Objectives:

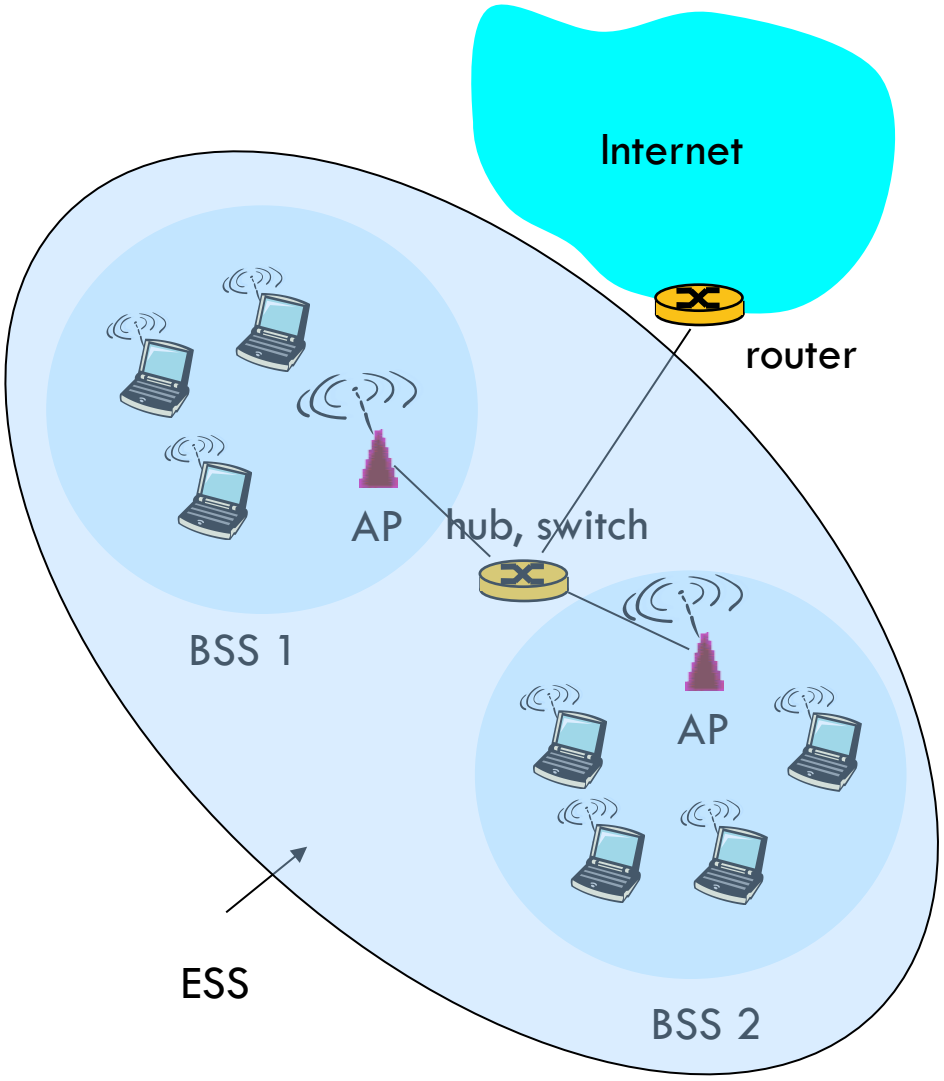
1) Understanding the basic operations of WLANs
2) WLAN security
3) Wireless body area networks (IEEE 802.15.6)

Readings:

1. Kurose & Ross, Computer Networking: A Top-Down Approach (6th Edition), Chapt 6.3

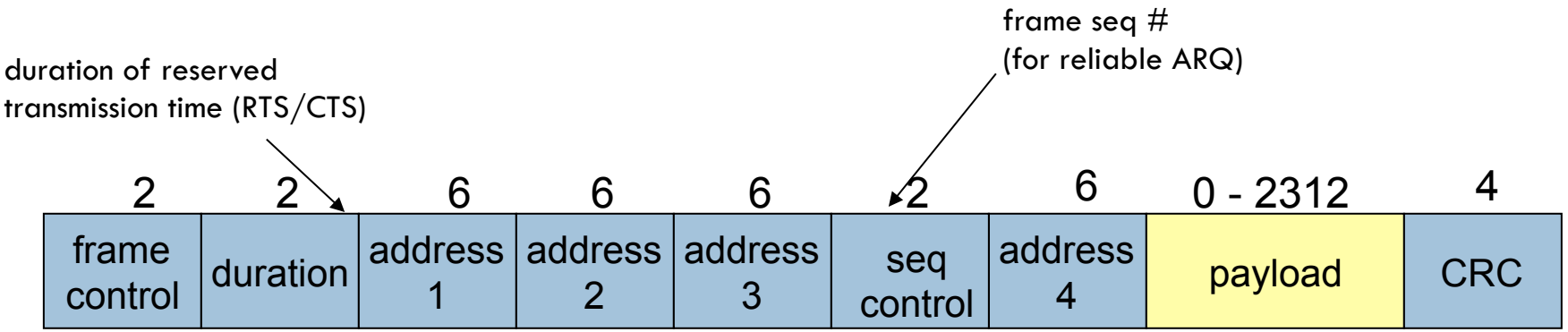
WIRELESS LAN/PAN/BAN

802.11 LAN architecture



- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell")
  - in infrastructure mode contains wireless hosts and access point (AP): base station
  - ad hoc mode: hosts only (IBSS)
- Distribution system (DS)
- Extended service set (ESS)
  - Two or more basic service sets interconnected by DS

802.11 frame: addressing



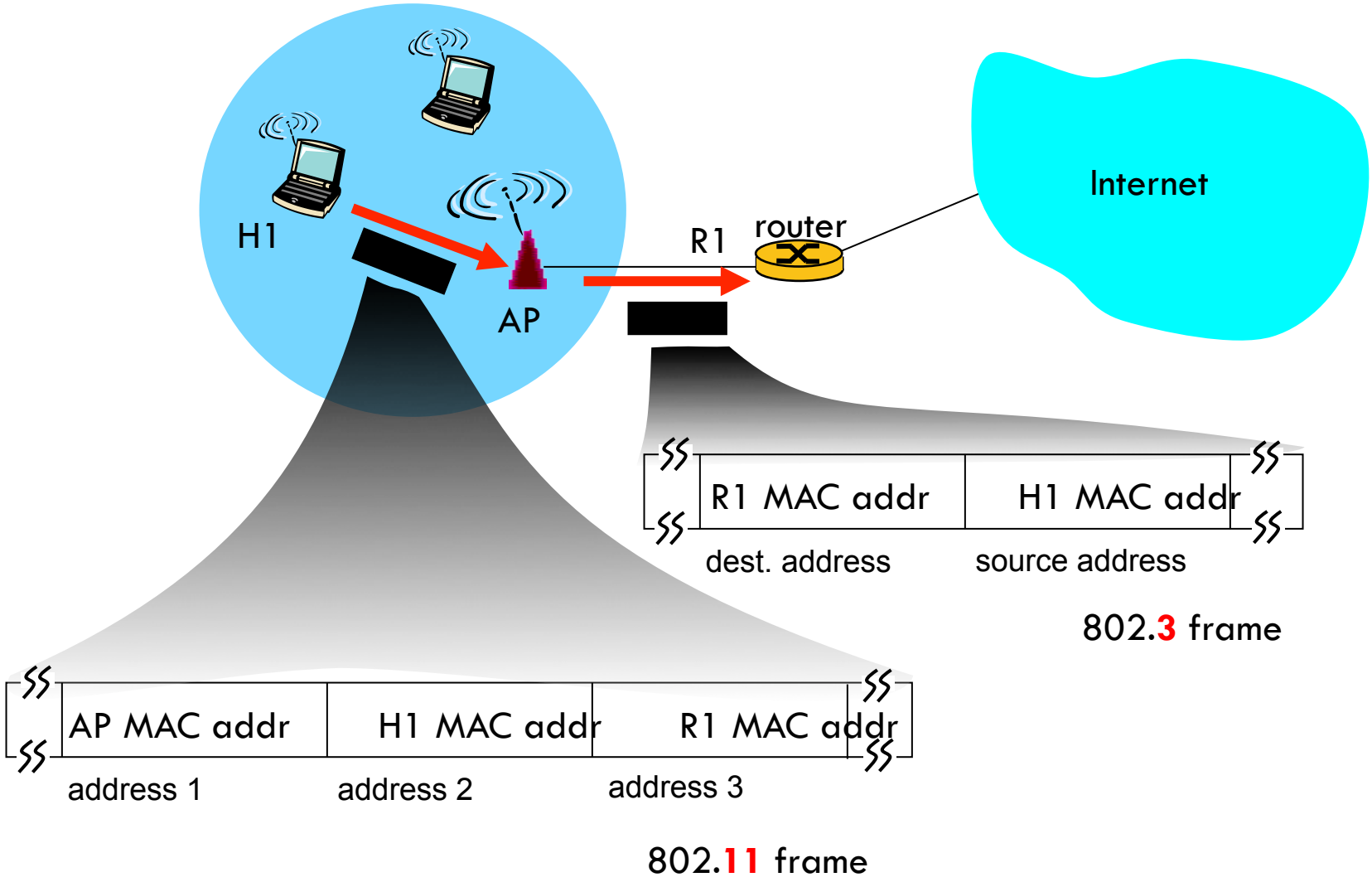
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

