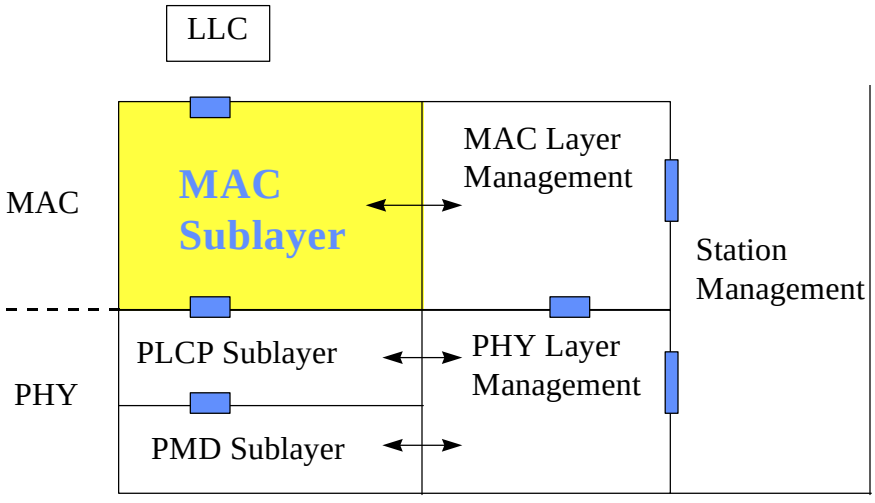
802.11 Tutorial

802.11 MAC Entity:

MAC Basic Access Mechanism

Privacy and Access Control

802.11 Protocol Entities



802.11 Tutorial March 96

Main Requirements

- Single MAC to support multiple PHYs.
  - Support single and multiple channel PHYs.
  - and PHYs with different *Medium Sense* characteristics
- Should allow overlap of multiple networks in the same area and channel space.
  - Need to be able to share the medium.
  - Allow re-use of the same medium.
- Need to be *Robust for Interference*.
  - Microwave interferers
  - Other un-licensed spectrum users
  - Co-channel interference
- Need mechanisms to deal with *Hidden Nodes*.
- Need provisions for *Time Bounded Services*.
- Need provisions for Privacy and Access Control.

 3

802.11 Tutorial March 96

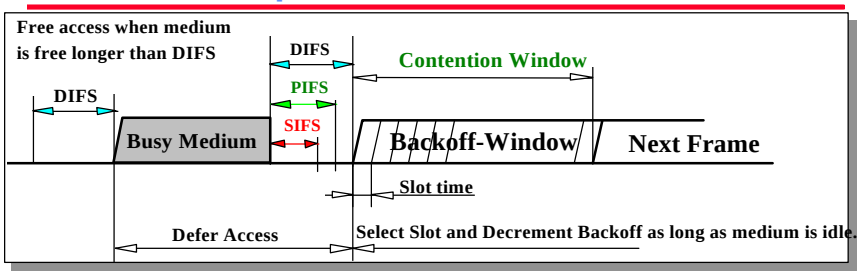
Basic Access Protocol Features

- Use Distributed Coordination Function (DCF) for efficient medium sharing without overlap restrictions.
  - Use CSMA with Collision Avoidance derivative.
  - Based on *Carrier Sense* function in PHY called ***Clear Channel Assessment*** (CCA).
- Robust for interference.
  - ***CSMA/CA + ACK*** for unicast frames, with MAC level recovery.
  - CSMA/CA for Broadcast frames.
- Parameterized use of RTS / CTS to provide a ***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.
- Includes fragmentation to cope with different PHY characteristics.
- Frame formats to support the access scheme
  - For Infrastructure and Ad-Hoc Network support
  - and *Wireless Distribution System*.

 4

802.11 Tutorial March 96

CSMA/CA Explained

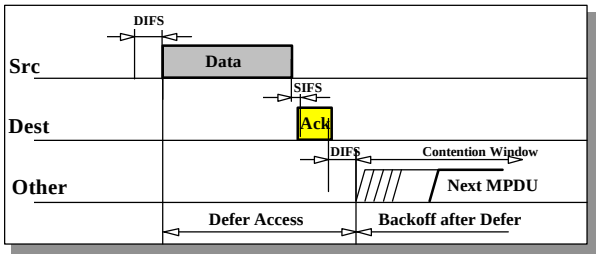


- Reduce collision probability where mostly needed.
  - Stations are waiting for medium to become free.
  - Select Random Backoff after a Defer, resolving contention to avoid collisions.
- Efficient Backoff algorithm stable at high loads.
  - Exponential Backoff window increases for retransmissions.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

