lecture 7 Data Link Layer - LAN

Local Area Network (LAN)

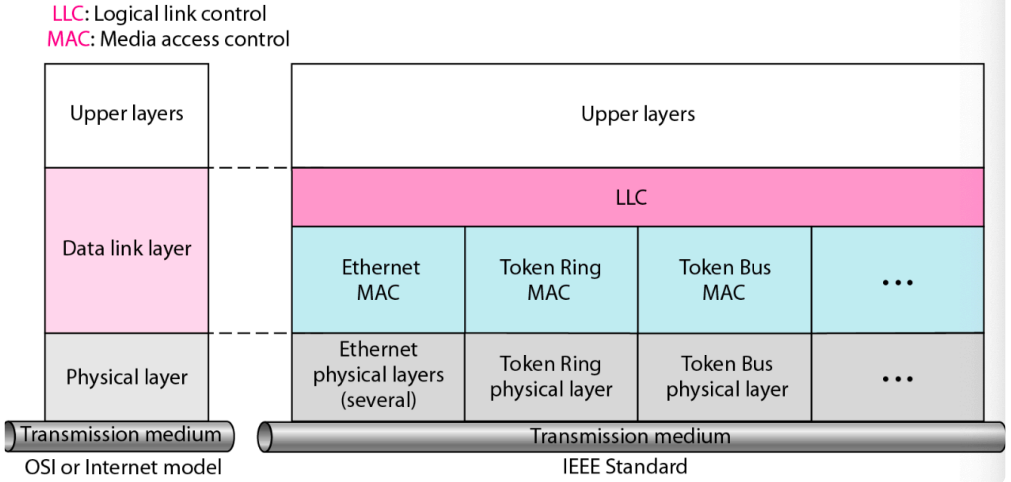
Introduction

- Local Area Networks (LANs): The use of *shared transmission media* or shared *switching capacity* to achieve *high data rates* over *relatively short distances*
- Technologies:
  - Topology: bus, tree, ring, star
  - Transmission medium
  - Medium Access Control

four main architectures

- Ethernet
- Token Ring
- Token Bus
- Fiber Distributed Data Interface (FDDI)
- first three are **IEEE802**, FDDI is an ANSI

- IEEE Project 802 specifies the detailed functions of layers 1 and 2 (and small parts of layer 3)



IEEE802 Standards

- 802.1 - Internetworking

- 802.2 - *Logical link control*
  - upper sublayer
  - *format and interface to the network layer*
  - common to all IEEE802 LAN and MAN
- 802.x - *Medium access control*
  - lower sublayer
  - **access method**

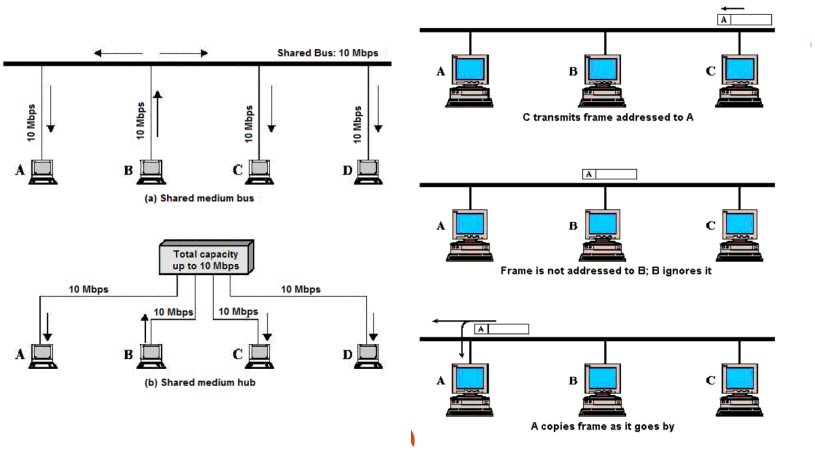
802.3 Ethernet

- most common LAN technology
- use **CDMA/CD** as the access method

Ethernet

Topology

- shared medium bus
- all signals are broadcast to every connected node (half-duplex)
- For 10Base-T, physical topology is a *star*, but logical topology is a *bus*



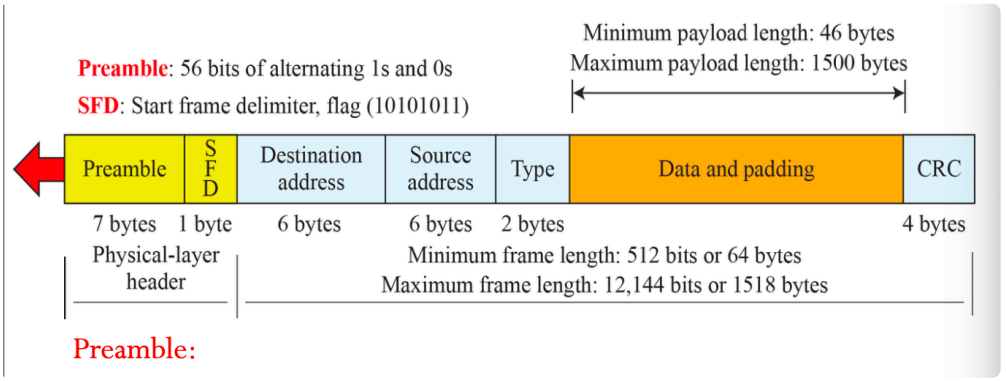
Data Access in Ethernet

- *NIC* (network interface card) *pick up the frame* intended for itself (base on the *physical address*)

Ethernet Frame Structure

- Min: 64 bytes

- Max: 1518 bytes



Preamble:

- 7 bytes with pattern 10101010 followed by one byte with pattern 10101011, *used to synchronize* receiver and sender clock rates

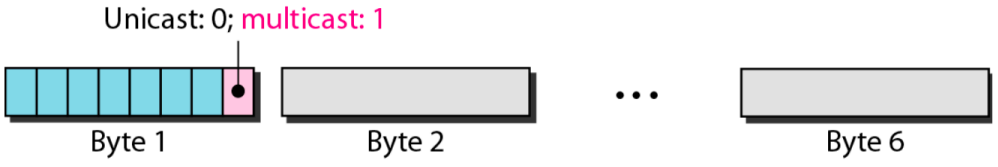
Address

- 6 bytes
- if NIC receive destination or broadcast address (ARP packet), pass data in frame to network-layer protocol
- discard frame

Type: *higher layer protocol*
CRC: *cyclic redundancy check*, simply dropped

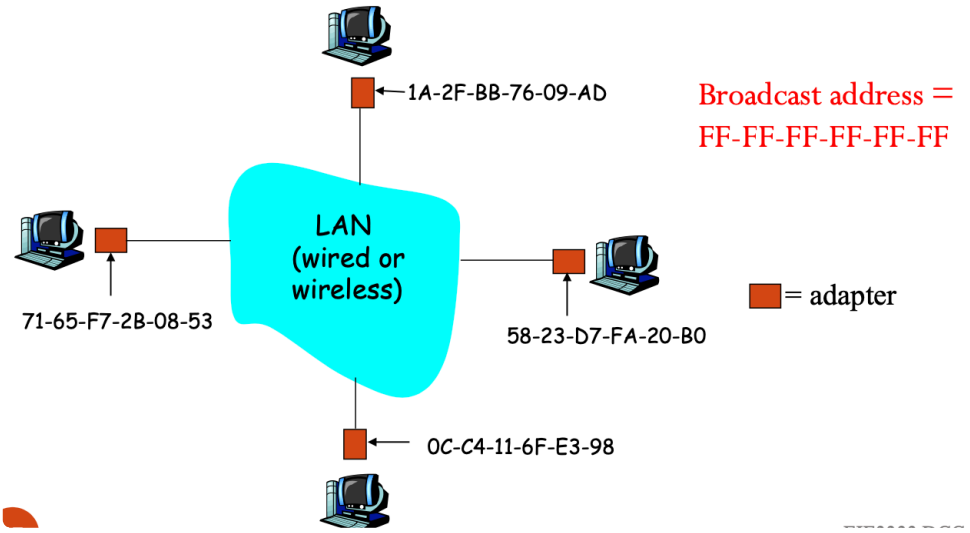
MAC address

- LAN/ physical / Ethernet address
- get **datagram** from one interface to another *physically-connected* interface
  - **48 bits** burned in the **NIC adapter ROM** 网卡适配器ROM
- least significant bit of the first byte defines the type of address
  - 0: unicast,



