教育部資通訊科技人才培育先導型計畫

IEEE 802.11技術簡介

任課老師：陳懷恩
助理教授兼任資訊工程研究所所長
電算中心資訊網路組組長
國立宜蘭大學
Email: wechen@niu.edu.tw

Outline

- IEEE 802.11 Family
- IEEE 802.11 Standard's Evolution
- Management features of 802.11
- How does a station join an existing cell
- Competing technologies to IEEE 802.11

Adv. vs. Disadv.

- Advantages
  - Without cabling for client devices
  - Low cost
  - “Wi-Fi Certified”
  - Widely available
  - …
- Disadvantages
  - Spectrum assignments not consistent worldwide
  - Power consumption
  - Limited range
  - Wi-Fi pollution
  - …

802.11 Family

802.11		
a	High-speed Physical Layer in the 5GHz Band	Finished
b	Higher-speed Physical Layer Extension in the 2.4GHz Band	Finished
d	Specification for operation in additional regulatory domains	Finished
e	MAC Quality of Service (QoS) Enhancements	
f	Inter-Access Point Protocol (IAPP)	Finished
g	Further Higher Data Rate Extension in the 2.4 GHz Band	Finished
h	Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe	Finished
i	MAC Security Enhancements	Finished
j	4.9 GHz – 5 GHz Operation in Japan	Finished
k	Specification for Radio Resource Measurement	
m	Revision of 802.11	
n	Enhancements for Higher Throughput	
p	Wireless Access for the Vehicular Environment	
r	Fast Roaming/Fast BSS Transition	
s	ESS Mesh Networking	
t	Recommended Practice for Evaluation of 802.11 Wireless Performance	
u	Interworking with External Networks	
v	Wireless Network Management	

Standards Evolution of 802.11

Mesh Extensions	802.11s
QoS Extensions	802.11e, 802.11r
Security Extensions	802.11i
Radio & Regulatory	802.11d, 802.11h, 802.11j, 802.11k
Higher Data Rates	802.11b, 802.11a, 802.11g, 802.11n

Standard Evolution Goal

- Quality of Service
- Security
- Interconnection
- Performance & Coverage
  - Performance improvement
    - Modulation Scheme
    - Channel Bonding
    - Frame Burst mode
    - MISO, MIMO
  - Coverage extension
    - Smart Antenna
    - MIMO

802.11 Family

- 802.11: the original standard with 1Mbit/s and 2Mbit/s in the 2.4GHz band.
- 802.11a:
  - High-speed physical layer (OFDM)
  - operates in 5 GHz band with a maximum raw data rate of 54 Mbit/s
- 802.11b:
  - Enhancements to 802.11 to support 5.5 and 11 Mbit/s
  - FHSS, DSSS
  - Operates in 2.4 GHz band

- 802.11d:
  - International (country-to-country) roaming extensions (2001)
- 802.11e:
  - Medium Access Control (MAC) Quality of Service (QoS) enhancement
- 802.11f:
  - Inter-Access Point Protocol
- 802.11g:
  - Applied OFDM to the 2.4 GHz band
  - Data rate up to 54 Mbit/s
  - backwards compatible with b

- 802.11h
  - provides Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) to the 802.11a MAC
  - solves problems like interference with satellites and radar using the same 5 GHz frequency band
- 802.11i
  - Medium Access Control (MAC) security enhancements
- 802.11j
  - designed specially for Japanese market
  - allows operation in 4.9 to 5 GHz band
- 802.11n
  - Higher throughput improvements using MIMO (multiple input, multiple output antennas)