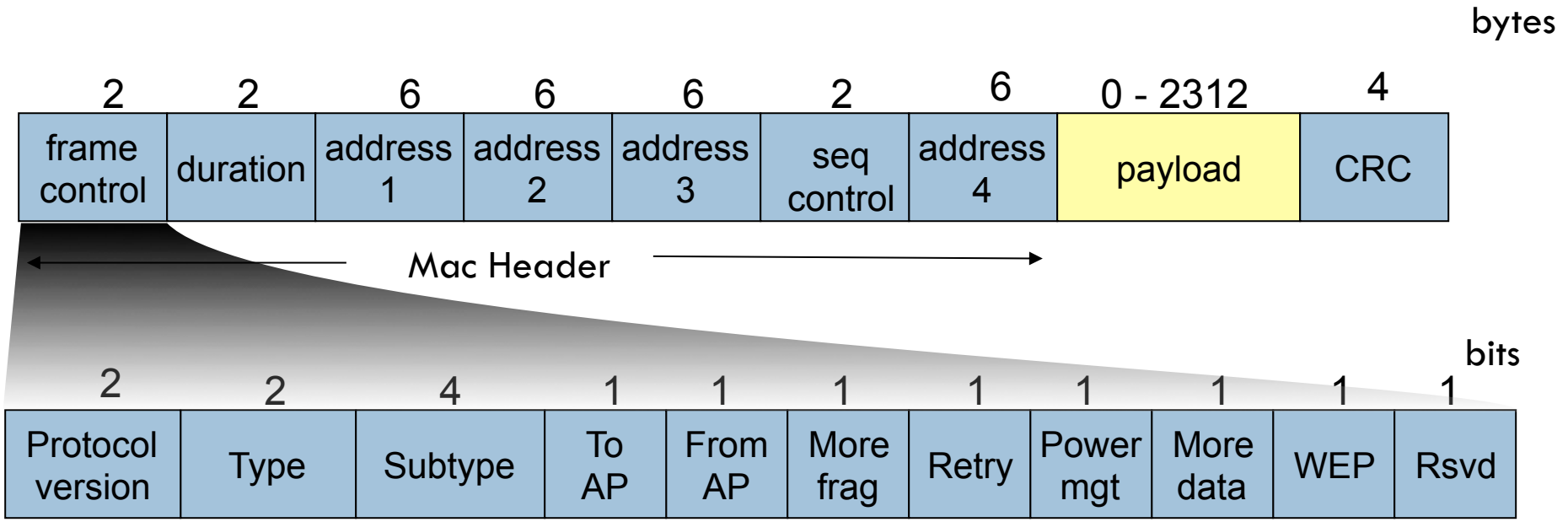
Address 3: MAC address of router interface to which AP is attached or MAC address of another station on the BSS

Address 4: used only in ad hoc mode

802.11 frame: addressing



802.11 frame: more

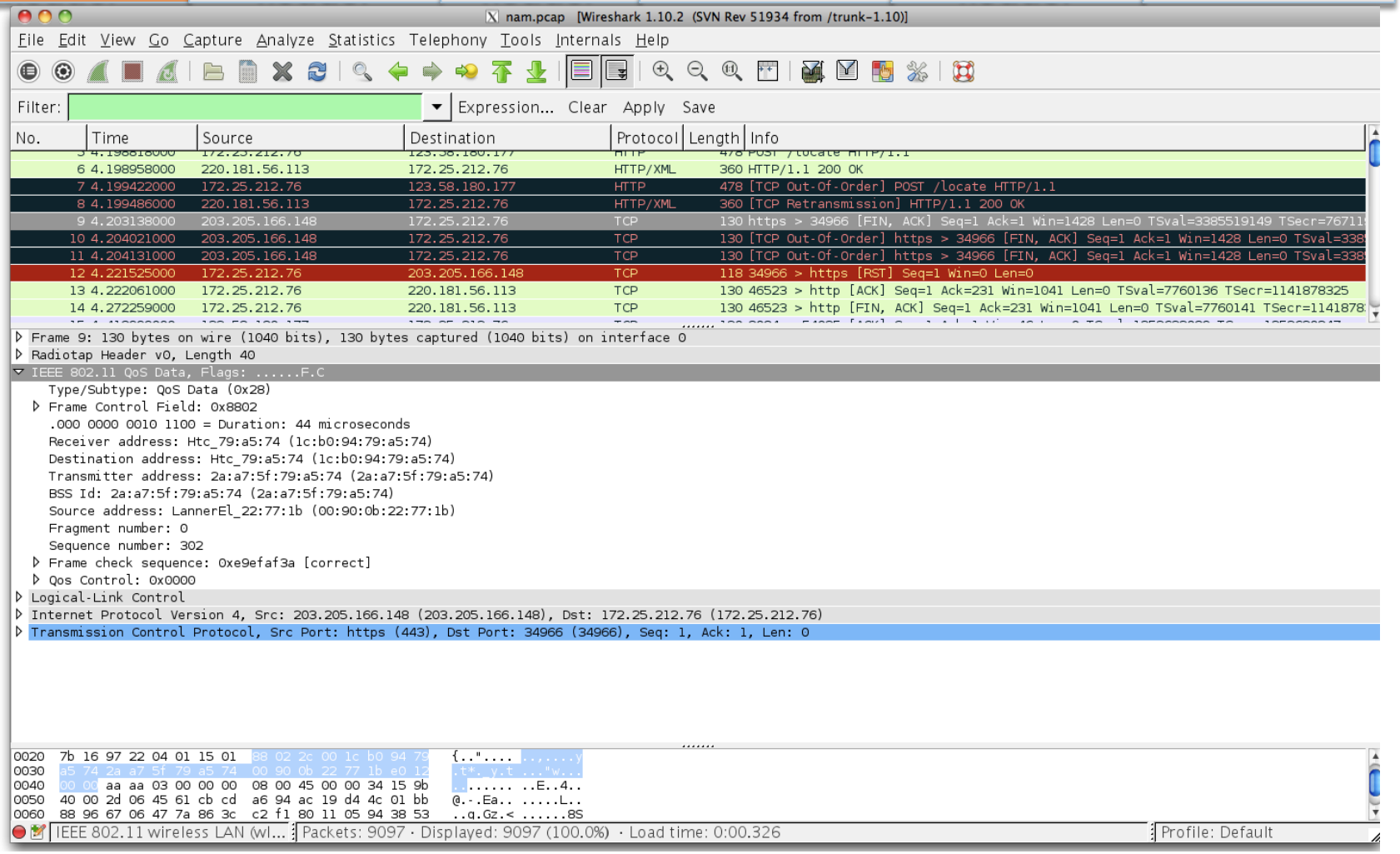


frame type (control, management, data)

Subtype:
Control: ACK, RTS, CTS
Management: authentication, association, beacon …

Where is MAC Frame?

Radiotap header	802.11 header	802.3 header	IP header	TCP/UDP header	App payload



Frame Types

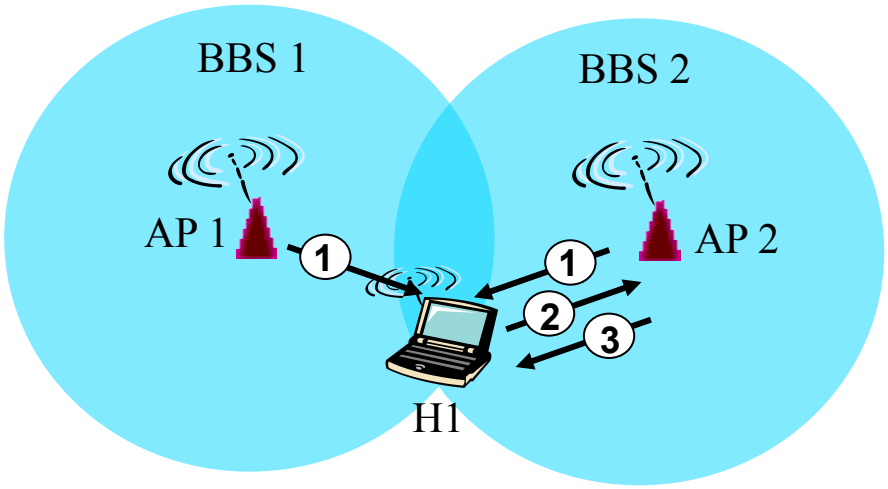
- Management frame (0)
  - Beacon (8)
  - (De)association request/respond (0/1)
  - Announcement traffic indication message
  - Authentication/Deauthentication
- Control frame (1)
  - Poll frame & poll response frame
  - RTS
  - CTS
  - ACK
  - Power save (PS-poll)
- Data frame (2)
  - Data (2)
  - QoS Data (8)
  - There is no limitation on the frame size unlike Ethernet

http://www.willhackforsushi.com/papers/80211_Pocket_Reference_Guide.pdf

Association

- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing service set identifier and AP's MAC address
    - SSID is 32 octets long
    - One SSID per network (BSS or IBSS)
  - selects AP to associate with; initiates association protocol
  - may perform authentication
  - will typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning

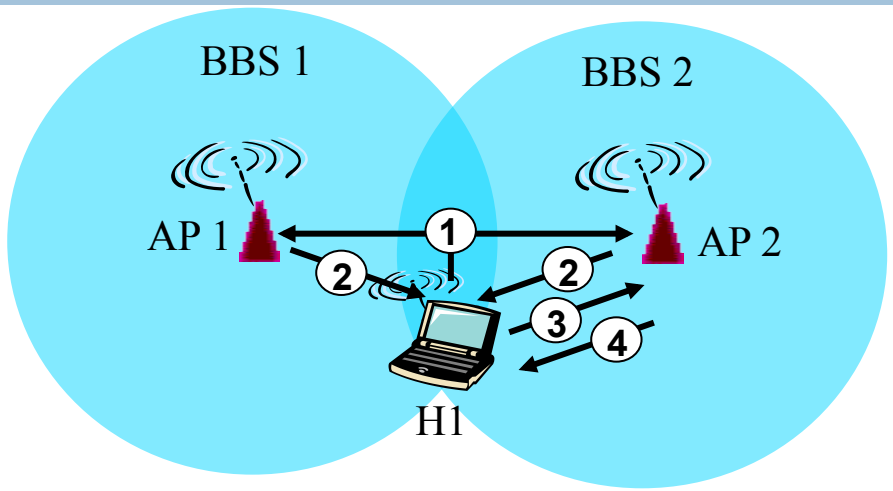


- *Passive Scanning:*

(1) beacon frames sent from APs

(2) association Request frame sent: H1 to selected AP

(3) association Response frame sent: H1 to selected AP



- *Active Scanning*:

(1) Probe Request frame broadcast from H1

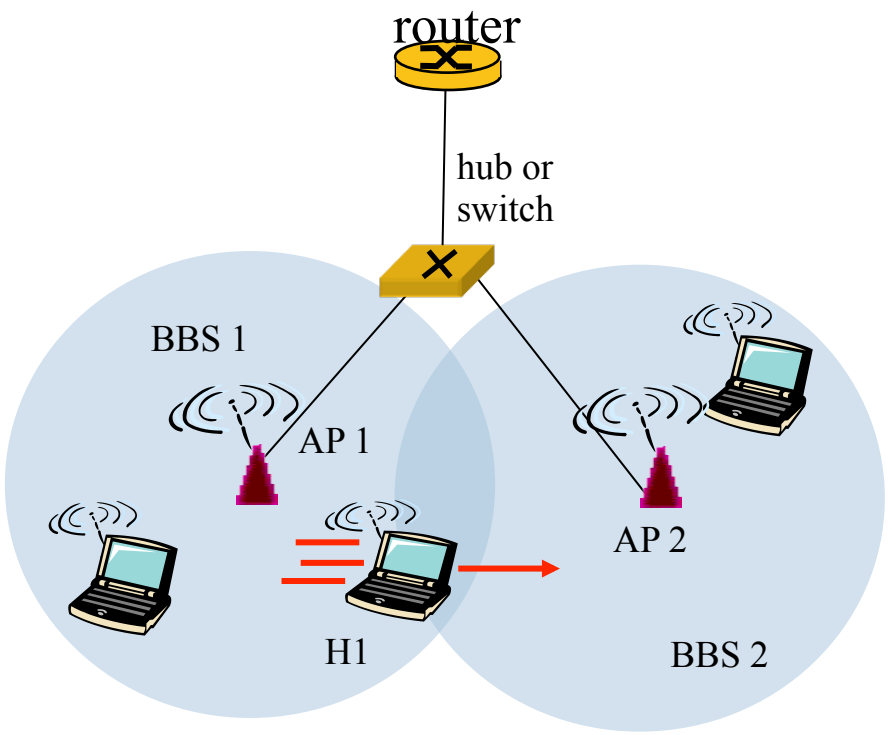
(2) Probes response frame sent from APs

(3) Association Request frame sent: H1 to selected AP

(4) Association Response frame sent: H1 to selected AP

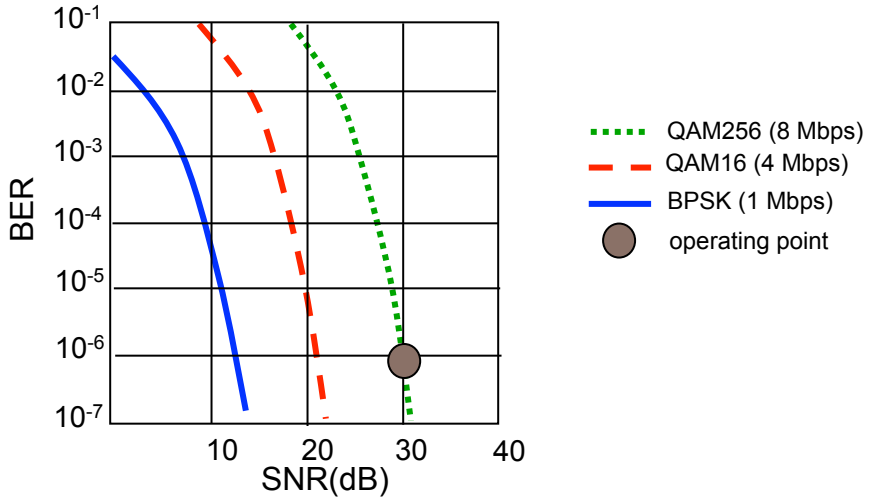
802.11: mobility within same subnet

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning : switch will see frame from H1 and "remember" which switch port can be used to reach H1



Rate Adaptaion

- Rate Adaptation
- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies

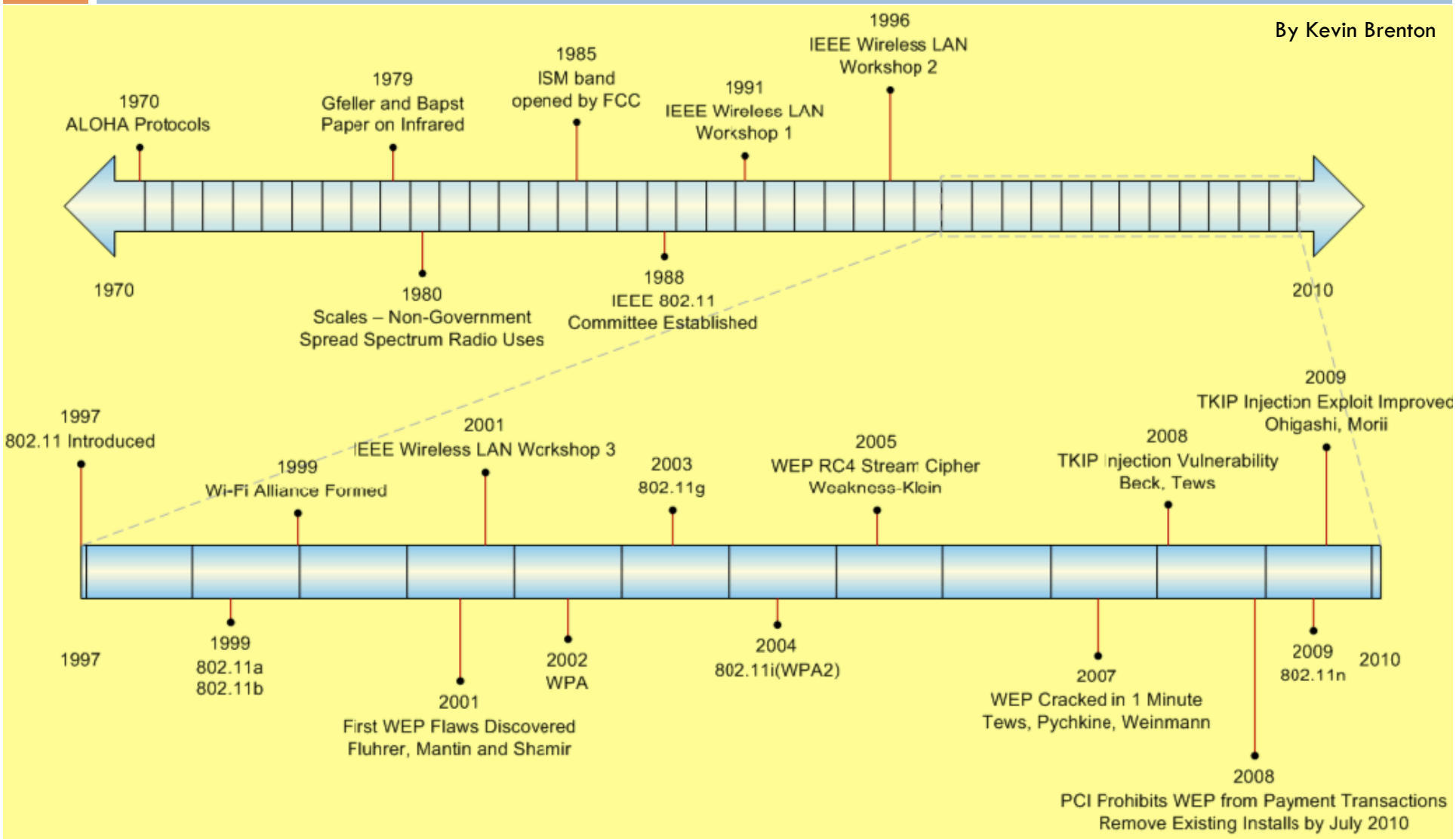


1. SNR decreases, BER increase as node moves away from base station
2. When BER becomes too high, switch to lower transmission rate but with lower BER

Power Management

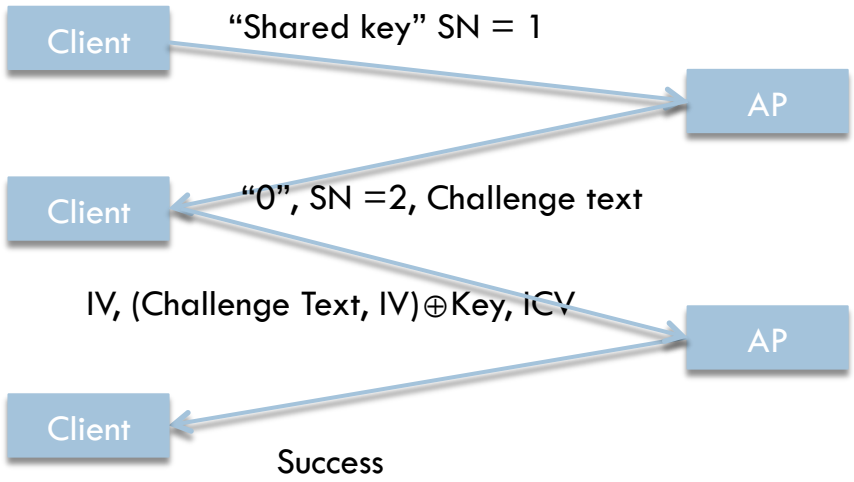
- node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

WLAN Security Timeline



Authentication in WEP

- Open authentication (= no authentication)
  - The station identifies authentication algorithm as "Open system"
  - The AP responds with status code "0" for success
- Shared key authentication



Epic failure!