 5

802.11 Tutorial March 96

CSMA/CA + ACK protocol

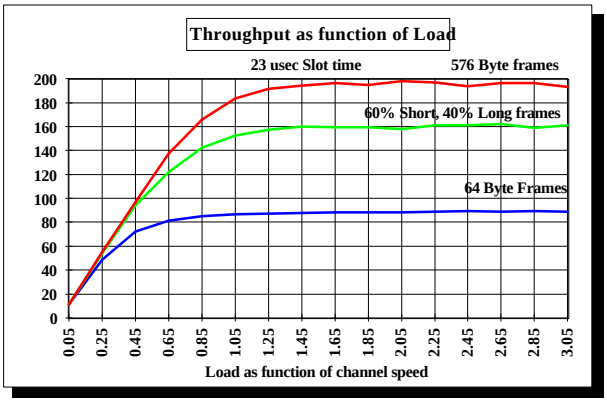


- Defer access based on *Carrier Sense*.
  - CCA from PHY and *Virtual Carrier Sense* state.
- Direct access when medium is sensed free longer then DIFS, otherwise defer and backoff.
- Receiver of directed frames to return an ACK immediately when CRC correct.
  - When no ACK received then retransmit frame after a random backoff (up to maximum limit).

 6

802.11 Tutorial March 96

Throughput Efficiency



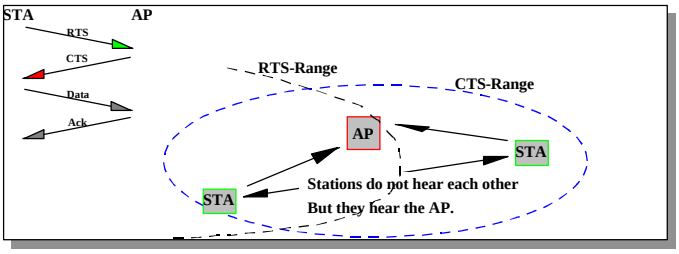
- **Efficient and stable throughput.**
  - **Stable throughput at overload conditions.**
  - **To support "Bursty Traffic" characteristics.**

 7

802.11 Tutorial March 96

"Hidden Node" Problem

- **Transmitters contending for the medium may not *"Hear each other"* as shown below.**

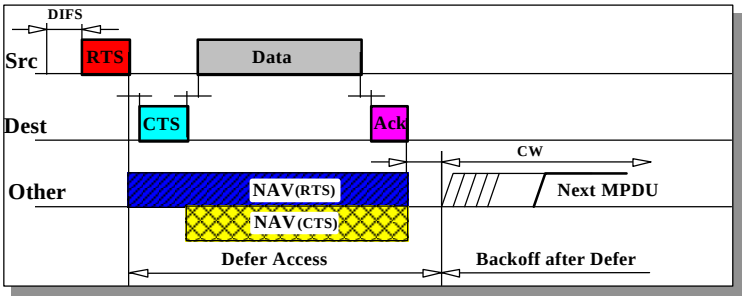


- **Separate Control frame exchange (RTS / CTS) between transmitter and receiver will *Reserve the Medium* for subsequent data access.**
  - ***Duration* is distributed around both Tx and Rx station.**

 8

802.11 Tutorial March 96

"Hidden Node" Provisions

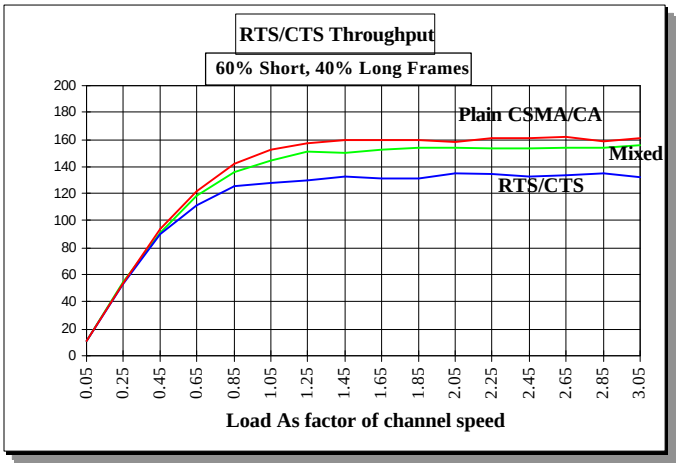


- ***Duration*** **field in RTS and CTS frames distribute** ***Medium Reservation*** **information which is stored in a** ***Net Allocation Vector (NAV)*****.**
- **Defer on either NAV or "CCA" indicating** ***Medium Busy*****.**
- **Use of RTS / CTS is optional but must be implemented.**
- **Use is controlled by a** ***RTS_Threshold*** **parameter per station.**
  - **To limit overhead for short frames.**

 9

802.11 Tutorial March 96

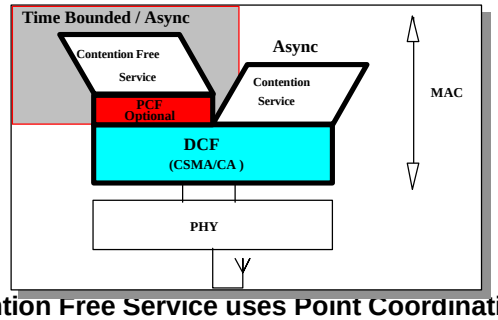
RTS/CTS Overhead Impact



Good mixed Throughput (long inbound frames) efficiency.