Primary IEEE 802.11 Specifications

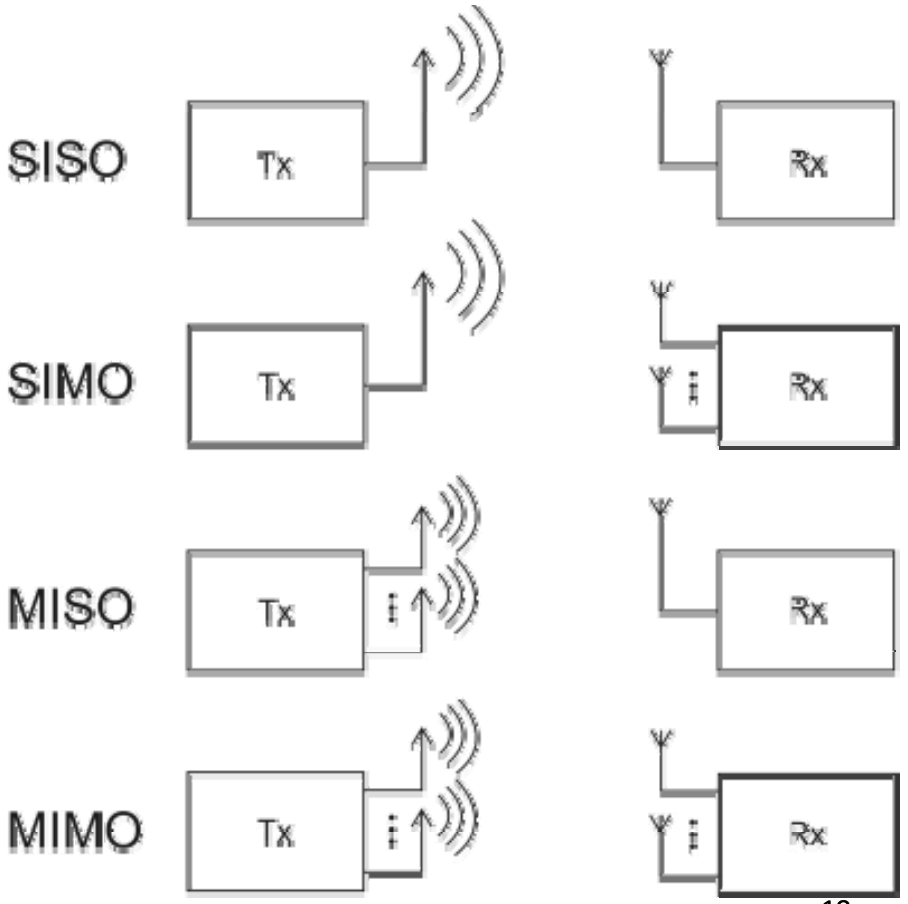
	802.11b	**802.11a**	**802.11g**	**802.11n**
Standard Approved	Dec-99	Jan-00	Jun-03	Dec-07 (Expected)
Maximum Data Rate	11 Mbps	54Mbps	54 Mbps	600 Mbps
Different Data Rates Configurations	4	8	12	576
Typical Range	70m	30 m	50m	60m
Modulation techniques	DSSS, CCK	OFDM	DSSS, CCK, OFDM	DSSS, CCK, OFDM (HT)
RF Band	2.4GHz	5GHz	2.4GHz	2.4/5GHz
Number of Spatial Streams and Antenna	1	1	1	1-4
Channel bandwidth	20MHz	20MHz	20MHz	20 or 40MHz
Number of Non-Interleaving Channels	3	23	3	26

Pros & Cons

Standard	Pros	Cons
802.11b	lowest cost; signal range is good and not easily obstructed	slowest maximum speed; home appliances may interfere on the unregulated frequency band
802.11a	fast maximum speed; regulated frequencies prevent signal interference from other	highest cost; shorter range signal that is more easily obstructed
802.11g	fast maximum speed; signal range is good and not easily obstructed	costs more than 802.11b; appliances may interfere on the unregulated signal frequency
802.11n	fastest maximum speed and best signal range; more resistant to signal interference from outside sources	standard is not yet finalized; costs more than 802.11g; the use of multiple signals may greatly interfere with nearby 802.11b/g based networks