Wired Equivalent Privacy (WEP)

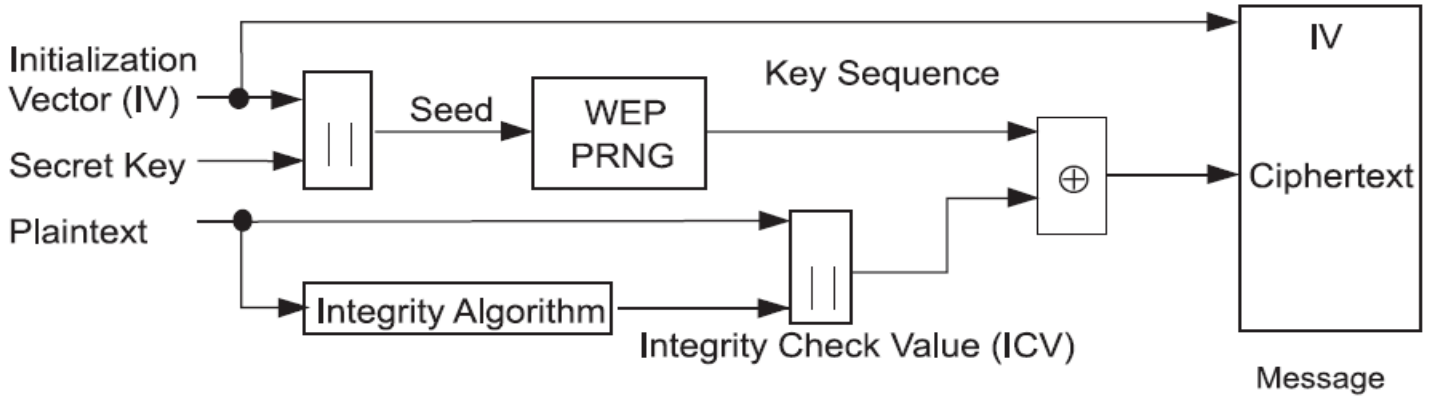


Figure 44—WEP encipherment block diagram

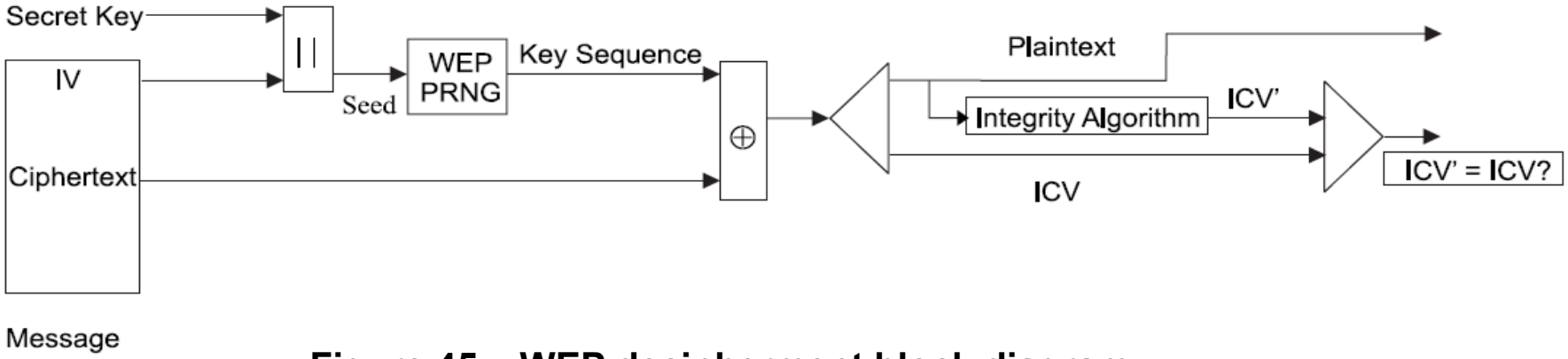
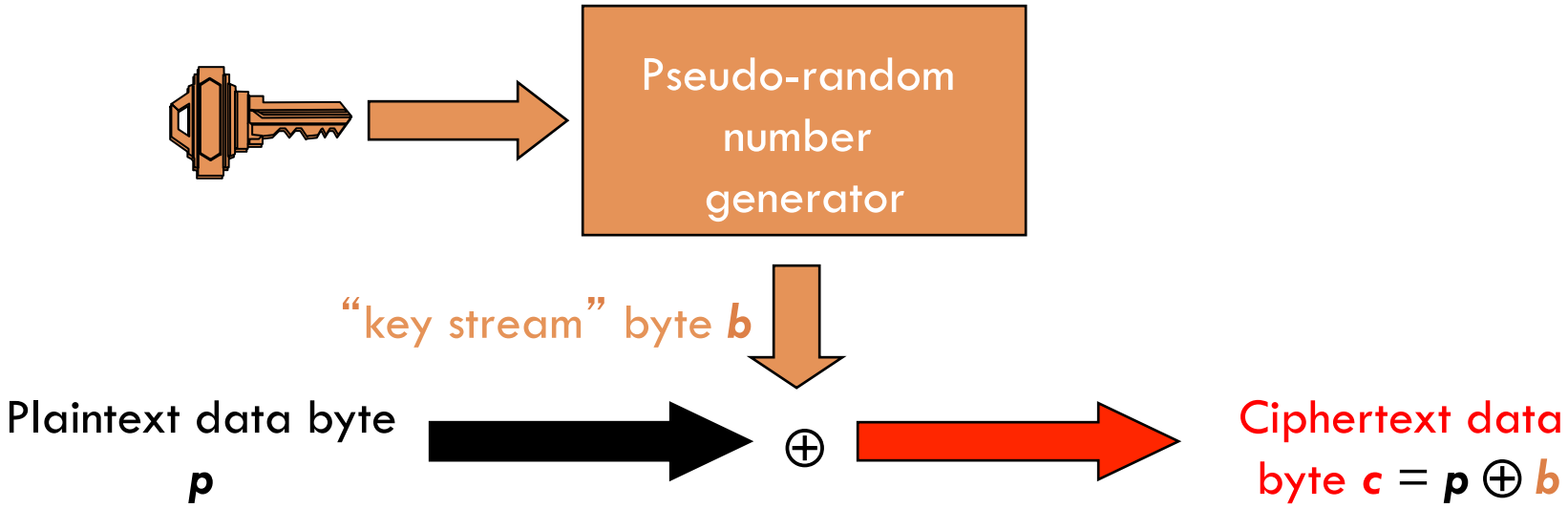


Figure 45 – WEP decipherment block diagram

Review of the cipher RC4

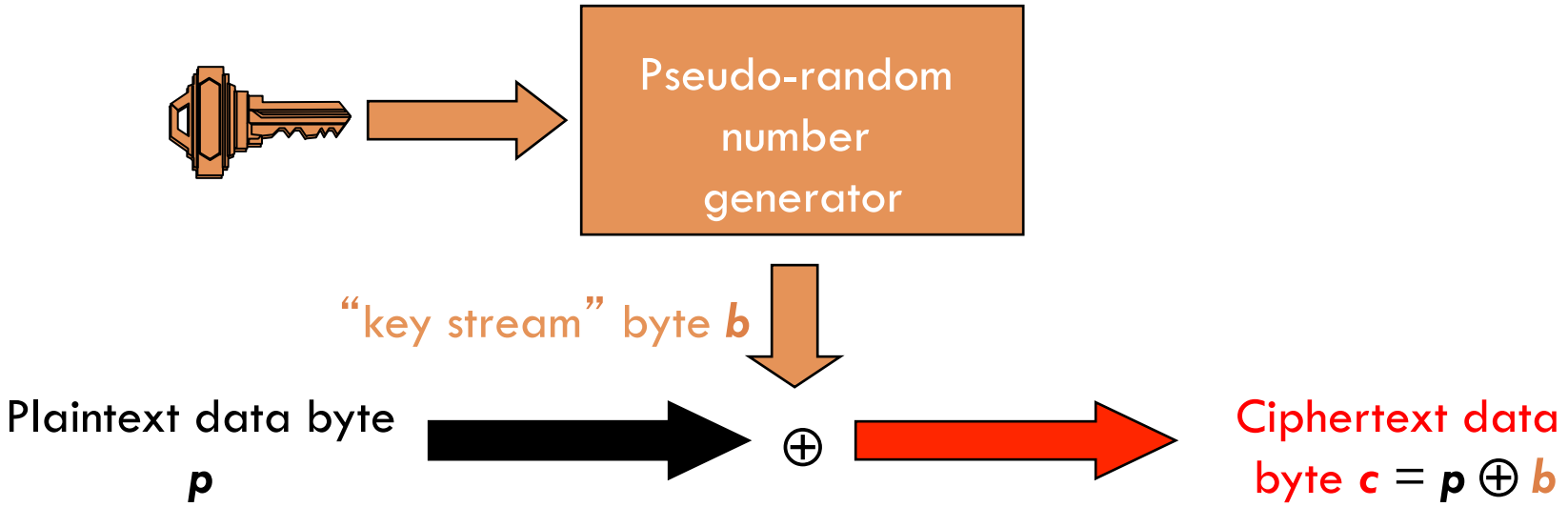


Decryption works the same way: $p = c \oplus b$

Thought experiment: what happens when p_1 and p_2 are encrypted under the same "key stream" byte b?

$$c_1 = p_1 \oplus b \quad c_2 = p_2 \oplus b$$

Review of the cipher RC4



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

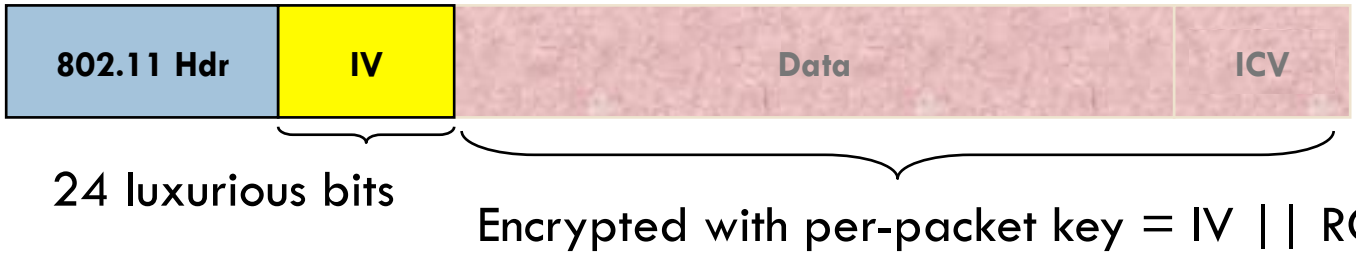
Thought experiment: what happens when p_1 and p_2 are encrypted under the same "key stream" byte b?

$$c_1 = p_1 \oplus b \quad c_2 = p_2 \oplus b$$

Then: $c_1 \oplus c_2 = (p_1 \oplus b) \oplus (p_2 \oplus b) = p_1 \oplus p_2$

The need for a different IV for each frame!

Collision attacks



•RC4 key must be changed at least every 2^{24} packets or data is exposed through IV collisions!

