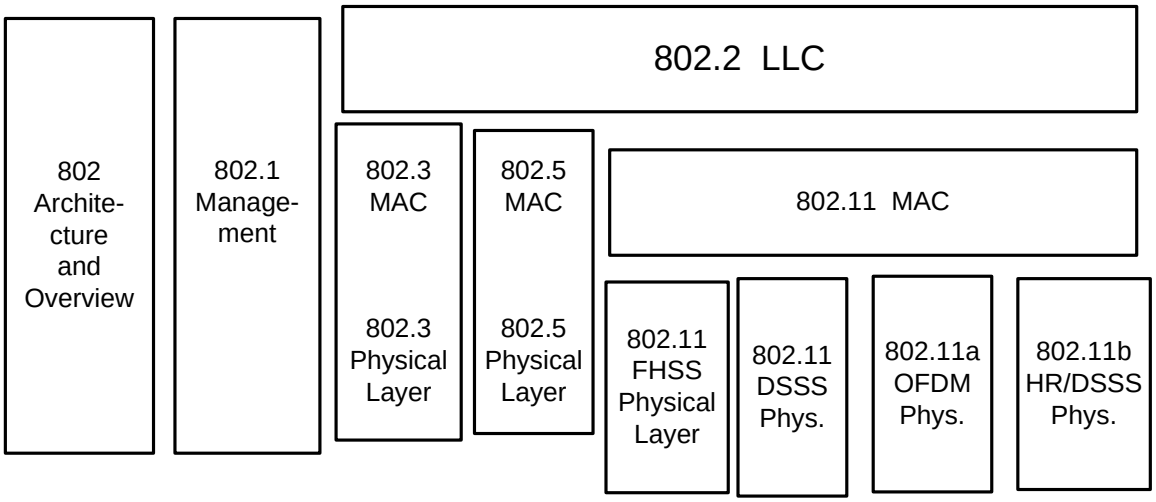
V.802.11 Wireless LAN

- **In wireless LAN, mobile stations use RF (Radio Frequency) link to communicate with each other**

IEEE 802 LAN Technology Family Tree



V.1.Backgrounds and Introduction

Radio Communication Fundamentals, An Introduction

- **Wireless LAN uses RF (radio frequency) signal to transmit digital information**
  - **RF signal is transmitted through wireless medium to the destination**
- **Relationship between Frequency and Wavelength of RF signal**

Frequency * Wavelength (aka Lamda) = C, the speed of light

- **C (Speed of Light), measured in meters per second, is a constant**
- **Frequency measured in Hz or cps (cycles per second) in the old days**
- **Wavelength measured in meters**

- **Frequency and wavelength are inversely proportional to one another**
- **The shorter the wavelength, or the higher the frequency, attenuation of RF signal is more severe**
- **The shorter the wavelength, it is easier for the RF signal to be reflected, focused and controlled**
  - **If freq > 300 MHz, RF signal can be easily focused by a parabolic reflector such as antenna**
- **Focusing a signal and directing it towards a destination means transmitting device requires far less power than if it were transmitting in all directions**
- **Usually higher frequency means higher data rate**
  - **Usually, 1 bps is encoded for 1Hz, but sometimes, more bits such as 4 bits may be encoded for 1 Hz**
  - **Assuming that a transmitter is encoding 1 bit per cycle, then the data rate for one with freq = 1 MHz should be 100 times faster than the one with freq = 10 KHz**

Overview of Wireless Communication

- In theory, wireless communication can operate anywhere in the frequency range of the electromagnetic (or e-m) wave spectrum - from 200 KHz all the way up to infrared frequency range of 200 THz (1000 MHz).
- Table 1 is a description of the e-m spectrum

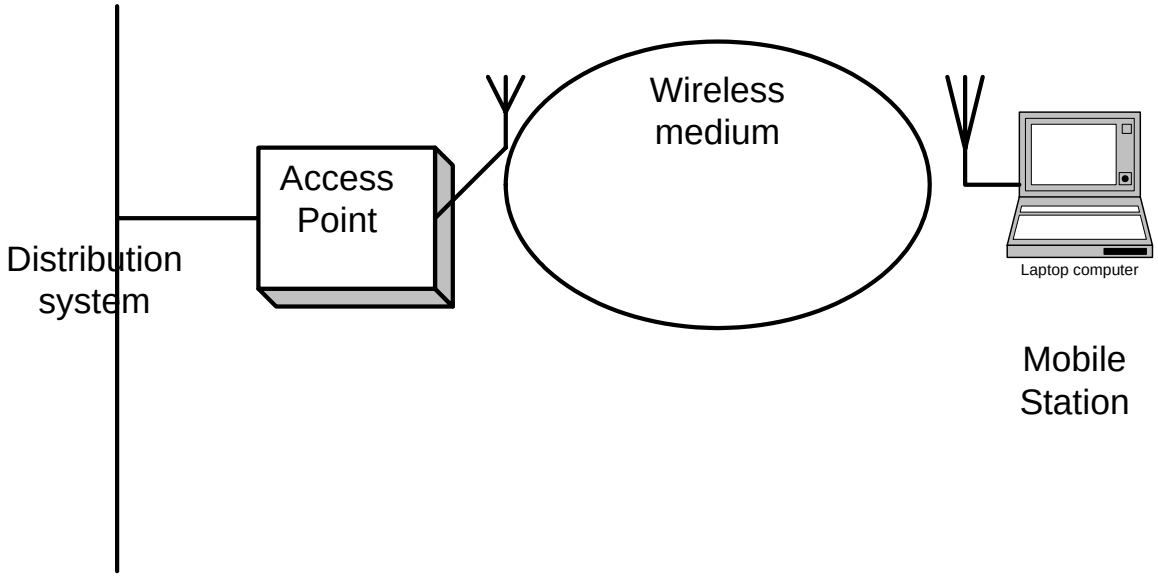
Table 1

	Freq. Range	Application
HF	10 ~ 100 MHz	– AM Broadcast – Radio Broadcast
VHF	100~1000 MHz	– TV Broadcast – FM radio Broadcast – Paging
UHF	1GHz ~ 10 GHz	– Cell Phones – Wireless LAN – Paging
Microwave	10 GHz ~2000 GHz	– Satellite Communication – Microwave – RADAR
Infrared	Over 2000 GHz	– Garage Door Operator – TV Control – Infrared Wireless LAN

Why the usages of the e-m wave spectrum need to be regulated and licensed?

- Uncontrolled uses would lead to chaotic communication
  - Two users using the same RF frequency to transmit the signal will cause interference of the RF signal, causing the message to be garbled
  - Critical and emergency messages cannot be received correctly; Potentially could lead to severe situations
- Every country, the government imposes some form of control on the usage of e-m spectrum through licensing or regulation
- For most of the industrial countries, there is a shortage of bandwidth and the entire e-m spectrum is over-subscribed
- The only exception is the ISM (Industrial, Scientific and Medical) Bands, no licensing is required
  - IEEE 802.11 Wireless LAN uses the ISM bands
  - 3 Bands in the ISM:
    - Lower band: 902 – 928 MHz
    - Middle band: 2.4 – 2.48 GHz
      - ▲Recognized all over the world for wireless LAN usage
    - Upper band: 5.7 – 5.85 GHz

802.11 Wireless LAN (WLAN) Components



Components of 802.11 LAN

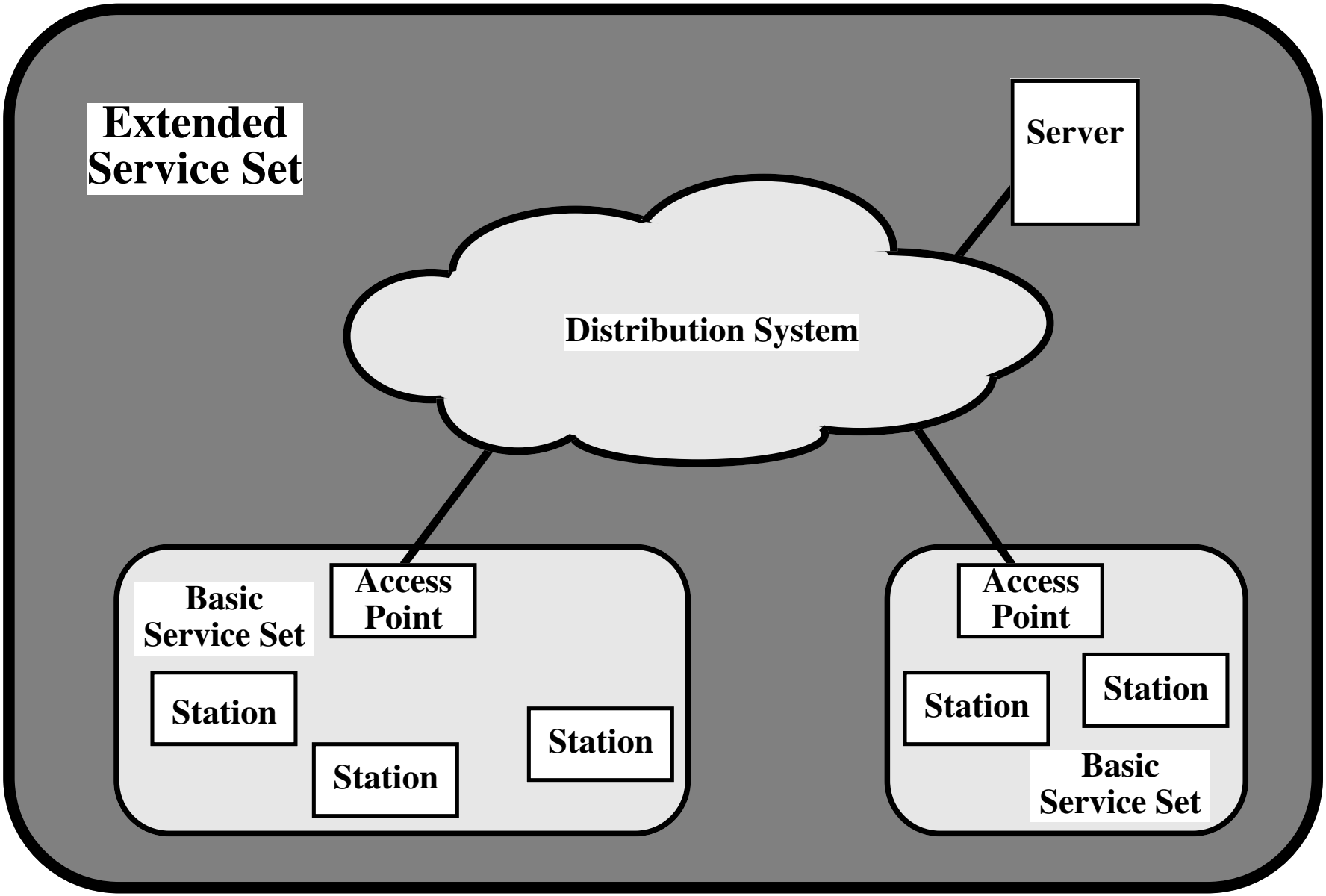


Figure 10.15 IEEE 802.11 Architecture

♦ 802.11 Nomenclature and Design

- **Distribution system (DS) – the logical component of 802.11 used to forward frames to their destination**
  - **For most commercial products, the DS is implemented as a combination of a bridging engine and a DS medium which is used to relay frames between APs (Access Points) or between APs and computing devices attached to the DS**
- **AP (Access Points) – perform the wireless-to-wired bridging function.**
  - **Two interfaces - one wireless network interface, the other, wired network interface, usually of type Ethernet/802.3 CSMA/CD**
  - **For infrastructure network, mobile stations can not communicate directly, must always go through AP**
- **Wireless Medium – initially two RF (Radio Frequency) and one IR (Infrared) physical layers were standardized by 802.11**
  - **IR, currently not popular and practically not used**
  - **FH (Frequency Hoping) RF layer, currently also not popular**
  - **At the moment, only the Direct Sequence RF layer is widely used**
- **Mobile stations or stations**
  - **Computing devices with wireless network interfaces**

Two types of networks in 802.11:

- **Ad-hoc network or Independent Basic Service Set (IBSS)**
  - **No AP existed, and mobile stations communicate directly with each other**
  - **Usually existed for a short period of time**
    - **Simplest case is one with only two mobile stations**
- **Infrastructure Network**
  - **Always with AP, and AP is attached to the DS (Distribution System)**
  - **No mobile stations (abbr. as stations) can communicate directly, must always go through AP**
  - **The area which is reachable by the RF signal from the AP defines the Basic Service Area**
  - **All the stations within the Basic Service Area and the AP forms a BSS**

What is Basic service Set (or BSS)?

- **Basic building block of an 802.11 network.**
- **For IBSS, two stations within the BSS can communicate directly with each other**
- **For infrastructure network, two stations within the BSS can communicate with each other indirectly through AP**
- **Each BSS is uniquely identified by a 48-bit binary integer called BSSID**

What is BSSID?

- **Each BSS is assigned a unique BSSID, a 48 bit binary integer that distinguishes it from other BSSs**
  - **Station uses BSSID for filtering of MAC frames from other BSS area**
  - **if BSSID does not match, then the MAC frame is filtered by MAC layer**
  - **Several distinct 802.11 network may overlap physically, BSSID prevents one network from receiving link-layer broadcast or multicast from a physically overlapping network**
  - **For infrastructure network, BSSID = MAC address of the wireless interface of the AP**
  - **In IBSSs, for each BSS created, a unique 48 bit binary random integer is created to represent the BSS**
- **Broadcast BSSID – the all-1 s BSSID is the broadcast BSSID**
  - **Frames that uses the broadcast BSSID pass through any BSSID filtering in the MAC**
  - **Used only when mobile stations try to locate a network by sending probe requests**
    - **For probe frames to detect the existence of a network, they must not be filtered by the BSSID filter**
    - **ProbeRequest is the only frame allowed to use the broadcast BSSID**

802.11 Wireless LAN provides the following network services

- Each of the services will be discussed in more details later on

Service	Description
Distribution	Service used for delivery of frame to destination
Integration	Frame delivery to an IEEE 802 LAN outside the WLAN
Association	Used to establish the AP which serves as the gateway to a particular mobile station
Reassociation i.e. roaming	When station is moved from one BSS to the other, reassociation is used to change from the old AP to a new AP
Disassociation	Removes the wireless Station from association from AP
Authentication	Establish identity prior to establishing association
Deauthentication	Used to terminate authentication, and by extension, association
Privacy	Provides protection against Eavesdropping
MSDU delivery	Delivers data to the recipient

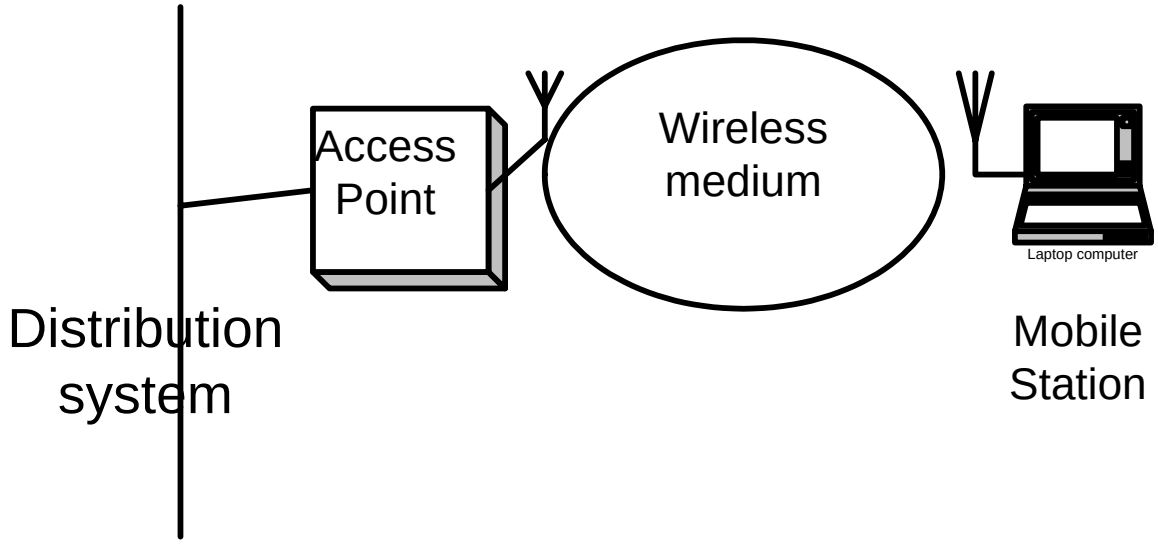
Independent BSS (IBSS)

In the simplest case, IBSS has only two mobile stations

Each IBSS is uniquely identified by a BSSID, a 48-bit random integer generated when the BSS is created.

Infrastructure Structure Network

-consists of at least one AP connected to the backbone distribution system

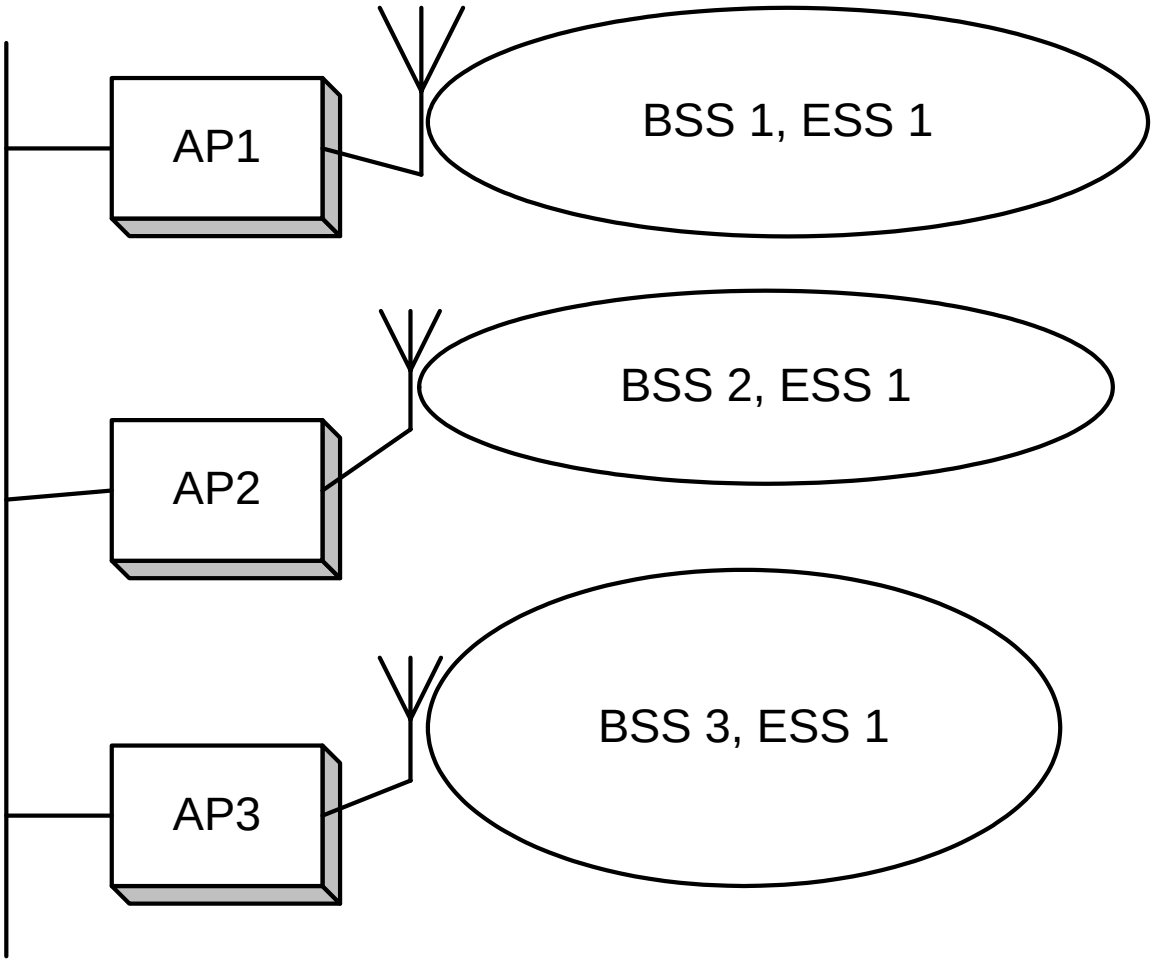


Components of 802.11 LAN

- **BSSID = MAC address of the wireless interface of the AP**
- **Area reachable by RF signal from AP defines the BSS area**

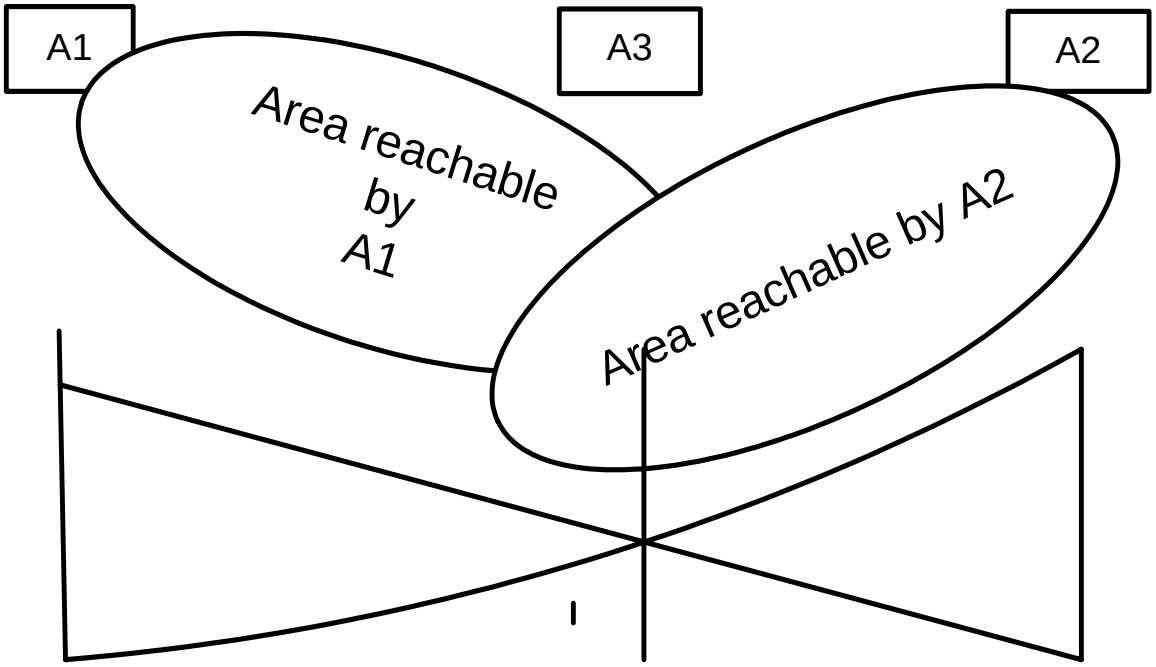
What is an ESS (Extended Service Set)?

- **Multiple BSSs chained together with the same DS**
  - **Each BSS is connected through an AP to the DS**
  - **For 802.11, the backbone network or DS is Ethernet-based network such as**
    10/100 Base T shared media, 10/100 Base T switch, Gigabit Ethernet switch and etc.



Extended Service Set

Hidden Node Problem with wireless LAN



- **The diagram shows A1 and A2 are in the hidden area of each other.**
  - **RF signal from A1 not detectable at A2, and vice versa.**
  - **A1 and A2, not aware that the other is transmitting**
- **A3 is within the area reachable by both A1 and A2.**
- **Signal as received by A3 from both A1 and A2 is garbled because of collision**

Why Collision Detection will not work?

- In RF link, transceiver is usually half duplex. To build full-duplex transceiver requires expensive electronics
- Stations A1 and A2 are each in the hidden areas of each other, they have no way to know that the other is transmitting
  - A1 and A2 potentially could simultaneously transmit and not aware of it
  - A1 and A2 do not know that collision occurred, however, RF signal as received by A3 is garbled because of the colliding of signals from the two sources

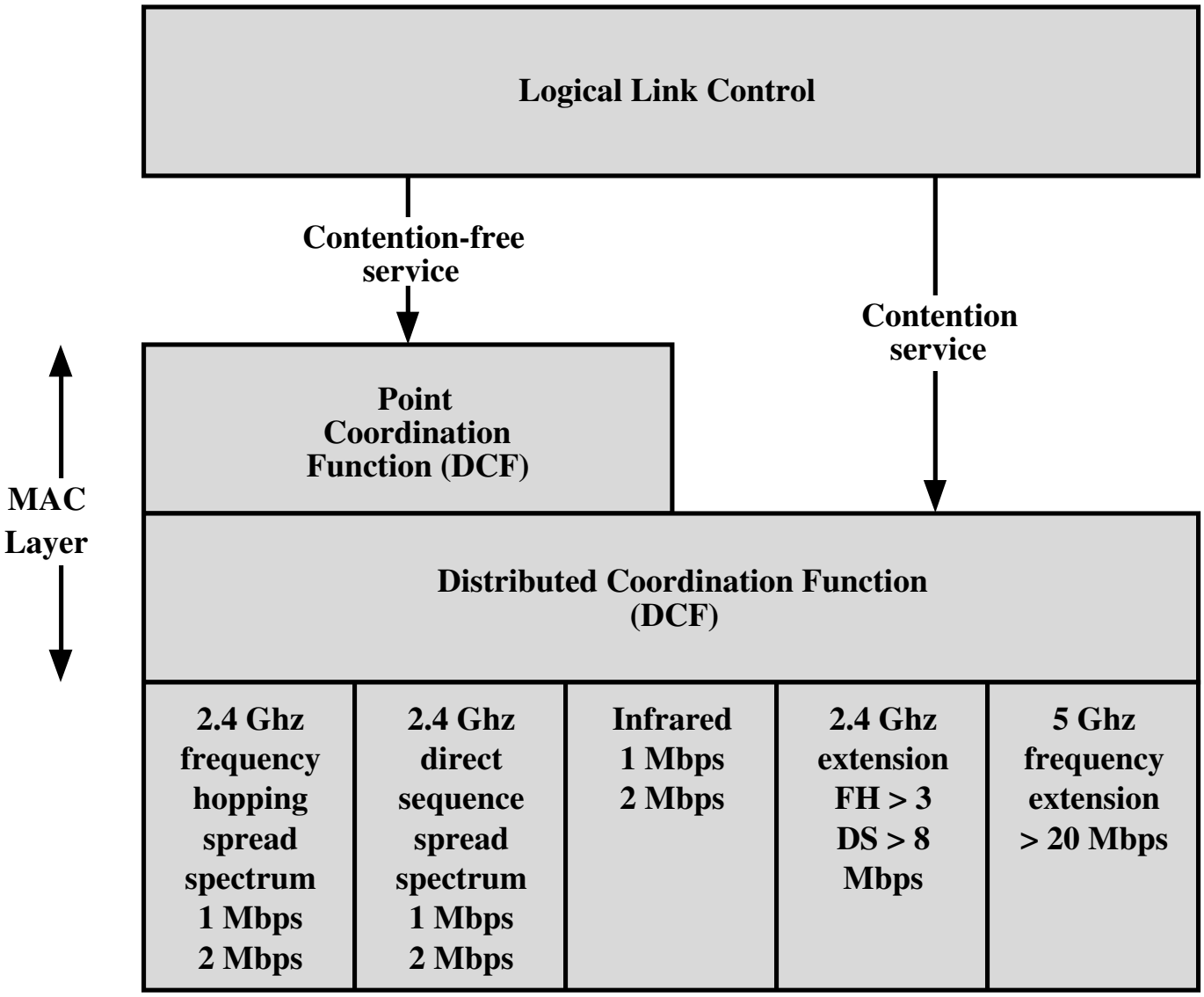


Figure 10.16 IEEE 802.11 Protocol Architecture

802.11 MAC Requirements

- **Single MAC to support multiple PHYs**
  - **Support single and multiple channel PHYs**
- **Allow overlap of multiple networks in the same area and channel space**
- **Robust for Interference**
  - **Microwave interferers**
  - **Other un-licensed spectrum users**
  - **Co-channel interference**
- **Provide mechanisms to deal with Hidden Nodes**
- **Provide for Time Bounded Services**
  - **Must also provide contention free service**
- **Provisions for Privacy and Access control**

Two types of carrier-sensing functions

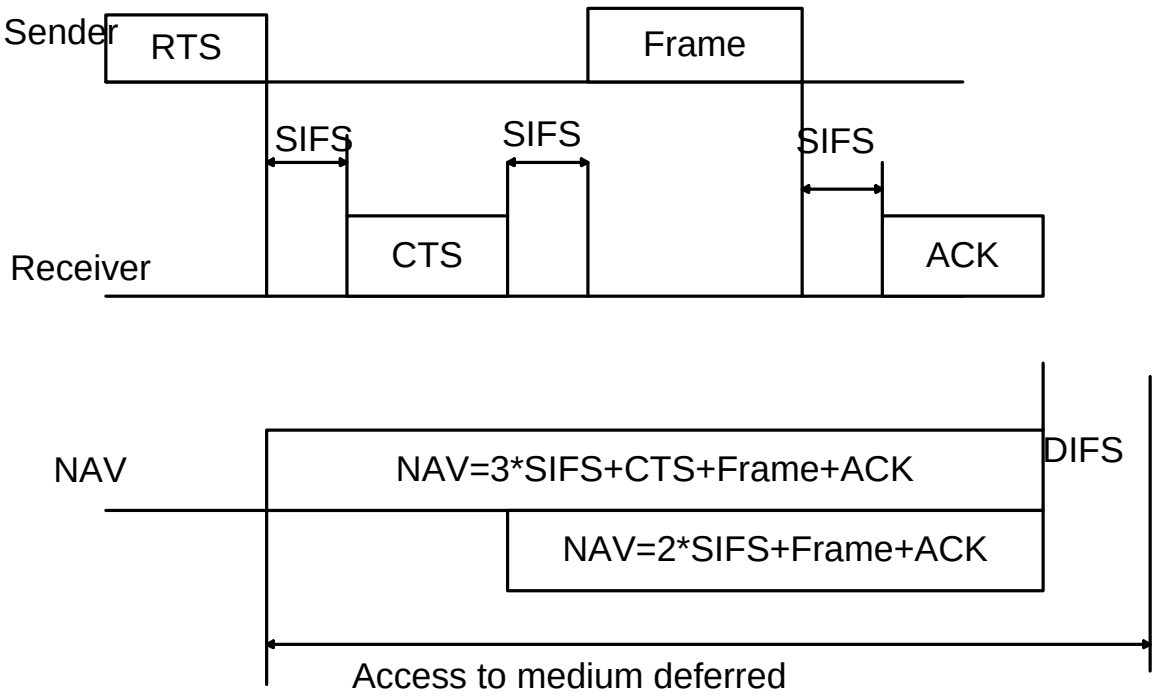
- **Physical Carrier-sensing : More difficult to implement in RF link environment**
  - **In RF link, transceiver is usually half-duplex. To build full-duplex transceiver requires expensive electronics**
- **Virtual carrier-sensing**
  - **Provided by a NAV (Network Access Vector).**
    - **NAV is a timer that reserves a period of time the RF medium is to be used**
    - **Value contained in the Duration field (2 bytes) of wireless MAC frame – MAC frame format to be shown later**
    - **Most of 802.11 frames carries a NAV i.e., data frames and control frames such as RTS,CTS and ACK, all carries a NAV value.**
    - **By using NAV, station can be sure that atomic operations such as RTS/CTS, data frame and ACK will not be interrupted.**

Hidden Node Problem

- **Collision detection difficult in wireless LAN because of:**
  - **hidden nodes problem**
  - **wireless transceivers are generally half-duplex**
- **Stations in 802.11 usually use RTS and CTS signals to clear out an area before the transmission of data frames**
- **When RTS is sent, the sender also reserves the RF medium for a time period 3*SIFS+CTS+Data +ACK to ensure that the atomic operation of RTS,CTS,Data and ACK not going to be interrupted.**
- **CTS reserves the RF medium for a time period 2*SIFS + Data + ACK**

Table. NAV value for different types of frames

Frame type	NAV
RTS	3*SIFS+CTS+Data Frame+ACK
CTS	2*SIFS+Frame+ACK
Data Frame (if last or only) segment	SIFS+ACK
Data Frame (if not last segment)	3*SIFS + 2*ACK + fragment
ACK	0



Using the NAV for virtual carrier sensing

Basic Access Protocol Features

- **Use Distributed Coordination Function (DCF) for efficient medium sharing without overlap restrictions**
  - **Use CSMA with Collision Avoidance derivative**
- **Use ACK to ensure robust for interference**
  - **CSMA/CA + ACK for unicast frames, with MAC level recovery**
  - **CSMA/CA for Broadcast and multicast frames**
- **Use RTS/CTS to provide Virtual Carrier Sense function to protect against Hidden Nodes**
  - **Duration information is distributed by both transmitter and receiver through separate RTS and CTS Control Frames**
- **MAC frame formats supporting the following 3 types of networks or access schemes**
  - **Infrastructure network**
  - **Ad-Hoc network or IBSS**
  - **WDS (Wireless Distribution System)**

♦ Why CSMA/CA + ACK?