LAN address

- each adapter on LAN has *unique LAN address*



- allocation administered by IEEE
- Manufacturer bus portion of MAC address space
- **flat address** - portability

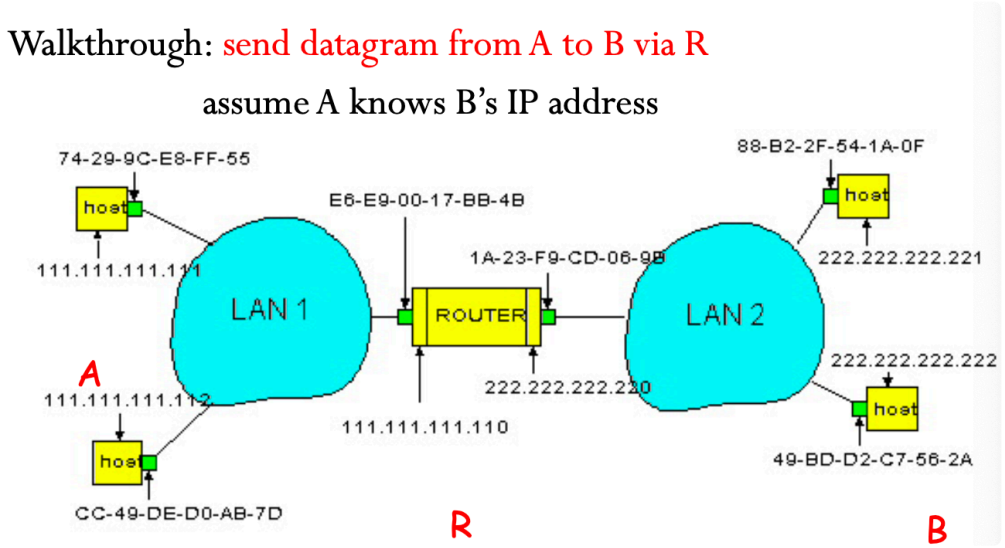
ARP: Address Resolution Protocol

- Each IP node (Host, Router) on LAN has an **ARP table**
- ARP Table: IP/MAC address mappings for some LAN nodes `<IP, MAC, TTL>`
- TTL: time after which address mapping will be forgotten (20 mins)

same LAN(network)

- A wants to send datagram to B, and B's MAC not in A's ARP table
- A broadcast ARP query packet `FF-FF-FF-FF-FF-FF`
  - all machine receive
- B receives ARP packet, replies to A with its MAC
  - frame sent to A's MAC (*unicast*)
- A *caches* IP to MAC in its ARP table and times out
  - soft state: information that times out unless refreshed
- **plug and play**
  - with out intervention from network administrator

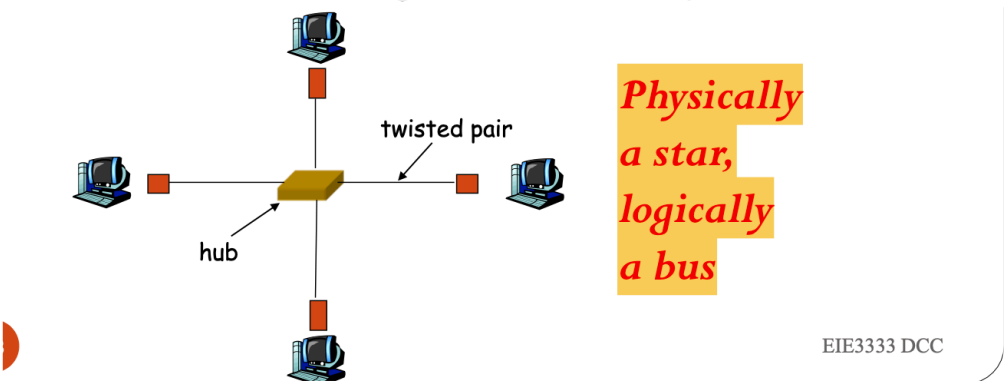
Routing to another LAN



- *Two ARP tables in router R*
- A creates datagram with source A, destination B
- A use ARP to get *R MAC* 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 adapter receives frame and R adapter receives frame
- R remove IP datagram from frame, knows it is destined to B
- R use ARP to get B MAC
- R create frame containing *A to B IP datagram* sends to B

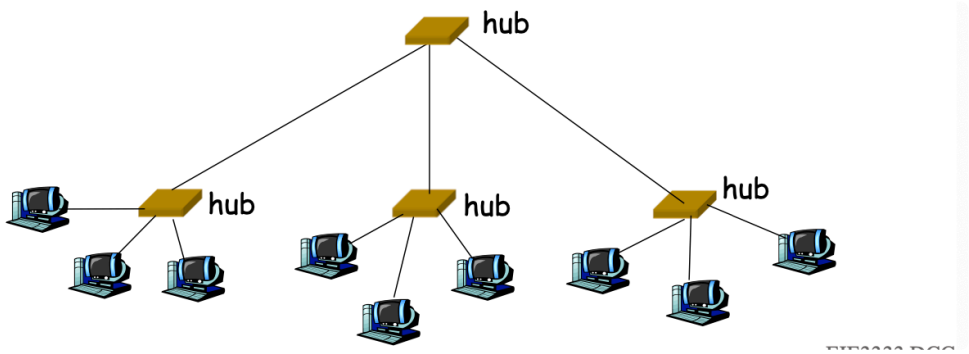
Hubs

- physical-layer repeater
- from one link go out to all other links
- *No CSMA/CD* at hubs
- network management



- **Backbone hub** interconnect LAN segments

- extend maximum distance
- larger collision domain
- can not interconnect 10BaseT and 100BaseT



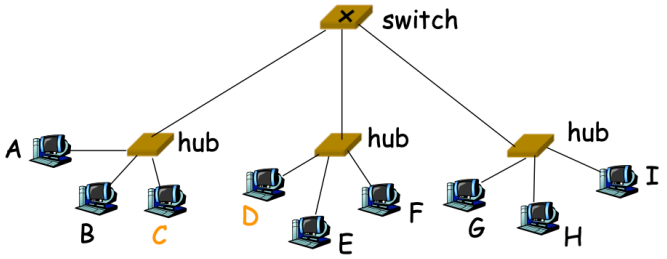
Switch

- **Link layer device**
- store and forward Ethernet frames
- Examines frame header and *selectively* forwards based on *MAC destination address*
- use *CSMA/CD*
- **transparent**: unaware of presence of switches
- Frame Forwarding: *like a routing problem*

