# Topic 4

## Wireless LAN – IEEE 802.11

What we will learn in this lecture:

- Basics of IEEE 802.11
- MAC layer
  - CSMA/CA
- Security
  - WEP protocol

# Wireless LANs: Characteristics

- Types
  - Infrastructure based
  - Adhoc
- Advantages
  - Flexible deployment
  - Minimal wiring difficulties
  - More robust against disasters (earthquake etc)
  - Historic buildings, conferences, trade shows,…
- Disadvantages
  - Low bandwidth compared to wired networks (1-10 Mbit/s)
  - Proprietary solutions
  - Need to follow wireless spectrum regulations

# Transmission: Infrared vs. Radio

- Infrared
  - uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)
- Advantages
  - simple, cheap, available in many mobile devices
  - no licenses needed
  - simple shielding possible
- Disadvantages
  - interference by sunlight, heat sources etc.
  - many things shield or absorb IR light
  - low bandwidth
- Example
  - IrDA (Infrared Data Association) interface available everywhere

- Radio
  - typically using the license free ISM (Industrial Scientific Medical) band at 2.4 GHz (or **Unlicensed National Information Infrastructure** (**U-NII**) at 5.0 Ghz)
- Advantages
  - experience from wireless WAN and mobile phones can be used
  - coverage of larger areas possible (radio can penetrate walls, furniture etc.)
- Disadvantages
  - very limited license free frequency bands
  - shielding more difficult, interference with other electrical devices
- **Example**
  - WiFi, WaveLAN, HIPERLAN, Bluetooth

# Wireless LAN

- operate in a local area
  - less than 100 m
- provide access to wired LANs and the Internet
- provide high data rates
  - currently, up to 54 Mbps

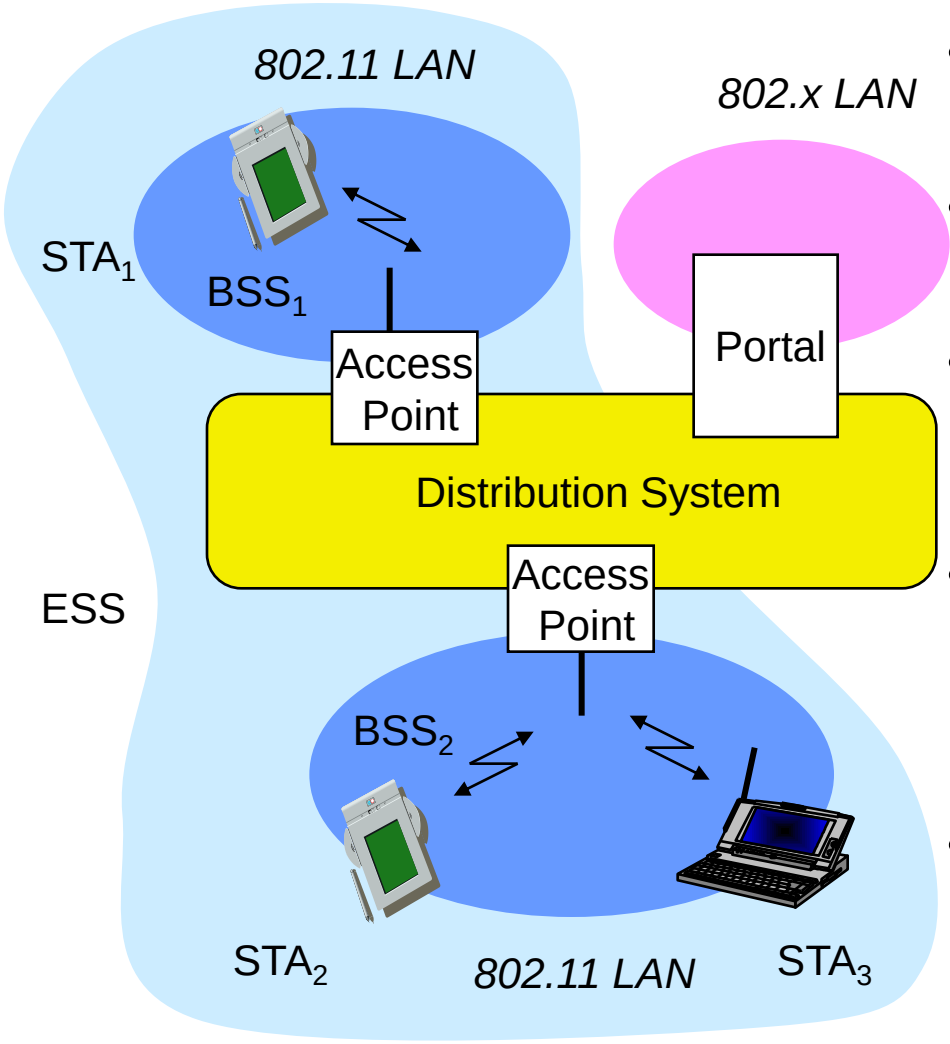
# Major Standards for WLAN

- HIPERLAN
  - High Performance Radio LAN
  - European standard
- IEEE 802.11
  - US standard
  - today, it holds the entire market
  - Only this standard will be mainly discussed here

# Two Modes of IEEE 802.11

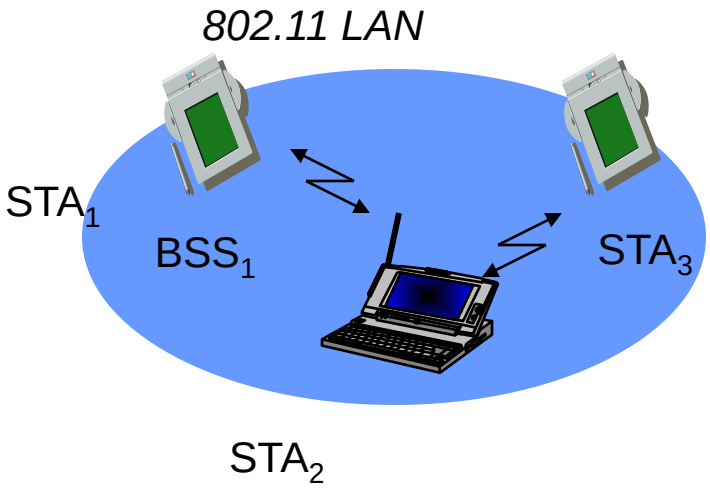
- Infrastructure Mode
  - Terminals communicate to an access point.
- Ad Hoc Mode
  - Terminals communicate in a peer-to-peer basis without any access point.

# 802.11 - Infrastructure Mode

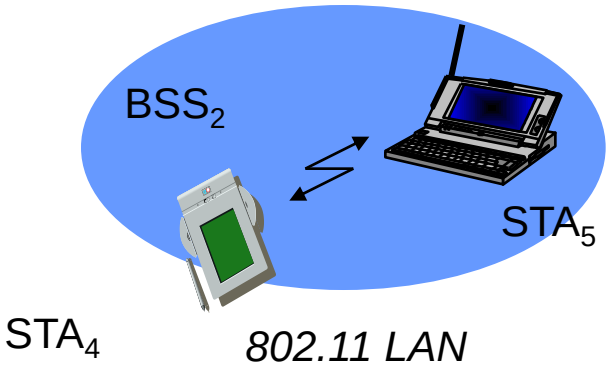



- Station (STA)
  - Wireless terminals
- Basic Service Area (BSA)
  - Coverage area of one access point
- Basic Service Set (BSS)
  - group of stations controlled by the same AP
- Distribution System (DS)
  - Fixed infrastructure used to connect several BSS to create an Extended Service Set (EES)
- Portal
  - bridge to other (wired) networks

# 802.11 – Ad Hoc mode




- Terminals communicate in a peer-to-peer basis.



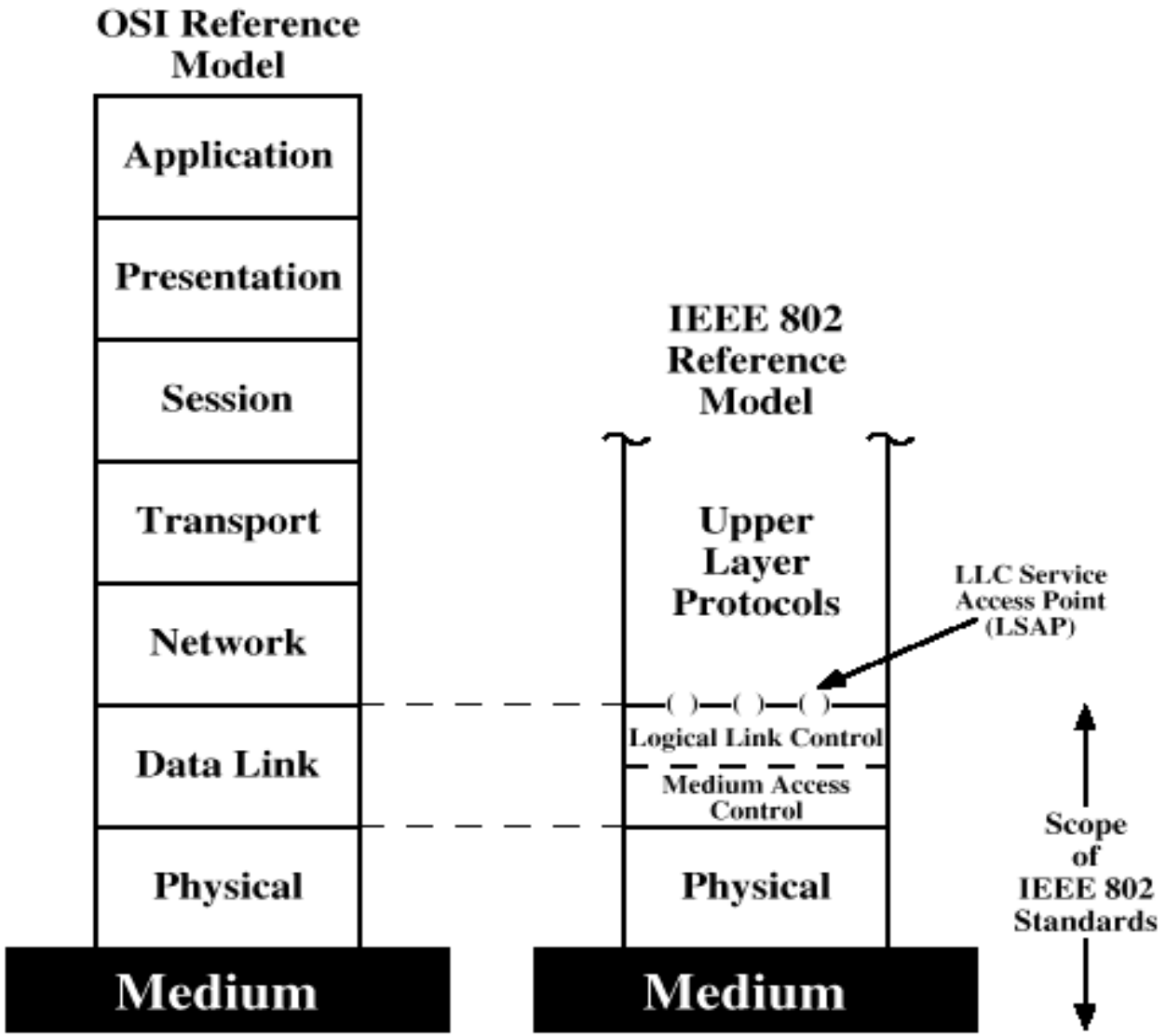
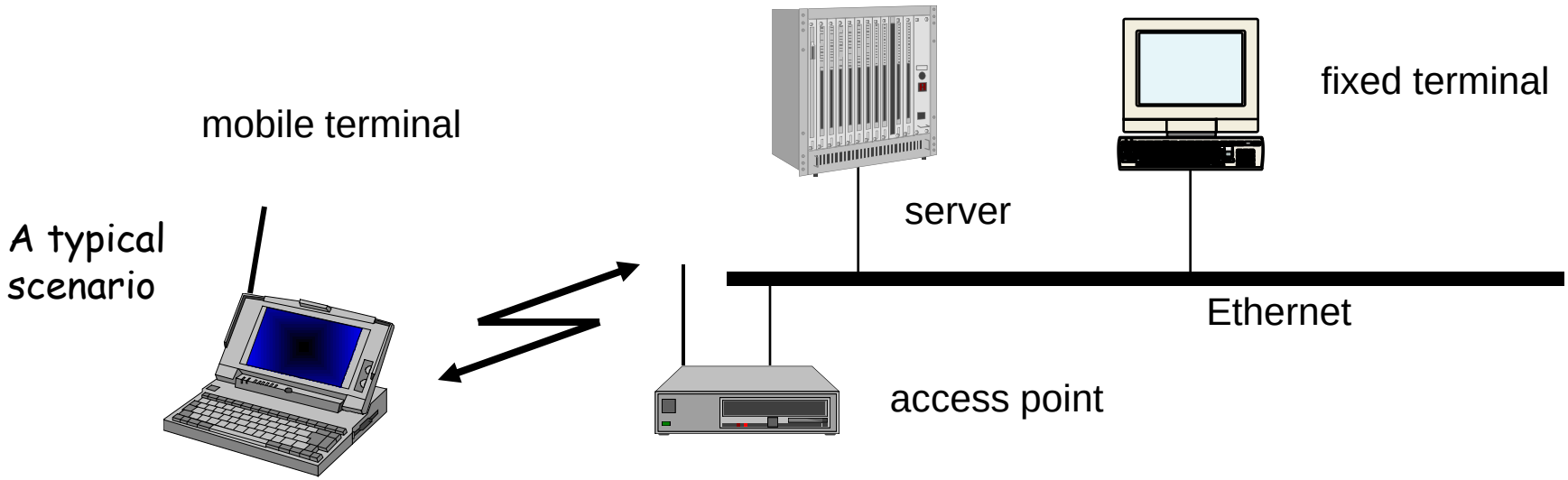
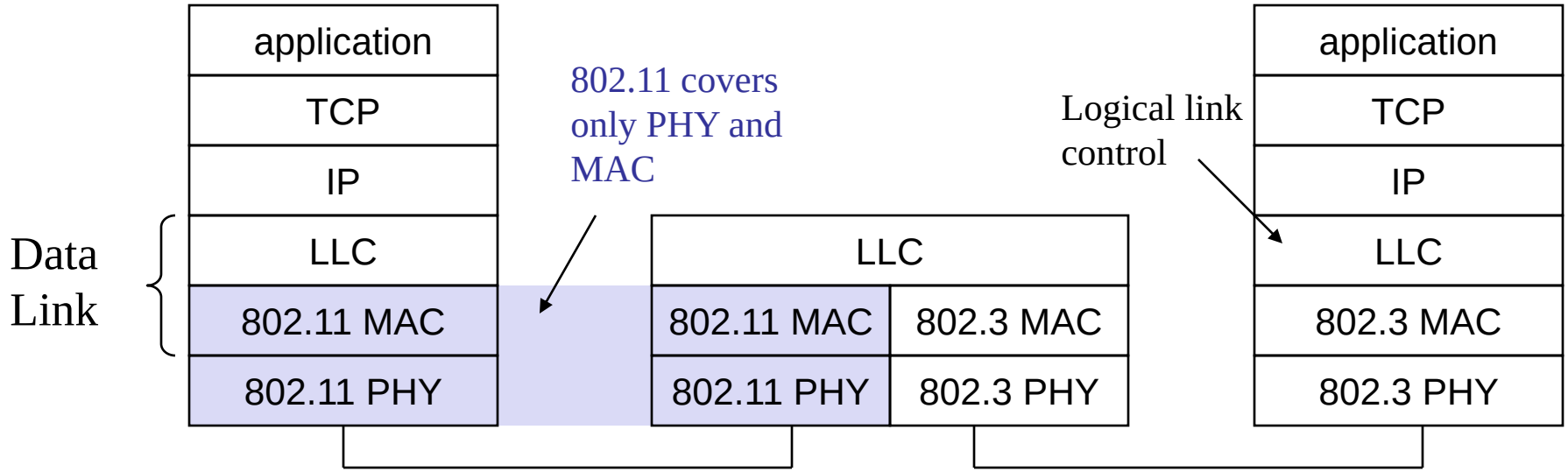