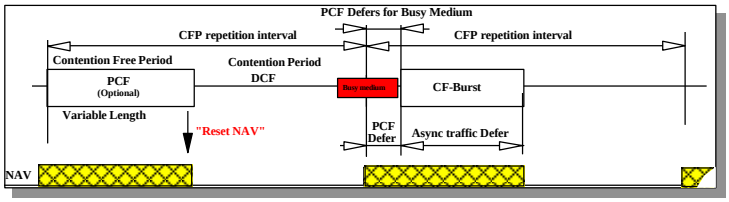
 10

Optional Point Coordination Function (PCF)



- Contention Free Service uses Point Coordination Function (PCF) on a DCF Foundation.
  - PCF can provide lower *transfer delay* variations to support ***Time Bounded Services***.
  - Async Data, Voice or mixed implementations possible.
  - Point Coordinator resides in AP.
- Coexistence between Contention and optional Contention Free does not burden the implementation.

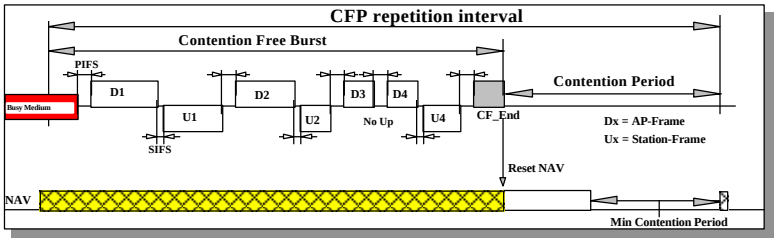
Contention Free operation



- Alternating ***Contention Free*** and ***Contention*** operation under PCF control.
- NAV prevents *Contention* traffic until reset by the last PCF transfer.
  - So variable length *Contention Free* period per interval.
- Both PCF and DCF defer to each other causing PCF Burst start variations.

802.11 Tutorial March 96

PCF Burst

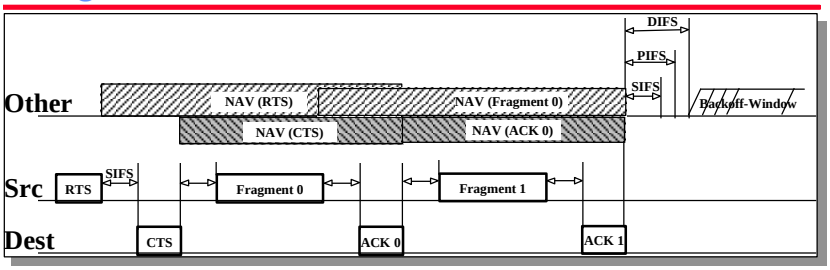


- CF-Burst by Polling bit in CF-Down frame.
- Immediate response by Station on a CF_Poll.
- Stations to maintain NAV to protect CF-traffic.
- Responses can be variable length.
- “Reset NAV” by last (CF_End) frame from AP.
- "ACK Previous Frame" bit in Header.

 13

802.11 Tutorial March 96

Fragmentation

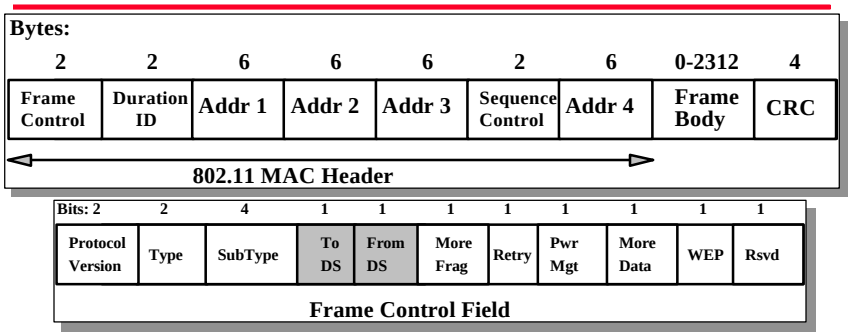


- Burst of Fragments which are individually acknowledged.
  - For Unicast frames only.
- Random backoff and retransmission of failing fragment when no ACK is returned.
- *Duration* information in data fragments and Ack frames causes NAV to be set, for medium reservation mechanism.

 14

802.11 Tutorial March 96

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.

 15

802.11 Tutorial March 96

Address Field Description

To DS	From DS	Address 1	Address 2	Address 3	Address 4
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

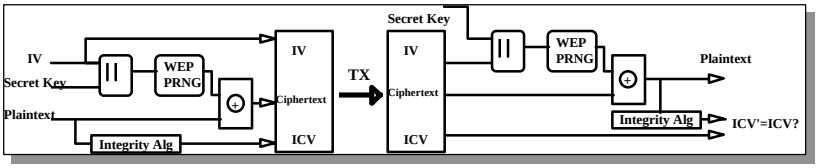
- Addr 1 = All stations filter on this address.
- Addr 2 = Transmitter Address (TA)
  - Identifies transmitter to address the ACK frame to.
- Addr 3 = Dependent on *To* and *From DS* bits.
- Addr 4 = Only needed to identify the original source of WDS (***Wireless Distribution System)*** frames.

