlling (S: Supervisor)

Practical LLC

- Error checking and flow control (I-frame and S-frame) are used by some upper protocols (NetBIOS).
- U-frame encapsulate PDU without numbering (unnumbered) and therefore NO flow control or error checking are provided.
- Most upper protocols of LLC (TCP/TP) support error checking and flow control
  - Only use LLC as “Unacknowledged connectionless” with U-frame.

Ethernet LAN

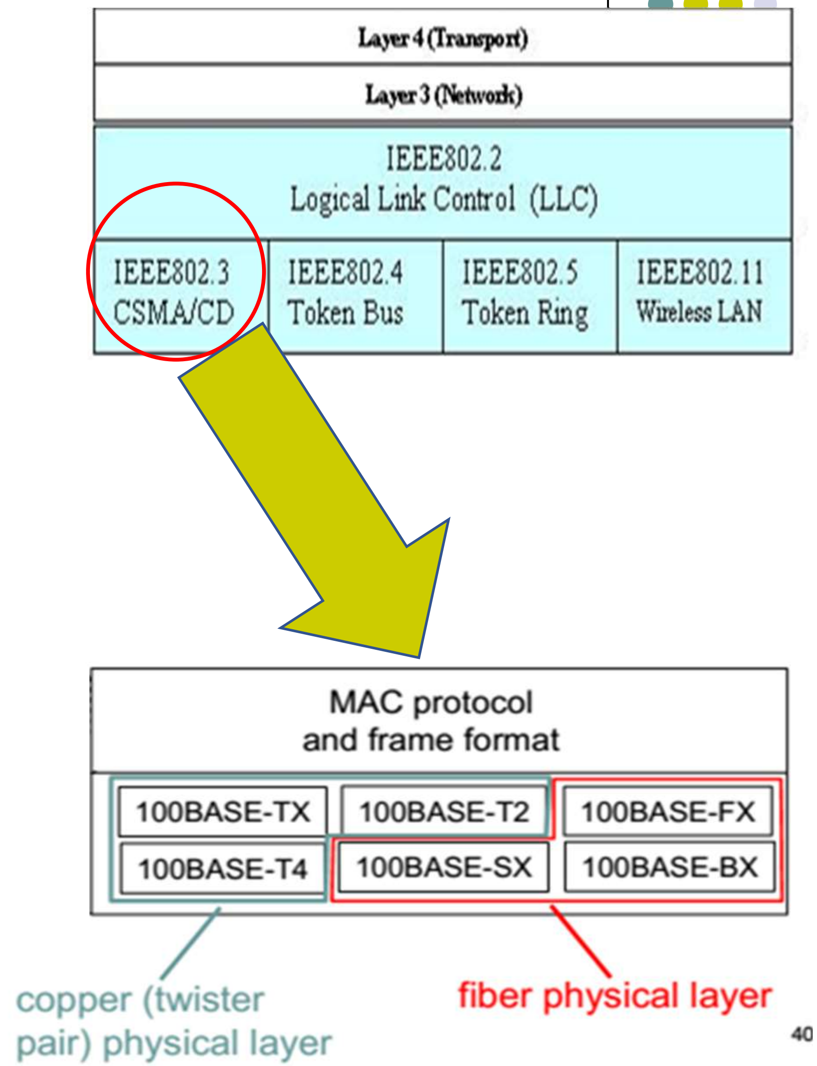
- Layer 2 technology for communication in LAN, invented in 1976
- Standardized in IEEE 802.3
- Ethernet LAN could have different speeds: 3 Mbps – 10 Gbps
  - Ethernet: 10BaseT, 10Base2…



Metcalfe's Ethernet sketch

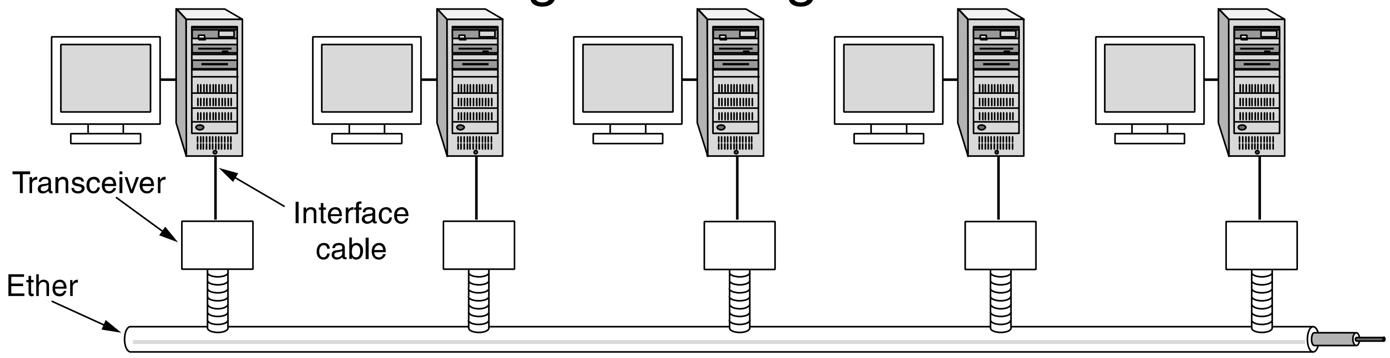
Ethernet: IEEE802.3

- Functions:
  - Media access control (Data-link)
  - Encode signals in cables (Physical)
- CSMA/CD
- Supported cables :
  - Coaxial cables
  - 10BASE-TX: twisted-pair with the bandwidth of 10Mbps
  - 100BASE-TX (fast ethernet): twisted-pair with the bandwidth of 100Mbps
  - Giga Ethernet FX: optical cables (Gbps)



Classical Ethernet

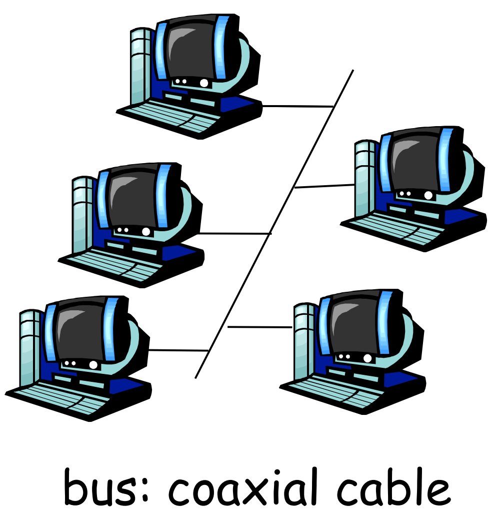
- Bus topology was popular in the past
- All nodes share the same communication medium. Could used a central hub for connecting nodes.
- Use CSMA/CD for media access control.
- Use Manchester encoding at Physical layer
- Use coaxial cable
- Thick Ethernet: Max segment length 500m without converter
- Thin Ethernet: Max segment length 185m without converter

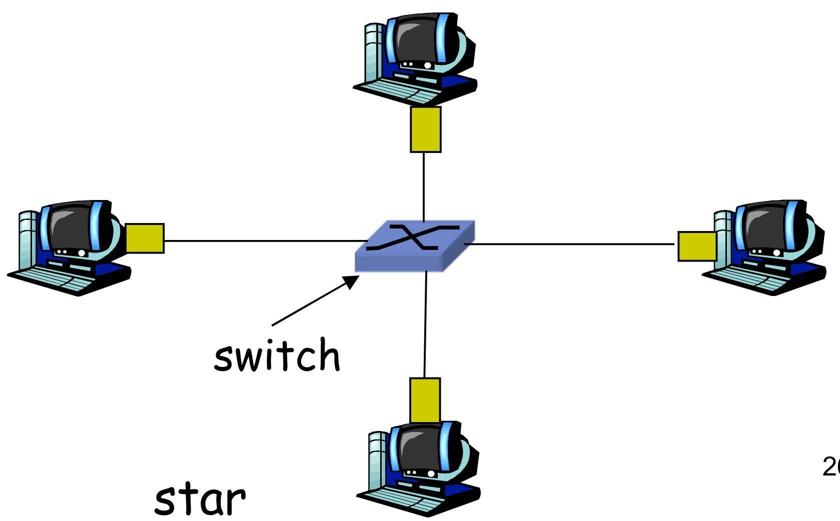


Ref: Computer Network, Tanenbaum

Switched Ethernet

- Switched Ethernet (nowdays):
  - Star topology,
  - Use a central switch Ethernet
  - The switch outputs a frame only to the port linking to the destination ➔ independent connection for each pair of two nodes
  - No collision
  - No media access control is needed.





