Lecture 2

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 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

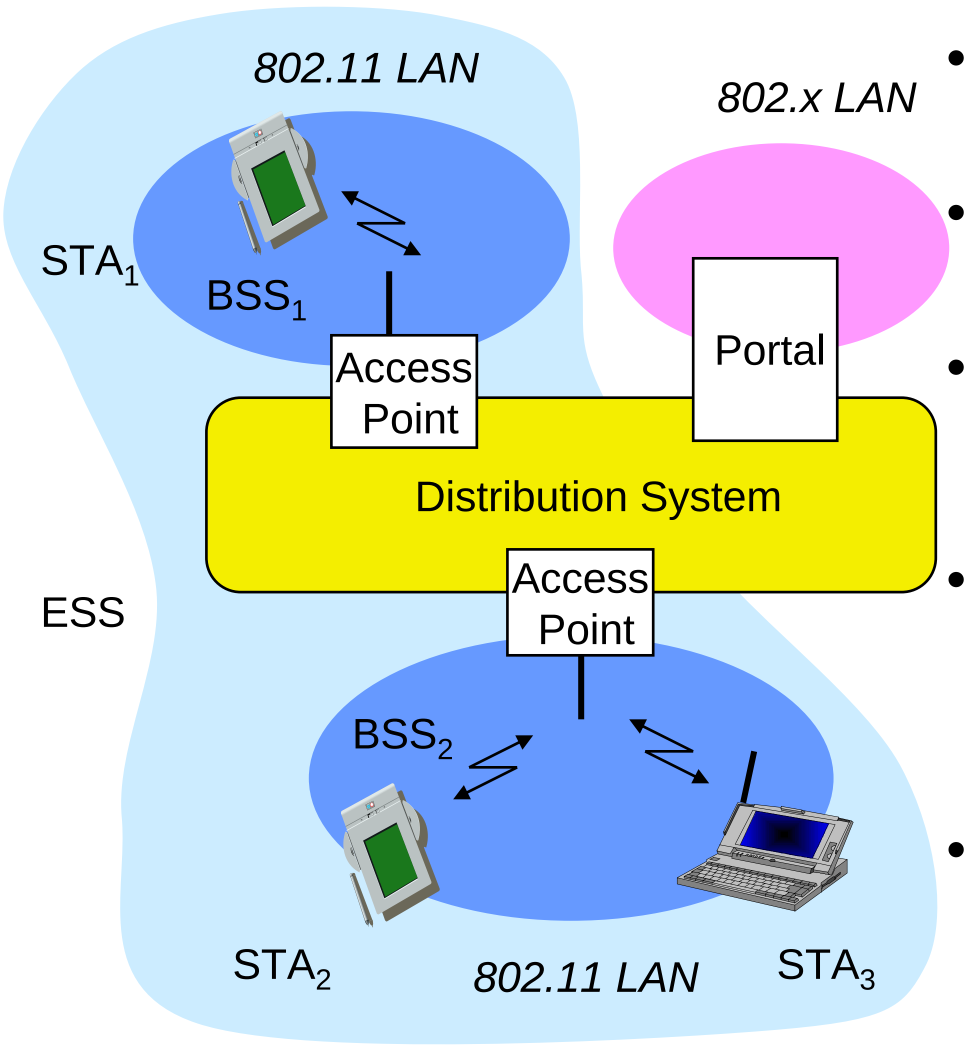
- HIPERLAN
  - High Performance Radio LAN
  - European standard
- IEEE 802.11
  - US standard
  - today, it holds the entire market
  - Only this standard will be discussed in our course

Two Modes of IEEE 802.11

- Infrastructure Mode
  - Terminals communicate to an access point.

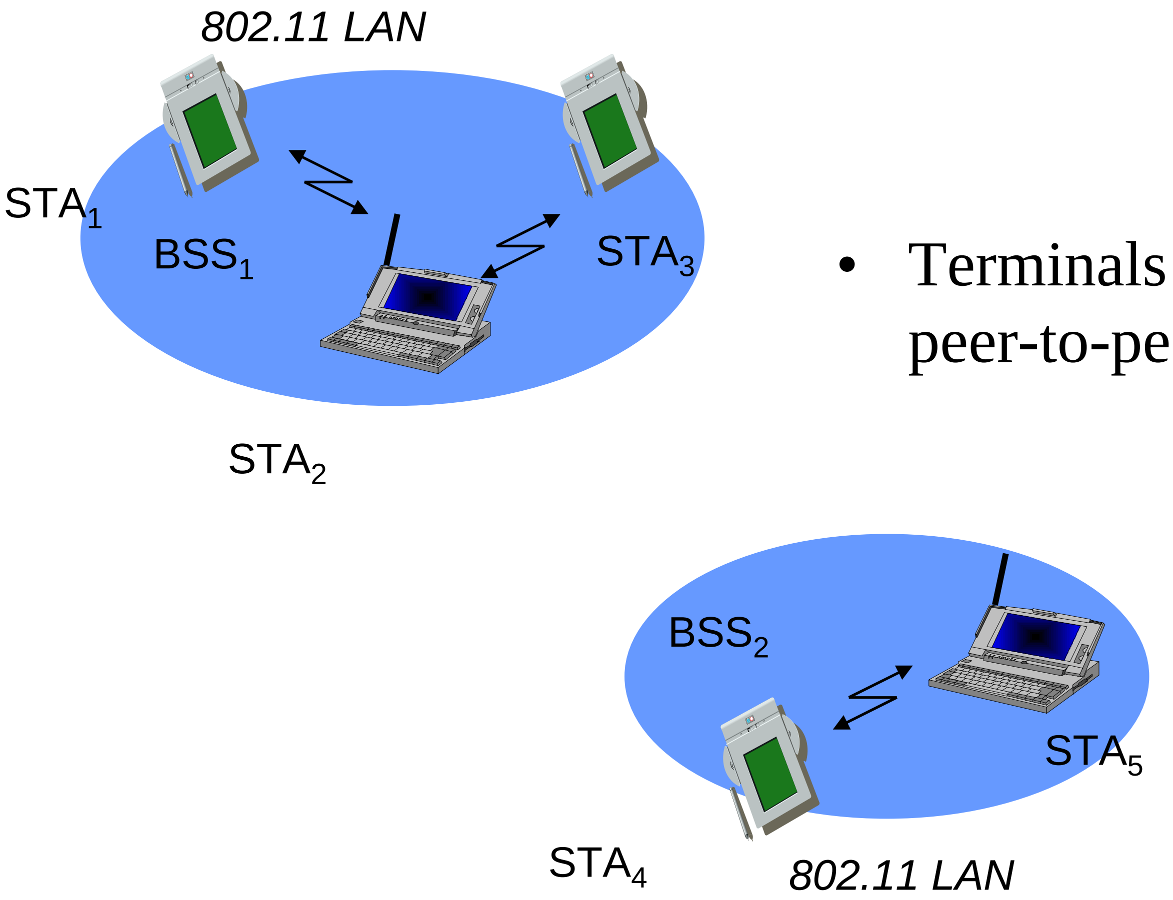
- Ad Hoc Mode
  - Terminals communicate in a peer-to-peer basis without any access point.

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.