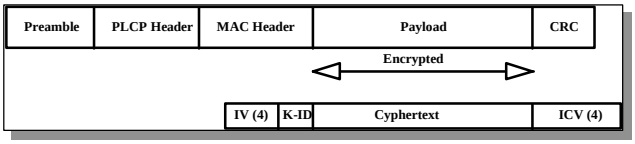
 16

Privacy and Access Control

- Goal of 802.11 is to provide "Wired Equivalent Privacy" (WEP)
  - Usable worldwide
- 802.11 provides for an Authentication mechanism
  - To aid in access control.
  - Has provisions for "OPEN", "Shared Key" or proprietary authentication extensions.
- Optional (WEP) Privacy mechanism defined by 802.11.
  - Limited for Station-to-Station traffic, so not "end to end".
    - » Embedded in the MAC entity.
  - Only implements "Confidentiality" function.
  - Uses RC4 PRNG algorithm based on:
    - » a 40 bit secret key (No Key distribution standardized)
    - » and a 24 bit IV that is send with the data.
    - » includes an ICV to allow integrity check.
  - Only payload of Data frames are encrypted.
    - » Encryption on per MPDU basis.

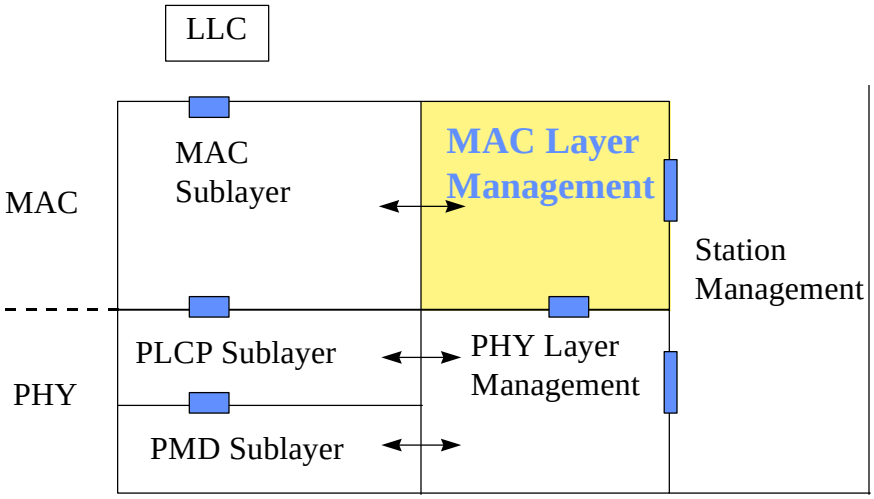
Privacy Mechanism





- 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.
  - If integrity check fails then frame is ACKed but discarded.

Support for Mobility



MAC Management Layer

- **Synchronization**
  - **finding and staying with a WLAN**
  - **Synchronization functions**
    - **» TSF Timer, Beacon Generation**
- **Power Management**
  - **sleeping without missing any messages**
  - **Power Management functions**
    - **» periodic sleep, frame buffering, Traffic Indication Map**
- **Association and Reassociation**
  - **Joining a network**
  - **Roaming, moving from one AP to another**
  - **Scanning**
- **Management Information Base**

Synchronization in 802.11

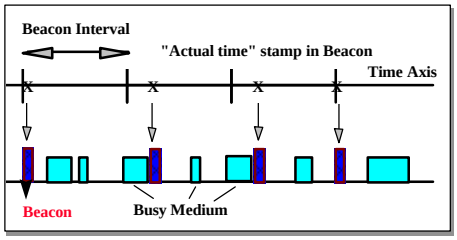
- Timing Synchronization Function (TSF)
- Used for Power Management
  - Beacons sent at well known intervals
  - All station timers in BSS are synchronized
- Used for Point Coordination Timing
  - TSF Timer used to predict start of Contention Free burst
- Used for Hop Timing for FH PHY
  - TSF Timer used to time Dwell Interval
  - All Stations are synchronized, so they hop at same time.

Synchronization Approach

- All stations maintain a local timer.
- Timing Synchronization Function
  - keeps timers from all stations in synch
  - AP controls timing in infrastructure networks
  - distributed function for Independent BSS
- Timing conveyed by periodic Beacon transmissions
  - Beacons contain Timestamp for the entire BSS
  - Timestamp from Beacons used to calibrate local clocks
  - not required to hear every Beacon to stay in synch
  - Beacons contain other management information
    - » also used for Power Management, Roaming

802.11 Tutorial March 96

Infrastructure Beacon Generation



- APs send Beacons in infrastructure networks.
- Beacons scheduled at Beacon Interval.
- Transmission may be delayed by CSMA deferral.
  - subsequent transmissions at expected Beacon Interval
  - not relative to last Beacon transmission
  - next Beacon sent at Target Beacon Transmission Time
- Timestamp contains timer value at transmit time.