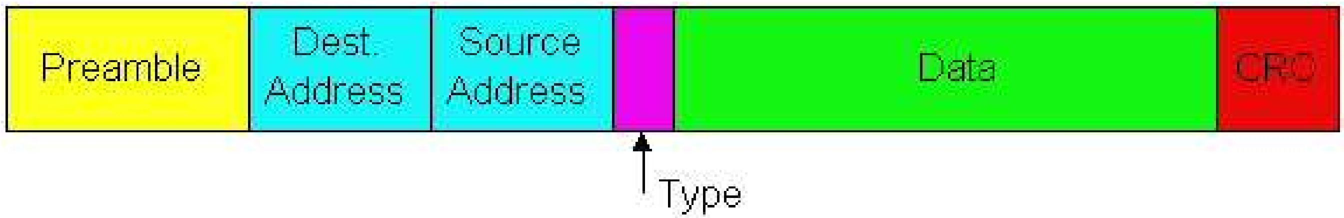
Ethernet frame

- Preamble: Marking the starting of a frame
- Address: Physical addresses of source and destination
  - 6 bytes
- Type: Uppper layer protocol (IP, Novell IPX, AppleTalk, …)
- Checksum: Error detection code. CRC??

Bytes	8		6	6	2	0-1500	0-46	4
(a)	Preamble		Destination address	Source address	Type	Data	Pad	Check-sum
(b)	Preamble	SOF	Destination address	Source address	Length	Data	Pad	Check-sum

Figure 4-14. Frame formats. (a) Ethernet (DIX). (b) IEEE 802.3.

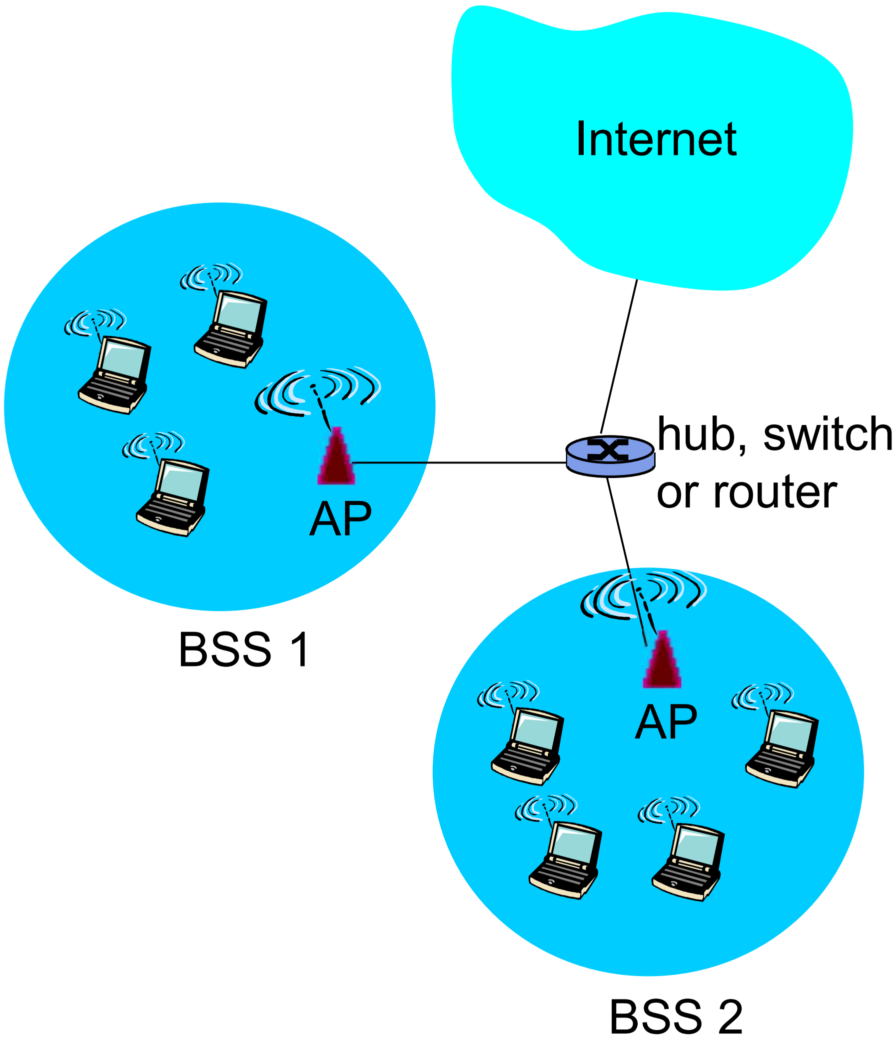
Structure of Ethernet frame



- Preamble: Marking the starting of a frame
- Address: Physical addresses of source and destination
  - 6 bytes
- Type: Uppper layer protocol (IP, Novell IPX, AppleTalk, …)
- Checksum: Error detection code. CRC??

Wireless LAN

Overview of 802.11 LAN



- Include base station = access point and stations with wireless network interfaces
- Base station mode
  - Basic Service Set (BSS)
    - wireless hosts
    - access point (AP): base station
- Ad hoc mode:
  - Stations pay also the role of AP

Standards

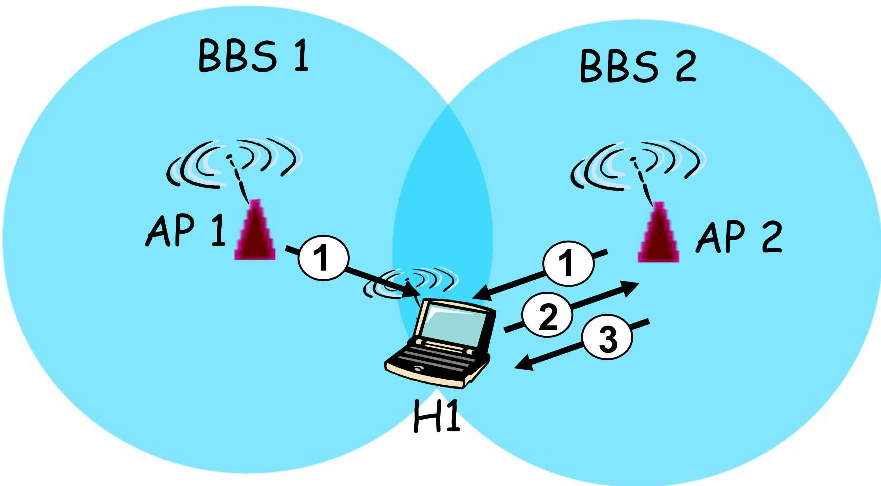
- 802.11b
  - Band 2.4-5 GHz (unlicensed spectrum)
  - Maximum speed 11 Mbps
- 802.11a
  - Band 5-6 GHz
  - Maximum speed 54 Mbps
- 802.11g
  - Band 2.4-5 GHz
  - Maximum speed 54 Mbps
- 802.11n: use multiple antennas (MIMO)
  - Band 2.4-5 GHz
  - Maximum speed 200 Mbps

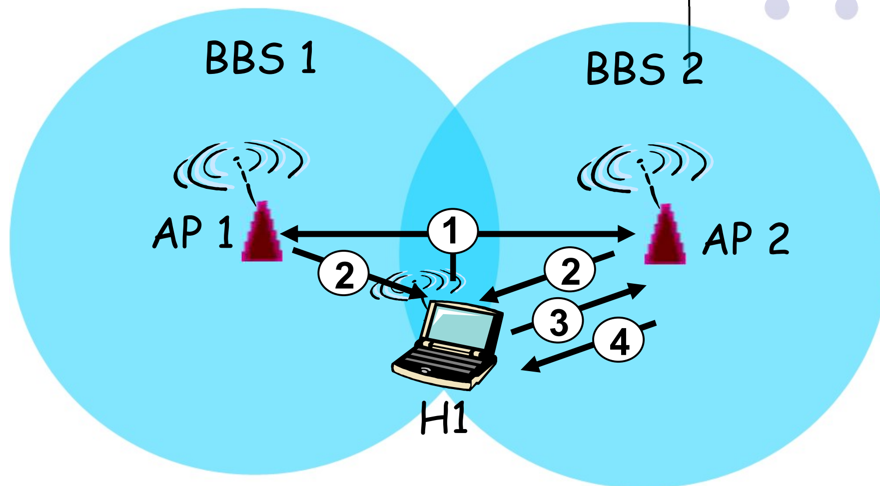
- Employ CSMA/CA for multiple access control
- Working in 2 modes : base-station and ad hoc

802.11: Chanel and connection

- Band is divided into 14 chanels spaced 5MHz apart. Europe uses 13 channels, America uses 11 channels, Japan uses 14 channels.
  - Admin chooses a working frequency for AP (may leave AP to choose automatically)
- Station: need to connect to an AP
  - Scan channels, listen to initial frames (*beacon frames)* containing the ID (SSID) and MAC address of the AP
  - Choose one AP.