Self Learning

- switch has a **switch table**
- `MAC address, Interface, Time Stamp`
- *learn location of sender*

Suppose D replies back with frame to C



Address	Interface
A	1
C	1
D	2
E	2
G	3

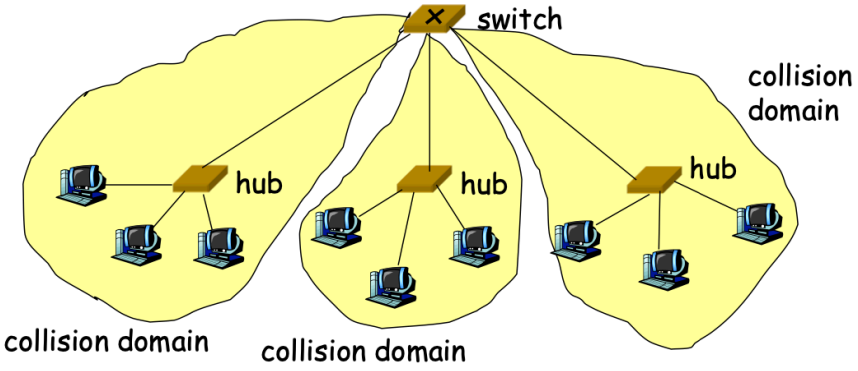
- Switch receives frame from D
  - notes D is on interface 2, add D entry in the table
  - because C is in the table, switch selectively forwards frame only to interface 1
- frame received by C

Collision Domains

- devices must compete to communicate
- *All ports of a hub*
- *Every port of a switch*
- switch break the segment into *smaller* collision domains

Switch: Traffic Isolation

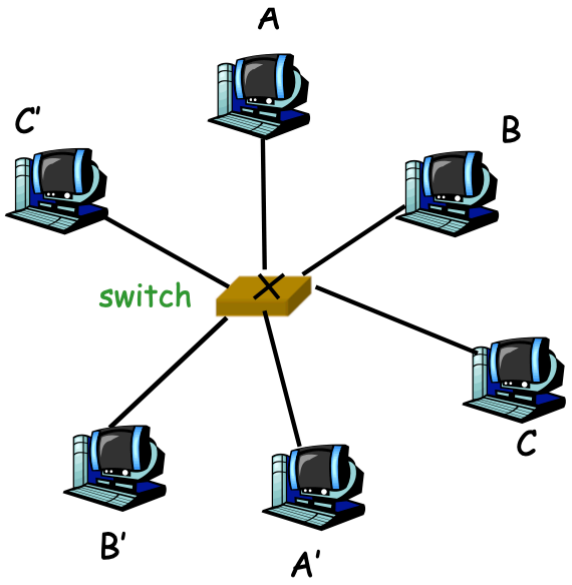
- switch **filters** packets



Switch: Dedicated Access 专线接入

- many interfaces
- direct connection
- more than one station transmitting at a time, no collisions
- **Full duplex**
- *multiplying* capacity of LAN

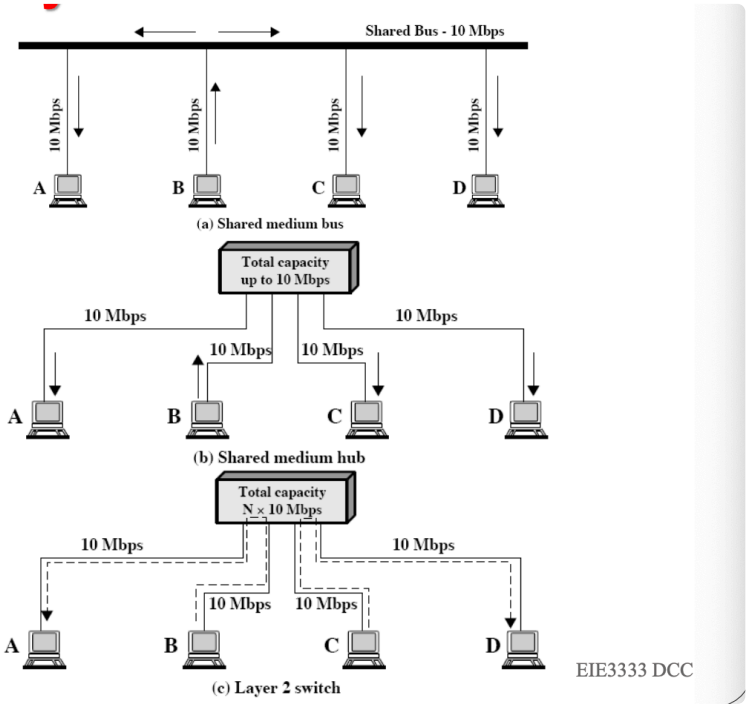
- A-A' and B-B' simultaneously



Broadcast Domain

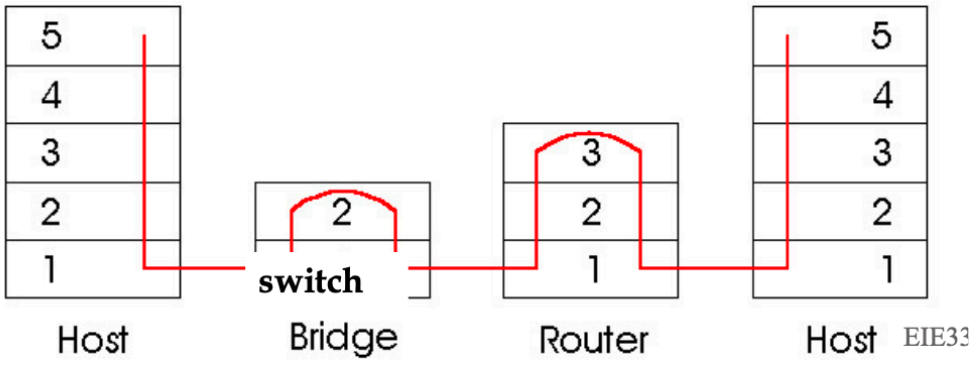
- switch will forward broadcast traffic to **all interface except** the originated from
- a lot of broadcast traffic might impact your network performance, *reducing size*
- **Router break broadcast domain**
- **VLANs** on switch also **break broadcast domain**

Total capacity



Switch vs Router

- *store and forward*
- router: network layer devices, switch: link layer devices
- Routers: **routing table**, **routing algorithms**
- Switch: **switch table, filter, learning algorithms**

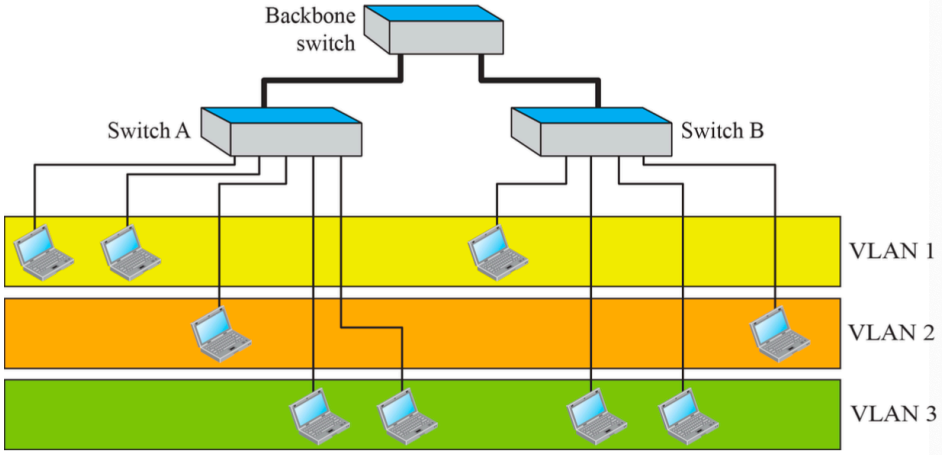


Virtual LANs

Virtual LANs

- local area network configured by **software** not by physical
- 802.1Q
- consists of a logical group of stations, independent of their actual physical location
- logically segmented
- without restriction on physical locations
- information to *identify a packet as a part of a specific VLAN* is **inserted by a switch** and **preserved through switch** and **router connection**
- one broadcast will reach every station belonging to the same vlan, but not any other
- **dynamically reconfigured**