**Figure 14.1 IEEE 802 Protocol Layers Compared to OSI Model**

# Protocol Architecture



# Functions of Each Layer

- Physical Layer
  - Encoding/decoding of signals
  - Bit transmission/reception
- Medium Access Control (MAC) Layer
  - On transmission, assemble data into a frame for transmission
  - On reception, disassemble frame and perform error detection
  - Coordinate users' access to the transmission medium
- Logical Link Control (LLC) Layer
  - Provide an interface to upper layers
  - Perform flow and error control

# Physical Layer

802.11 supports 3 different PHY layers

- Infrared
  - simple and cheap
  - requires line of sight (LOS)
- Radio (2 types)
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
  - can cover a larger area (e.g. penetrate walls)

# Main IEEE 802.11 Standards

| Standard | Spectrum | Bit Rate | Transmission | Compatibility |
|---|---|---|---|---|
| 802.11 (1997) | wavelength between 850 and 950 nm; 2.4 GHz | 1/2 Mbps | Infrared / FHSS / DSSS | N/A |
| 802.11a (1999) | 5.0 GHz | 54 Mbps | OFDM | None |
| 802.11b (Wi-Fi) (1999) | 2.4 GHz | 11 Mbps (ARS) | DSSS | 802.11 |
| 802.11g (June, 2003) | 2.4 GHz | 54 Mbps | OFDM | 802.11 / 802.11b |
| 802.11n (Sept, 2009) | 2.4 GHz or 5 GHz | 600 Mbps (PHY & MAC) | MIMO, OFDM | all |

# How to join a network?

Infrastructure Mode

# Steps to Join a Network

1. Discover available network
   - i.e. basic service set (BSS)
2. Select a BSS
3. Authentication
4. Association

# 1. Discovering Available Network

- Passive Scanning
  - Each AP broadcasts periodically a Beacon frame, which includes:
    - AP's MAC address, Network name (also known as Service Set Identifier, SSID), etc.
- Active Scanning
  - Station sends a Probe Request frame
  - AP responses with a Probe Response frame, which includes
    - AP's MAC address, SSID, etc.
- A method (Active or passive) is chosen according to the power consumption/performance trade-off.

# 2. Choosing a Network

- The user selects from available networks
- Common criteria for selecting a network are:
  - User choice
  - Strongest signal
  - Most recently used

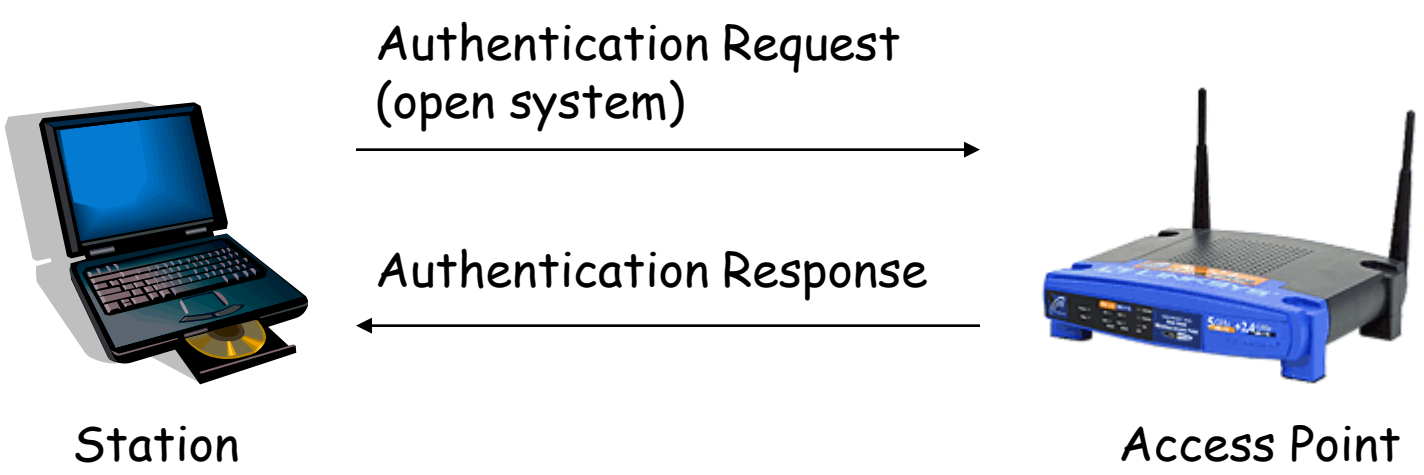
# 3. Authentication

- Authentication
  - A station proves its identity to the AP.

- Two Mechanisms
  - Open System Authentication
  - Shared Key Authentication

# Open System Authentication

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



# Shared Key Authentication

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

Station

Authentication Request
(shared key)

128-byte "Challenge" text string, generated randomly

"Challenge" text string, encrypted with shared key

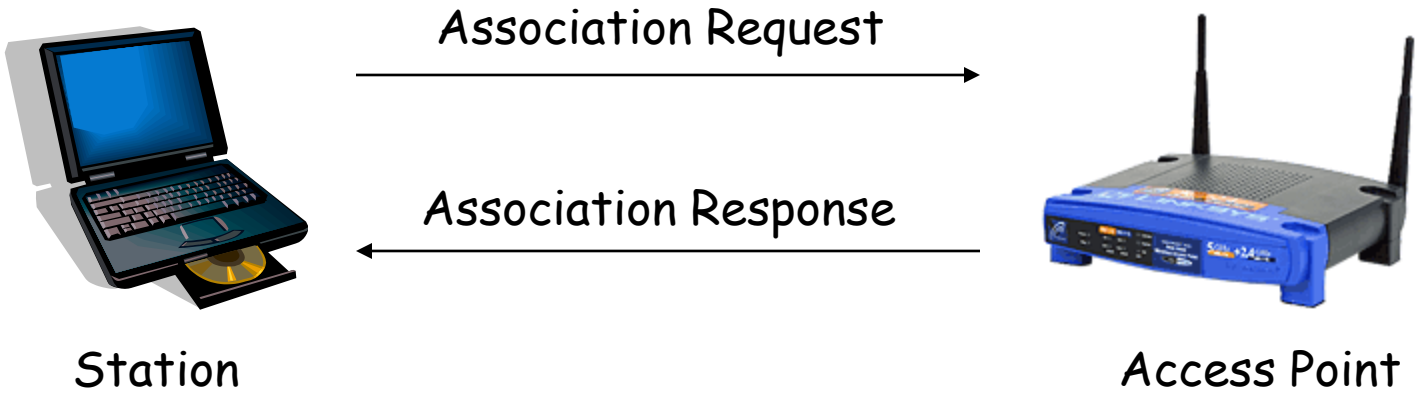
Positive or negative response based on decryption result

Access Point

Note: "Challenge" is encrypted by WEP algorithm.

# 4. Association

The station needs to register to the AP.



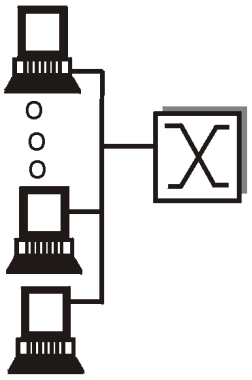

During this process, the wireless devices make transitions from one state to others. These states are: (1). Unauthenticated and Unassociated. (2). Authenticated and unassociated and (3). Authenticated and associated

# How to transmit?

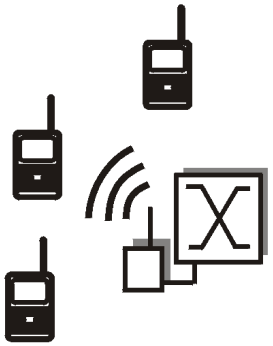
The MAC layer

# Media Access Control

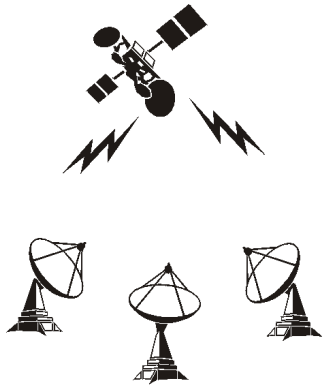
- How to share a common medium among the users?



shared wire
(e.g. Ethernet)



shared wireless
(e.g. Wavelan)



satellite


cocktail party

# Motivation

- Can we apply media access methods from fixed networks?