- **In a wired link such as Ethernet, it is reasonable to assume that the transmitted frame will reach the destination correctly**
- **In RF link, esp. in the unlicensed ISM bands, because of the existence of other unlicensed devices such as microwave ovens and other power generating equipments, all transmissions are likely subjected to interferences**
- **Data transmissions in 802.11 always require acknowledgements**
  - **Sender is responsible for performing error recovery**
  - ***For every transmitted data frame, if it is unicast, ACK is always required***
    - * ***if*** **no ACK received within time out period, sender assume it is lost and retransmit the data frame**

♦ MAC Access Modes

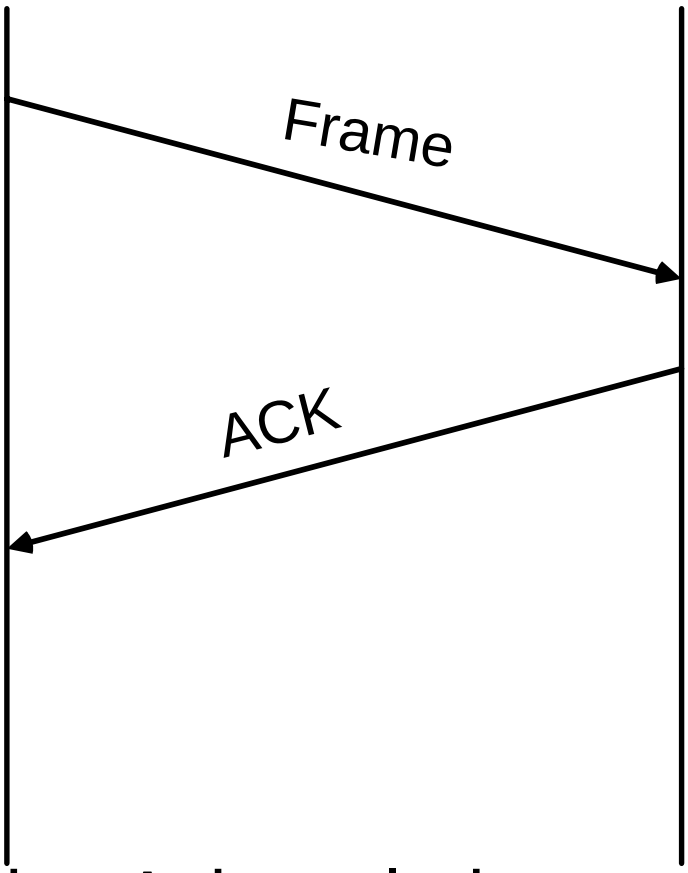
- **Normal delivery services - provided by DCF**
  - **access to wireless medium is controlled by a coordination function, an Ethernet-like CSMA/CA (collision avoidance) called DCF (distributed coordination function)**
- **Contention-free (CF) services - provided by PCF (Point Coordination Function) and built on top of DCF**
  - **Make provisions for Time Bounded Services**
  - **Few products (if any) implements PCF**
  - **CF service is provided by AP**
  - **The concept of PCF not to be covered in CS771**

CSMA/CA Explained

- **Reduce collision probability where mostly needed**
  - **Stations waiting for medium to become free or idle**
  - **If busy, defer and then select Random backoff after a Defer, resolving contention to avoid collisions**
- **Exponential Backoff algorithm stable at high loads**
  - **Exponential Backoff window increases for retransmissions**
- **Implement different fixed priority levels**
  - **Allow coexistence of both immediate response and contention free service which is PCF (Point Coordinating Function)**
  - **Four IFS (Interframe space) are defined i.e.,**
    - **SIFS, PIFS, DIFS and EIFS with SIFS the shortest, EIFS, the longest**
    - **SIFS < PIFS < DIFS < EIFS**
    - **Frame with the shortest IFS represents the highest priority**
  - **PIFS is used for CF-services**
    - **Few products if any implemented CF-services**
      - **Most traffics uses DCF which provides Ethernet or CSMA/CD like contention-based service**

♦ CSMA/CA + ACK protocol

- **Defer access based on Carrier Sense**
  - **Physical carrier sense and Virtual Carrier sense**
- **Direct access when medium is sensed free longer than DIFS, otherwise defer and Backoff**
- **Receiver of unicast frame to return ACK immediately if CRC correct**
  - **When no ACK received within timeout period, sender retransmits frame (up to maximum limit)**
  - **Data delivery and ACK are considered as a single atomic exchange**
  - **For broadcast/multicast frames, no ACK is required**



Positive Acknowledgement of data transmission

Wireless LAN MAC Scheme

Step1).A station with frame to transmit, first listen to the medium

- **If medium is idle, and stays on idle for longer than the DIFS period, transmit immediately else go to step 2.**
- **When finished go to step 4 .**

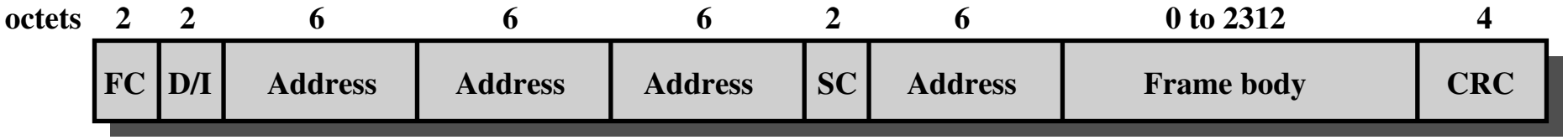
Step 2). Medium is busy

- **Defer and waits for the medium to become idle longer than DIFS and go to step 3 for random backoff else go to step 1 and start all over again**

Step3. Compute random backoff time.

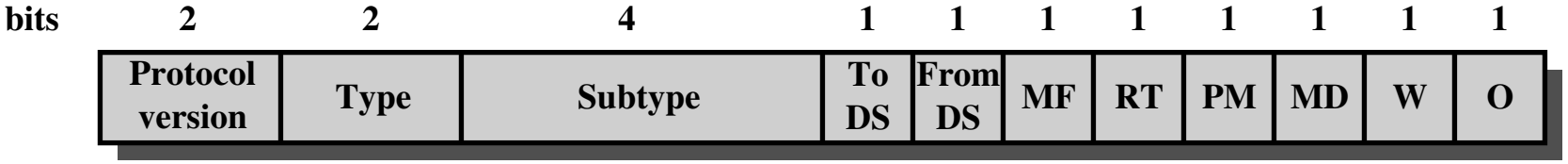
- **similar to 802.3 CSMA/CD Binary Exponential Back-off Scheme**
- **If media is still idle additionally for backoff time, transmit immediately else go to step 1 and start all over again**

Step 4. Process complete



FC = Frame control
D/I = Duration/Connection ID
SC = Sequence control

(a) MAC frame



DS = Distribution system
MF = More fragments
RT = Retry
PM = Power management
MD = More data
W = Wired equivalent privacy bit
O = Order

(b) Frame control field

Figure 10.18 IEEE 802.11 MAC Frame Format

802.11 MAC Frame Format (Cont.)

- **MAC header format differs for the following 3 types of frame**
  - **Control frames (several fields are omitted)**
  - **Management frames**
  - **Data frames**
- **FC (Frame Control) – 2 bytes**
  - **Version (2 bits) - only one version i.e. 00, is specified by 802.11**
  - **Type (2 bits) - 00 – Management, 01 – control, 10 – Data Frames**
  - **Sub Type or Stype (4 bits) - to specify a special frame type such as RTS, CTS, ACK, PS-POLL, Probe Request/Response, Authentication Request/Response and etc.**
  - **ToDS (1 bit) - ToDS = 1 if AP is the receiver**
  - **FromDS (1 bit) - FromDS = 1 if AP is the transmitter**
  - **MoreFrag (1 bit)**
  - **Retry (1 bit)**
  - **WEP (1 bit)**
    - **If WEP = 1, then the frame is a WEP frame and WEP (wired equivalent privacy) scheme is implemented**
  - **PwrMgmt or (PM) - 1 bit.**
    - **If PM =1, then the mobile station is in power saving mode**
  - **Order - 1 bit**

802.11 MAC Frame Format Cont.

- **Duration or DUR/AID – 2 bytes.**
  - **For most of the frames, DUR = NAV (Network Allocation Vector), i.e. access to the medium is restricted during the time as specified in NAV**
  - **For broadcast/multicast frame, DUR = 0**
  - **For some frames, DUR/AID means AID (association ID)**
    - **After a station becomes associated with an AP, the AP assigns an AID which is an integer between 1 and 2007 to the station**
    - **When a mobile station waked-up from dozing mode, it send PS-POLL to request for buffered frames. The PS-POLL must give the mobile station's AID number**
- **Address - 4 MAC addresses, each is 6 bytes long, same as 802.3 CSMA/CD MAC address**
- **SC (Sequence Control) – 2 bytes, for fragment control and for filtering of duplicate caused by ACK mechnism**
- **Framebody - variable length frame body**
- **FCS - 4 bytes, same as FCS in 802.3 MAC frame**

Association ID (AID)

In the PS-POLL frame, the DUR/AID field is an association ID rather than a value which is NAV. When mobile stations becomes associated with an AP, the AP assigns a value called AID from the range of 1 to 2007.

Address Field Description

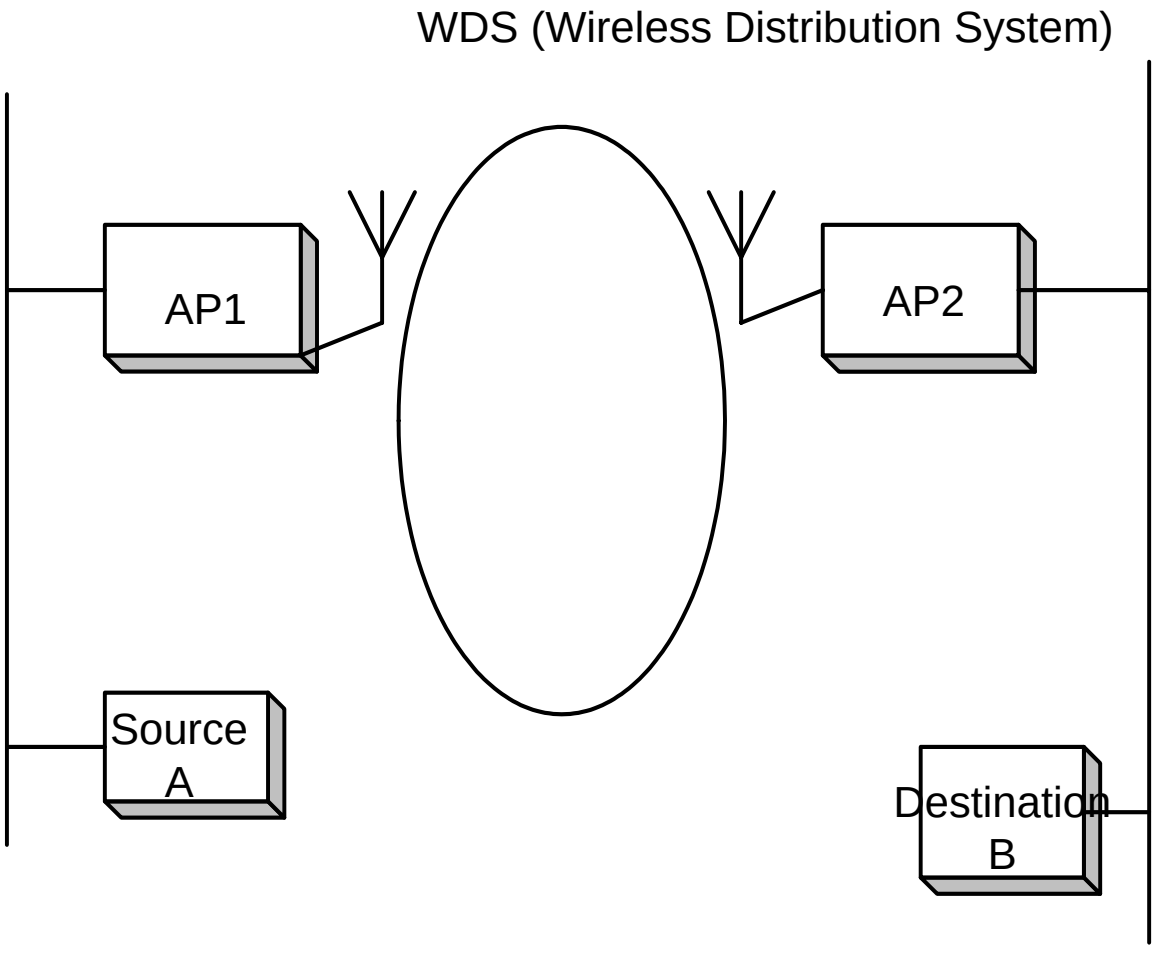
- **Adr1, the Receiver Address (RA) = All stations filter on this address**
  - **If adr1 = bc or mc, then BSSID is also checked**
    - ∗ **stations respond only to broadcast and multicasts originating in the same basic service set (BSS)**
    - ∗ **bc or mc from other BSS area are filtered**
- **Adr2, the transmitter address (TA)**
  - **Identifies transmitter so that the receiver can send the ACK frame to**
- **Adr3 = Dependent on the 2 bits ToDS and FromDS**
- **Adr4 = Only needed to identify the original source of WDS frames**

To DS	From DS	Adr1	Adr2	Adr3	Adr4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Note:

ToDS	FromDS	Meaning
0	0	IBSS network, no AP involved, 3 addresses used
0	1	Sent from AP to station, 3 addresses used
1	0	Sent to AP, 3 addresses used
1	1	WDS mode, 4 addresses used

In the WDS as shown in the following, to send a frame from Source A to destination B, the communication path must go through two access point AP1 and AP2. The wireless MAC frame from AP1 to AP2, the 4 addresses are:
Adr1= AP2, Adr2 = AP1, Adr3 = DA = B,
Adr4 = SA = A



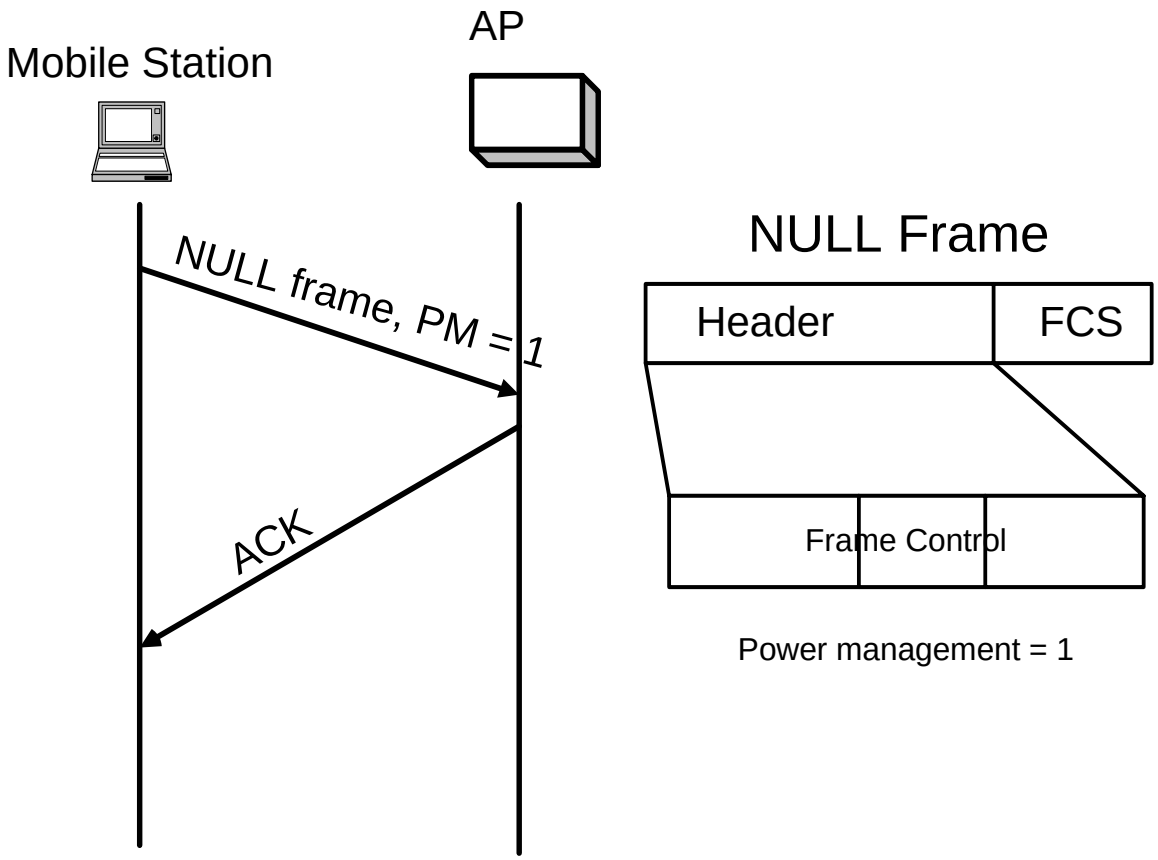
Three types of frames in 802.11

- **Data Frames –**
  - **Upper layer packet is encapsulated into data frame**
- **the pack horses of 802.11 for hauling data from station to station**
- **Control Frames – RTS, CTS, ACK and PS-POLL**
- **Management Frames – handles how a station joins a wireless network**

Type (2 bits)	Subtype (4 bits)
Data	Data
	Data+CF-Ack
	Data+CF-poll
	Data+CF-Ack+CF-Poll
	Null
	CF-Ack
	CF-Poll
	CF-Ack+CF-Poll
Control	RTS
	CTS
	ACK
	PS-POLL
Management	Beacon
	Probe Request/Response
	Disassociation Request/Response
	AuthenticationRequest/Response
	DisauthenticationRequest/Response
	AssociationRequest/Response

What is Data Frame?

- **Used to transfer data from one station to the other**
  - **In contention-free period, data frames may be used to acknowledge other frames, saving the overhead of interframe spaces and separate ack**
    - **Example:**
      - **Data+CF-Ack, Data+CF-poll, Data+CF-Ack+CF-Poll**
  - **NULL frame –**
    - **A special type of data frame which contains no data to inform the AP about its power management status**
    - **consisted of a MAC header followed by the FCS trailer**
    - **If PM = 1, then station enters dozing state and AP starts to buffer the frames targeted at the mobile station**



After receiving NULL frame with PM=1, AP starts to buffer the frames for MS.

IBSS Data frames

- Always 3 addresses – adr1 (RA) = DA, adr2 (TA) = SA, adr3 = BSSID and ToDS = FromDS = 0
  - For broadcast or multicast, the receiver always checks the BSSID, and passes only frames that matches the current BSSID to higher protocol layers.

Infrastructure Data Frames

- Either FromDS or ToDS must be 1
- Always 3 addresses
- FromDS =1 means the MAC frame is sent to mobile station from AP
- ToDS =1 means MAC frame is sent to AP from mobile station

FromDS	ToDS	Adr1	Adr2	Adr3
1	0	DA/RA	BSSID/TA	SA, creator of the MAC frame
0	1	BSSID	TA/SA	DA, actual destination of the MAC frame

- Frames using WEP
  - If WEP =1 in FC, then the frames are protected by WEP, not a new frame type.
  - Frame body field begins with the WEP header (see 802.11 security)
  - More details to be discussed later in 802.11 Security

Control Frames

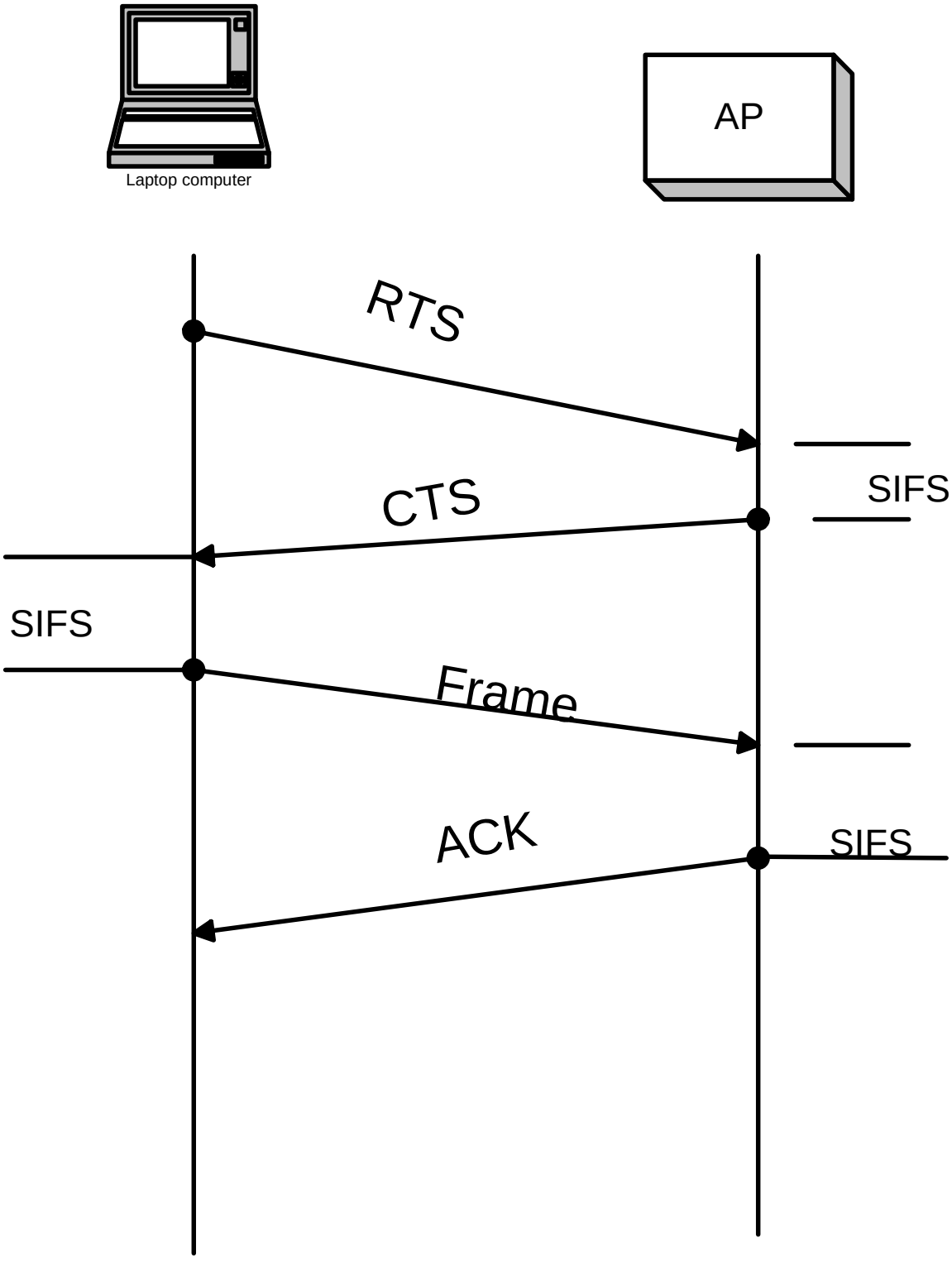
- 4 control frames i.e., RTS, CTS, ACK and PS-POLL
- Require one or two MAC addresses
- FC
  - Protocol – 00
  - Type – control or 10
  - Sub Type – indicates the type of control frames
  - More Frag (MF) – not fragmented, and always 0
  - Retry – always 0
  - PM – indicates the power management state of the sender after the conclusion of the current frame exchange
  - More Data (MD) – More data bit only used with management and data frames, always 0
  - WEP – always 0
  - Order - always 0

- Relationship between NAV and Control Frames
  - For control frames RTS,CTS and ACK, DUR/AID always means NAV value
    * Except for the target, all the receivers set timer = NAV value
    * Until the timer reaches 0, the station is not allowed to access the RF medium
  - For PS-POLL, DUR/AID always means AID having a value between 1 and 2007.

Control Frames

- **RTS – RTS and CTS together are considered as a single atomic exchanges**
  - **Requires 2 addresses i.e. Adr1= RA (Receiver Address), and Adr2 = TA (Transmitter Address)**
- **CTS – requires only 1 address i.e., RA**
- **ACK - requires only 1 address i.e., RA**
  - **If MoreFrag = 0, either a complete frame or the final fragment is transmitted, set DUR = 0; No need to reserve the medium for further usage**
  - **If MoreFrag = 1, the NAV value as specified in DUR is the same as CTS**

- **PS-POLL**
  - **station in power-saving mode, either in active mode or in dozing or sleeping mode.**
  - **Station in sleeping mode, periodically waked up to listen to Beacon frame**
    - **IF TIM (Traffic Identification Map) in the Beacon Frame indicates that frames are buffered, station sends PS-POLL to request for the buffered frames**
    - **For details, see discussion on 802.11 MAC Management frame**
  - **Only 2 address fields are used, adr1 = BSSID (MAC addr of the AP), Adr2 = TA or address of the mobile station**
  - **For PS-POLL, DUR/AID always means AID (association ID) value**
    - **AID value is between 1 and 2007**


Laptop computer
AP
RTS
CTS
SIFS
SIFS
Frame
ACK
SIFS

MAC Management Layer

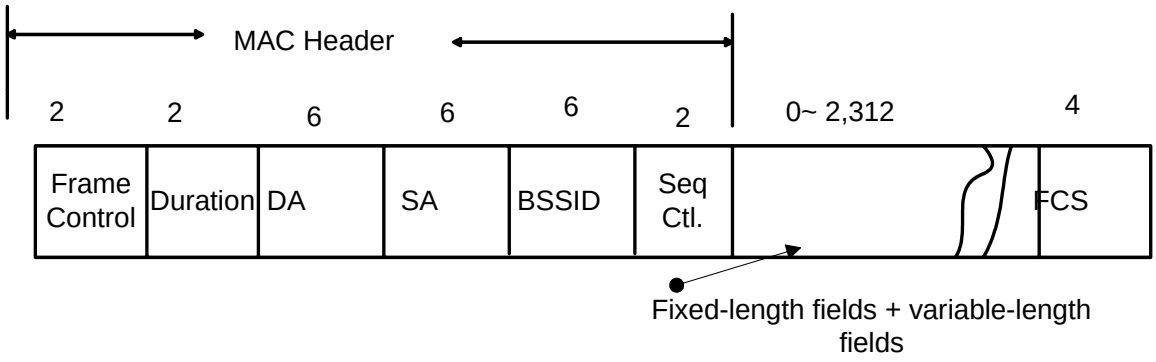
- **Synchronization**
  - **Time Synchronization Function (TSF) – Beacon carries a Timestamp, which is used to synchronize all the clocks within the BSS**
  - **Beacon Generation**
- **Power Management**
  - **Allows stations sleeping without missing any messages**
  - **Power Management functions - 802.11 allows station to enter periodic sleep without losing any messages**
    - **If transceiver is off, station is sleeping or dozing**
    - **if transceiver is on, station is awake or active**
    - **If station is sleeping, AP frame buffers the frames for the sleeping stations**
    - **AP periodically sends out Beacon signals**
      - **TSF – Timestamp in the Beacon frame is used to synchronize all the clocks within the BSS**
      - **Traffic Indication MAP (TIM) contains information about status of buffered frames for mobile stations**
- **Association - Before a station joins the network, it must first become associated with an AP**
- **Reassociation – When a station is moved to a different BSS, it must become reassociated with a new AP**

Synchronization in 802.11

- **Timing Synchronization Function (TSF)**
  - **Beacon frame contains a timestamp which is used to calibrate all the local clocks within the BSS**
  - **All station timers in BSS are synchronized**
- **Used for Power Management**
  - **Beacons sent at well known intervals called Beacon-interval**
  - **Listen-interval = multiple of Beacon-intervals i.e., N*Beacon-interval, where N = an integer**
    - **At listen-interval, station waked up to listen to Beacon frames**
    - **If TIM in the Beacon signal indicates that frames are buffered for the mobile station, station issue PS-POLL to retrieve the buffered frames from AP**
- **Used for Point Coordination Timing**
  - **TSF Timer used to predict start of Contention Free burst**
  - **Currently, PCF is not implemented in any 802.11 products**
- **If FH (Frequency Hopping) PHY is to be used, then all the timers within the BSS must also be synchronized**
  - **FH PHY or FHSS (Frequency Hopping Spread Spectrum) currently not used**
  - **TSF Timer used to time Dwell interval**
  - **All stations are synchronized, so they hop at same time**

How to maintain Synchronization?