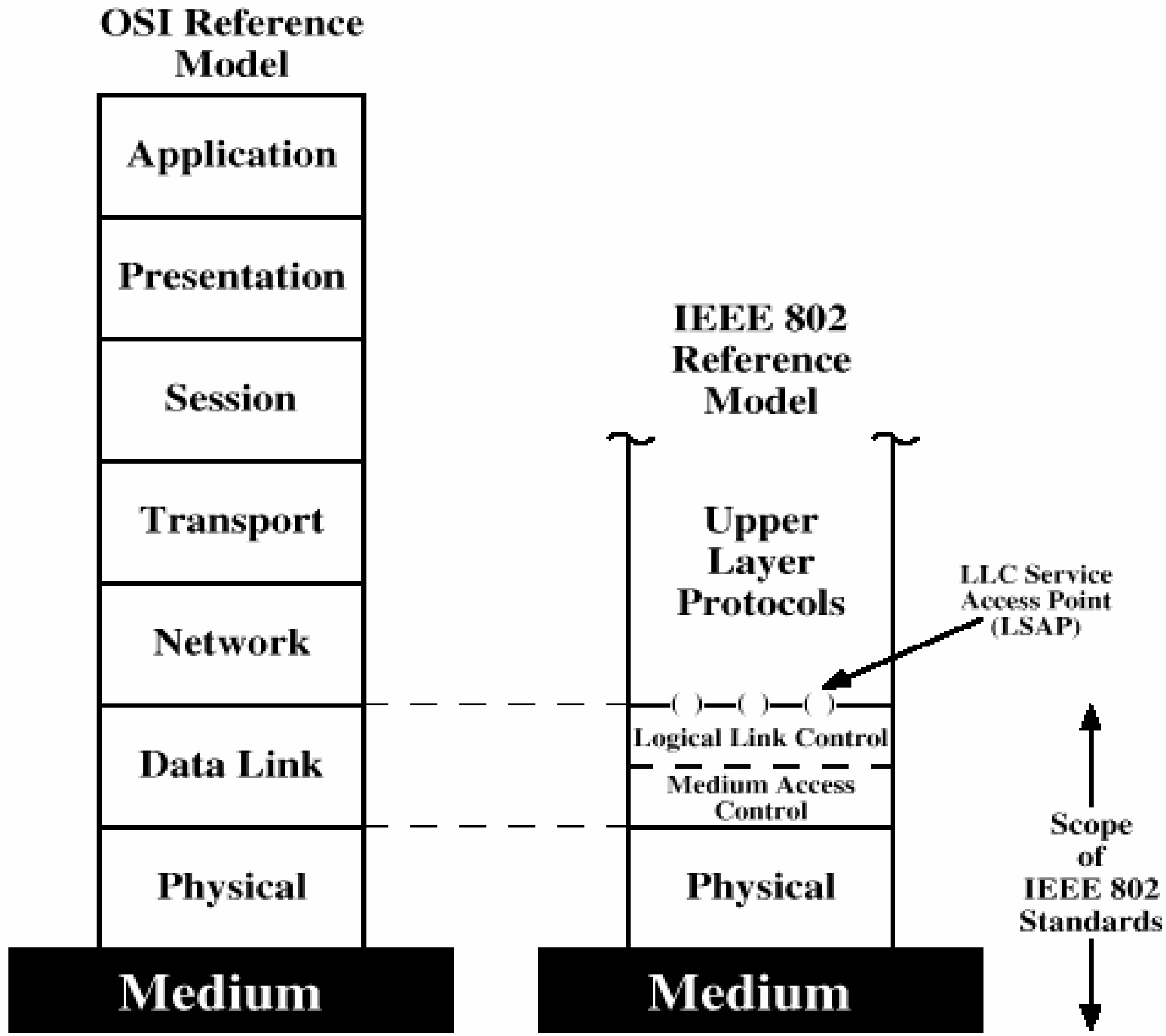
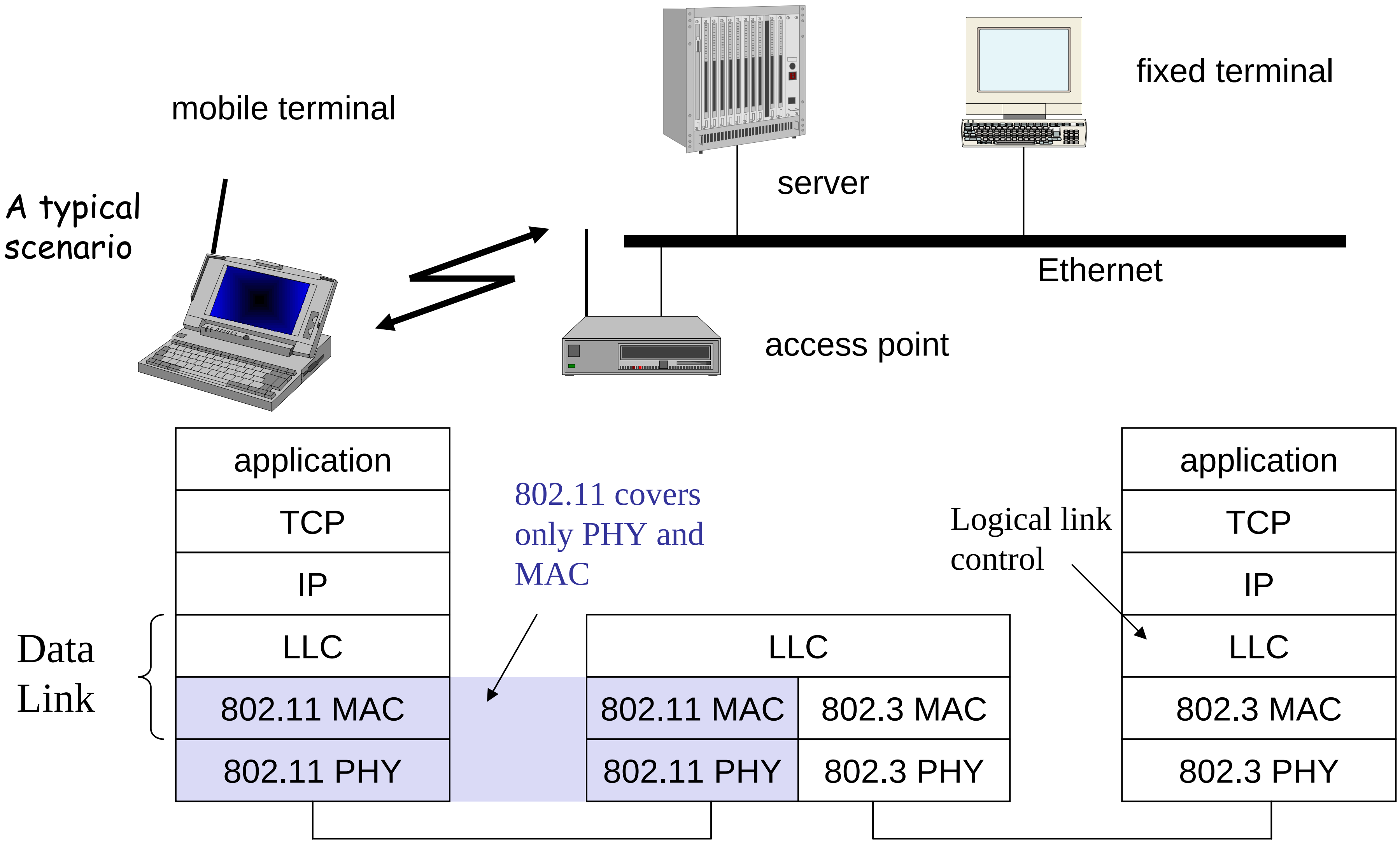


Figure 14.1 IEEE 802 Protocol Layers Compared to OSI Model

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
- Radio (2 types)
  - Frequency Hopping Spread Spectrum
  - Direct Sequence Spread Spectrum
  - can cover a larger area (e.g. penetrate walls)

IEEE 802.11 Standards

Standard	Spectrum	Bit Rate	Transmission	Compatibility
802.11	wavelength between 850 and 950 nm; 2.4 GHz	2 Mbps	Infrared / FHSS / DSSS	N/A
802.11a	5.0 GHz	54 Mbps	OFDM	None
802.11b (Wi-Fi)	2.4 GHz	11 Mbps	DSSS	802.11
802.11g	2.4 GHz	54 Mbps	OFDM	802.11 / 802.11b

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 (aka (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.

2. Choosing a Network

- The user selects from available networks
- Common criteria:
  - User choice
  - Strongest signal
  - Most recently used