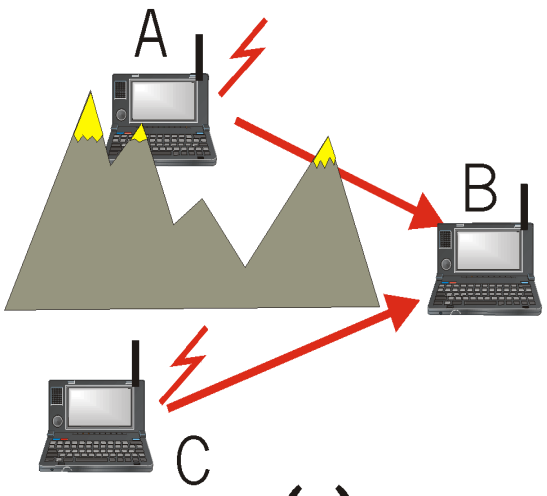
- Example: CSMA/CD
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - Method used in IEEE 802.3 Ethernet

# CSMA/CD

- *Carrier Sense: Listen before talk*
  - Sense the channel
  - If the channel is idle, transmit
  - If the channel is busy,
    - waits a random amount of time
    - sense the channel again
- *Collision Detection: Stop if collision occurs*
  - If there is a collision,
    - stops transmission immediately,
    - waits a random amount of time
    - senses the channel again

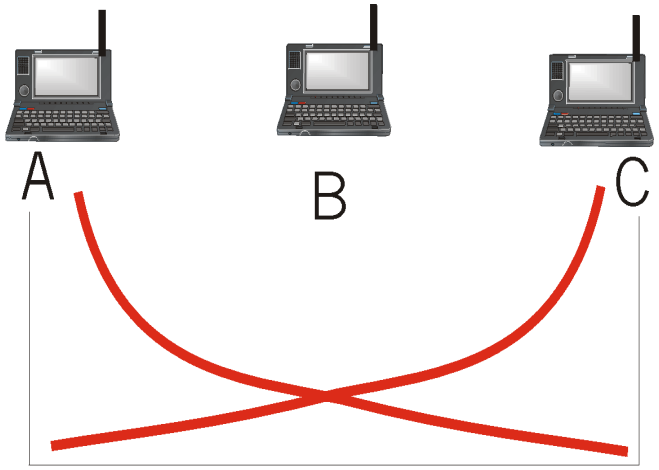
# Hidden Terminal Problem

- *A*, *C* cannot hear each other (CS fails)
- Collisions at *B*, undetected (CD also fails)




(a)

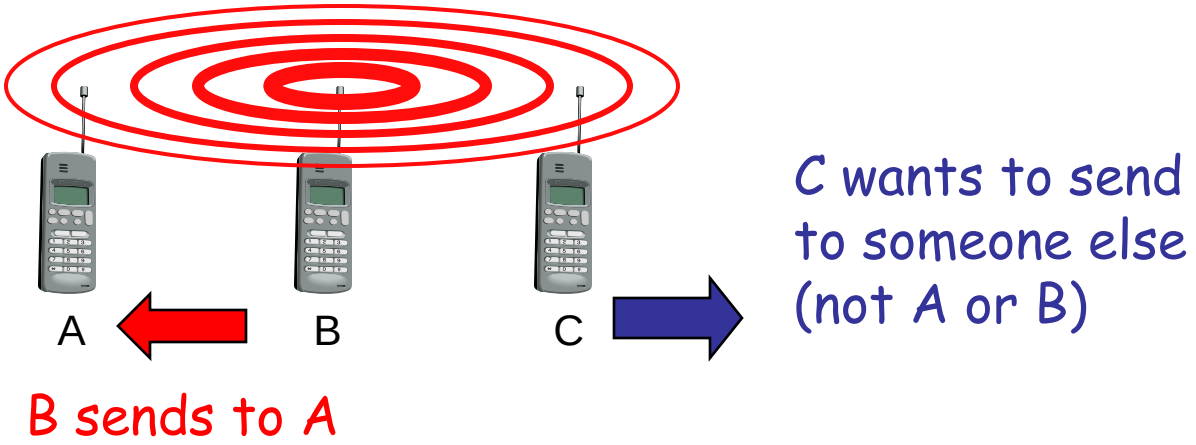
Obstacles




(b)

Signal Attenuation

# Exposed Terminal Problem

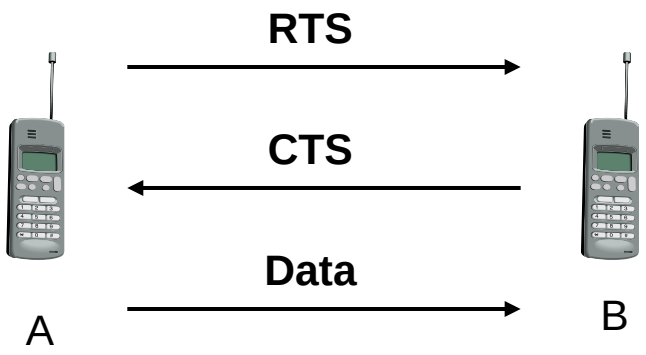



- *C* has to wait, since CS signals a medium in use
- But A is outside the radio range of *C*; therefore waiting is not necessary
- *C* is "exposed" to *B*

# (MACA) Multiple Access with Collision Avoidance

- IEEE 802.11 is based on the idea of MACA
- MACA uses a three-way handshake protocol
- Short signaling packets are used
  - RTS (request to send)
    - sender request the right to send from a receiver with a short RTS packet before it sends a data packet
  - CTS (clear to send)
    - receiver grants the right to send as soon as it is ready to receive
- The sender then sends the DATA.
- Signaling (RTS/CTS) packets contain
  - sender address
  - receiver address
  - packet size (or duration of data transmission)

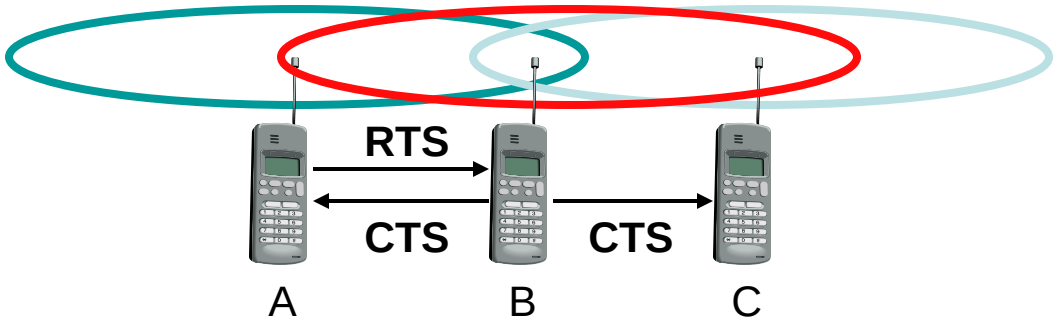
# An Illustration: 3-way handshake




Can it solve the hidden terminal problem?

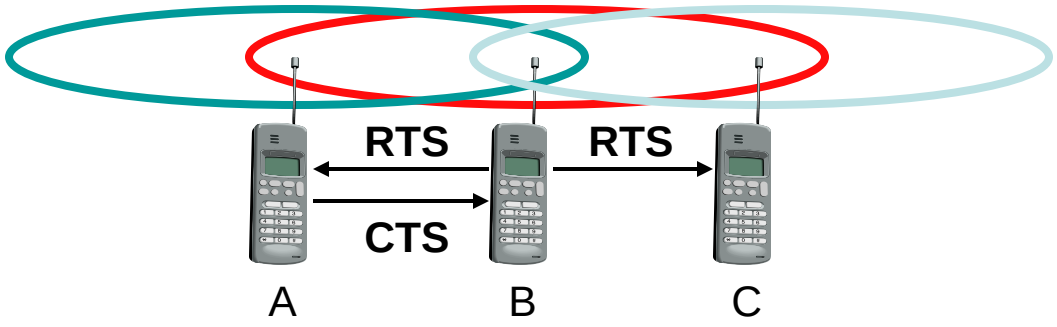
Can it solve the exposed terminal problem?

# A Solution: Hidden Terminal




- MACA avoids the hidden terminal problem
  - Both A and C want to send to B
  - A sends RTS first
  - C waits after receiving CTS from B

# A Solution: Exposed Terminal

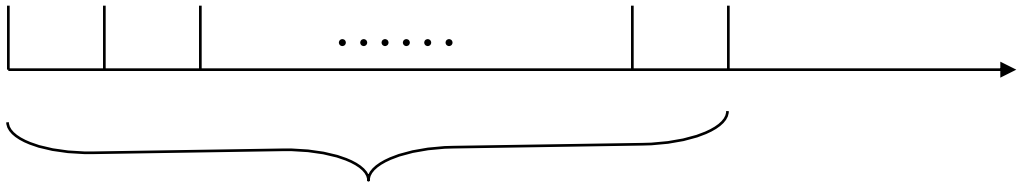



- MACA avoids the exposed terminal problem
  - B wants to send to A, while C to another terminal
  - now C does not have to wait, for it cannot receive CTS from A

# Packet Collision

- Collisions may occur during RTS-CTS exchange.

packet collision occurs




Next attempt: Transmit at a random slot over the contention window

How large is the contention window?

# Binary Exponential Backoff

- The contention window size is adjusted dynamically.
  - binary exponential backoff is used.

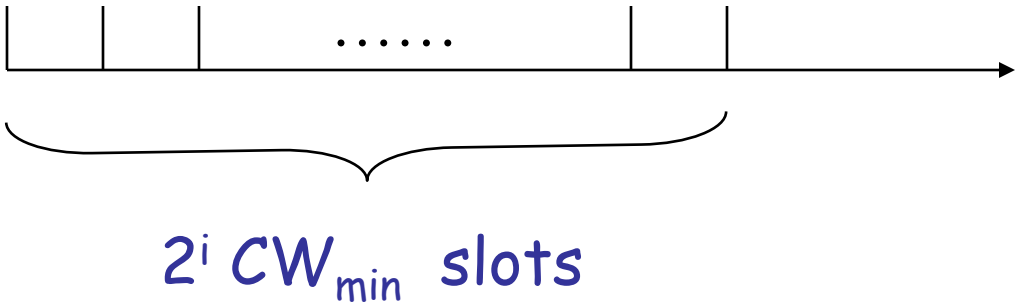
- When a terminal fails to receive CTS in response to its RTS, it increases the contention window
  - *cw* is doubled (up to an upper bound, $CW_{max}$)

- When a node successfully completes a data transfer, it restores *cw* to $CW_{min}$

# Binary Exponential Backoff

- The contention window size is doubled whenever a collision occurs.

A packet experiences i collisions



# (MACAW) MACA for Wireless LAN

- Fair access of media by learning/setting backoff counter value from a packet transmission (carried in packet header)
- Wild oscillation on backoff counter value is prevented by defining new **Multiplicative Increase Linear Decrease** (MILD) backoff updation functions (multiplied by 1.5 and decreased by 1)
- Changes in basic message exchange (RTS-CTS-DATA)
  - Inclusion of ACK packet (i.e. RTS-CTS-DATA-ACK)
    - If sender after sending DATA does not receive ACK, it schedules data packet for retransmission.
    - If not DATA but ACK was lost, the receiver will return ACK after receiving RTS for retransmitted packet

# (MACAW) MACA for Wireless LAN

- Inclusion of DS (Data Sending) packet (i.e. RTS-CTS-DS-DATA-ACK)
- After successful exchange of RTS-CTS, sender sends a small control packet (DS) so that all stations which are in the vicinity of sender can know that the RTS-CTS exchange was successful and a data transmission is about to follow.
- These overhearing stations defer all transmissions until the DATA-ACK transmission is over (Restriction in transmissions by exposed terminals).
- If a Node has to send more than one Frame, it has to wait a random time after each successful transmission and compete with other adjacent nodes
- Request for RTS (RRTS) is sent to a node (who is initially unaware of receiver being waiting for a data transfer to complete) to immediately proceed with a normal RTS-CTS sequence.

