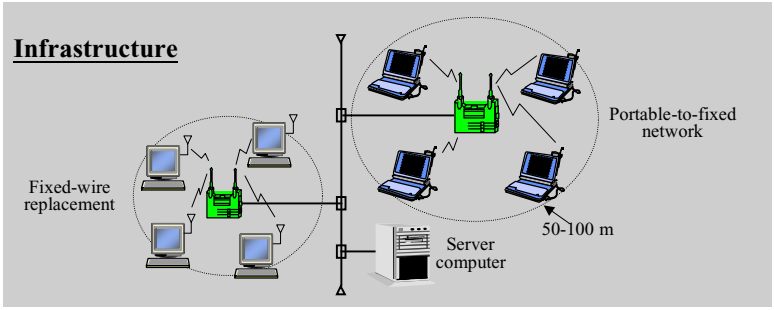
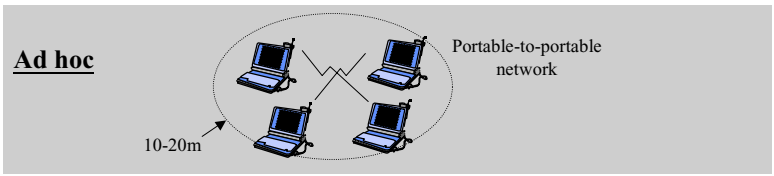
Introduction to Wireless LAN

Po-Ning Chen, Professor
Depart. Of Communications Engineering
National Chiao-Tung University

Topologies of Wireless

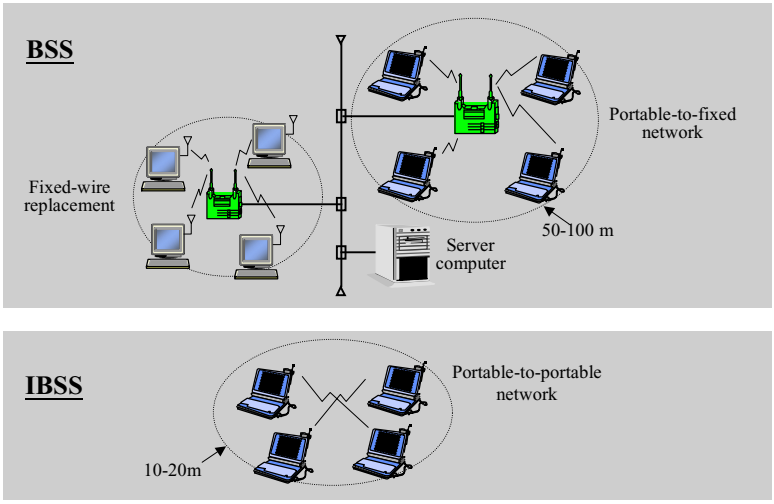
- **Infrastructure versus ad hoc**





Topologies of Wireless

- BSS (Basic Service Set) versus IBSS (Independent BSS)



Topologies of Wireless

- In an infrastructure BSS, all mobile stations communicate with the AP
  - If one mobile station in a BSS must communicate with another mobile station in the same BSS, the communication is sent first to the AP and then from the AP to the other mobile station.

Topologies of Wireless

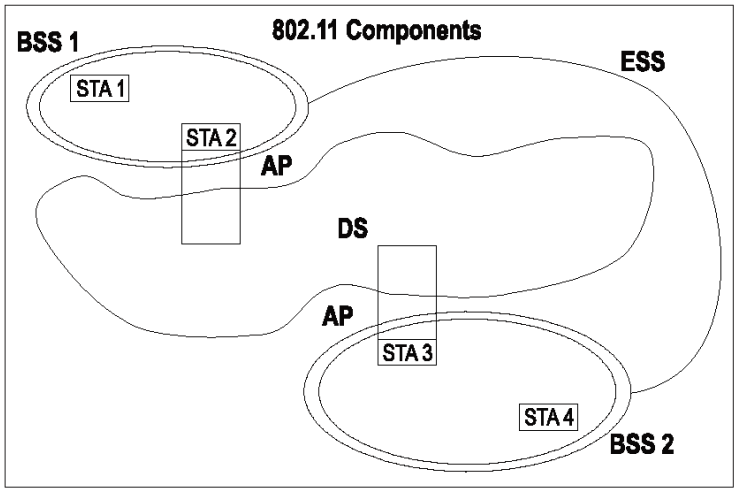


Figure 3—Extended service set

5

Transmission Scheme of Wireless LAN

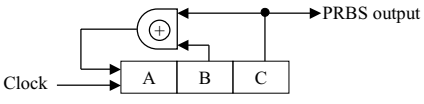
- Transmission Schemes
  - Spread Spectrum
    - » Direct Sequence Spread Spectrum
    - » Frequency Hopping Spread Spectrum
  - Direct Modulation
    - » On-Off Keying
    - » Pulse-Position Modulation
  - Carrier Modulation
    - » Single-Carrier modulation
    - » Multi-subcarrier modulation

6

Direct Sequence Spread Spectrum

- **DSSS to wireless LAN**
  - **Frequency band : ISM (Industrial Scientific Medical) band**
  - **Pseudo-random sequence advantage (PN sequence)**
    - » **Balanced property**
    - » **Run-length property**
    - » **Add-and-Delay property**