Introduction of 802.11n

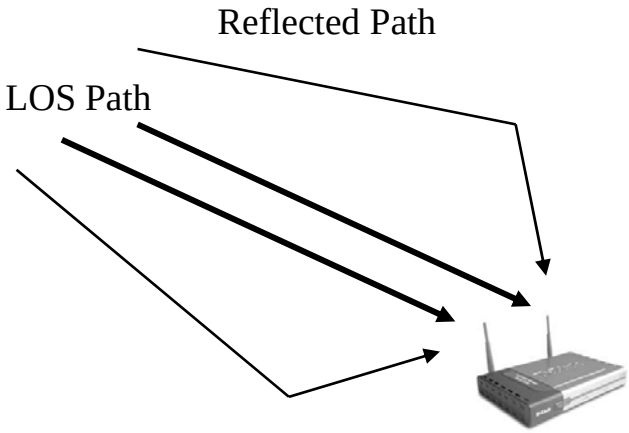
- SISO and diversity antennas
  - Single Input and Single Output is common architecture.

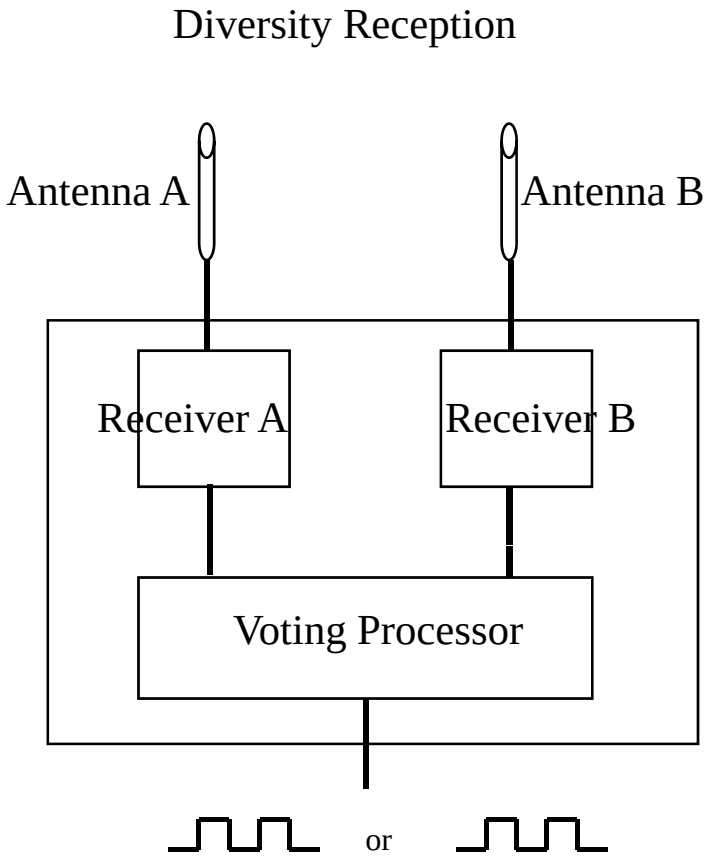


Introduction of 802.11n

- Antenna Diversity
  - To reduce the effects of multipath, dropouts on signal quality and throughput.
  - Two independent antennas and radio systems are used for transmitting and receiving signals.
  - Voting processor choose which radio has better signal path to client.