# IEEE 802.11 MAC Protocols

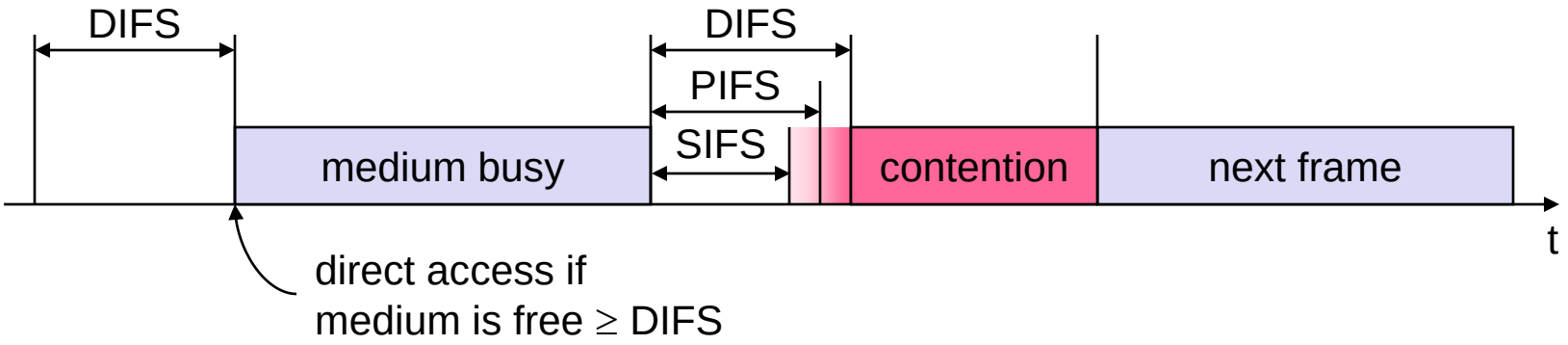
- Two traffic services are supported
  - **Asynchronous Data Service**
    - Best-effort services
  - **Time-bounded Service (optional)**
    - Guarantee a maximum delay
    - Available only in infrastructure mode

# Two Classes of Access Mechanisms

- Distributed Coordination Function (DCF)
  - Support asynchronous data services
  - CSMA/CA (with minor modification)
  - CSMA/CA with RTS/CTS exchange (optional)
- Point Coordination Function (PCF) (optional)
  - Support time-bounded services
  - Polling from AP

# Inter-Frame Spacings (for waiting time before medium access)

- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF IFS)
  - lowest priority, for asynchronous data service
- EIFS (Extended IFS)
  - Longest IFS used by a station that has received a pkt that it could not understand (duration info for virtual carrier sense).



# Method 1a: CSMA/CA

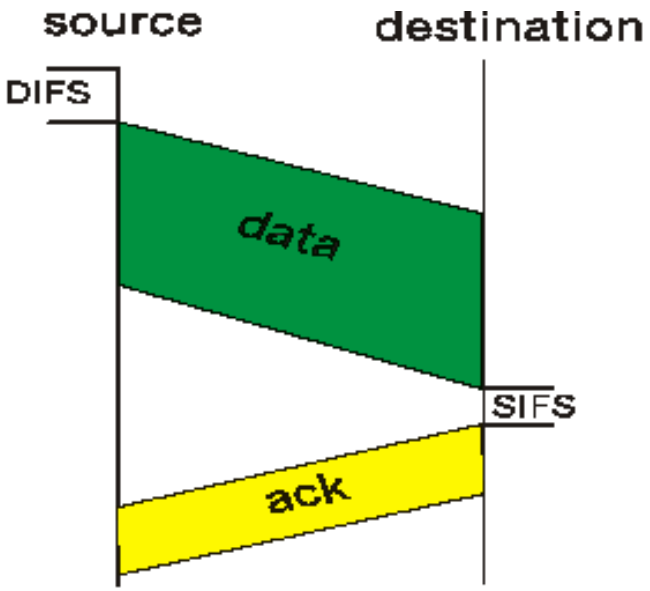
802.11 CSMA/CA: sender

- if sense channel idle for **DIFS** sec.(plus a RBT(Random Backoff Time) if the medium was busy)
  then transmit entire frame (no collision detection)
- if sense channel busy
  then wait for the channel to become idle for DIFS and choose a random backoff time and countdown the backoff timer for every free slot

802.11 CSMA/CA: receiver

if received OK

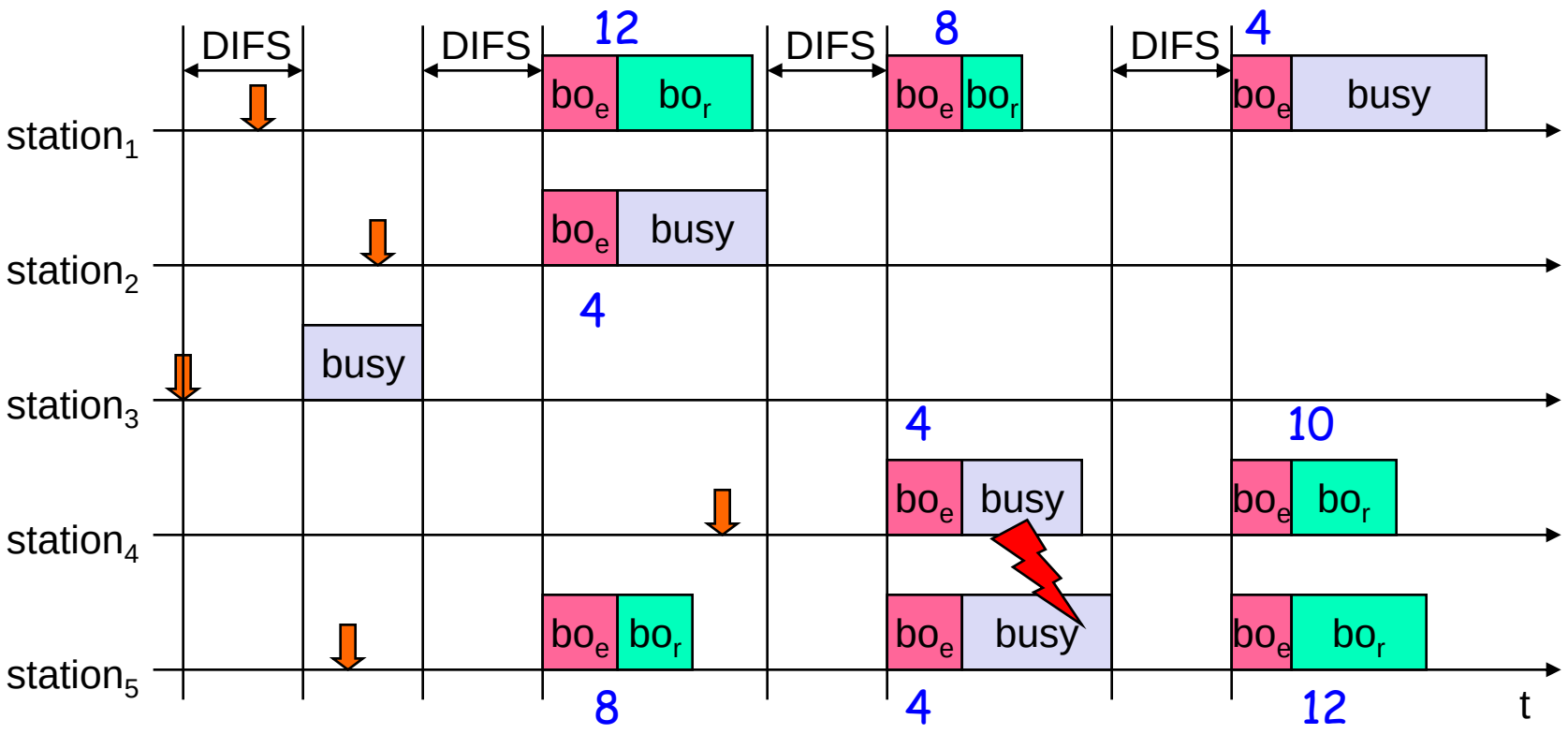
return ACK (16 bytes) after **SIFS**




DIFS: Distributed Inter Frame Spacing

SIFS: Short Inter Frame Spacing

# Example (with backoff timer)




busy — medium not idle (frame, ack etc.)

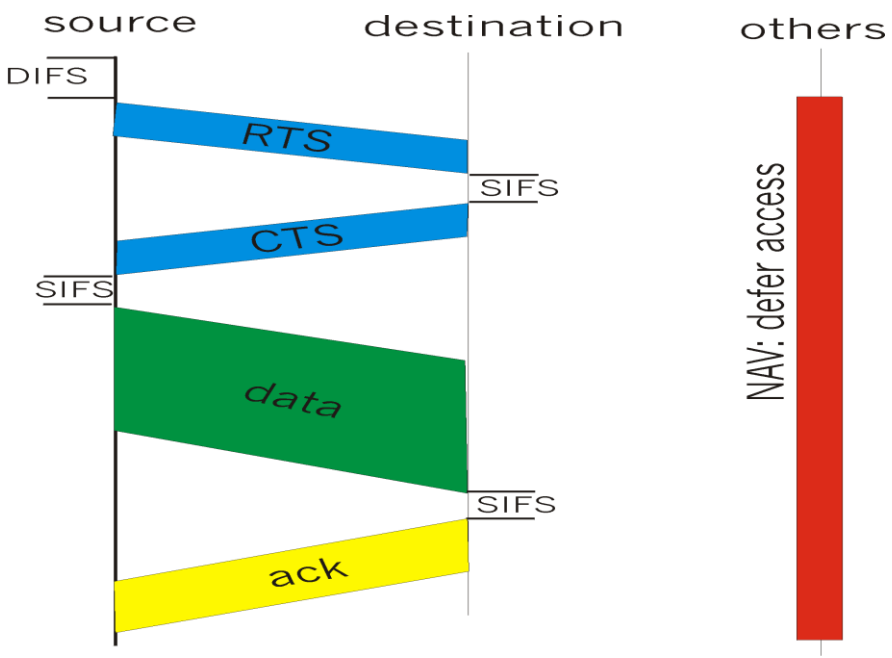
packet arrival at MAC

$bo_e$ — elapsed backoff time

$bo_r$ — residual backoff time

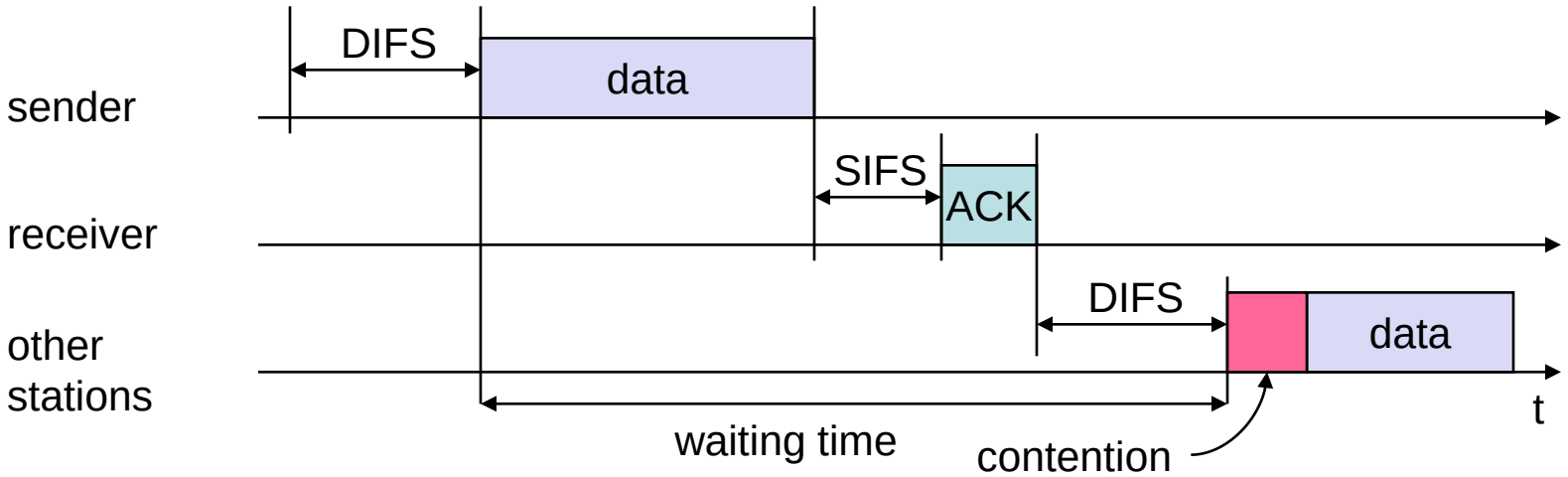
# Method 1b: CSMA/CA with RTS-CTS

- CSMA/CA: explicit channel reservation
  - sender: send RTS (20 bytes)
  - receiver: reply with CTS (16 bytes)
- CTS reserves channel for sender, notifying (possibly hidden) terminals