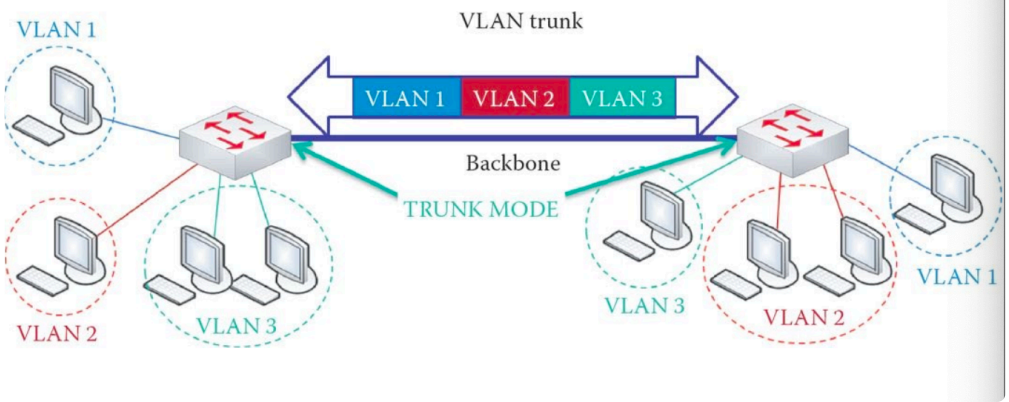
- Two switches in a backbone using VLAN software



Access Mode or Trunk Mode

- in the *access mode*, the interface belongs to *one and only one vlan*, normally attached to an *end user device or a server*
- *trunk mode*: multiplexes traffic for *multiple VLANs* over **same physical link**
- **trunk links interconnect switches**
- in order to multiplex vlan traffic, *special protocols* **encapsulate or tag** (mark), the frames so that the receiving devices knows to *which vlan the frame belongs*
- Trunk protocols are either proprietary (Cisco proprietary Inter-Switch ISL) or based upon IEEE802.1Q

- Trunk mode ports used with VLAN switches



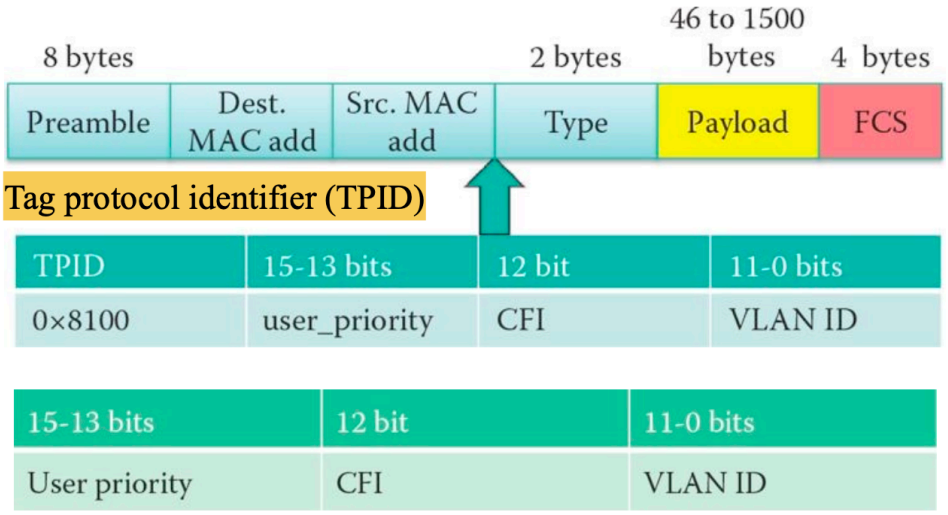
Tagging Frame for vlan Identification

- adding a **vlan identification header** to the frame, through *trunk link*

- Switches tag frames to identify the vlan they belong to. Different tagging protocols exists; IEEE802.1Q: *the structure* of the tagging header added to the frame
- *Switches add vlan tags* to the frames **before placing them into trunk links and remove the tags before forwarding frames though non trunk ports**
- the frames transverse any number of switches via trunk lines and still be forwarded within the correct vlan at the destination

VLAN Tag 802.1Q

- Tagging a frame by inserting an 802.1Q header



TPID	15-13 bits	12 bit	11-0 bits
0×8100	user_priority	CFI	VLAN ID

15-13 bits	12 bit	11-0 bits
User priority	CFI	VLAN ID

- **User Priority (3 bits)**: *priority level of the frame*
- **Canonical Format Indicator (1 bit)**: zero for Ethernet switches, used for compatibility between Ethernet and Token Ring network, 802.3 use and 802.5 non-canonical format
- **vlan ID (12 bits)**: *identifies the vlan id* to which frame belongs to

VLAN Configuration

- **four vlan configuration**
  - port group
  - source MAC address
  - network layer information, (protocol or network address)
  - IP multicast group
- *port group* one **main disadvantage**: the network administrator *must reconfigure* vlan membership when a user moves from one port to another
- *source MAC address* allows a administrator to *add or drop* a host **without physically reconnecting it**

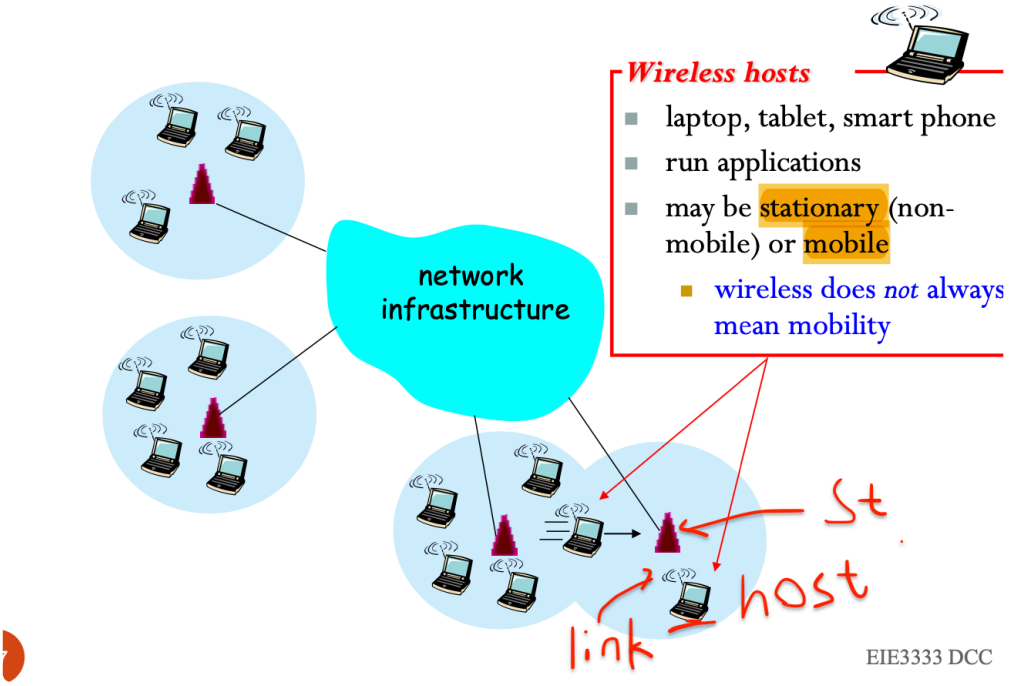
- *network layer protocol or IP address* configuration **flexibility of dynamically** such as VoIP
- *multicast group* is also **flexible**