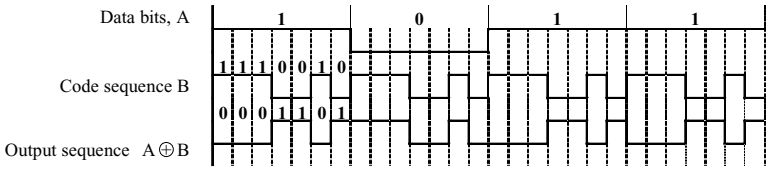
Direct Sequence Spread Spectrum



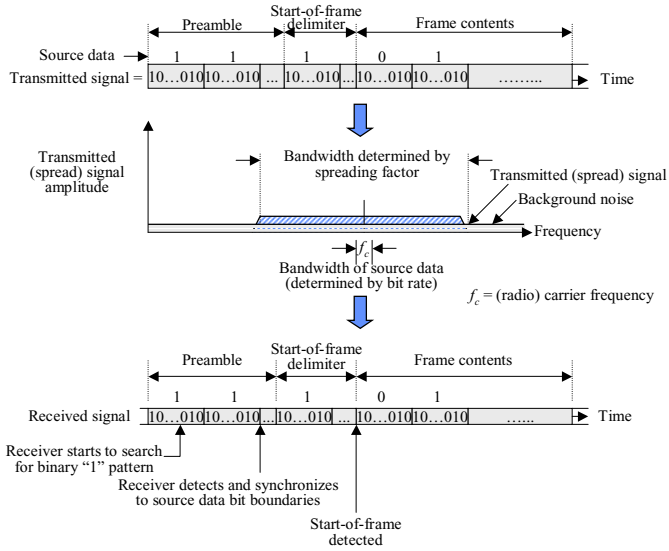
PRBS = Pseudorandom binary sequence

Clock	A	B	C
0	1	1	1
1	0	1	1
2	0	0	1
3	1	0	0
4	0	1	0
5	1	0	1
6	1	1	0

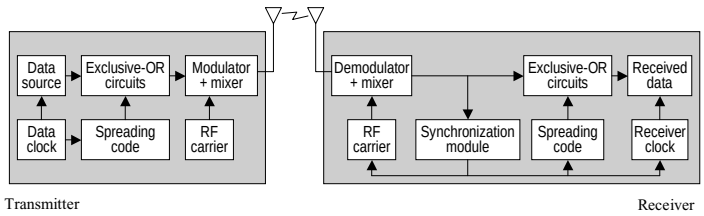
PRBS



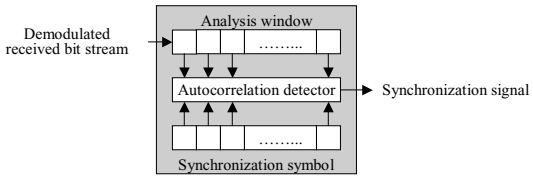
Direct Sequence Spread Spectrum



Direct Sequence Spread Spectrum

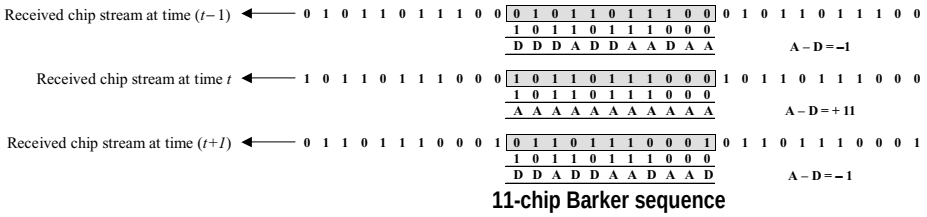


Transmitter and receiver schematic

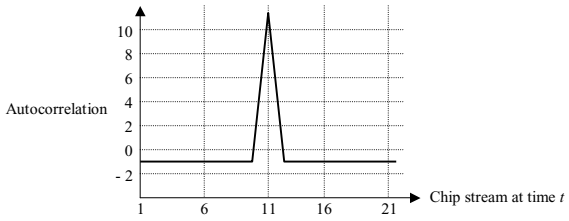


Synchronization module schematic

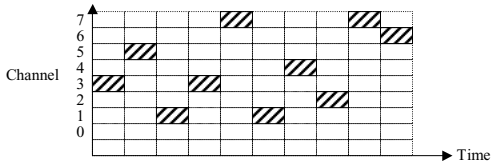
Direct Sequence Spread Spectrum



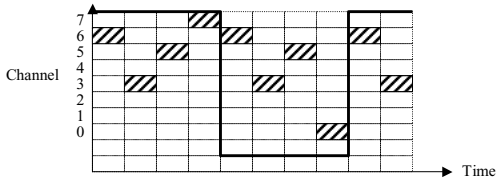
11-chip Barker sequence



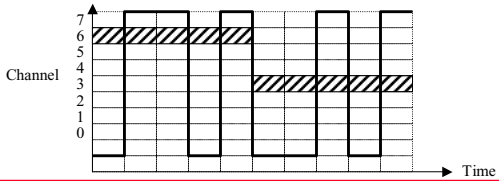
Frequency Hopping Spread Spectrum



Fast frequency-hopping

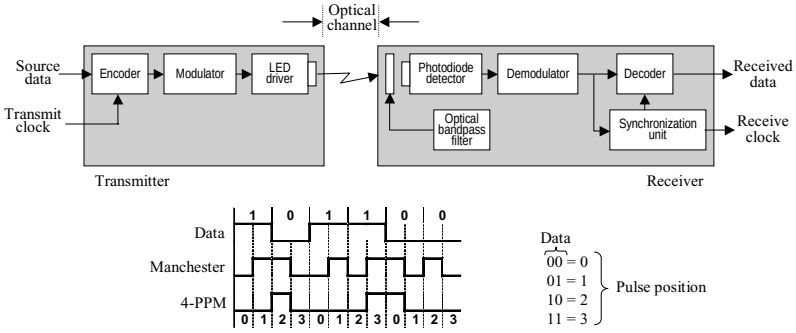


Slow frequency-hopping



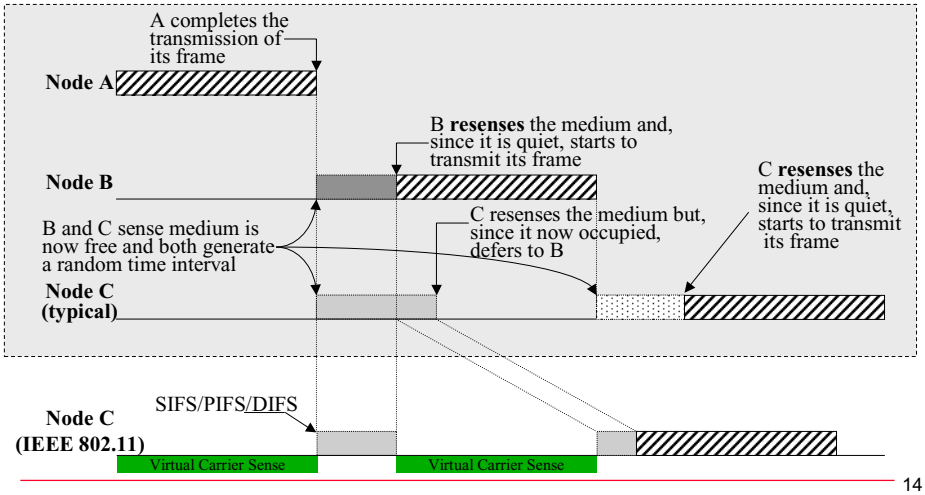
Direct Modulation

- Applications
  - Infrared Phy
- Modulation Schemes
  - OOKPPM
    - » Reducing the optical power



CSMA/CA

- Typical CSMA/CA – LBT (listen before talk) scheme
  - IEEE 802.11 CSMA/CA is slightly modified.



Standards

- IEEE 802.11
  - Finalized in June of 1997 and revised in 1999
  - (1997 version) one MAC (DFW CSMA/CA) supports multiple PHYs (DSSS, FHSS, Direct-modulated Infrared, Carrier-modulated Infrared and Multi-subcarrier-modulated Infrared)
    - 1&2 Mbps using either DSSS or FHSS
    - 1&2 Mbps using Direct-modulated Infrared
    - 4 Mbps using Carrier-modulated Infrared
    - 10 Mbps using Multi-subcarrier-modulated Infrared
  - (In-building) Operation Range = 50~150 m
  - Quality of Service
    - (optional) Point Coordination Function

15

Standards

- IEEE 802.11
  - IEEE Std 802.11a
    - Approved on September 16, 1999
    - Orthogonal frequency domain multiplexing (OFDM) radio in the UNII bands, delivering up to 54 Mbps data rates
  - IEEE Std 802.11b
    - Approved on September 16, 1999
    - Extension to the DSSS PHY in the 2.4 GHz band, delivering up to 11 Mbps data rates

16

Main Requirements and Basic Features

- **Single MAC to support multiple PHYs.**
  - **MAC = DFW CSMA/CA**
  - **PHY = DSSS, FHSS, Direct-modulated Infrared, Carrier-modulated Infrared and Multi-subcarrier-modulated Infrared**
- **Robust for Interference.**
  - **Interference from Microwave interferers/Other un-licensed spectrum users/Co-channel interference**
  - ***CSMA/CA + ACK* for unicast frames, with MAC level recovery.**
  - **CSMA/CA for Broadcast frames (if within a BSS or IBSS)**

Transmit Power Level

Maximum output power	Geographic location	Compliance document
1000 mW	USA	FCC 15.247
100 mW (EIRP)	Europe	ETS 300–328
10 mW/MHz	Japan	MPT ordinance for Regulating Radio Equipment, Article 49-20

17

Main Requirements and Basic Features

- **General Channel Assignment**
  - **Adjacent cells using different channels can operate simultaneously without interference if the distance between the center frequencies is at least 25 MHz.**

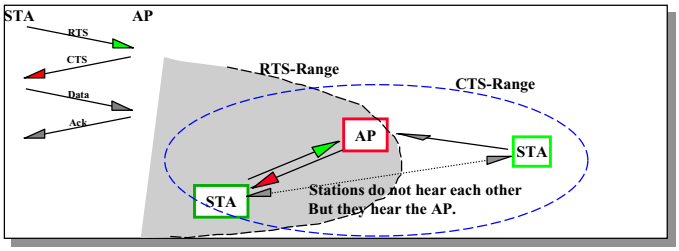
		Regulatory domains					
CHNL_ID	Frequency	X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32' France	X'40' MKK
1	2412 MHz	X	X	X	—	—	—
2	2417 MHz	X	X	X	—	—	—
3	2422 MHz	X	X	X	—	—	—
4	2427 MHz	X	X	X	—	—	—
5	2432 MHz	X	X	X	—	—	—
6	2437 MHz	X	X	X	—	—	—
7	2442 MHz	X	X	X	—	—	—
8	2447 MHz	X	X	X	—	—	—
9	2452 MHz	X	X	X	—	—	—
10	2457 MHz	X	X	X	X	X	—
11	2462 MHz	X	X	X	X	X	—
12	2467 MHz	—	—	X	—	X	—
13	2472 MHz	—	—	X	—	X	—
14	2484 MHz	—	—	—	—	—	X