Scanning mechanism: active/passive





Passive Scanning:

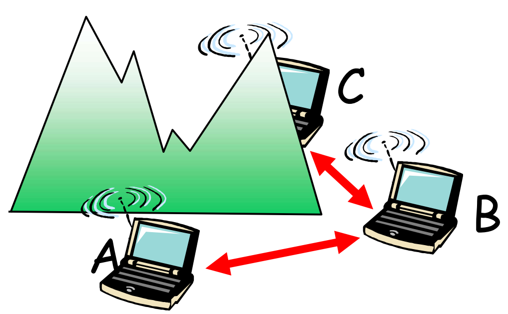
(1) Beacon frames are sent from APs
(2) H1 send a connection request to AP2
(3) AP2 accepts the request

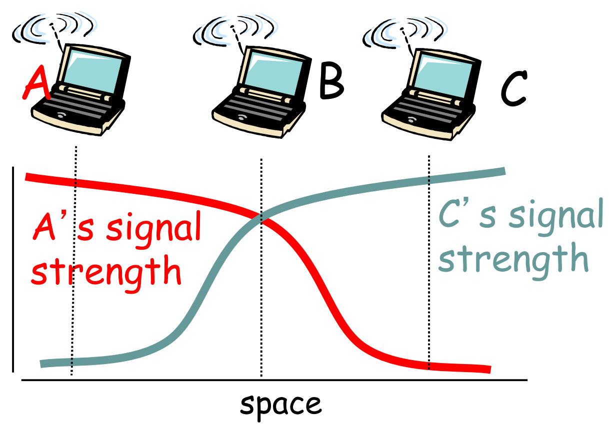
Active Scanning:

(1) H1 broacast the request to find an AP
(2) APs reply with their information
(3) H1 send a connection request to AP2
(4) AP2 accepts the requests

IEEE 802.11: Multiple access control

- 802.11: CSMA
- 802.11: CA – Collision Avoidance
  - It is difficult to implement Collision detection (CD) in wireless environment.
  - In some cases, it is even impossible to detect the collision : hidden terminal, fading





IEEE 802.11 MAC Protocol: CSMA/CA

Sender

1 If the channel is available during **DIFS** time then

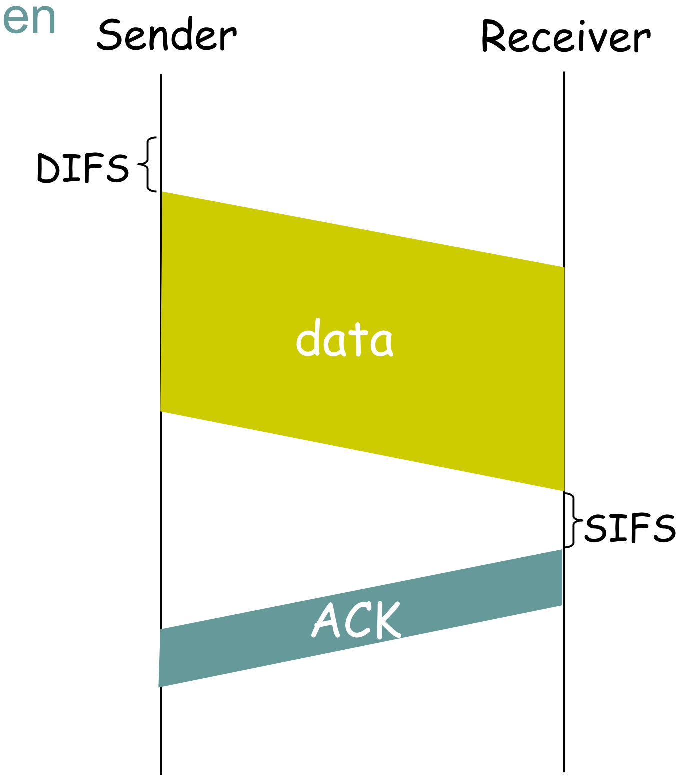
Send the entire frame (no CD)

2 if channel is busy then

Starting random back-off (waiting)

At the end of back-off time, send data

If no ACK is received, double the back-off time and try again.



Receiver

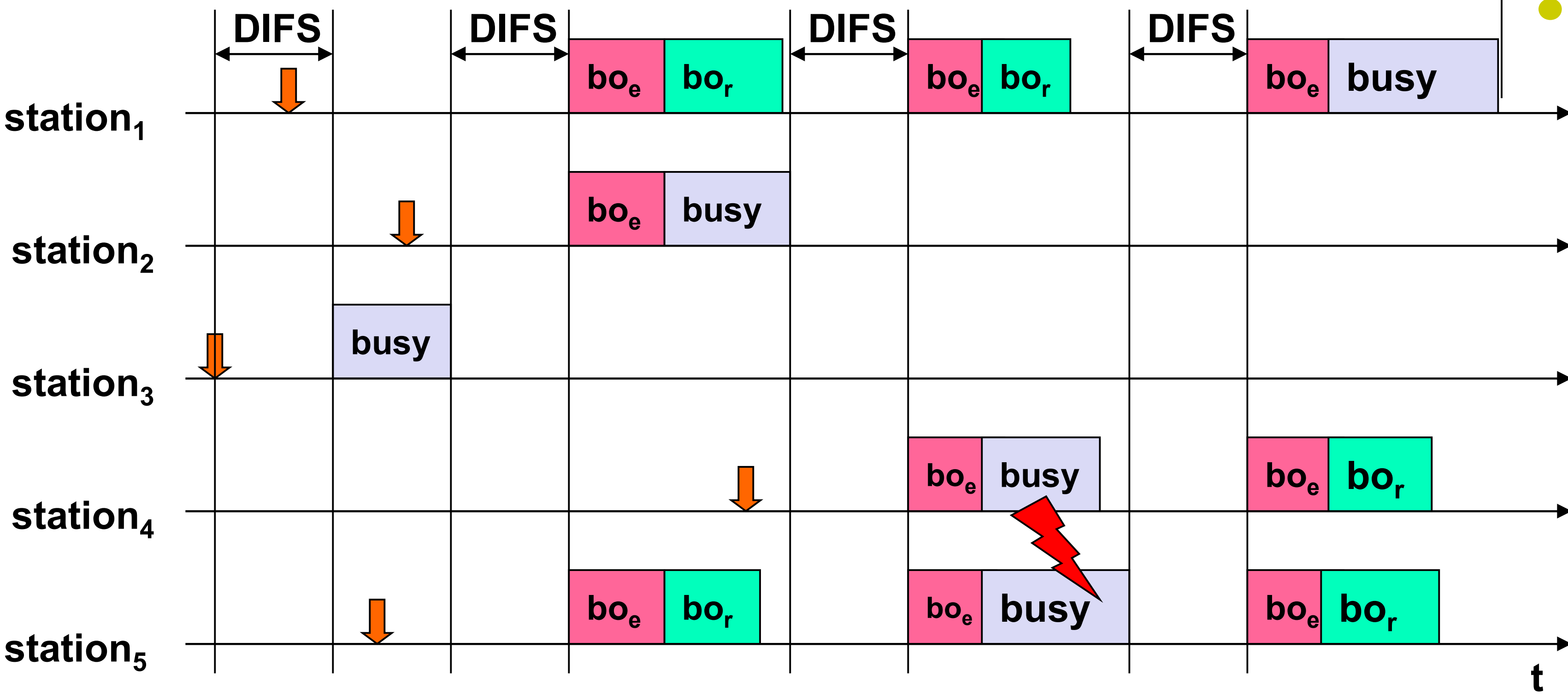
- If receive well a frame then

reply by an ACK after **SIFS**

DIFS: Distributed Inter Frame Space
SIFS: Short Inter Frame Space

Why need ACK?