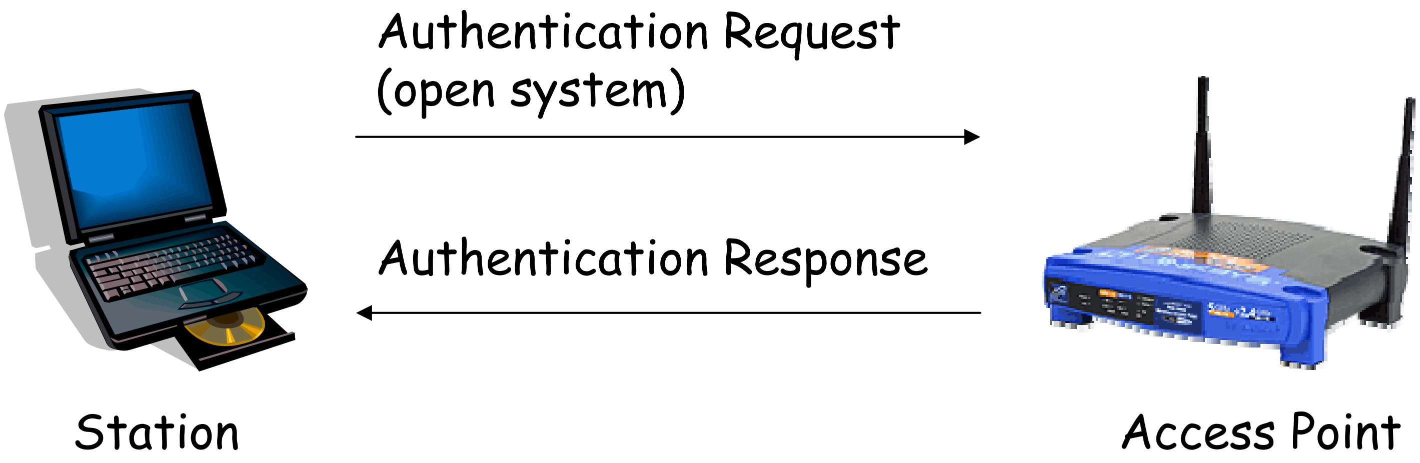
3. Authentication

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

- Two Mechanisms
  - Open System Authentication
  - Shared Key Authentication

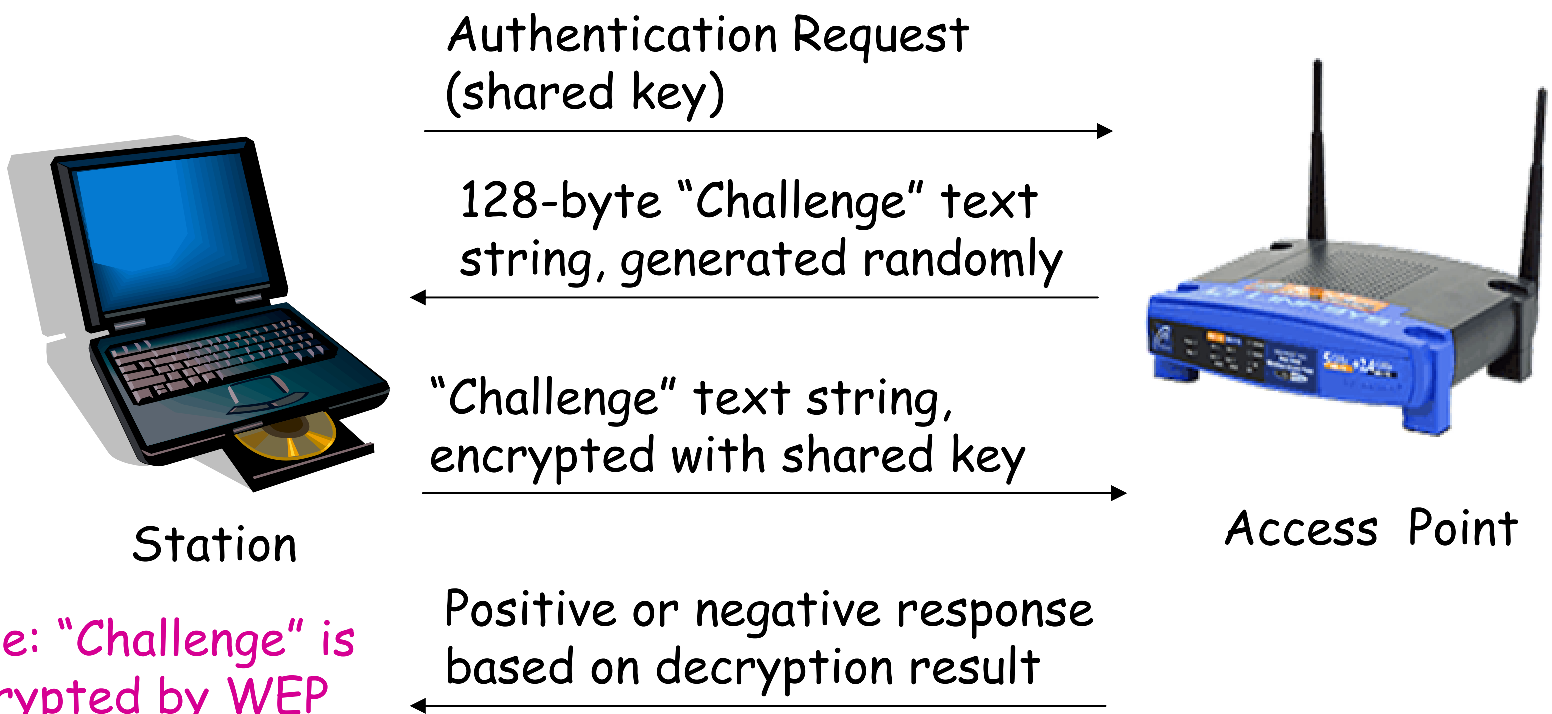
Open System Authentication

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



Shared Key Authentication

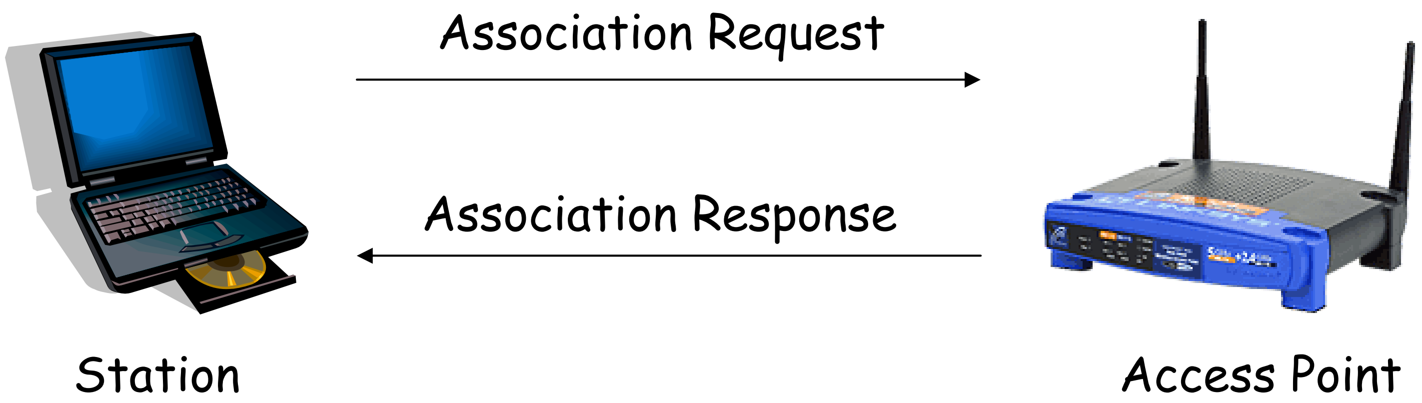
It is assumed that the station and the AP somehow agrees on a shared secret key via a channel independent of IEEE 802.11.



Note: "Challenge" is encrypted by WEP algorithm.

4. Association

The station needs to register to the AP.

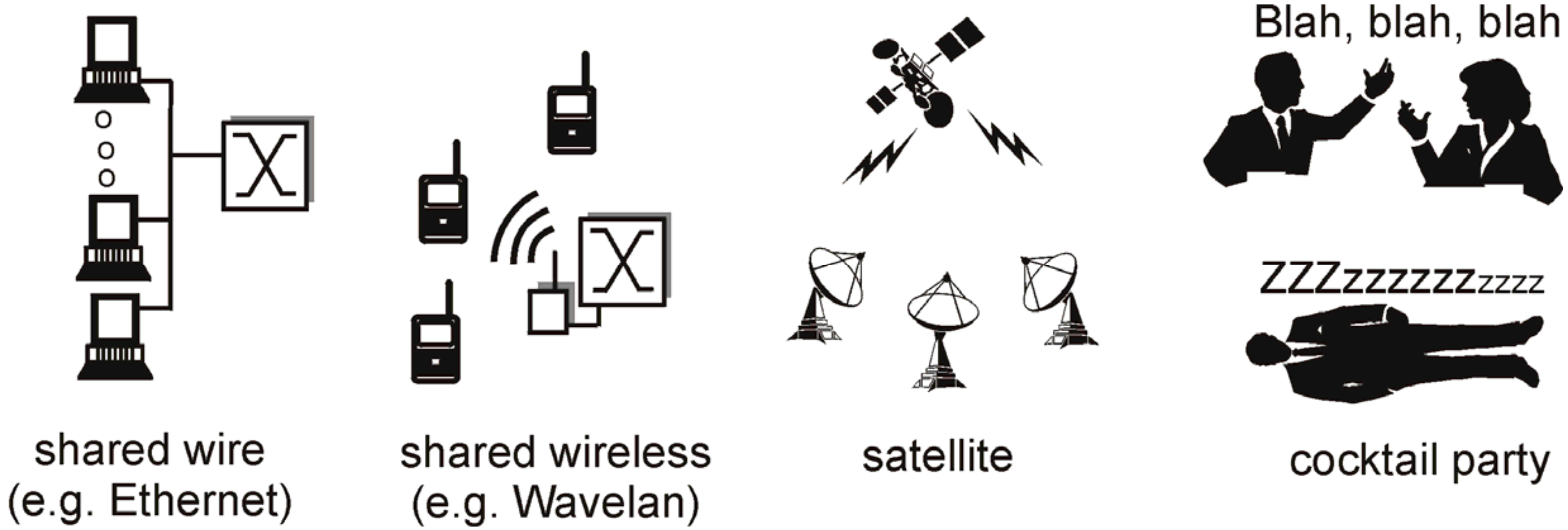


How to transmit?

The MAC layer

Media Access Control

- How to share a common medium among the users?



Motivation

- Can we apply media access methods from fixed networks?