- All stations maintain a local timer
- Timing Synchronization Function
  - Keeps timers from all stations in synch
  - AP control timing in infrastructure networks
  - Distributed function for IBSS (Independent BSS)
    - Not to be discussed in CS771
- Timing conveyed by periodic Beacon transmissions
  - Beacons contain Timestamp for the entire BSS
  - Timestamp used to calibrate local clocks
    - Not required to hear every Beacon to stay in synch



Generic Management Frame

♦ Management Frame Format

Management frame consists of the following fields:

- **FC (Frame Control) : 2 bytes**
- **DUR : 2 bytes**
- **Adr1: 6 bytes, RA (receiver address)**
- **Adr2: 6 bytes, TA (transmitter address)**
- **Adr3: 6 bytes, BSSID i.e., AP address**
  - **If BSSID = broadcast BSSID, then any stations can receive the frame**
  - **Otherwise, only the wireless stations that matches the BSSID receives the MAC frame**
- **Frame body – Most of the data contained in the frame body uses fixed-length fields (often referred to as fixed fields), and variable-length fields called elements.**
  - **Element is tagged with a type number and size, followed by information**
  - **If element not supported by 802.11 device, it just simply ignored**

Fixed-length fields

- **Authentication Algorithm Number (16 bits)**

Value	Meaning
0	Open system authentication
1	Shared –key authentication
2 ~ 65,535	reserved

- **Authentication Transaction Sequence Number (16 bits)**
  - **Authentication is a multistep process that consists of a challenge from the AP and a Response from the mobile station attempting to associate**
  - **The 2-byte sequence number is used to keep track of the progress in the authentication exchange**
- **Beacon interval (16 bits)**
  - **Number of time units (TUs) between beacon transmissions, each TU = 1024 microseconds**
  - **Usually, 10 beacon per second or 0.1 second**
- **Capability Information (16 bits)**
  - **Used in Beacon transmissions to advertise the network's capabilities**
- **Current AP address (48 bits)**
- **Listen Interval (16 bits)**
  - **Number of Beacon intervals that stations wait between listening for Beacon frames**
  - **Allow mobile stations to indicate how long the AP must retain buffered frames**
- **Association ID (16 bits)**
  - **Range between 1 ~ 2007**
- **Timestamp (64 bits)**
  - **Allow synchronizations in a BSS**

Management Frames

- **BEACON**
  - **Transmitted at regular intervals i.e., Beacon-interval, to announce the existence of a network**
  - **Allow mobile stations to find and identify a network as well as match parameters for joining the network**
  - **Consists of Timestamp, Beacon Interval, Capability information, SSID, and other IE's (information elements) such as TIM**
  - **Timestamp is for the synchronization of all the clocks in a BSS**
  - **TIM indicates which stations have buffered traffic waiting to be picked up**
- **Probe Request**
  - **Mobile station is in power-saving mode may not be able to transmit Probe Request**
  - **Mobile station uses Probe Request to scan an area for existing 802.11 networks**
  - **A Probe Request contain 2 fields:**
    - **SSID (Service Set ID), aka network name**
    - **Supported data rates**
  - **If infrastructure mode, AP uses the two fields to determine whether the mobile station can join the network**
  - **If SSID matches the AP's SSID, and supported data rates matches the network requirement, then AP send Probe Response**

Management Frames Cont.

- **Probe Response**
  - **If SSID matches the AP's SSID, and supported data rates matches the network requirement, then AP send Probe Response indicating success**
- **Authentication request/response –**
  - **Before a mobile station can become associated with a network, it must 1st authenticated to the network**
  - **In infrastructure network, mobile station to become authenticated to the network, it must 1st send Authenticate Request to the access point, and receive a successful Authentication Response**
- **Association request/Response -**
  - **Mobile station must 1st become associated with the network before it can send any data to the distribution system**
    - **Similar to plug the wire into a wired LAN network**
  - **In the association request, station also proposes listen-interval i.e., the period that it will wake-up to listen to Beacon frames**
  - **If the Association Response is successful, station formally joins the network**
- **Disassociation request – used to end an association relationship**
- **Disauthentication request – used to end an authentication relationship**

Management Frames Cont.

- **Reassociation Request/Response –**
  - station moving from one BSS area to the other within the same ESS
    is required to reassociate with the network before using the distribution system
  - ReassociationRequst contains a parameter which is the address of current AP
  - ReassociationRequest/Response allows the newly associated AP to request the original (or old) AP to transfer all the buffered frames to the newly associated AP and assigns a new AID to the mobile station

Scanning

- Scanning required for many functions
  - Finding and joining a network
  - Finding a new AP while roaming
- 802.11 MAC uses a common mechanism for all PHY
  - single or multi channel
- Passive Scanning
  - Find networks simply by listening for Beacons
- Active Scanning
  - On each channel, station sends out Probe Request, wait for Probe Response
- Beacon or Probe Response contains information necessary to join new network

To join an wireless network, mobile station must go
through the following 3 phases of activities

- **Scan for a network**
- **Authenticated to the network**
- **Associate with the network**
  - **After the 3 phases are completed, station is allowed to send traffic to the distribution system**

♦ 3 phases of active scanning for joining a network

- **Phase 1 Probe Request/Response**
  - **A mobile station in power-saving mode may skip this phase only by listening the BEACON frames**
- **Phase 2 Authentication Request/Response**
- **Phase 3 Association Request/Response**
  - **A mobile station joins a BSS after receiving a success Association Response**

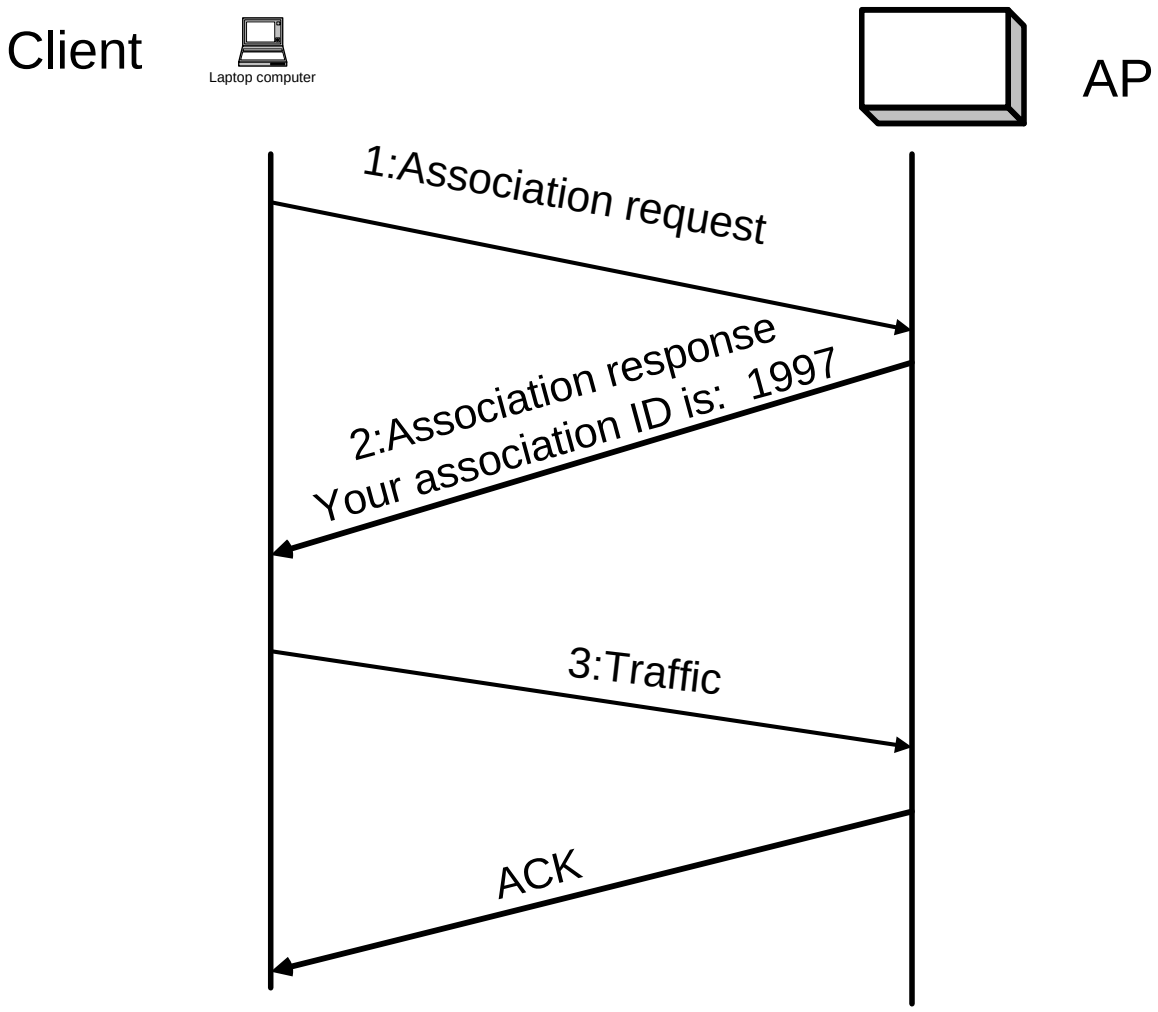
Authentication - 802.11 specifies two types of authentications

i.e., Open-system Authentication and Shared-Key Authentication

- **Details to be discussed in the section on 802.11 Security**

Association – once authenticated, stations can associate with the access point (or reassociate with a new AP) to gain full access to the network

- **Equivalent to plug the wire to the wired Ethernet Hub/Switch**
- **A record-keeping procedure that allows the DS (Distribution System) to keep track of the location of each mobile station , so frames destined for them can be forwarded to the correct AP**
- **Once associated, AP assigns AID to the station**


Client
Laptop computer
AP
1:Association request
2:Association response
Your association ID is: 1997
3:Traffic
ACK

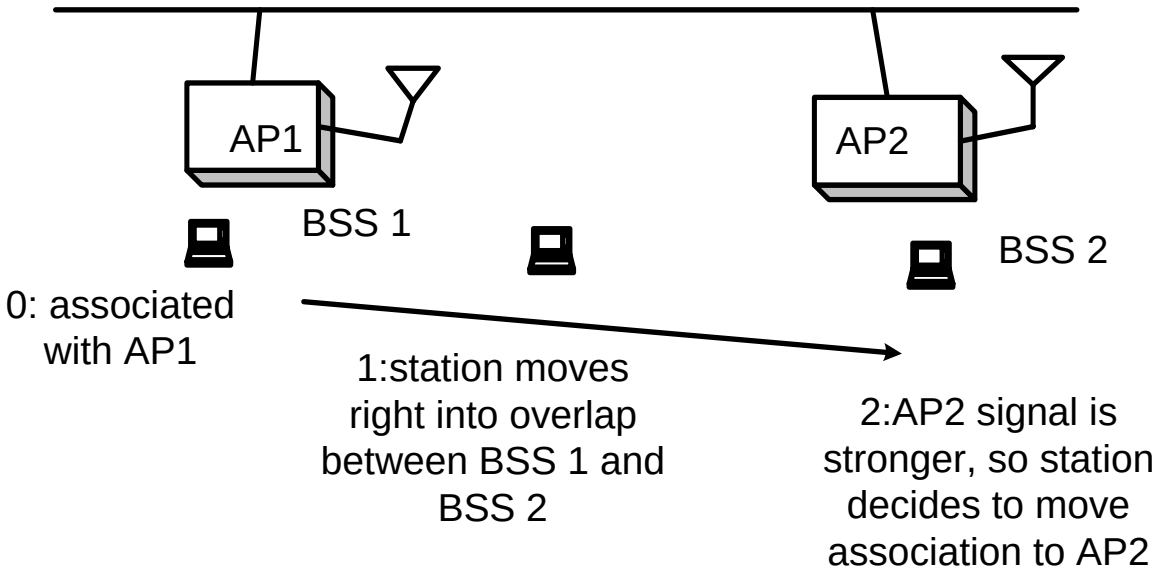
What is Roaming?

- Mobile stations may move …
  - beyond the coverage area of their Access Point
  - but within the range of another Access Point
- Reassociation allows station to continue operation

Roaming Approach

- Station decides that link to its current AP is poor
- Station uses scanning function to find another AP
  - or uses information from previous scans
- Stations sends Reassociation Request to new AP
- If Reassociation Response successful,
  - then station has roamed to th new AP
  - else station scans for another AP
- If AP accepts Reassociation Request
  - AP indicates Ressociation to the Distribution System (DS)
  - DS information is updated
  - Normally old AP is notified through DS

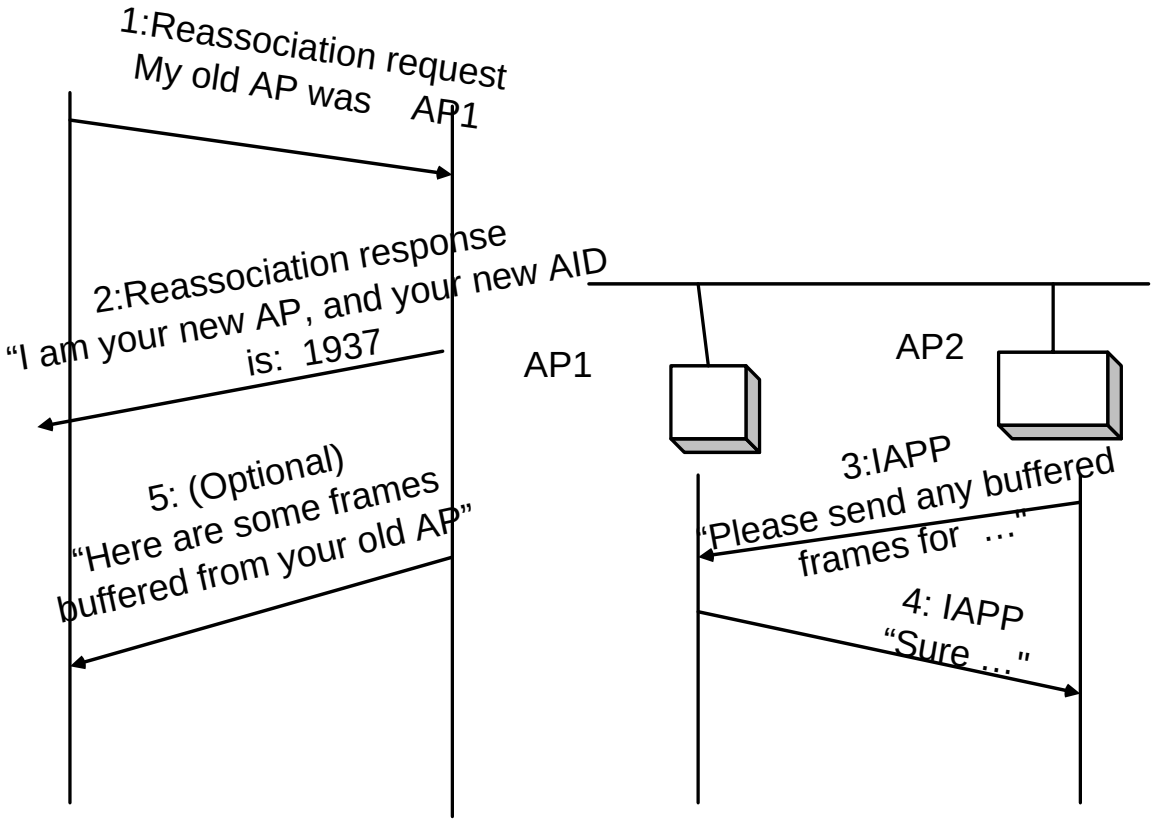
More on Reassociation



Step	Action
0	Station is associated with AP1
1	Station moves right into the overlap area between AP1 and AP2
2	AP2 signal is stronger, so station decides to move association to AP2
3	Station authenticates to AP2
4	Station reassociates with AP2
5	Station begins using the network

Reassociation -

- **Result of reasociation, new AP will inform the old AP to send all the buffered frames to the new AP**



Power Management

- **Mobile devices are battery powered**
  - **Battery is critical resource for mobile stations**
- **How can mobile stations be powered off during idle periods, yet maintain an active session?**
- **802.11 Power Management Protocol:**
  - **allows transceiver to be off as much as possible**
  - **is transparent to existing protocols**
    - **possible to trade off throughput for battery life**

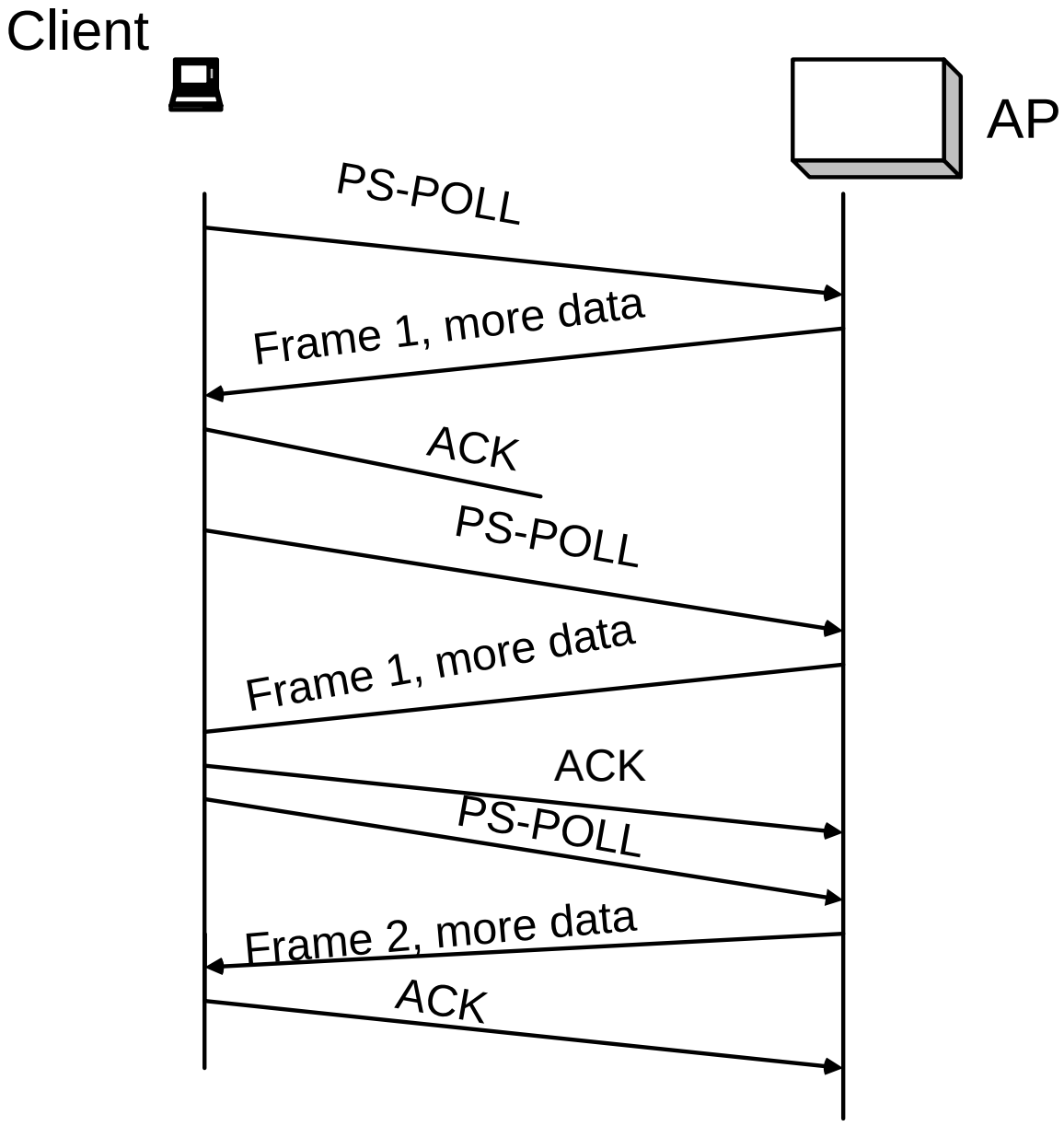
Power Management Approach

– conducted through joint effort of the AP and mobile station

- Allow idle stations to go to sleep
  - Station's power save mode stored in AP
- APs buffer frames for sleeping stations
  - AP announces through periodic Beacon signal which stations have frames buffered
  - Beacon contains a Traffic Indication Map (TIM) indicating which stations have frames waited to be picked up
- Power saving stations wake up periodically i.e., Listen-interval
  - When listen-interval expires, station wake up to Listen for Beacons
- TSF (Time Synchronizing Function) assures AP and Power Save stations are synchronized
  - Stations will wake up to hear a Beacon
  - TSF timer keeps running when stations are sleeping
  - Synchronization allows extreme low power operation
- Broadcast frames are also buffered in AP
  - All broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent at expected DTIM (Delivery Traffic Indication Map) interval
  - DTIM interval is a multiple of TIM interval
- Stations wake up prior to an expected DTIM
- If TIM indicates frame buffered
  - Station sends PS-POLL and stays awake to receive data

    else station sleeps again

Interaction between AP and station



Summary - 802.11 MAC Management Frames

- **Beacon**
  - **Timestamp, Beacon interval, Capabilities, ESSID,**
    Supported Rates, parameters
  - **Timestamp for synchronization of all the clocks within the BSS area**
  - **Area where Beacon signal appears defines the BSS area**
  - **Traffic Indication Map (TIM) indicates which stations have buffered frames waiting to be picked up**
- **Probe (Request and Response)**
- **Authentication (Request and Response)**
- **Association (Request and Response)**
- **Disassociation Request (notify)**
- **Reassociate (Request and Response)**
- **Deauthentication Request (Notify)**

V.2. 802.11 Security

Security side of 802.11 networks requires several things

- **Protecting the 'network' from intruders**
  - **Require authentication of users**
- **Data confidentiality and Integrity**
  - **Protecting DATA from eavesdropping - requires some type of encryption to protect confidentiality of data**
  - **Data integrity**
    - **if data is tampered or modified during transit, receiver must be able to detect and discard the frame**
- **The ability to manage the users credentials**
  - **WEP keys, user names, passwords, etc.**

802.11 WEP (Wired Equivalent Privacy) – Encryption

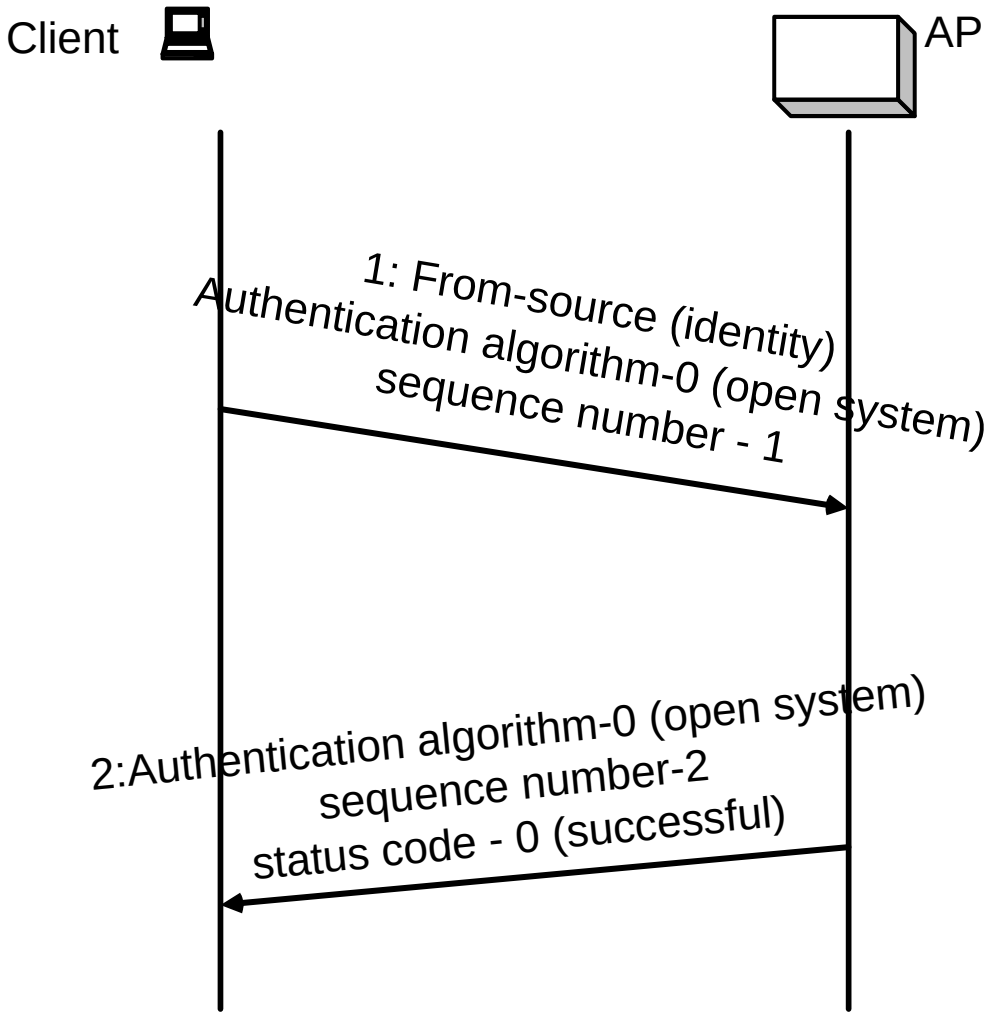
- **Encryption options**
  - **No encryption**
  - **40-bit encryption - not used anymore**
  - **104-bit encryption – currently always use 104 bit encryption**

Privacy and Access Control

- **Goals of 802.11 WEP is to provide "Wired Equivalent Privacy" (WEP)**
  - **Same level of security equivalent to wired Ethernet**
- **Two types of Authentication mechanisms**
  - **Open Authentication - allows everybody to come in or no authentication at all**
  - **Shared key authentication - stations that possess the same secret key, are allowed to be authenticated**

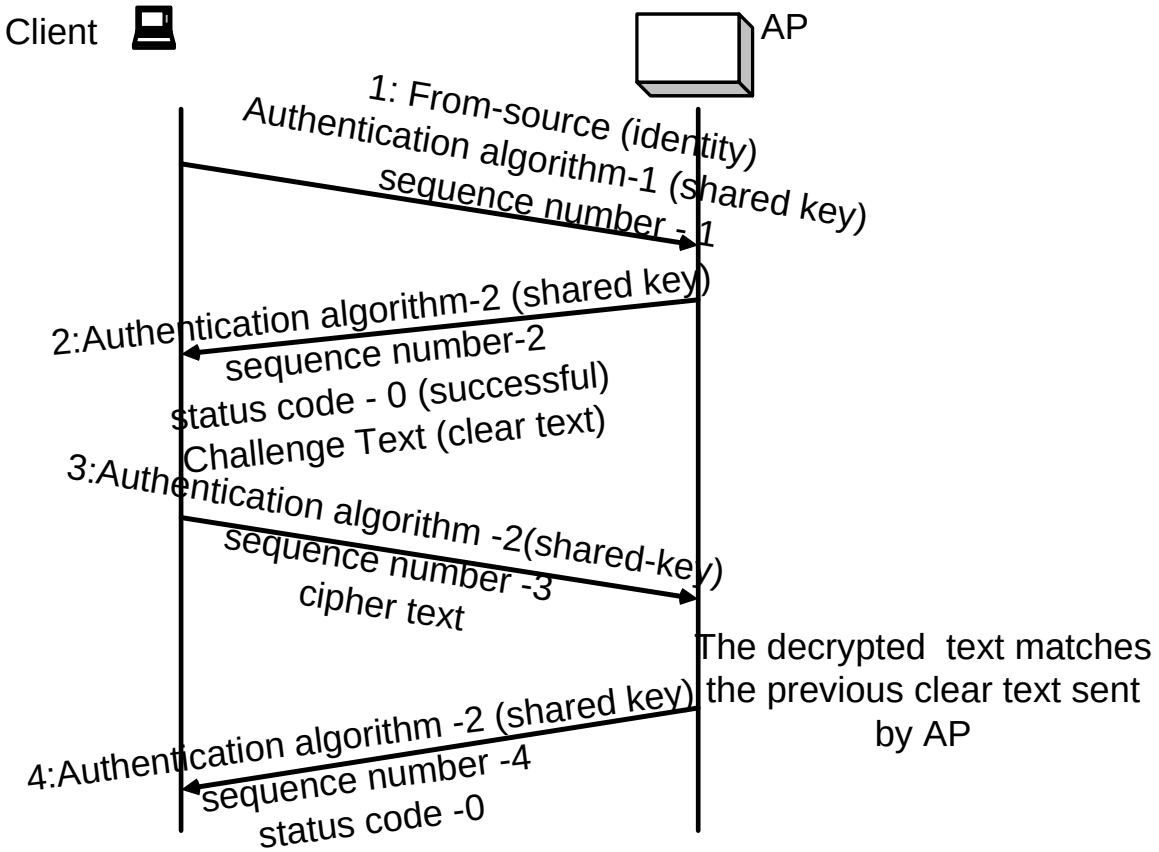
Two types of Authentication by 802.11

- **Open Authentication – AP accepts the mobile station at face value without verifying its identity**
  - **Open authentication means no authentication at all**
- **Shared-key Authentication**
  - **802.11 WEP specifies that only stations that share the same secret i.e., those who know the secret key K is allowed to be authenticated**



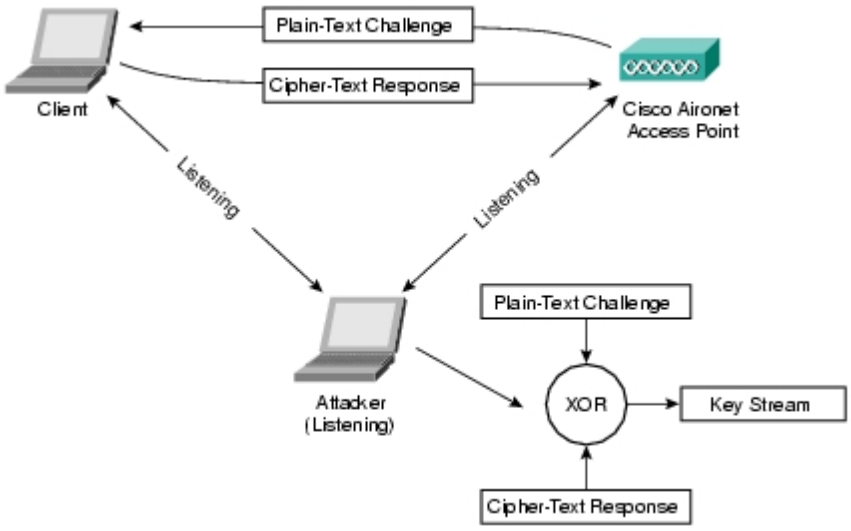
Open-system Authentication Exchange

What is Shared-Key Authentication?