Example of CSMA/CA on 802.11



busy	Using channel	bo$_e$	backoff time (elapsed)
⇩	Request to send data	bo$_r$	backoff time (residual)

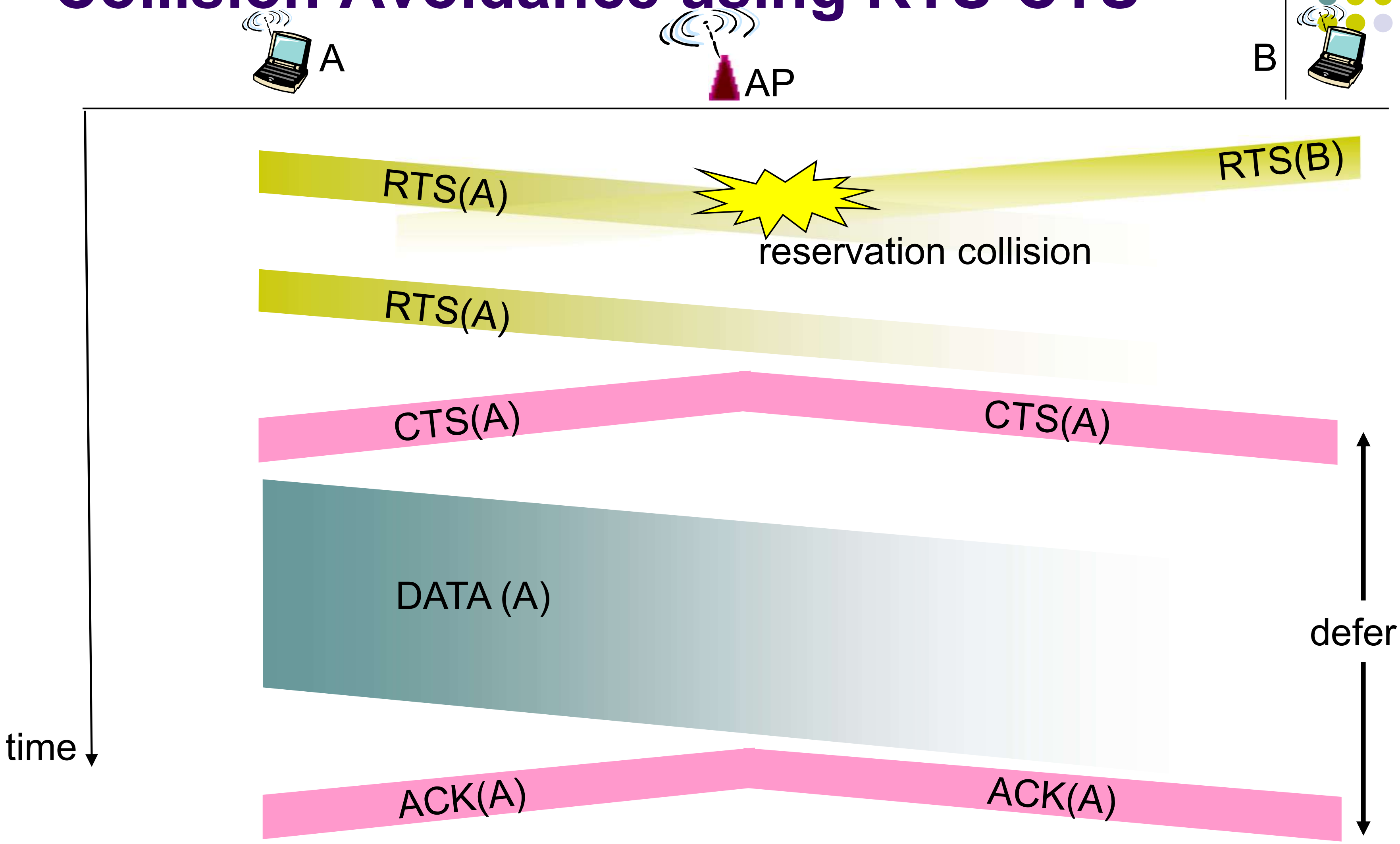
Avoid Collision mechanism

Idea: Sender can reserve channel without random access→ avoid collision for long frame

- Sender send frame RTS (request-to-send) to BS using CSMA
  - RTS may meet a collision (with low probability because the frame is short)
- BS broadcast the frame CTS (clear-to-send CTS) to answer
- All stations receive CTS
  - Sender send data frame
  - All other stations has to cancel the intention to send frames.