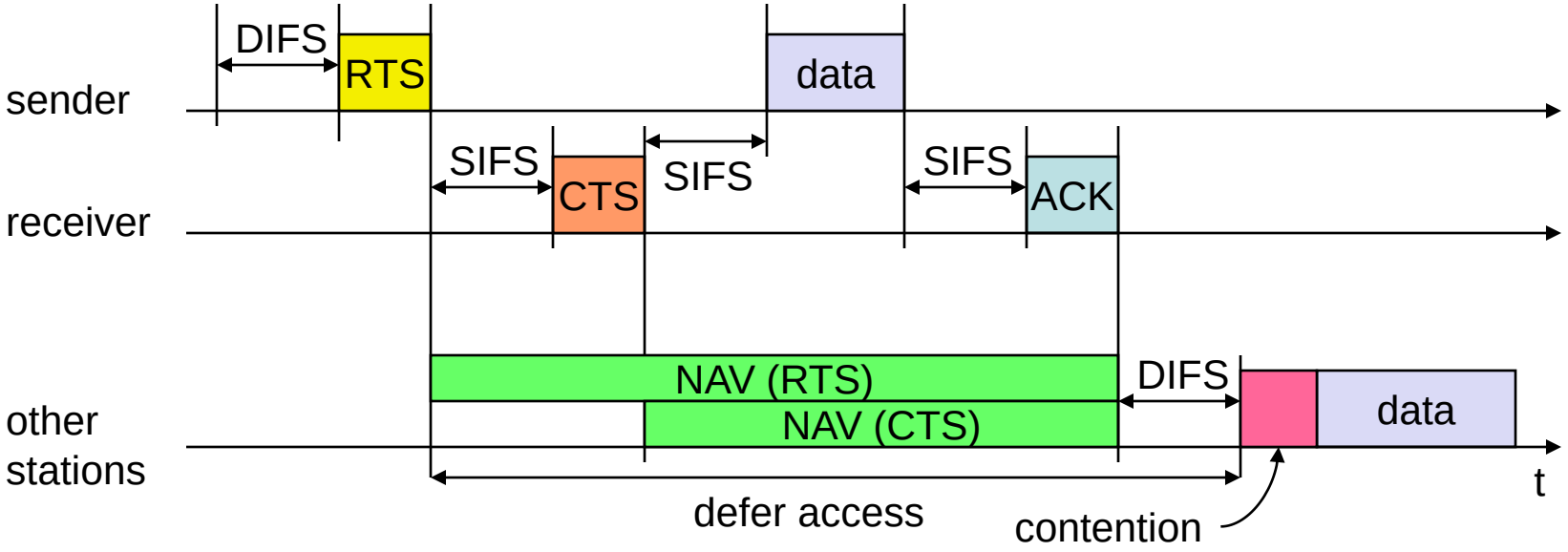

4-way handshake

# No Collision during Data Transmission




How can other stations know how long the waiting time is?

# Net Allocation Vector (reserves the medium for one sender exclusively)




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

Other stations hear the RTS packet set their NAV accordingly.

The CTS packet also has the duration field.

Other stations hear the CTS packet set their NAV accordingly.

# Using RTS/CTS

- Removes (reduces) hidden terminal problem
- Collision may occur at the beginning of transmission (RTS/data packets)
- Non-negligible overhead (b/w and delay) due to extra control frames
- RTS Threshold to determine when to use/disable RTS/CTS option (based on frame size)

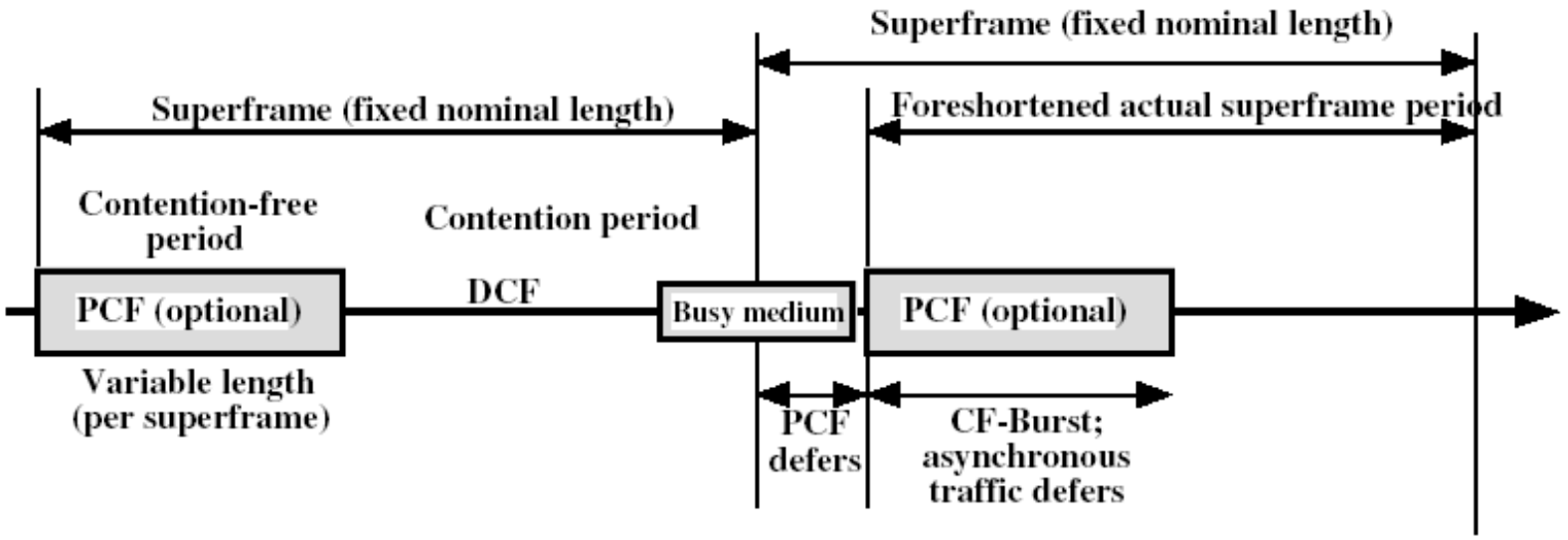
# Fragmentation

- Probability of erroneous frame is much higher in Wireless LAN compared to wired LAN (BER is higher) assuming same frame length.
- Using shorter frames to decrease error prob of frames
- IEEE 802.11 specifies a fragmentation mode
- MAC layer adjusts the frame size according to current error rates.
- RTS carries duration of 1st frag including ACK
- Frag 1 carries the duration of frag2 + ACK2 and ACK1 carries duration (as CTS) and so on.

# Method 2: Point Coordination Function

- Polling by the access point (or point coordinator)
- Sends polling message after waiting for PIFS
- Since PIFS is smaller than DIFS, it can lock out all asynchronous traffic
  - To prevent this, an interval called **superframe** is defined.

# Two parts of a Superframe




## Contention-free Period:

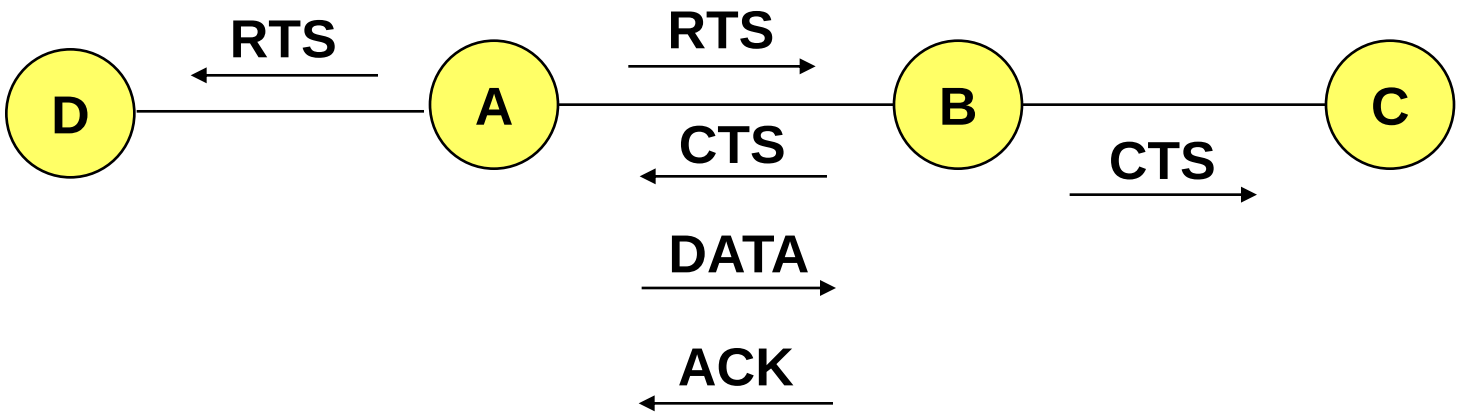
The point coordinator polls stations with time-bounded service in a round-robin fashion

## Contention Period:

The point coordinator idles for the remainder of the superframe, allowing for asynchronous access.

# MAC: Reliability

- Wireless links are prone to errors. High packet loss rate detrimental to transport-layer performance.
- Solution: Use of acknowledgements
  - When B receives DATA from A, B sends an ACK.
  - If A fails to receive an ACK, A retransmits the DATA.
  - Both C and D remain quiet until ACK (to prevent collision of ACK).
  - Expected duration of transmission+ACK is included in RTS/CTS packets.
  - This approach adopted in many protocols [802.11].

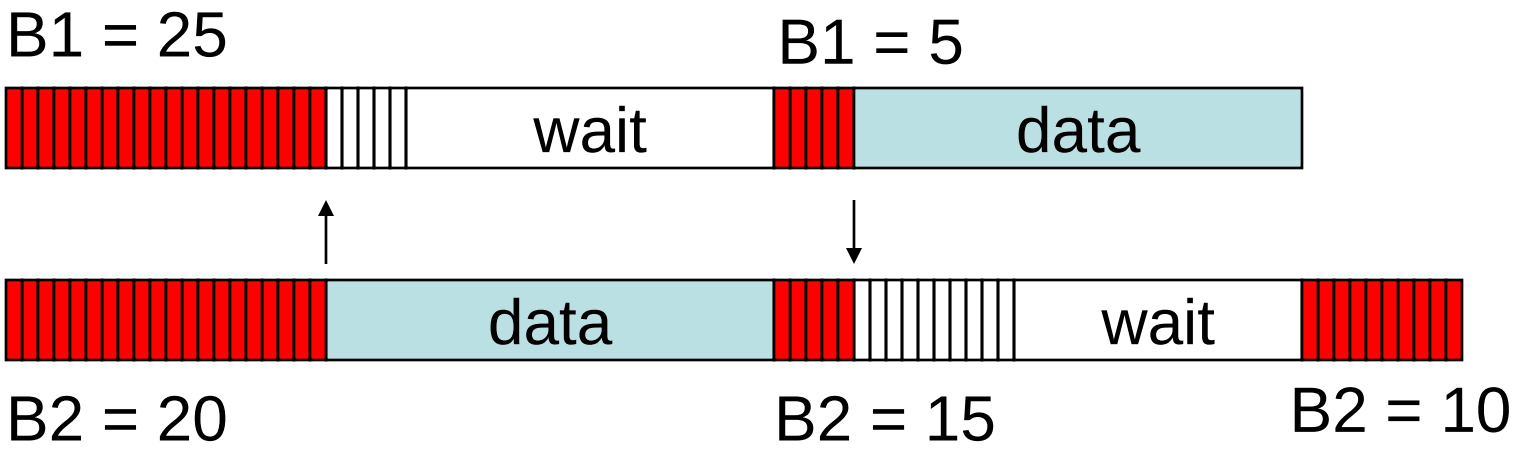



- Collision of RTS/CTS packets can happen (hidden terminal).
  - If no CTS, retransmit RTS after backoff.