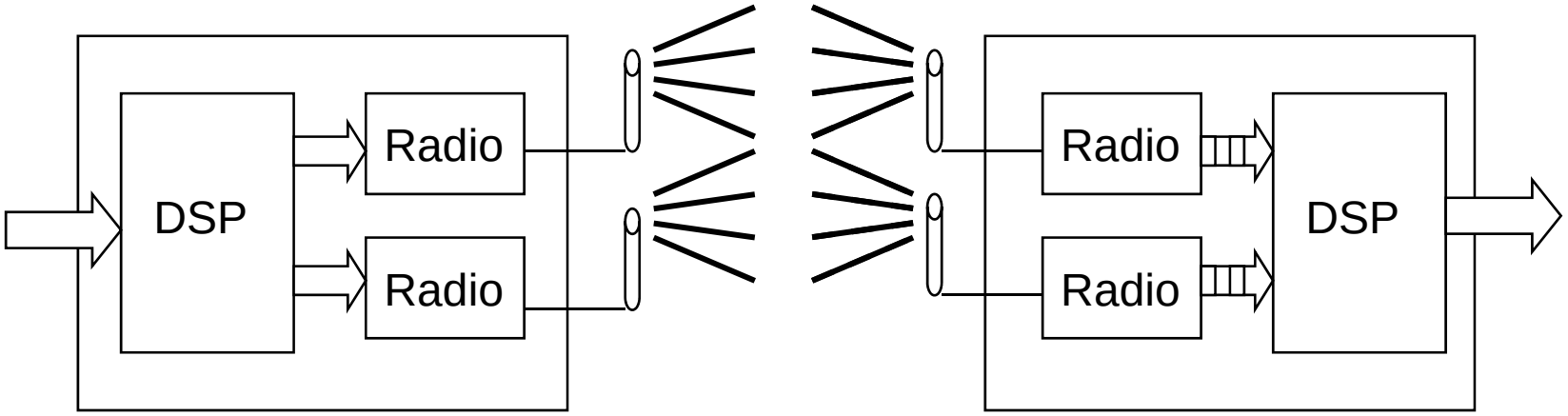
Introduction of 802.11n





How does MIMO works?

- A data stream is divided into multiple unique streams.
- Data streams are transmitted at the same time.
- MIMO takes the advantage of multipath.
- MIMO receiver combines all streams.