Avoid collision thanks to the reservation made by small size control frames

Collision Avoidance using RTS-CTS



802.11 frame: Addressing

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

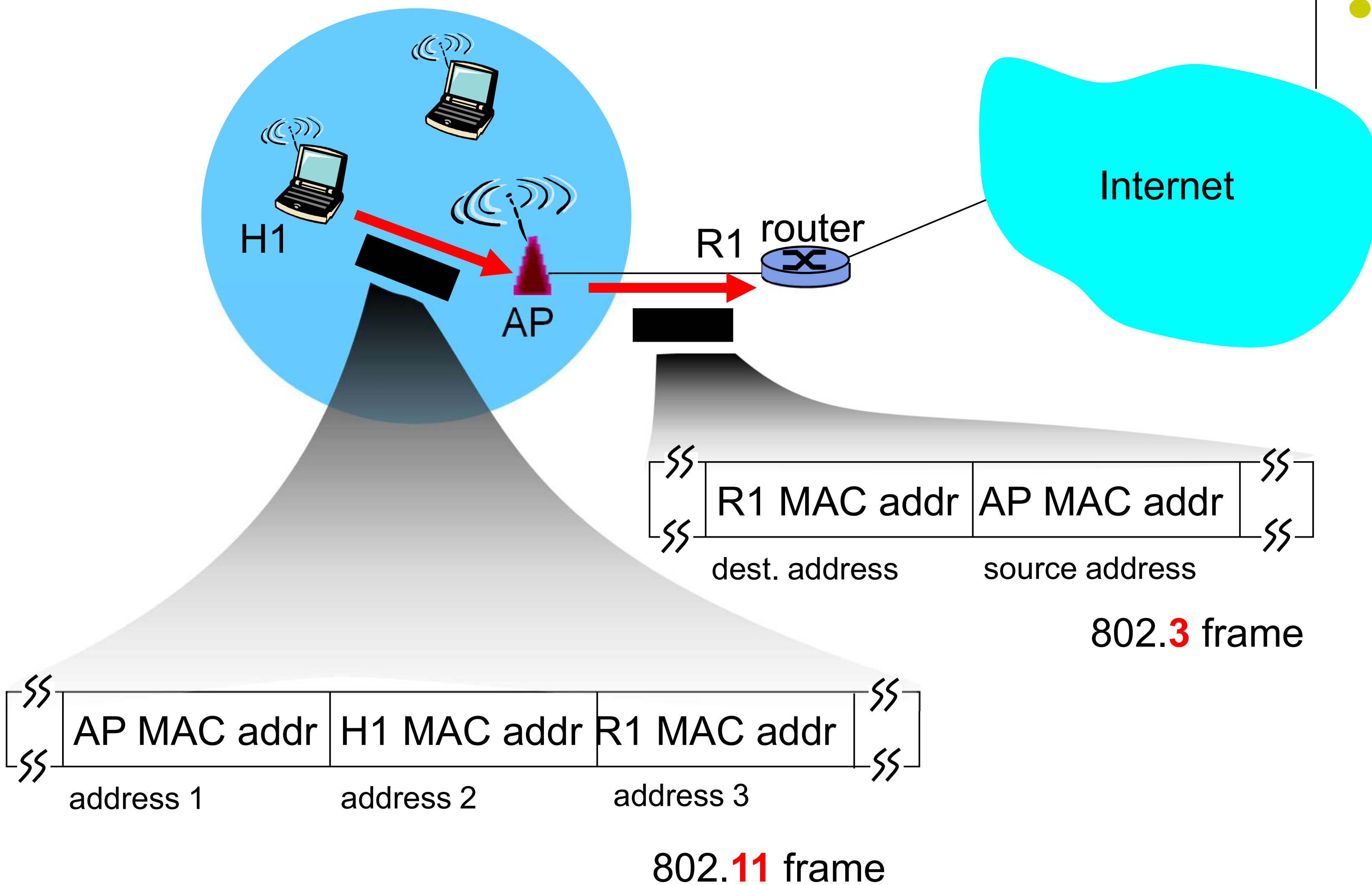
Address 1: address of the destination

Address 2: address of the source

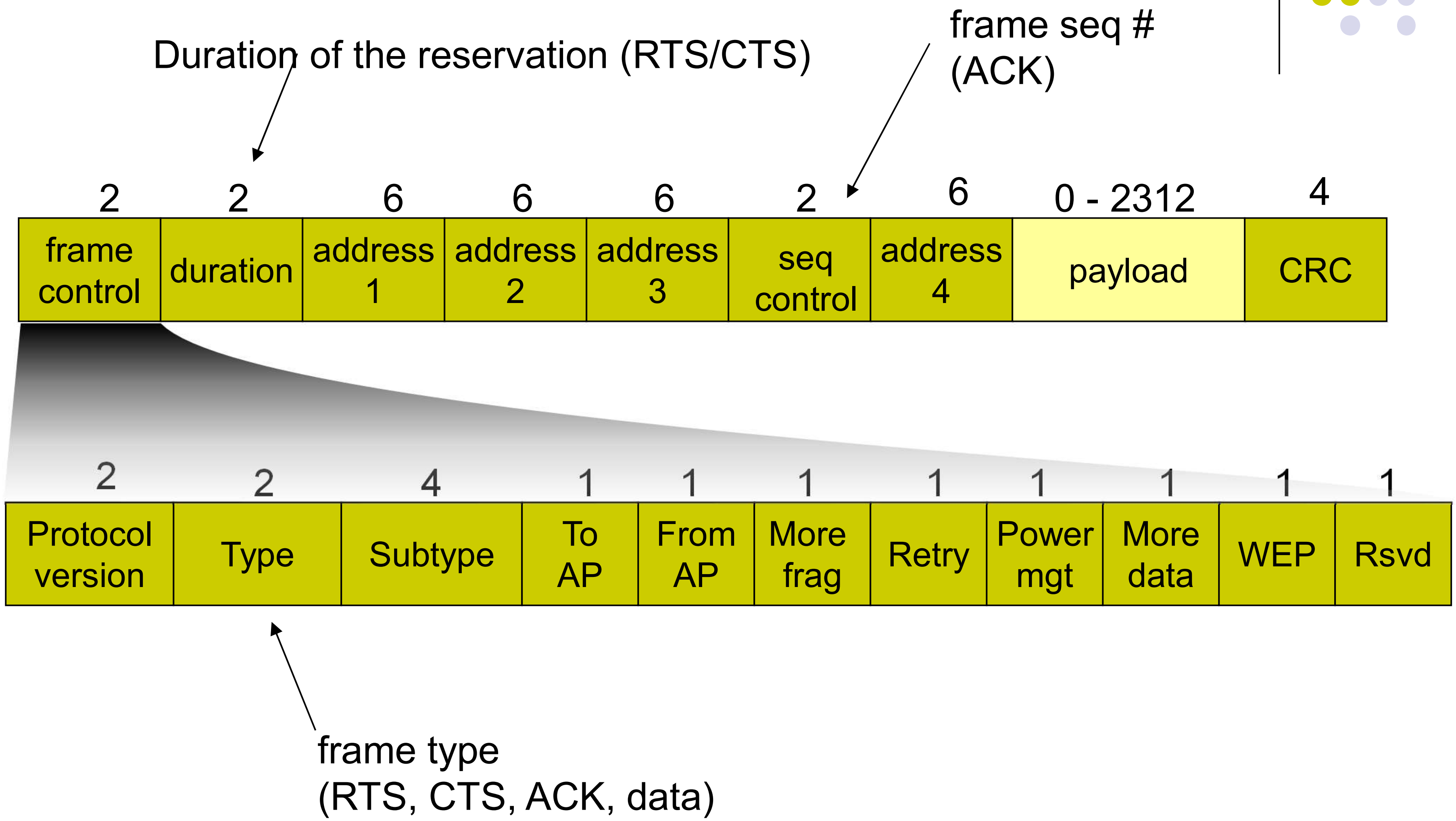
Address 3: MAC address of the router attached to the AP

Address 4: Using in adhoc mode

802.11 frame: Addressing



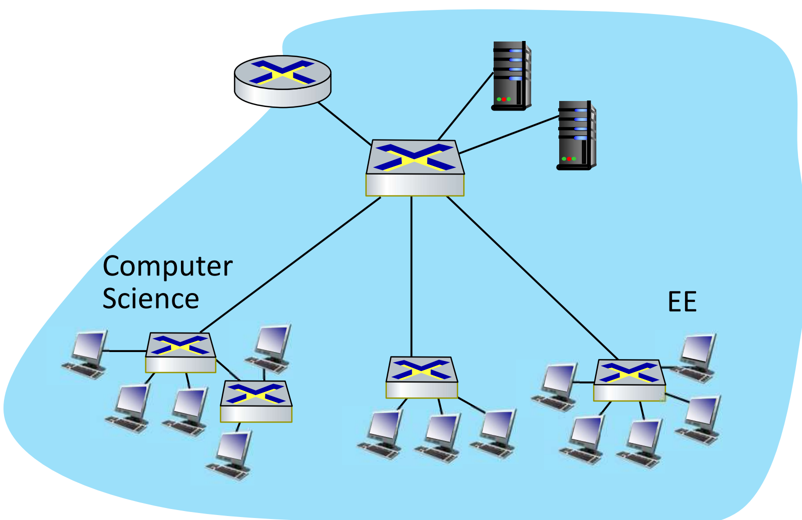
802.11 frame


Duration of the reservation (RTS/CTS)
frame seq #
(ACK)
2 2 6 6 6 2 6 0 - 2312 4
frame control
duration
address 1
address 2
address 3
seq control
address 4
payload
CRC
2 2 4 1 1 1 1 1 1 1 1
Protocol version
Type
Subtype
To AP
From AP
More frag
Retry
Power mgt
More data
WEP
Rsvd
frame type
(RTS, CTS, ACK, data)

Virtual LAN

Virtual LANs (VLANs): motivation

Q: what happens as LAN sizes scale, users change point of attachment?

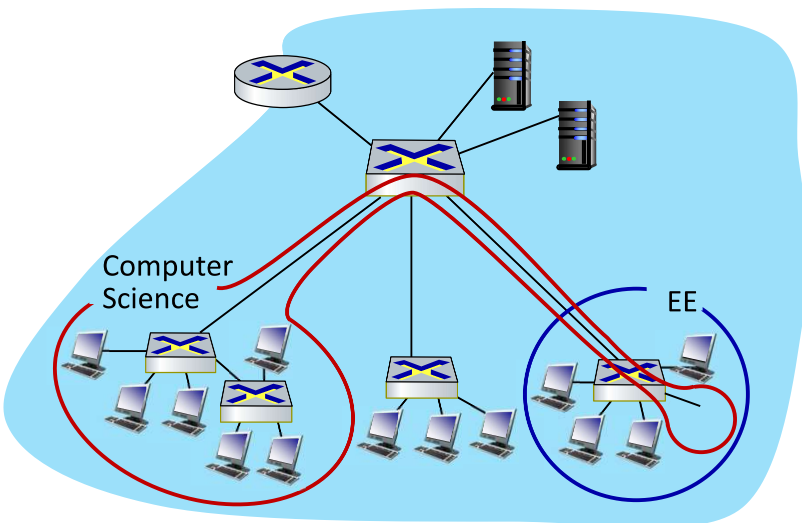


single broadcast domain:

- *scaling:* all layer-2 broadcast traffic (ARP, DHCP, unknown MAC) must cross entire LAN
- efficiency, security, privacy issues

Virtual LANs (VLANs): motivation

Q: what happens as LAN sizes scale, users change point of attachment?



single broadcast domain:

- *scaling:* all layer-2 broadcast traffic (ARP, DHCP, unknown MAC) must cross entire LAN
- efficiency, security, privacy, efficiency issues

administrative issues:

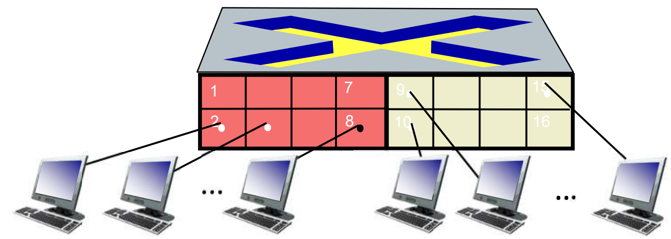
- CS user moves office to EE - *physically* attached to EE switch, but wants to remain *logically* attached to CS switch

Port-based VLANs

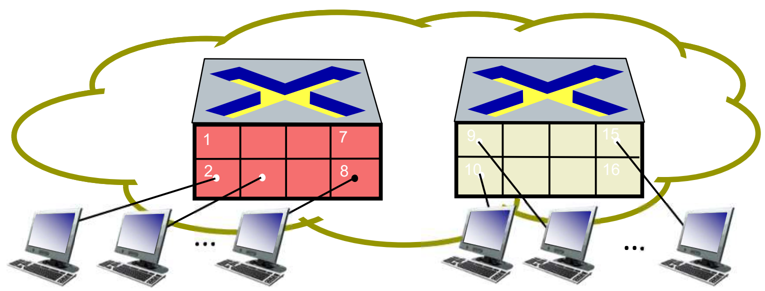
Virtual Local Area Network (VLAN)

switch(es) supporting VLAN capabilities can be configured to define multiple *virtual* LANS over single physical LAN infrastructure.