Shared Key Authentication Problems

- **Shared key Authentication is worse than worthless. Not just provides no authentication, but also exposes the secret.**



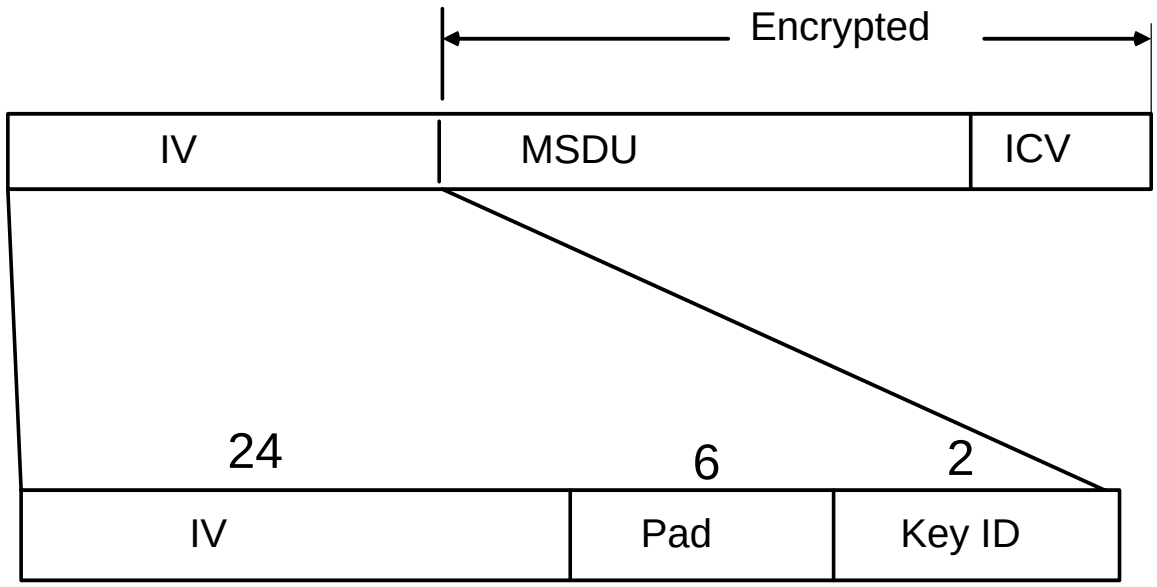
♦ 802.11 WEP Privacy mechanism

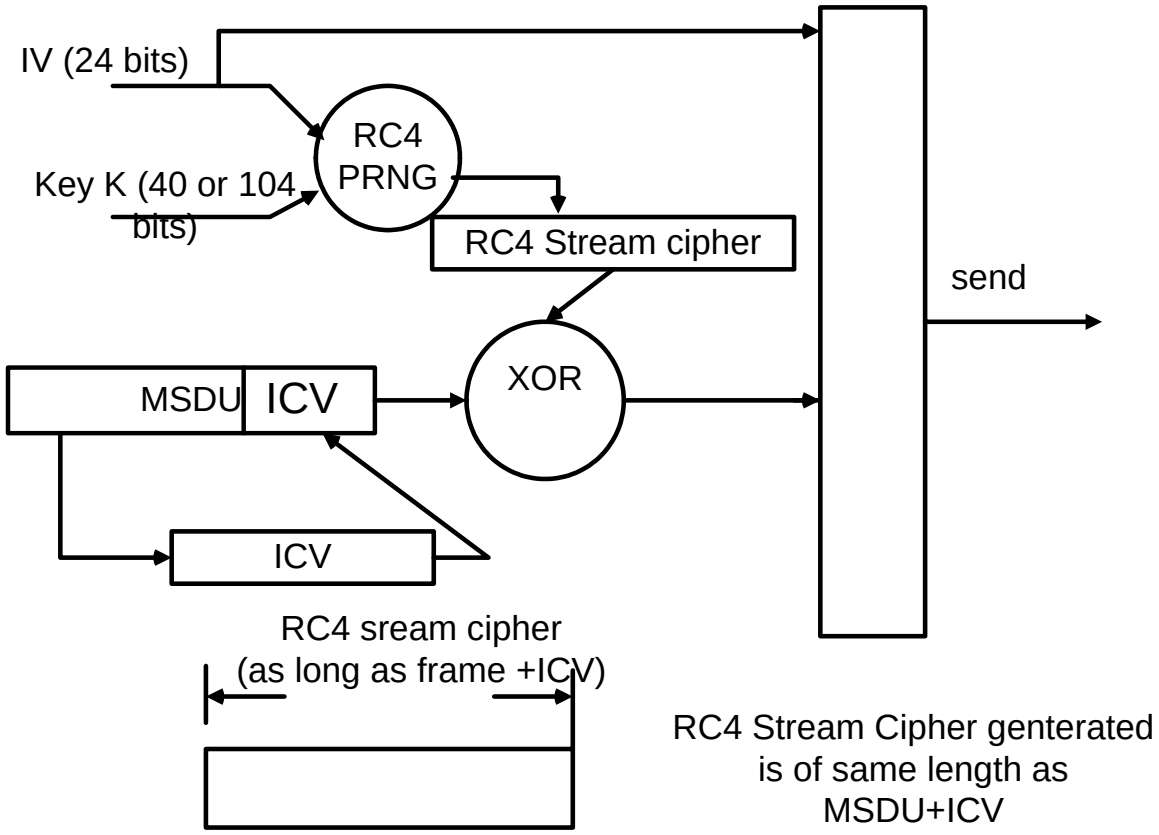
- **Only payload of Data frames (i.e. MSDU) plus ICV are encrypted**
  - * **ICV (Integrity Check Value) is provided to allow for integrity check**
  - * **ICV is similar to the CRC except that is computed and added on before encryption**
  - * **Set WEP =1 in FC (Frame Control) of 802.11 MAC frame to indicate that WEP used**
- **MSDU and ICV are encrypted using RC4 encryption algorithm**
  - * **A 104 bit secret key and a 24 bit IV (Initialization Vector) are concatenated to initialize the RC4 encryption engine and generate a pseudorandom sequence of bytes**
    - **→ pseudorandom means:**
      - **as far as attacker is concerned, it is totally random a sequence of bytes, but to the two end points with knowledge of secret key K and IV, always produces the same random sequence of bytes**
  - * **Each frame can have a new IV, or IV can be reused for a limited time**

802.11 WEP Scheme

Confidentiality and Integrity Handled simultaneously

- Frame (or MSDU) 1st runs through an integrity check algorithm, generating a checksum called ICV.
  - ICV protects the contents against tampering by ensuring that the frame is not altered in transit
  - Then the frame and ICV are concatenated together and encrypted - ICV is not available to casual attackers
- To enable the receiver to decrypt the frame, IV is placed in the header of the frame which is a clear text





- **PRNG : Pseudorandom number generator**

Stream Cipher vs. Block Cipher

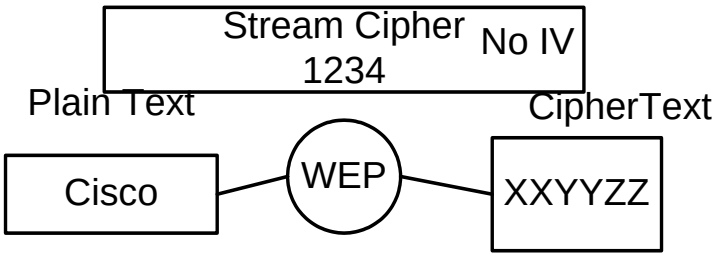
- **Stream Cipher**
  - **Input data is treated as continuous stream**
  - **At the highest level, stream cipher acts like a black box, which takes a sequence of ordinary data (plaintext) and produces a sequence of totally different output data called ciphertext**
  - **The internal state of stream cipher is continuously updated until all the data in the input stream is processed**
  - **The process is more like sausage machine**

- **Block Cipher**
  - **Input data is broken into fixed length block**
  - **Take a block of ordinary data as input and produces a block of ciphertext**
  - **The state of block is reset for each block before processing**
  - **More like making doughnut**

What is IV?

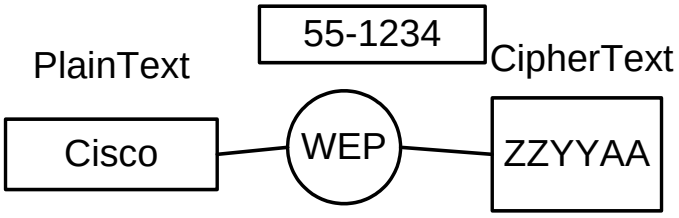
- **Without IV, the same clear text will produce the same cipher text again and again**
- **With IV, then as IV changed, the cipher text also changed; more difficult for the attacker to figure out the secret key K**

What is an IV?



Without an IV, the same PlainText will always produce the same CipherText; An eavesdropper will be able to 'see' patterns and predict PlainText

Stream Cipher -with IV



With the IV,the cipherText will change as the IV changes; more difficult for an eavesdropper to 'See' patterns and predict PlainText

Same plaintext should not generate same ciphertext packet

IV is random, and changes per packet

What is RC4?

- A stream cipher
- At the highest level, RC4 is like a black box that takes one byte from a input stream and produces a corresponding but different byte (ciphertext) for the output
- Decryption is the reverse process and uses the same key as for encryption
  - If a sequence of data is encrypted twice by RC4, it will produce the same plaintext
- RC4 has two phases of activities
  - Phase 1. Initialization – use the key value to construct some internal tables
  - Phase 2. Encryption – input data is encrypted
- Each packet is treated as a new stream of data which ensures that if one packet is lost, the following packet can still be decrypted.

Why WEP is not Secure?

- **Authentication – the basic requirements for authentication in WLAN are:**
  - **Robust method of proving identity that cannot be spoofed**
  - **Method of preserving identity over subsequent transactions that cannot be transferred**
  - **Mutual Authentication**
  - **Authentication key independent from encryption key**

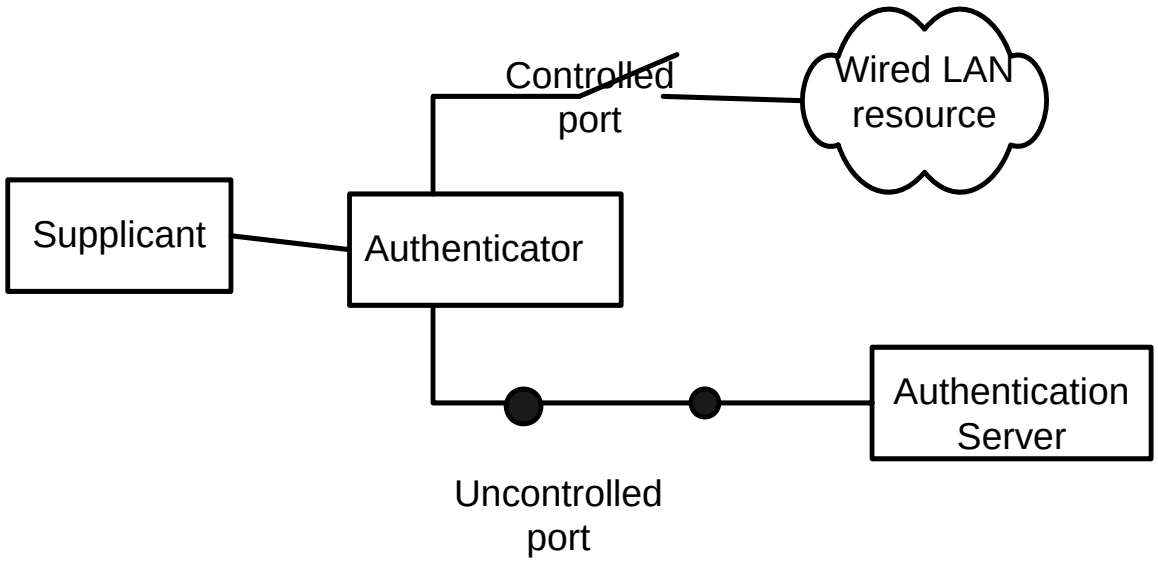
  - **802.11 WEP fails on all 4 of the requirements, the shared key authentication is worse than worthless**
- **No Access Control - WEP practically provide no access control.**
  - **After a device is authenticated, he/she is allowed access**
  - **AP keeps a list of allowable MAC addresses – but MAC address can be easily forged**
- **No Replay Attack Prevention - an attacker can collect and store a large number of intercepted frames and try to send later on**
  - **AP has no way to prevent those replay attack**
- **Message Modification Prevention -**
  - **ICV, the Integrity Check Value is produced using a linear method, same as CRC.**
  - **Cryptographic specialist proved that it is subject to bit flipping attack**
- **Message Privacy – two factors that affects the WEP privacy**
  - **IV Reuse - With only 24 bits for IV, sooner or later the IV value will be used.**
    - **Once the same IV is detected, the attacker can try to break the secret**
  - **RC4 Weak Keys – Cryptographic experts have shown that certain RC4 weak keys will expose the secret**

What is a “Weak” IV?

- In the RC4 (PRNG) algorithm, the Key Scheduling Algorithm (KSA) creates an IV-based on the base key
- A flaw in the WEP implementation of RC4 allows “weak” IVs to be generated
- Those Weak IVs “gives away” info about the key bytes they were derived from
- An attacker will collect enough weak IVs to reveal bytes of the base key

IEEE 802.1X

- **A simple concept to implement the access control at the point where the user tried to join the network**
- **Has 3 components :**
  - **Supplicant – the end user machine that seeks access to network resources**
  - **Authenticator – Controls the network access**
    - For Ethernet hub/switch, a one-to-one relationship between Supplicant and Ethernet port. Authenticator is at the Ethernet port
    - For 802.11 WLAN, MS (or STA) is the Supplicant and AP, the Authenticator
  - **Authentication Server – Makes the authorization decision**
    - Example: RADIUS server which performs actual processing

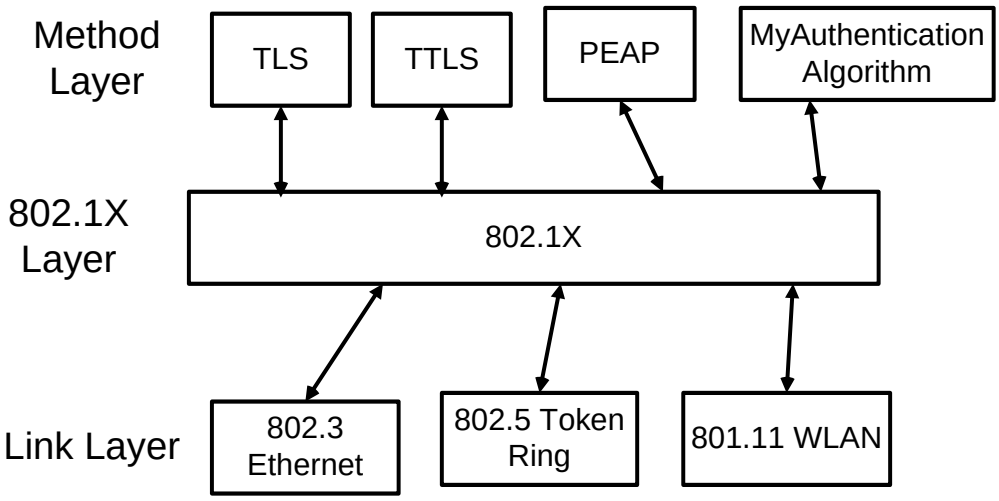


- **Before the supplicant is authenticated,**
- **the uncontrolled port is open, and controlled port blocked.**
- **Uncontrolled ports allows authentication traffic to flow between Supplicant and Authentication Server**
- **Authentication exchange is logically carried out between the supplicant and the authentication server**
- **The controlled port is close after the supplicant is authenticated, and supplicant (or STA) can access the network resources.**

EAP (Extensible Authentication Protocol) Principle

- **Part of IETF(Internet Engineering Task Force) standards.**
- **Similar in concept to actor's agent, take an actor to a movie director and perform introduction**
  - **while actor and director are talking, sit back and do nothing**
  - **After they finish talking, jump in and close the deal**
  - **Extensible because the actual authentication method to be used not specified**
  - **Can be any of the following:**

  *** Transport layer Security (TLS) over EAP i.e., EAP-TLS, Tunneled TLS (TTLS) over EAP or mymehtod over EAP**



Only 4 types of messages are defined in EAP:

- For Request and Response, it is further divided using type field. RFC defines only the 1st 6 types.

- **Request**
- **Response**
- **Success**
- **Failure**

Type field:

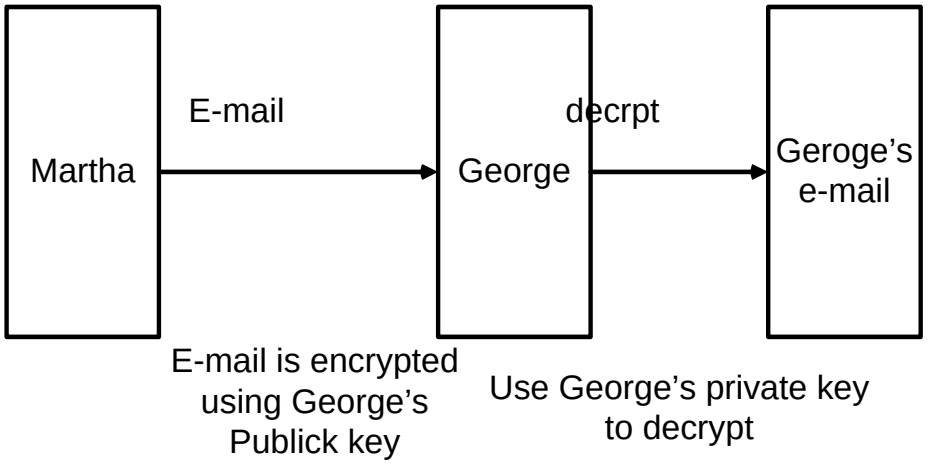
- **= 1, Identity**
- **= 2, notification,**
- **= 3, NAK**
- **For type > 6, refer to a specific authentication method and defined by IANA.**
  - **Type = 13, refer to EAP-TLS**

EAP-TLS (Transport Layer Security)

- To understand EAP-TLS, , need to know what is PKI (public key infrastructure).

What is PKI (Public Key Infrastructure) ?

- **Encryption can use either symmetric keys or asymmetric keys**
  - **Symmetric means the same secret key K is used for both encryption and decryption**
  - **Asymmetric means encryption and decryption are using different set of keys**
- **PKI encryption, based on a pair of asymmetric keys - a public and a private key.**
  - **Public and private keys exist in pairs, and are mathematically related**
  - **public key, known to the public, but private key, only the owner knows**
  - **Data encrypted with the owner's public key can only be decrypted with the owner's private key ; the reverse, also true.**



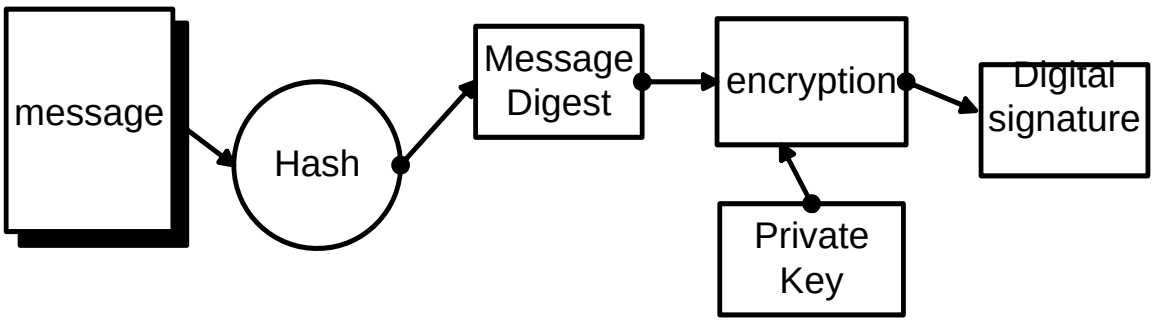
Note: If George and Martha know the public key of each other, then a secure communication channel between the two is established

Everything sent to Martha is encrypted with Martha's public key, and only Martha can open it. The reverse is also true.

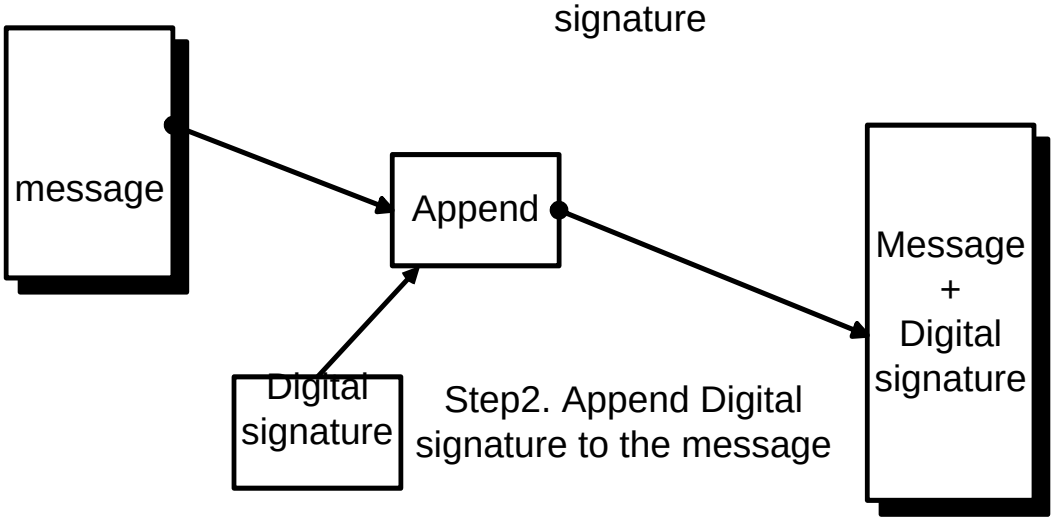
Message sent to George is encrypted with George's public key. Even if the message is intercepted, the attacker can not read the message. George is the only person with knowledge of his private key can decrypt and read the message.

What is Digital Signature?

- Digital signature is a "stamp" by the author of the document/data to prove that the authenticity of the author
- To create a digital signature,
  - The author 1st hash (e.g., RC4) the message/data created and generate a Message Digest (or MD)
    * MD digest the original message/data into a few lines
  - The author then uses its private key to encrypt MD and produces a digital signature or "digital stamp".
  - The digital signature is then appended to the message/data to be sent out
    * Same concept as the author signs a document after one is created
  - At the receiving end, the authenticity of the author is proved if the digital signature can be decrypted by the public key of the author
  - In addition, if the document is altered, modified or tampered during transit, the recipient can quickly detect.



Step1. Use private key to encrypt the MD and creates digital signature



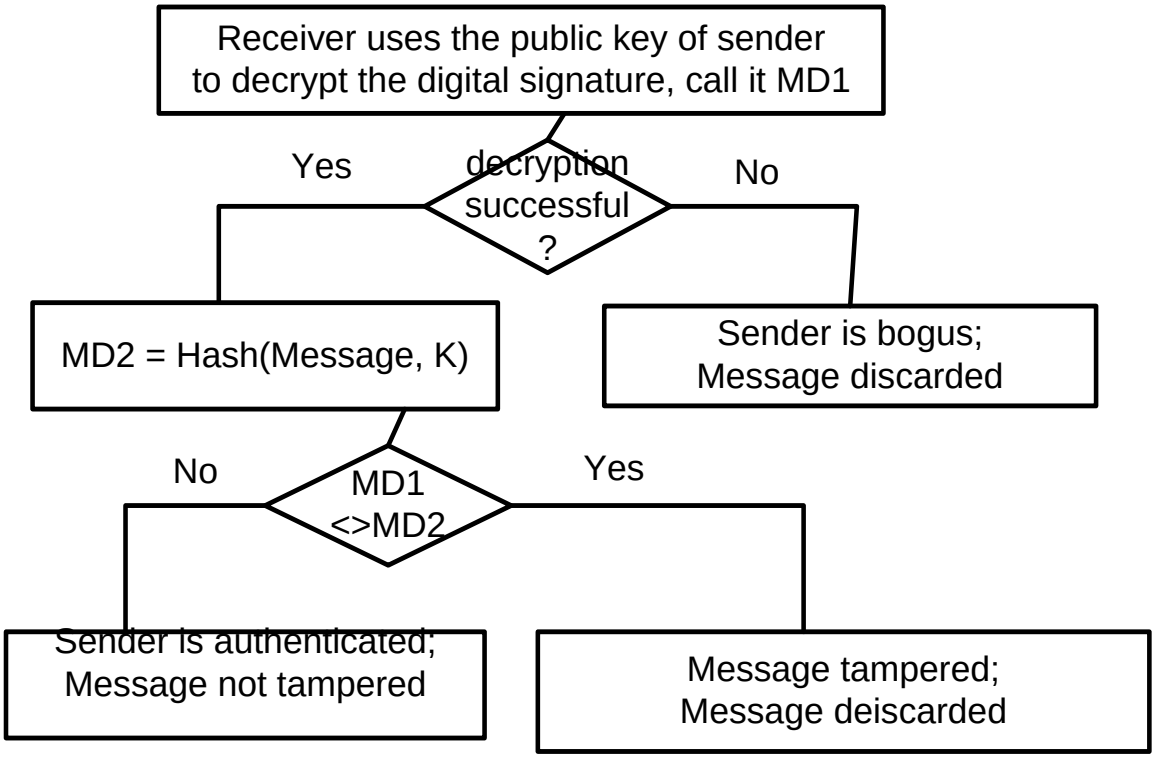
Step2. Append Digital signature to the message

What is Hashing?

- **Used frequently in cryptography – the purpose is to combine two or more numbers to produce a result such that it is extremely hard or impossible to reverse the process.**
- **Example: If C = hash(A,B), then knowledge of C tells you nothing about A and B**
- **One application of hashing is to protect a master key by generating a temporary session key.**
  - **Suppose A = 128-bit master key and B = time of the day, then**
    C = hash(A, B), a new 128-bit session key .
  - **Even if an attacker knows the values of B and C, it is practically impossible to derive the master key A**
- **Another usage of HASHING - to produce a MD (Message Digest) or to generate a MIC (Message Integrity Check).**
  - **MD or MIC is obtained by combining a large number of bits into a small number**
  - **Suppose you hash 8000 bits or 1000 bytes with a secret key to produce a result 64 bits long. By sending the message with MIC, the receiver can check whether the message is intact or altered.**
  - **Even if a single bit of 1000 bytes is altered, the resulting 64 bits hash would be totally different**

Verification of the digital signature – a reversal process

- The receiver uses the author's public key to decrypt the digital signature
  - If decryption fails, then it proves that it was not sent by the author and discarded else call the result MD1
- Then use hashing algorithm (e.g., RC4) to hash the message/data to create a new Message Digest, called MD2
- If MD1 = MD2, then it proves that the message/data received not modified or altered during transit
  - Otherwise the document is modified or tampered, and is discarded by the receiver


Receiver uses the public key of sender to decrypt the digital signature, call it MD1
decryption successful ?
Yes
No
MD2 = Hash(Message, K)
Sender is bogus; Message discarded
MD1 <>MD2
No
Yes
Sender is authenticated; Message not tampered
Message tampered; Message deiscarded

What is Digital Certificate?

- A data structure made up of the following pieces of information:
  - Certificate version
  - Serial number
  - Certificate issuer
  - User name
  - User's public key
  - Validity period
- Distributed by a certificate authority (or CA), an independent and trusted authority, that joins a public key to a user.

What is TLS (Transport Layer Security)?

- Same as SSL (Secure Socket Layer), a proprietary protocol by Netscape
- TLS, an IETF standard and documented in RFC

S1).Client send hello and CNOUNCE to server (client → server)

- Nounce means N (value) once, a random number that never repeats. For regular random numbers, occasionally the number repeats

- Client generates a CNOUNCE and send to the server

Hello includes: cipher suites i.e, type of certificate to be used, encryption and integrity methods to be used.

S2). Server send hello (server → client) including SNOUNCE and session-ID

- Server after receiving the client hello, also generated a nounce value called SNOUNCE and session ID.

Note:

- **a security session once established can resume multiple times, and each time before it is resumed, client always use the session-ID to refer to a particular session.**

At this stage, client and server have:

- **synchronized their status**
- **An agreed session-id**
- **exchanged two nounce values i.e., SNOUNCE,CNounce**

TLS (Continured)

S3). Server then proceed to send server certificate (Server → client) to the client and issues request for client certificate.

- Client checks the validity of the server certificate and proceed to extract the pub-key of server.

S4). Client sends its certificate (Client → Server) to the server.

- Server also check the validity of the client certificate and proceed to extract the Public-key of THE client.

- At this point, both client and server know the Public key of each other.

- a secure communication channel is thus established between the client and the server.

Client uses the two random numbers i.e., SNOUNCE and CNounce, and other information to generate a random number called pre-master key.

Client uses the secure channel to send the pre-mater key to the server by encrypting the pre-master key with the pub-key of Server.

- If server able to decrypt the pre-masterkey,it proves that server is the owner of the its publickey.

S5).Client proceed to prove that it is indeed the holder of the certificate.

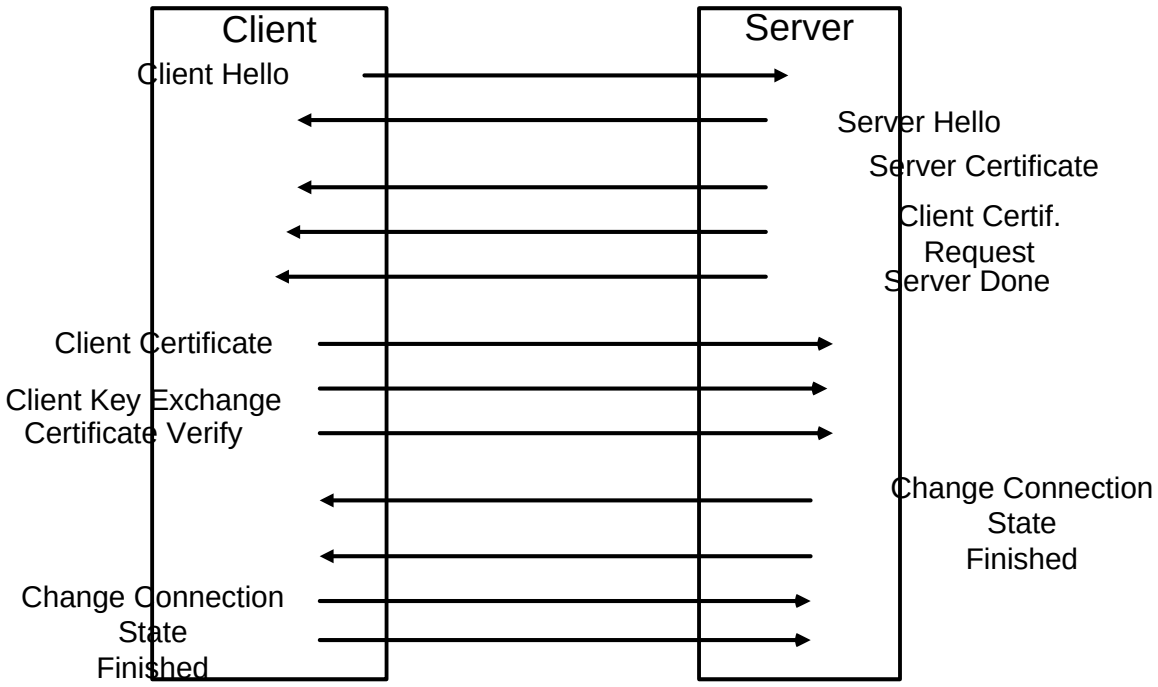
To prove that claim, client hashed together all the messages sent and received together with the digital signature, and send to the server.