Wireless LAN

Wireless LAN

- Wireless Local Area Network (*WLAN or Wi-Fi*)
- Two challenge :
  - Wireless
  - Mobility 流动性

Element



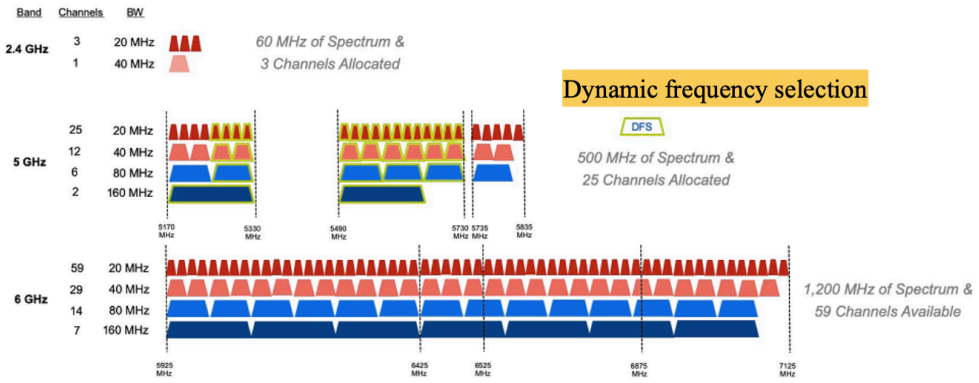
- Wireless host : stationary or mobile
- Base station
  - typically connected to *wired network*
  - relay - wired network and wireless host in its "area"*cell tower 802.11 access point*
- Wireless link
  - connect mobiles to base station
  - used as **backbone link**

- **multiple access protocol** coordinates link access
- *various* data rates, transmission distance

Characteristics

- Decreased signal strength: radio signal attenuates
- Interference 干扰 from other sources: 2.4GHz shared by other devices...
- Multipath propagation: radio signal arriving at destination at slightly different times

bands in the three bands: 2.4GHz, 5GHz and 6GHz



Wireless Network Architecture

Two configuration

- Infrastructure Mode
- Ad hoc Mode

Two service sets are defined

- Basic service set (BSS)
- Extended service set (ESS)

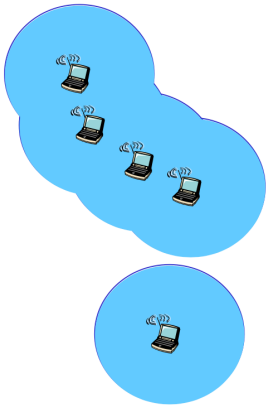
WLAN configuration

Infrastructure Mode

- base station connects mobiles into *wired network*
- handoff: mobile *changes base station* providing connection to wired network

Ad hoc mode

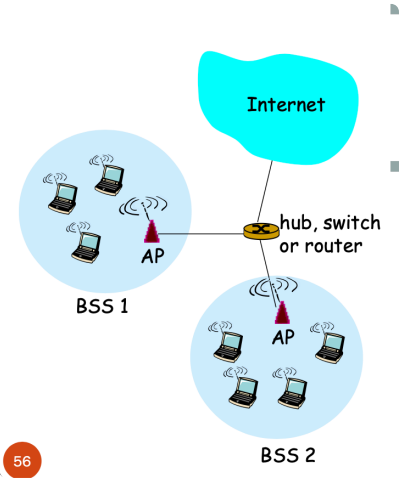
- *no base station*
- node can *only transmit to other node* within link coverage
- nodes organize themselves into a network: route among themselves



Service Sets

Basic Service Set

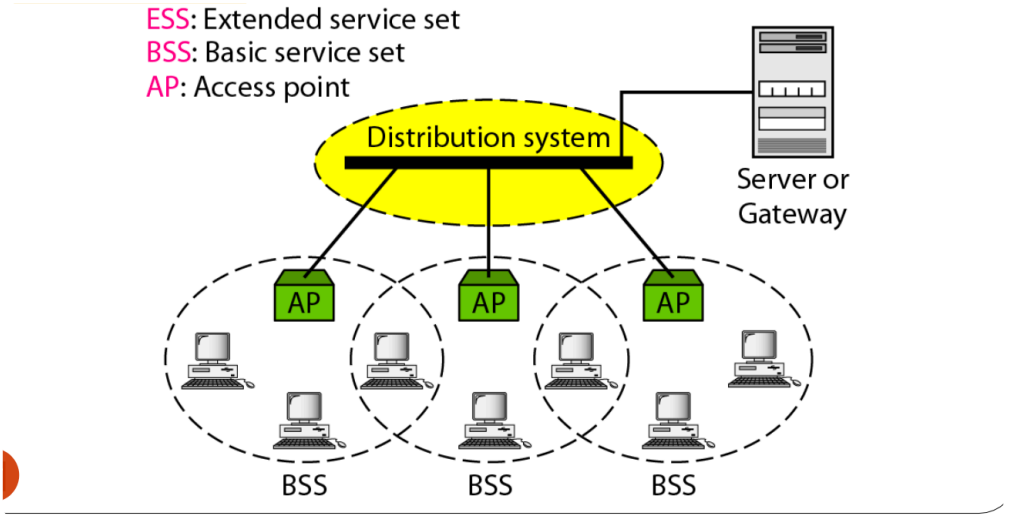
- wireless host communicates with *base station*
  - base station = **AP** access point
- **BSS** in infrastructure mode contains
  - wireless hosts
  - AP: base station
  - ad hoc mode: host only



Extended Service Set

- several BSS *connected by a distribution system*

- behaves like a single network
- Distribution system can be any networks but usually a **backbone wired Ethernet**



Service Set Identifier (SSID)

- SSI is used to **identify the access point** and its **associated wireless network**
- a list of wi-fi name is ssid
- How the people know the existence of a wifi network?
  - AP *periodically send* beacon frames, includes *AP's SSID and MAC address*
  - device *scans* the available frequency channels, seeking beacon frames

802.11 Channels Association

- 802.11b: 2.4-2.485GHz spectrum divided into **11** channels at different frequencies
  - AP admin *chooses frequency for AP*
  - *Interference possible*: channel can be the same as neighboring AP
- Host: must **associate** with an AP
  - listening for **beacon frames**
  - selects AP
  - authentication
  - Dynamic Host Configuration Protocol (**DHCP**) to get **IP address in AP's subnet**