* IC (Canada)

18

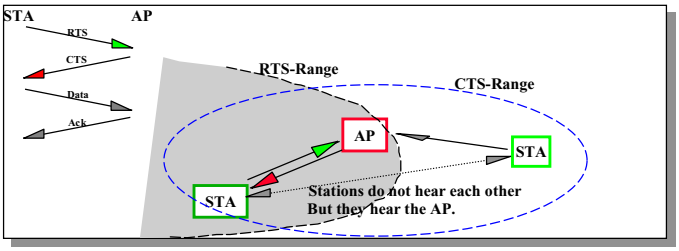
Main Requirements and Basic Features

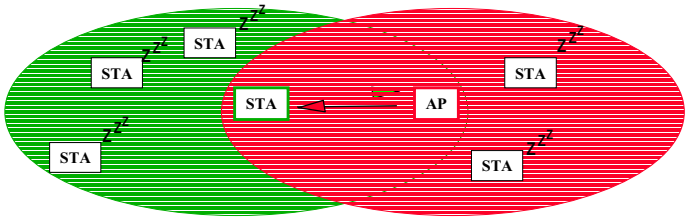
- Mechanisms to deal with "*Hidden Nodes*."
  - DFW CSMA/CA



19

Main Requirements and Basic Features

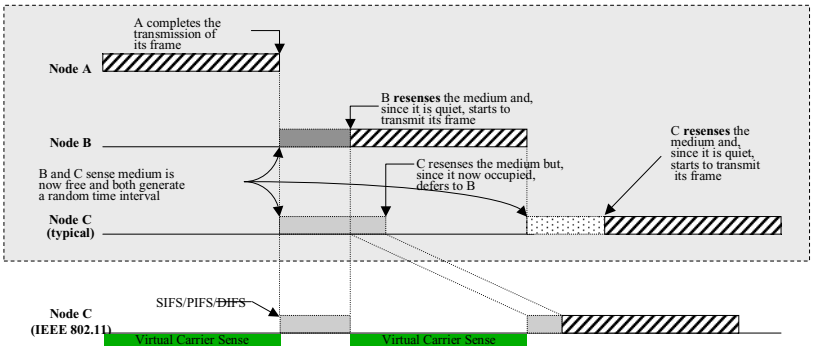




20

Main Requirements and Basic Features

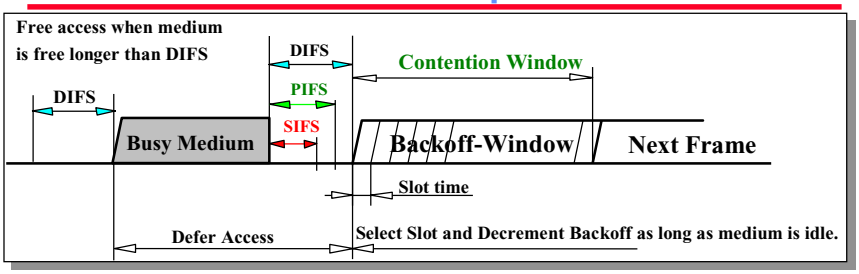
- Mechanisms to deal with "*Hidden Nodes*."
  - Parameterized use of RTS/CTS to provide a ***Virtual Carrier Sense*** function to protect against *Hidden Nodes*.



IEEE 802.11 Distributed Coordination Function

- To summarize,
  - DFW CSMA/CA (RTS/CTS) to prevent "hidden node"
  - ACK to DATA frame to provide reliable transmission
  - Virtual Carrier Sense to save power
    - » duration information provided by RTS frame and CTS frame
  - SIFS/PIFS/DIFS to give priority to more urgent frames, such as the ACK frame following a DATA frame or the CTS frame followed an RTS frame.
    - » SIFS = Short inter-frame space
    - » PIFS = Point-coordination function interframe space
    - » DIFS = Distributed coordination function interframe space
  - Exponential Back-off Windows to prevent heavy load congestion.

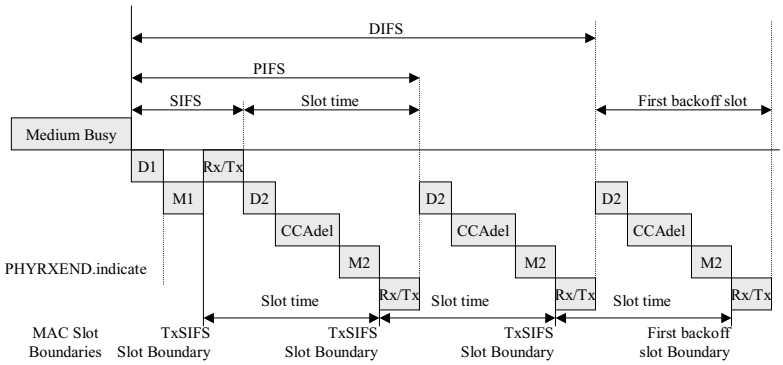
IEEE 802.11 CSMA/CA Explained



- Reduce collision probability where mostly needed.
  - Stations are waiting for medium to become free.
  - Select Random Backoff after a Defer, resolving contention to avoid collisions.
- Efficient Backoff algorithm stable at high loads.
  - Binary exponential Backoff window increases for retransmissions.
  - * Backoff timer elapses only when medium is idle.
- Implement different fixed priority levels (S/P/DIFS)
  - To allow immediate responses and PCF coexistence.

Timing Intervals - SIFS/PIFS/DIFS

- Five time intervals are specified, where two are determined by the PHY, and three are built from the previous two.



D1 = aRxRFDelay + aRxPLCPDelay (referenced from the end of the last symbol of a frame on the medium)
D2 = D1 + Air Propagation time
Rx/Tx = aRXTXTurnaroundTime (begins with a PHYTXSTART.request)
M1 = M2 = aMACPrcDelay
CCAdel = aCCATime – D1

Suggested values of Timing Intervals

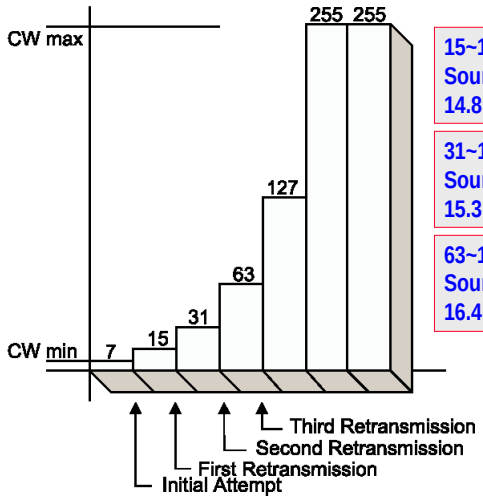
- FHSS
  - aSlotTime = 50us and aSIFSTime = 28us
- DSSS
  - aSlotTime = 20us and aSIFSTime = 10us
- IR
  - aSlotTime = 8us and aSIFSTime = 7us (IEEE Std 802.11-1997)
  - aSlotTime = 8us and aSIFSTime = 10us (IEEE P802.11/D10, 14 Jan. 1999: Table 75)

CSMA/CA + ACK protocol

- (Transmitter) Recovery Procedure and Retransmit Limits
  - Error Recovery shall be attempted by retrying transmissions.
  - Retry shall continue until *successful* or *retry limit* is reached.
  - Retry attempts for failed transmission shall continue until the *Short Retry Count (default 7, < RTSThreshold)* for MPDU is equal to *Short Retry Limit* or *Long Retry Count* is equal to *Long Retry Limit (default 4, >= RTSThreshold)* .
- (Receiver) Duplicate Detection and Recovery
  - Duplicate frame filtering is facilitated the inclusion of a *Sequence Control Field* associated with the transmitted frames.
  - A Destination STA shall cache <*Source MAC Address, sequence number, fragment number* >, and it shall discard a duplicate frame which matches the cache and whose Retry bit = 1.