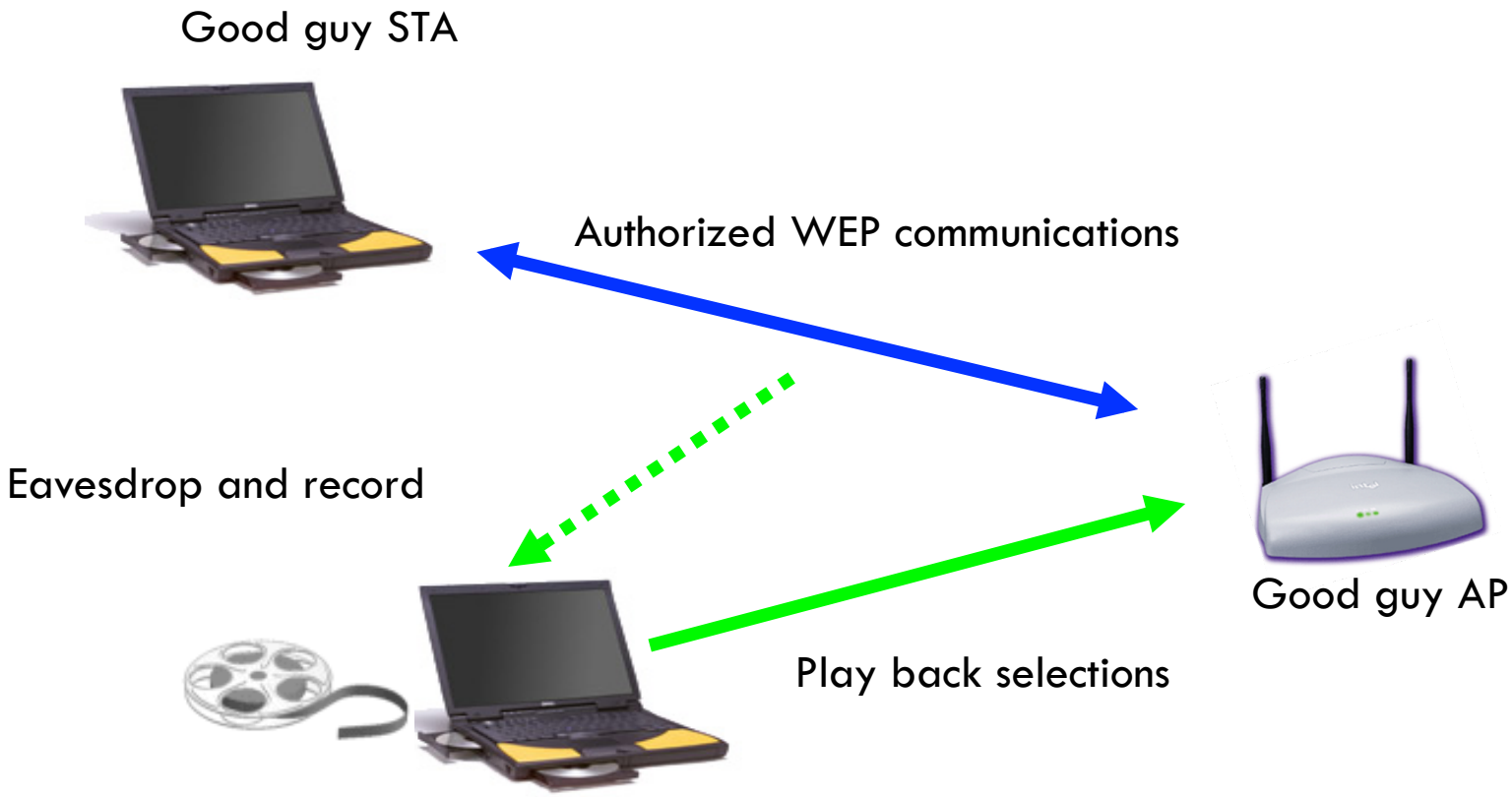
Some implemented IV selection strategies:

• Random: Collision probability P_n two packets will share same IV after n packets is $P_2 = 1/2^{24}$ for $n = 2$ and $P_n = P_{n-1} + (n-1)(1-P_{n-1})/ 2^{24}$ for $n > 2$.

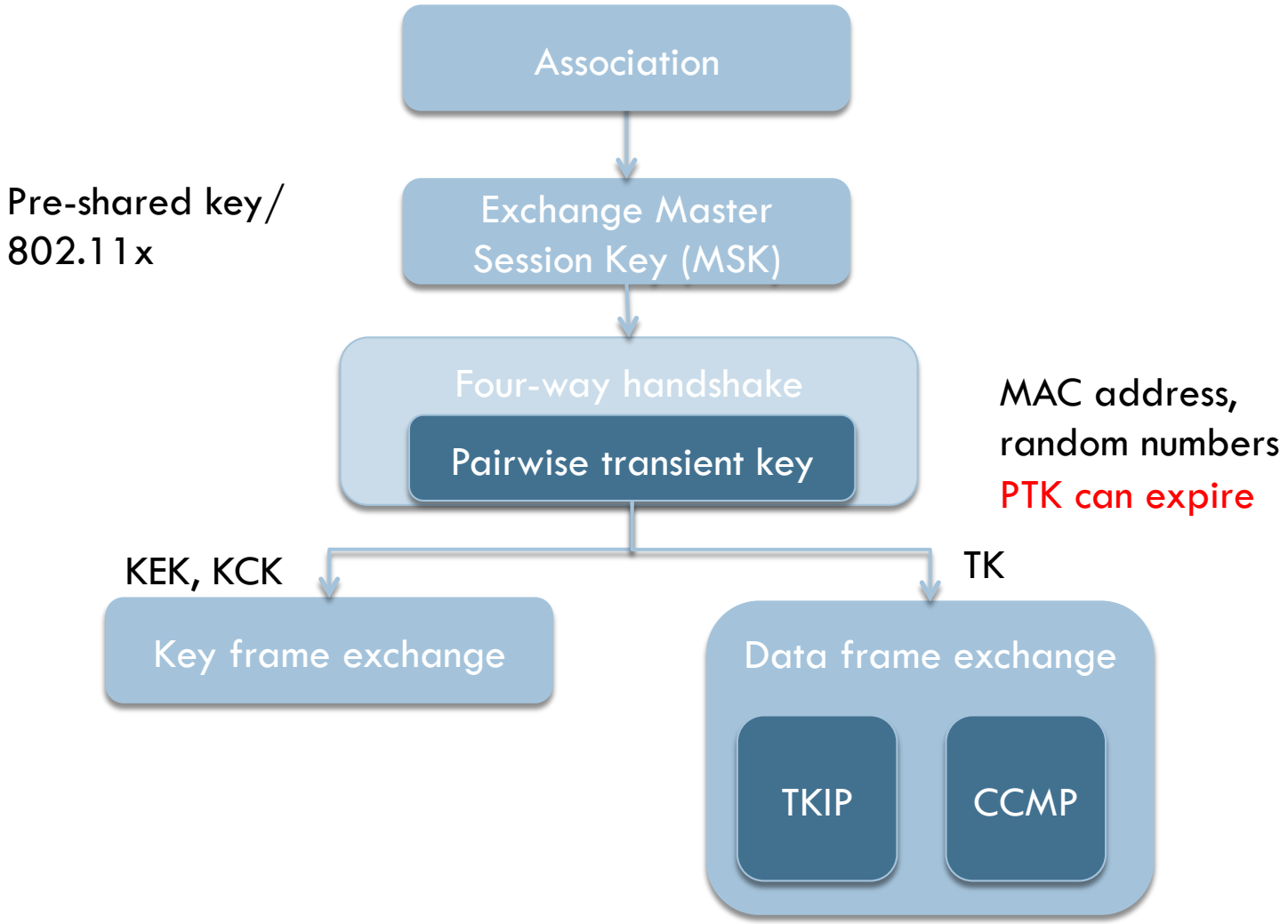
- ❑ 50% chance of a collision exists already after only 4823 packets!!!

• Increment from 0: Collision probability = 100% after ***two*** devices transmit