The server performs the following two steps:

a).Use the public key of client to decrypt the digital signature. If decrypted successfully, call the result MD1 and go to step b).

b).Server then hash together all the messages sent and received and call the result MD2.

If step a) fails, or MD1 <> MD 2, then it proves that the client is bogus



TLS Message Exchange Summary

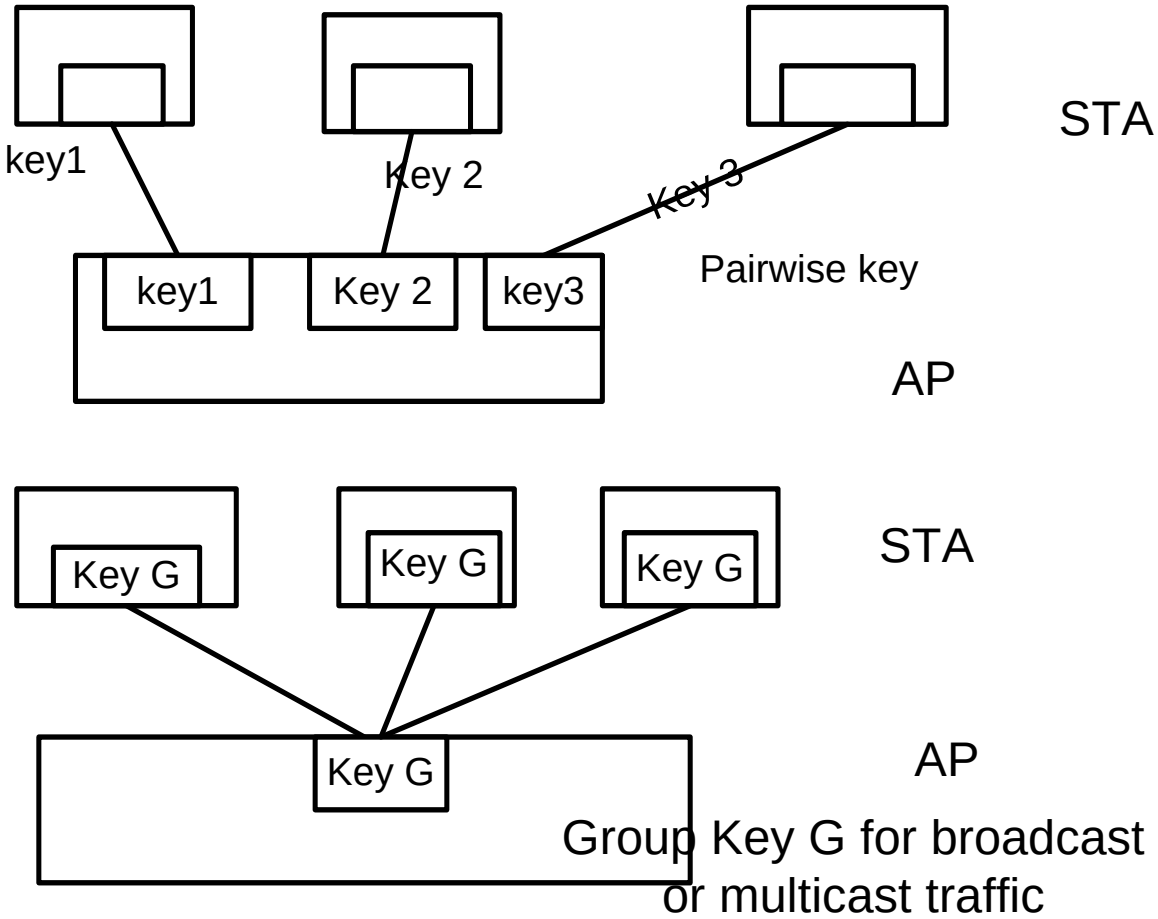
Two Ways Handshakes between TLS client and server

From	To	Remark
Server	Client	EAP-Request Identity
Client	Server	EAP Response Identity
Server	Client	EAP-TLS (start)
Client	Server	EAP-TLS Client hello and CNOUNCE -type of certificate, encryption algorithm and integrity check method used -client nounce value i.e., CNOUNCE
Server	Client	EAP-TLS Server hello and SNOUNCE -server certificate, server nounce value i.e., SNOUNCE; Request for client certificate
Client	Server	Client verifies server certificate, and extracts the server public key Client sends client certificate
Client	Server	Client uses CNOUNCE and SNOUNCE and a random number to generate a pre-mater secret key i.e., Pre-master key Client uses the server's public key to encrypt the pre-master secret and send to the server; if server able to decrypt and obtain the pre-master key, it proves that server is indeed the owner of the public-key
Client	Server	See Note:Client proceeds to prove that it is thw owner of its public key

Note: Client creates a MD by hashing of all the messages sent and received, and signs the
Messages with its digital signature.
If server is able to verify, then the client is indeed the legal owner of the certificate, otherwise,
either it is the bogus owner of the certificate or the messages are tampered or modified.

WPA and RSN Key Hierarchy

- **802.11i defines a RSN (Robust Secure Network)**
  - **A brand new wireless network security scheme, does not consider limitation of any legacy 802.11 hardware problems**
    - * **802.11 legacy hardware not very powerful, can not implement full version of RSN**
  - **Wi-Fi introduces an interim solution called WPA (Wireless Protected Access) which implements only a subset of RSN**
    - * **WPA does not require any hardware upgrade**
    - * **Addressing WEP security weakness by introducing TKIP (Temporal keys Integrity Protocol) which requires only software upgrade**
- **Pairwise vs Group keys**
  - **Pairwise key, used for unicast traffic, to protect communication between STA and AP**
    - **For each pair of STA and AP, a distinct pairwise key is used**
    - **Each STA , once associated with the AP, must store a pairwise key, and AP, one pairwaise key for each STA it is communicating with**
  - **Group Key – shared by AP and a group of trusted parties**
    - **For delivery of broadcast or multicast traffic**

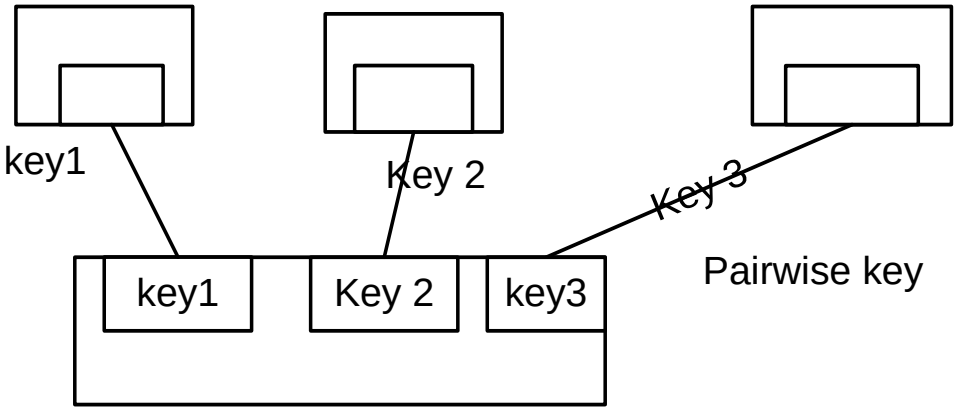

key1
Key 2
Key 3
STA
key1
Key 2
key3
Pairwise key
AP
Key G
Key G
Key G
STA
Key G
AP
Group Key G for broadcast
or multicast traffic

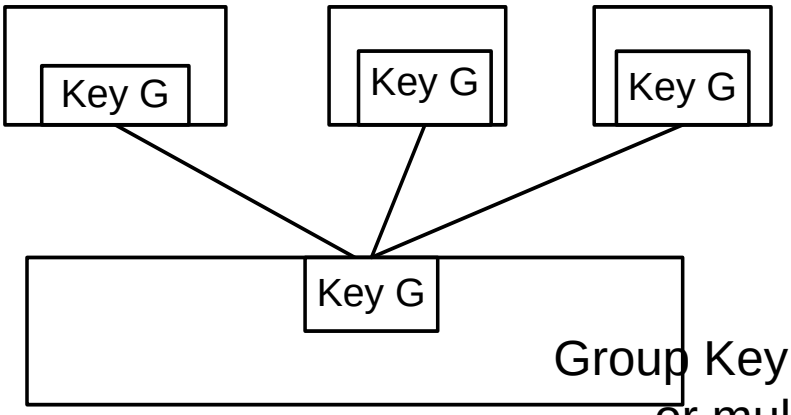
◆ Preshared keys vs Server-based keys

- **Preshared keys are installed on the AP and in the STA by some method outside of WPA/RSN**
  i.e, bypass upper layer authentication process
- **Upper layer authentication e.g., EAP-TLS, allows the STA and an AS to generate matching secret keys, and then AS arrange for the AP to get a copy of secret keys for use in session protection**

◆ **Pairwise Key Hierarchy**

- **The PMK is the top of the pairwise key hierarchy**
- **For each STA, there is a different PMK, and from this, all other pairwise keys are derived**





Group Key G for broadcast or multicast traffic

S1).Supplicant and AS (Authentication Server) performs mutual authentication

The default authentication method is EAP-TLS.

S2).Supplicant and AS, then generate matching PMK

- **AS then delivers PMK through a secure channel to the AP.**
  - * **802.11i does not specify how AS should deliver PMK to the AP, but WPA, specifies that transfer of PMK to AP should use RADIUS protocol**
- **After AP obtains PMK, AP issues EAP–success message to the Supplicant, and according to 802.1X, the control port is close, and data start to flow.**
- **However, in WPA/RSN, further hurdles need to clear before data can flow**

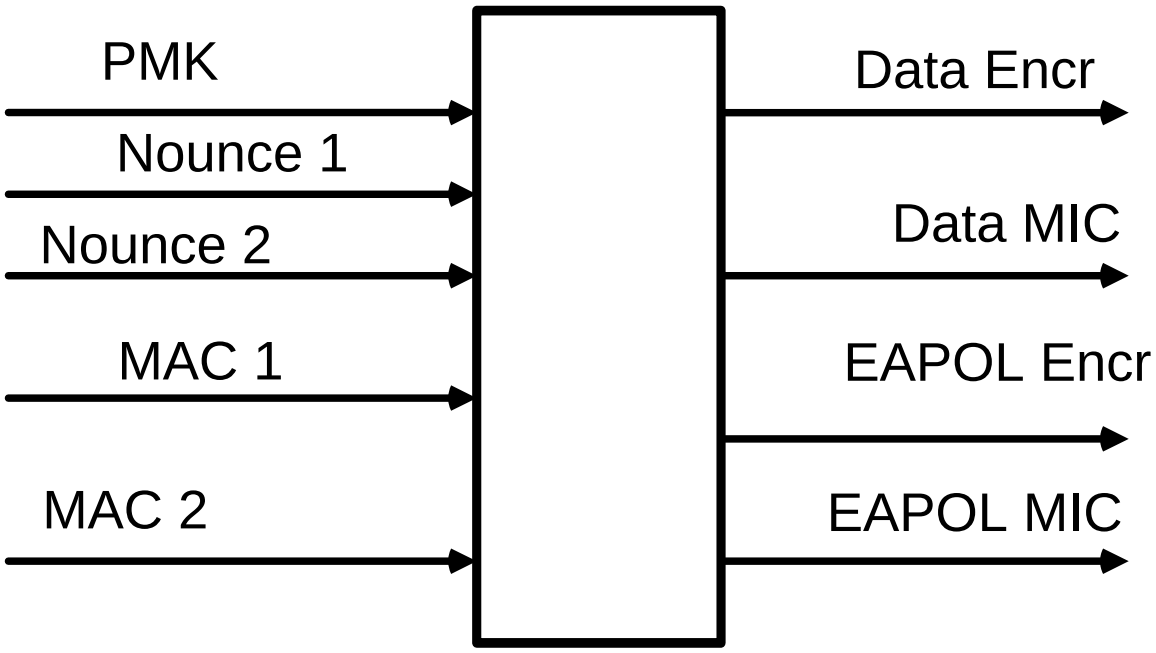
PMK – not used for any security operations, is used to derive four separate keys in protecting the wireless link i.e.,

- * **Two layers i.e., EAPOL handshakes and the user's data**
- * **two cryptographic functions – encryption and integrity**

- **PTK (pariwise transient key) consists of four Separate keys described as follows:**
  - **The 4 keys are recomputed every time a mobile device becomes associated to the AP and is therefore transient**
  - **To introduce liveness, two nounce values (nounce 1 and nounce 2) are used, one generated by the supplicant, the other, by the AP are used in the computation of of temporal keys**

The four keys are:

* **Data Encryption key (128 bits)**
* **Data Integrity key (128 bits)**
* **EAPOL-Key Encryption key (128 bits)**
* **EAPOL-Key Integrity key (128 bits)**



Temporal Key Computation

Note: MAC 1 and MAC 2 are the two MAC addresses of AP and mobile stations STA

Four Way handshakes to prove that AP is not a bogus

- **Requirement: AP and STA must prove to each other that they both possess A copy of the secret PMK**
- **In WPA/RSN, the process of proving key ownership is combined with the process of deriving the temporal keys using a key message exchange**
- **The nounce selected by the Authenticator (AP) is called ANOUNCE, and that of the supplicant, SNOUNCE.**
  Note: nounce, means N (value) once, a random number that never repeat

Message (A): Authenticator → Supplicant

- **First EAPOL-key message contains ANOUNCE value**
- **As soon as the supplicant received message (A), it proceeded to compute the temporal keys using the 4 parameters i.e., PMK, ANOUNCE, SNOUNCE, MAC 1 and MAC 2**
- **MAC 1: MAC address of AP or BSSID, MAC 2: MAC address of Supplicant**

Message (B): Supplicant → Authenticator

- **The EAPOL-key message contains SNOUNCE and MIC**
- **MIC value is computed using the DIK**
- **As soon as SNOUNCE is received, Authenticator proceeds to compute its own PTK.**
- **If the MIC value in message B is verified as correct based on the computed PTK, it proves that Supplicant possess the correct copy of PMK**

Comment: At this point, the 1st half of the four-way exchange is completed. Both sides now have derived the four temporal keys and the authenticator has verified that the supplicant has a matching PMK.

Message (C): Authenticator → Supplicant including sequence number and MIC

- **MIC is the message integrity check, computed based on the 4 keys of PTK**
- **Message C informs Supplicant that the Authenticator is ready to start using the new keys for encryption**
- **If supplicant can verify that the MIC value is correct, then it proves that the Authenticator possess the matching PMK**
- **Message C was sent in plain text, and Authenticator does not install PTK until it receives message D, which is an ACK**

Message (D): Supplicant → Authenticator

- **Message D acknowledges the completion of four-way handshakes and indicates that the supplicant will now install the keys and start encryption.**

The four-way handshakes accomplished the following:

1. **ANOUNCE and SNOUNCE value exchanged**
2. **Both sides have computed the temporal keys (PTK)**
3. **Supplicant and Authenticator, each has proved to the other that it possesses knowledge of PMK**
4. **Both sides have synchronized and turned on encryption of unicast keys.**

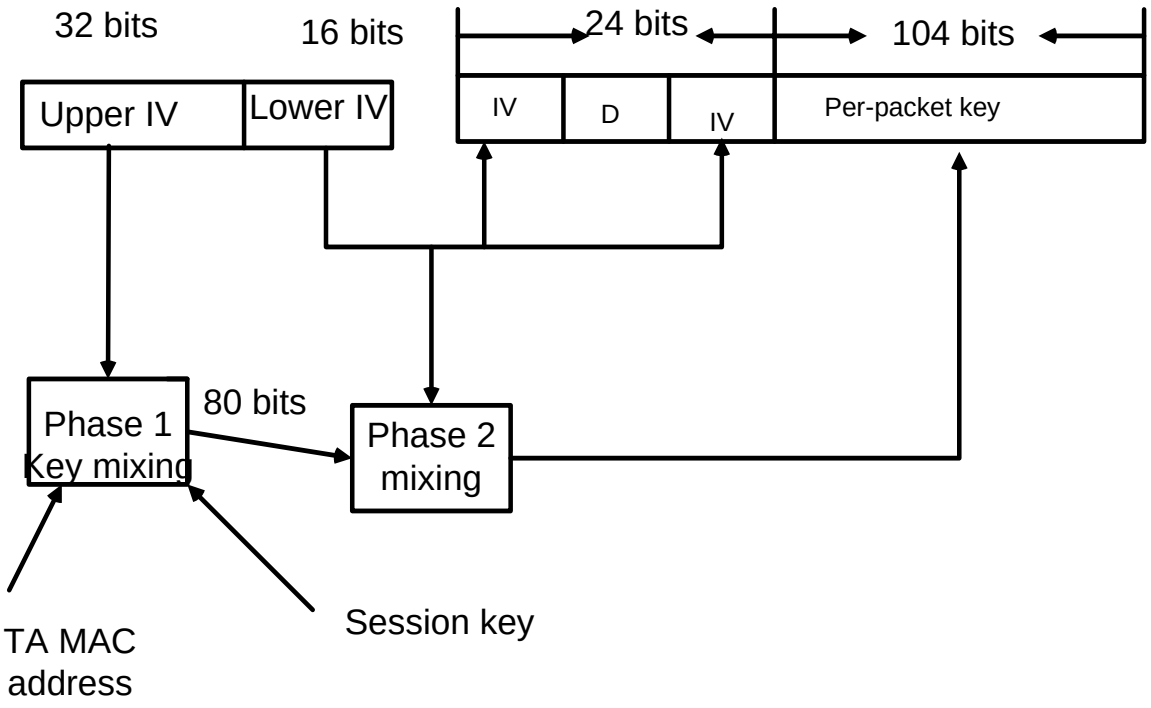
Why Temporal Key Integrity Protocol (TKIP)?

- **Table 1 summarizes the Weakness of WEP**

Table 1

1	IV value is too short and not protected from resue
2	The way keys are constructed from the IV makes it susceptible to weak key attacks 9FMS attack)
3	No effective detection of message tampering (message integrity)
4	It directly uses the master key and has no built-in provision to update the keys
5	No protection again message replay

- 802.11 WEP has been shown to be ineffective as a data-privacy mechanism, the
  enhancement to WEP is collectively known as TKIP
- TKIP provides the following major enhancements:
  - A message integrity check (MIC), known as Michael, function on all WEP-encrypted data frames
  - Per-packet keying on all WEP-encrypted data frames
    * Base key and IV hashed to obtain per packet encryption key
    * For each packet to be transmitted, it use a distinct per-packet key to encrypt the data
    * Even for the same pair of STA and AP, the per-packet key of STA → AP
      and that of AP →STA is different because TA MAC address is factored in phase 1 mixing
      - IV size increased to 48 to prevent IV reuse
      - Add a sequence counter to the MAC frame to prevent replay attack



Creating the RC4 Encryption Key

Table 1 Weakness of WEP

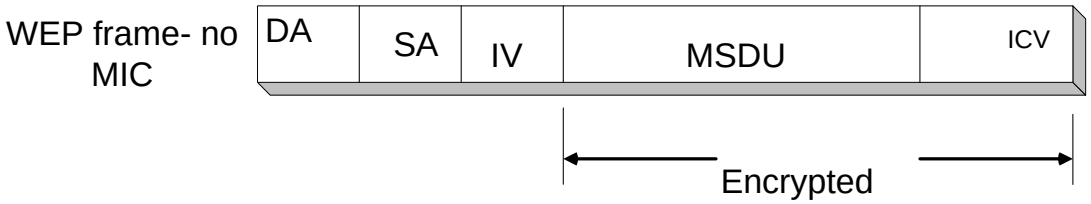
1	**IV value is too short and not protected from resue**
2	**The way keys are constructed from the IV makes it susceptible to weak key attacks 9FMS attack)**
3	**No effective detection of message tampering (message integrity)**
4	**It directly uses the master key and has no built-in provision to update the keys**
5	**No protection again message replay**

Table 2 Changes from WEP to TKIP

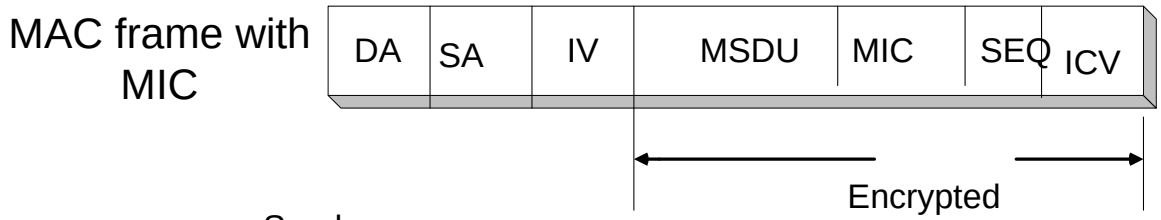
Purpose	**Change**	**Weakness addressed**
Message Integrity	**Add a message integrity protocol to prevent tampering that can be implemented in software on a low-powered microprocessor**	**(3)**
IV selection and use	**Change the rules for how IV values are selected and resuse the IV as a replay counter**	**(1) (3)**
Per-packet key mixing	**Change the encryption key for every frame**	**(1) (2) (3)**
IV size	**Increase the size of the IV to avoid ever reusing the same IV**	**(1) (4)**
Key management	**Add a mechanism to distribute and change the broadcast key**	**(4)**

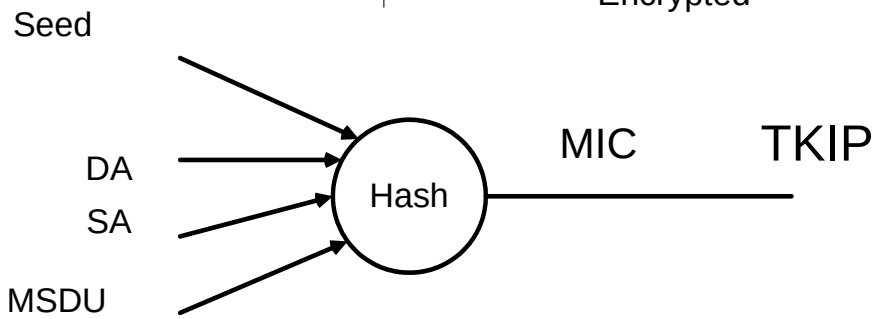
Message Integrity Check (MIC)

- **The MIC augments the ineffective ICV of 802.11 WEP standard.**
  - **Designed to solve two major vulnerabilities:**
  - **MIC adds a sequence number field to the wireless frame. The AP will drop frames received out of order**
  - **Frame tampering/bit flipping – MIC feature adds a MIC field to the wireless frame which is not vulnerable to the same mathematical shortcomings as the ICV of 802.11 WEP**
- **The MIC is based on seed value, destination MAC, source MAC and payload**
  - **Any change to these values will change MIC value**

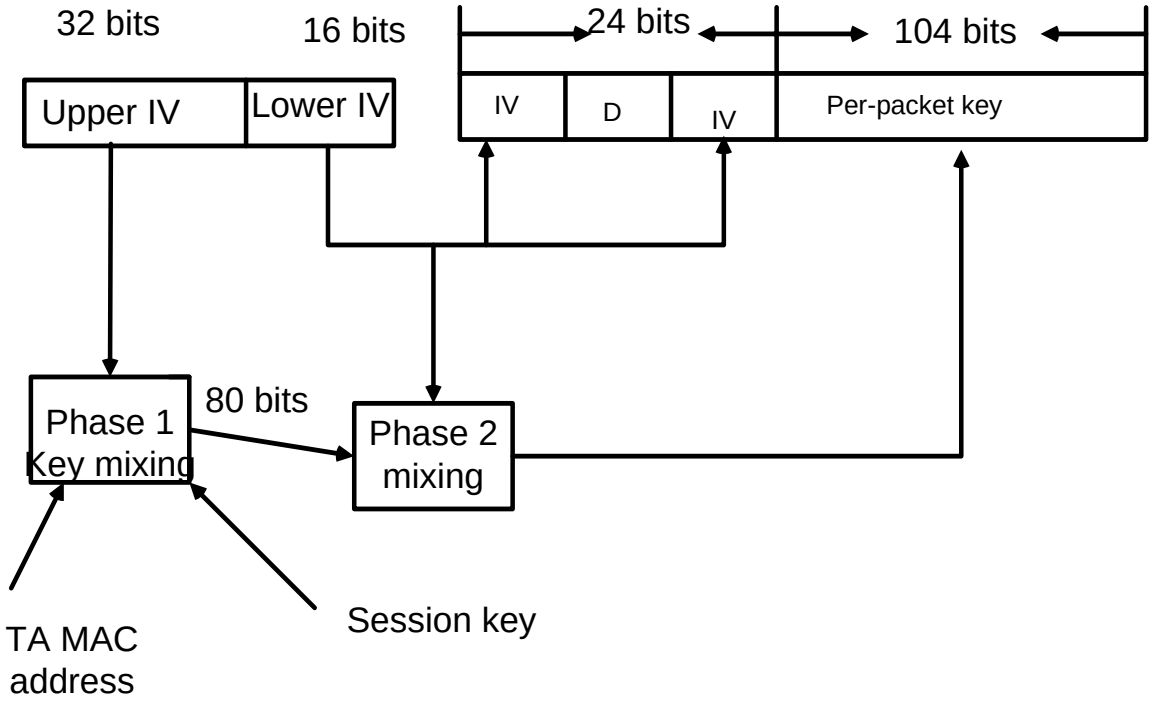

WEP frame- no MIC
DA
SA
IV
MSDU
ICV
Encrypted

802.11 WEP


MAC frame with MIC
DA
SA
IV
MSDU
MIC
SEQ
ICV
Encrypted


Seed
DA
SA
MSDU
Hash
MIC
TKIP

The following explains how the per packet key is generated:



Creating the RC4 Encryption Key

All the data in phase 1 computation is relatively static – need to re-compute only after 2^16 or roughly 65536 packets.
Phase 2, a quicker computation which includes item that changes every packet.

v.3.Contention-Free Service with PCF

- an optional part of the 802.11 specification
- products not required to implement PCF and few products, if any, implement now
- IEEE 802.11 designed the PCF so that stations that implement only the DCF will interoperate with point coordinator; the point coordinator will coordinate the Contention-Free service
- CF-Free service not provided full-time - Periods of contention-free service alternate with the standard DCF-based service
- Relative size of the contention-free period can be configured

What is Contention-free services?

- Access to the medium is restricted by the point coordinator implemented in the AP
- Associated stations can transmit data only when they are allowed to do so by the point coordinator
  - Similar to token-based networking protocols, with the point coordinator's polling taking the place of a token
  - All transmissions must be acknowledged

- **Frame types used in contention-free services:**
  - **Data – used by AP in sending a frame to a station and does not need to ack**
  - **A previous transmission**
  - **CF-Ack - used by stations to acknowledge the receipt of a frame when no data needs to be transmitted**

Frame types (Cont.)