802.11 Passive/Active Scanning

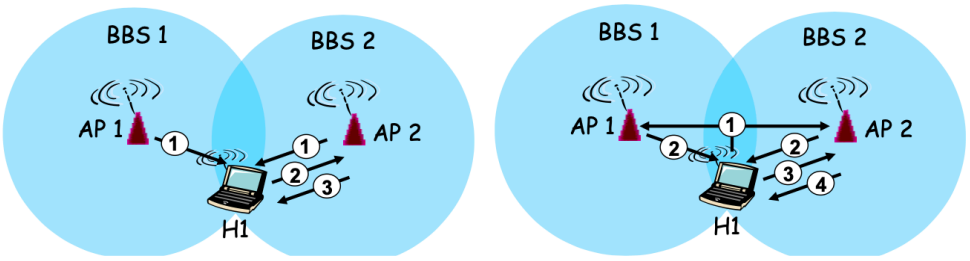
Passive Scanning

1. beacon from APs

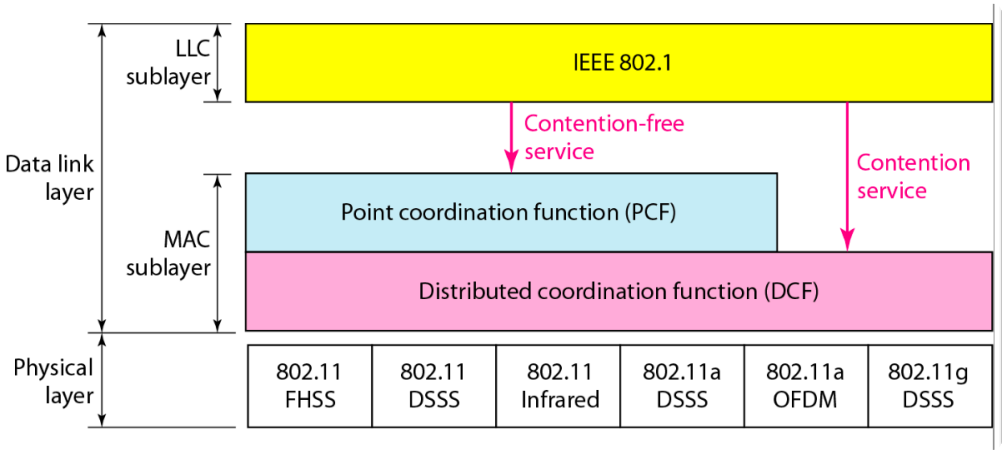
2. association Request frame H1 to AP
3. association Response frame AP to H1

Active Scanning

1. *Probe Request frame* **broadcast** from H1
2. *Probe response frame* from APs
3. Association Request frame H1 to AP
4. Association Response frame AP to H1



MAC layers in IEEE 802.11 standard



802.11: Multiple Access

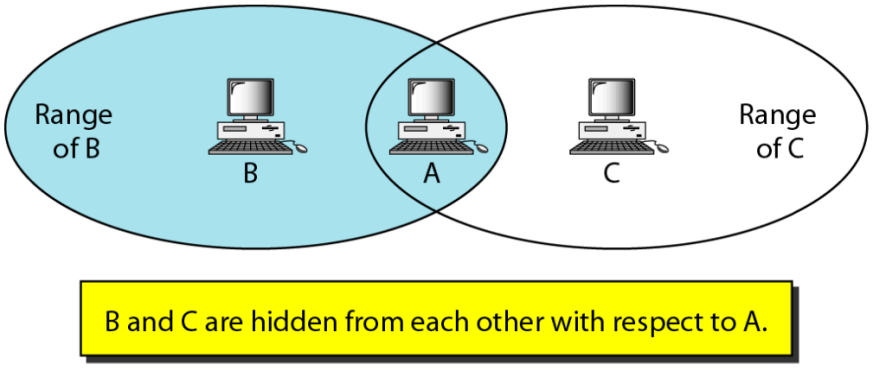
- Avoid collisions
- **CSMA - sense before transmitting**
- **no collision detection**
  - different to receive (sense collisions) when transmitting due to weak received signal
  - hidden terminal, fading Cannot sense all collisions
  - **Avoid collisions** CSMA/CA(avoid) **distributed coordination function (DCF)**

Access Method

- **DCF CSMA / CA** (mandatory) (Basic Access)
  - *randomized* **back-off** mechanism
  - *Minimum distance* between consecutive packets
  - **ACK packet** for acknowledgement
- **DCF with RTS/CTS** (optional)
  - *RTS-CTS-DATA-ACK*
  - physical carrier sensing + **NAV (network allocation vector)** containing *time value* that indicates the duration up to which medium is expected to be busy
  - *Every packet contains the duration info* for the remainder of the message
  - Every node overhearing a packet continuously **update its own NAV**
- **PCF** (optional)
  - **polling** is used, contention free

Hidden Node Problem

- fuzzier boundaries
- each node may not be able to communicate with every other node



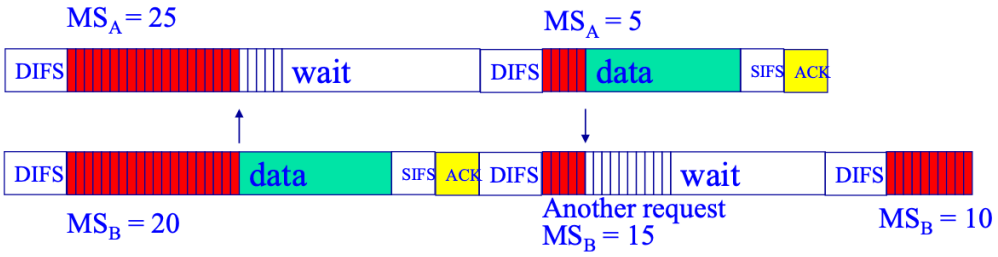
802.11 MAC

- **Inter frame spacing IFS**
  - short IFS, PCF IFS (PIFS), DCF IFS (DIFS)
- Priorities
  - different inter frame spaces
  - *SIFS*
    - **highest priority** for *ACK, CTS, polling response*
  - *PIFS*
    - **medium priority** for *time-bounded service using PCF*
  - *DIFS*
    - **lowest priority** for *asynchronous data service*