port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……

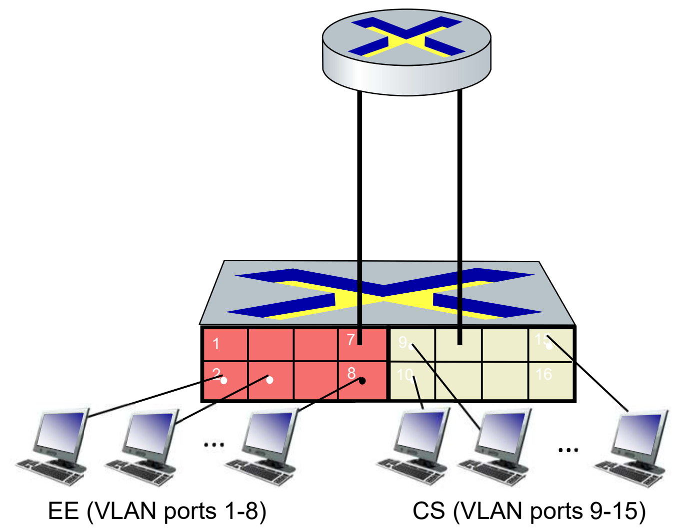


… operates as multiple virtual switches

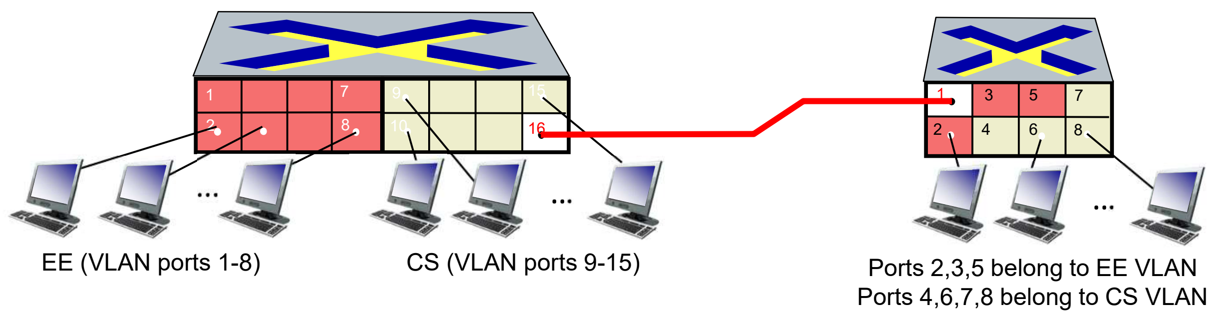


Port-based VLANs

- traffic isolation: frames to/from ports 1-8 can *only* reach ports 1-8
  - can also define VLAN based on MAC addresses of endpoints, rather than switch port
- dynamic membership: ports can be dynamically assigned among VLANs
- forwarding between VLANS: done via routing (just as with separate switches)
  - in practice vendors sell combined switches plus routers



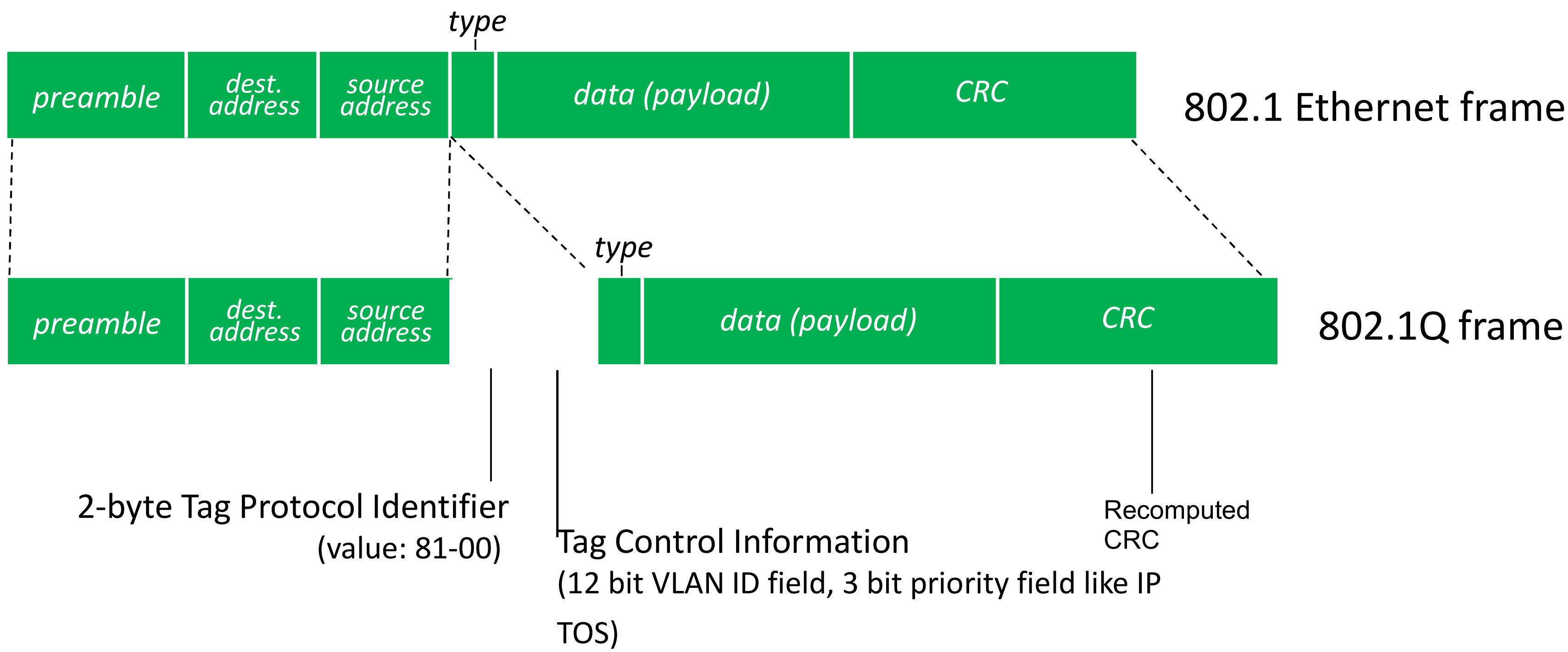
VLANS spanning multiple switches



trunk port: carries frames between VLANS defined over multiple physical switches

- frames forwarded within VLAN between switches can't be vanilla 802.1 frames (must carry VLAN ID info)
- 802.1q protocol adds/removed additional header fields for frames forwarded between trunk ports

802.1Q VLAN frame format



Access network using optical cables

Access network

- A type of telecommunications network which connects subscribers to their immediate service provider
- Popular services for clients/ customers
  - Telephone
  - Television
  - Data transmission. For example: ADSL

Architect of an access network

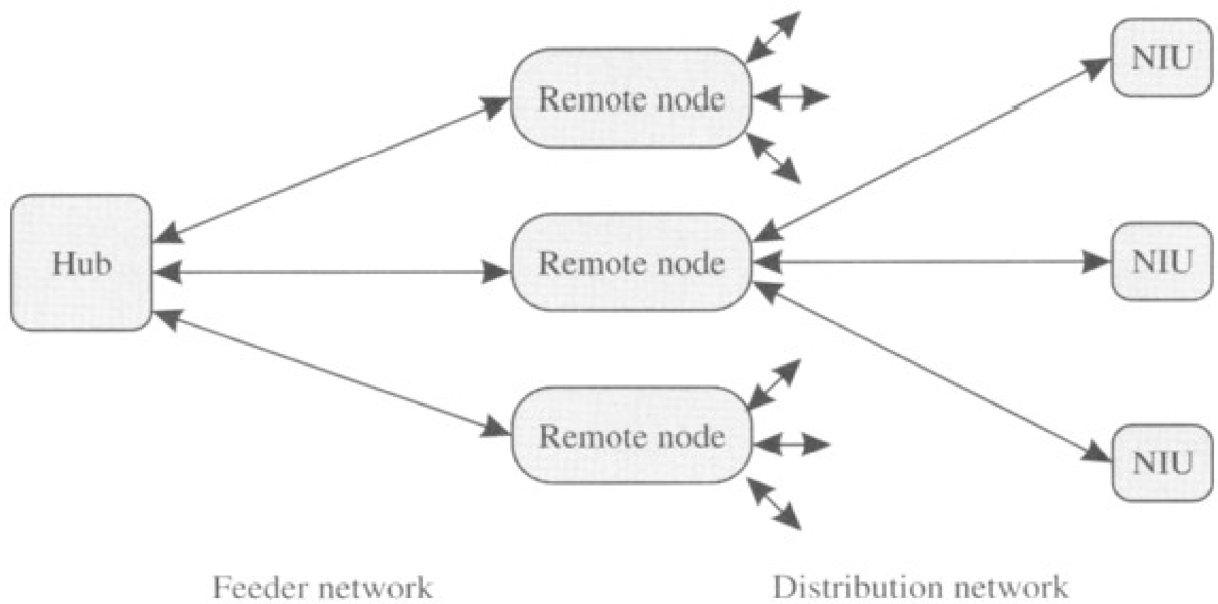


Figure 11.1 Architecture of an access network. It consists of a hub, which is a telephone company central office or cable company head end, remote nodes deployed in the field, and network interface units that serve one or more individual subscribers.

