Computer Networks

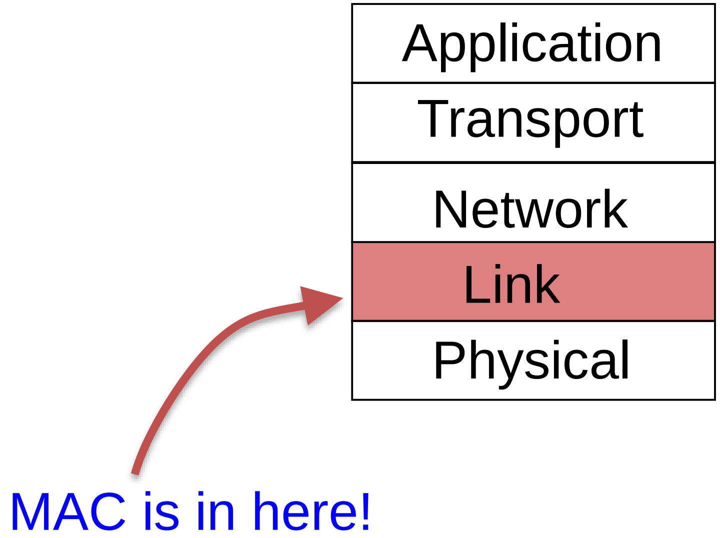
L5 – Medium Access Control Sublayer II

Lecturer: CUI Lin

Department of Computer Science
Jinan University

The MAC Sublayer

- Responsible for deciding who sends next on a multi-access link
  - An important part of the link layer, especially for LANs



Topics for MAC

- Channel Allocation Problem
- Multiple Access Protocols
- Ethernet
- Wireless LANs
- Data Link Layer Switching

Wireless LANs (WLAN)


Free 免費
WiFi


此巴士設有
免費Wi-Fi上網服務
Free Internet Access on Wi-Fi Bus


PCCW
Wi-Fi
在此啟動
Available here

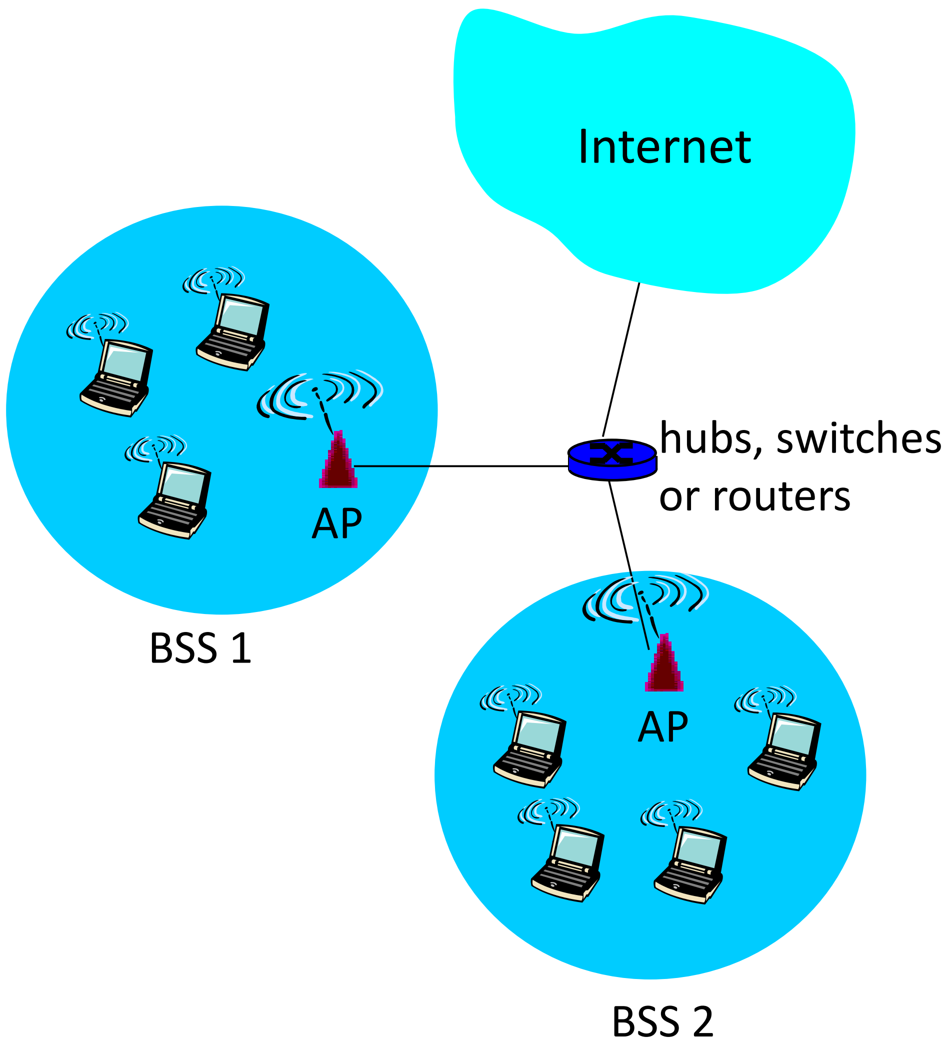
WiFi vs. IEEE 802.11

IEEE 802.11

Two Modes of Wireless LANs

- Infrastructure Mode
  - Wireless hosts communicate to an access point (AP), which typically connects to wired networks
  - Access point is responsible for sending packets between wired networks and wireless hosts in its area
- Ad Hoc Mode
  - Wireless hosts communicate in a peer-to-peer basis without any access point

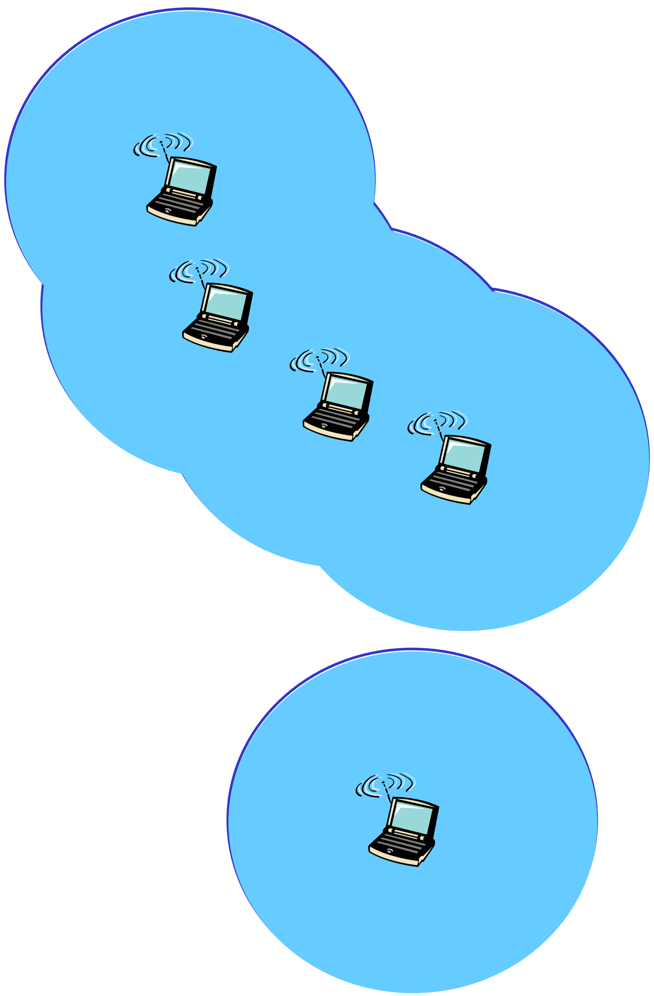
Infrastructure Mode



Infrastructure Mode

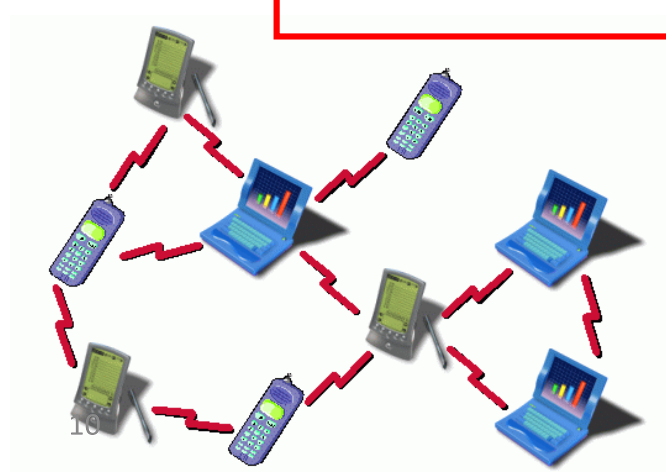
- base station connects mobiles into wired network
- Base station = access point (AP)

Ad Hoc Mode



Ad Hoc Mode

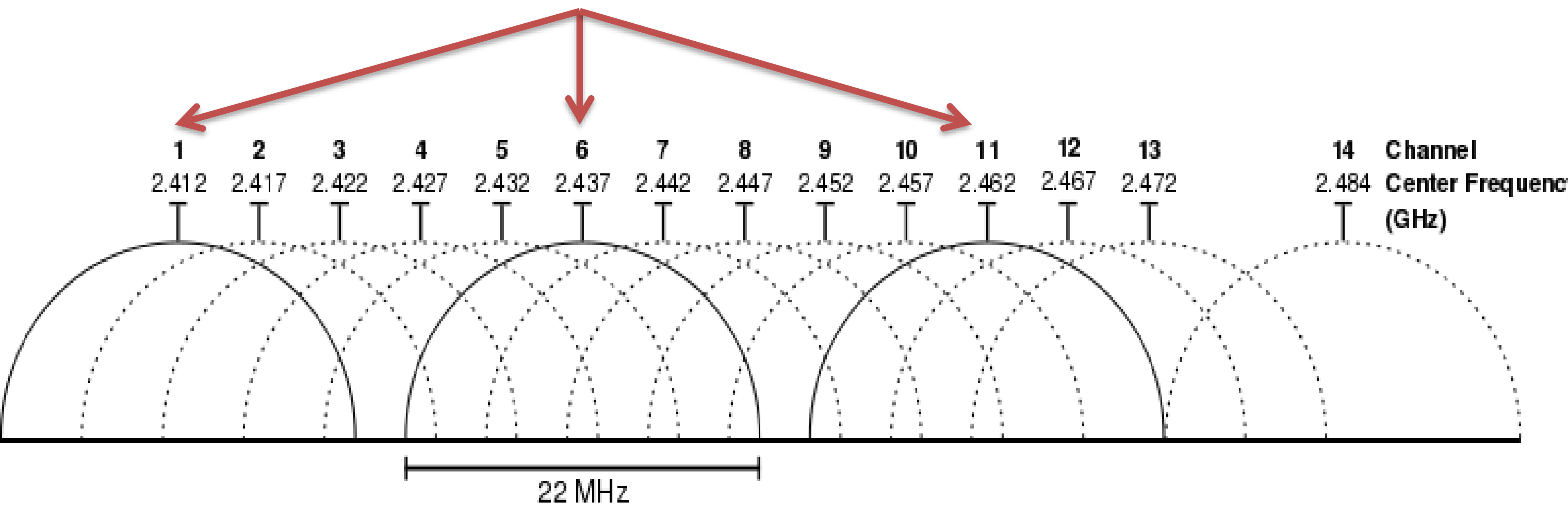
- No base stations
- nodes can only transmit to other nodes within coverage
- nodes organize themselves into a network: route among themselves