DCF CSMA/CA Basic Access

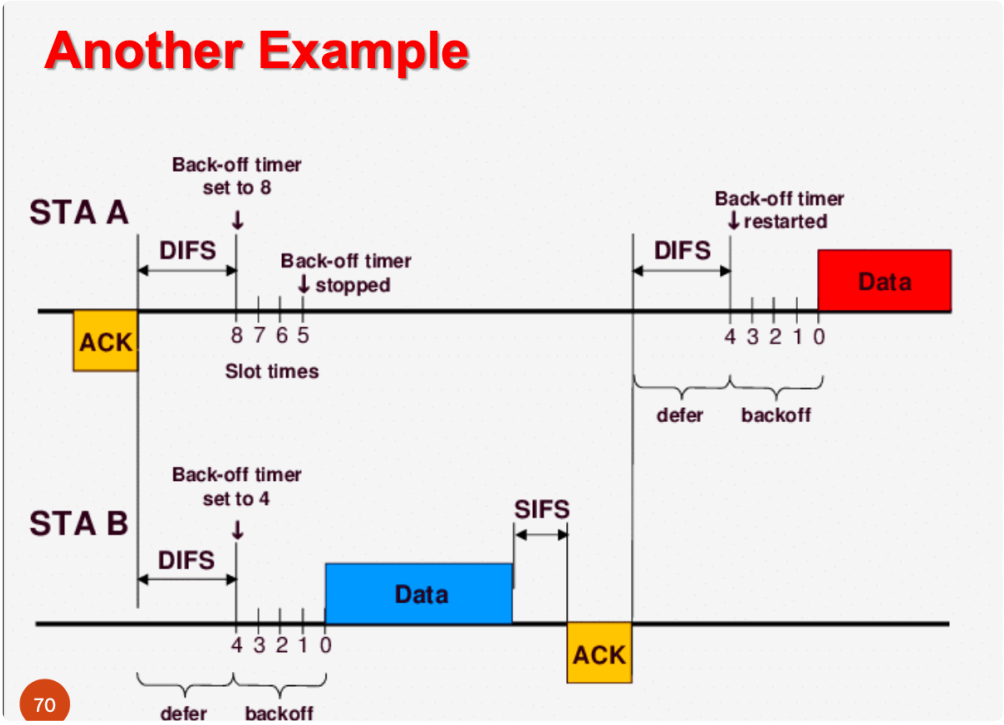
- listen to the same medium
- busy wait until the end of current transmission
- **again waits** for an **additional predetermined time** period **DIFS**
- **picks up a random number of slots** (the *initial value of backoff counter*) within a contention window to wait before transmitting its frame
- listen up to chosen slot **[0, CW]**
- other MSs during **this time period** (backoff time), the MS **freezes its counter**
- **resumes count down** after other MSs finish transmission **plus DIFS**
- Backoff Time = **random(0, CW) * slot time**
- The set of **CW values** is the *sequentially ascending powers of 2, minus 1* (1, 3, 7, 15...)
- **Slot time** = Time needed for *detecting a frame* + *Propagation delay* + Time needed to *switch from the Rx state to Tx state* + Time to *signal to the MAC layer* the state of the channel

Random Delay Helps CSMA/CA



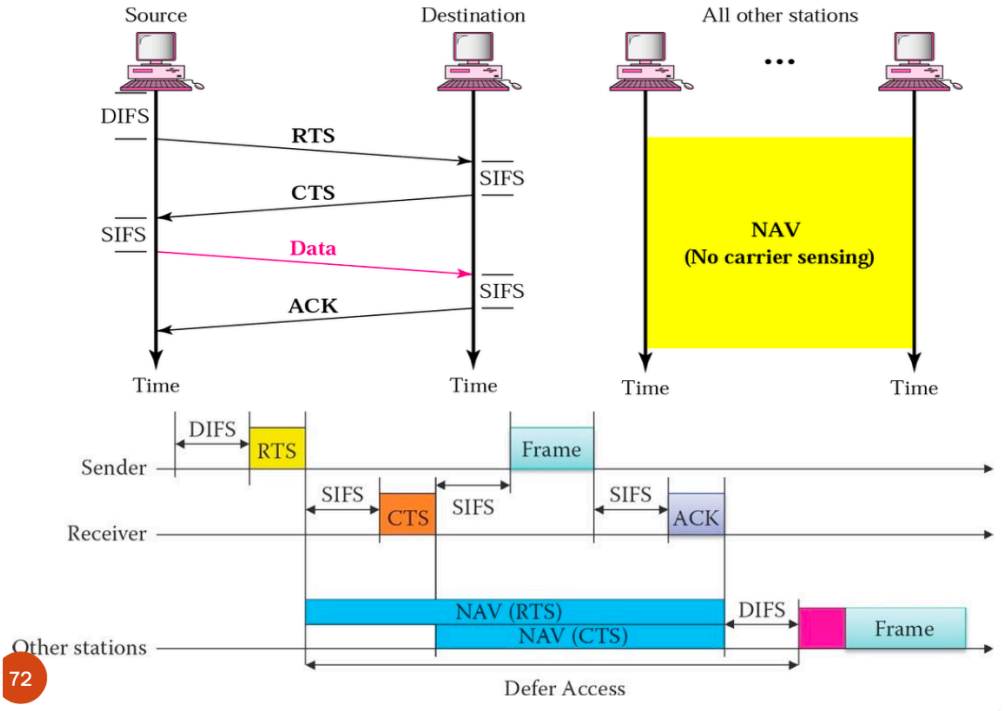
CW = 31, MS_A and MS_B are backoff intervals at nodes A and B

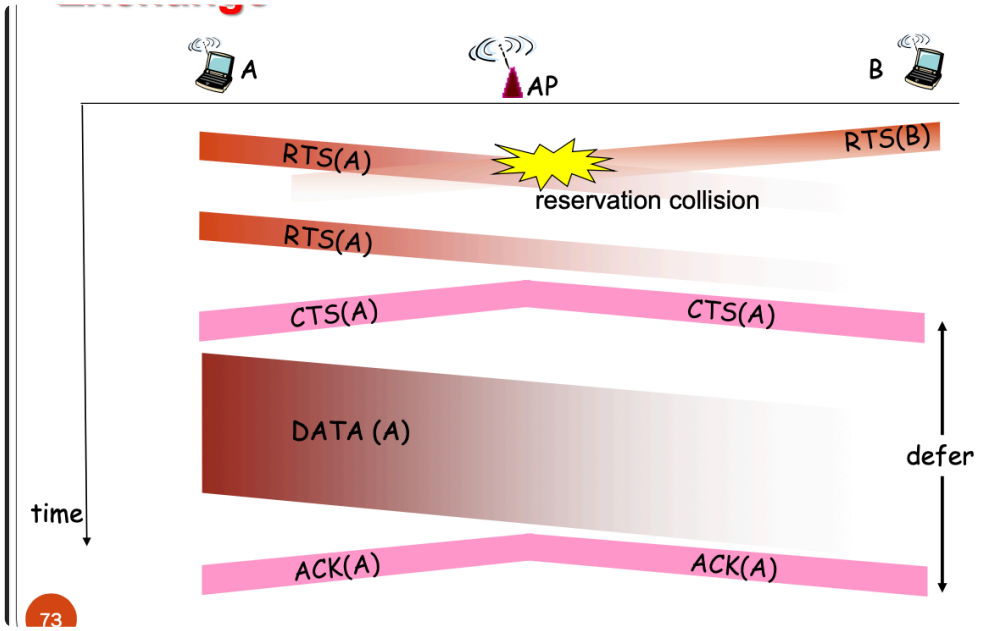
- We assume for this example that CW = 31
- MS_A and MS_B have chosen a backoff interval of 25 and 20, respectively
- MS_B will reach zero before five units of time earlier than MS_A
- When this happens, MS_A will notice that the medium became busy and freezes its back-off interval currently at 5
- As soon as the medium becomes idle again, MS_A resumes its backoff countdown and transmits its data once the backoff interval reaches zero