CSMA/CA + ACK protocol

- Binary exponential backoff window



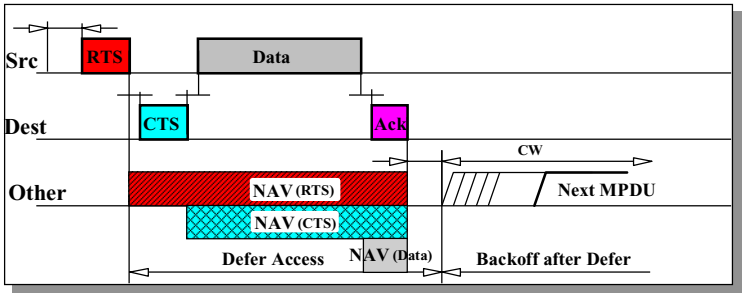
15~1023 for FHSS PHY
Source: IEEE Std 802.11-1997
14.8.2 FH PHY attributes: Table 49

31~1023 for DSSS PHY
Source: IEEE Std 802.11-1997
15.3.2 DSSS PHY MIB: Table 58

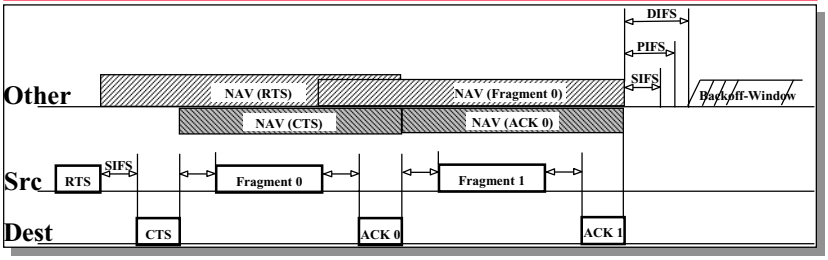
63~1023 for IR PHY
Source: IEEE Std 802.11-1997
16.4 PHY attributes: Table 74

"Hidden Node" Provisions

- NAV(Net Allocation Vector) Set and Reset
  - All STAs receiving a valid frame shall update their NAV in the *Duration Field*.
  - All of the RTS/CTS/DATA frames contains NAV field.

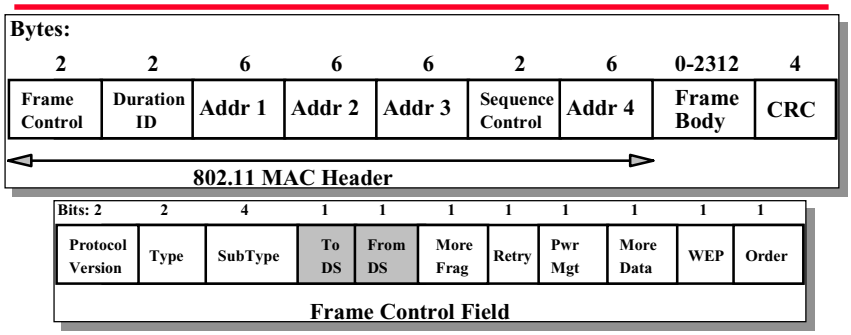


Fragmentation



- **Fragment Bursts** which are individually acknowledged.
  - For Unicast frames only.
- ***Duration*** information in data fragments and Ack frames causes NAV to be set, for medium reservation mechanism.

Frame Formats



- **MAC Header format differs per Type:**
  - Control Frames (several fields are omitted)
  - Management Frames
  - Data Frames
- **Includes Sequence Control Field for filtering of duplicate caused by ACK mechanism.**

Types and Sub-types

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved

31

Types and Sub-types

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention Free (CF)-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000–1111	Reserved
11	Reserved	0000–1111	Reserved

32

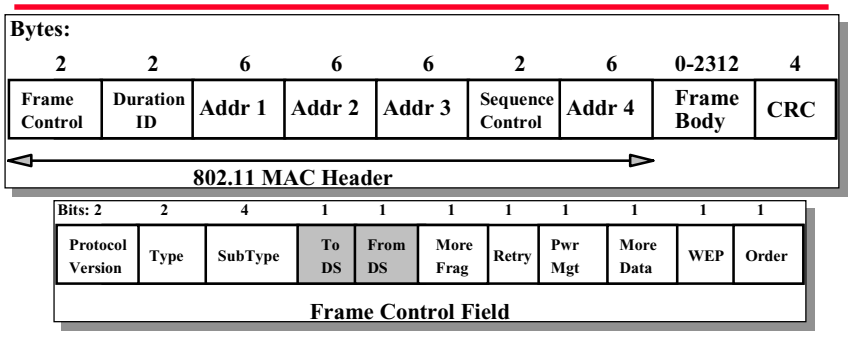
Address Field Description

Function	To DS	From DS	Address 1	Address 2	Address 3	Address 4
IBSS	0	0	RA = DA	SA	BSSID	N/A
From the AP	0	1	RA = DA	BSSID	SA	N/A
To the AP	1	0	RA = BSSID	SA	DA	N/A
Wireless DS	1	1	RA	TA	DA	SA

- SA = The source that originates the frame
- DA = The (final) destination of the frame
- RA = The next immediate intended recipient
- TA = The transmitter of the current transmission
- BSSID = The MAC address of the associated AP of the current frame transmitter (or a random number generated by the station that starts the IBSS)

* Where the content of a field is shown as N/A, the field is omitted.

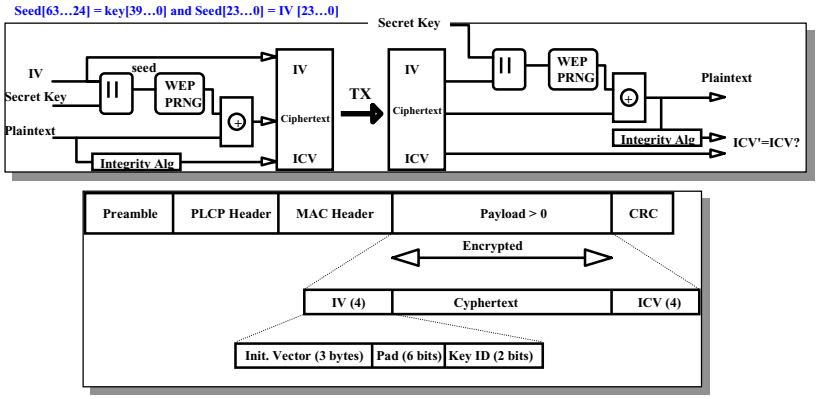
More Data Subfield



- More Data
  - For AP: More frames are buffered at the AP for the mobile station.

Privacy and Access Control

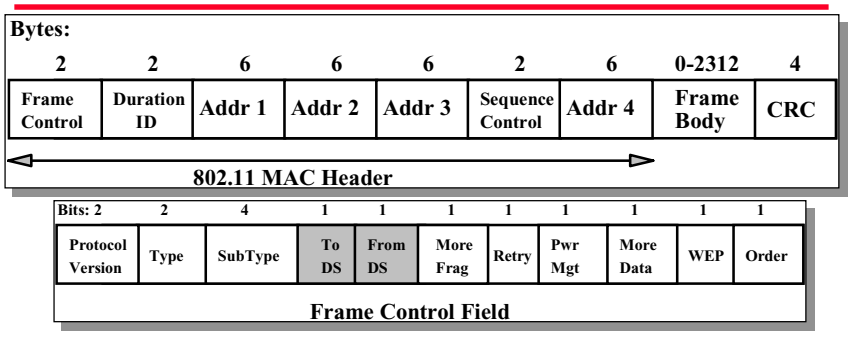
- Goal of 802.11 is to provide "Wired Equivalent Privacy" (WEP)



- WEP bit in Frame Control Field indicates WEP used.
  - Each frame can have a new IV, or IV can be reused for a limited time.