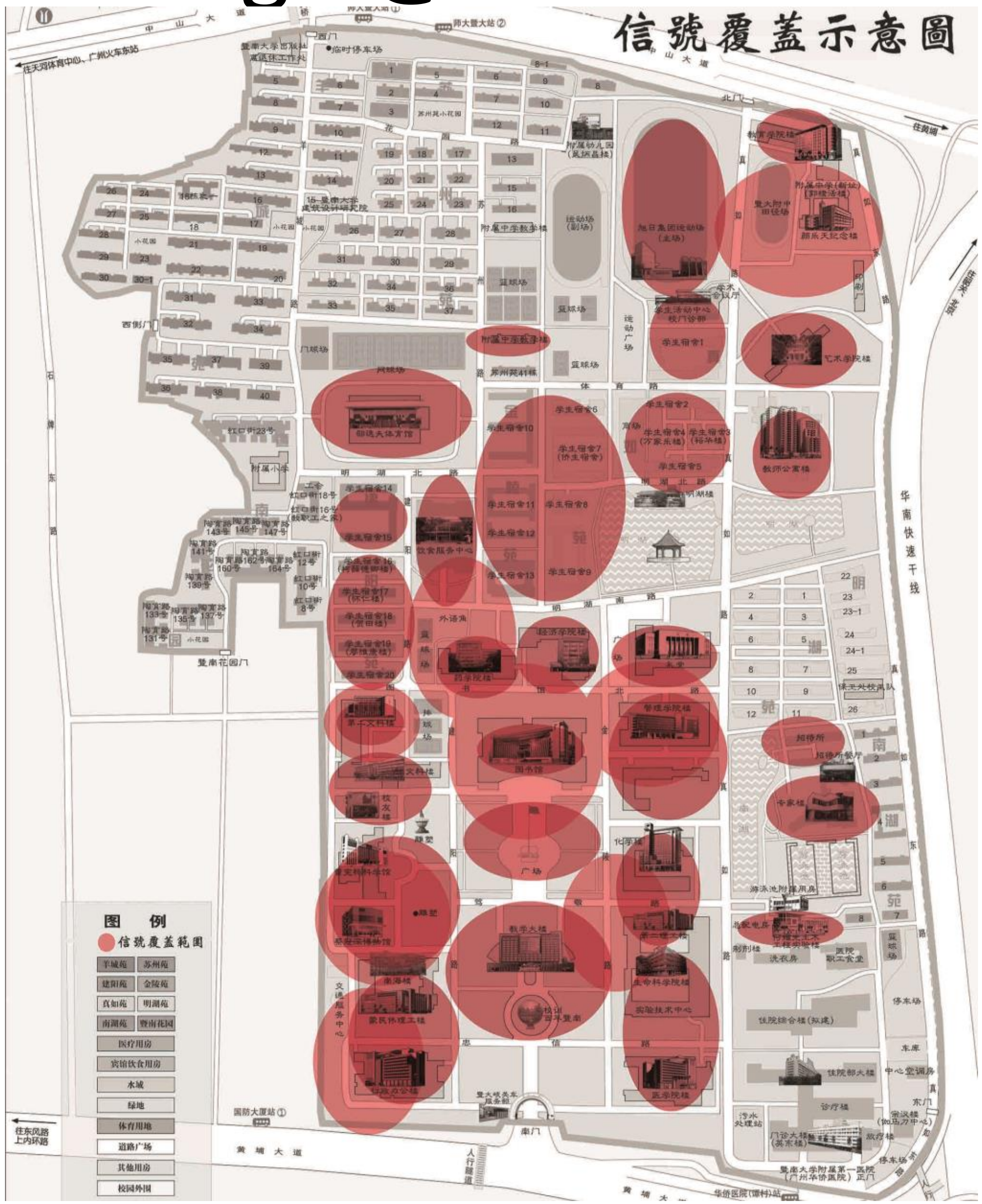
Channels and Association

- Assign a Service Set Identifier (SSID, 1~32 bytes string) to each AP
- Also assign a channel number to the AP
  - 802.11 defines 11~14 partially overlapping channels (2.4GHz band)
    - Any two channels are non-overlapping channel if and only if they are separated by four or more channels
- WiFi jungle
  - Any physical location where a station can receives a strong signal from two or more APs
- A station needs associate with exactly one of the APs

Graphical representation of WiFi channels in 2.4 GHz band



WiFi Coverage @ JNU Main Campus



The 802.11 Physical Layer

- NICs are compatible with multiple physical layers
  - 802.11 a/b/g

Ref wiki for more details

- The adjustment called rate adaptation depending on if the signal to be weak or clear

Wi-Fi Alliance

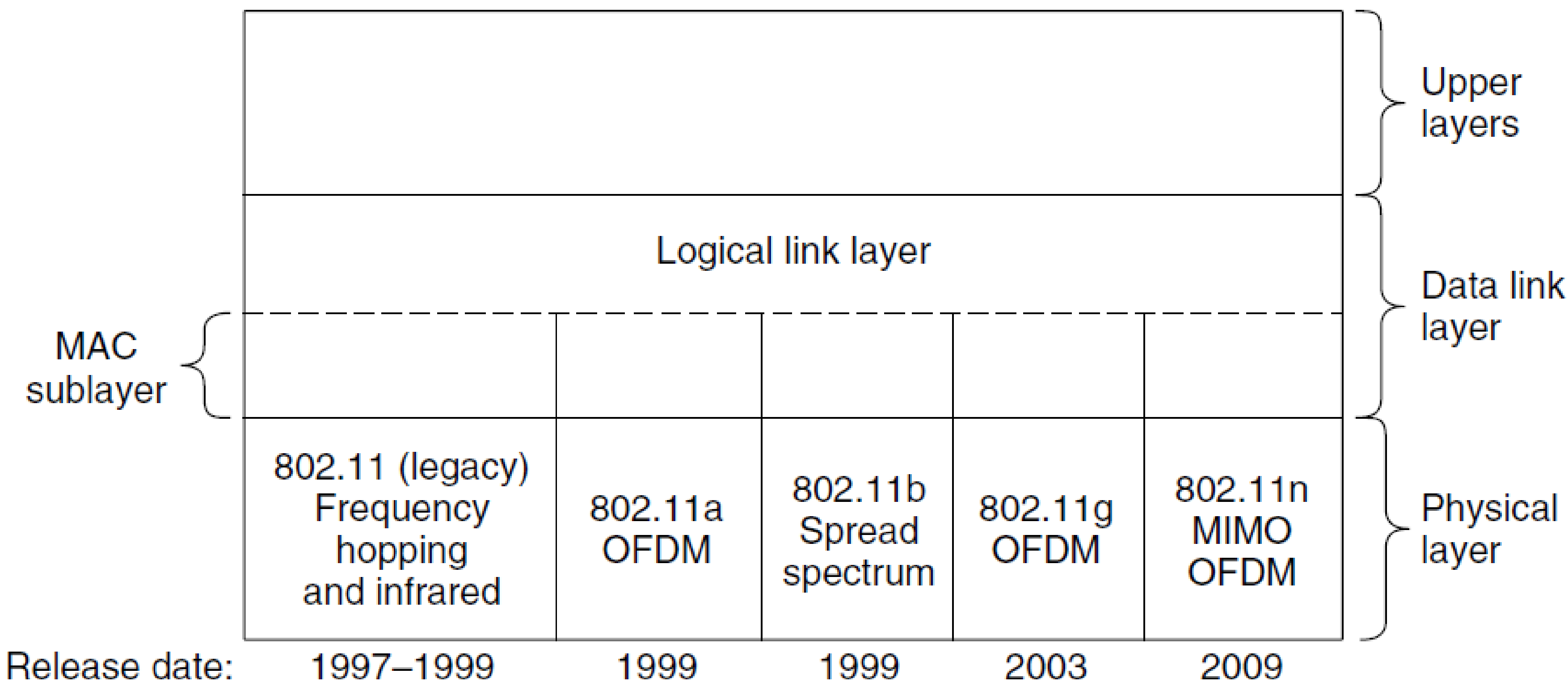
Name	Year	WiFi version	Technique	Max. Bit Rate	Indoor Range	Outdoor range
802.11b	1999	Wi-Fi 1	DSSS, 2.4 GHz	11 Mbps	~38m	~140m
802.11a	1999	Wi-Fi 2	OFDM, 5 GHz	54 Mbps	~35m	~120m
802.11g	2003	Wi-Fi 3	OFDM, 2.4 GHz	54 Mbps	~38m	~140m
802.11n	2009	Wi-Fi 4	OFDM with MIMO, 2.4/5GHz	600 Mbps	~70m	~250m
802.11ac	2013	Wi-Fi 5	MIMO on 5GHz	>1.3Gbps	~35m	~120m?
802.11ax	2019/09/16	Wi-Fi 6	OFDM, MU-MIMO, 2.4/5GHz etc.	9.6 Gbps*	N.A.	~250m?

* Depending upon number of spatial streams and channel used

Wi-Fi 7 is on the way…

The 802.11 Architecture and Protocol Stack

- MAC is used across different physical layers

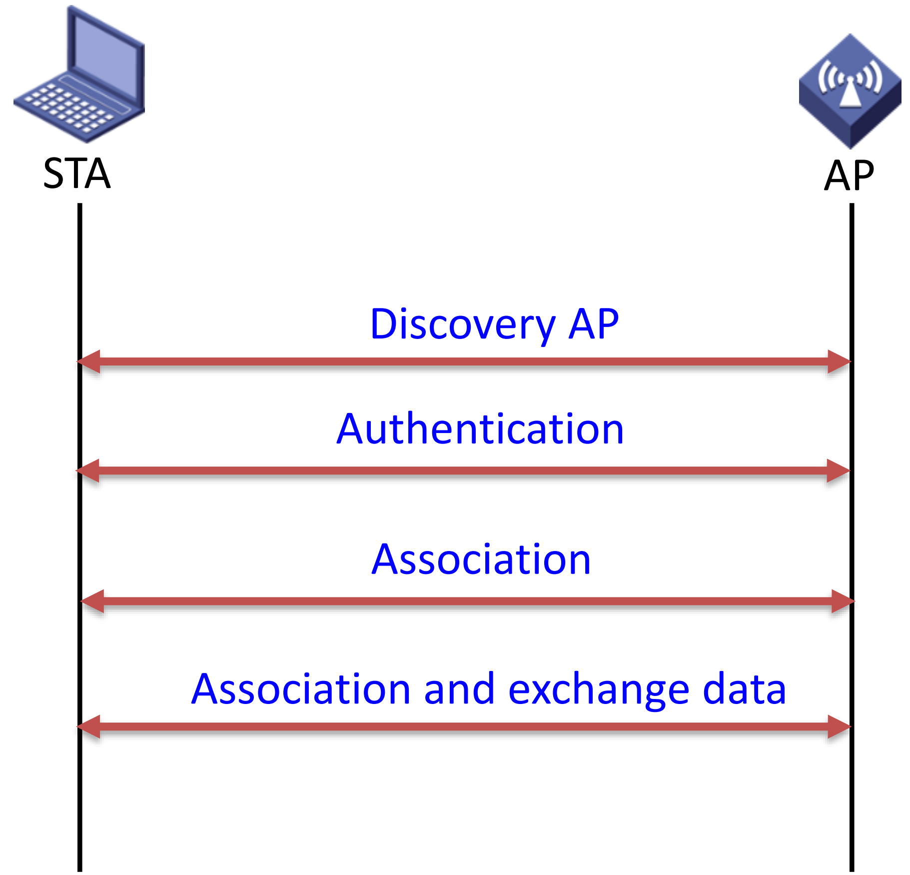


Q: How does your wireless host join a network?