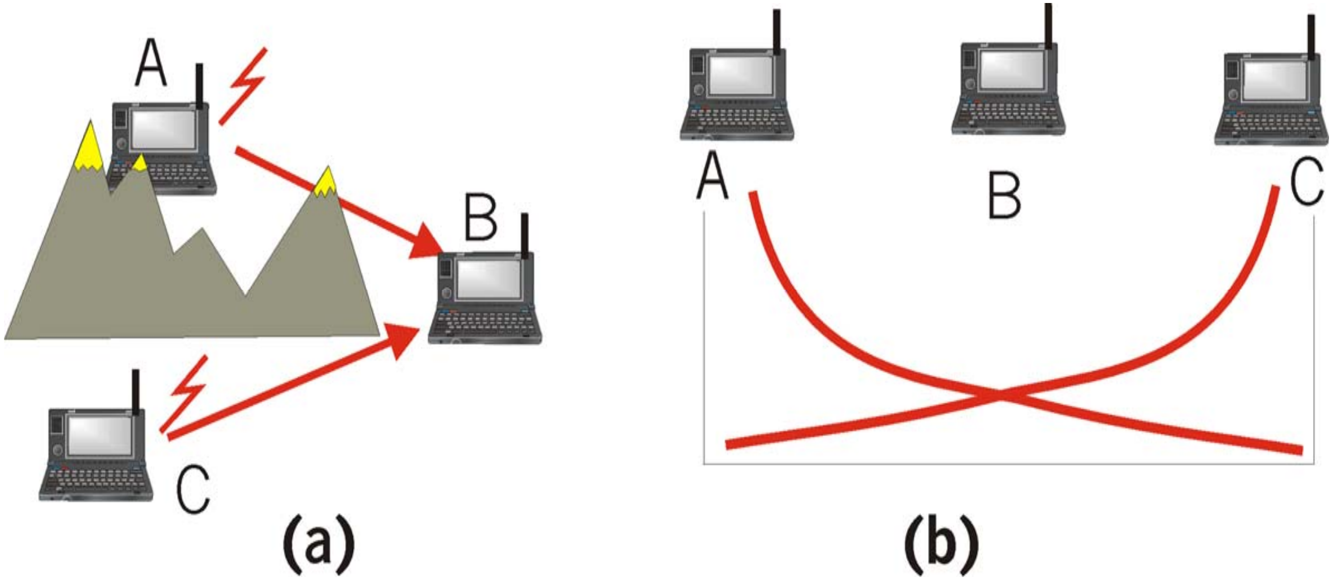
- Example: CSMA/CD
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - Method used in IEEE 802.3 Ethernet

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

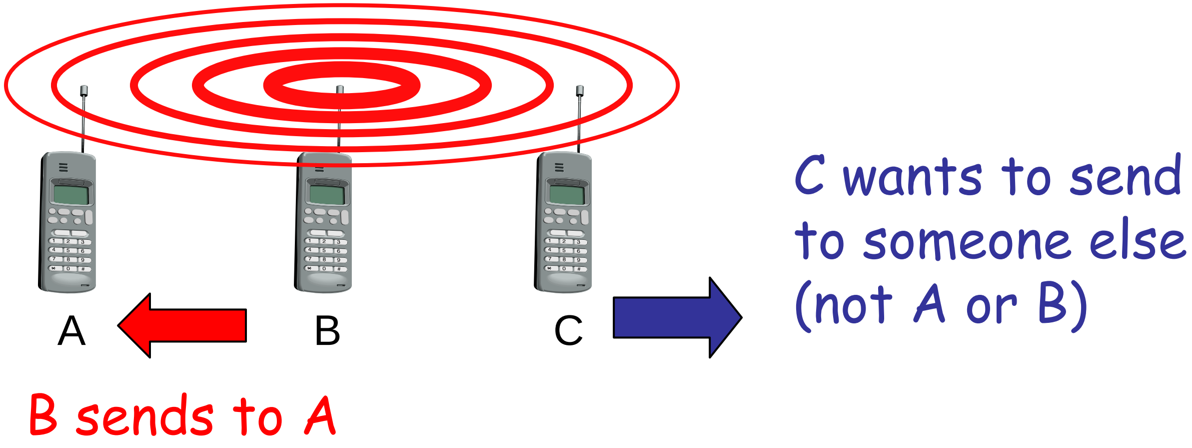
- *A*, *C* cannot hear each other (CS fails)
- Collisions at *B*, undetected (CD also fails)



Obstacles

Signal Attenuation

Exposed Terminal Problem

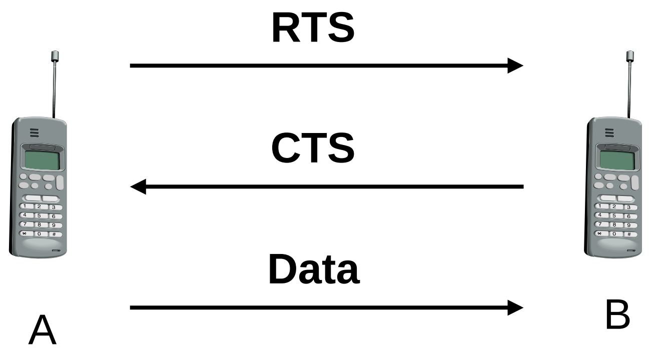


- *C* has to wait, since CS signals a medium in use
- But A is outside the radio range of *C*; therefore waiting is not necessary
- *C* is "exposed" to *B*

(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)
    - a sender request the right to send
  - CTS (clear to send)
    - the receiver grants the right to send
- The sender then sends the data.

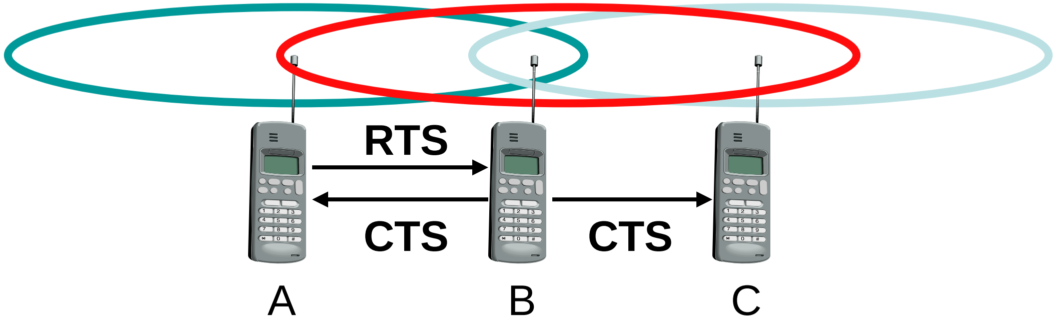
An Illustration: 3-way handshake



Can it solve the hidden terminal problem?

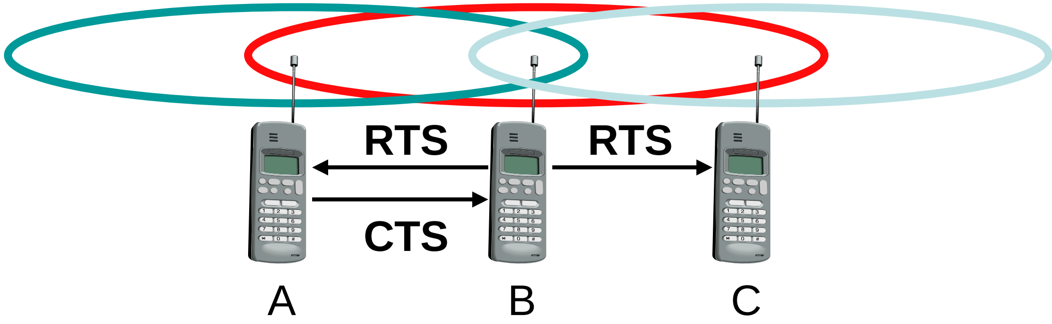
Can it solve the exposed terminal problem?

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

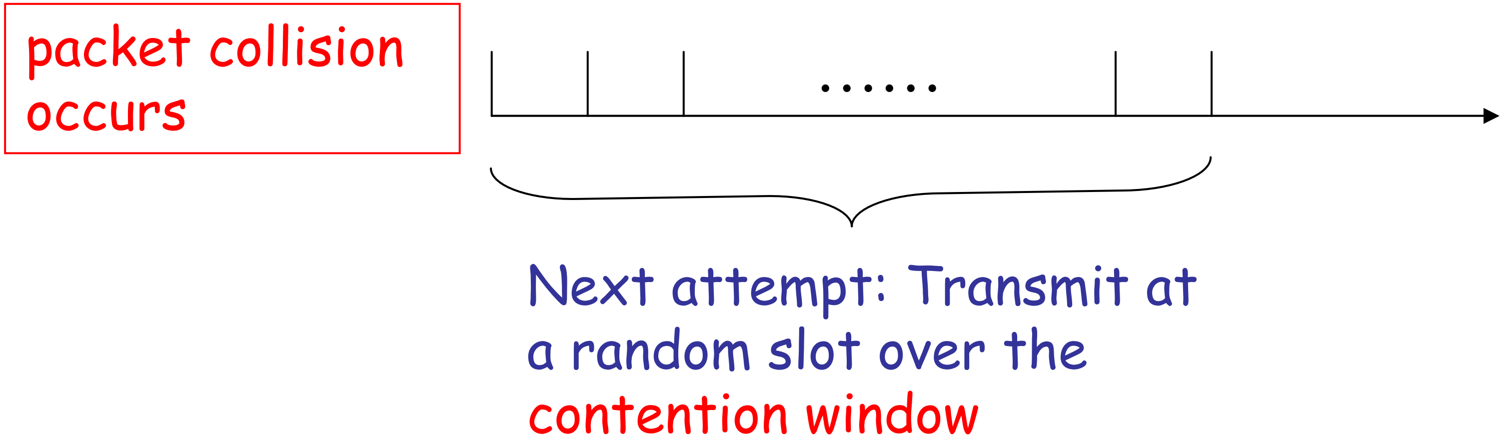
A Solution: Exposed Terminal



- 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.