35

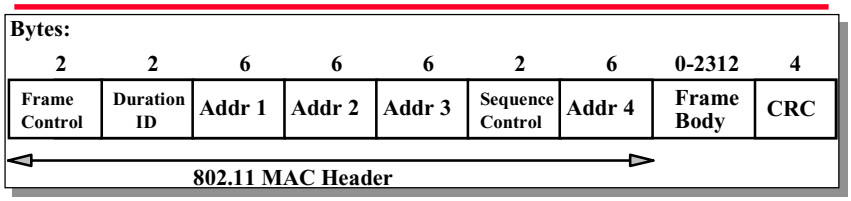
Order Subfield



- Order = 1
  - Strictly ordering must be maintained.

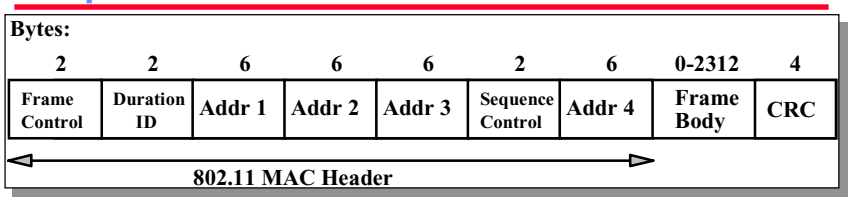
36

Duration/ID Field



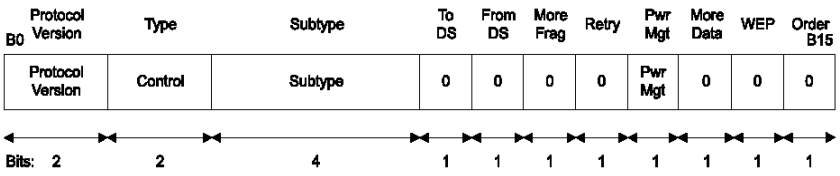
- Bit15 = 0
  - Bits 14-0 = remaining duration in microseconds of a frame exchange (NAV); ceiling function value will be taken if a non-integer is rendered.
- Bit 15 = 1 and Bit 14-0 = 0
  - This is a CFP frame.
- Bits 15-14 = 11
  - Bits 13-0 = AID (from 0 to 2007), specifically in a PS-POLL frame.

Sequence Control Field



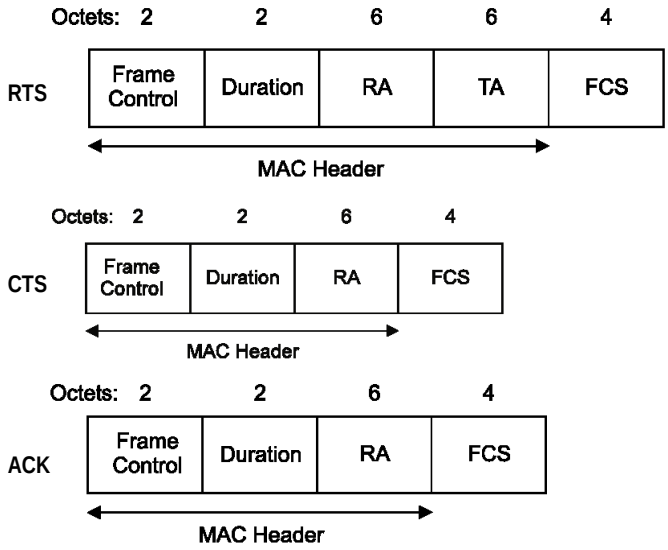
- Sequence Control = 12 bit Sequence Number + 4 bit Fragment Number
  - Sequence Number : A unique wrap-back number for each MSDU; remain constant for re-transmission
  - Fragment Number : A unique wrap-back number for each MPDU; remain constant for re-transmission

Control Frames

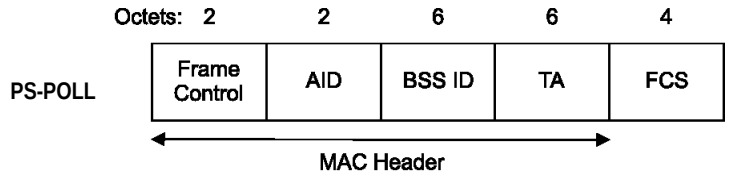


- The subfield within the frame control field of control frames are set as above.

Control Frames



Control Frames



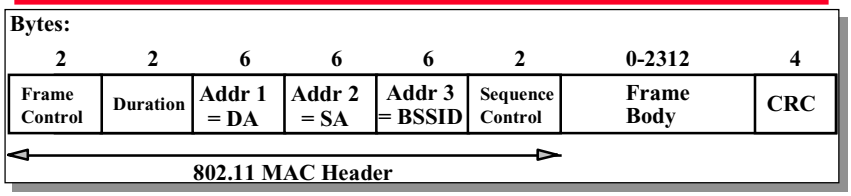
41

Data Frames

- Data and Null (a special subtype of data frames)
  - The sole purpose for the null data frame is to carry the power management bit in the frame control field to the AP, when a station changes its power management state.

42

Management Frames



- Frame Body
  - Fixed fields
  - Variable-length information elements
    - » Must be in the order of increasing identifiers

MAC Management Frames

- Beacon
  - Fixed fields : 64-bit timestamp (TSF timer value), 16-bit beacon Interval (in the unit of 1024us = one TU), 16-bit capability
  - Information element : ESSID, supported rates, one or more PHY parameter sets, *optional* contention-free parameter set, *optional* IBSS parameter set, *optional* Traffic Indication Map (TIM)
- Probe
  - Fixed field : capability
  - Information element : ESSID, supported rates
- Probe Response
  - Same as Beacon except no TIM

MAC Management Frames

- Association Request
  - Fixed field : capability, 16-bit listen interval (in units of beacon interval)
  - Information element : ESSID, supported rates
- Association Response
  - Fixed field : capability, 16-bit status code, 16-bit AID (same format as Duration)
  - Information element : supported rates
- Reassociation Request
  - Reassociation can only be applied to an AP that has the same ESSID with the previous associated AP.
  - Same as Association Request except an additional 6-byte current AP address fixed field
- Reassociation Response
  - Same as Association Response

45

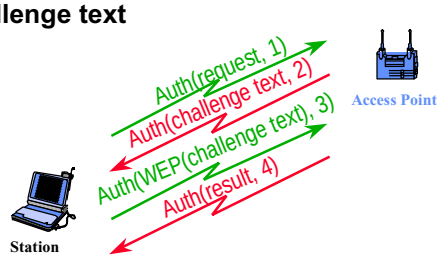
Status Codes (with additions made in 802.11b)

Status code	Meaning
0	Successful
1	Unspecified failure
2–9	Reserved
10	Cannot support all requested capabilities in the Capability Information field
11	Reassociation denied due to inability to confirm that association exists
12	Association denied due to reason outside the scope of this standard
13	Responding station does not support the specified authentication algorithm
14	Received an Authentication frame with authentication transaction sequence number out of expected sequence
15	Authentication rejected because of challenge failure
16	Authentication rejected due to timeout waiting for next frame in sequence
17	Association denied because AP is unable to handle additional associated stations
18	Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter
19	Association denied due to requesting station not sup-porting the Short Preamble option
20	Association denied due to requesting station not sup-porting the PBCC Modulation option
21	Association denied due to requesting station not sup-porting the Channel Agility option

46

MAC Management Frames

- Disassociation
  - Fixed field : 16-bit reason code
  - No Information element
- Authentication
  - Fixed field : 16-bit authentication algorithm number (0 for “open system” and 1 for “shared key”), 16-bit authentication transaction sequence number (start from 1), status code
  - Information element : challenge text
- Deauthentication
  - Fixed field : reason code
  - No Information element