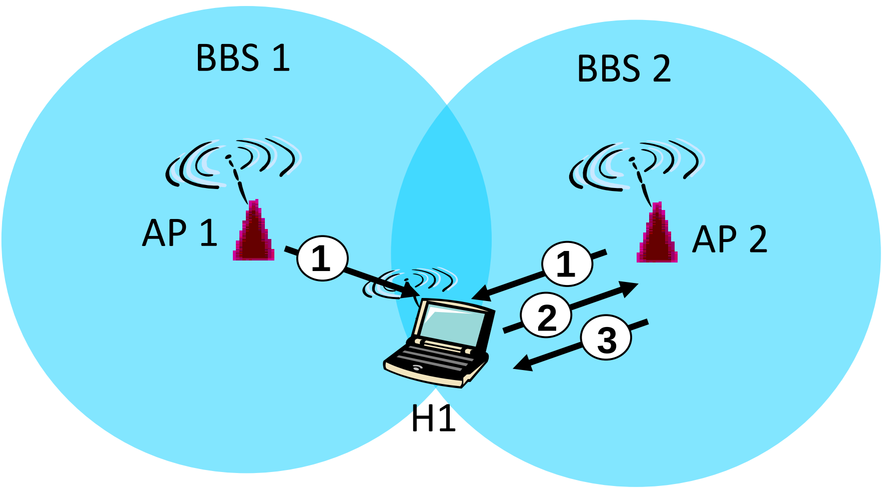
Infrastructure Mode

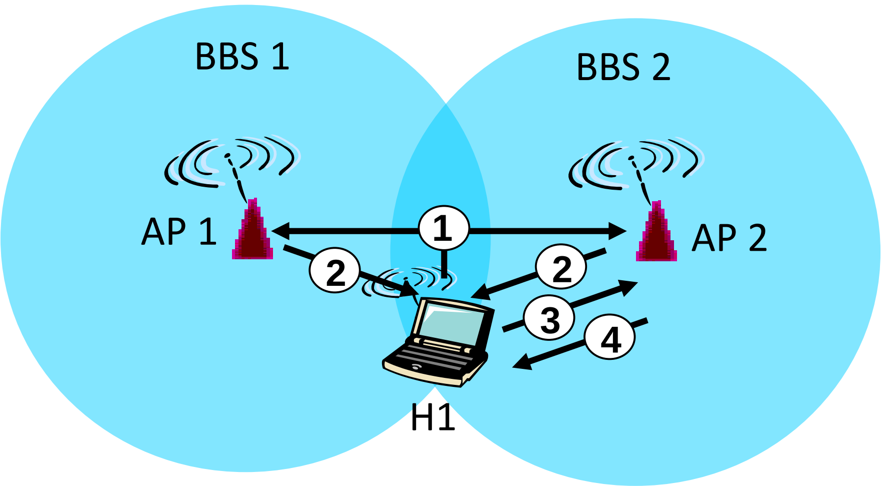
Steps to Join a Network

1. Discover available networks
2. Select a network
3. Authentication
4. Association



1. Discovering Available Networks 802.11: passive/active scanning





Passive Scanning:

(1) Beacon frames periodically sent from APs, which include AP's MAC address, Network name, etc.

(2) Association Request frame sent: H1 to selected AP2

(3) Association Response frame sent: AP2 to selected H1

Active Scanning:

(1) Probe Request frame broadcast from H1

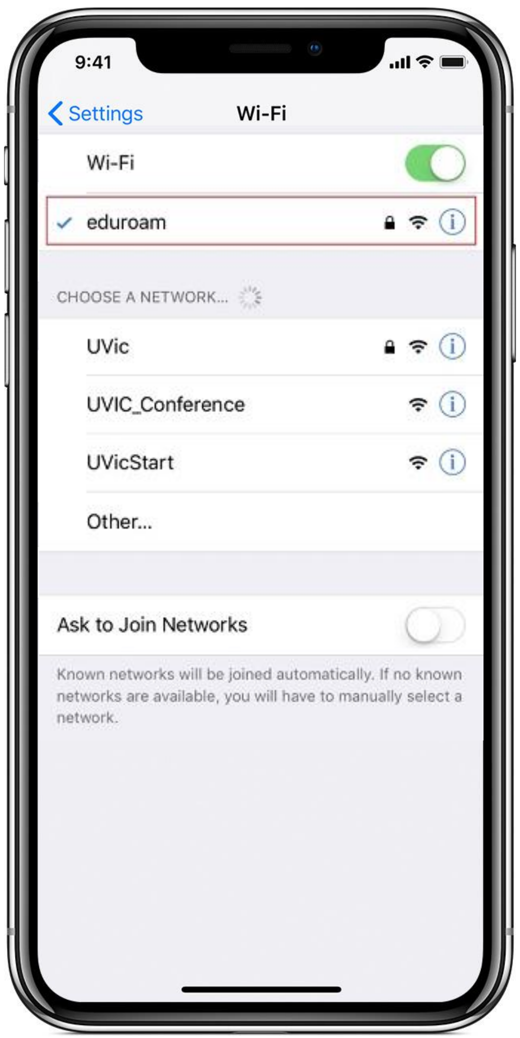
(2) Probes response frame sent from APs, which include AP's MAC address, SSID, etc.

(3) Association Request frame sent: H1 to selected AP2

(4) Association Response frame sent: AP2 to selected H1

2. Choosing a Network

- The user selects from available networks,

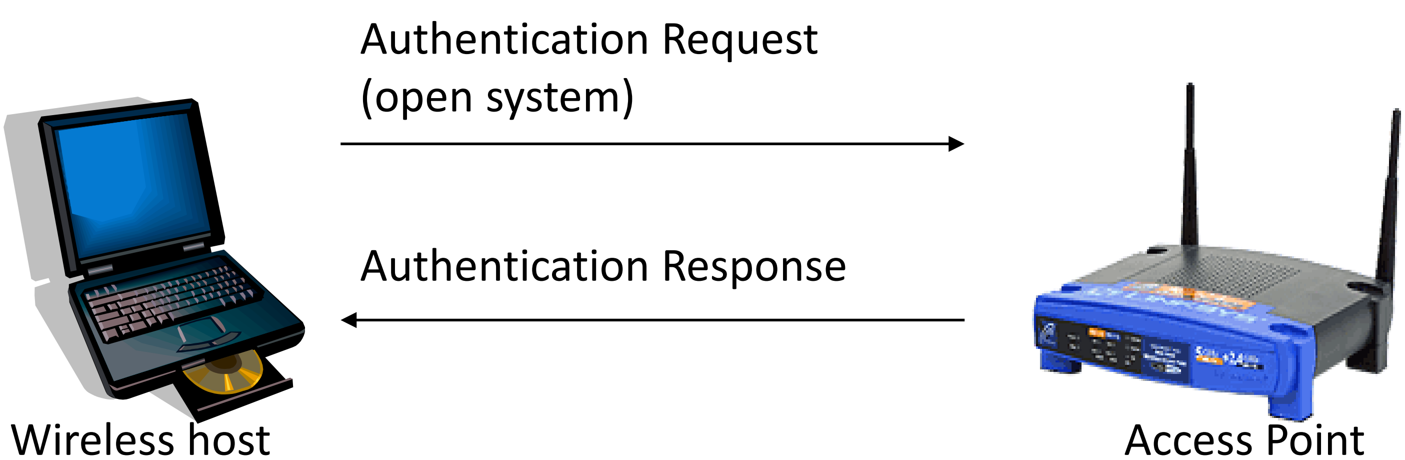


3. Authentication

- Authentication
  - A wireless host proves its identity to the AP.
- Two Mechanisms
  - Open System Authentication
  - Shared Key Authentication

Open System Authentication

- The default authentication protocol for 802.11.
- Authenticates anyone who requests authentication.
  - NULL authentication (i.e. no authentication at all)



Shared Key Authentication

It is assumed that the wireless host and the AP somehow agrees on a shared secret key via a channel independent of IEEE 802.11.

Wireless host

Authentication Request (shared key)

"Challenge" text string, generated randomly

"Challenge" text string, encrypted with shared key

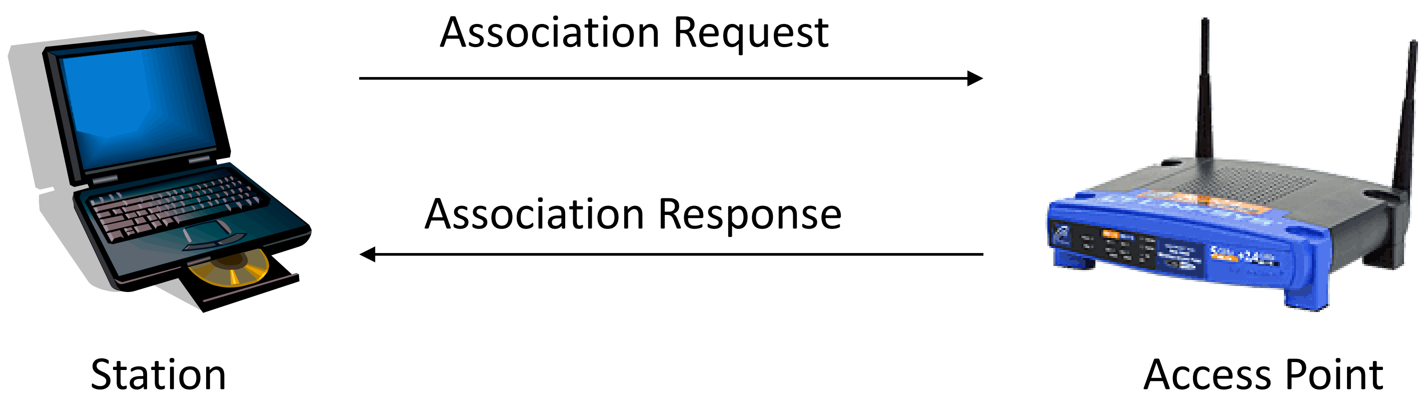
Positive or negative response based on decryption result

Access Point (AP)

Note: "Challenge" is encrypted by algorithm, e.g, WEP/WPA2.