# MAC: Collision Avoidance

- With half-duplex radios, collision detection is not possible
- Collision avoidance: Once channel becomes idle, the node waits for a randomly chosen duration before attempting to transmit
- IEEE 802.11 DCF
  - When transmitting a packet, choose a backoff interval in the range [0,cw]; cw is contention window
  - Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - When backoff interval reaches 0, transmit RTS
- Time spent counting down backoff intervals is part of MAC overhead
- *large* cw leads to larger backoff intervals
- *small* cw leads to larger number of collisions

# DCF Example




**cw = 31**

**B1 and B2 are backoff intervals at nodes 1 and 2**

# MAC: Congestion Control

- Number of nodes attempting to transmit simultaneously may change with time; some mechanism to manage congestion is needed.
- IEEE 802.11 DCF: Congestion control achieved by dynamically choosing the contention window cw
- Binary Exponential Backoff in DCF:
  - When a node fails to receive CTS in response to its RTS, it increases the contention window
    - cw is doubled (up to a bound **CWmax**)
  - Upon successful completion data transfer, restore cw to **CWmin**
- Optimization: MACAW
  - 802.11: cw reduces much faster than it increases
  - Backoff: multiply cw by 1.5 (instead of doubling)
  - Restore: Reduce cw by 1 (instead of CWmin)
  - cw reduces slower than it increases. Exponential increase linear decrease
  - Avoids wild oscillations of cw when congestion is high.

# MAC: Energy Conservation

- Wireless nodes need to conserve power ("resource poor").
- **Typical solution:** Turning the radio off when not needed
- Power Saving Mode in IEEE 802.11 (Infrastructure Mode)
  - An Access Point periodically transmits a beacon indicating which nodes have unicast frames waiting for them (Traffic Indication Map, TIM)
  - Each power saving (PS) node wakes up periodically to receive the beacon
  - If a node has a packet waiting, then it sends a **PS-Poll**
    - After waiting for a backoff interval in [0,CWmin]
  - Access Point sends the **DATA** in response to PS-poll

# MAC: Energy Conservation (cont'd)

- Power Saving Mode in IEEE 802.11 (Infrastructure Mode)
  - An Access Point periodically (usually with period which is multiple of beacon period) transmits a beacon indicating whether any broadcast packets waiting for the nodes Delivery Traffic Indication Message (DTIM)
  - Each power saving (PS) node wakes up periodically to receive the beacon
  - If a PS node has a broadcast packet waiting, then it remains awake to receive the broadcast packets which are delivered immediately after the transmission of DTIM

# MAC: Energy Conservation (cont'd)

- Power Saving Mode (PSM) in IEEE 802.11 (Infrastructure less Mode)
  - In PSM, time is divided into beacon intervals
  - At the start of each beacon interval, every node stays awake for a duration, called the ATIM (Ad hoc Traffic Indication Message) window
  - During ATIM Window, nodes exchange control packets to determine whether they need to stay awake for the rest of the beacon interval
  - In PSM, a source node buffers packets for the destination that is in doze mode, and these packets are announced during a subsequent ATIM window using an ATIM frame
  - Transmission of an ATIM frame is performed using CSMA/CA

# MAC: Energy Conservation (cont'd)

- A node sending an ATIM frame remains awake for the rest of the beacon interval
- A node that receives an ATIM frame replies by sending an ATIM-ACK and remains awake for the entire beacon interval.
- Transmission of one or more data packets can now take place during the beacon interval, after the end of the ATIM window
- The size of ATIM window has a significant impact on energy savings and throughput achieved by nodes

# MAC Protocols: Summary

- Wireless medium is prone to hidden and exposed terminal problems

- Protocols are typically based on CSMA/CA
- RTS/CTS based signaling
- Acks for reliability

- Contention window is used for congestion control
- IEEE 802.11 wireless LAN standard
- Fairness issues are still unclear

# MAC Frame format

# IEEE 802.11 Frame format

| Preamble | PLCP Header | MAC Data | CRC |
|---|---|---|---|

**Preamble:** PHY dependent and includes – Synch (80 bit sequence of alternating 0s and 1s), SFD (Start of Frame delimiter which consists of the 16-bit binary pattern 0000 1100 1011 1101)

**PLCP Header:** Always transmitted at 1Mbps and contains logical information used by the PHY layer to decode the frame. It consists of

PLCP_PDU Length Word: which represents the no of bytes contained in the pkt.

PLCP Signaling Field : Rate information encoded in 0.5 Mbps increments from 1Mbps to 4.5 Mbps

HEC: 16 bit CRC error detection field

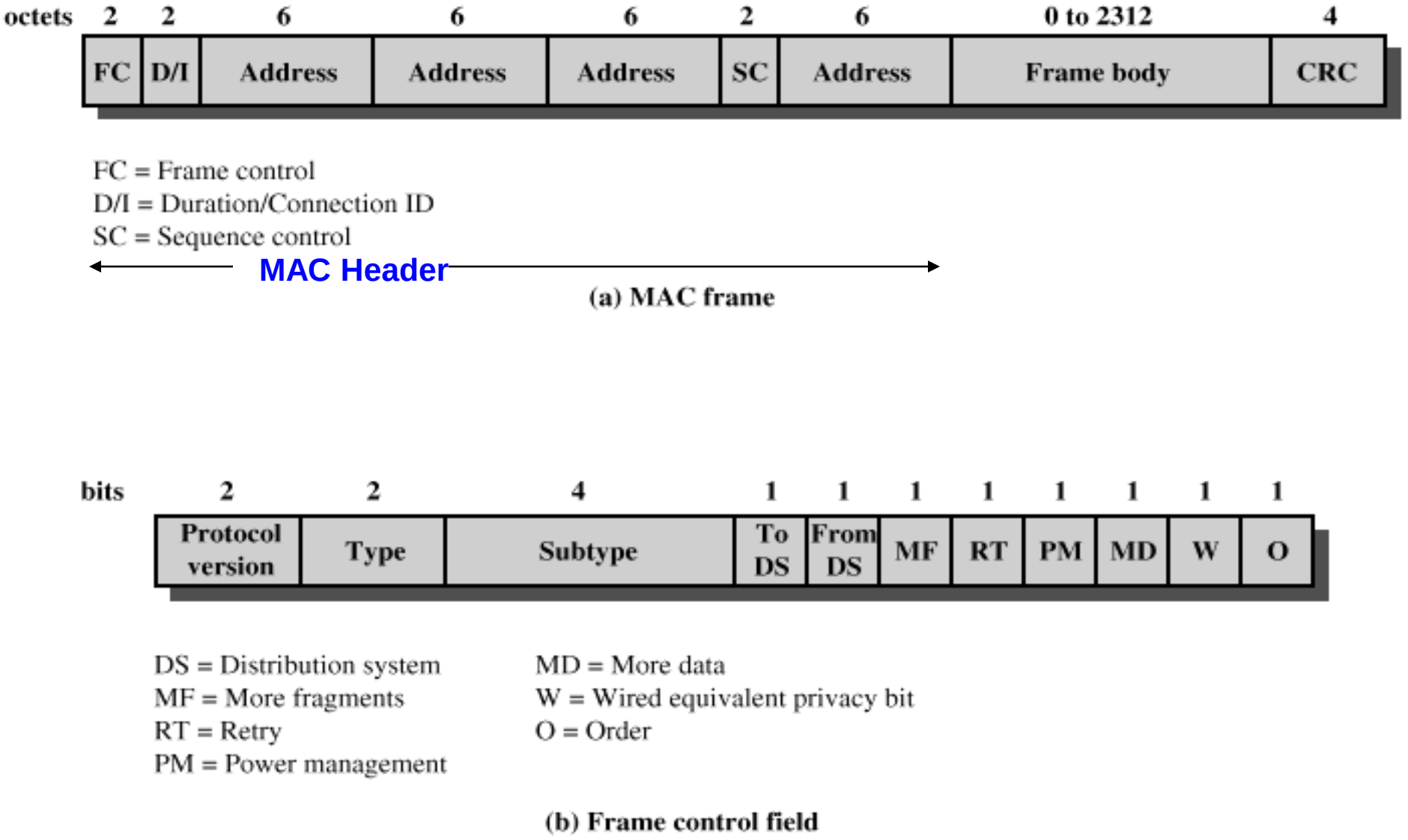



**Figure 14.8 IEEE 802.11 MAC Frame Format**

# MAC Frame Fields

- Frame Control – frame type, control information
- Duration/connection ID – channel allocation time (or STA ID in PS-poll messages)
- Addresses – context dependant, types include source and destination (may contain up to 4 addresses depending on ToDS and FromDS fields)

| ToDS | FromDS | Add1 | Add2 | Add3 | Add4 |
|---|---|---|---|---|---|
| 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 |

# MAC Frame Fields

- Add1 is always the Recipient Address (may be AP or end-station depending on ToDS)
- Add2 is always the Transmitter Address (may be AP or end-station depending on FromDS)
- Add3 is in most cases the remaining/missing address (FromDS: original SA, ToDS: orginal DA)
- Add4 is used on special case where a Wireless DS is used and the frame is being transmitted from one AP to another.
- Sequence control – numbering and reassembly (frag no. & seq. no)
- Frame body – MSDU or fragment of MSDU
- Frame check sequence – 32-bit Cyclic Redundancy Check

# Frame Control Fields

- Protocol version – 802.11 version (0 for current version)
- Type – management, control or data (11 reserved)

  magmt: system integration, form ESS, Synchronization
- Subtype – identifies function of frame (Association (Request, Response), Reassociation (Request, Response), Probe (R&R), Beacon, ATIM, Disassoc etc), (PS-poll, RTS, CTS, ACK, CF End etc), (Data, Data+CF-Ack, Data+CF-Poll, Data+CF-Ack+CF-Poll, CF-Poll etc)
- ToDS – 1 if destined for DS (to be forwarded by AP)
- FromDS – 1 if frame is coming from the DS (leaving DS)
- More fragments – 1 if fragments follow
- Retry – 1 if retransmission of previous frame

# Frame Control Fields

- Power management – 1: transmitting station will be in sleep mode after transmission of this frame (AP maintains an updated record of the PS mode nodes). Multicasts and Broadcasts are stored by AP and transmitted at pre-known time (DTIM), where all PS nodes who wish to receive this kind of frames should be awake.
- More data – Indicates that station has more data to send (used by AP in PS mode to indicate that there are more frames buffered to this station, station can use this for changing state from PS to active or vice-versa).
- WEP – 1 if wired equivalent protocol is implemented
- Order – 1 if any data frame is sent using the Strictly Ordered service

# Control Frame Subtypes

- Power save – poll (PS-Poll)
- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgment
- Contention-free (CF)-end
- CF-end + CF-ack

# Data Frame Subtypes

- Data-carrying frames
  - Data
  - Data + CF-Ack
  - Data + CF-Poll
  - Data + CF-Ack + CF-Poll
- Other subtypes (don’t carry user data)
  - Null Function
  - CF-Ack
  - CF-Poll
  - CF-Ack + CF-Poll

# Management Frame Subtypes

- Association request
- Association response
- Reassociation request (Roaming process)

  How does roaming in LAN diff. from roaming in Cellular networks? (packet based, temporary disconnection result is retransmission in upper layer)
- Reassociation response
- Probe request (Active Scanning)
- Probe response
- Beacon (timestamp,SSID, TIM etc)

# Management Frame Subtypes

- Announcement traffic indication message
- Dissociation
- Authentication
- Deauthentication