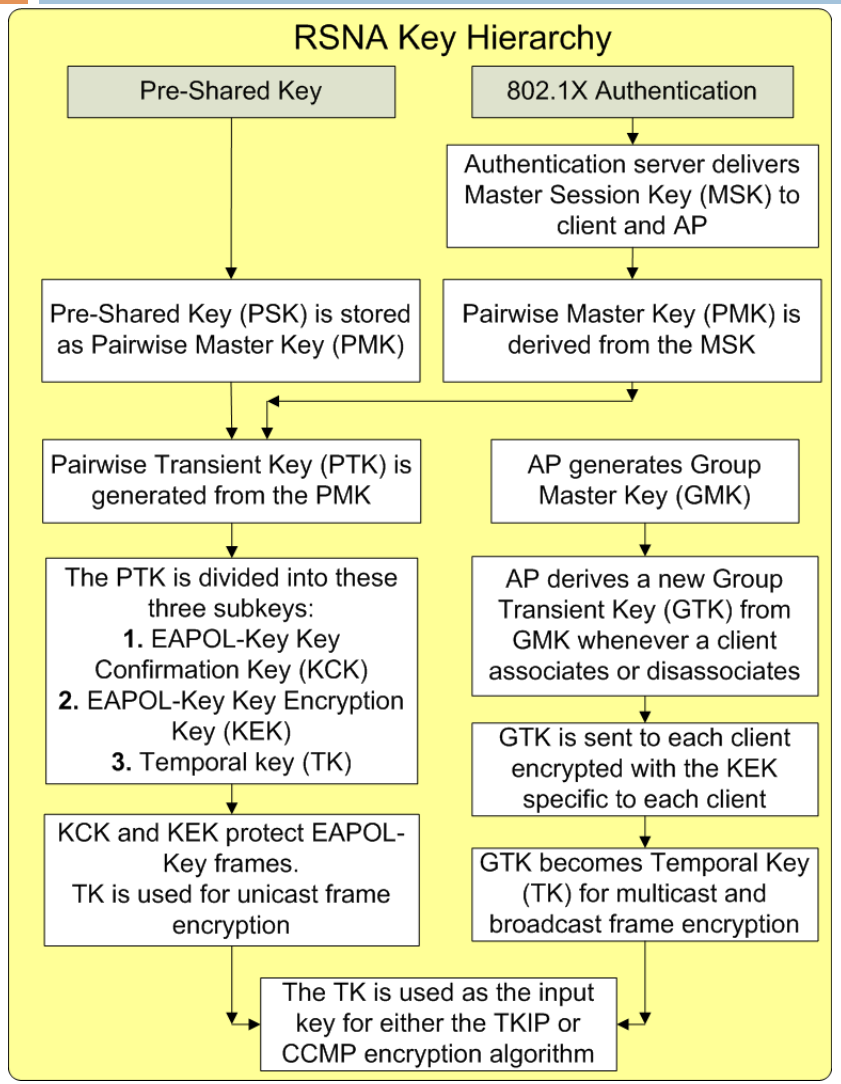
Replay attacks



Overview of 802.11i

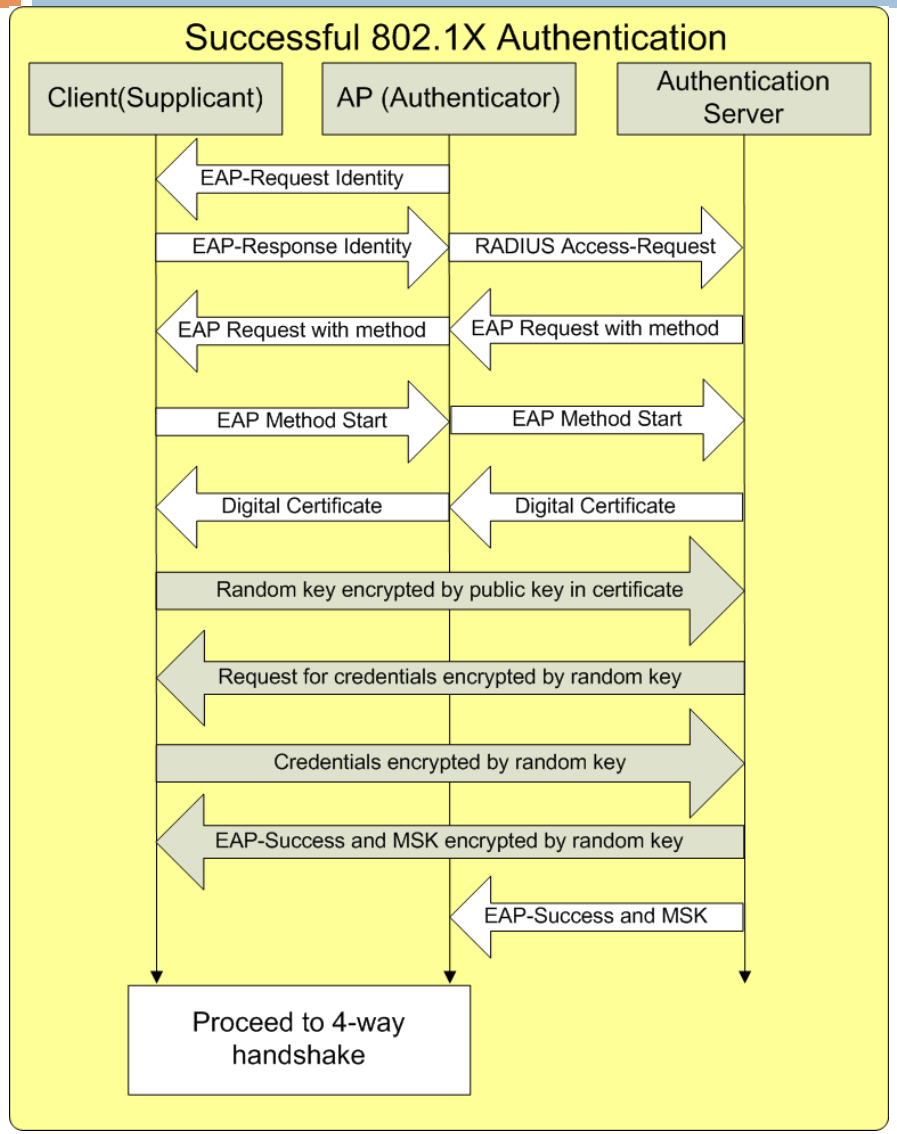


Key generation in 802.11i



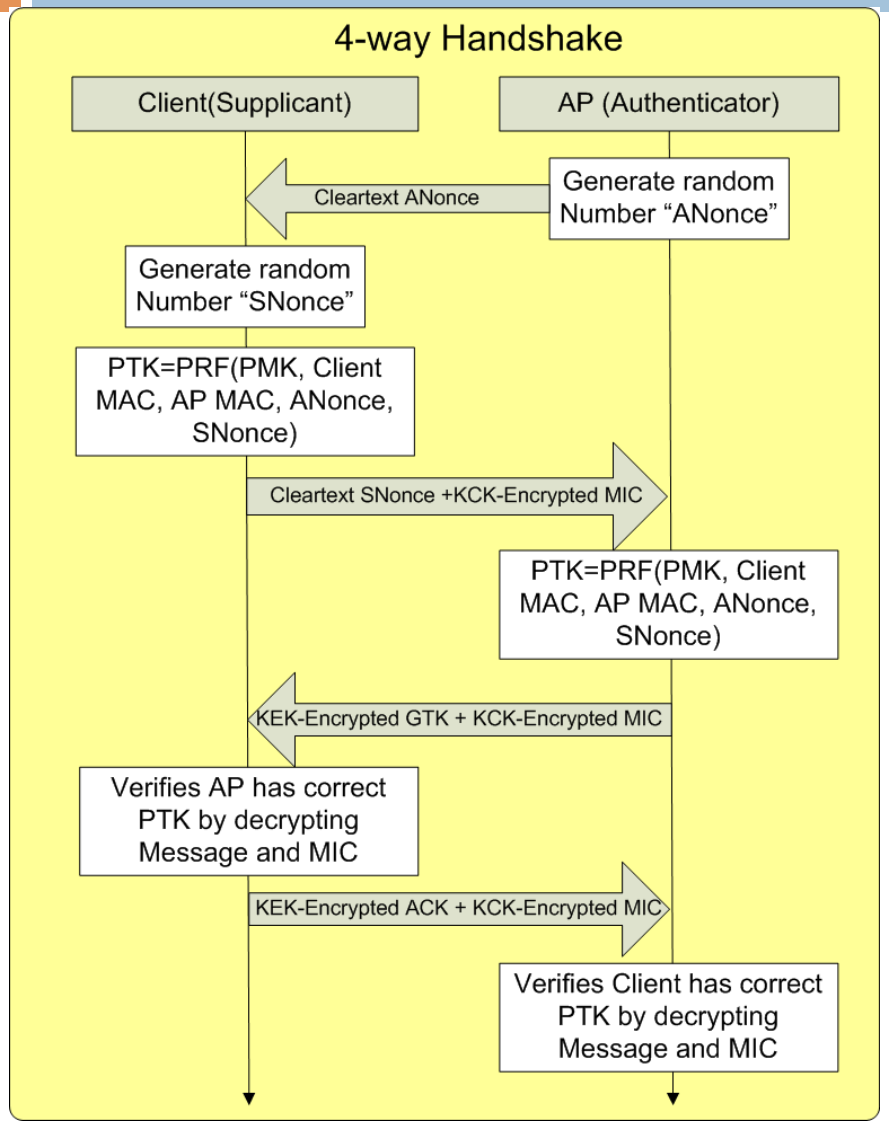
- One weakness of using PSK is that it is common to all users and cannot be easily revoked
- Pairwise transient key (PTK) is generated via the 4-way handshake
- GTK is common to all clients for broadcast/ multicast

Generation of MSK in 802.1X



- Done after association, before 4-way handshake
- The resulting PMK is unique to each client
- Different extended authentication protocols (EAP) can be used
  - EAP-TLS
  - EAP-TTLS
  - EAP-TTLS/MSCHAPv2
  - PEAPv0/EAP-MSCHAPv2
  - PEAPv1/EAP-GTC
  - EAP-SIM
  - EAP-AKA

4-way handshake authentication



- PTK is unique to the client/AP pair
- Traffic cannot be decrypted by other clients

Summary

- Discussed 802.11 MAC frame formats
- Frame exchanged for authentication, association, data security/integrity
- Wireshark is your friend!

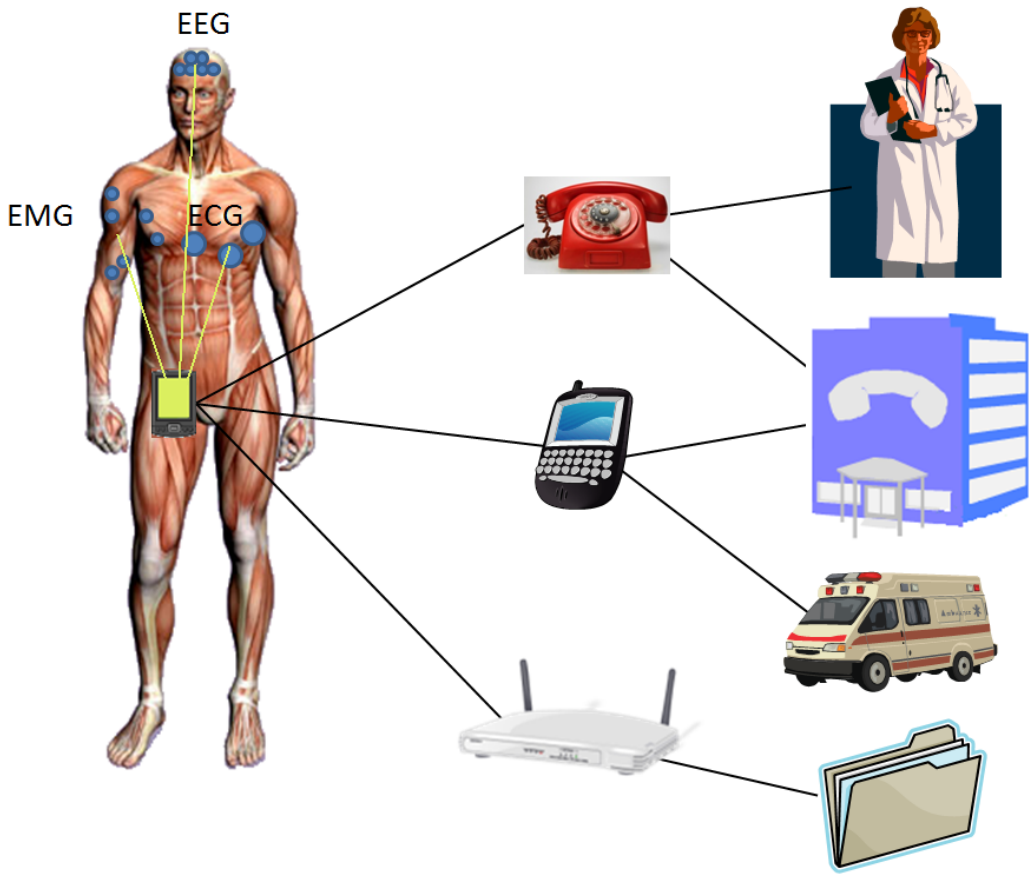
Body Area Networks (BAN)