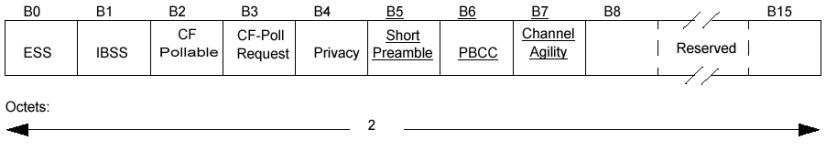
Reason codes

Reason code	Meaning
0	Reserved
1	Unspecified reason
2	Previous authentication no longer valid
3	Deauthenticated because sending station is leaving (has left) IBSS or ESS
4	Disassociated due to inactivity
5	Disassociated because AP is unable to handle all currently associated stations
6	Class 2 frame received from nonauthenticated station
7	Class 3 frame received from nonassociation station
8	Disassociated because sending station is leaving (has left) BSS
9	Station requesting (re)association is not authenticated with responding station
10–65 535	Reserved

MAC Management Frames

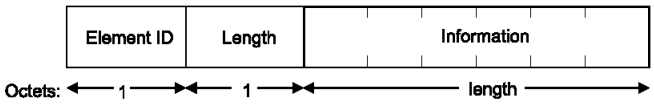
- Announcement TIM (ATIM)
  - No fixed field and Information element
  - Use to notify other station in an IBSS that the sender of the ATIM frame has traffic buffered and waiting to be delivered to the station addressed in the ATIM frame

Capability Information Fixed Field



- ESS and IBSS
  - Only significant in Beacon and Probe Response
  - AP : ESS = 1 and IBSS = 0
  - Mobile station in an IBSS : ESS =0 and IBSS = 1
- CF Pollable and CF-Poll Request
  - Be discussed in PCF
- Privacy, Short Preamble, PBCC, Channel Agility
  - 1 = the function is implemented/supported by the AP

Information Elements



Information element	Element ID
SSID	0
Supported rates	1
FH Parameter Set	2
DS Parameter Set	3
CF Parameter Set	4
TIM	5
IBSS Parameter Set	6
Reserved	7–15
Challenge text	16
Reserved for challenge text extension	17–31
Reserved	32–255

Service Set Identity (SSID)

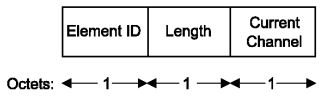
- **SSID**
  - **Can be up to 32 bytes in length.**
    - » **When its length equals zero, SSID = "broadcast" identity that is used in Probe Request frame when the mobile station is attempting to discover all 802.11 WLANs in its vicinity.**
  - **Can be ASCII characters or multibyte binary values.**

Supported Rates

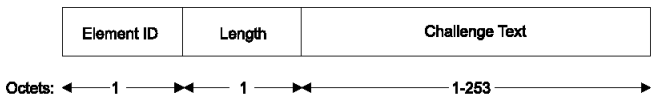
- **Supported Rates**
  - **Can be 1~8 bytes long, each byte represents a single rate.**
  - **The most significant bit indicates whether the rate is mandatory or not, while the remaining 7 bits represent the rate value.**
  - **Before IEEE 802.11b, the rate is measured in unit of 500Kbps, which pose an upper limit of 63.5Mbps. After the standardization of IEEE 802.11b, the rate now indicates by a simple label (hence, no upper limit is imposed.)**
  - **E.g., X'82' = 1Mbps belongs to the mandatory BSS basic rate set.**
  - **E.g., X'04' = 2Mbps does not belong to the mandatory BSS basic rate set.**

DS and Challenge Text Parameter Sets

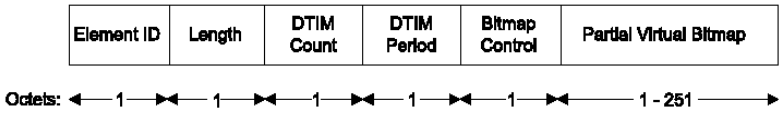
DS parameter set



Challenge Text



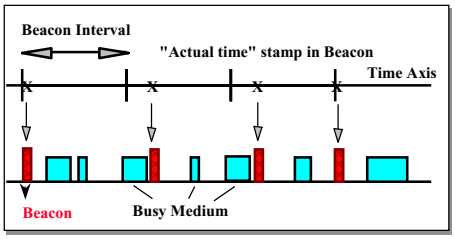
TIM information element



- DTIM Count = DTIM Countdown Number
- DTIM Period = DTIM Interval in unit of beacon intervals
- Bitmap Control
  - MSB bit = more buffered multi/broadcast frames
  - Remaining 7 bits = [N1/2], where bits 1 ~ [N1*8]-1 in Partial Virtual Bitmap are all zero.
- Length = (N2-N1)+4, where bits (N2+1)*8 ~ 2007 in Partial Virtual Bitmap are all zero.

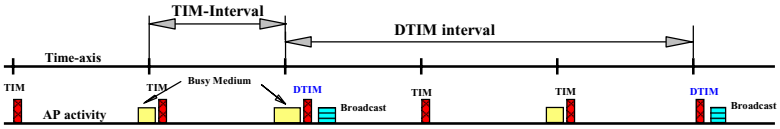
Synchronization in 802.11

- 64-bit Timing Synchronization Function (TSF) running at 1MHz, used for time-based mechanisms



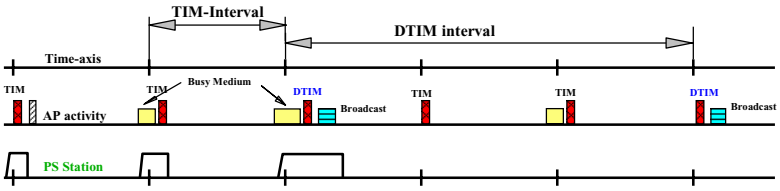
- APs send Beacons in infrastructure networks.
- Beacons scheduled at Beacon Interval.
- Transmission may be delayed by CSMA deferral.
  - subsequent transmissions at expected Beacon Interval
- Timestamp contains timer value at transmit time.

Infrastructure Power Management



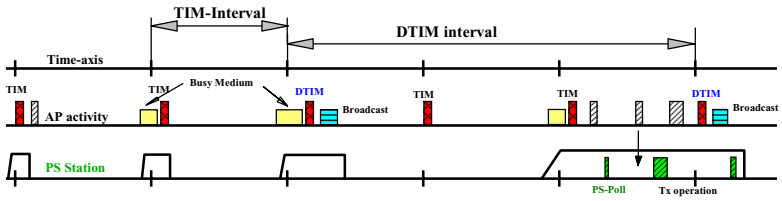
- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after DTIM
  - DTIM interval is a multiple of TIM interval

Infrastructure Power Management



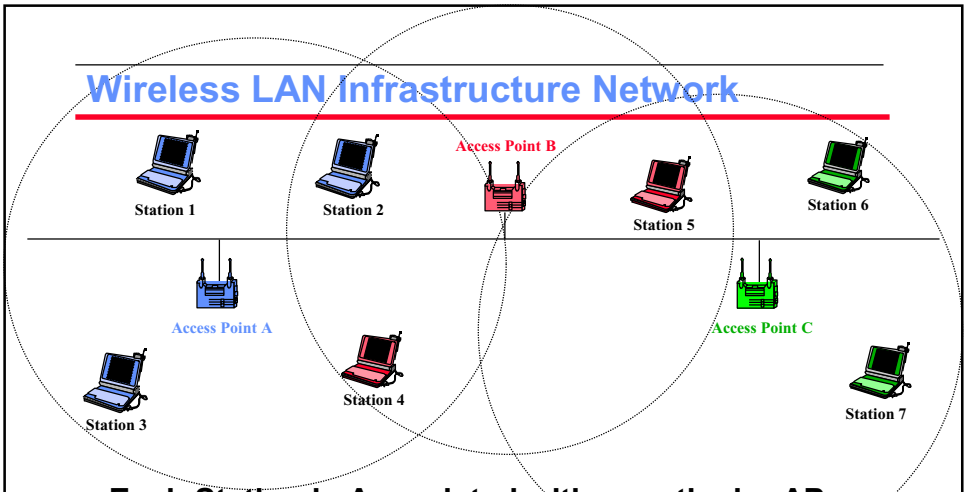
- Stations wake up prior to an expected (D)TIM.