 23

802.11 Tutorial March 96

Power Management

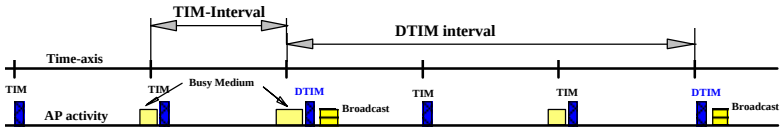
- Mobile devices are battery powered.
  - *Power Management* is important for mobility.
- Current LAN protocols assume stations are always ready to receive.
  - Idle receive state dominates LAN adapter power consumption over time.
- How can we power off during idle periods, yet maintain an active session?
- 802.11 Power Management Protocol:
  - allows transceiver to be off as much as possible
  - is transparent to existing protocols
  - is flexible to support different applications
    - » possible to trade off throughput for battery life

 24

Power Management Approach

- Allow idle stations to go to sleep
  - station's power save mode stored in AP
- APs buffer packets for sleeping stations.
  - AP announces which stations have frames buffered
  - Traffic Indication Map (TIM) sent with every Beacon
- Power Saving stations wake up periodically
  - listen for Beacons
- TSF 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
- Independent BSS also have Power Management
  - similar in concept, distributed approach

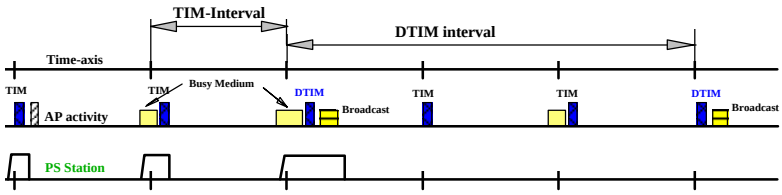
Infrastructure Power Management



- 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

802.11 Tutorial March 96

Infrastructure Power Management

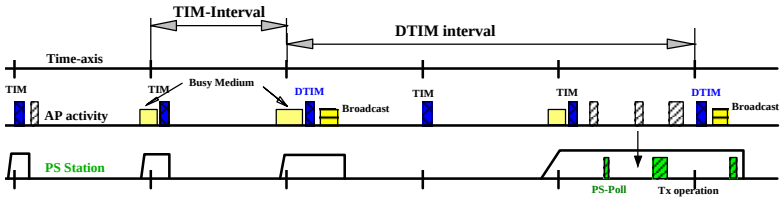


- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after DTIM
  - DTIM interval is a multiple of TIM interval
- Stations wake up prior to an expected (D)TIM.

 27

802.11 Tutorial March 96

Infrastructure Power Management

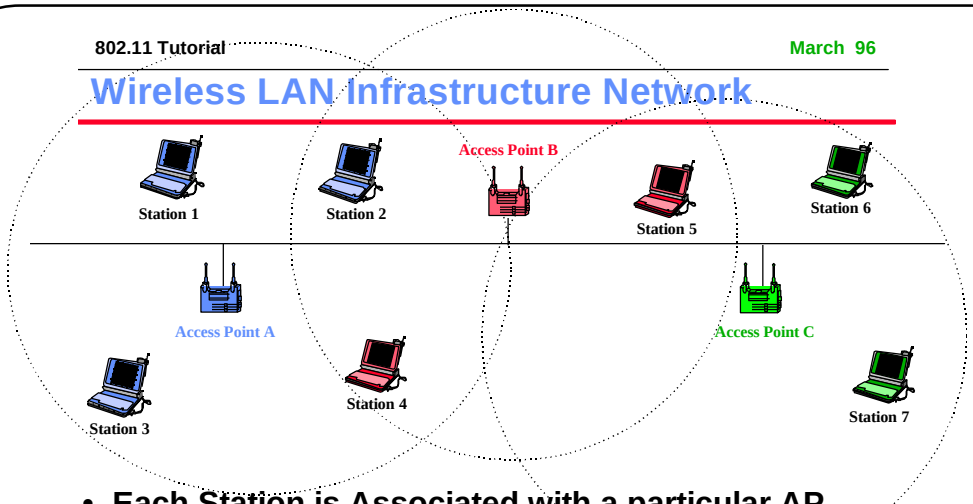


- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after DTIM
  - DTIM interval is a multiple of TIM interval
- Stations wake up prior to an expected (D)TIM.
- If TIM indicates frame buffered
  - station sends PS-Poll and stays awake to receive data
  - else station sleeps again