How large is the contention window?

Binary Exponential Backoff

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

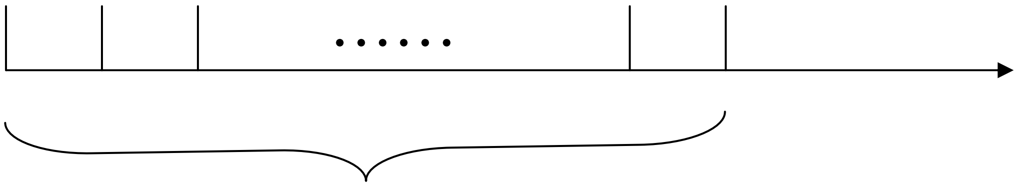
- When a terminal fails to receive CTS in response to its RTS, it increases the contention window
  - *cw* is doubled (up to an upper bound, CW_{max})

- 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



$2^i\ CW_{min}$ slots

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

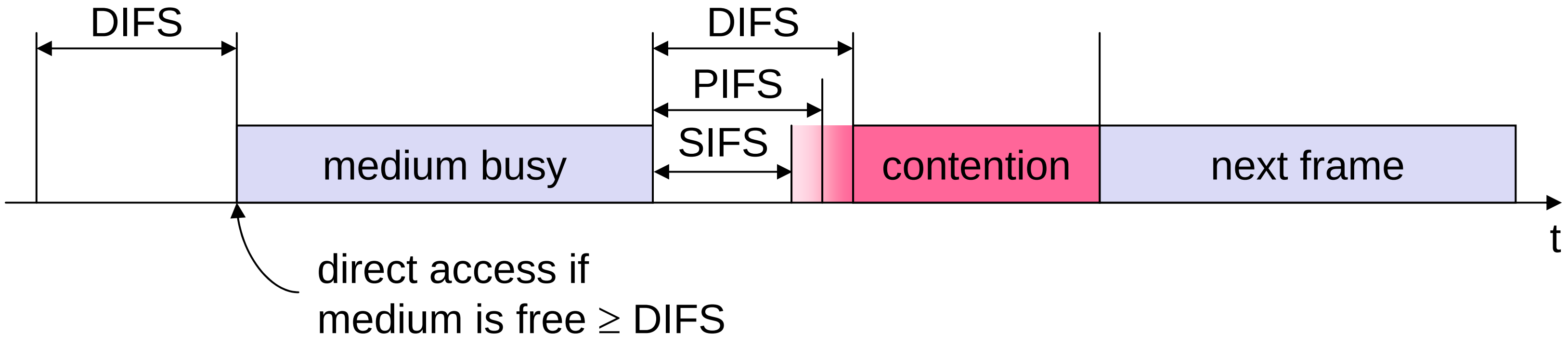
Two Classes of Access Mechanisms

- Distributed Coordination Function (DCF)
  - Support asynchronous data services
  - CSMA/CA
  - CSMA/CA with RTS/CTS exchange (optional)

- Point Coordination Function (PCF) (optional)
  - Support time-bounded services
  - Polling from AP

Inter-Frame Spacings

- 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



Method 1a: CSMA/CA

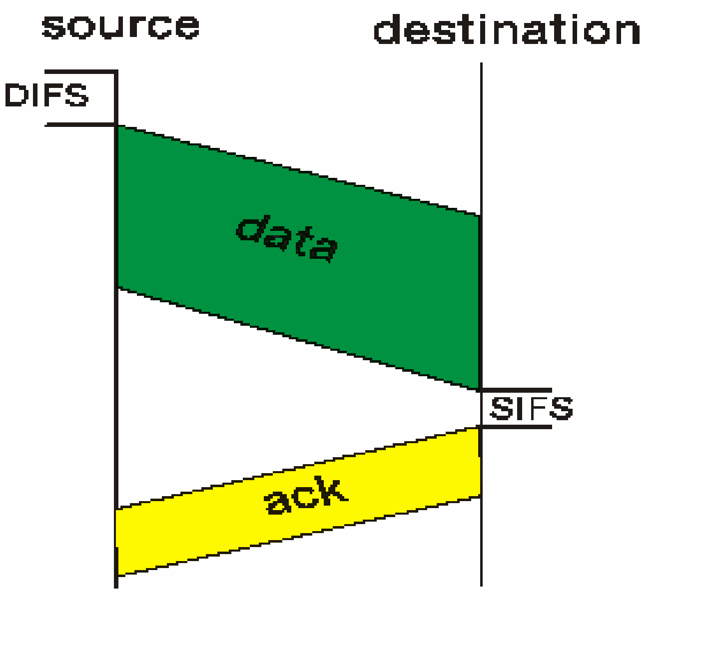
802.11 CSMA/CA: sender

- if sense channel idle for **DIFS** sec.
  then transmit entire frame (no collision detection)

-if sense channel busy
  then wait a random time

802.11 CSMA/CA: receiver

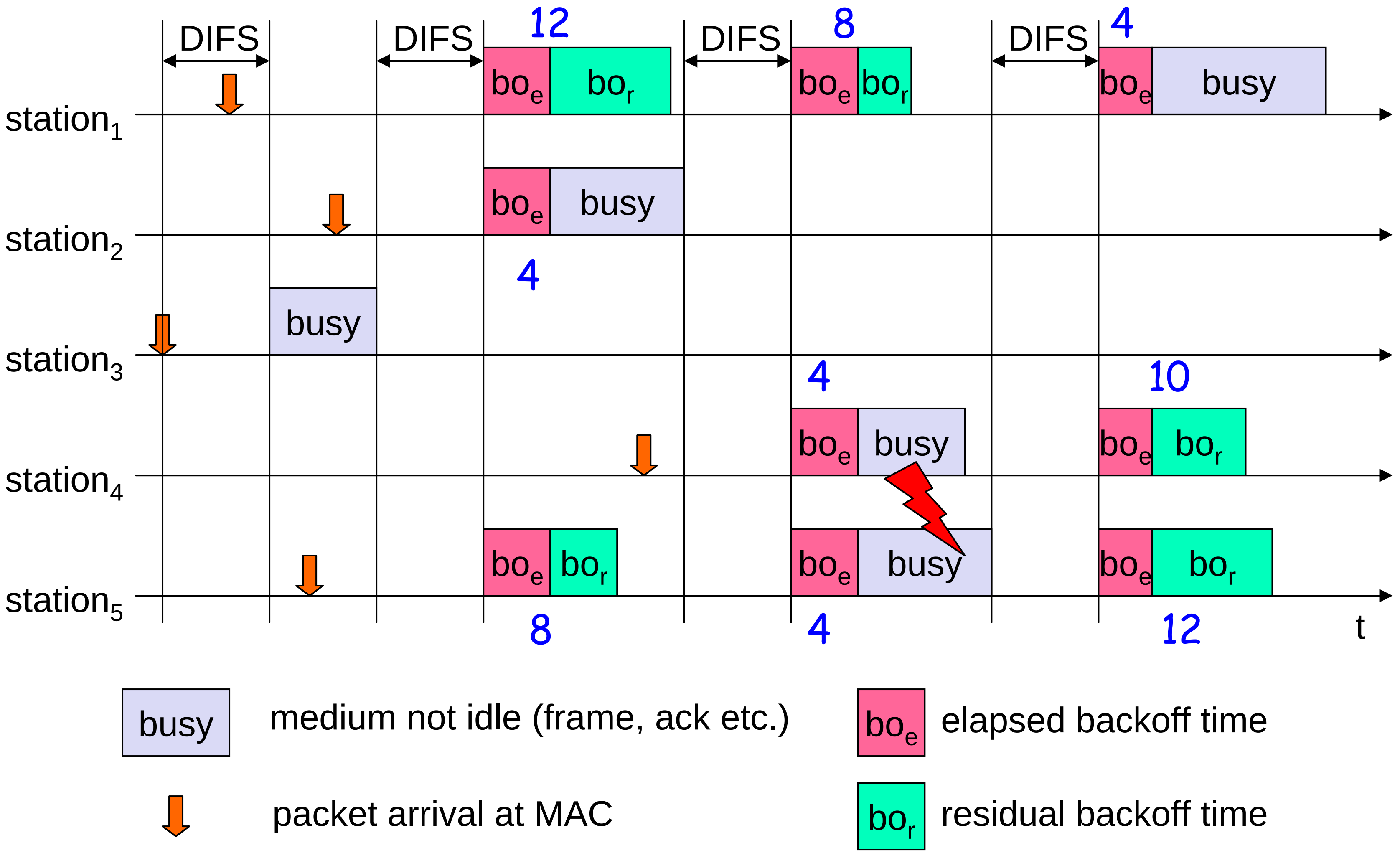
if received OK
  return ACK (16 bytes) after **SIFS**