- **Longer than the control frame ACK, and may not actually be used**
- **CF-Poll – sent by the AP to a mobile station to give the station the right to transmit a single buffered frame**
- **Data + CF-Ack - combines data transmission with an acknowledgment**
- **Data + CF-Poll - sent by the AP to transmit data and request one pending frame from mobile station**
- **CF-Ack + CF-Poll - this frame ack one of the AP's clients and request a buffered frame from the next station in the polling list**
- **Data + CF-Ack + CF+Poll - Data + CF-Ack is sent to the same AP'client, and CF-Poll, to next station in polling list**
- **CF-End - this frame ends the contention-free period and returns control of the medium to the contention-based mechanism of the DCF**
- **CF-End + CF-Ack - same as CF-End, but also ack the previously transmitted frame**

V.4.Current Status of IEEE 802.11 Standards

♦ 802.11 Standard

- **approved: 1997**
- **Initially three physical layers are specified**
  - **two RF links (i.e., Frequency Hoping and Direct Sequence) and one IR (Infrared) link**
  - **IR link currently not popular and rarely used**
- **Data rate: 1 or 2 Mbps**

♦ 802.11b Standard

- **Approved: July 1999**
- **Maximum data rate: 11 Mbps**
- **Uses the middle of ISM bands i.e., 2.4 ~ 2.497 GHz**
- **Benefits: Optimal choices for less dense networks in larger areas**
- **Adoption: More than 98% of current installed base of WLAN in both business and homes**
- **Also being deployed in "hot spots" such as hotels, airports and Starbucks**
- **Cost: lowest cost solution when implementing small wireless networks**
- **Capacity: 32 users per Access Point**

♦ 802.11a

- **Approved: July 1999**
- **Max. Data Rate: 54 Mbps**
- **Modulation: OFDM (Orthogonal Frequency Division Multiplexing)**
- **3 Bands:**

Band type	Freq Range	Power Output
Lower band	5.15 ~ 5.35 GHz	50 mW
Middle Band	5.425 ~ 5.675 GHz	250 mW
Upper band	5.725 ~5.875 GHz	1 W

- **Advantage – Free from interference from 2.4 GHz cordless phones, microwave ovens, etc. operated in the neighborhood; seamlessly coexists with 802.11 b devices**
- **Speed: 2 to 5 times the data rate of 802.11b in a typical office environments up to 255 feet**
- **Density: 802.11a systems have more available non-overlapping channels than 802.11b to allow higher system capacity than 802.11b systems**
- **Cost: Higher price per Access Point, but increased density and throughput potentially lowers costs per user and price per Mbps**
- **Capacity : 64 users per access Point**

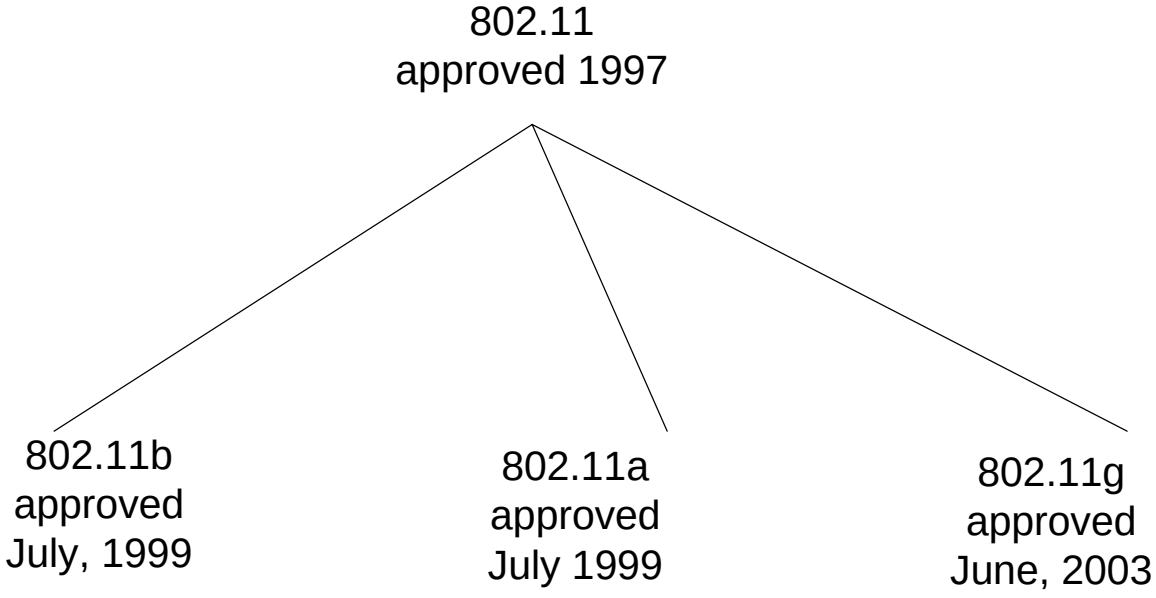
♦ 802.11g

- **Status: approved June 11, 2003**
- **Max data rate: 54 Mbps**
- **Modulation: OFDM and CCK**
- **Band: 2.4 ~2.497 GHz**
- **Backward compatible with 802.11b**

802.11 Compatibility

AP	Client Mobile Station
802.11a	802.11a only
802.11b	Either 802.11b or 802.11g
802.11g	802.11b or 802.11g

Status of 802.11 Standards



♦ Dual Band Offerings

- **Cisco Aironet 1200 Wireless LAN**
  - **Access Point – two adapters, one supports 802.11a community, and the other, 802.11b community**
- **fully IEEE 802.11a and 802.11b compliant for wireless network**
- **Benefits: Ultimate in interoperability and protects existing WLAN investment**
- **Client Adapters (PC Cards, USB & PCI cards) – either 802.11a or 802.11b connectivity**
- **Seamlessly roam – between 802.11b and 802.11a networks**
- **Architecture – eliminates any backward compatibility concerns and preserves infrastructure investment, maintaining overall affordability**
- **Offers both 802.11a and 802.11b along with options of using either**

V.5.802.11 Physical Layer

- **Spread spectrum technique - To reduce the radio interference, government has specified that the ISM band must use spread spectrum**
- **What is Spread Spectrum Communications?**
  - **Developed initially for military and intelligence requirements.**
  - **The essential idea:**
    - **to spread the information signal over a wider bandwidth to make jamming and interception more difficult**

♦ Two Types of Spread Spectrums

- **Direct Sequence Spread Spectrum (DSSS)**
  - **Each bit in the original signal is represented by multiple bits in the transmitted signal, know as chipping code**
  - **The chipping code spreads the signal across a wider frequency band in direct proportion to the number of bits used**
  - **Multiple user data can be transmitted concurrently over exactly the same spread of freq.**
- **Frequency Hopping SS (FHSS)**
  - **A transmission is synchronous between the sending and receiving stations such that they switch channel or hop in a pseudo-random pattern**

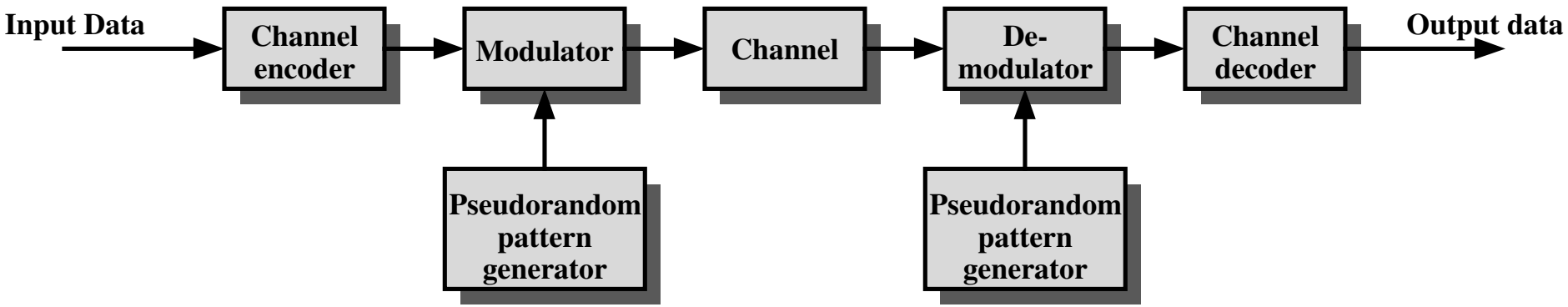
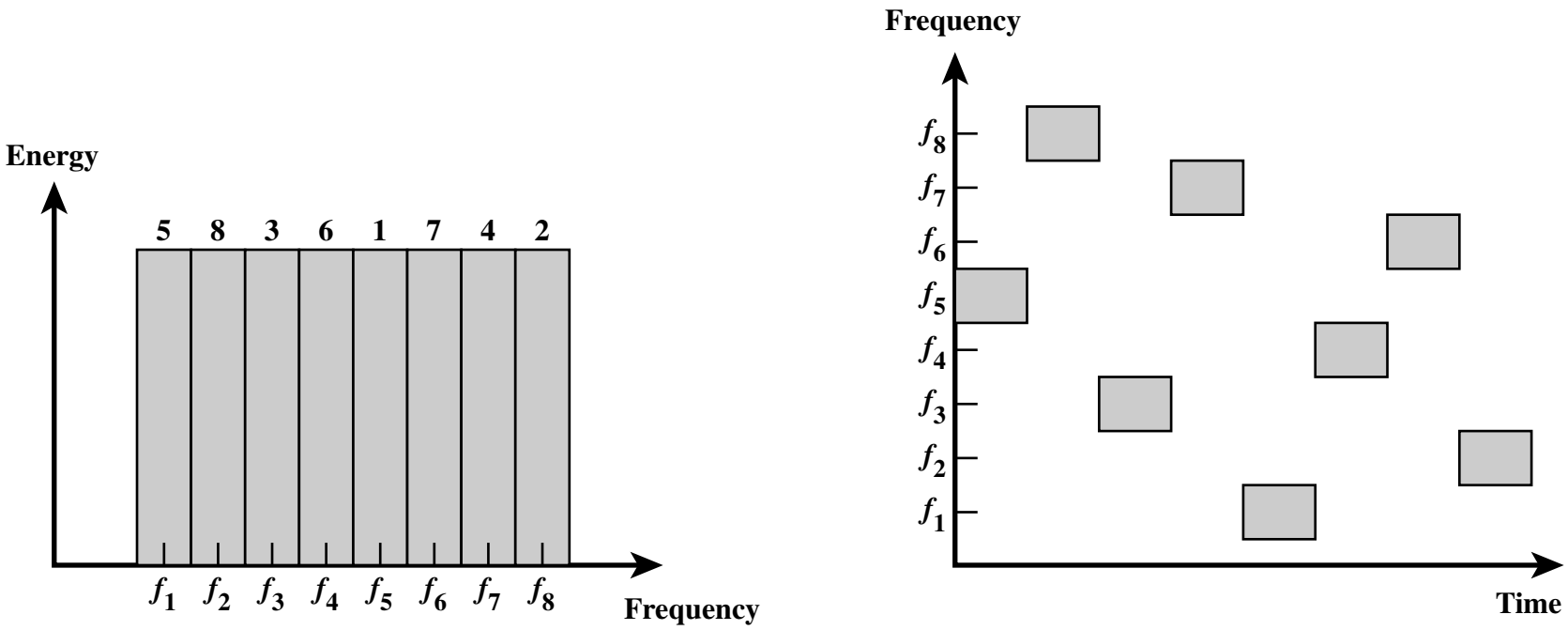
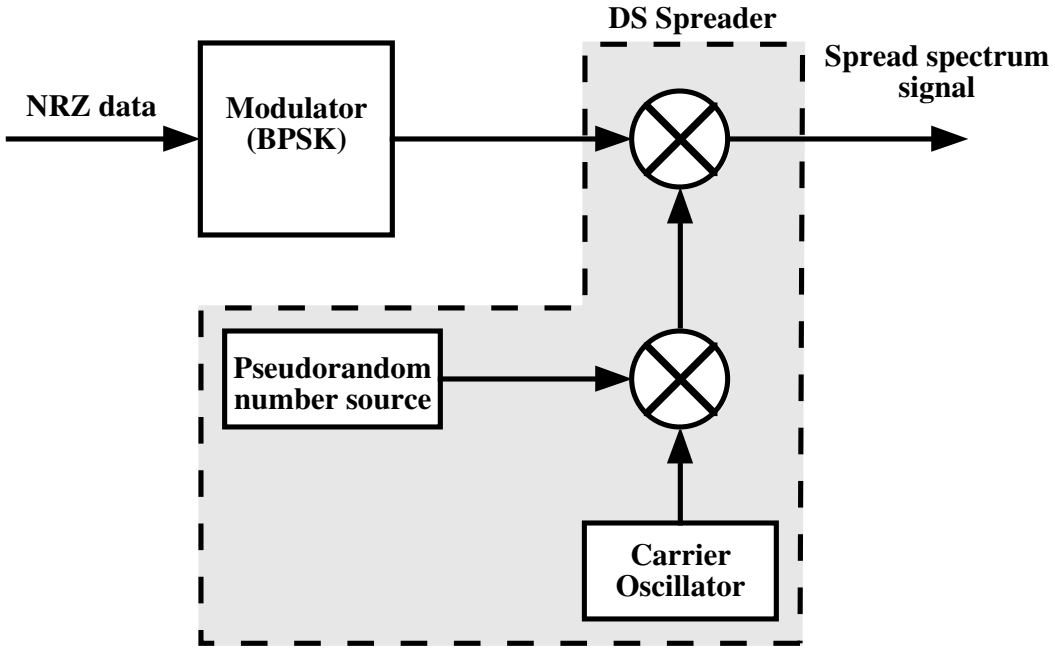


Figure 10.8 General Model of Spread Spectrum Digital Communication System

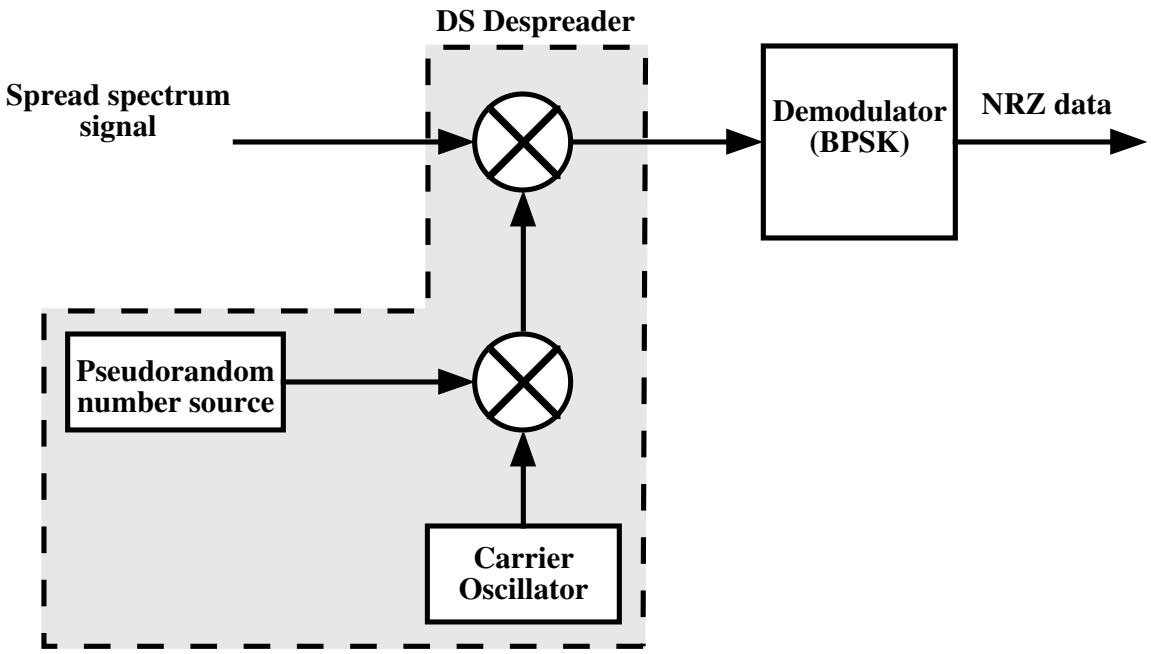


(a) Channel assignment **(b) Channel use**

Figure 10.9 Frequency Hopping Example



(a) Transmitter



(b) Receiver

Figure 10.12 Direct Sequence Spread Spectrum System

VI.802.2 LLC

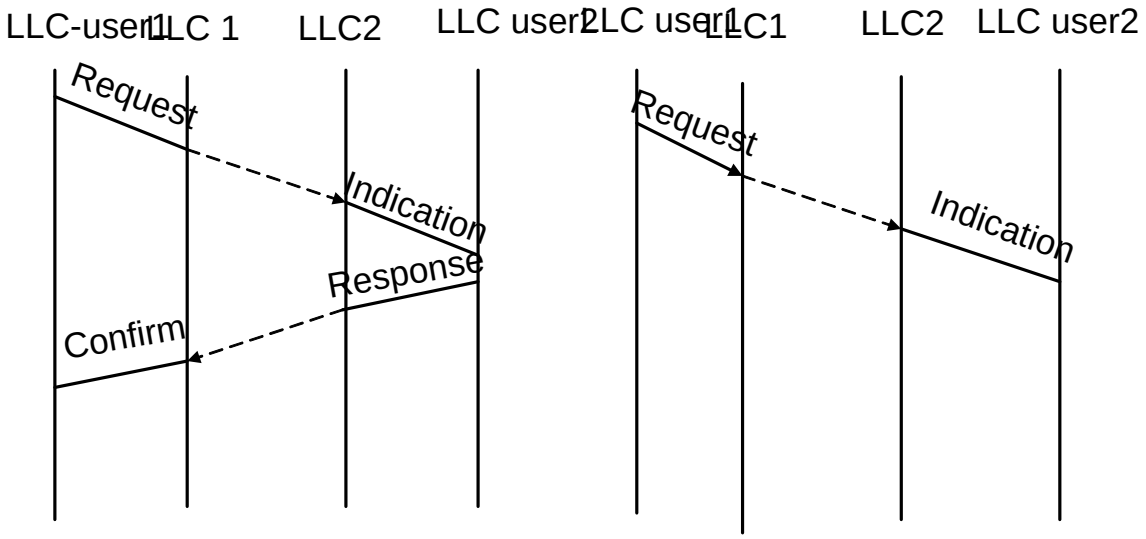
802.2 LLC (Logical Link Control) Sublayer

- **Responsible for medium-independent data link functions**
  - **Allows a LLC user to access the services of a LAN data link services without having to concern with the form of MAC or physical medium used**
- **The data link layer of the OSI model is responsible for the transmission of data from one system to another.**
- **ISO has defined a data link layer protocol, used extensively in WAN, called Higher-level Data Link Control (HDLC).**
- **The LAN Data link protocol is different from those used in WAN; but uses the same HDLC principles.**
- **In IEEE/ISO LAN Architectures, the data link layer is split into 2 sublayers i.e. LLC (Logical Link Control) and MAC (Media Access Control).**
  - **In WAN environment, the DLC concerns 1 to 1 or 1 to N communication**
  - **In LAN environment, it is any-to-any communication.**

LLC-PDU

- **The data unit exchanged between two LLC entities is called LLC-PDU.**
- **LLC sublayer adds PCI (Protocol Control Information) in the form of a header to each message received from LLC user (i.e., LLC-SDU) which creates an LLC-PDU.**

Time Sequence Diagrams for Service Primitives



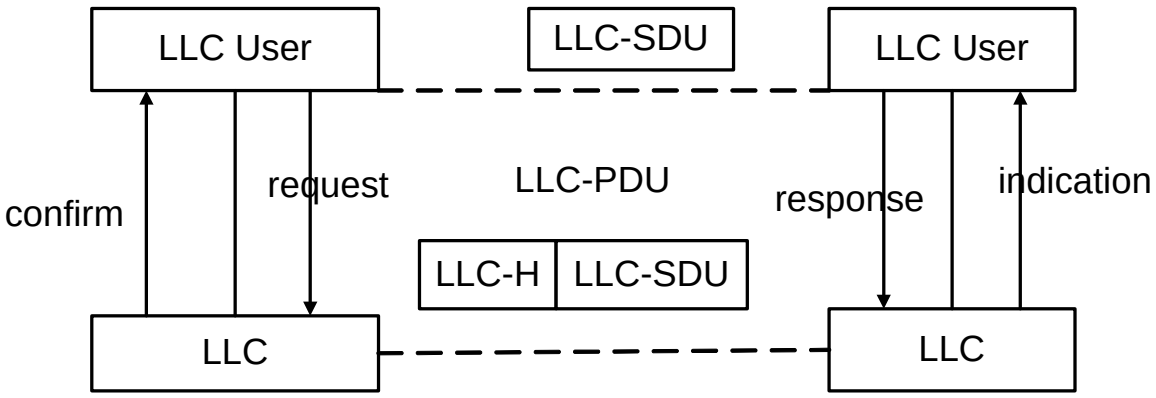
a).Confirmed Service

B). Nonconfirmed service

Time Sequence Diagrams for Service Primitives

LLC Service Definition

- **Provides data transportation service to the LLC users**
- **Service Definition is defined in terms of time sequence diagrams, service primitives and parameters.**
  - **The service primitives are tied to the type of services provided.**
- **Three classes of services:**
  - **Class 1.Unacknowledged Connectionless Service**
  - **Class 2.Connection-oriented Service**
  - **Class 3.Acknowledged Connectionless Service**



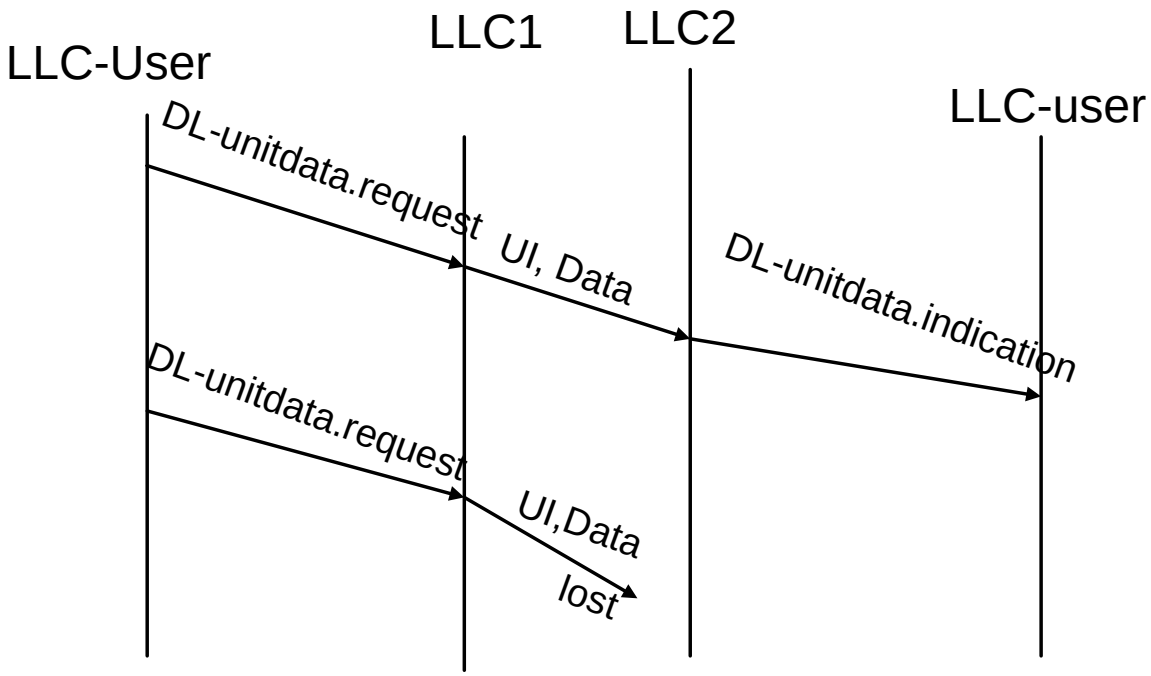
LLC Service Primitives

Service Primitive	Parameters
Unacknowledged Connectionless Service	
DL-UNITDATA.request	Source-address, destinaion-address,data, priority
DL-UNITDATA.indication	Source-address, destinaion-address,data, priority
Connection-Oriented Service	
DL-CONNECT.request	Source-address, destinaion-address, priority
DL-CONNECT.indication	Source-address, destinaion-address, priority
DL-CONNECT.response	Source-address, destinaion-address, priority
DL-CONNECT.confirm	Source-address, destinaion-address, priority
DL-DATA.request	Source-address, destinaion-address,data
DL-DATA.indication	Source-address, destinaion-address,data
DL-DISCONNECT.request	Source-address,destination-address
DL-DISCONNECT.indication	Source-address,destination-address,reason
DL-RESET.request	Source-address,destination-address
DL-RESET.indication	Source-address,destination-address,reason
DL-RESET.confirm	Source-address,destination-address

Logical Link Control Primitives Cont.

- **source-addr and destination-addr: referred to as the LAN data link address**
  - **LAN data link address is a logical combination of MAC addr and SAP addr**
- **For data transmission request, full source and destination addresses must be specified**
- **data : specifies the information to be transmitted**
- **priority : specifies the priority desired for the transmission.**
  - **For 802.3 CSMA/CD and 802.11 CSMA/CA, priority is ignored.**

- **Class 1.Unacknowledged Connectionless Service**
  - **Equivalent to Datagram Service.**
    - **No Link Connection established.**
    - **No flow control or error control mechanisms**
  - **Support individual (i.e., 1 to 1), Multicast, or Broadcast addressing**
  - **Also called 'Unreliable Data Transfer'**
    - **Unreliable means Data Transfer not acknowledged and no guarantee that data will be delivered.**



Unacknowledged Connectionless Service

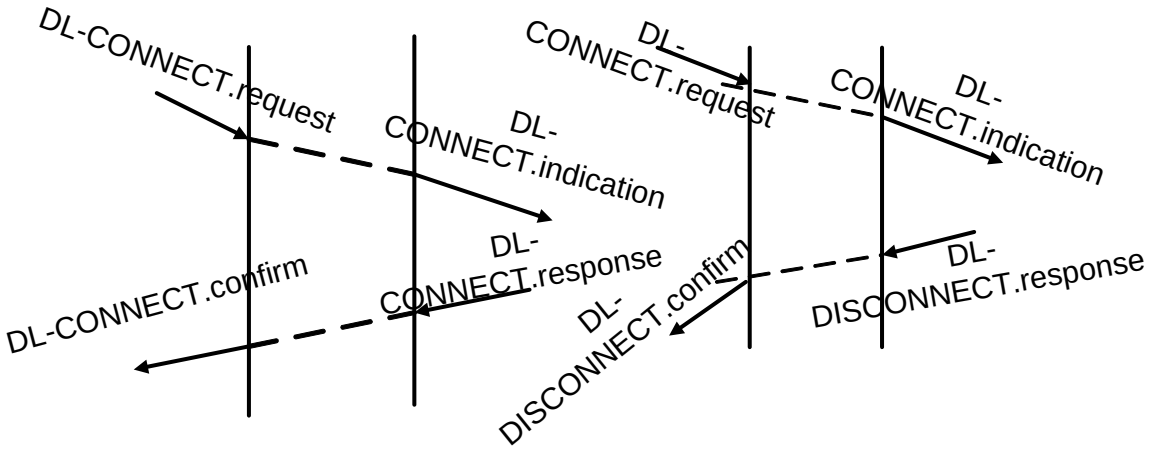
LLC Services Cont.

Class 2 .Connection-Oriented Service

- Allow two communicating users to set up a logical connection for data transfer
- LLC user can request or be notified of the establishment of termination of a logical connection
- Data transfer can only begin after connection is established
- Point-to-point or individual address only
- Provides flow control, sequencing and error recovery
- Also called 'RELIABLE Data Transfer'
  - In LAN environment, RELIABLE data transfer does not always mean it is better than UNRELIABLE data transfer.

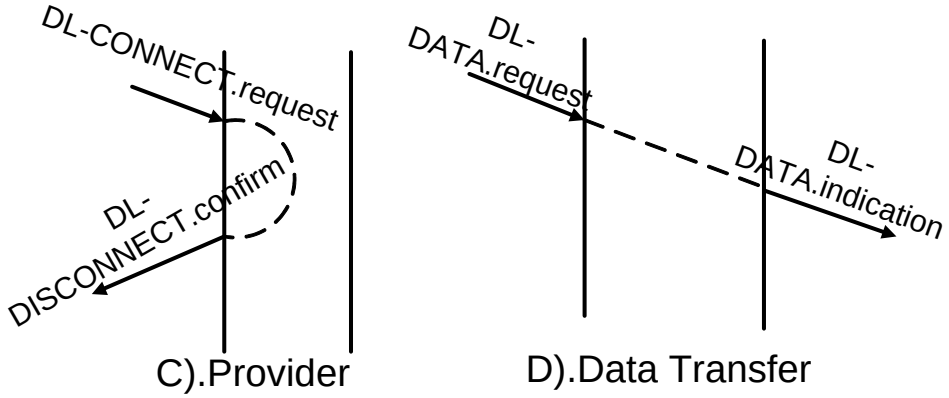
Class 3.Acknowledged Connectionless Service

- Provides a mechanism by which a user can send a unit of data and receive an acknowledgement that the data was delivered, without the necessity of setting up a connection.
- Requires almost as much overhead as connection-oriented service.
  - Suitable for time critical factory environment.
- Point-to-Point Only
- Not a single vendor implements class 3 Acknowledged Connectionless service



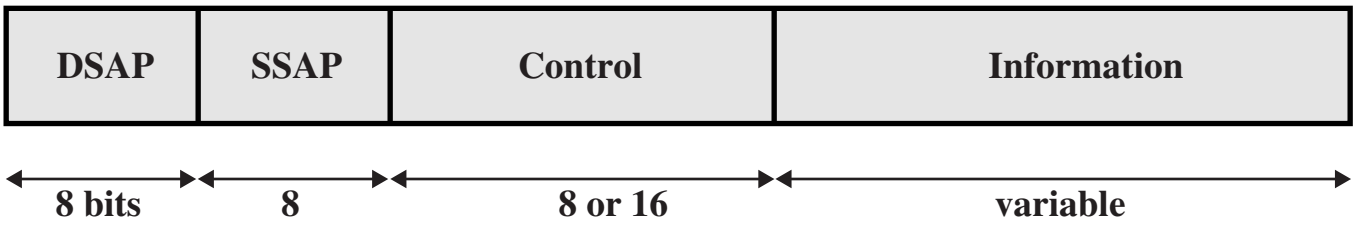
A).Successful connection establishment

B).Remote rejection

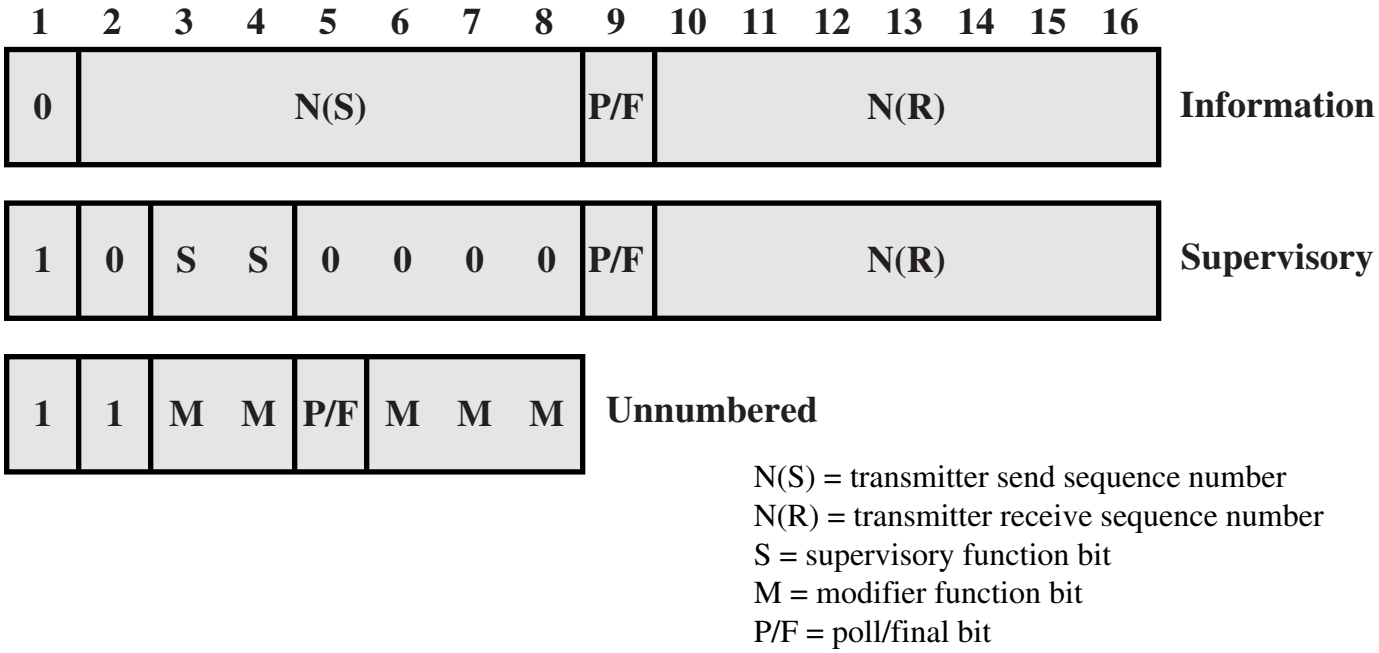


C).Provider Rejection

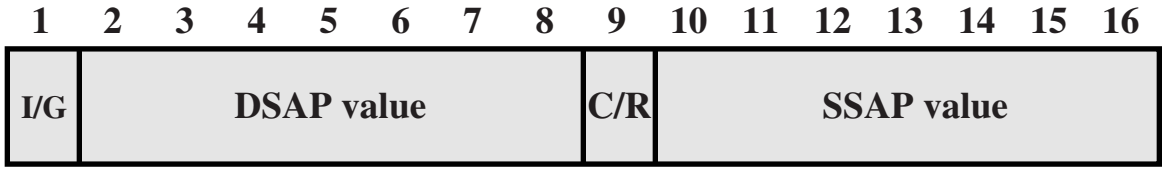
D).Data Transfer



(a) PDU format



(b) Control field formats



(c) LLC address fields

Figure 6.2 LLC Protocol Data Unit Formats

LLC protocol specification

- **Defines both LLC-PDU frame formats and the rules that govern the way the PDUs are exchanged in order to provide the service to the user.**

LLC-PDU Frame Format

- **DSAP (Destination SAP) Address**
  - **Identifies the LLC sublayer user or users that are to receive the LLC-PDU.**
  - **Either an individual address, identifying a single SAP or a group address, a set of SAPs.**
  - **Global SAP address i.e., X'FF', identifies all active SAPs in a station**
- **SSAP (Source SAP) Address**
  - **Always an individual address identifying a single SAP.**
  - **If $(SSAP)_0 = 0$, the LLC-PDU is a command ; if $(SSAP)_0 = 1$, a Response.**
  - **LLC Sublayer User Multiplexing**
  - **SAP address allows different types of LLC users to coexist in the same LAN data link.**

SAP (Service Access Point)

- **LLC users request data transmission service through a SAP into the LLC sublayer.**
- **Normally, an LAN implementation allows more than one user to concurrently access the services of LAN data link.**
- **LLC sublayer has the overall responsibility of controlling the exchanges of messages between individual users of the LLC sublayer service.**

SAP Address

- The LLC sublayer uses the SAP address to ensure that the LLC-PDU is delivered to a proper LAN data link user.