Architect of an access network

- Hub
  - Provider side
- NIU: Network Interface Unit
  - Client side
  - Connect with a user or an enterprise
- Remote Node
  - In a broadcast network, RN distribute data from Hub to all NIU
  - In a switched network, RN receives data from Hub and distributes different data flows to different NIU

Optical access network: FTTx

- Using optical cables to transfer data within a distribution network to ONU (Optical Network Unit)
  - Goal: optical cables to the closest subscribers
- **FTTCab** (*Fiber To The Cabinet*): cables end at a cabinet, last connection to subscribers using coaxial cables (under 1km)
- **FTTC** (*Fiber To The Curb*) / **FTTB**(*Fiber To The Building*); ONU serves 8-64 subcribers, use coaxial cables from ONU to NIU (under 100m)
- **FTTH** (*Fiber To The Home*); ONUs implement thee functionalies of NIUs;
  - ONU can be optical modem

Optical access network : FTTx

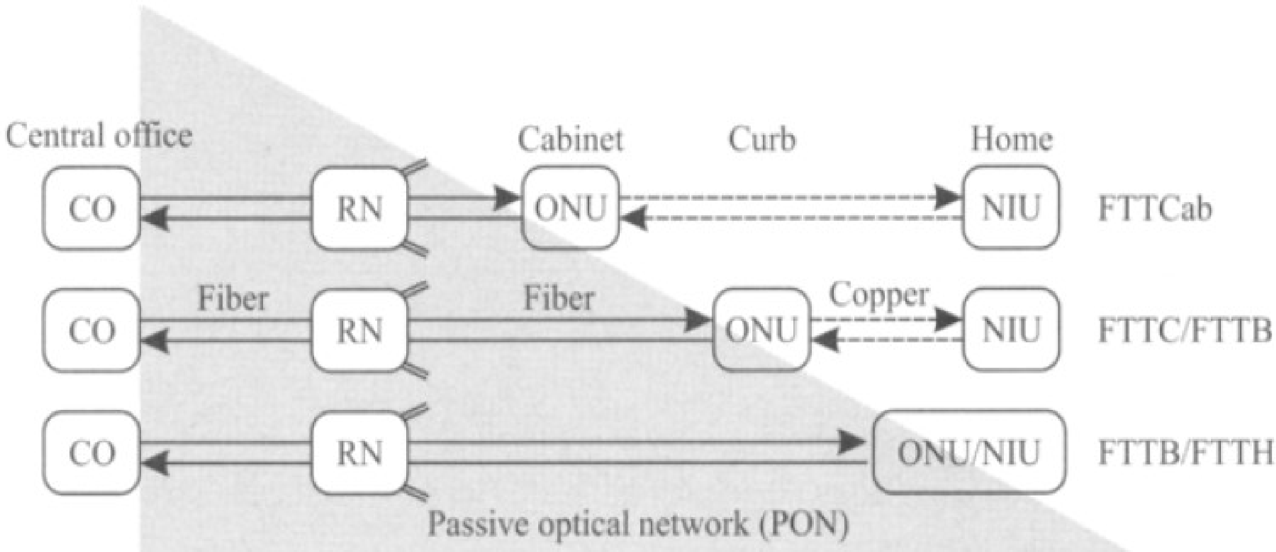
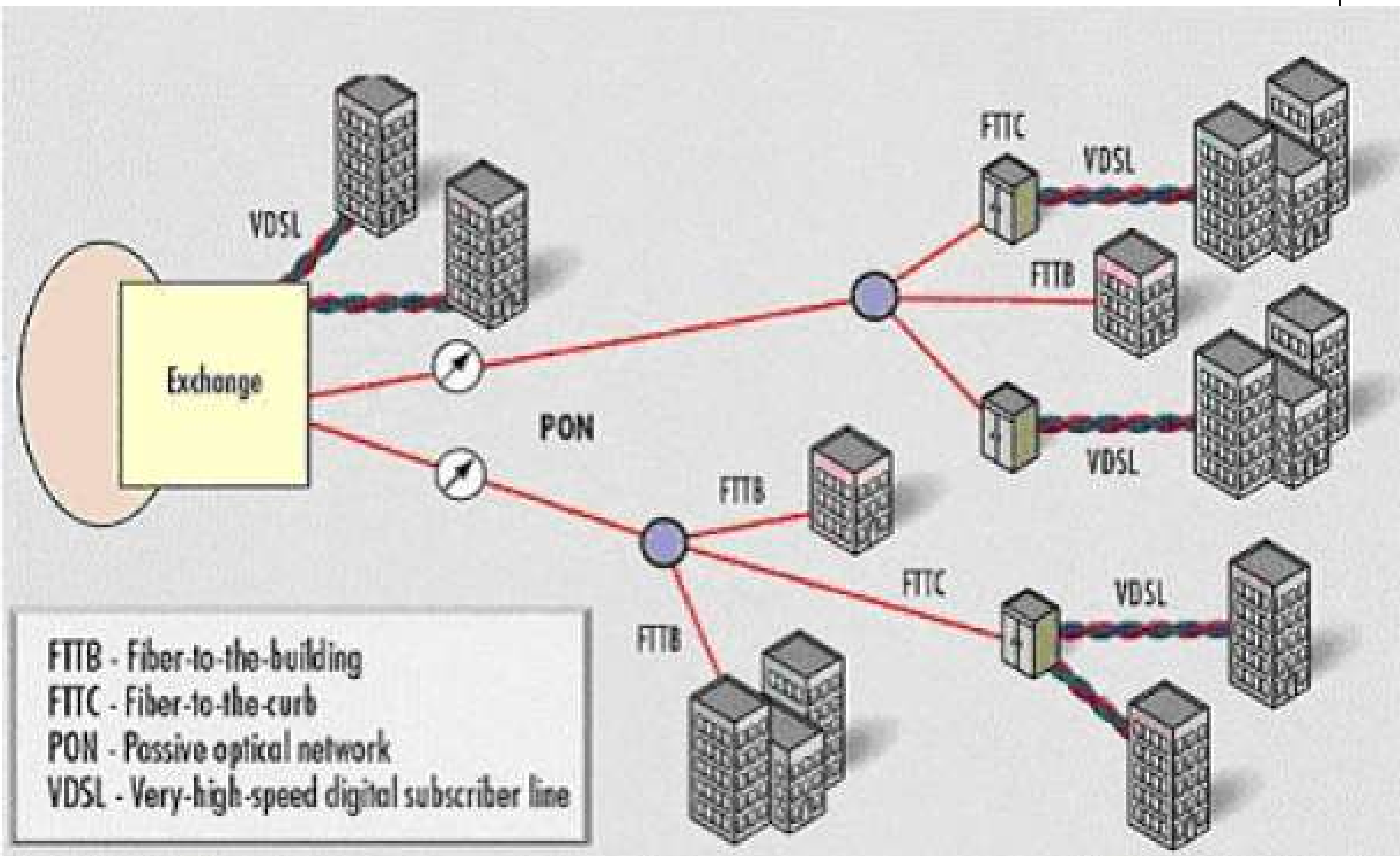


Figure 11.5 Different types of fiber access networks, based on how close the fiber gets to the end user. In many cases, the remote node may be located at the central office itself. The ONUs terminate the fiber signal, and the links between the ONUs and the NIUs are copper based.

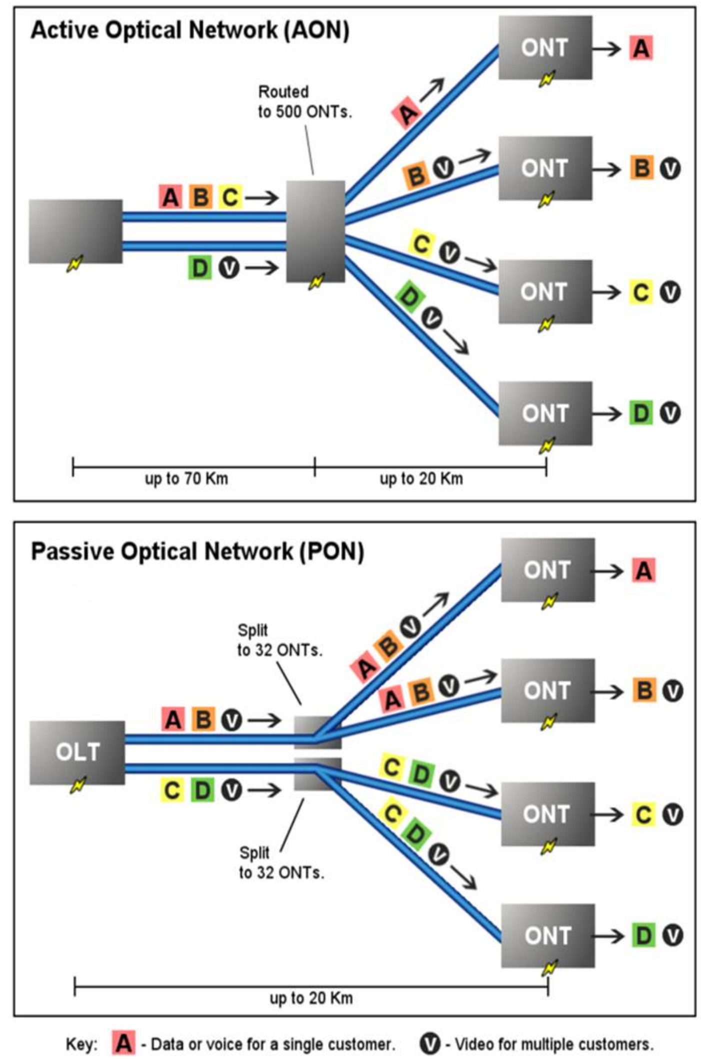
- PON: Passive Optical Network: between CO and ONU
- ONU: can be optical modem.