DIFS: Distributed Inter Frame Spacing

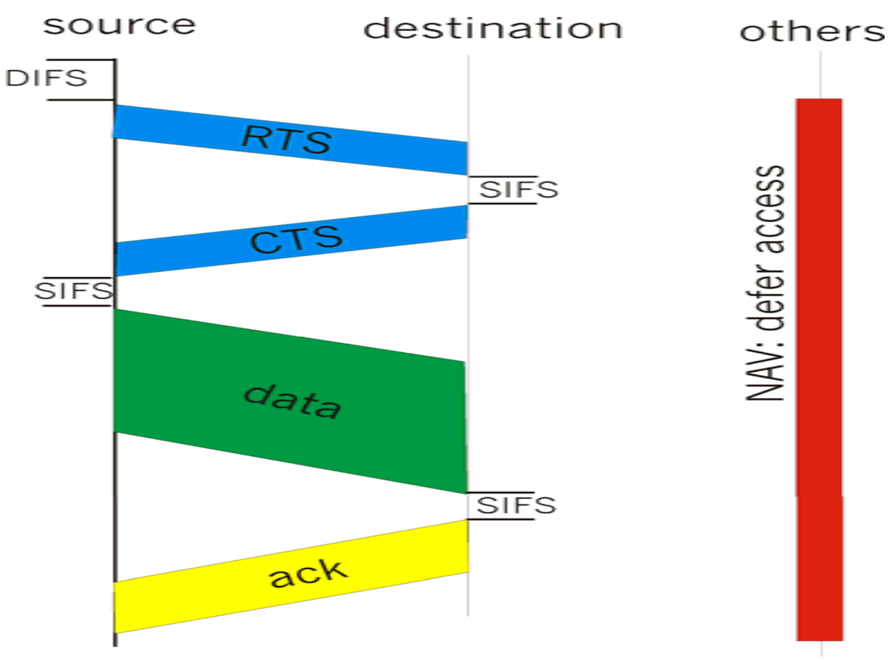
SIFS: Short Inter Frame Spacing

Example


DIFS
DIFS
DIFS
DIFS
12
8
4
station1
station2
station3
station4
station5
boe
bor
busy
4
4
10
8
4
12
t
busy
medium not idle (frame, ack etc.)
boe
elapsed backoff time
packet arrival at MAC
bor
residual backoff time

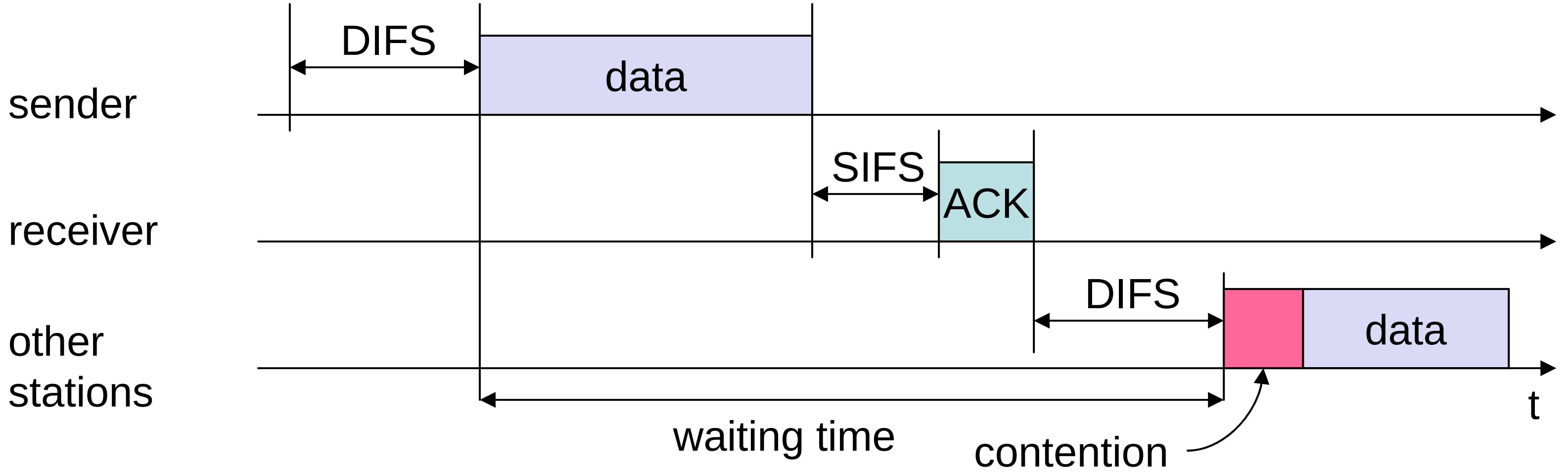
Method 1b: CSMA/CA with RTS-CTS

- 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



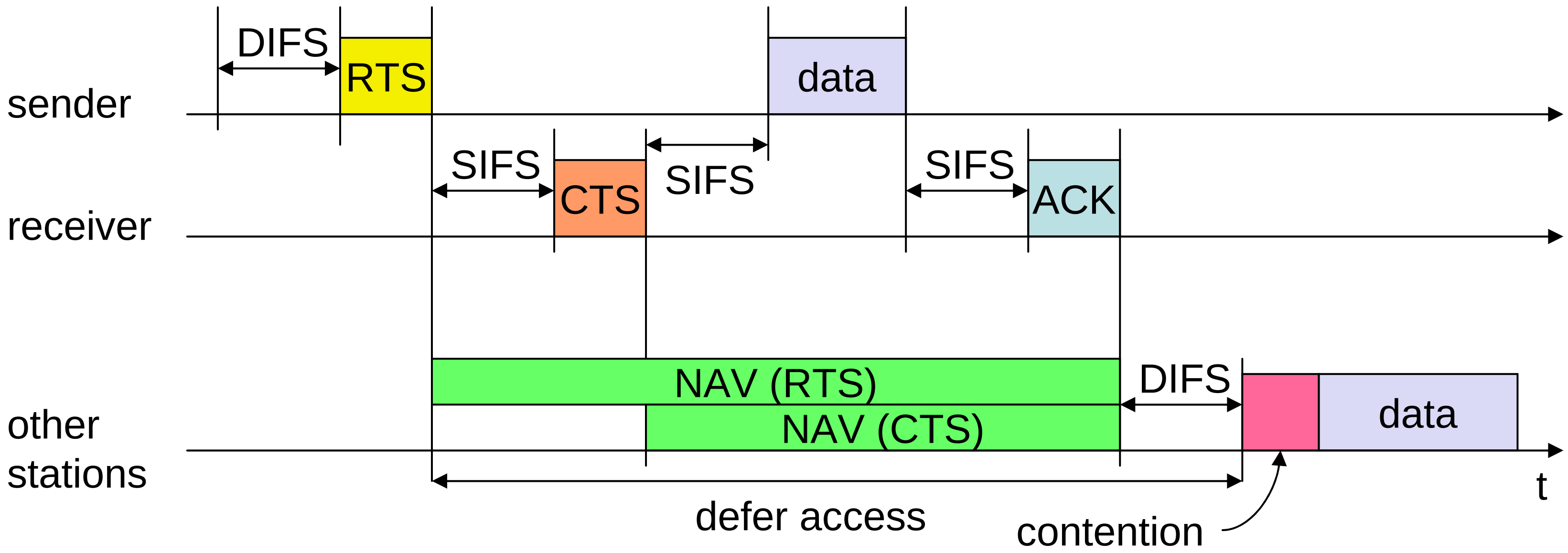
4-way handshake

No Collision during Data Transmission



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

Net Allocation Vector



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.

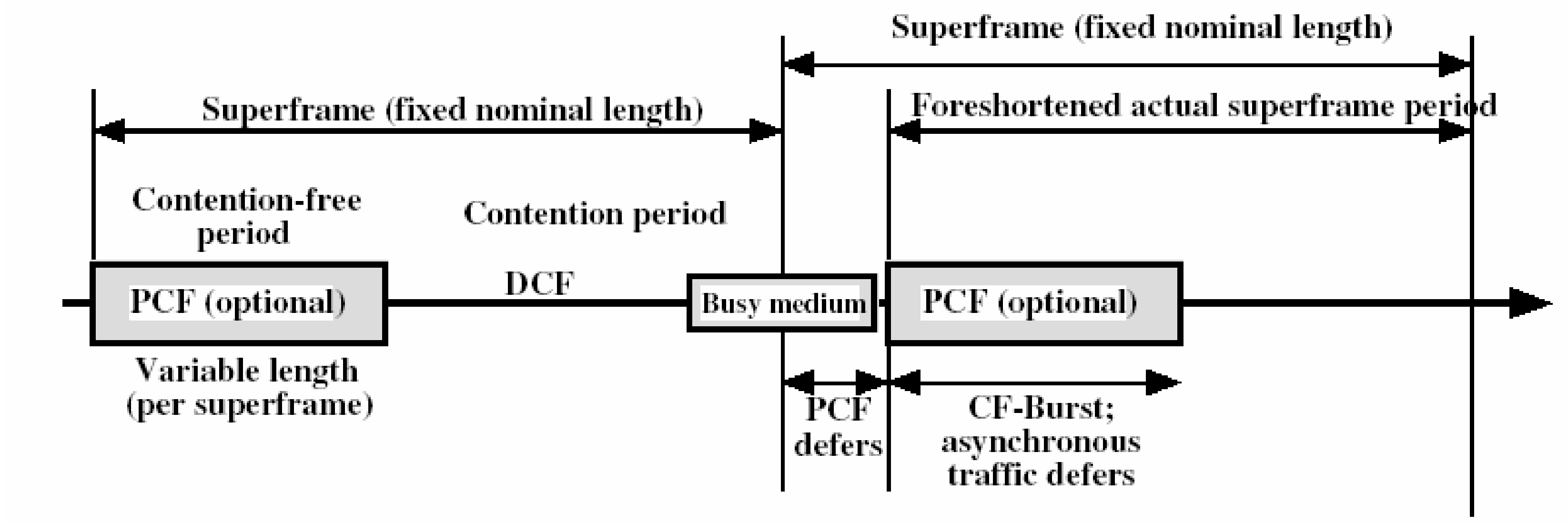
The CTS packet also has the duration field.