Infrastructure Power Management

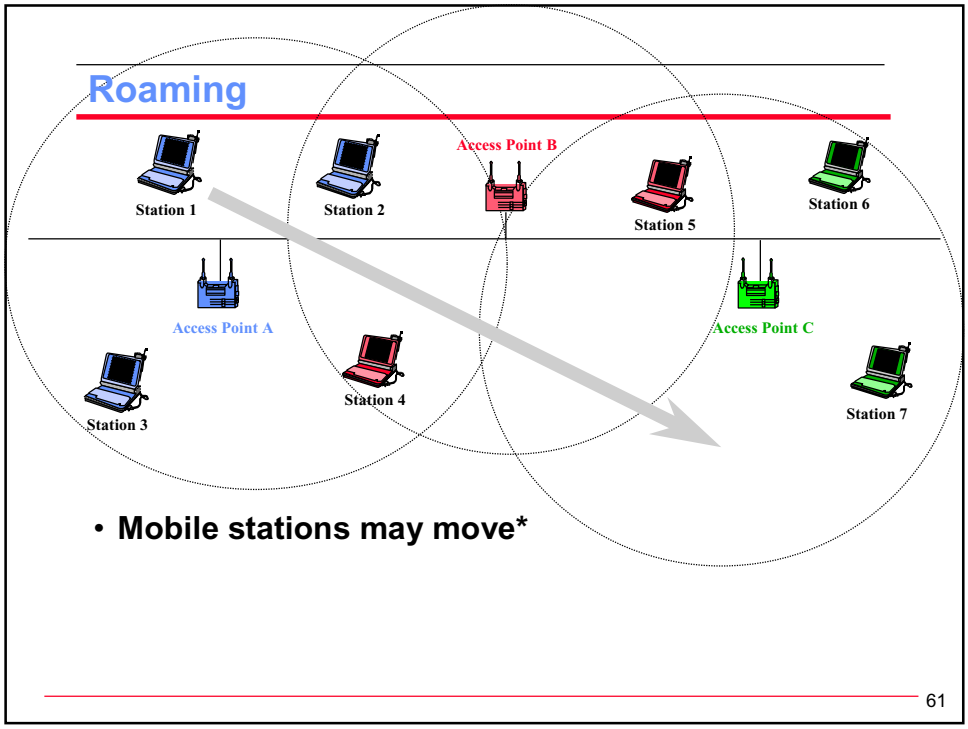


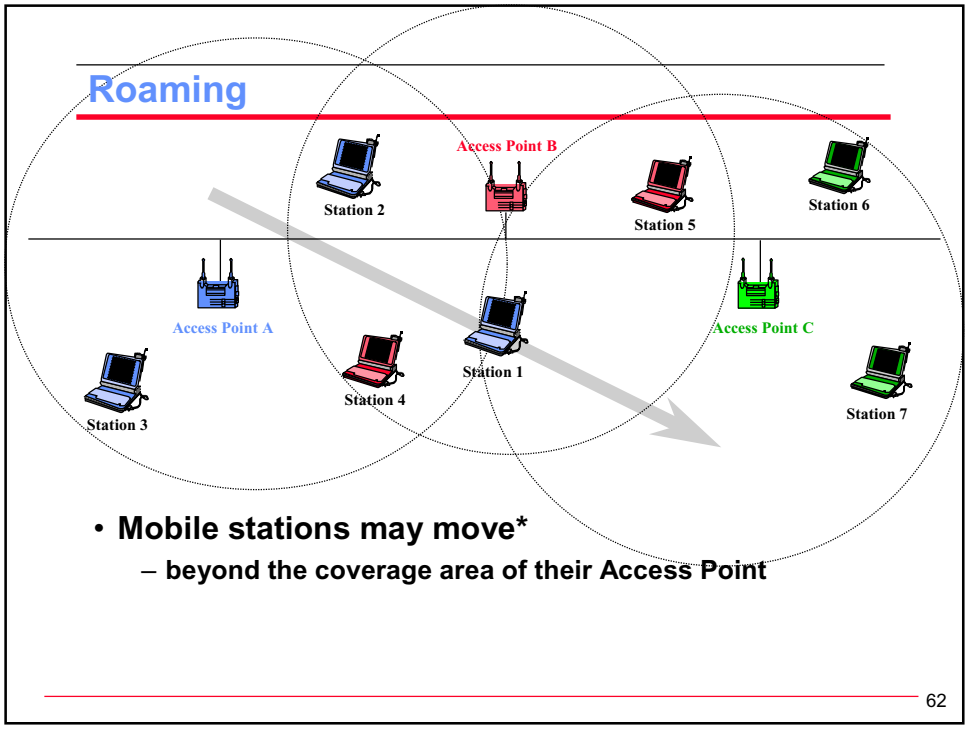
- If TIM indicates frame buffered
  - station sends PS-Poll and stays awake to receive data
  - else station sleeps again