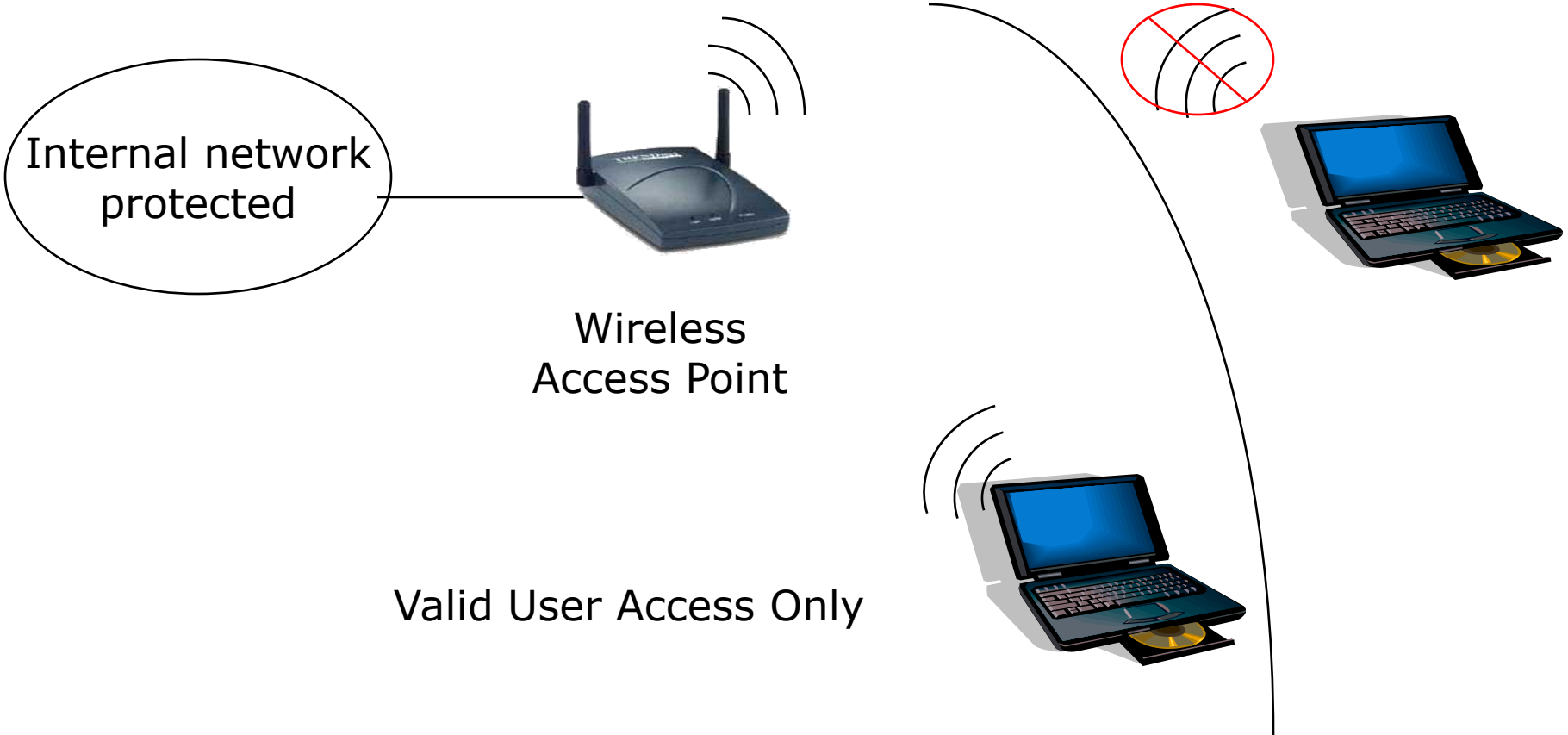
# Is it Secure?

The IEEE 802.11 Security Problem

# WLAN Security Problem

Conventionally, an organization protect itself by limiting external connections to a few well protected openings called firewall.

For wireless networks, anyone within the radio range can eavesdrop on the communication.



# Basic Security Mechanisms

1. Network Access Control based on SSID
2. MAC Address Filtering
3. Wired Equivalent Privacy (WEP)
   - Shared Key Authentication
   - Data Encryption

# Mechanism 1: SSID

- Only those stations with knowledge of the network name, or SSID, can join.
- The SSID acts as a shared secret.
- Is it secure?

# SSIDs are “useless”!

- AP periodically broadcasts the SSID in a beacon frame.
- Beacon frames are sent unprotected.
- A hacker can easily identify the SSID.

# Mechanism 2: MAC Address Filtering

- A MAC address list is maintained at each AP.
- Only those stations whose MAC addresses are listed are permitted access to the network.
- Is it secure?

# MAC Address as Identity is Weak

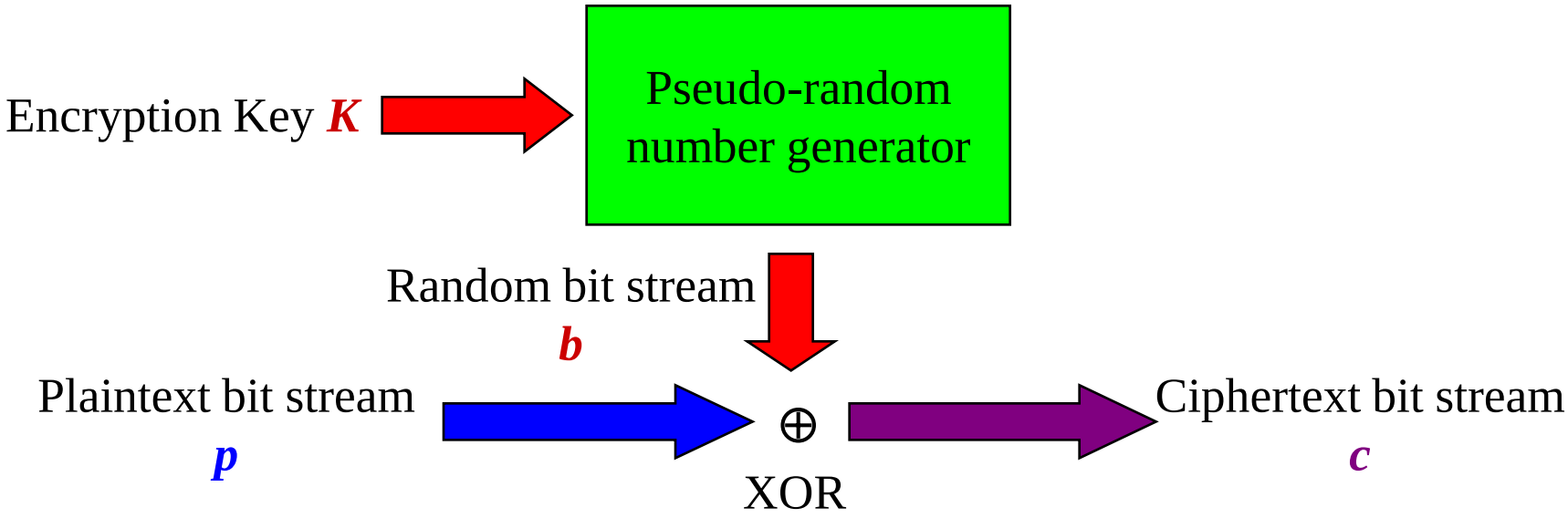
- MAC addresses are easily sniffed by an attacker since they must be sent unprotected.

- Most wireless LAN cards allow changing of their MAC addresses by software.

# Mechanism 3: WEP

- Wired Equivalent Privacy (WEP)
  - The objective is to provide confidentiality similar to wired LAN.
- WEP is used to provide two types of security:
  - Authentication (to prevent unauthorized access to the network)
  - Encryption (to prevent eavesdropping)
- WEP uses an encryption algorithm based on RC4.

# Basic Idea of RC4




Decryption works in the same way: $p = c \oplus b$

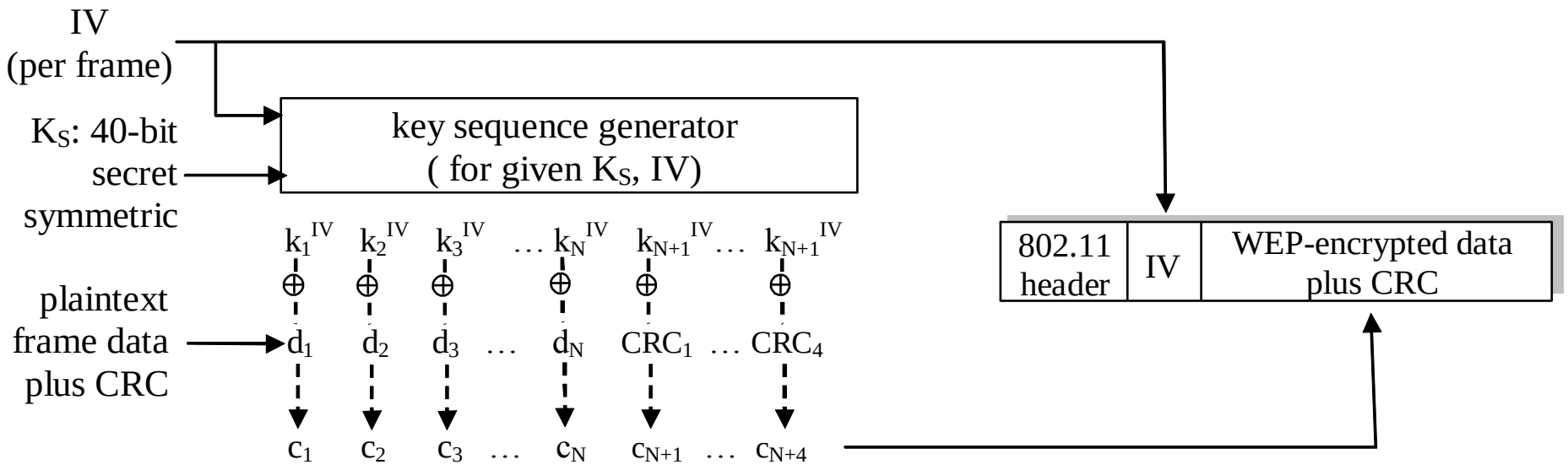
# How WEP uses RC4?

- Station and AP share a 40-bit secret key
  - **semi-permanent**
- Station appends a 24-bit initialization vector (IV) to create a 64-bit key
- The 64-bit key is used to generate a key sequence, $k_i^{\mathbf{IV}}$
  - $k_i^{\mathbf{IV}}$ is used to encrypt the $i$-th data bit, $d_i$:

$$c_i = d_i \text{ XOR } k_i^{\mathbf{IV}}$$

  - **IV and encrypted bits, $c_i$ are sent.**

# 802.11 WEP encryption




Sender-side WEP encryption

**Note** :

1. IV changes from frame to frame.
2. IV is sent unencrypted.

# Shared Key Authentication

- Shared key authentication is based on WEP.
- AP sends challenge text *d*.
- Station generates an IV and use the secret key K to generate a key stream, $k^{IV}$.
- Station then computes the ciphertext *c* using the key sequence
  - $c = d$ XOR $k^{IV}$
- Station sends IV and *c* to AP.

# Authentication without a Key

- A **hacker** can record one **challenge/response**.
  - The hacker now knows ***d***, ***c*** and IV.
- The **hacker** can compute the key sequence $k^{IV}$.
  - $k^{IV} = d$ XOR $c$
- The hacker can use IV and $k^{IV}$ to encrypt **any subsequent challenge.**
- The hacker can now authenticate to the target network
  - without knowing the shared secret key.