4. Association

The wireless hosts needs to associate (i.e. register) with an AP.



Q: After your mobile phone is connected to the WiFi, how to transmit frames?

The MAC layer

Can CSMA/CD work properly in wireless LANs?

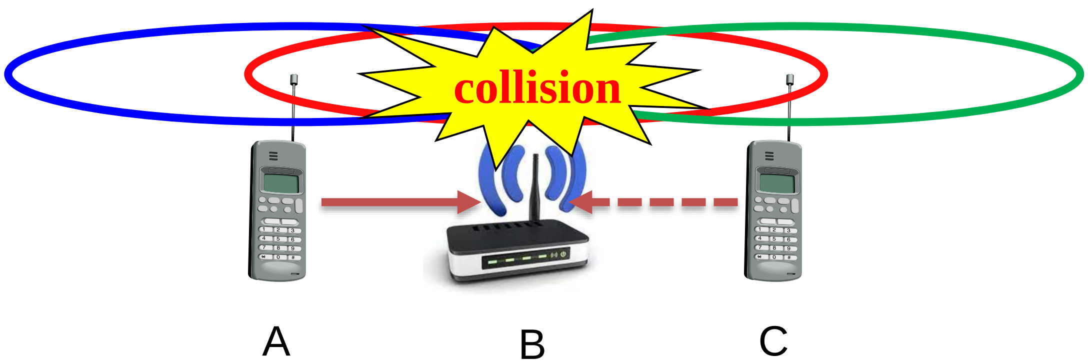
Brief Review CSMA/CD in Ethernet

- Carrier Sense Multiple Access (CSMA): Listen before talk
  - Sense the channel
  - If the channel is idle, transmit immediately
  - If the channel is busy,
    - waits a random amount of time (i.e. random backoff time)
    - sense the channel again
- Collision Detection (CD): Stop if collision occurs
  - If there is a collision,
    - stops transmission immediately,
    - waits a random amount of time
    - senses the channel again

- Can CSMA/CD work properly in IEEE 802.11 wireless LANs?

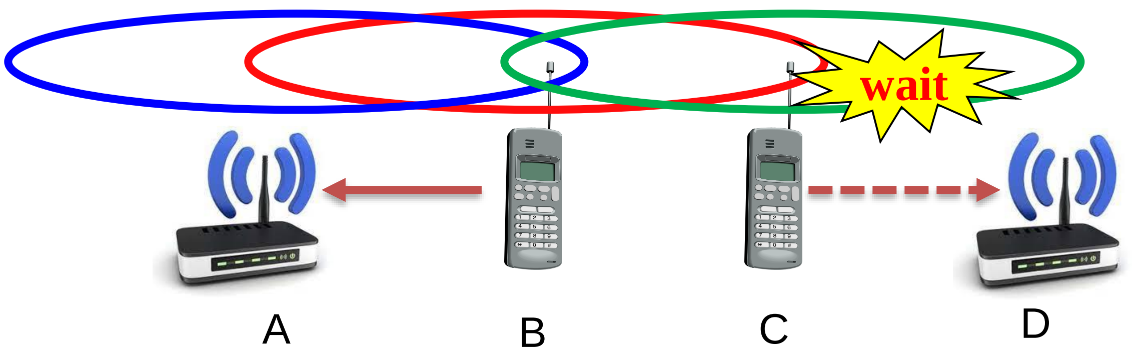
Hidden and Exposed Terminal Problems

- Hidden terminals (隐藏终端)
  - A sends to B, C cannot receive A
  - C wants to send to B, C senses a “free” medium (CS fails)
  - Collision at B, A cannot receive the collision (CD fails)
  - A is “hidden” for C, vice versa



Hidden and Exposed Terminal Problems

- Exposed terminals (暴露终端)
  - B is sending to A, C wants to send to D
  - C has to wait, it senses the channel busy
  - But A is outside the radio range of C, therefore waiting is not necessary
  - C is “exposed” to B



Actually, No CSMA/CD in Wireless LAN

- Wireless LAN: *no* collision detection!
  - Instead of simply detecting collisions, the goal is to *avoid collisions:* CSMA/CA (Collision Avoidance) at the first place.

MACA - Collision Avoidance

- MACA (Multiple Access with Collision Avoidance) uses *short* signaling packets for collision avoidance
  - RTS (request to send) (20 bytes): a sender request the right to send from a receiver with a short RTS packet before it sends a data packet
  - CTS (clear to send) (14 bytes): the receiver grants the right to send as soon as it is ready to receive
- Signaling packets contain
  - sender address
  - receiver address
  - packet size

How to avoid collisions?

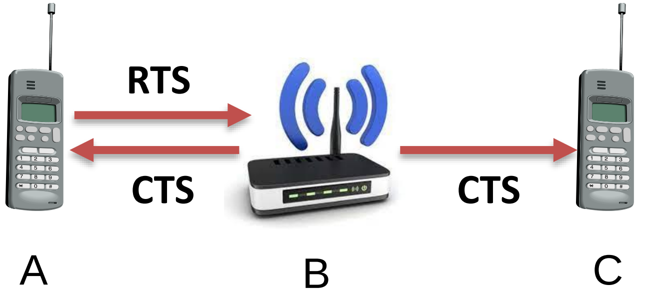
Idea: allow sender to "reserve" channel rather than random access of data frames

- Sender first transmits *small* request-to-send (RTS) frame to receiver using CSMA
  - RTSs may still collide with each other (but they're short)
- Receiver broadcasts clear-to-send (CTS) in response to RTS
- RTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

Avoid data frame collisions completely
using small reservation packets! (RTS/CTS)

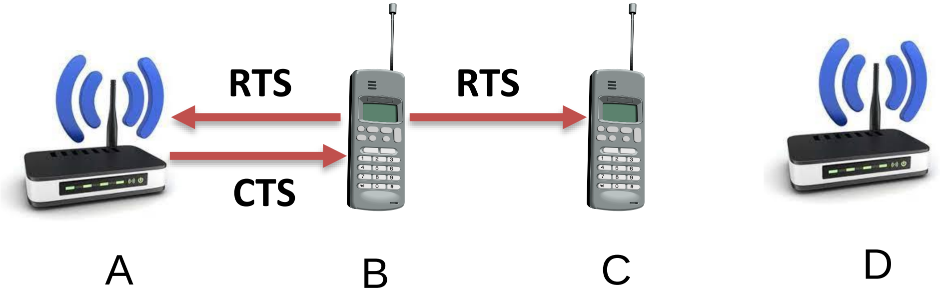
MACA: RTS/CTS Scheme

- RTS/CTS avoids the problem of hidden terminals
  - A and C want to send to B
  - A sends RTS first
  - C waits after receiving CTS from B



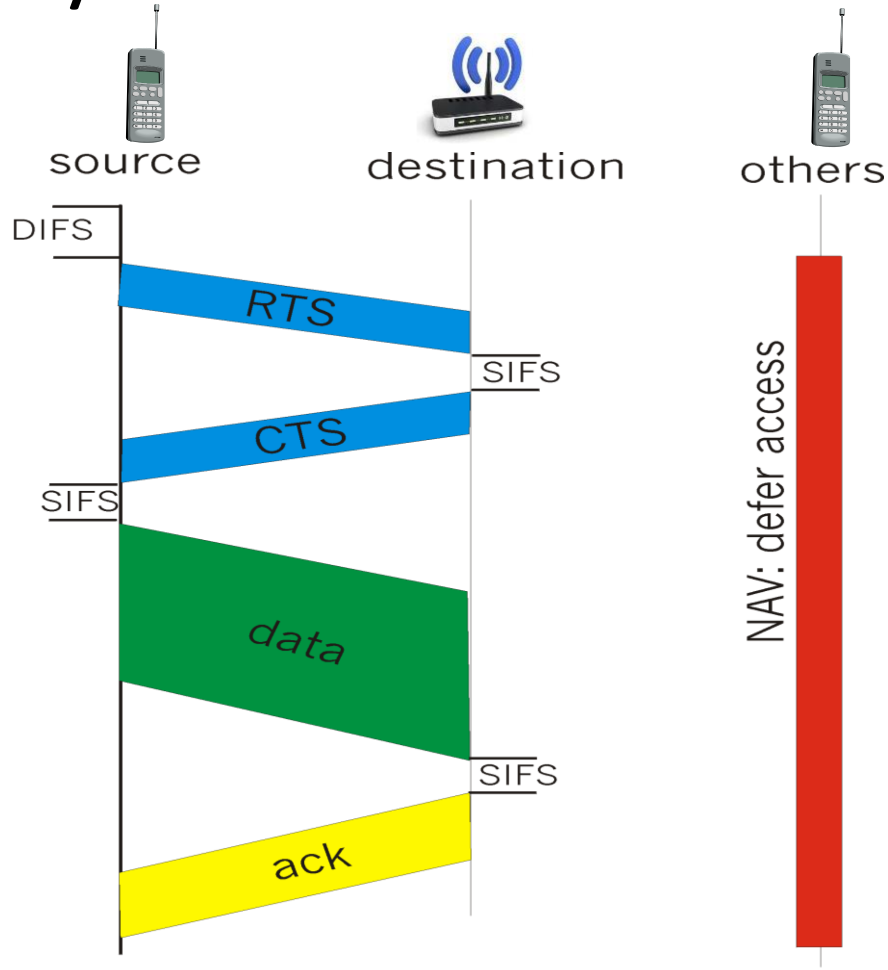
MACA: RTS/CTS Scheme

- RTS/CTS avoids the problem of exposed terminals
  - B wants to send to A, C want to send to D
  - C does not have to wait since it cannot receive CTS from A



IEEE 802.11: CSMA/CA with RTS-CTS

- CSMA/CA: explicit channel reservation
  - sender: send RTS
  - receiver: reply with CTS
- CTS reserves channel for sender, notifying (possibly hidden) terminals