Optical access network FTTx



AON vs. PON

- Remote Note (Distribution nodes) share data to destinations
- AON: Active Optical Network
    - Network use active technology (RN consumes electricity)
    - Remote Node analyses and route packets to destinations
    - Cable length could be up to 100km
- PON: Passive Optical Network
    - Passive Network (No external energy source is need for RN)
    - RN (Splitter) only repeat signals to all ports
    - Upstream: MUX from different sources by TDM (TDM PON) or WDM (WDM PON)
    - Limit cable length (20km)



EPON: Ethernet PON

- EPON: PON transports Ethernet frame
- Chiều xuống (down stream)
  - Broadcast common data

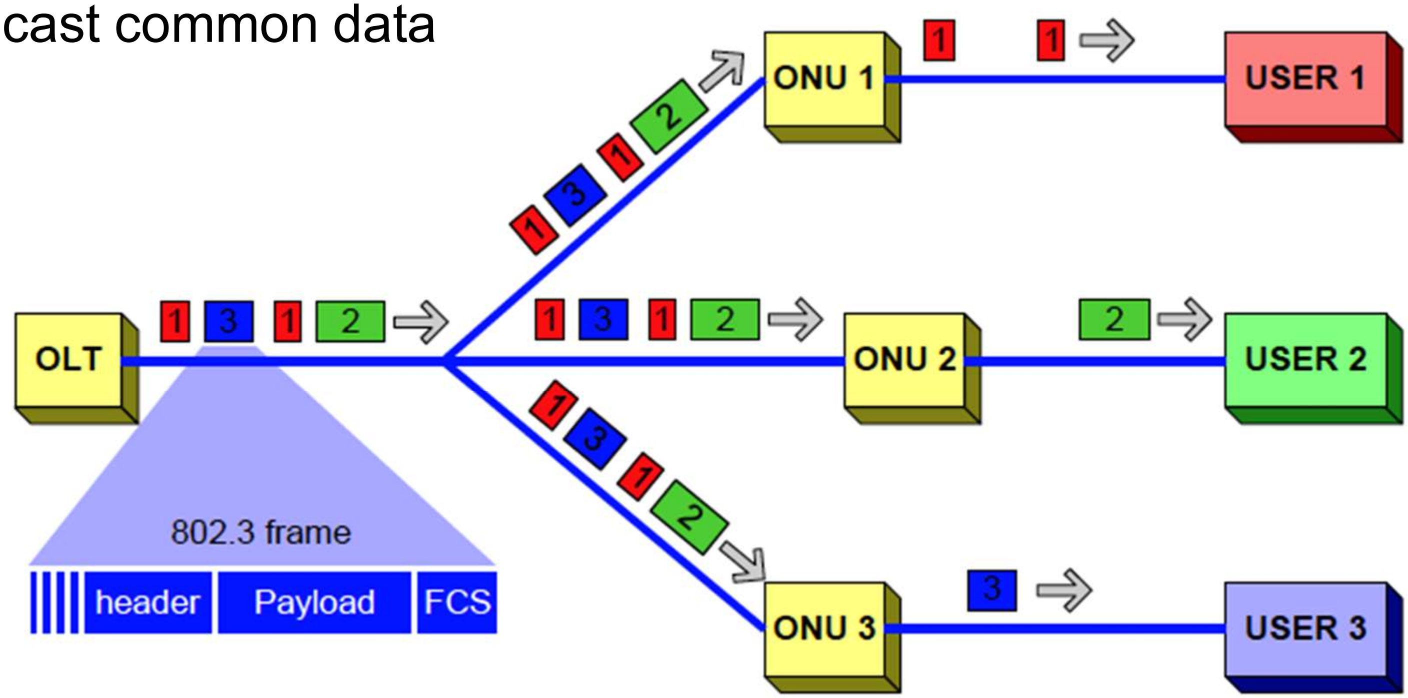


Figure 8-6. Downstream traffic in EPON.

EPON

- Chiều lên (Upstream): multiplexing by TDM of user Ethernet frames from different sources to shared OLT-RN connection
- EPON is a type of TDM PON

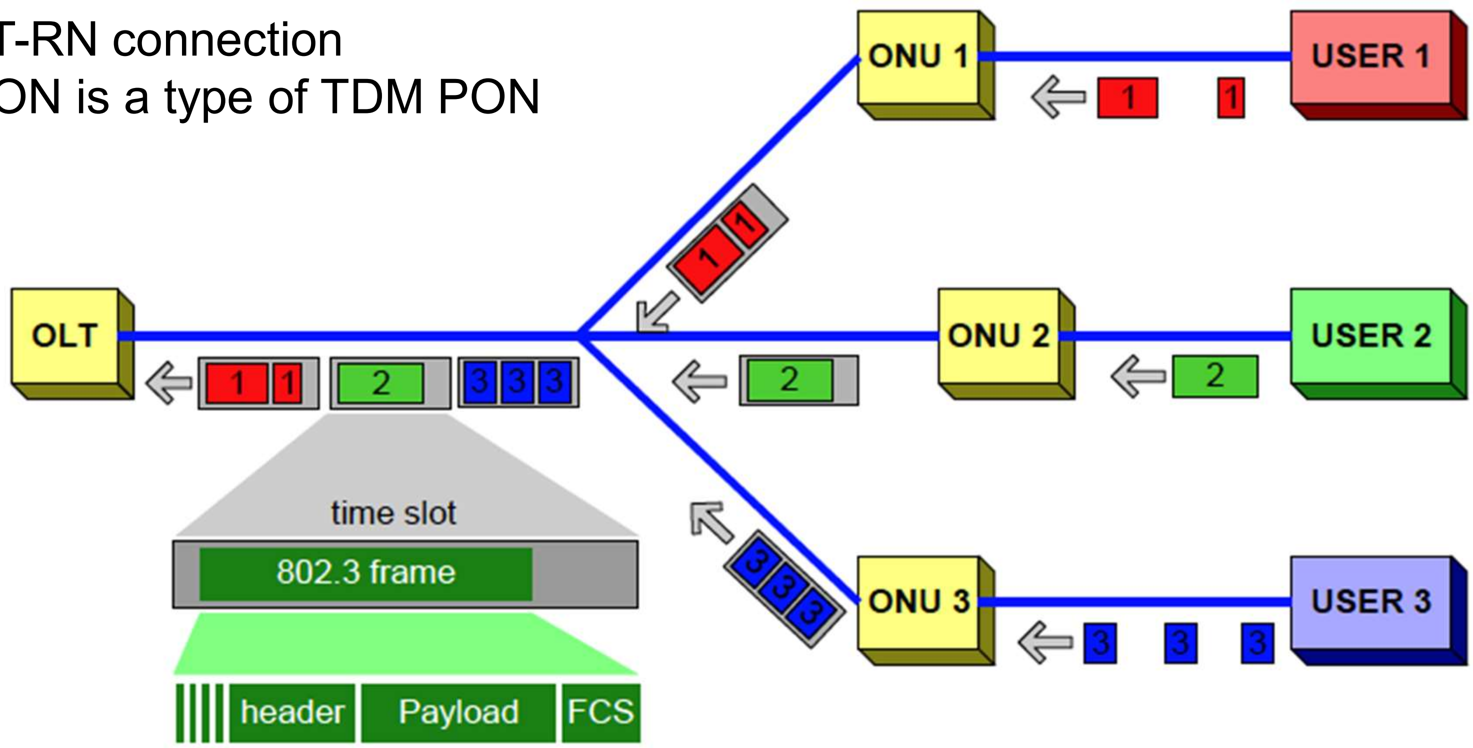


Figure 8-7. Upstream traffic in EPON.

GPON: Gigabit Capable PON

- GPON can be used to transport different types: Ethernet, ATM, voice …
- Data from OLT to subscribers use a shared channel between OLT and RN
  - Downstream broadcast
  - Upstream TDM
  - Data encapsulted in GPON frames have fields of receiver ID (for downstream), and sender ID (for upstream)

WPON (WDM PON)

- Developing by countries, not standardized yet
- Each ONT use a wavelength to transfer data
- Remote node is AWG device having capability of mux-demux different wavelengths
- Wavelength routing PON