Other stations hear the CTS packet set their NAV accordingly.

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.

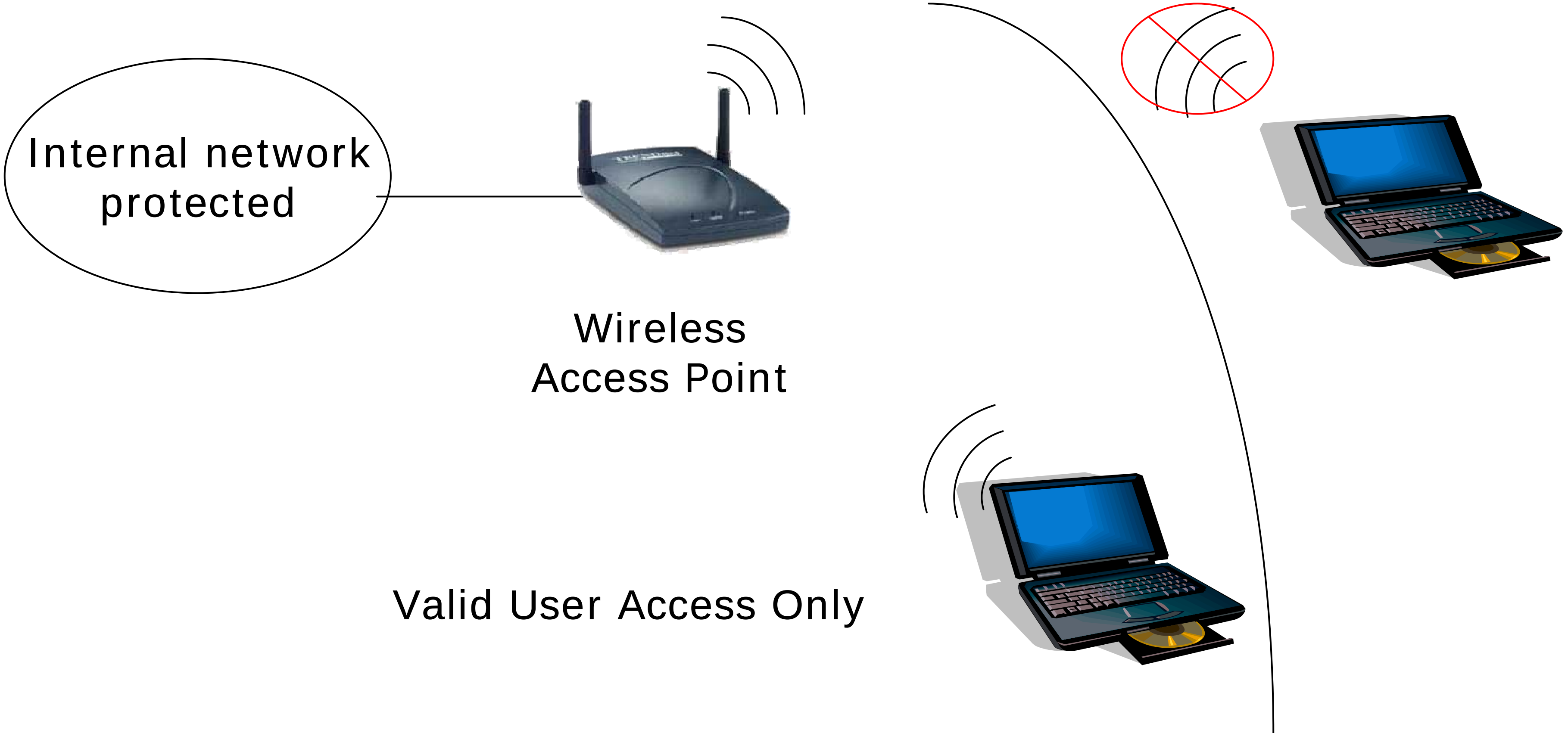
Is it Secure?

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

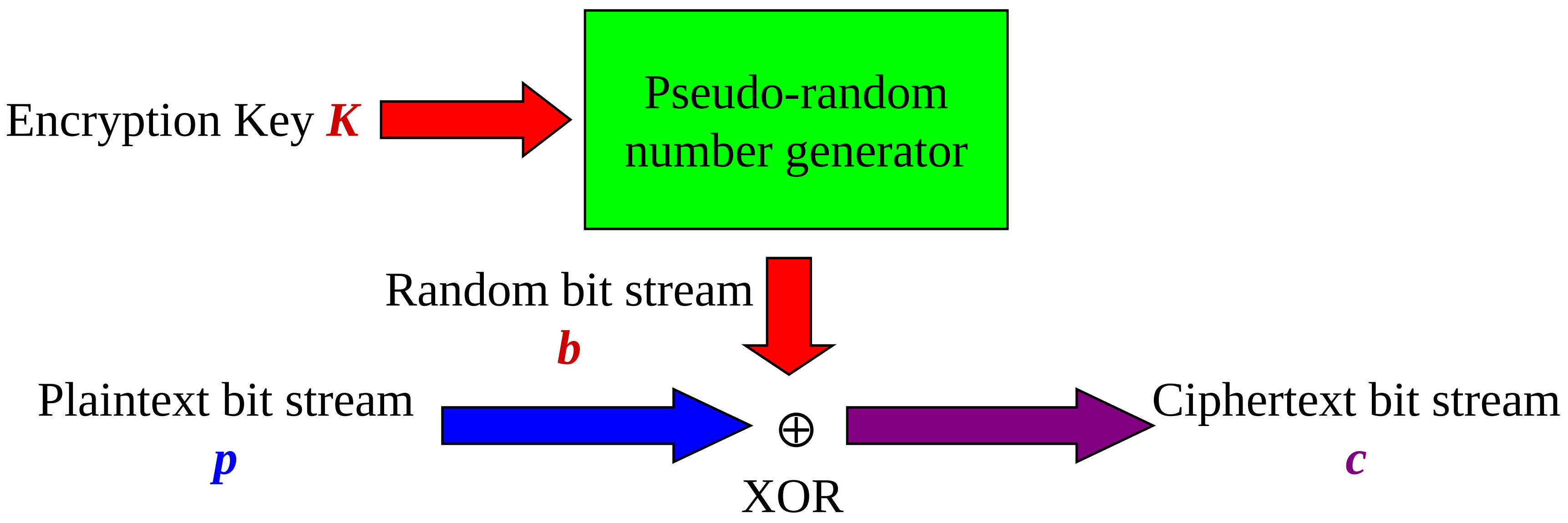
- MAC addresses are easily sniffed by an attacker since they must be sent unprotected.

- 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: $p = c \oplus b$

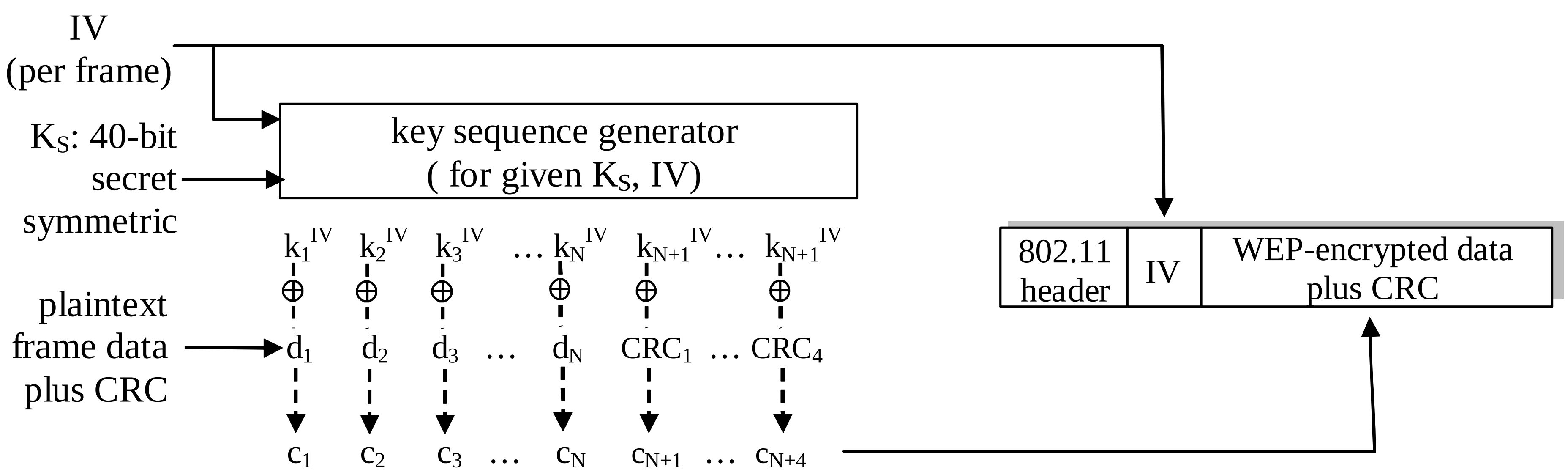
How WEP uses RC4?