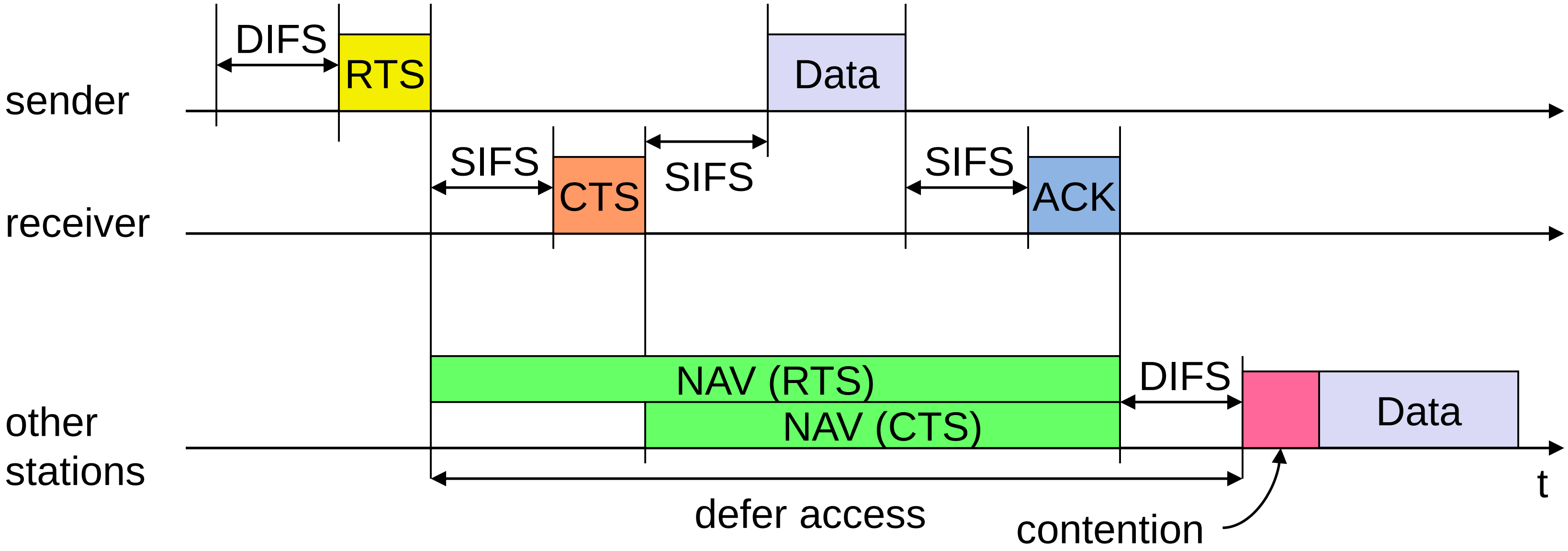


4-way handshake

DIFS – Distributed Inter-frame Space
SIFS – Short Inter-frame Space

DIFS > SIFS

How to determine the waiting time? --- Net Allocation Vector

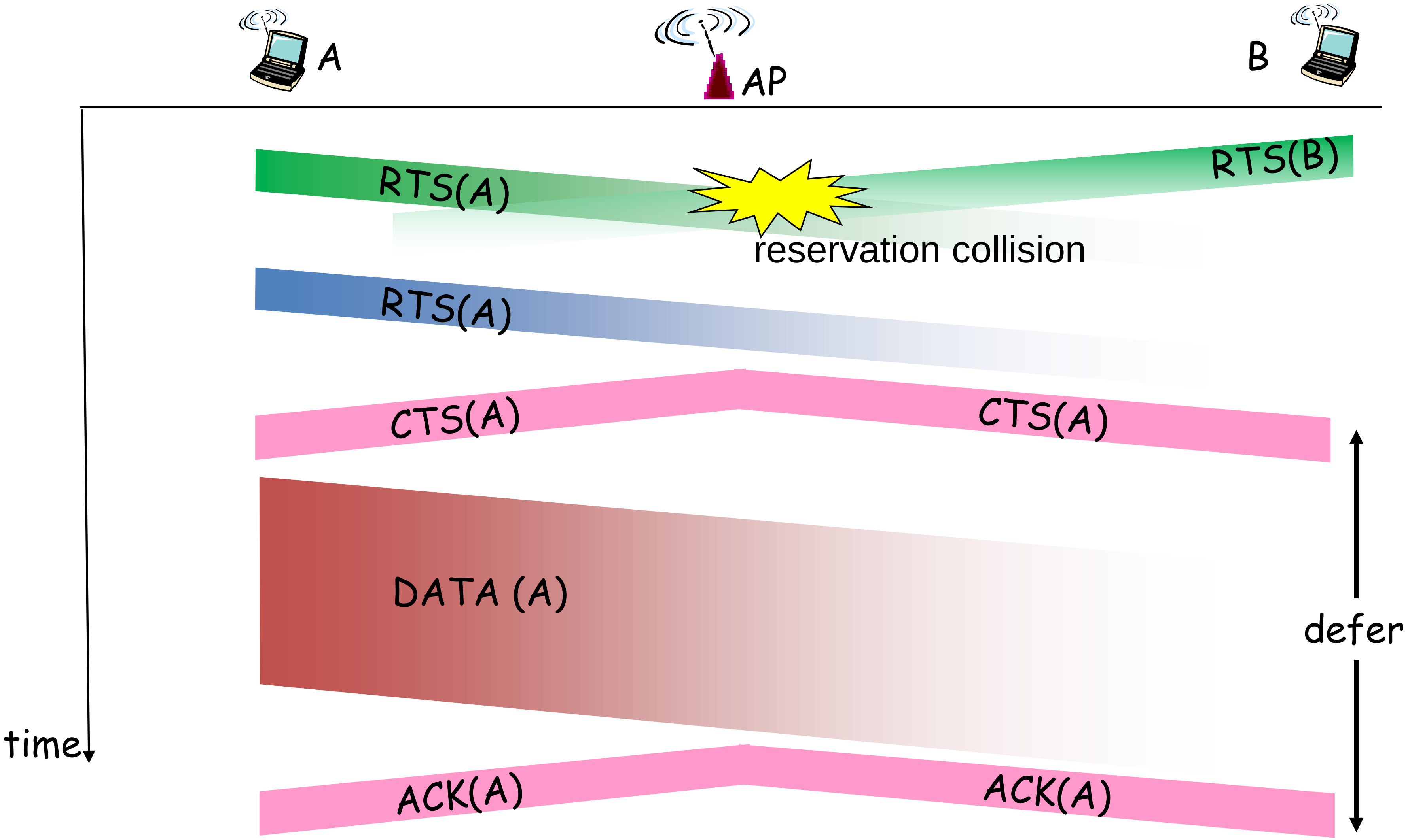


The RTS/CTS frames has a duration field, which consists of information about the length of data packet.

Other stations hear the RTS/CTS frames set their NAV accordingly.

Q: Under such approach, will the packets still collide?

Still Collision in RTS-CTS exchange



See Animation

Data Link Layer Switching

Connecting Multiple LANs --- Bridges

- Bridge (网桥) & Switch (交换机) are interchangeable terms
  - Operating in the data link layer
  - Examine the data link layer addresses to do routing
  - No check on payload field of frames, so
    - Can transport any kinds of packets: IPv4, IPv6, etc.
  - Can convert between different physical/data link types
- Network Devices
  - Hub (集线器) or repeater (中继器): just electronic amplification
  - Bridge & Switch
  - Router (路由器): operate at Network layer, which examine the addresses in packets and route based on them

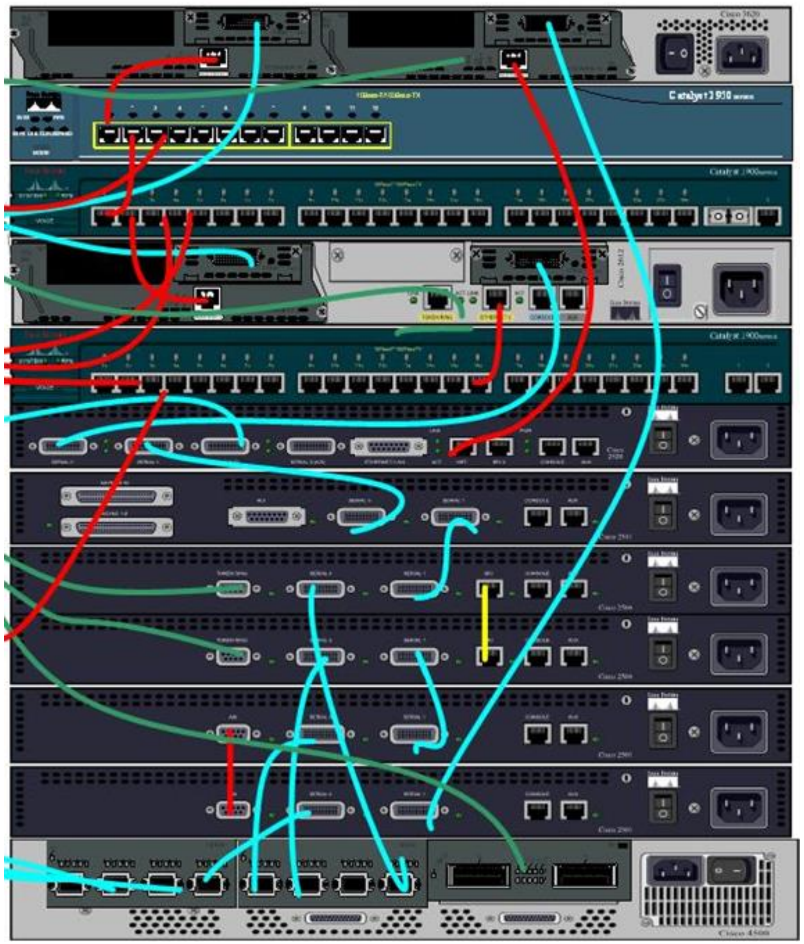
Repeaters, Hubs, Bridges, Switches, Routers & Gateways

- Devices are named according to the layer they process
  - A bridge or LAN switch operates in the Link layer

	Application layer	Application gateway	
	Transport layer	Transport gateway	
Layer 3 Switch →	Network layer	Router	路由器
	Data link layer	Bridge, switch	网桥/交换机
	Physical layer	Repeater, hub	中继器/集线器