 28

802.11 Tutorial March 96

Wireless LAN Infrastructure Network

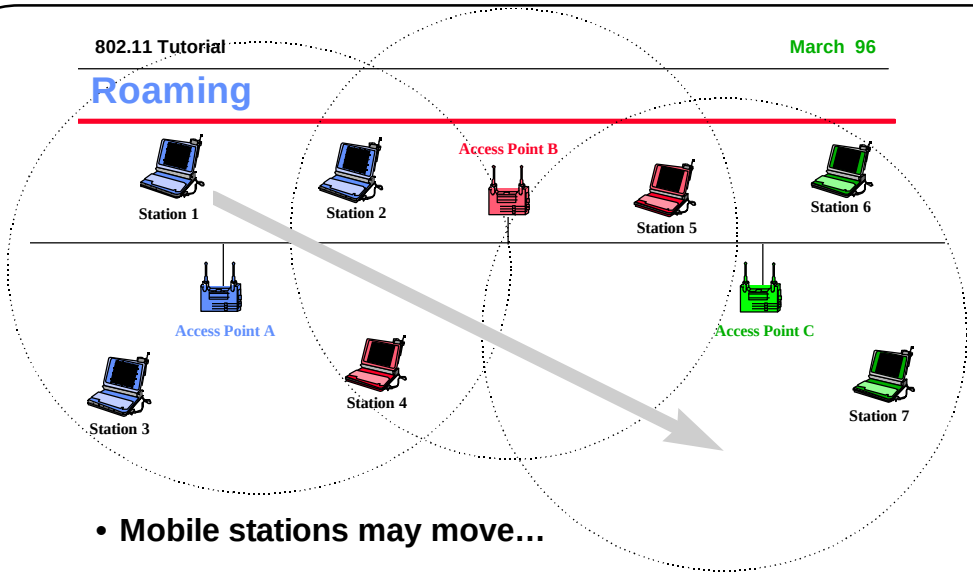


- Each Station is Associated with a particular AP
  - Stations 1, 2, and 3 are associated with Access Point A
  - Stations 4 and 5 are associated with Access Point B
  - Stations 6 and 7 are associated with Access Point C