- IEEE Assigned SAP address
  X'FE' -- OSI IP (Internet Protocl)
  X'FF' -- Global SAP

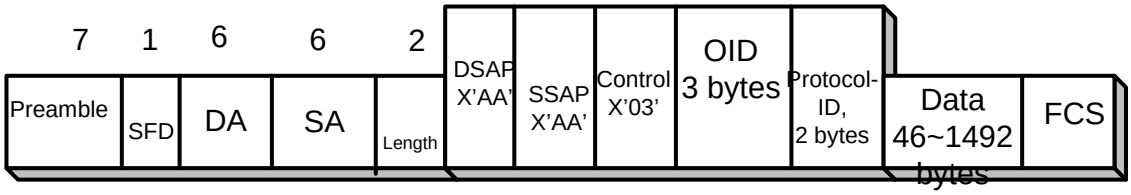
- Example of Vendor Extension -- IBM
  X'04' --SNA
  X'F0' -- NETBIOS
  X'F4' -- NETWORK Management.

$(DSAP)_0 = 0$	Individual SAP Address
$(DSAP)_0 = 1$	Group SAP address
$(DSAP)_1 = 0$	Not IEEE defined
$(DSAP)_1 = 1$	IEEE assigned
$(SSAP)_0 = 0$	Command
$(SSAP)_0 = 1$	Response

SNAP (Subnetwork Access Protocol)

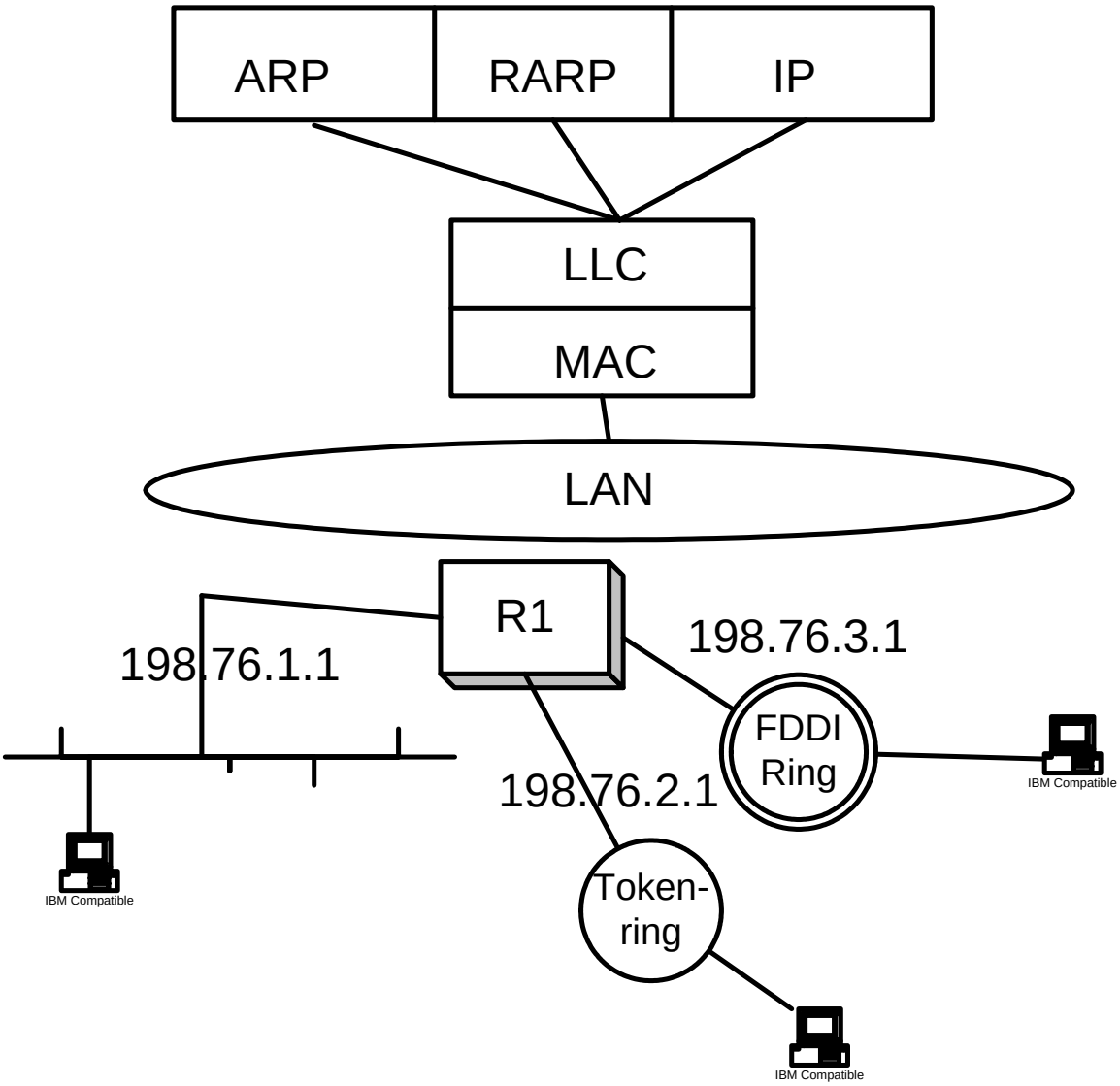
- **X'FE', assigned by IEEE to refer to ISO Internet protocol that operates at OSI Network layer.**
  - **OSI IP practically a dead issue, no LAN data link traffic today in existence conforms to OSI IP standard.**
- **SNAP, an extension of SAP concept which is defined by an IEEE**
- **Intended for use with private network layer protocol like DoD TCP/IP or IPX in Novell Netwares products.**
  - **SNAP-PDU consists of a header, 5 bytes in length.**
  - **The 1st three bytes of the header, organization-ID, identifies the organization, the remaining 2 bytes, protocol ID, identifies a special protocol like ARP, RARP or IP.**
  - **If SNAP is used, then DSAP = SSAP = X'AA' and control = X'03'**

IEEE 802.2 LLC PDU layout with SNAP



Address Resolution Protocol (ARP) Example

- **The ARP request is broadcast to all the stations in the physical network; any station which recognizes the destination IP address is mandatory required to send ARP Response back to the sending station**
- **After the two-way communication, destination MAC address is known**.



LLC Protocol Specification

- An LLC-PDU can take the form of either a command or a response. A command is sent by an LLC entity that is initiating a request or a data transfer operation. A response is sent by the distant LLC entity on reply to a command.
- The first bit of SSAP i.e., $(SSAP)_0$ indicates whether it is a command or a response.
- If $(SSAP)_0 = 0$, it is a command else a response.

Types of LLC-PDU

- **3 types of LLC-PDUs i.e., I-Format, S-Format and U-Format.**
- **Each type of LLC-PDU is identified by a unique CONTROL component.**
  - **Information LLC-PDUs (I-Format)**
    - **CONTROL field is 2 bytes in length; 7 bits for Ns (Next to Send) , 7 bits for Nr (Next to Receive), 1 bit for P/F**
    - **The primary function of I-format PDU is to carry user data. However, occasionally, also performs control function.**
  - **Supervisory LLC-PDUs (S-Format)**
    - **CONTROL field is 2 bytes in length; 7 bits for Nr (Next to Receive).**
    - **To carry information necessary to control the operation of the LLC sublayer protocol**
  - **Unnumbered LLC-PDUs (U-Format)**
    - **CONTROL field is 1 byte in length; No sequence number is included in the CONTROL component.**
    - **Either to carry user data or to perform special functions.**

- **I-format LLC-PDU CONTROL Field format**
  - **7 bits for Ns, 7 bits for Nr**
- **S-format LLC-PDU CONTROL field format**
  - **7 bits for Nr (Next to Receive)**
- **U-format LLC-PDU CONTROL Field format**
  - **No Ns or Nr is included**

Command	Meaning
UI	Unnumbered Information
XID	Exchange Identification
TEST	Loop-back test
RR	Receive Ready
RNR	Receive not ready
REJ	Reject
SABME	Set asynchronous balance mode extended
DISC	Disconnect
UA	Unnumbered acknowledgement
DM	Connection rejection
FRMR	Frame reject

a). Unacknowledged Connectionless Service

Unnumbered (U)	Command/ Response	
UI	C	Exchange user data
XID	C/R	Type of operation and window size information
TEST	C/R	Loop-back test

b).Connection-oriented Service

Information Frame		
I	C	Exchange user data
Supervisory Frame		
RR	C/R	Positive acknowledgement; ready to receive
RNR	C/R	Not ready to receive; request on hold
REJ	C/R	go back N
Unnumbered Frame		
SABME	C	Connection Request
DISC	C	Connection Termination request
UA	C	Unnumbered acknowledgement
DM	C	Connection Rejection
FRMR	R	Reports receipt of unacceptable frame

Types of LLC Protocol Operation

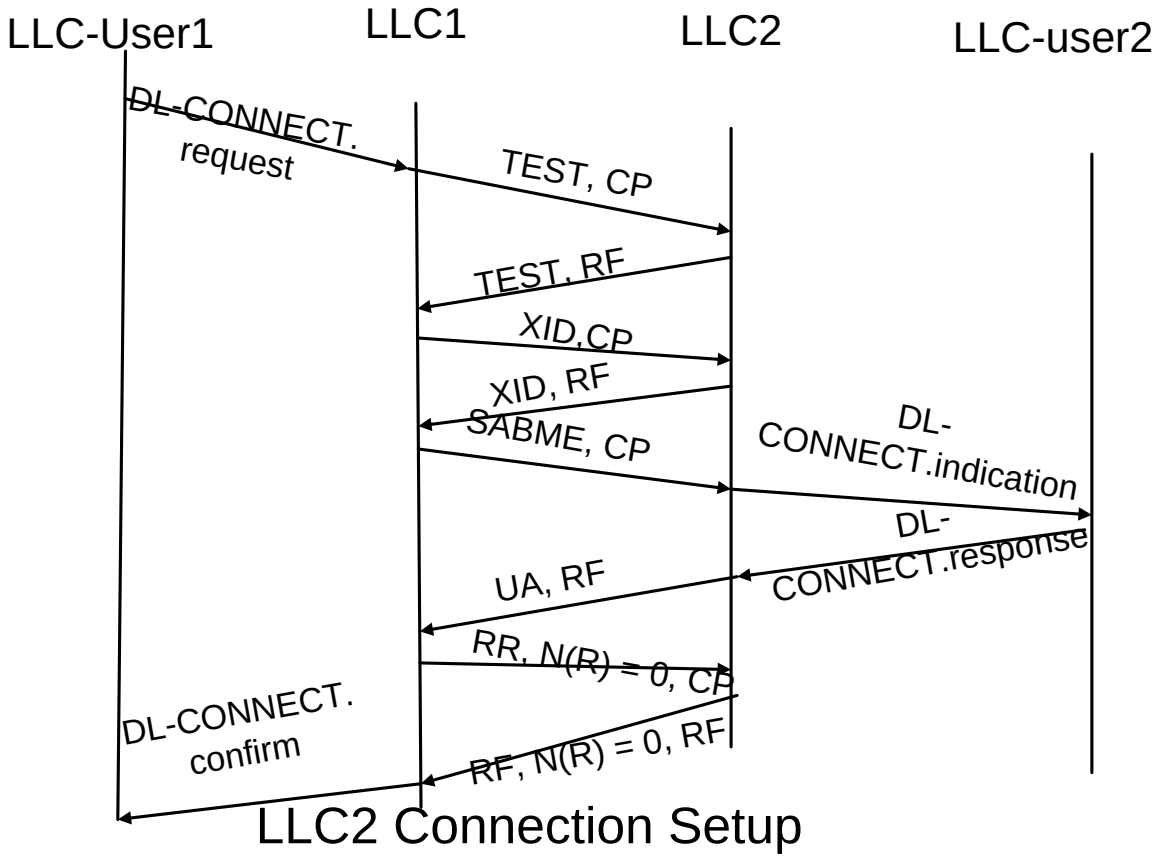
- **Type 1 Operation**
  - **Provides the connectionless LLC service**
- **Type 2 Operation**
  - **Provides the connection-oriented LLC service**
- **Type 3 Operation**
  - **Provides the acknowledged connectionless service.**

$(SSAP)_0$	P/F	Meaning
0	0	CNP : command no Poll
0	1	CP : command Poll
1	0	RNF: Unsolicited Response
1	1	RF : Solicited Response

LLC-PDUs for type 1 Operation

- **Unnumbered Information (UI)**
  - **UI commands and responses are used to convey user data between a pair of LLC entities.**
- **Exchange Identification (XID)**
  - **XID commands and responses are used to exchange information between a source and a destination LLC entity e.g., to find out the types of services provided, or to negotiate window-size.**
- **TEST**
  - **TEST commands and responses are used to conduct a loopback test of the transmission path between two LLC entities.**

Time Sequence Diagram for Service Primitives



LLC2 Connection Setup

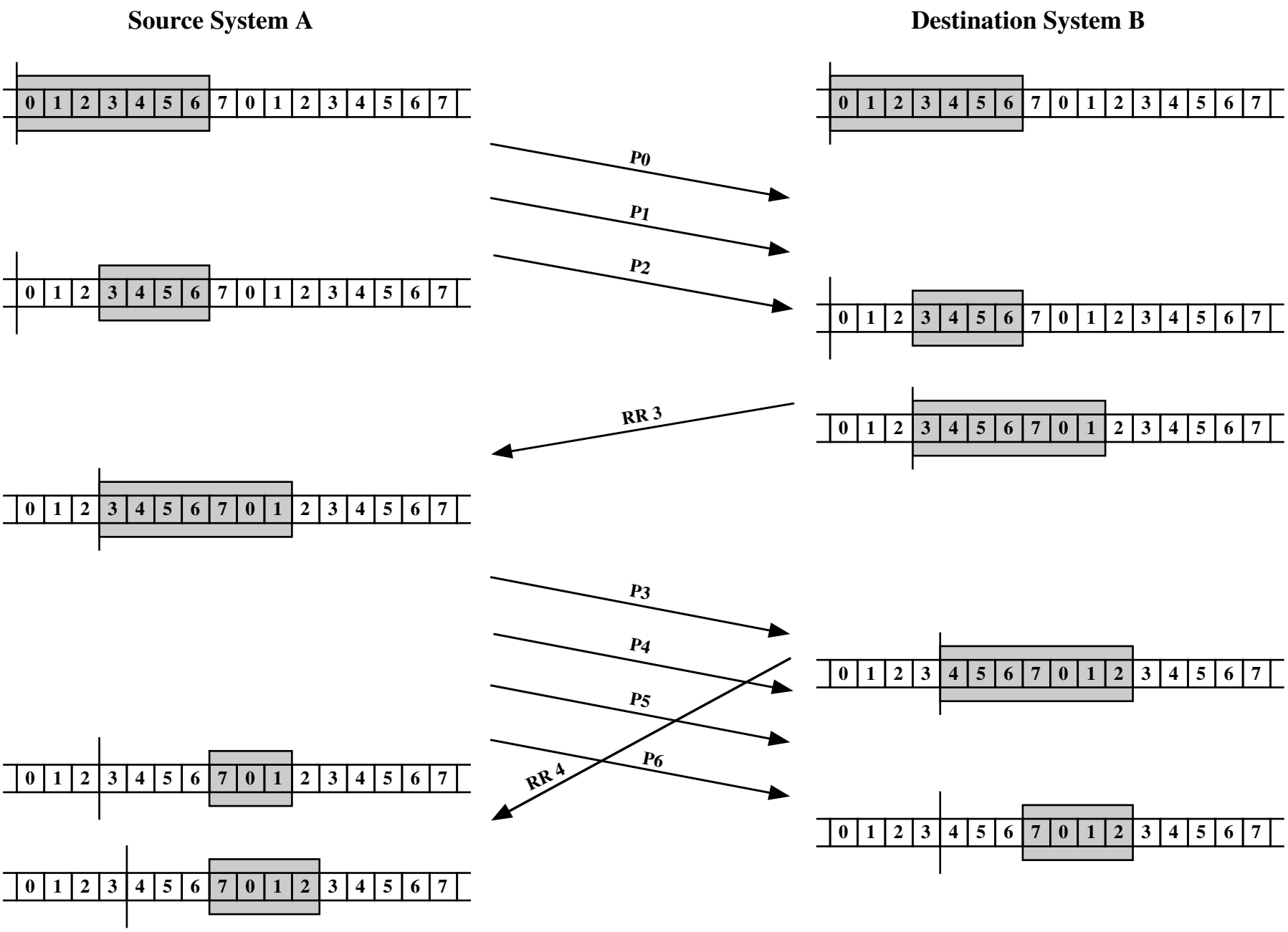


Figure 6.8 Example of a Sliding-Window Protocol

LLC-PDUs for Type 2 Operation

♦ I-format LLC-PDUs

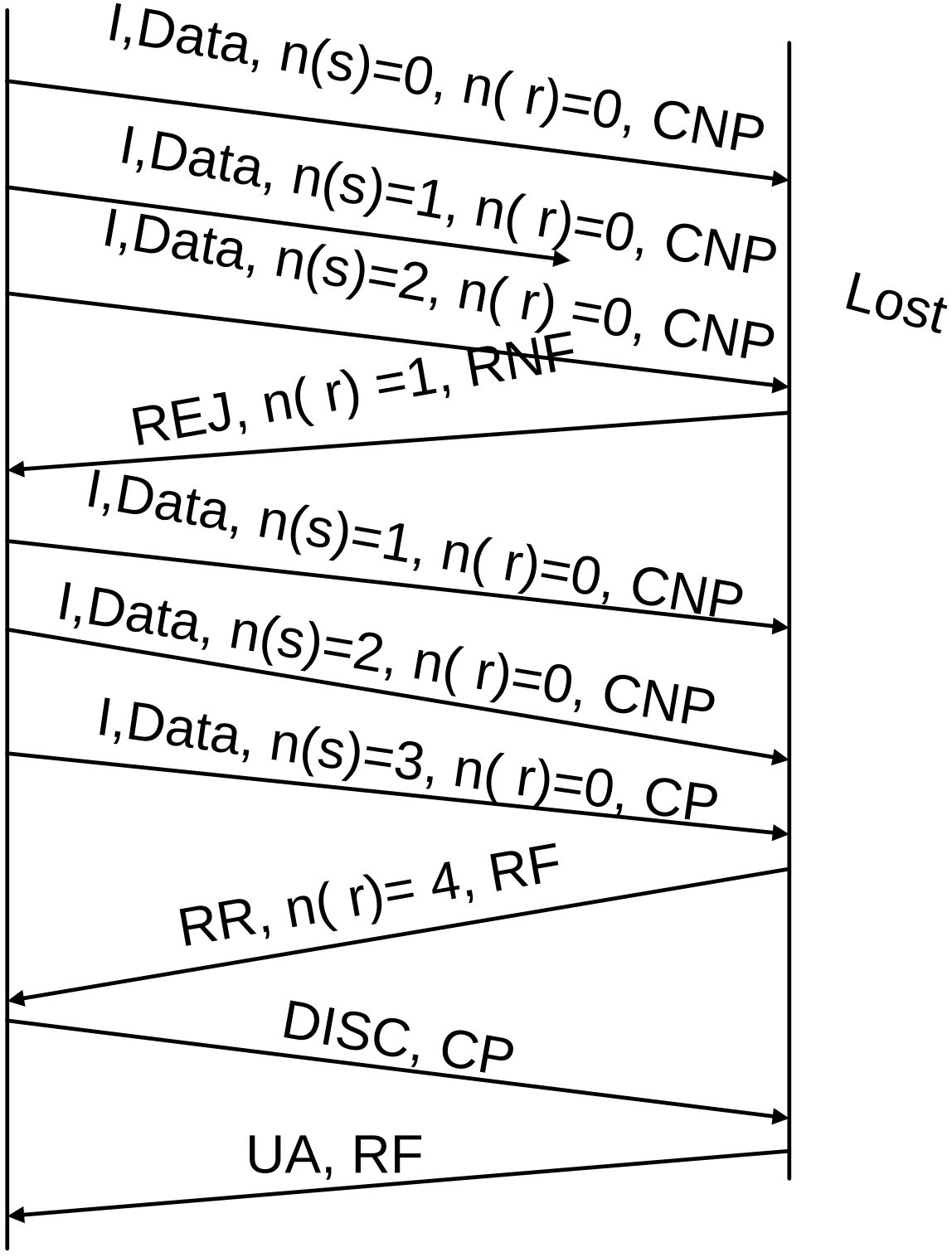
- **I-format LLC-PDU commands and responses are used to transfer user data between two communication LLC entities.**

♦ S-format LLC-PDUs

- **Receiver Ready (RR)**
  - **A RR response is used as an acknowledgment to the previous data transfer when there is no reverse traffic.**
  - **May also be used to indicate that the LLC entity is ready to resume receiving additional data after LLC-PDU transmission has been halted.**
- **Receiver Not Ready (RNR)**
- **Used to acknowledge receipt of an LLC-PDU and also to ask the sending end to halt transmission I-format LLC-PDU.**
- **RNR is used to handle possible internal constraints, such as lack of buffer space.**
- **Reject (REJ)**
  - **To reject an LLC-PDU and to ask that it and any subsequent LLC-PDU be retransmitted**

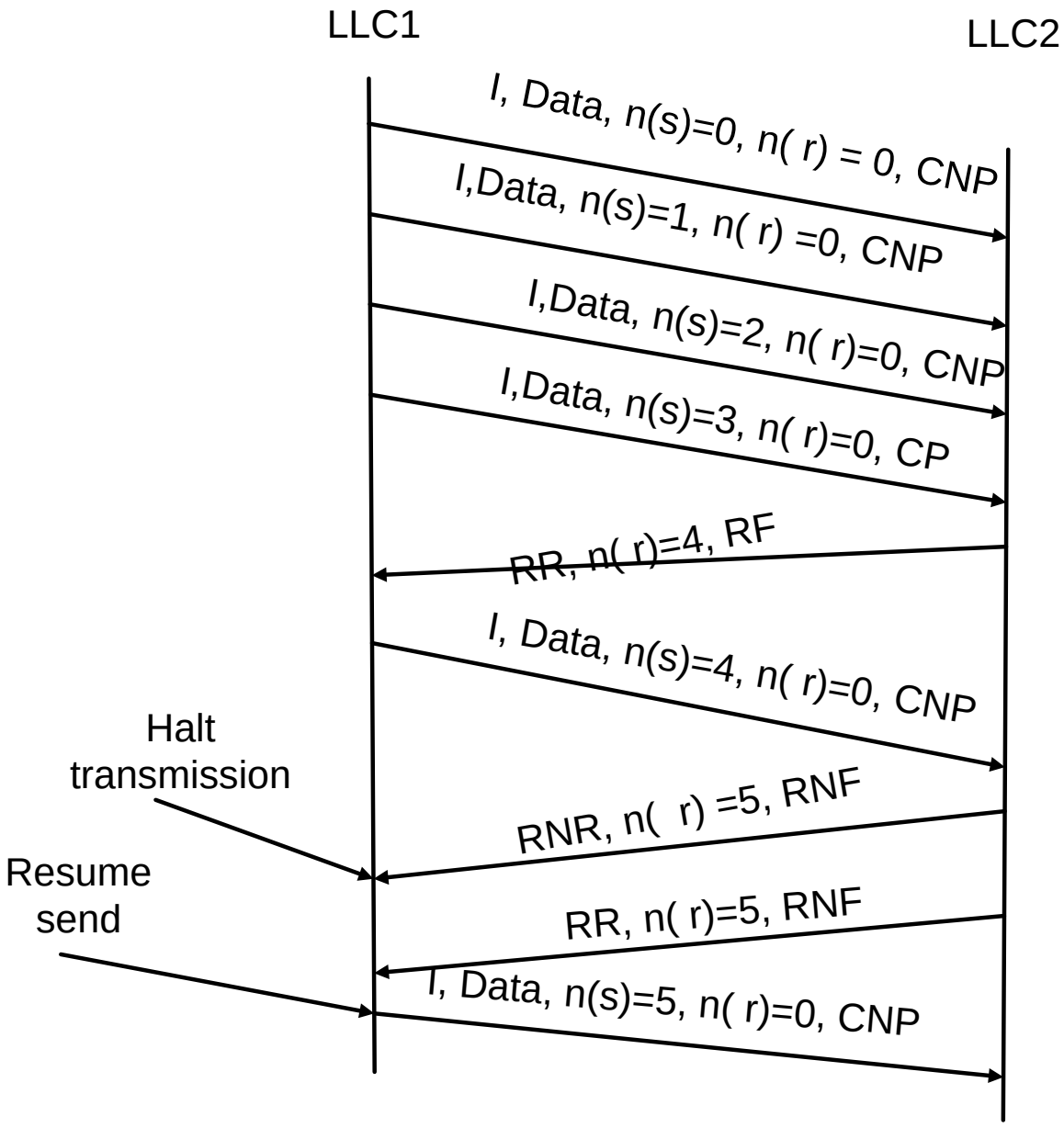
LLC-PDUs for Type 2 Operation (cont.)

- **U-Format LLC-PDU**
  - **Set Asynchronous Balanced Mode Extended (SABME)**
    - **To request the establishment of a link connection between a pair of LLC entities**
  - **Disconnect Mode (DM)**
    - **Sent as a response to reject LLC connection request**
  - **Frame Reject (FRMR)**
    - **FRMR is sent if destination LLC entity is unable to handle an LLC-PDU received, either invalid or not implemented**
    - **An invalid sequence number or has an information field that exceeds the maximum size.**
  - **Unnumbered Acknowledgment (UA)**
    - **Sent by a destination LLC sublayer as a positive acknowledgment**
  - **Disconnect (DISC)**
    - **To request the termination of a connection between a pair of LLC entities.**


I,Data, n(s)=0, n(r)=0, CNP
I,Data, n(s)=1, n(r)=0, CNP
I,Data, n(s)=2, n(r) =0, CNP
Lost
REJ, n(r) =1, RNF
I,Data, n(s)=1, n(r)=0, CNP
I,Data, n(s)=2, n(r)=0, CNP
I,Data, n(s)=3, n(r)=0, CP
RR, n(r)= 4, RF
DISC, CP
UA, RF

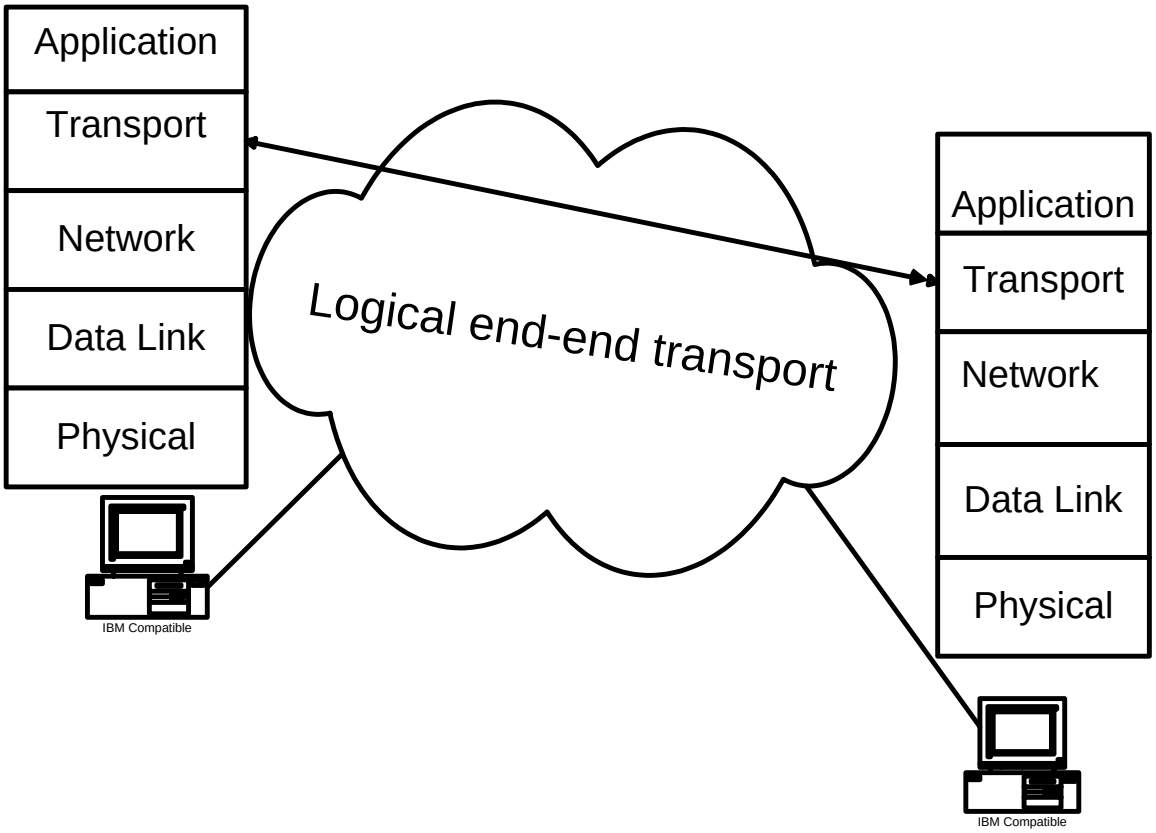
Potential usage of RNR and RR

- When receiving end LLC is congested, it can issue RNR requesting the sending end to HALT transmission
- When congestion is cleared, it can send RR to request for resumption of transmission


LLC1
LLC2
I, Data, n(s)=0, n(r) = 0, CNP
I,Data, n(s)=1, n(r) =0, CNP
I,Data, n(s)=2, n(r)=0, CNP
I,Data, n(s)=3, n(r)=0, CP
RR, n(r)=4, RF
I, Data, n(s)=4, n(r)=0, CNP
Halt transmission
RNR, n(r) =5, RNF
Resume send
RR, n(r)=5, RNF
I, Data, n(s)=5, n(r)=0, CNP

VII.Transport Services and Protocols

- **Provides logical communication between app's processes running on different hosts**
- **Transport protocols run in end systems**
- **Transport versus network layer services**
  - **Network layer: data transfer between two end-systems**
    provide only datagram service
  - **transport layer: data transfer between two processes or app's**
    - **relies on, but enhances network layer services**
    - **provides both connection-oriented and connectionless services**



Transport Protocol

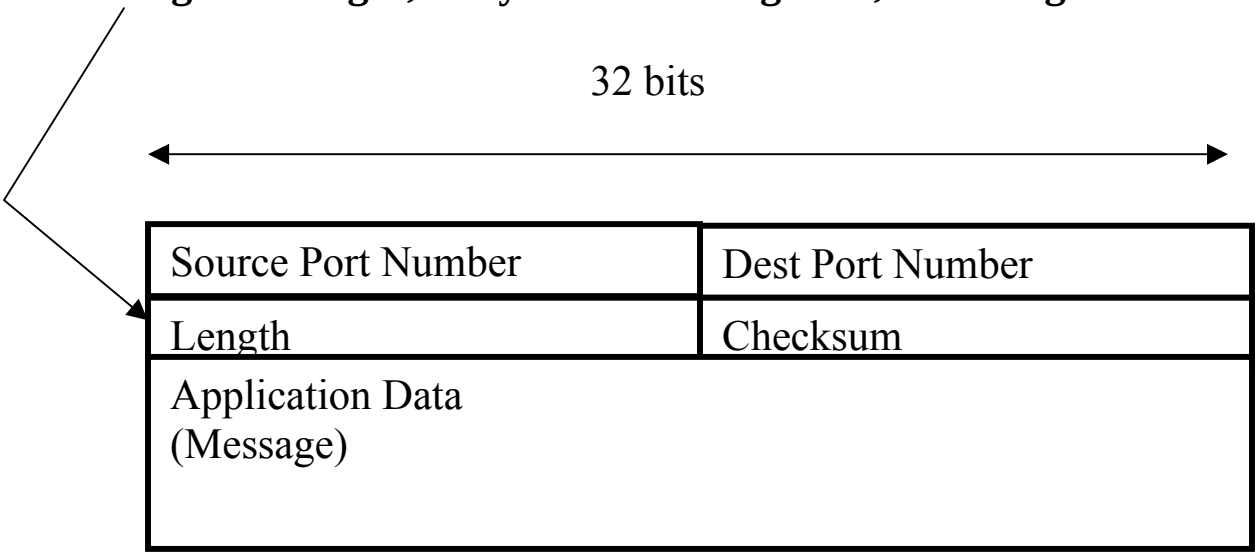
- **User Datagram Protocol (UDP) provides datagram service**
- **Transmission Control Protocol (TCP) provides reliable data transfer or connection-oriented service**

User Datagram Protocol (UDP)

- **UDP delivers independent messages, called datagrams between applications or processes on host computers**
- **Best effort delivery – no guaranteed that data will be delivered**
- **Checksum (optionally) guarantees integrity of data**
- **Endpoints of UDP are called ports – port is a binary integer between 1 and (2**16-1)**
- **Each UDP data transmission identifies a pair of sockets; a socket is a 2-tuple vector**

  i.e., <IP address, port number>
- **IP address identifies the host, and port number, a UDP port or process**

Length: Length, in bytes of UDP segment, including header



UDP headers

- UDP datagrams have a header that follows the hardware and IP headers:

H/W header	IP Header	UDP header	UDP Data	H/W trailer

- UDP header very simple:
  - Port numbers (i.e., source port and destination port) are a 16-bit binary integer (between 1 and 2**16-1)
  - Message length: length in bytes of UDP segment, including header
  - Checksum : detect "errors" in transmitted segment

UDP Checksum

Sender	receiver
Treat segment contents as sequence of 16-bit integers	Compute checksum of received segment
Checksum: 1's complement sum of segment contents Sender put checksum value into UDP checksum field	Check if computed checksum equals checksum field value: No – error detected, and UDP datagram discarded Yes – no error detected But maybe still errors

Why is there a UDP?