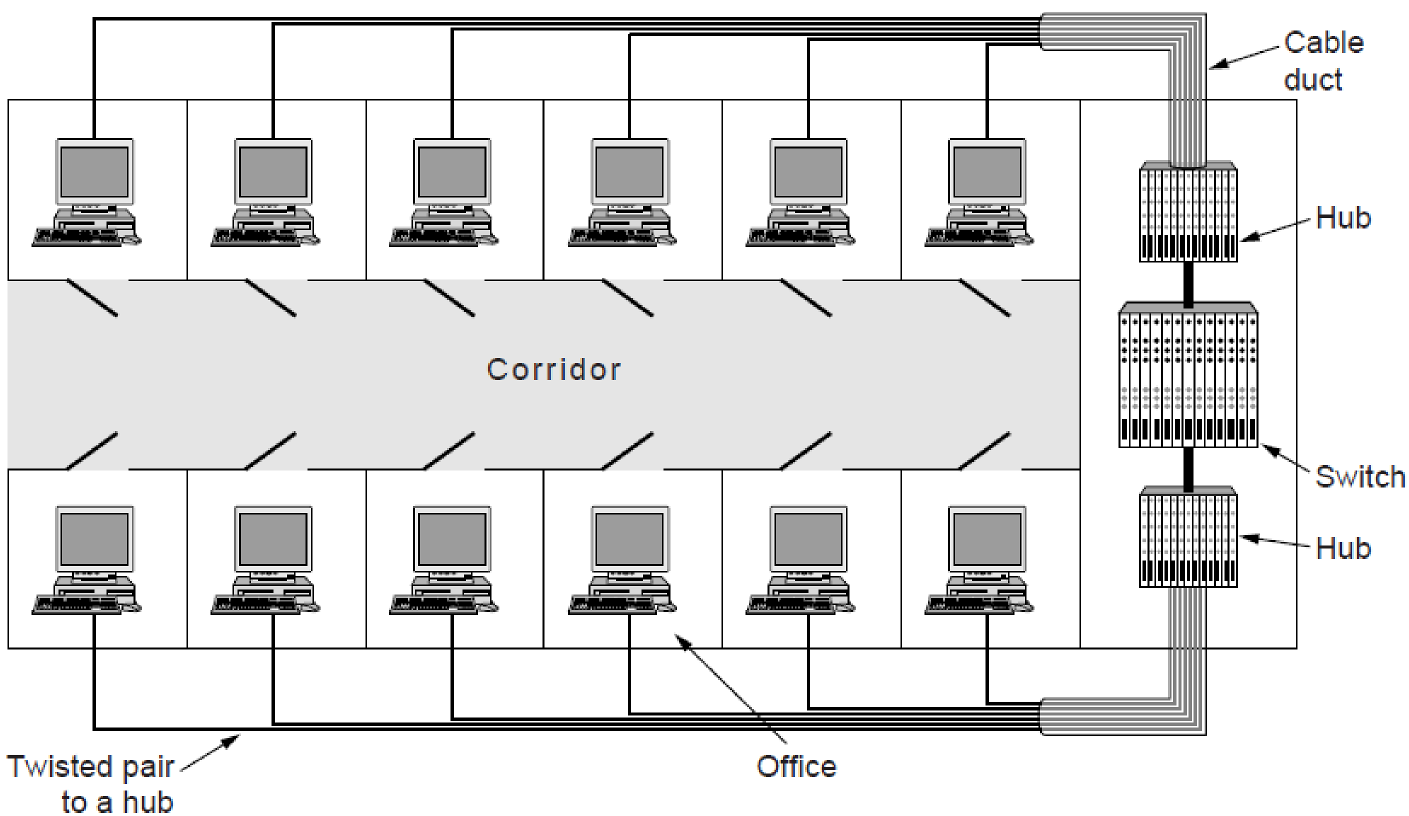
Switches and Routers

Cisco Rack



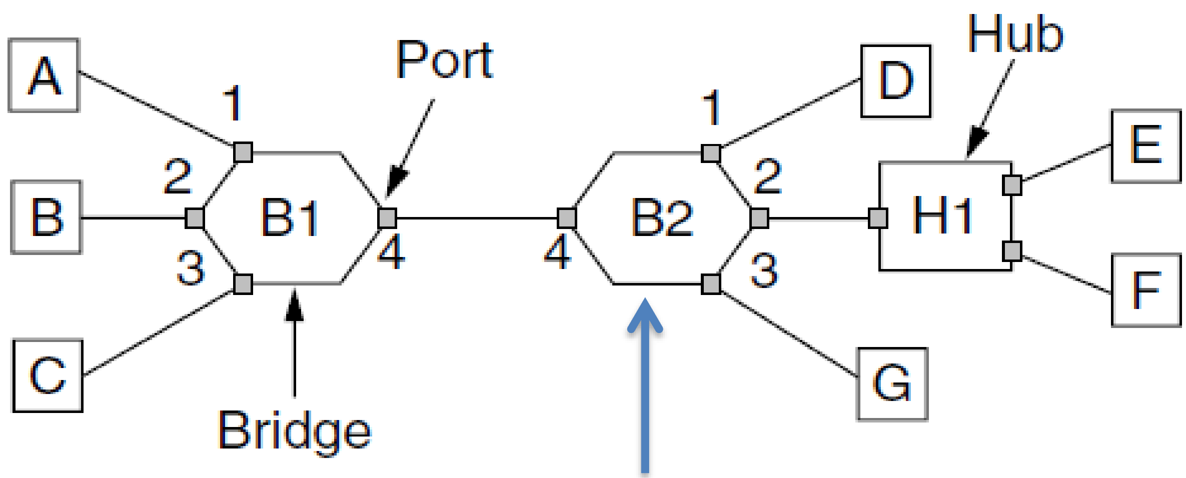
Uses of Bridges/Switches

- Common setup is a building with centralized wiring
  - Bridges (switches) are placed in or near wiring closets



Learning Bridges/Switches

- A bridge/switch operates as a switched LAN (not a hub)
  - Computers, bridges, and hubs connect to its ports



Hash table:

Destination	Port No.
D	1
B	4
…	…

Routing procedure

Depends on the port an incoming frame arrives on and the address to which it is destined:

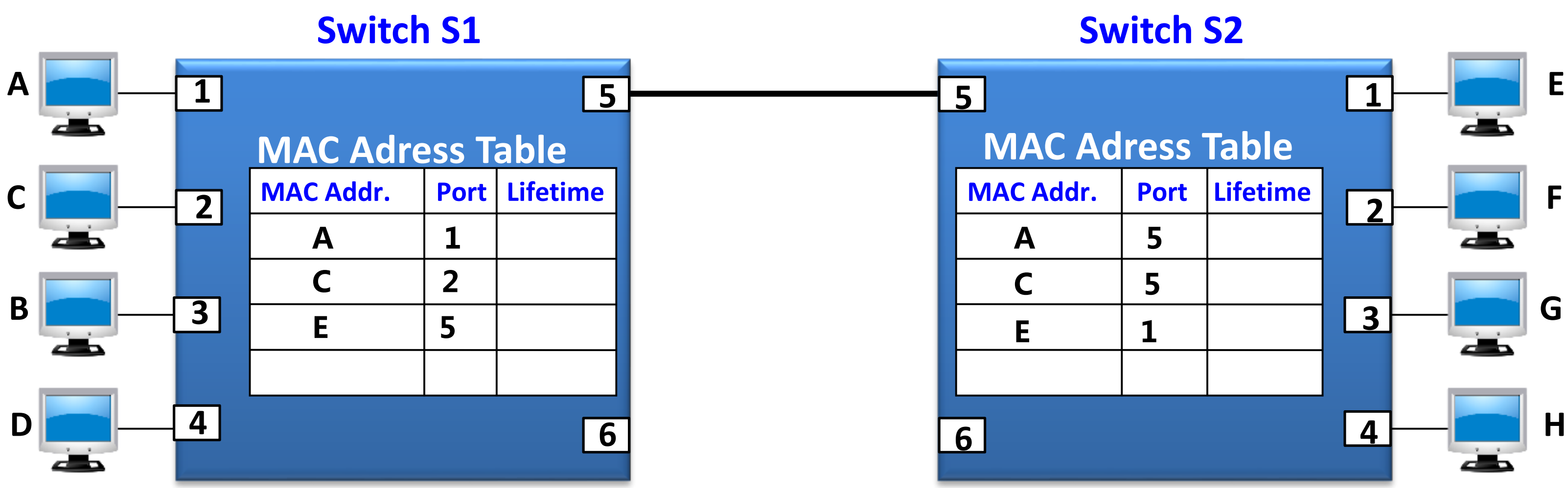
1. If the port for the destination address is the same as the source port, discard the frame
2. If the port for the destination address and the source port are different, forward the frame on to the destination port
3. If the destination port is unknown, use flooding and send the frame on all ports except the source port

Backward learning algorithm

- Backward learning algorithm to build hash table for switching
  - All the hash tables are empty initially. Forward frame to all ports (flooding)
  - By looking at the source address of incoming frames, bridge can tell which machine is accessible on which LAN. So make an entry.
  - Periodically, a process in the bridge scans the hash table and purges all entries more than a few minutes old

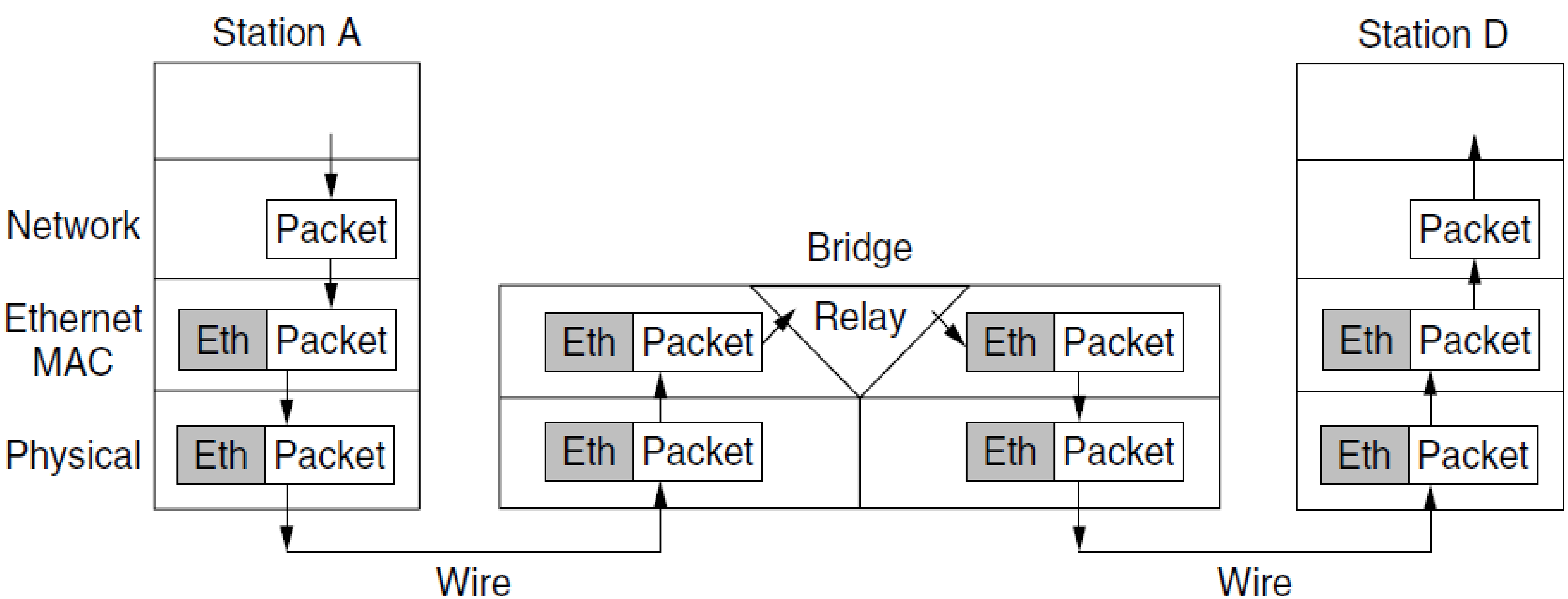
Backward learning algorithm

- Suppose A sends a frame to B, C sends a frame to E, and E sends a frame to A. What's the hash table of both switches?