CSMA/CA with RTS/CTS

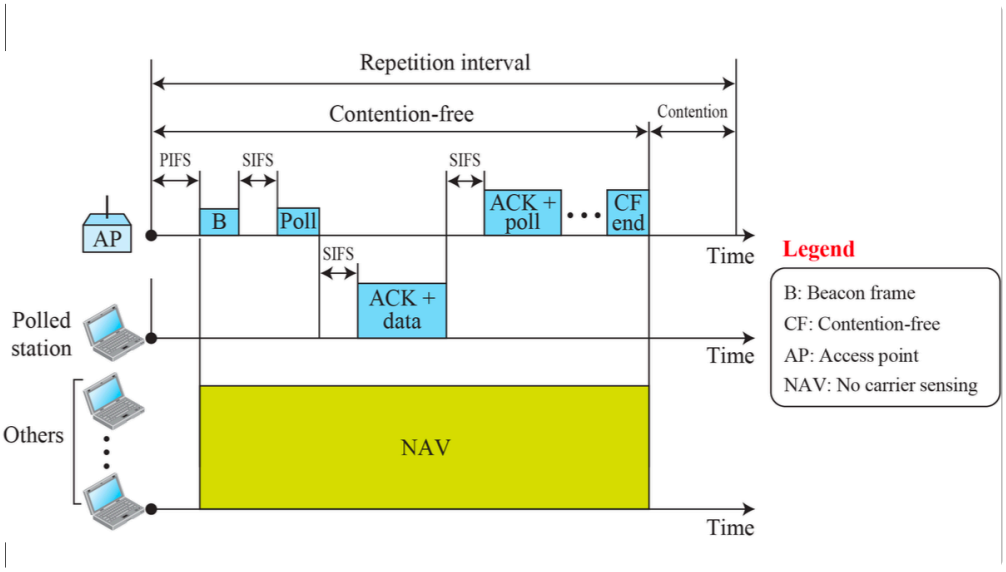
- **RTS (request to send)**
- Transmitter sends an RTS after medium has been idle for *time interval more than DIFS*
- **Receiver** responds with **CTS (clear to send)** after medium has been *idle for SIFS*
- Then Data is exchanged
- RTS/CTS is used for reserving channel for data transmission so that the collision can **only occur in control message**





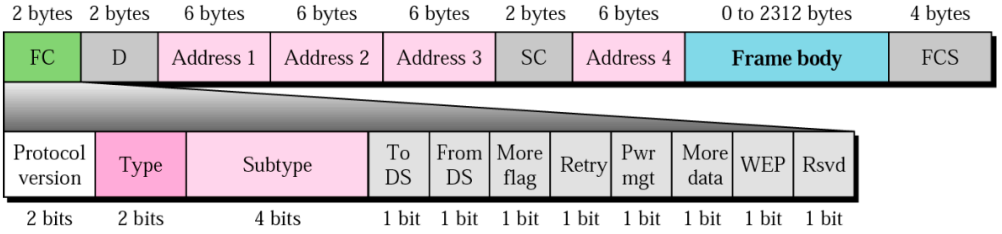
Point Coordination Function (PCF)

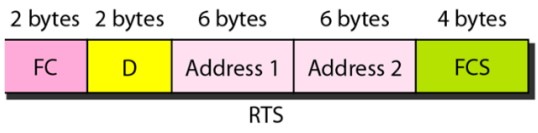
- **optional for an infrastructure network**
- **time-sensitive** transmission
- implement *on top of the DCF*
- **centralized, contention-free polling** access method
  - The *AP polls* stations that can be polled, *one station after another*
  - The polled station may send its data to the AP
- **Prioritize PCF over DCF**
  - *SIFS is the same as in DCF*
  - *PIFS is shorter than the DIFS*
  - An AP wanting to use *PCF is prioritized* over a station wanting to use only DCF
- Station only use DCF may not gain access to the medium
- **repetition interval**
  - repeated continuously
  - **contention-free CF** period
    - start with a *beacon frame* and ends with *CF end* frame
    - during which *NAV* applies to *all other station*
  - contention period to *allow the contention-based* station to use the medium

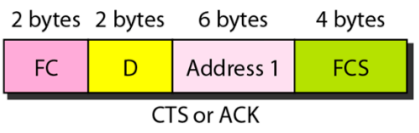


802.11 Frame Format

- **Frame Control FC** : type of the frame and control information
- **Duration D**: set the *value of the NAV*
- **Address**: *MAC address*
- **SC**: *Sequence control* (fragment number, sequence number)
- **Frame body**: information based on the frame type
- **Frame Check Sequence FCS** *CRC-32* error detection sequence







Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

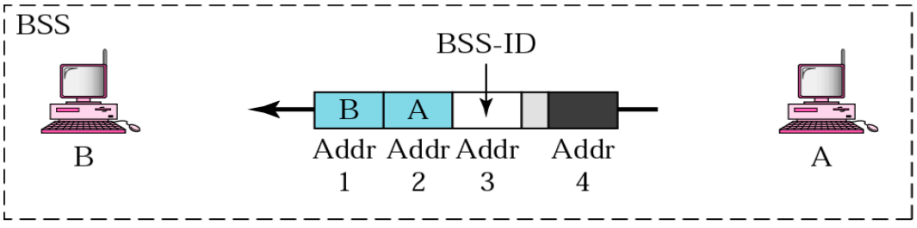
Frame Addressing

- **Four case to interpret the address** in the frame depending on to ds and from ds, in **FC** field

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

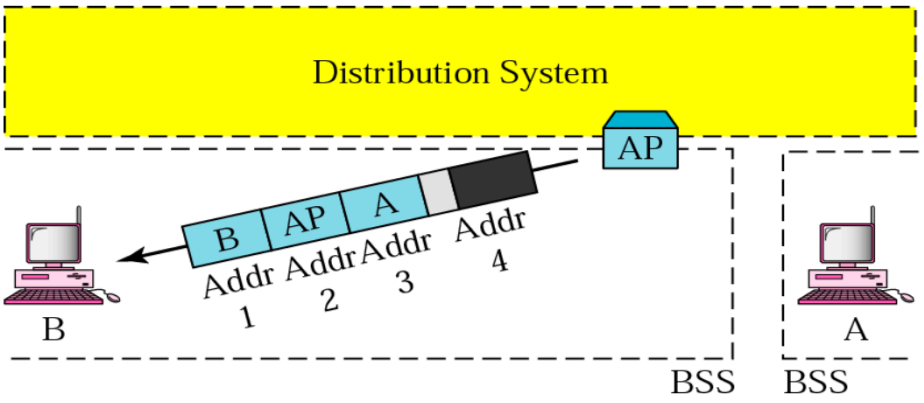
Addressing: Case 1

- To DS =0 and From DS=0
  - Not going to a distribution system
  - Not coming from a distribution system



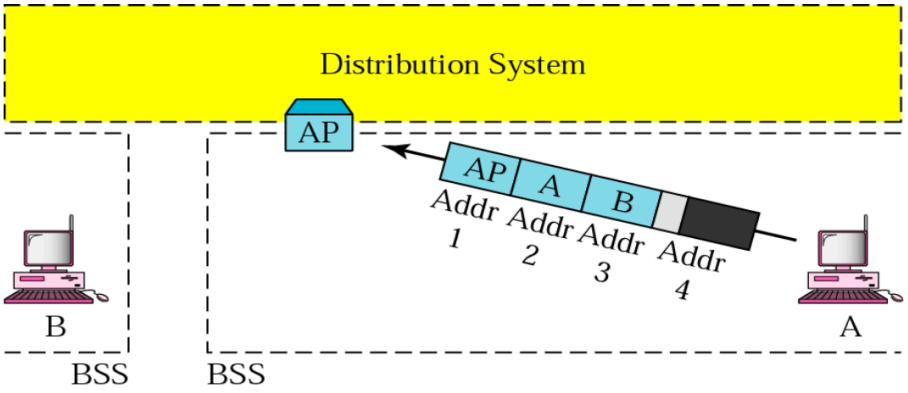
Addressing: Case 2

- To DS =0 and From DS=1
  - Not going to a distribution system
  - Coming from a distribution system



Addressing: Case 3

- To DS =1 and From DS=0
  - Going to a distribution system
  - Not coming from a distribution system



Addressing: Case 4

- To DS =1 and From DS=1
  - Going to a distribution system
  - Coming from a distribution system