 29

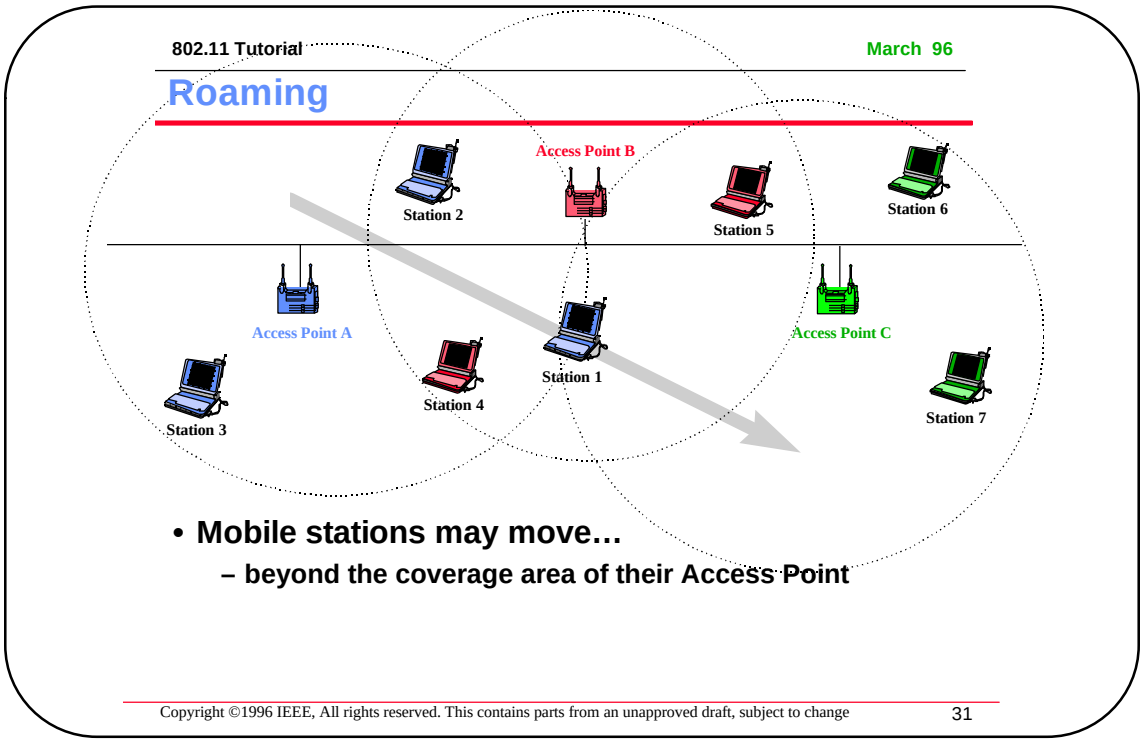
802.11 Tutorial March 96

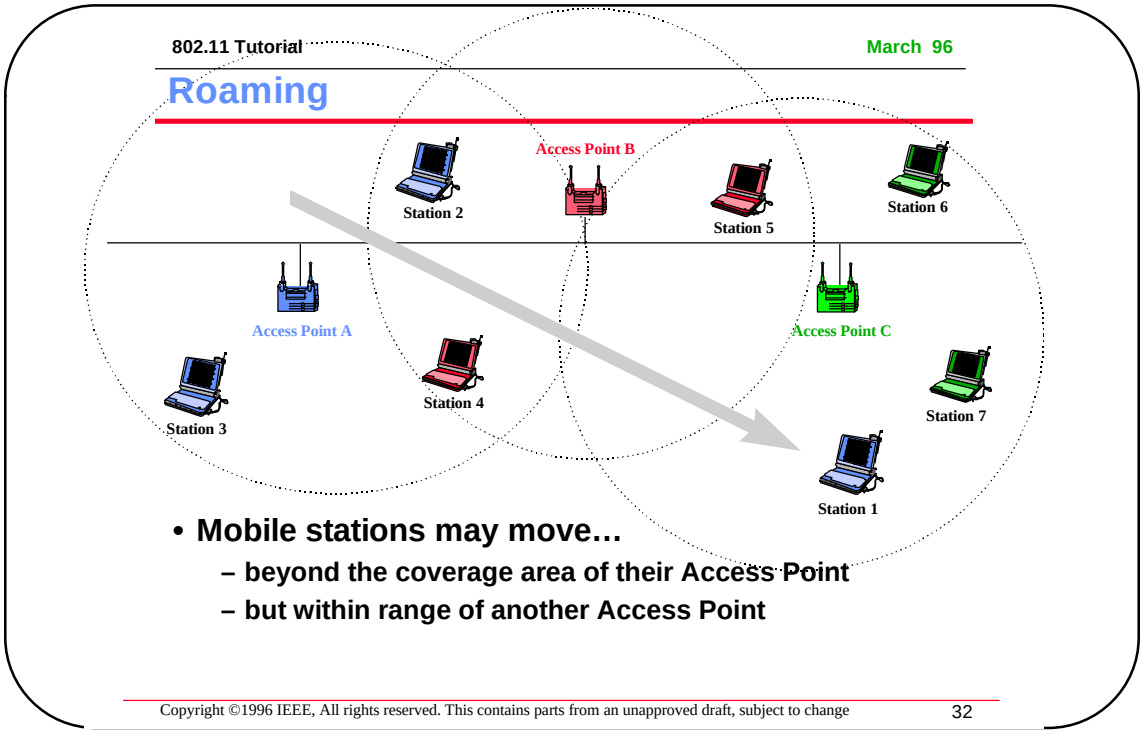
Roaming



- Mobile stations may move…

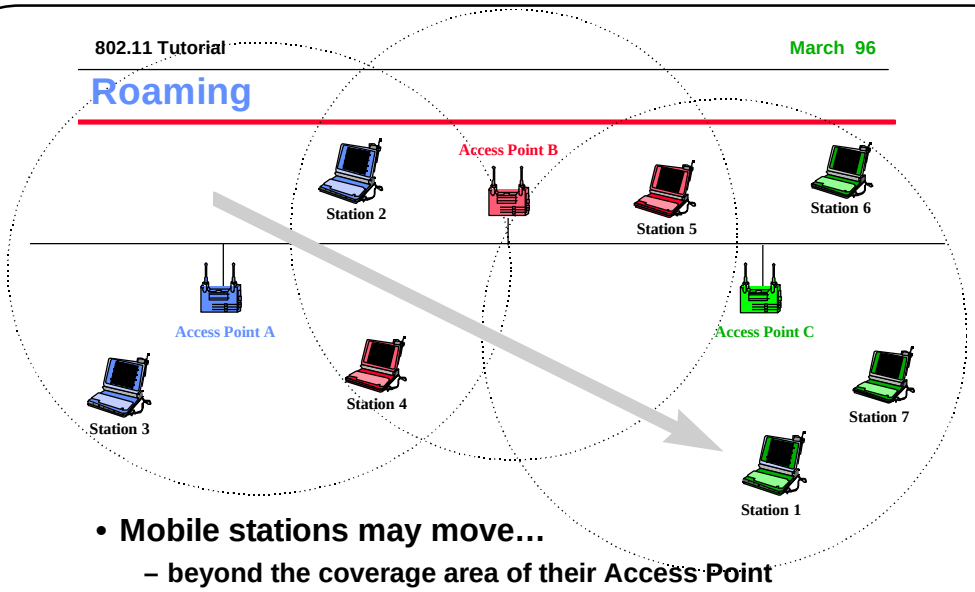
 30


802.11 Tutorial
March 96
Roaming
Access Point B
Station 2
Station 5
Station 6
Access Point A
Access Point C
Station 1
Station 4
Station 3
Station 7
• Mobile stations may move…
– beyond the coverage area of their Access Point
Copyright ©1996 IEEE, All rights reserved. This contains parts from an unapproved draft, subject to change
31


802.11 Tutorial
March 96
Roaming
Access Point B
Station 2
Station 5
Station 6
Access Point A
Access Point C
Station 4
Station 7
Station 3
Station 1
• Mobile stations may move…
– beyond the coverage area of their Access Point
– but within range of another Access Point
Copyright ©1996 IEEE, All rights reserved. This contains parts from an unapproved draft, subject to change
32

802.11 Tutorial March 96

Roaming



- 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

 33

802.11 Tutorial March 96

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
- 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