Protocol processing at bridge

- Bridges/switches extend the Link layer
  - **Use but don't remove** Ethernet header/addresses
  - **Do not touch** Network header



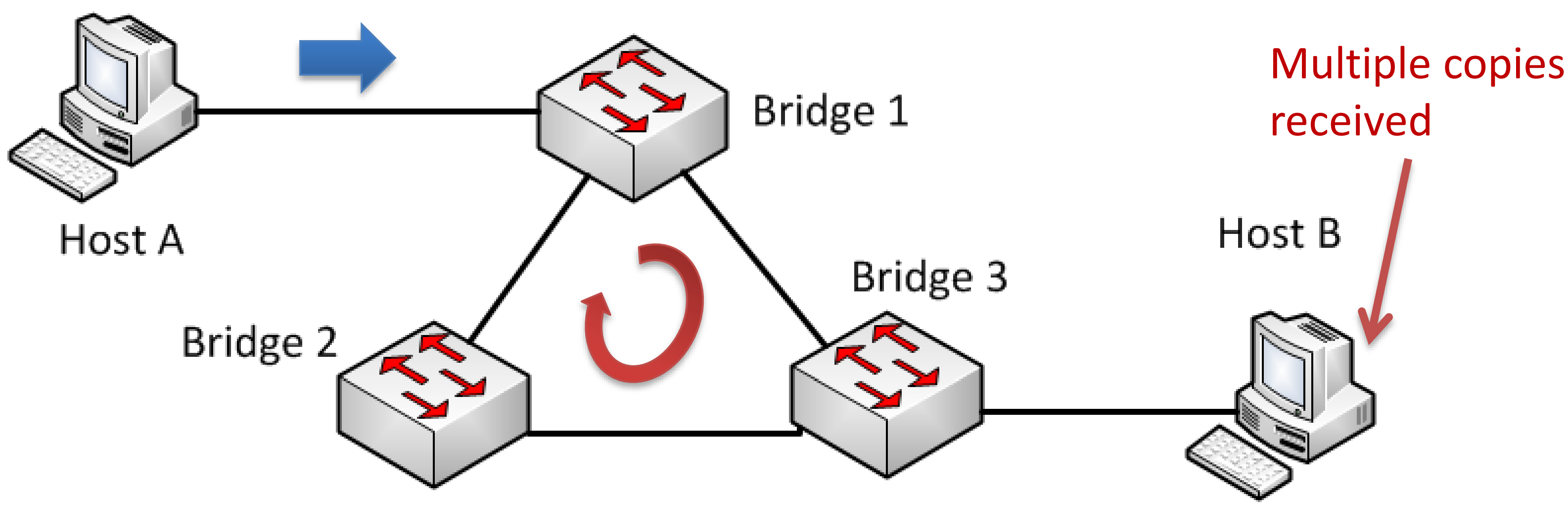
Bridge/Switches Design

Two basic architectures:

- Cut-through Switching:
  - Examining the packet destination address only before forwarding it on to its destination segment.
- Store-and-forward Switching:
  - Accepting and analyzing the entire packet before forwarding it to its destination.

Loop-free Bridge/Switch Topology

- Bridge topologies with loops and only backward learning will cause frames to circulate forever
- Solution
  - Only use a subset of forwarding ports for data to avoid loops
  - Selected with the spanning tree algorithm by Perlman



Radia Perlman: ”Mother of the Internet”

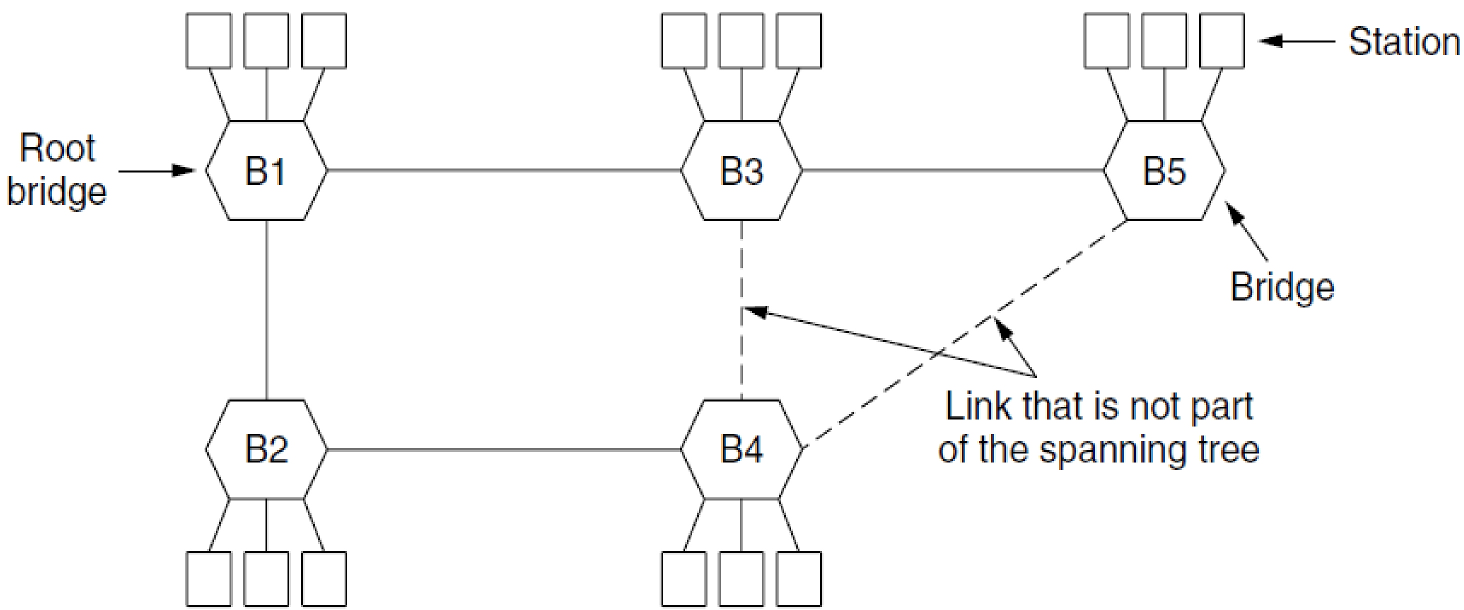
- Radia Perlman, PhD at MIT, worked at DEC, Novell, Sun and Intel
- Proposed STP and TRILL , and contributed a lot to IS-IS and OSPF
- She is sometimes referred to as the "*Mother of the Internet*", a title which she dislikes
- She wrote a poem, describing a network to be a beautiful tree in an oil painting:

I think that I shall never see
A graph more lovely than a tree.
A tree whose crucial property
Is loop-free connectivity.
A tree which must be sure to span.
So packets can reach every LAN.
First the Root must be selected
By ID it is elected.
Least cost paths from Root are traced
In the tree these paths are placed.
A mesh is made by folks like me
Then bridges find a spanning tree.

"2010 SIGCOMM Lifetime Achievement Award given to Radia Perlman"

Spanning Tree

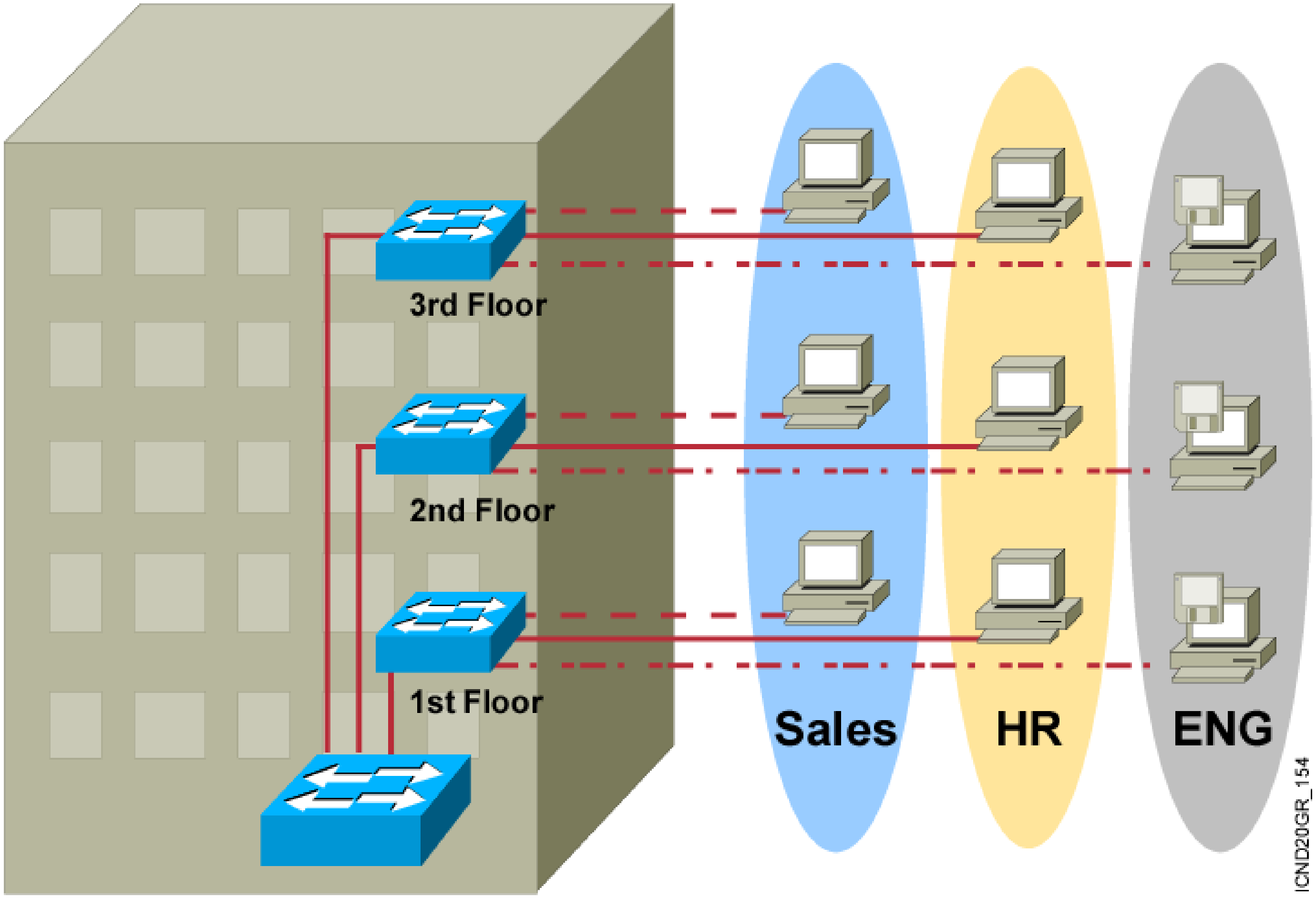
- Example
  - B1 is the root, two dashed links are turned off
  - B4 uses link to B2 (lower than B3 also at distance 1)
  - B5 uses B3 (distance 1 versus B4 at distance 2)



See Animation

Does it matter who is on which LAN?