- 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 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}.
  - $k^{IV} = d \text{ XOR } c$
- 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.

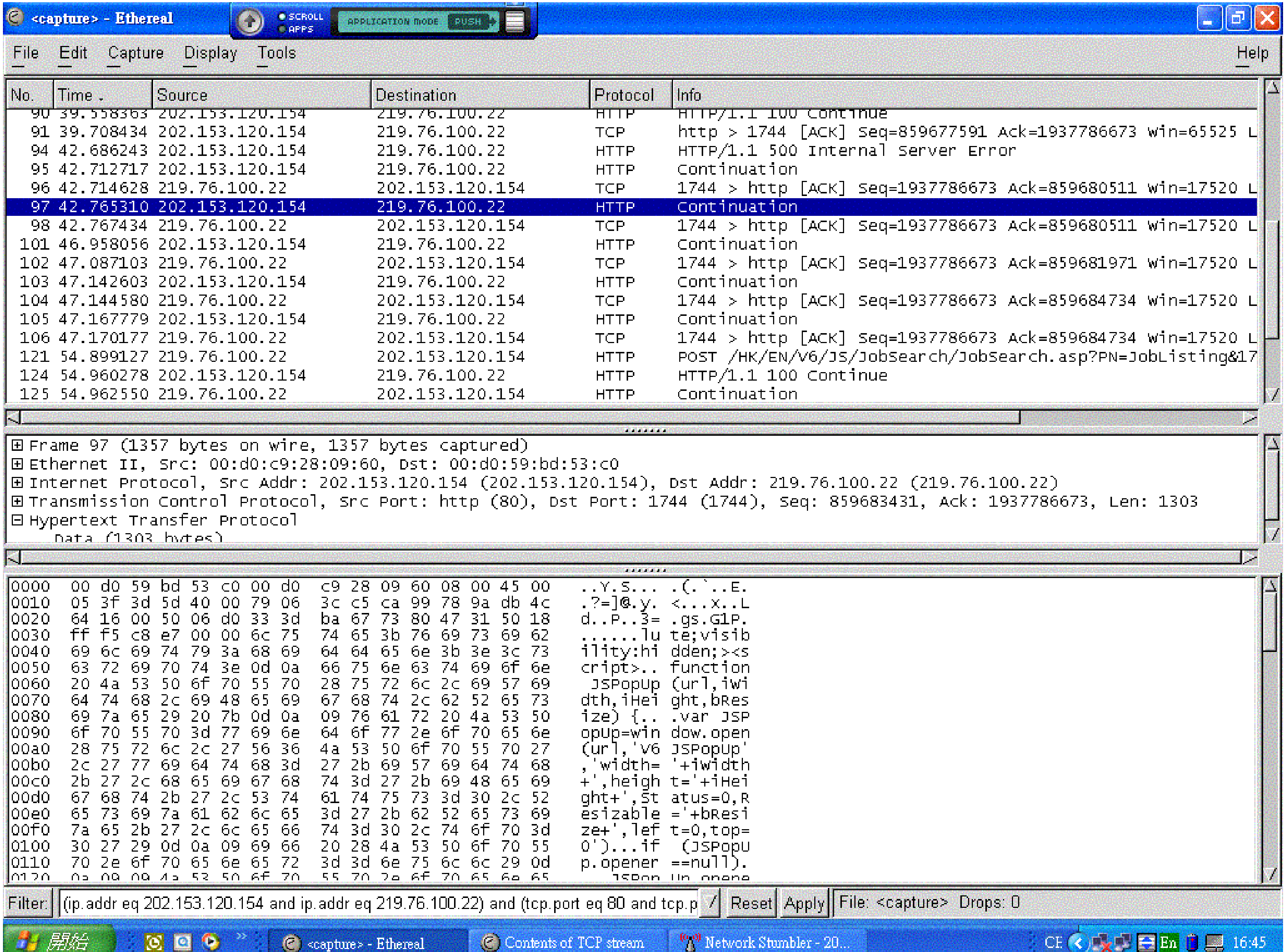
WEP Encrypted Traffic

- 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.

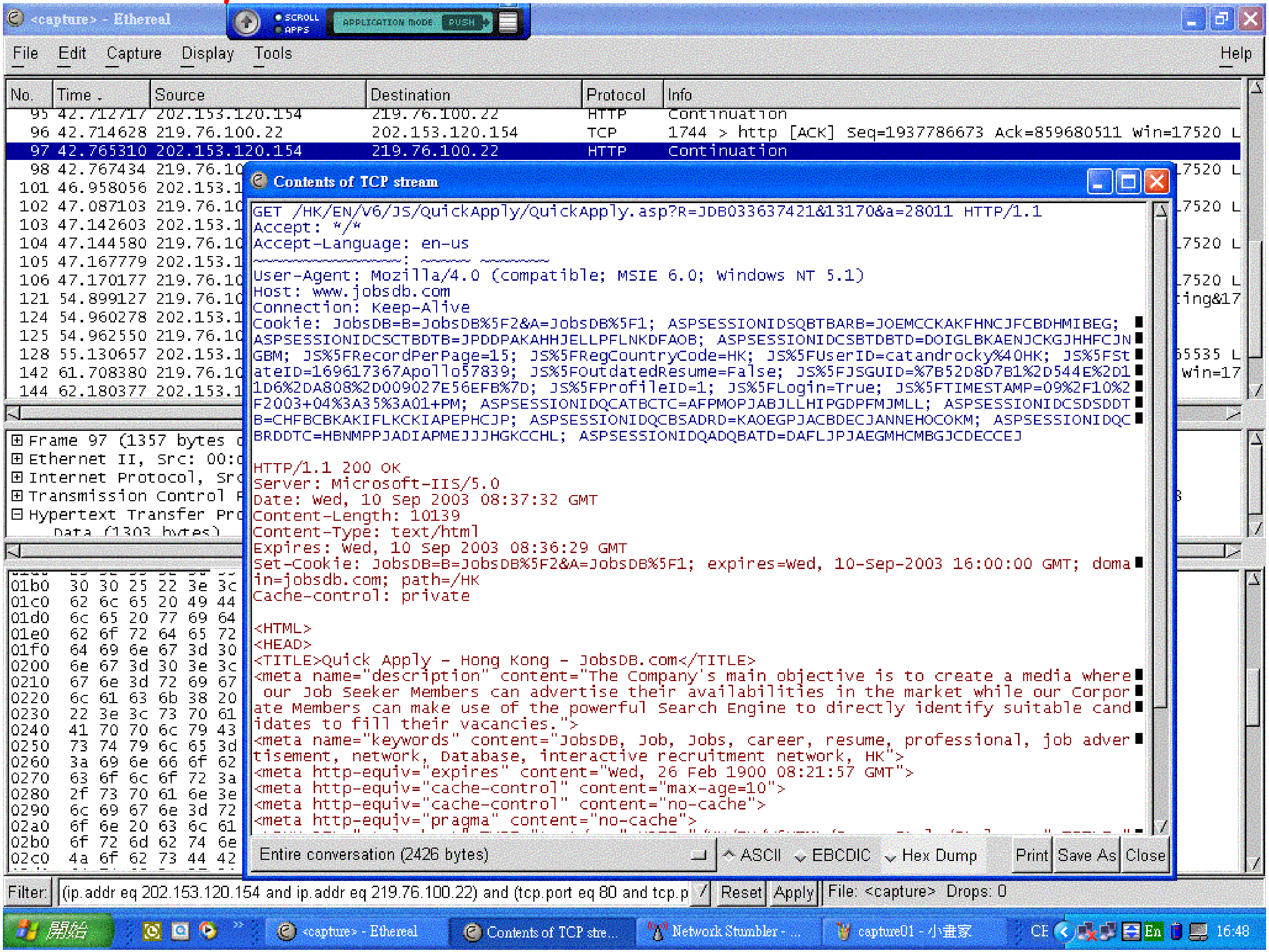
Secure or Not?

- 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

References

- IEEE 802.11 Basics and MAC layer
  - You can easily find relevant books in the library.
  - 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.