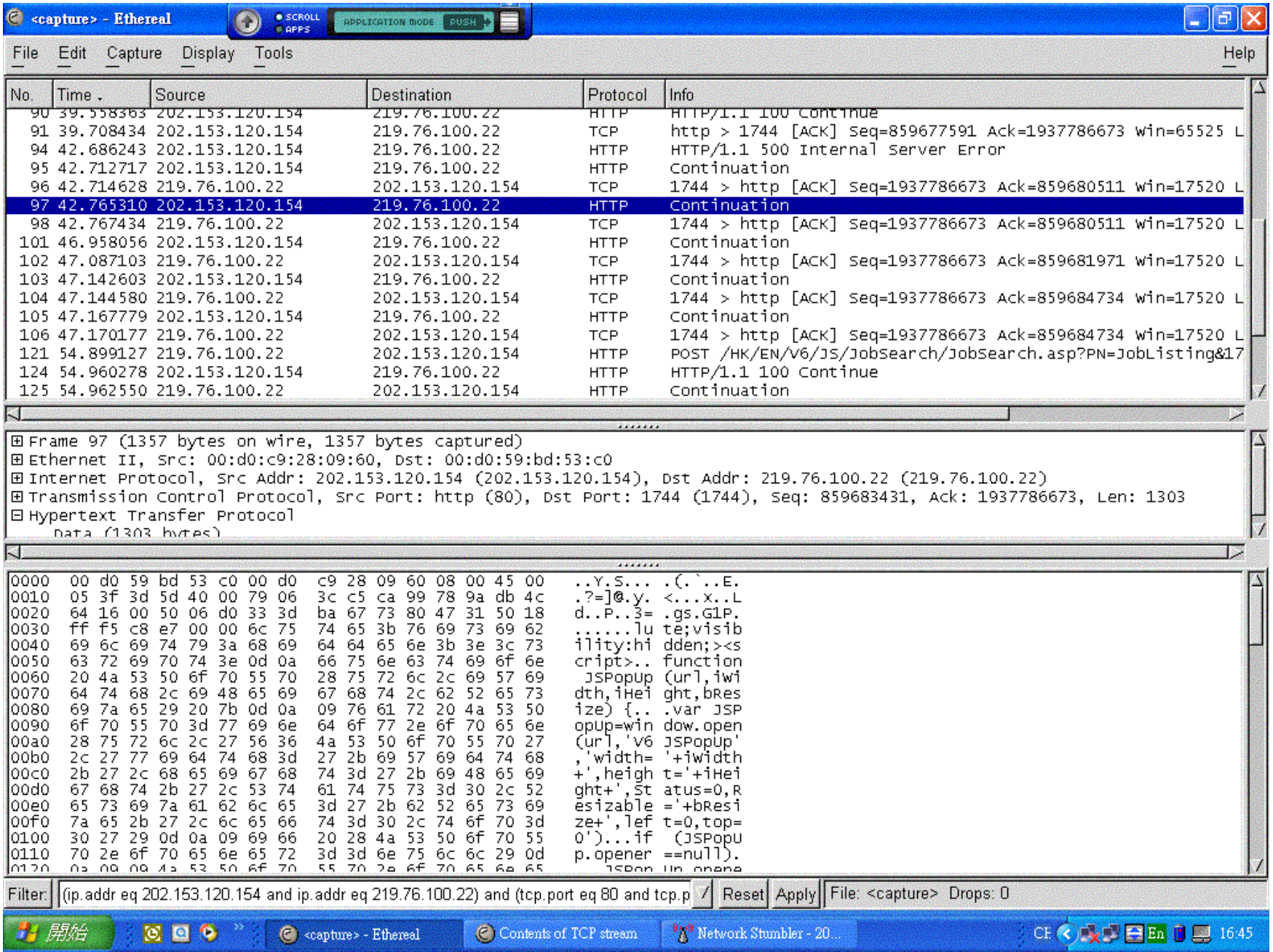
# WEP Encrypted Traffic

- Data encryption using WEP is NOT secure.
- Major reason:
  - IV has only 24 bits.
  - IV collisions (use of the same IV) occur frequently.
- Details omitted.

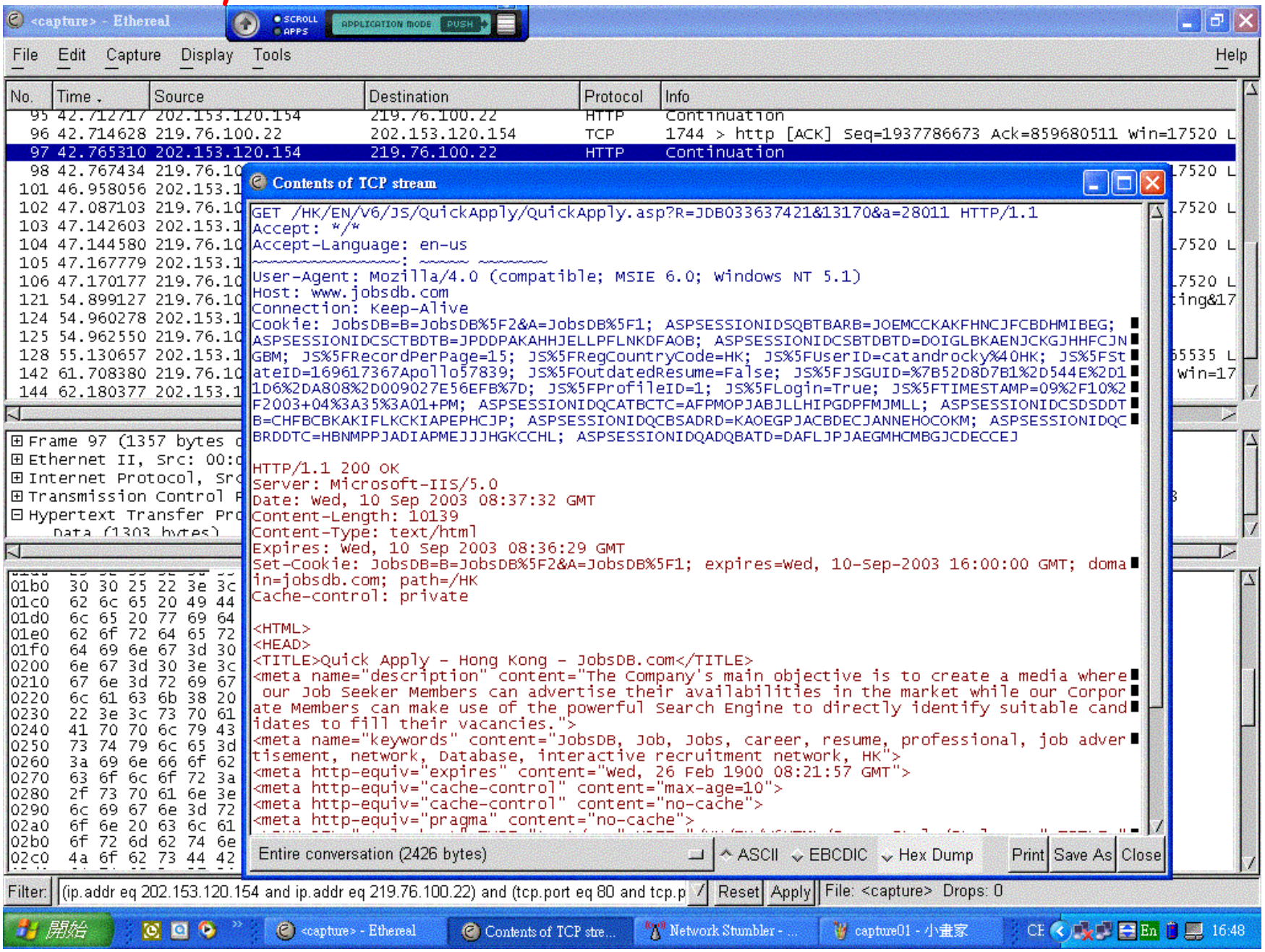
# Secure or Not?

- WEP has serious security flaw.
- In actual deployment, WEP is usually **disabled**.
- It is very easy to attack a wireless LAN.

# We may capture all the packets…



# We may even re-construct the TCP stream!



# Lessons learned…

- Encrypt your confidential data before ftp

- Use secure mode to check your email
  - https://webmail.cityu.edu.hk

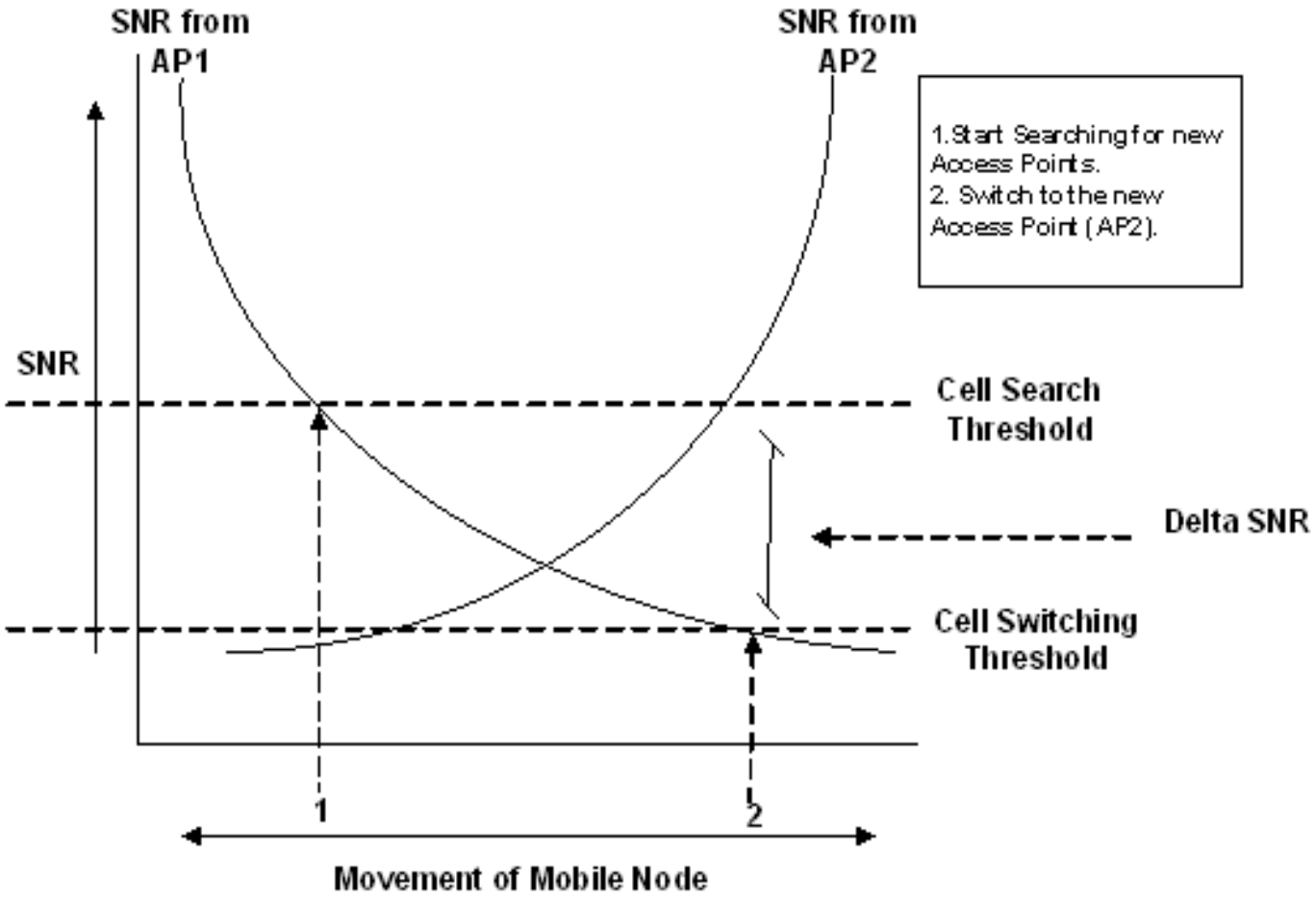
# Association and Roaming

- Performing a series of scans on different frequencies is called *sweeping*.
- There are two types of sweeps:
  - full sweeping, which goes through all the channel-list, and
  - short sweeping which skips the channels that do not have sufficient frequency distance from known active channels.

# Roaming

- When a mobile unit moves away from the AP, the SNR of the link drops, and will eventually drop below a threshold value (*cell search threshold)* which triggers the roaming algorithm.
- Mobile station initiates a sweeping to find a suitable access point to bind to.
- When the SNR drops below a second threshold ( *cell switching threshold)*, the roaming algorithm triggers a re-association by selecting another access point with a better SNR.

# Roaming


SNR from AP1
SNR from AP2
1.Start Searching for new Access Points.
2. Switch to the new Access Point (AP2).
SNR
Cell Search Threshold
Delta SNR
Cell Switching Threshold
1
2
Movement of Mobile Node

# References


- IEEE 802.11 Basics and MAC layer
  - J. Schiller, *Mobile communications*, Addison-Wesley, 2000.
- IEEE 802.11 Security
  - W. A. Arbaugh, N. Shankar, and Y. C. J. Wan, "Your 802.11 wireless network has no clothes," *http://www.cs.umd.edu/~waa/wireless.pdf*
  - J. Williams, "The IEEE 802.11b security problem, Part 1," pp. 90-95, *IEEE IT Professional*, Nov/Dec 2001.