 34

802.11 Tutorial March 96

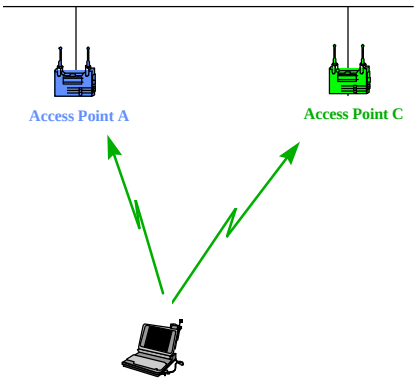
Scanning

- Scanning required for many functions.
  - finding and joining a network
  - finding a new AP while roaming
  - initializing an Independent BSS (ad hoc) network
- 802.11 MAC uses a common mechanism for all PHY.
  - single or multi channel
  - passive or active scanning
- Passive Scanning
  - Find networks simply by listening for Beacons
- Active Scanning
  - On each channel
    - » Send a Probe, Wait for a Probe Response
- Beacon or Probe Response contains information necessary to join new network.

 35

802.11 Tutorial March 96

Active Scanning Example



Steps to Association:

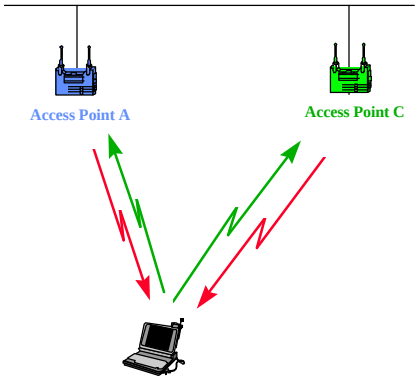
Station sends Probe.

Initial connection to an Access Point

 36

802.11 Tutorial March 96

Active Scanning Example



Steps to Association:

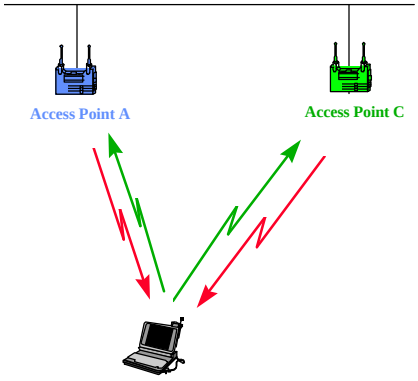
- Station sends Probe.
- APs send Probe Response.

Initial connection to an Access Point

 37

802.11 Tutorial March 96

Active Scanning Example



Steps to Association:

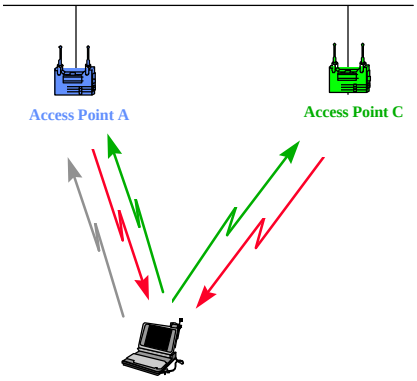
- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.

Initial connection to an Access Point

 38

802.11 Tutorial March 96

Active Scanning Example



Steps to Association:

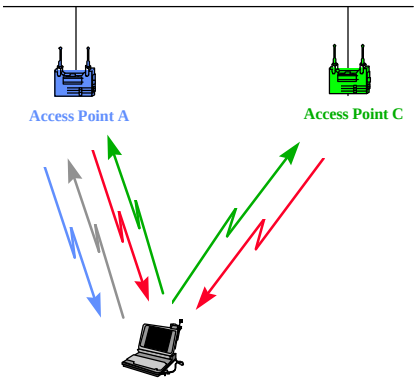
- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.

Initial connection to an Access Point

 39

802.11 Tutorial March 96

Active Scanning Example



Steps to Association:

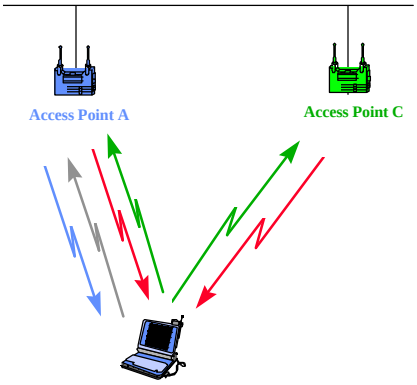
- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.
- AP sends Association Response.

Initial connection to an Access Point

 40

802.11 Tutorial March 96

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

 41

802.11 Tutorial March 96

MAC Management Frames

- **Beacon**
  - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
  - Traffic Indication Map
- **Probe**
  - ESSID, Capabilities, Supported Rates
- **Probe Response**
  - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
  - same for Beacon except for TIM
- **Association Request**
  - Capability, Listen Interval, ESSID, Supported Rates
- **Association Response**
  - Capability, Status Code, Station ID, Supported Rates

 42

More MAC Management Frames

- Reassociation Request
  - Capability, Listen Interval, ESSID, Supported Rates, Current AP Address
- Reassociation Response
  - Capability, Status Code, Station ID, Supported Rates
- Disassociation
  - Reason code
- Authentication
  - Algorithm, Sequence, Status, Challenge Text
- Deauthentication
  - Reason

802.11 MAC

the end…