Advantage of 802.11n

- Overcoming the multipath effect of RF
- Higher performance
- More coverage

What is 802.11n

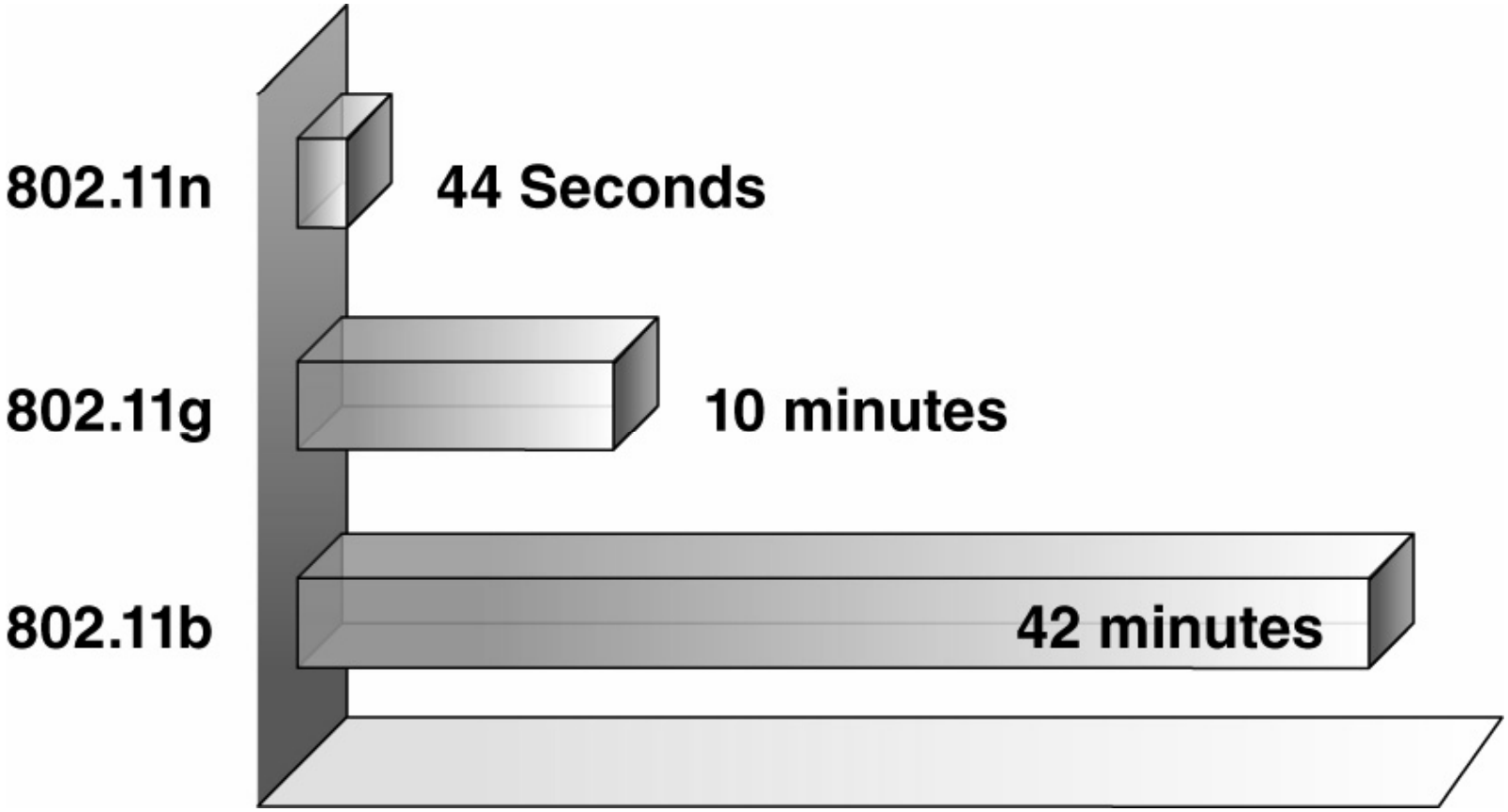
- New IEEE Standard (not approved yet)
- Uses MIMO radio technology
- Provides “wire-like” performance
- Data rate is from 100Mbps to 600Mbps which depends on implementation
- Supports both 2.4 GHz and 5 GHz
- Includes advances in QoS & Power Saving
- High definition video mode at 5 GHz
- Uses multiple streams
- Less interference and more channels

Major components of 802.11n

Features	Definition	Standard Status
Better OFDM	Supports wider bandwidth & higher code rate (max. data rate -- 65Mbps)	Mandatory
Space-Division Multiplexing	Multiple streams transmitted through multiple antennas	Optional Up to 4 spatial streams
Diversity	Exploits the existence of multiple antenna to improve range and reliability	Optional Up to 4 antennas
MIMO Power Save	Limit power consumption by utilizing multiple antennas only on as-needed basis	Mandatory