Bio-Medical

- EEG Electroencephalography
- ECG Electrocardiogram
- EMG Electromyography (muscular)
- Blood pressure
- Blood SpO2
- Blood pH
- Glucose sensor
- Respiration
- Temperature
- Fall detection

Sports performance

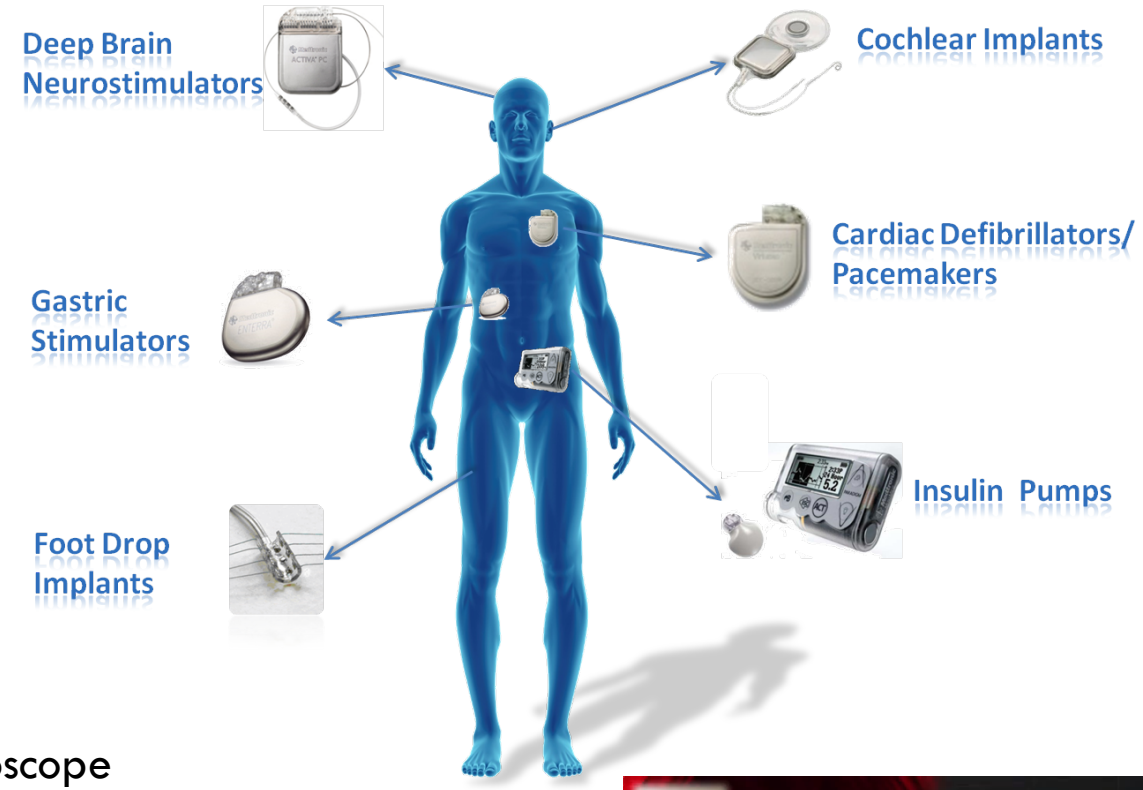
- Distance
- Speed
- Posture (Body Position)
- Sports training aid



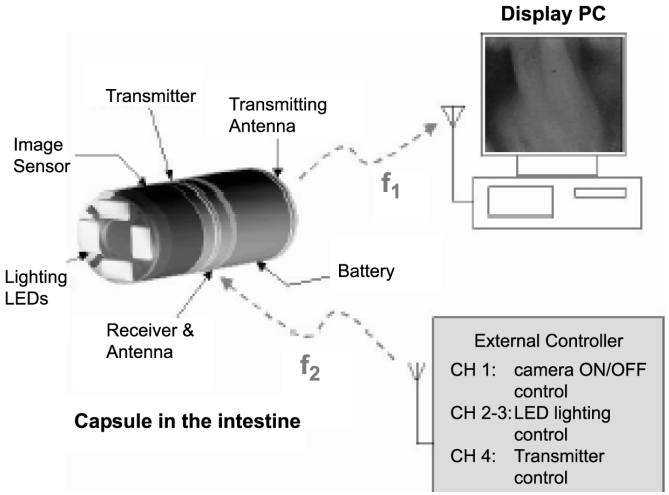
Wearable vs Implant

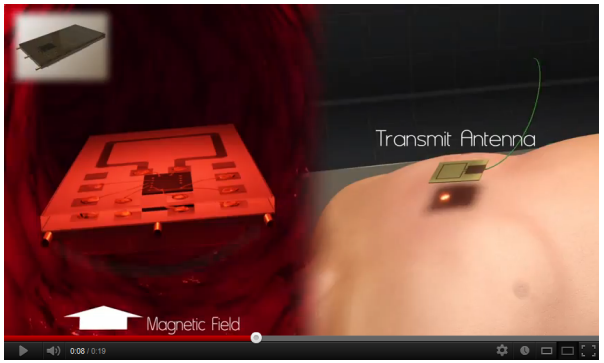
- Wearable BAN
  - Tele-metering or sensing vita signs available
  - On-body
  - Frequency less constrained
  - Short ranged
- Implant mBAN
  - Tele-control of (implanted) medical equipment and devices
  - Typically in the MCIS band (~400MHz)
  - Short ranged

WIRELESS IMPLANTABLE MEDICAL DEVICES



Wireless Endoscope





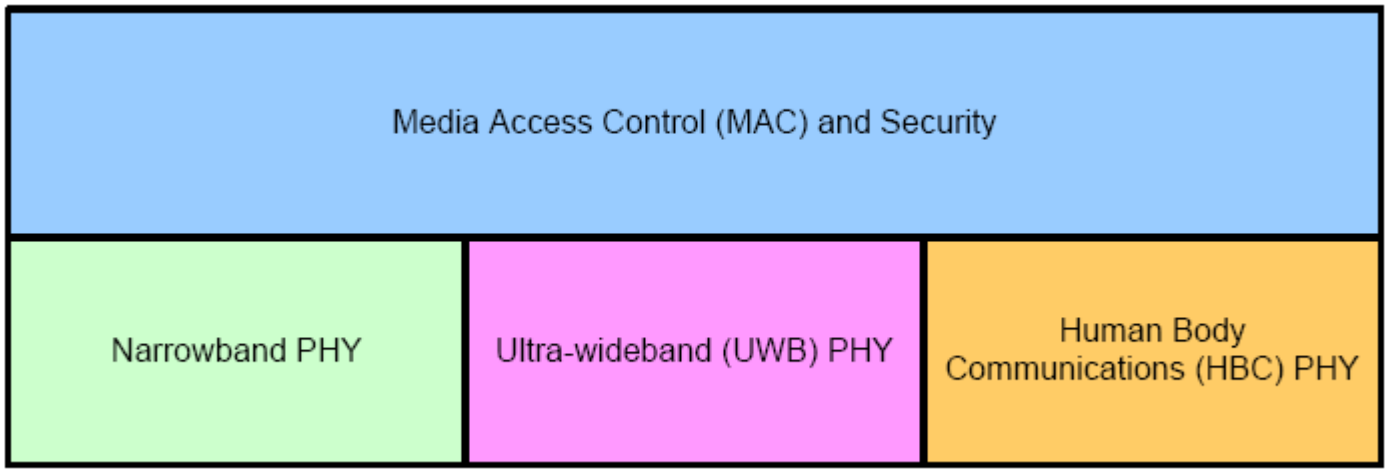
http://www.youtube.com/watch?v=oVCeGIrRGeY&feature=player_embedded

Wireless Body Area Network Standard

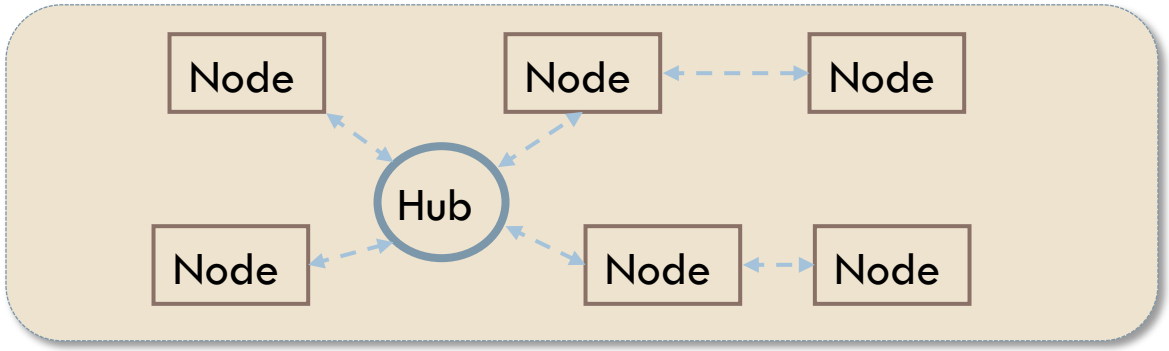
- A Body Area Network (BAN) is defined as:
  - "A communications technology that is optimized for low power consumption and operates in, on or around the human body to enable a variety of applications including medical, consumer electronics and personal entertainment"

- IEEE 802.15.6 defines the Physical (PHY) and Medium access control (MAC) layers
  - Short-range, low-power, Quality of Service (QoS) support in the vicinity of, or insides, a human body (but not limited to humans)