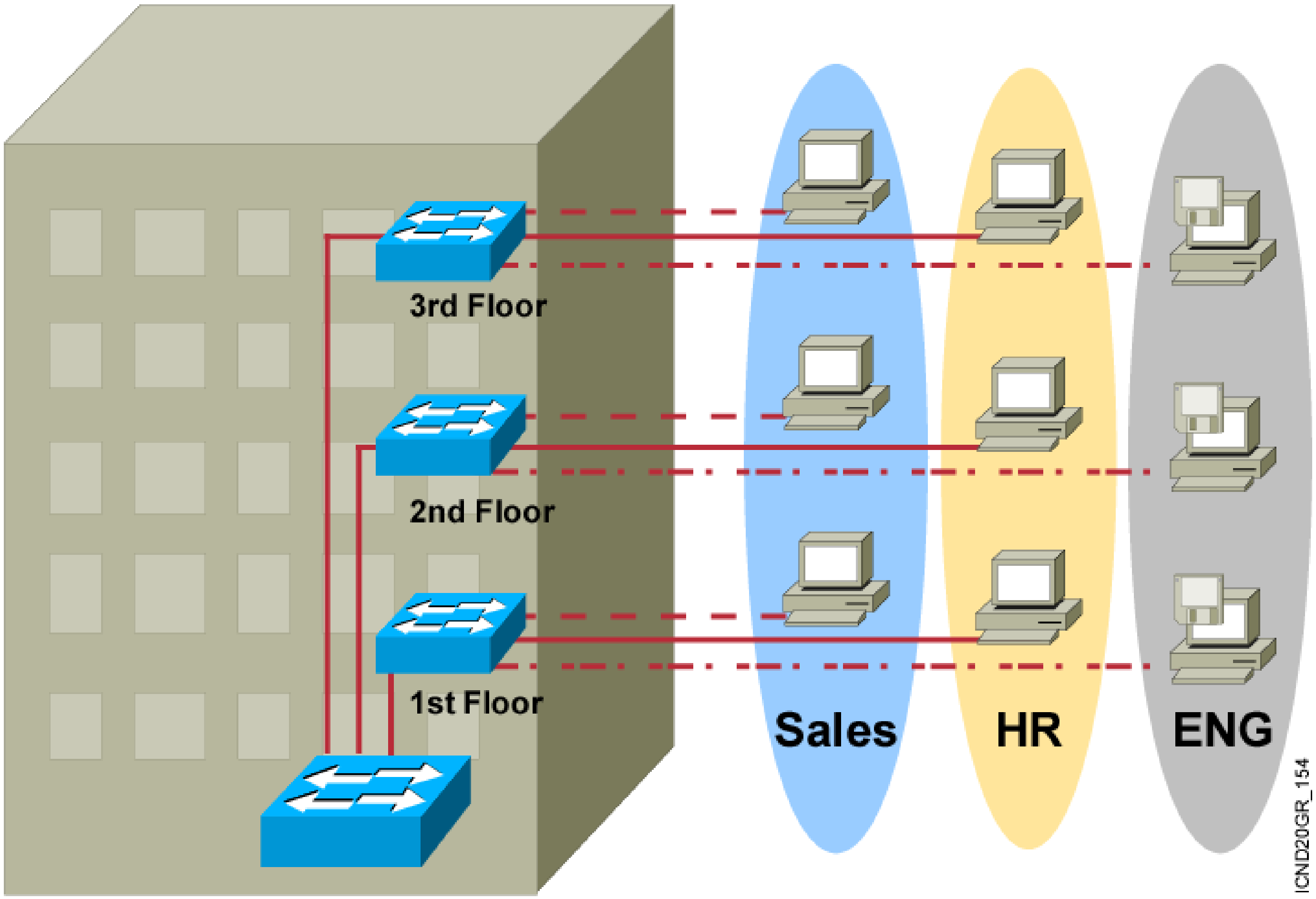
- Yes, it often matters



Does it matter who is on which LAN?

- Yes, it often matters.
- Better to group users on LANs to reflect the organizational structure rather than the physical layout of the building
  - Security: promiscuous mode (混杂模式)
  - Load
  - Broadcasting:
    - e.g. get MAC address for an IP packet (ARP)
    - Broadcast storm

VLAN (Virtual LAN) example



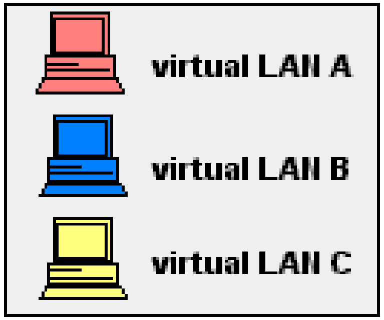
IEEE 802.1q

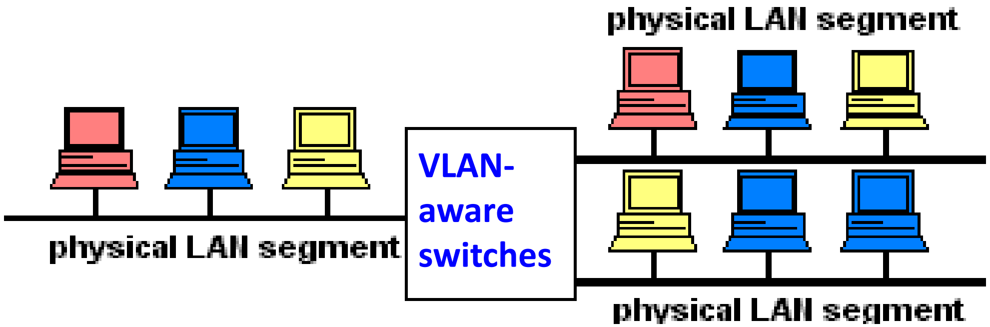
Rewire buildings entirely in software

A VLAN = A Broadcast Domain = Logical Network (Subnet)

Virtual LANs

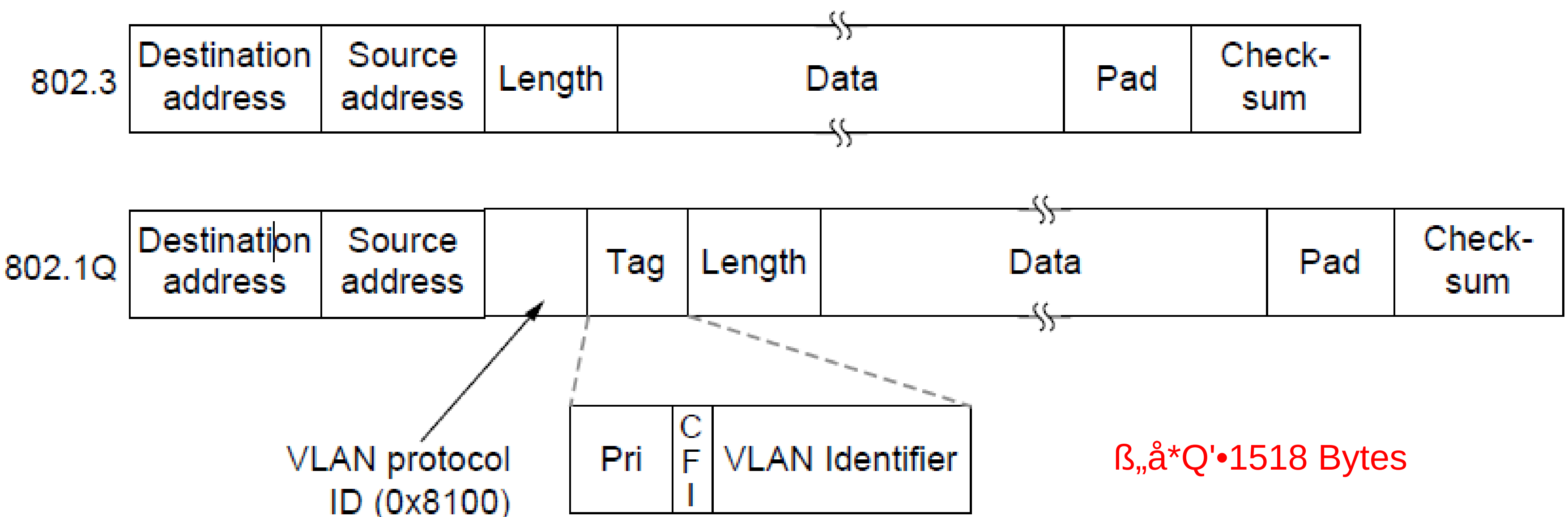
- VLANs splits one physical LAN into multiple logical LANs to simplify management tasks
  - VLANs are based on VLAN-aware switches
  - Ports are “colored” according to their VLAN and may be labeled with multiple VLAN colors
  - The configuration tables have to be set up in the bridges





Virtual LANs

- 802.1Q frames carry a color tag (VLAN identifier, 4 bytes)
  - Length/Type value is 0x8100 for VLAN protocol
  - *Priority* means class of service (COS)
- Between LANs communication each other through the router or network layer switch

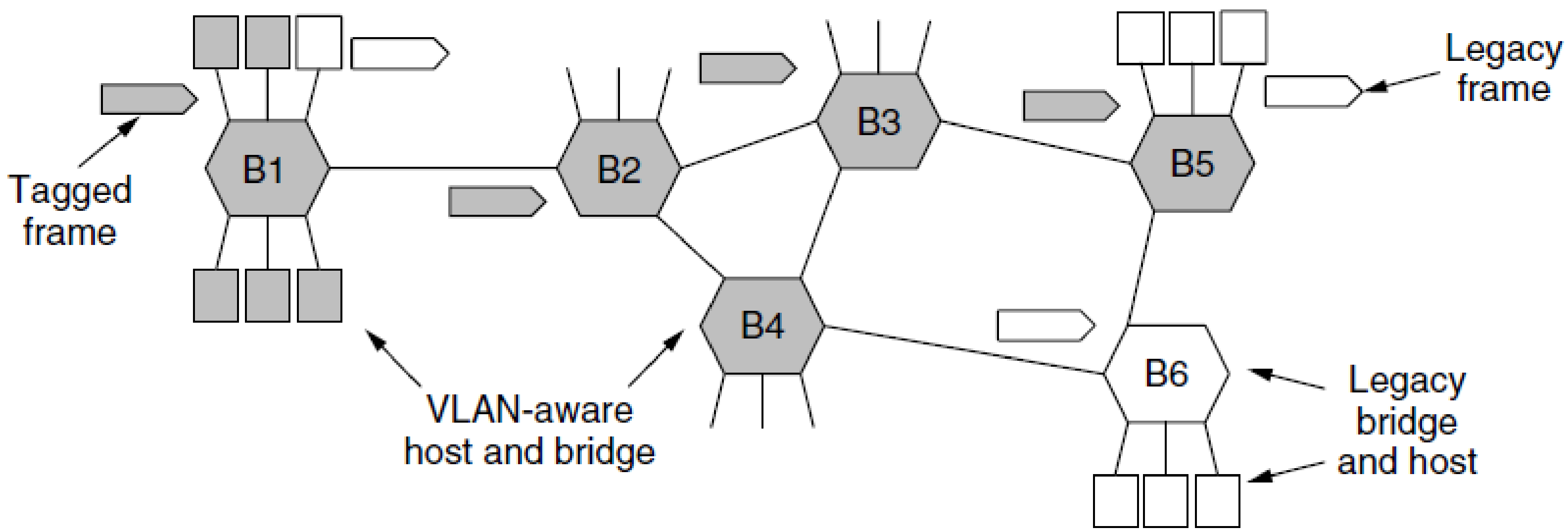


ß„å*Q'•1518 Bytes

Total frame length: 1522 bytes

Virtual LANs

- Bridges need to be aware of VLANs to support them
  - In 802.1Q, frames are tagged with their "color"
  - Legacy switches with no tags are supported



Review

- Wireless LAN
  - Hidden and Exposed terminals
  - CSMA/CA with RTS/CTS
- Data Link Layer Switching
- Spanning Tree Bridges
- Virtual LAN

Thank you!

Q & A