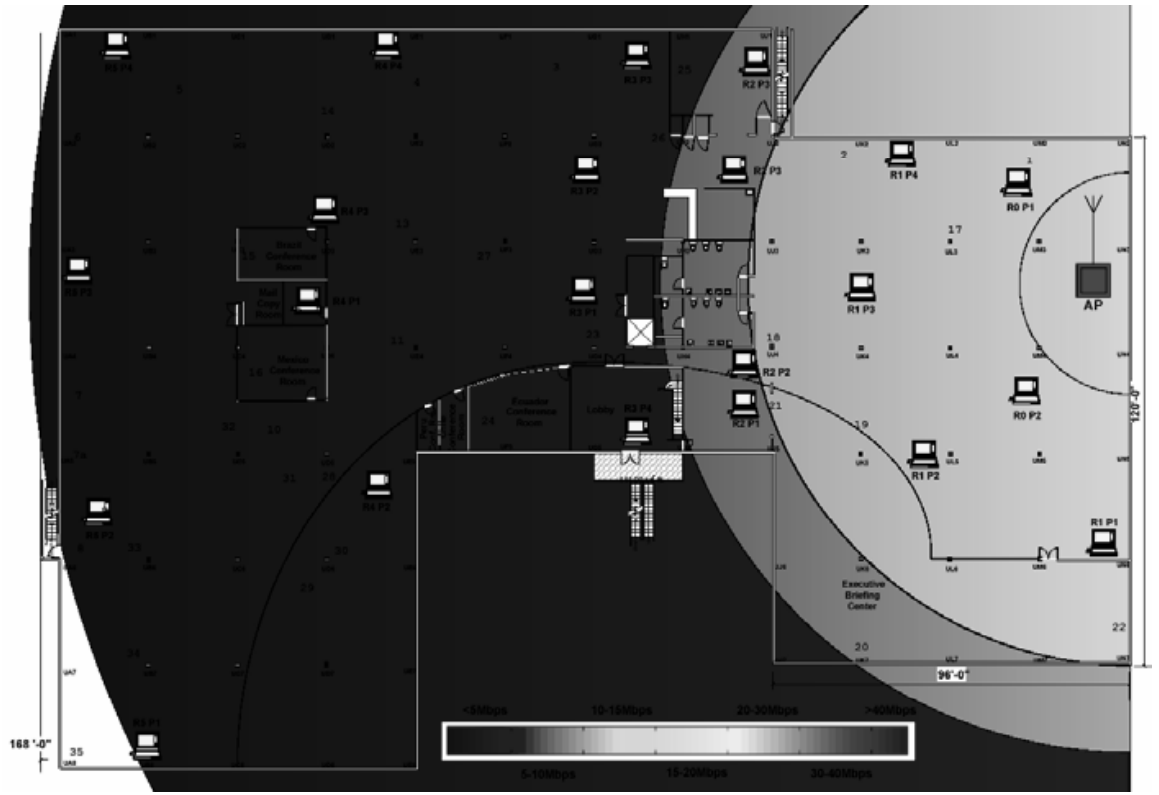
Major components of 802.11n (cont)

Features	Definition	Standard Status
40MHz Channels	Doubles data rates by doubling bandwidth from 20MHz to 40MHz	Optional
Aggregation	Allowing bursts of multiple data packets between overhead communications	Required
Reduced Inter-frame Spacing (RIFS)	Provides a shorter delay between OFDM transmissions than in 802.11a or g	Required
Greenfield Mode	Eliminates support for 802.11a/b/g devices in an all 802.11n network to improve efficiency	Optional