Architecture



BAN

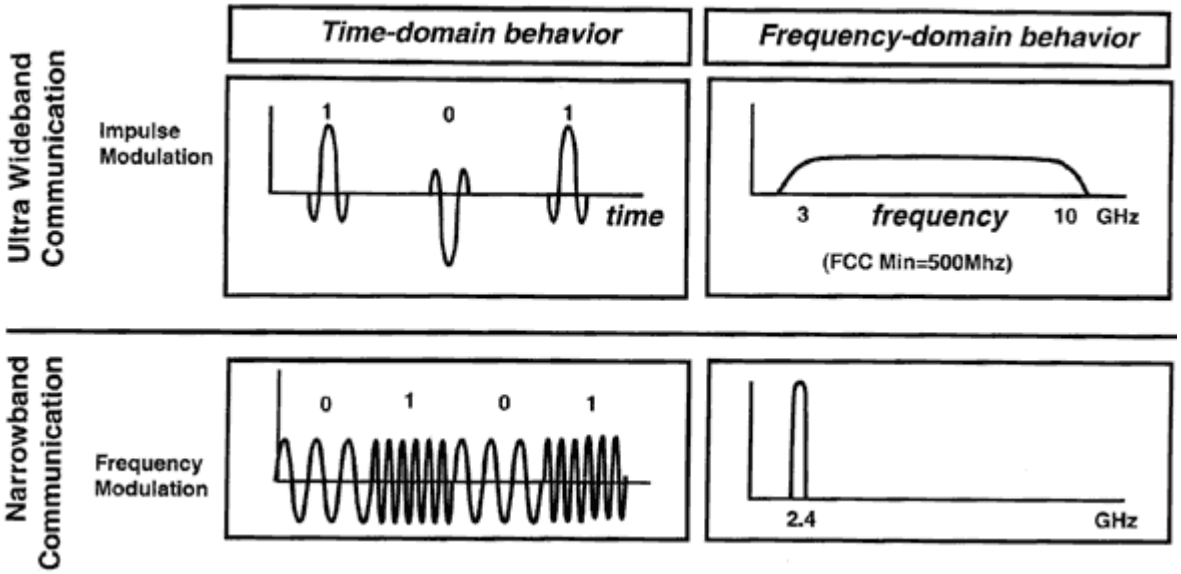


NarrowBand PHY

Band (MHz)	Number of Channels	Modulation	Symbol Rate (ksps)	Code Rate (k/n)	Spreading Factor (S)	Pulse Shape	Information Data Rate (kbps)	Support
402 – 405	10	π/2-DBPSK	187.5	51/63	2	SRRC	75.9	Mandatory
		π/4-DQPSK			1		151.8	
		π/8-D8PSK					303.6	
							455.4	Optional
863 – 870 902 – 928 950 – 956	14 60 16	π/2-DBPSK	250	51/63	2	SRRC	101.2	Mandatory
		π/4-DQPSK			1		202.4	
		π/8-D8PSK					404.8	
							607.1	Optional
2360 – 2400 2400 – 2483.5	39 79	π/2-DBPSK	600	51/63	4	SRRC	121.4	Mandatory
					2		242.9	
		π/4-DQPSK			1		485.7	
							971.4	

- low peak-power consumption (≤ 3 mA)
- Scalable data rates: 100 –1000 kbps
- Support for 10+ simultaneously operating networks

UWB PHY

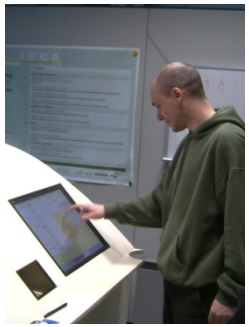


- Impulse radio (IR-UWB) and wideband FM (FM-UWB)
- Low interference
- Bit rate up to 12Mbps

Band group	Channel number	Central frequency (MHz)	Bandwidth (MHz)	Channel attribute
Low band	1	3494.4	499.2	Optional
	2	3993.6	499.2	Mandatory
	3	4492.8	499.2	Optional
High band	4	6489.6	499.2	Optional
	5	6988.8	499.2	Optional
	6	7488.0	499.2	Optional
	7	7987.2	499.2	Mandatory
	8	8486.4	499.2	Optional
	9	8985.6	499.2	Optional
	10	9484.8	499.2	Optional
	11	9984.0	499.2	Optional

Human Body Communication (HBC)

- Designed for exchanging data between devices by touching
  - The electrode in contact with the body is used for transmitting or receiving an electrical signal through the body to a device (e.g. smartphone)



e-Payment via touch screen

Exchange e-business cards via handshake

- HBC uses 21MHz band

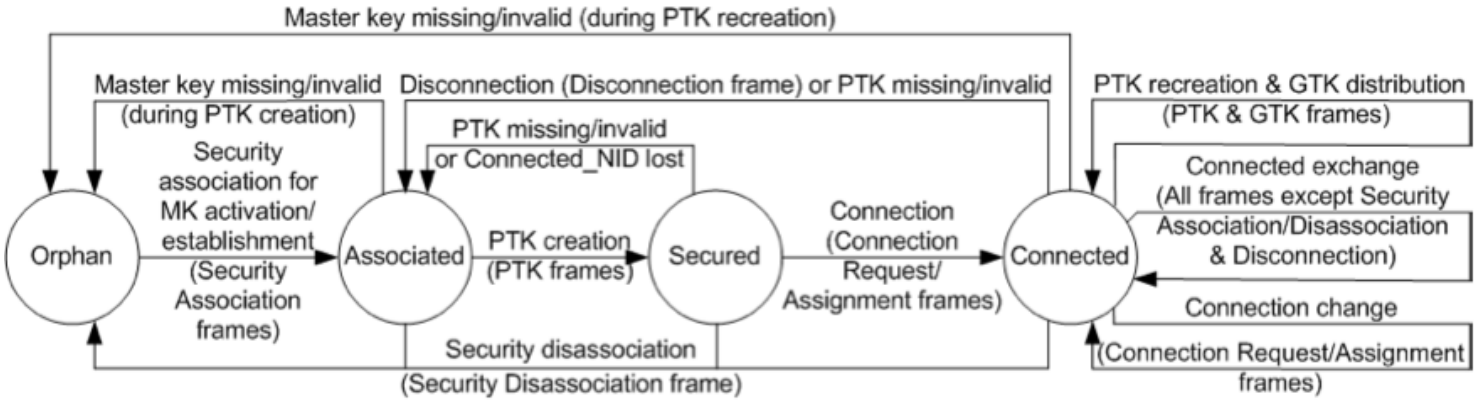
Data Rate (21MHz)
164 kbps
328 kbps
656 kbps
1.3125 Mbps

MAC Layer

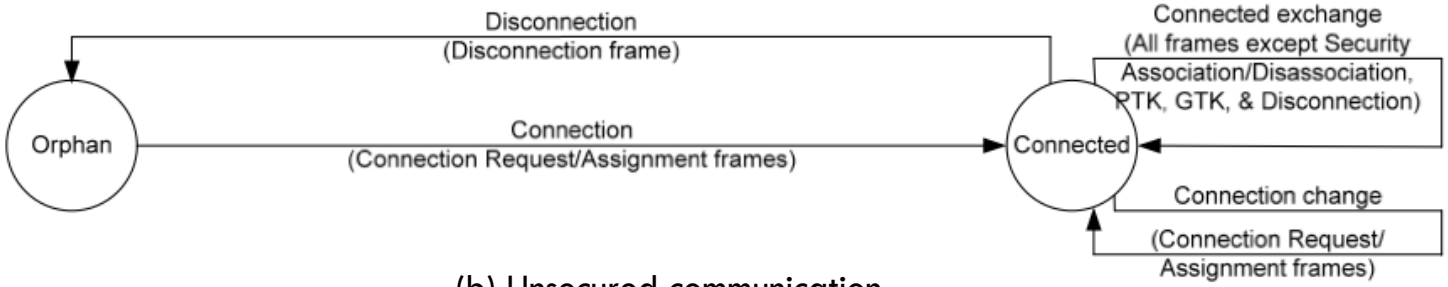
- Supports Quality of Service (QoS)
- Supports MICS band communication support
- Supports Emergency Communications
- Supports hub to node as well as node to node
- Strong Security
- Macroscopic and microscopic power management
- Coexistence and interference mitigation

Secured Communication

- Can choose from 1) unsecured communication 2) authentication but not encryption and 3) authentication and encryption



(a) Secured communication



(b) Unsecured communication

MAC support of Priority

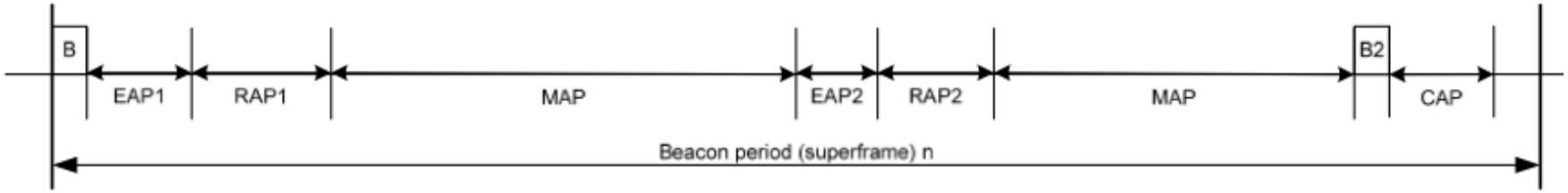
BAN Priority field encoding

Field value in decimal	BAN services
0	Non-medical services
1	Mixed medical and non-medical services
2	General health services
3	Highest priority medical services

User priority mapping

Priority	User Priority	Traffic designation	Frame type	Contention windows in CSMA/CA
Lowest	0	Background (BK)	Data	[16. 64]
]	1	Best effort (BE)	Data	[16, 32]
	2	Excellent effort (EE)	Data	[8, 32]
	3	Video (VI)	Data	[8, 16]
	4	Voice (VO)	Data	[4, 16]
	5	Medical data or network control	Data or management	[4, 8]
	6	High priority medical data or network control	Data or management	[2, 8]
Highest	7	Emergency or medical event report	Data	[1, 4]

Medium access



- Beacon mode with beacon periods (superframe)
  - B -- beacon
  - Exclusive access phase 1 (EAP1), exclusive access phase 2 (EAP2)
    - for highest priority data
  - Random access phase 1 (RAP1), random access phase 2 (RAP2)
    - (can be combined by EAPs)
  - Managed access phase (MAP), and
    - Scheduled up/down link transmissions
  - Contention access phase (CAP)

Other features

- Power management
  - Node can perform macroscopic power management by sleeping more than one beacon period, or
  - Microscopic power management within a beacon period
- Coexistence and interference mitigation among multiple BANs
  - Beacon shifting
  - Channel hopping (after dwelling in the current channel for a fixed number of beacon periods)
  - Active superframe interleaving
- Two-hop star topology extension