- No connection establishment
  - Connection establishment adds delay
- Simple: no connection state at sender, receiver
- Small UDP header, more efficient
- Better throughput
  - No acknowledgement, flow control and congestion control, source can pump data as fast as it could without waiting for the feedback from destination
- Can be 1-1 or 1-N, suitable for certain types of apps
- Certain app can tolerate occasional data loss

Selecting UDP port numbers

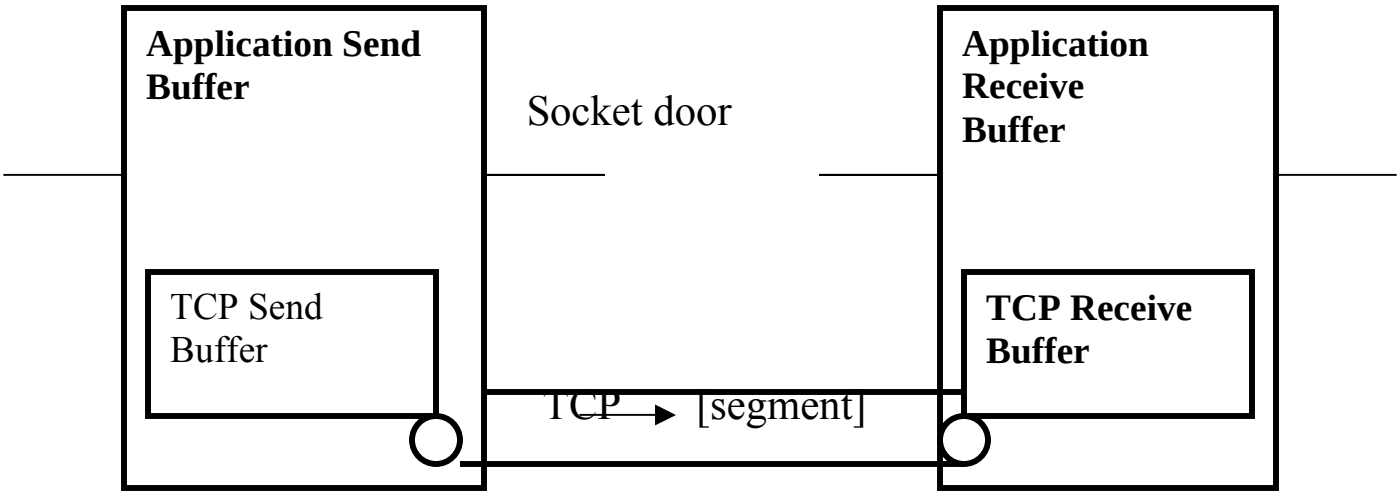
- Communicating computers must agree on a port number
- ``Server'' opens selected port i.e., reserved and well-know port, and waits for incoming messages
- ``Client'' selects local port and sends message to selected port
- Services provided by many computers use reserved, well-known port numbers as showing in the following table.
- Other services use dynamically assigned port numbers

Well-known port numbers

Port	Name	Description
7	echo	Echo input back to sender
13	daytime	Time of day (ASCII)
80	http	Web Server
53	domain	DNS

TCP Overview

- **connection-oriented:**
  - **Connection must be established before data transfer can begin**
  - **When communication is completed, connection must be terminated**
- **Point-to-point or 1-1:**
  - **One sender, one receiver**
- **100% Reliability**
  - **Use 'Acknowledgement and Retransmission' to achieve 100% reliability**
  - **For each TCP segment transmitted, sender also starts a timer.**
    - **If no Ack received within timeout period, sender retransmits the TCP segment**
- **Stream Interface**
  - **TCP considers data is sequenced but unstructured**
  - **Every byte of data has a sequence number**
- **Flow controlled**
  - **Using sliding window flow control to prevent sender from overwhelming receiver**
- **Full-duplex session protocol**
  - **Bi-directional data flow in the same connection**
- **Graceful session setup**
  - 3 way handshakes for session setup
- **Orderly session termination**
  - no TCP data lost


Application Send Buffer
Socket door
Application Receive Buffer
TCP Send Buffer
TCP Receive Buffer
TCP
[segment]

TCP segment structure

32 bits

Source port #			Dest port #
Sequence number			
Acknowledgement number			
Headler-length	Reserved, not used	syn,ack,fin,rst,psh,urg	RCVR window Size
Checksum			Ptr Urgent Data
Options (Not used)			
Application Data (variable length)			

Note:

Flag = (syn, ack,fin,rst,psh,urg)

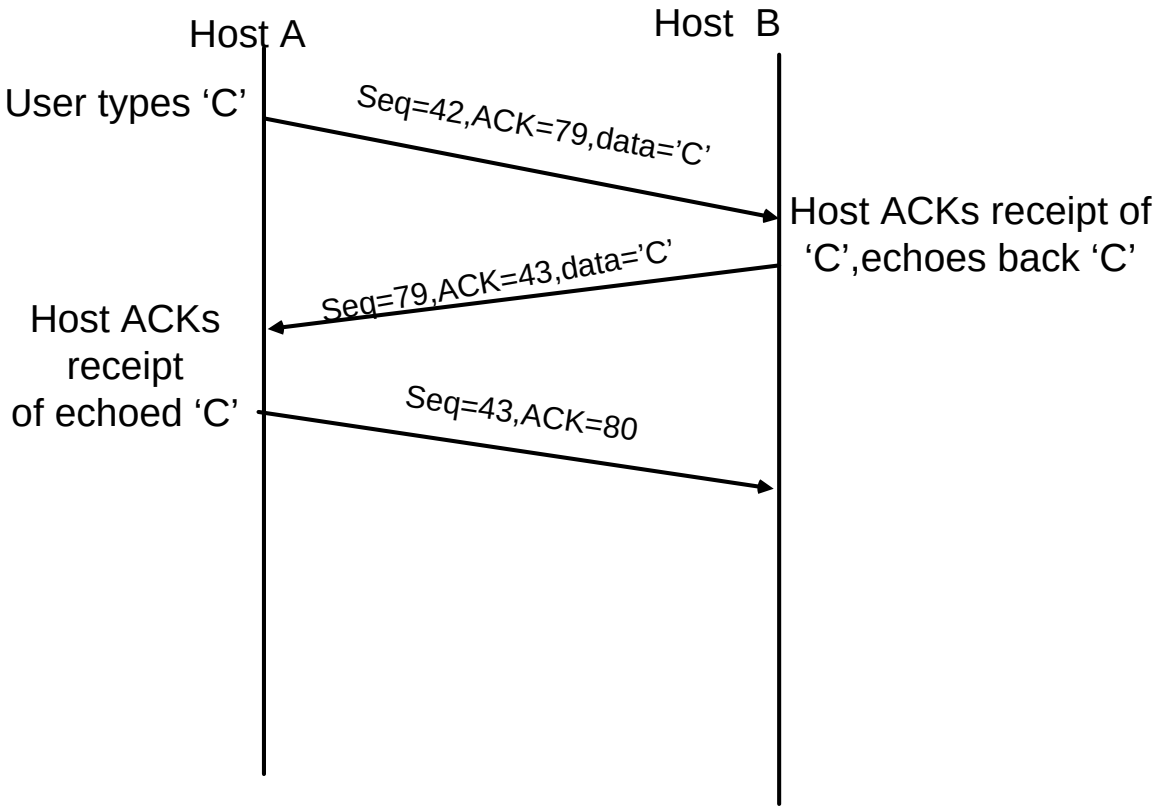
- **If syn=1, request to set up TCP connectin**
- **If ack=1, then ack-no contains valid acknowledgement number**
- **If fin=1, request to terminate the TCP connection**
- **If rst=1, request to reset the TCP connection**
- **Urg and psh, both are not used**

TCP Seq.#'s and ACK#

- **Seq.#'s:**
  - **Sequence number of first byte of data in the TCP segment**
- **ACK#:**
  - **Seq # of next byte of data expected from other side**
  - **Receiver acknowledges correct receipt of all data up to ACK# -1**

Q:how does receiver handles out-of-order segments

- **Up to the implementer, TCP spec does not say**



TCP:reliable data transfer

- Simplified sender, assuming one way data transfer
- No flow or congestion control

event	TCP action
Data received from app above	Create and send TCP segment; also starts timer for the transmitted segment
Timer timeout for segment with seq # =y	Retransmit the segment with seq# = y
ACK received, with ACK# = y	ACK processing

TCP: reliable data tranfer

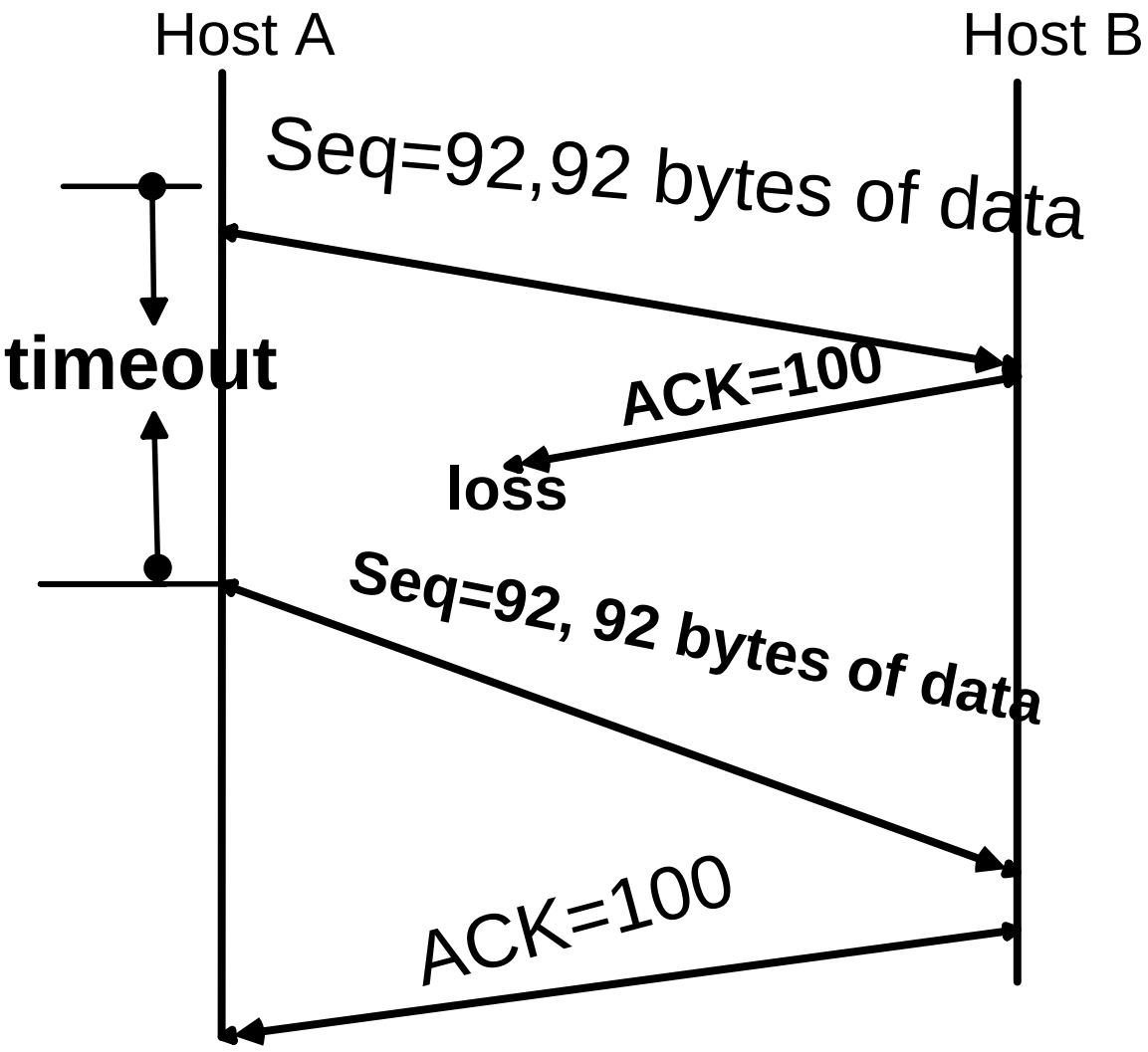
```
sendbase      =  initial_sequence number
nextseqnum =  initial_sequence number

loop (forever) {
   switch(event)
   event: data received from app above
        /* TCP create segment, start timer and send out the
                    segment     */
      create TCP segment with sequence number nextseqnum
      start timer for segment nextsequm
      pass segment to IP
      nextseqnum = nextseqnum + length(data)

   event: timer timeout for segment with sequence number y
     retransmit segment with sequence number y
      compute new timeout interval for segment y
      restart  timer for sequence number y

    event: ACK received, with ACK number = y
       if (y > sendbase) { /*cumulative ACK of all data up to y  */
        cancel all timers for segments with sequence numbers < y
        sendbase = y
       }
       else { /* a duplicate ACK for already ACKed segment */
          increment number of duplicate ACKs   received for y
          if (number of duplicate ACKs received for y ==3) {
             /* TCP fast retransmit    */
             resend segment with sequence number y
             restart timer for segment y
          }
  }   /*end of loop forever   */
```

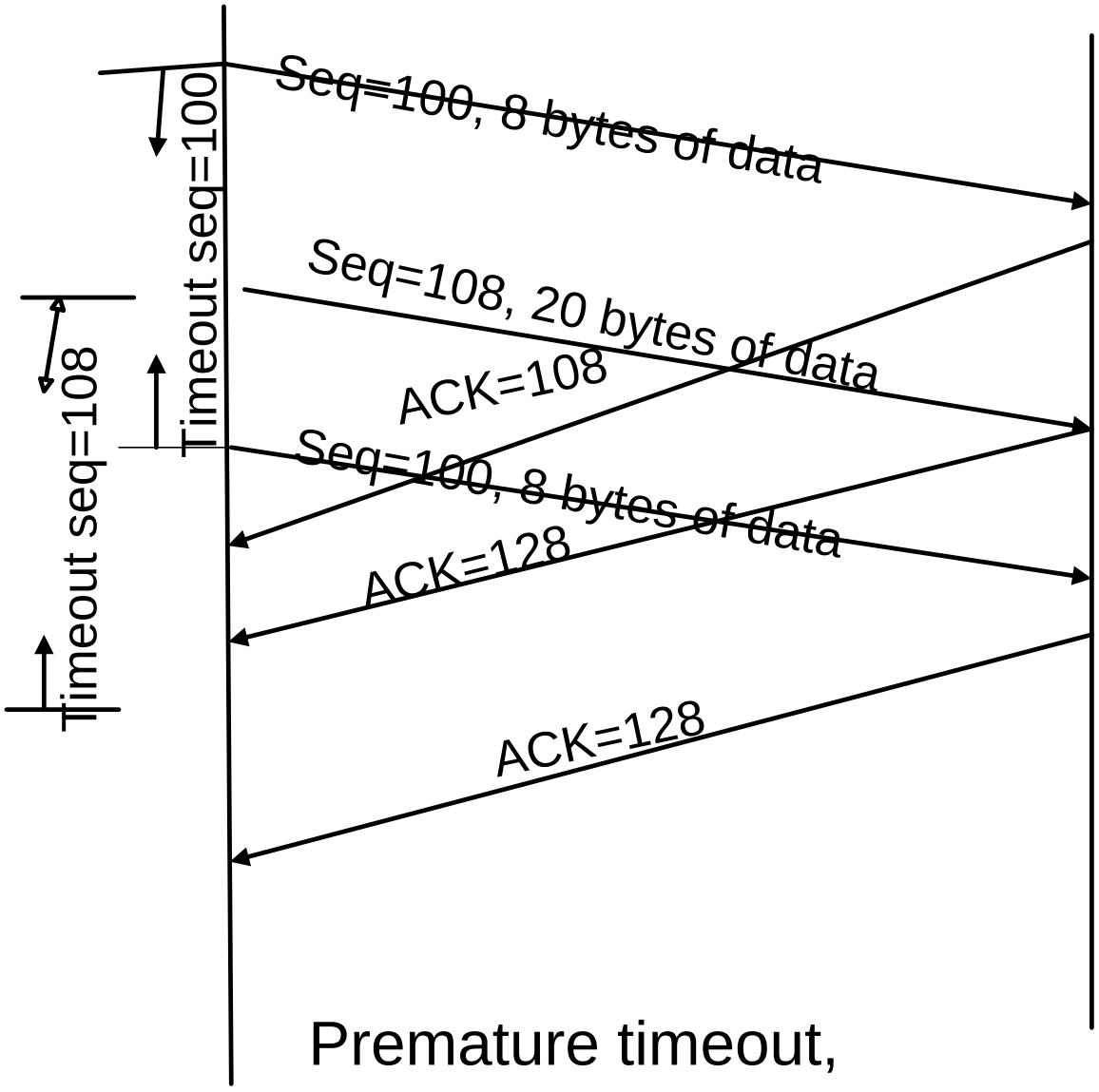
TCP ACK generation
RFC 1122, RFC 2581

Event	TCP Receiver action
In-order segment arrival, no gaps, everything else already ACKed	Delayed ACK. Wait up to 500 ms for next segment. If no next segment, send ACK
In-order segment arrival, no gaps, one delayed ACK pending	Immediately send single cumulative ACK
Out-of-order segment arrival Higher-than-expect seq.# gap detected	Send duplicate ACK, indicating seq.# of next expected byte
Arrival of segment that partially or completely fills gap	Immediate ACK if segment starts at lower end of gap

TCP: retransmission scenarios

TCP: retransmission scenarios





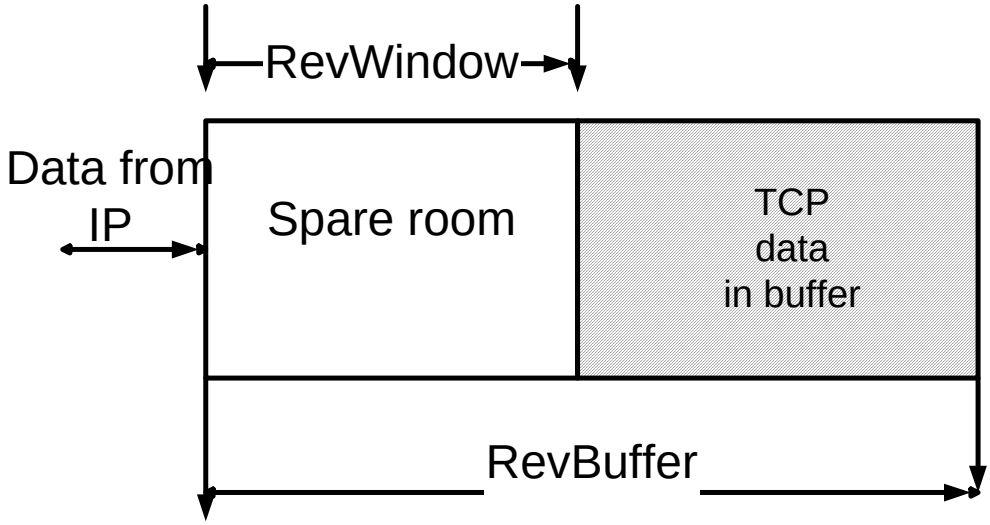
Premature timeout, cumulative ACKs

TCP Flow Control

- **Purpose: sender won't overrun receiver's buffers by transmitting too much, too fast**
- **Receiver: explicitly informs sender of (dynamically changing) amount of free buffer space**
  - **Window-size or RevWindow**
  - **RevBuffer = size of TCP Receiver Buffer**
  - **RevWindow = amount of spare room in buffer**
  - **Sender: keeps the amount of transmitted, unACKed data less than most recently received window-size**

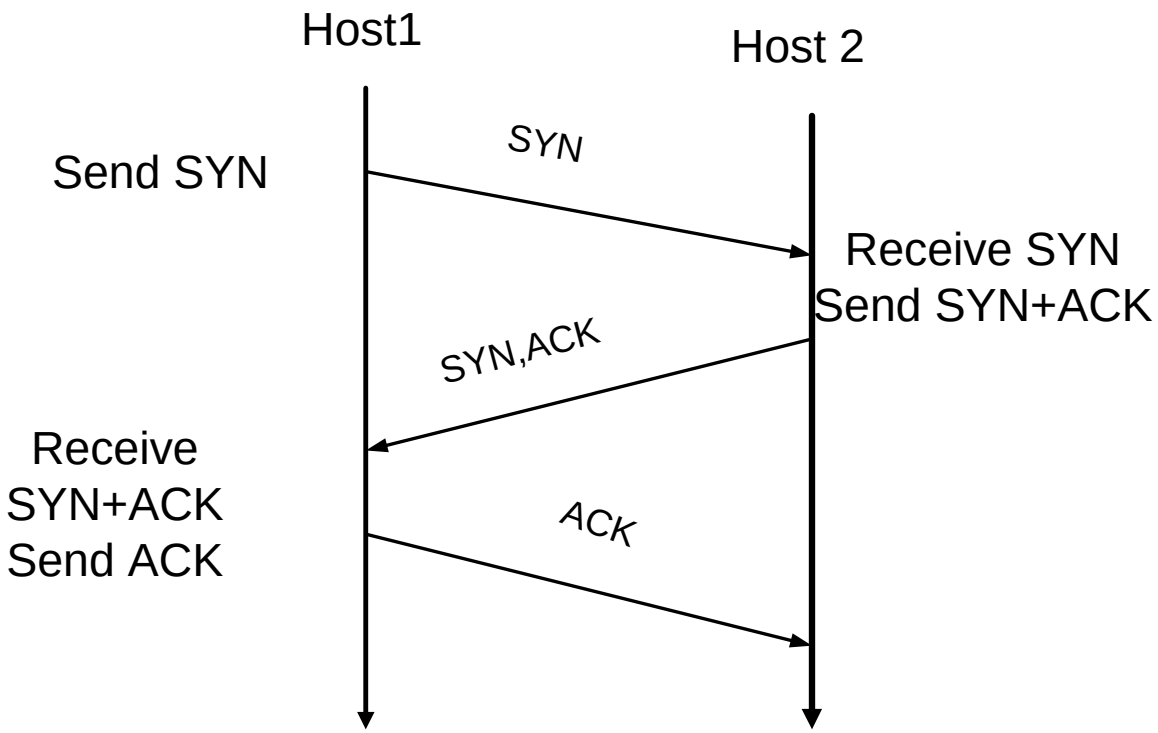
RevBuffer = size of TCP Receive Buffer

Rcvwindow = amount of spare room in Buffer



TCP Connection Management

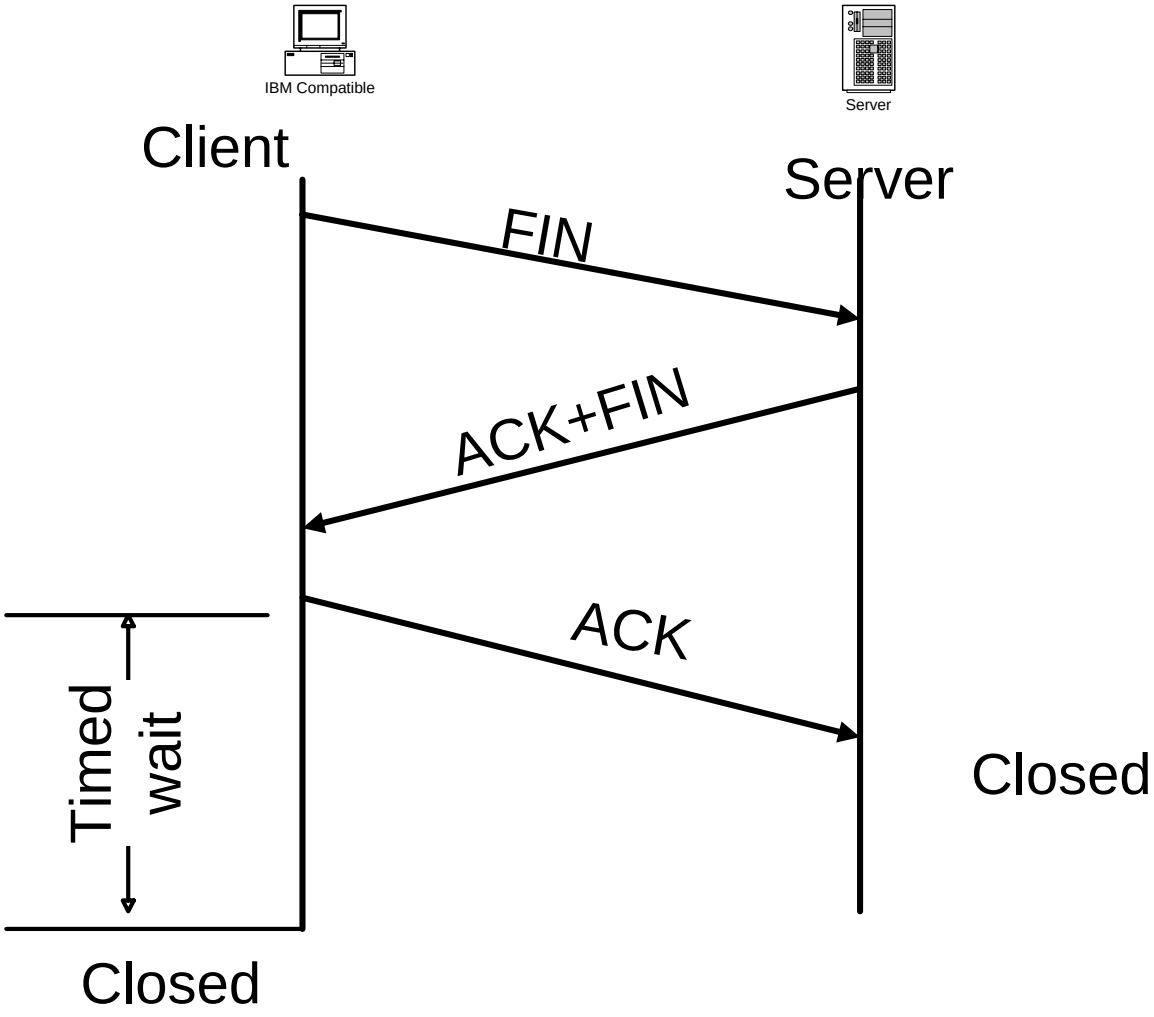
- **TCP connection must be established before exchanging data segment**
- **Initialize TCP variables:**
  - **Seq.# : a random binary integer between 0 and 2**32 –1**
  - **Flow control info e.g., RevWindow**
- **Client: connection initiator**
- **Server: contacted by client, accept connection**
- **Three way handshakes:**
  - **Step1: client sends to server: TCP SYN control segment which specifies initial seq.#**
  - **Step2: server receives SYN, responds with TCP SYN,ACK control segment**
    - **ACKs received SYN**
    - **Allocates buffers, and specifies RevWindow**
    - **Specifies server → receiver initial seq.#**
  - **Step3: client receives SYN and ACK, sends ACK**
    - **ACKs received SYN**
    - **Connection established**



3 ways handshakes for connection establishment

TCP Connection Management:Closing a connection

- Step1:Clinet sends TCP FIN control segment to server
- Step2: server receives FIN, replies with ACK & FIN
- Step3: client receives ACK & FIN, replies with ACK.
  - Enter "timeout" – will respond with ACK to received FINs
- Step4: server, receives ACK. Connection closed.



Connection Termination