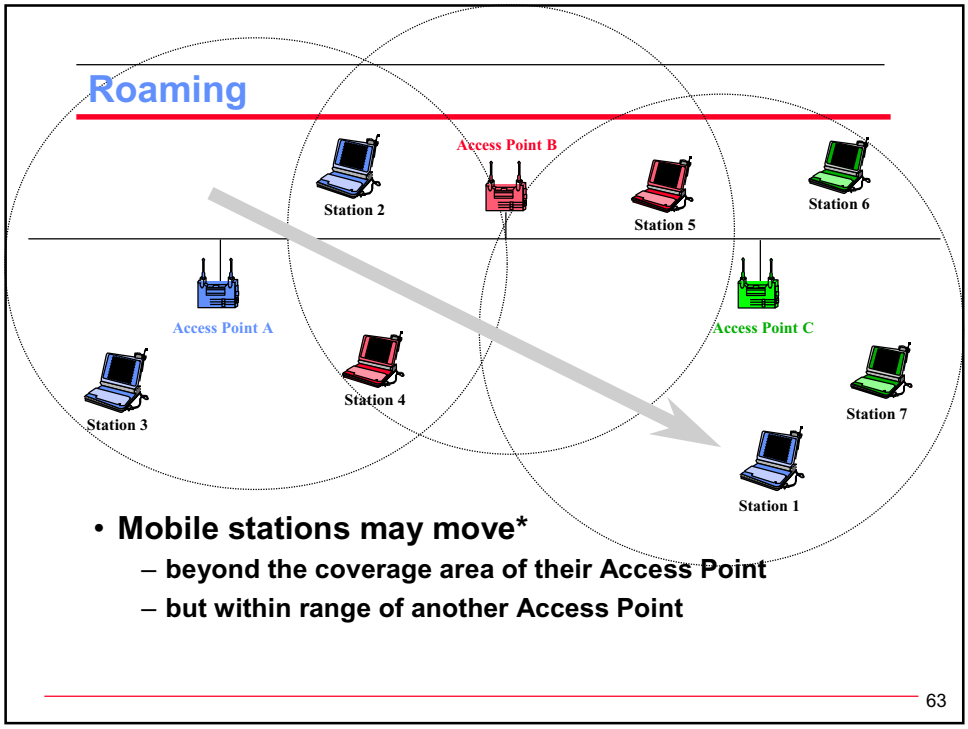
Wireless LAN Infrastructure Network

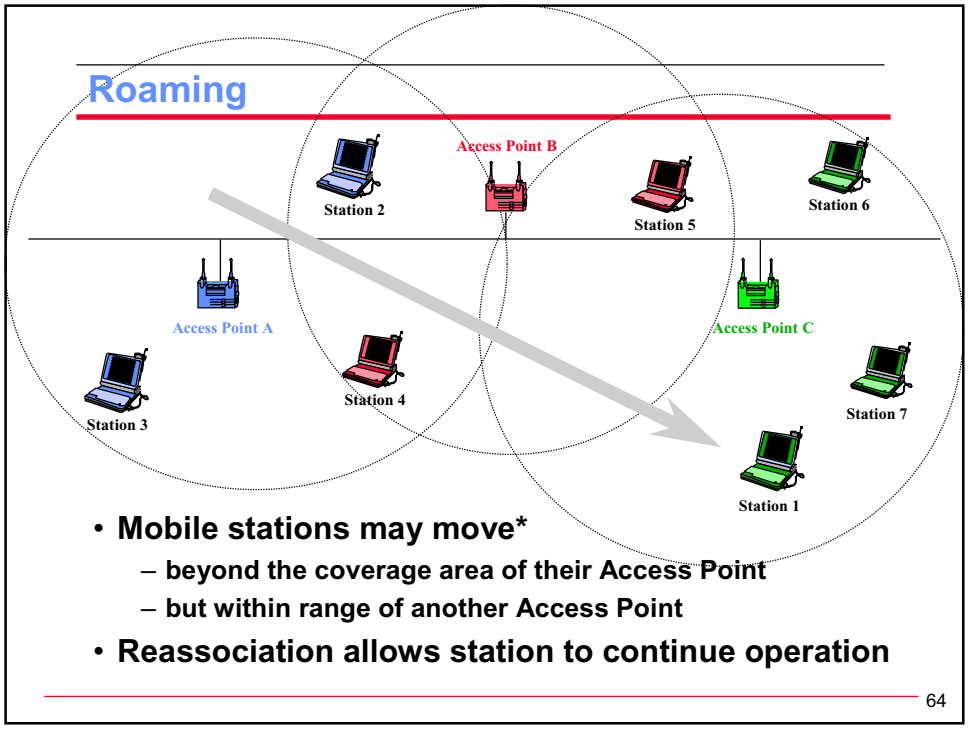


- Each Station is Associated with a particular AP
  - Stations 1, 2, and 3 are associated with Access Point A
  - Stations 4 and 5 are associated with Access Point B
  - Stations 6 and 7 are associated with Access Point C


Roaming
Station 1
Station 2
Access Point B
Station 5
Station 6
Access Point A
Access Point C
Station 3
Station 4
Station 7
• Mobile stations may move*
61


Roaming
Station 2
Access Point B
Station 5
Station 6
Access Point A
Access Point C
Station 3
Station 4
Station 1
Station 7
• Mobile stations may move*
– beyond the coverage area of their Access Point
62


Roaming
Access Point B
Station 2
Station 5
Station 6
Access Point A
Access Point C
Station 3
Station 4
Station 7
Station 1
• Mobile stations may move*
– beyond the coverage area of their Access Point
– but within range of another Access Point
63


Roaming
Access Point B
Station 2
Station 5
Station 6
Access Point A
Access Point C
Station 3
Station 4
Station 7
Station 1
• Mobile stations may move*
– beyond the coverage area of their Access Point
– but within range of another Access Point
• Reassociation allows station to continue operation
64

Roaming Approach

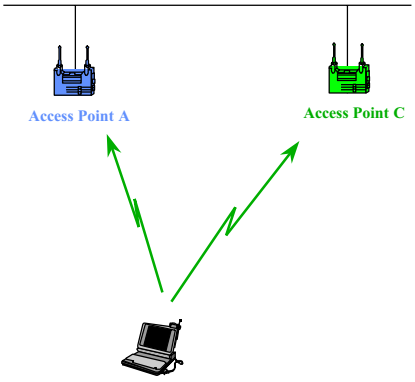
- Station decides that link to its current AP is poor using the information of
  - Carrier Sense and Energy Detection
  - RSSI (Receiver Signal Strength Indicator)
- Station uses scanning function to find another AP
- Station sends Reassociation Request to new AP
- If Reassociation Response is successful
  - then station has roamed to the new AP
  - else station scans for another AP
- If AP accepts Reassociation Request
  - AP indicates Reassociation to the Distribution System
  - Distribution System information is updated
  - normally old AP is notified through Distribution System

Scanning

- Passive Scanning
  - Find networks simply by listening for Beacons
- Active Scanning
  - On each channel
    - » Send a Probe,
    - » Wait for a Probe Response

Active Scanning Example

Steps to Association:



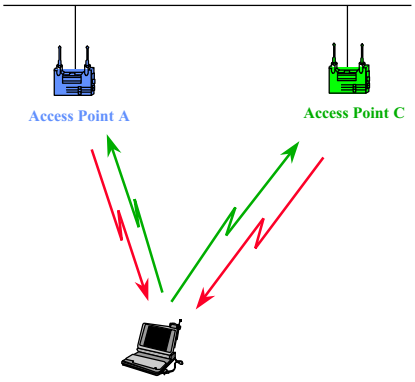
← Station sends Probe.

Initial connection to an Access Point

67

Active Scanning Example

Steps to Association:



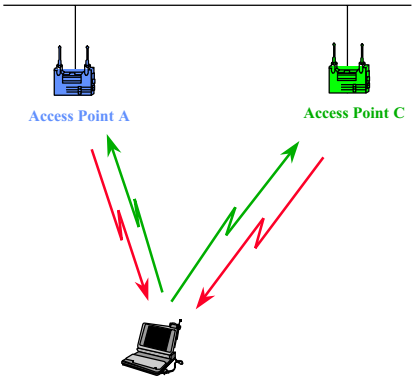
← Station sends Probe.

→ APs send Probe Response.

Initial connection to an Access Point

68

Active Scanning Example



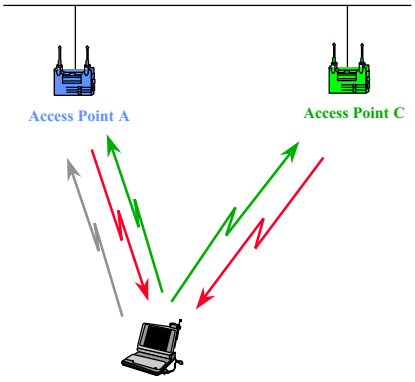
Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.

Initial connection to an Access Point

69

Active Scanning Example



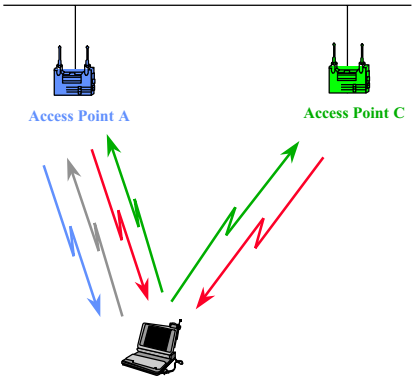
Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.

Initial connection to an Access Point

70

Active Scanning Example

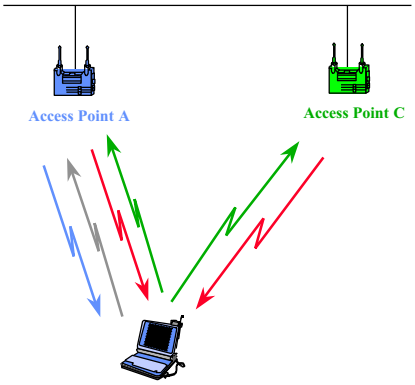


Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.
- AP sends Association Response.

Initial connection to an Access Point

Active Scanning Example



Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.
- AP sends Association Response.

Initial connection to an Access Point
- ReAssociation follows a similar process

Inter-Access Point Protocol (IAPP)

- Historical events of IAPP
  - Interoperability among APs is only least defined in the original IEEE 802.11 standard.
  - To resolve the issue, H. Moelard and M. Trompower proposed an Inter-Access Point Protocol (IAPP) in the form of an Internet draft standard to facilitate interoperability between IEEE802.11 compliant APs in 1998.
  - Noting the significance of such issue, the IEEE Standards Committee has established the Task Group F to standardize the implementation of IEEE 802.11 compliant Aps (jointly developed by Aironet, Lucent Technologies, and Digital Ocean).
  - On January 19, 2001, they proposed the first draft of the IAPP Recommended Practice.
    - "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE802.11 Operation," *IEEE802.11f pre-Draft*, January 2001.