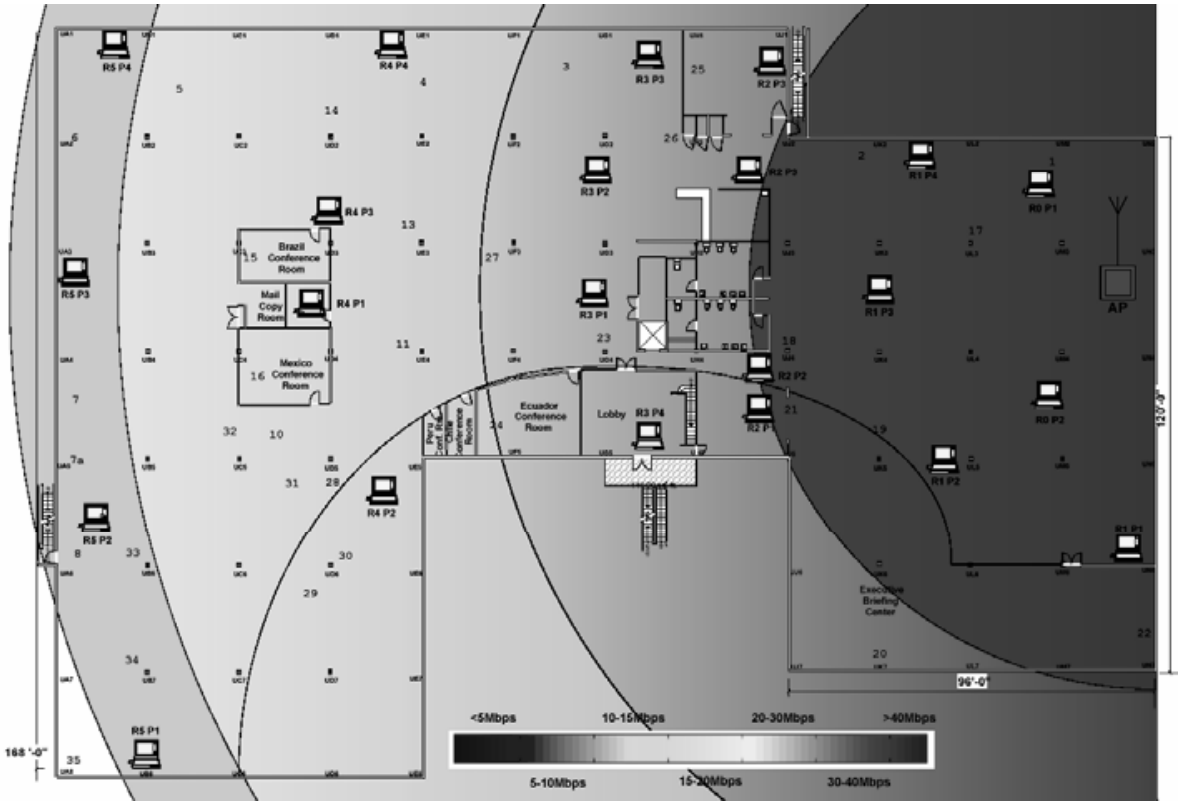


Time to transfer 30 min HD video.

Legacy 802.11a/g AP



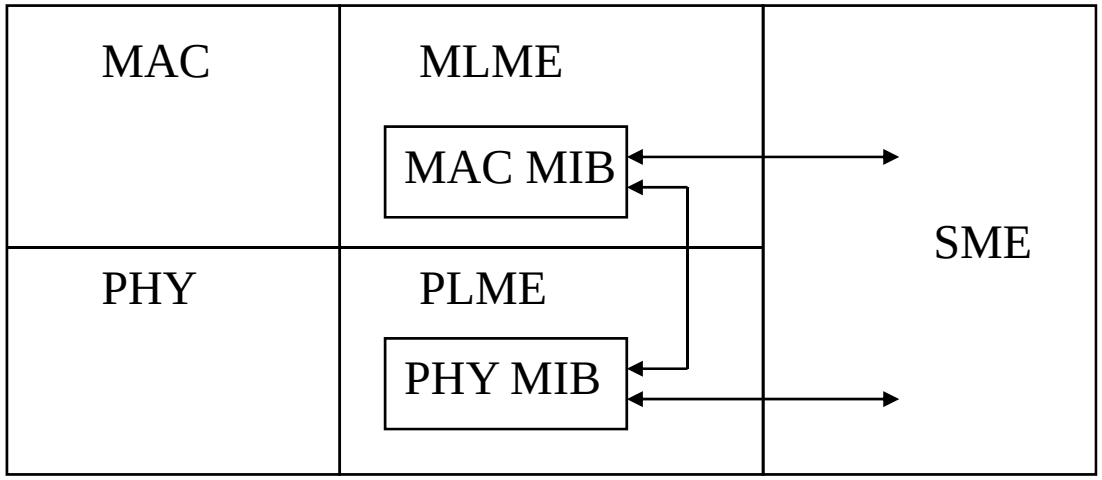
MIMO Technology



Management Issues

- Without tethering a wired network, the wireless medium is unreliable.
- Users can take advantage of the lack of physical boundaries.
- For a mobile devices, power consumption is always a critical problem.

Management Architecture



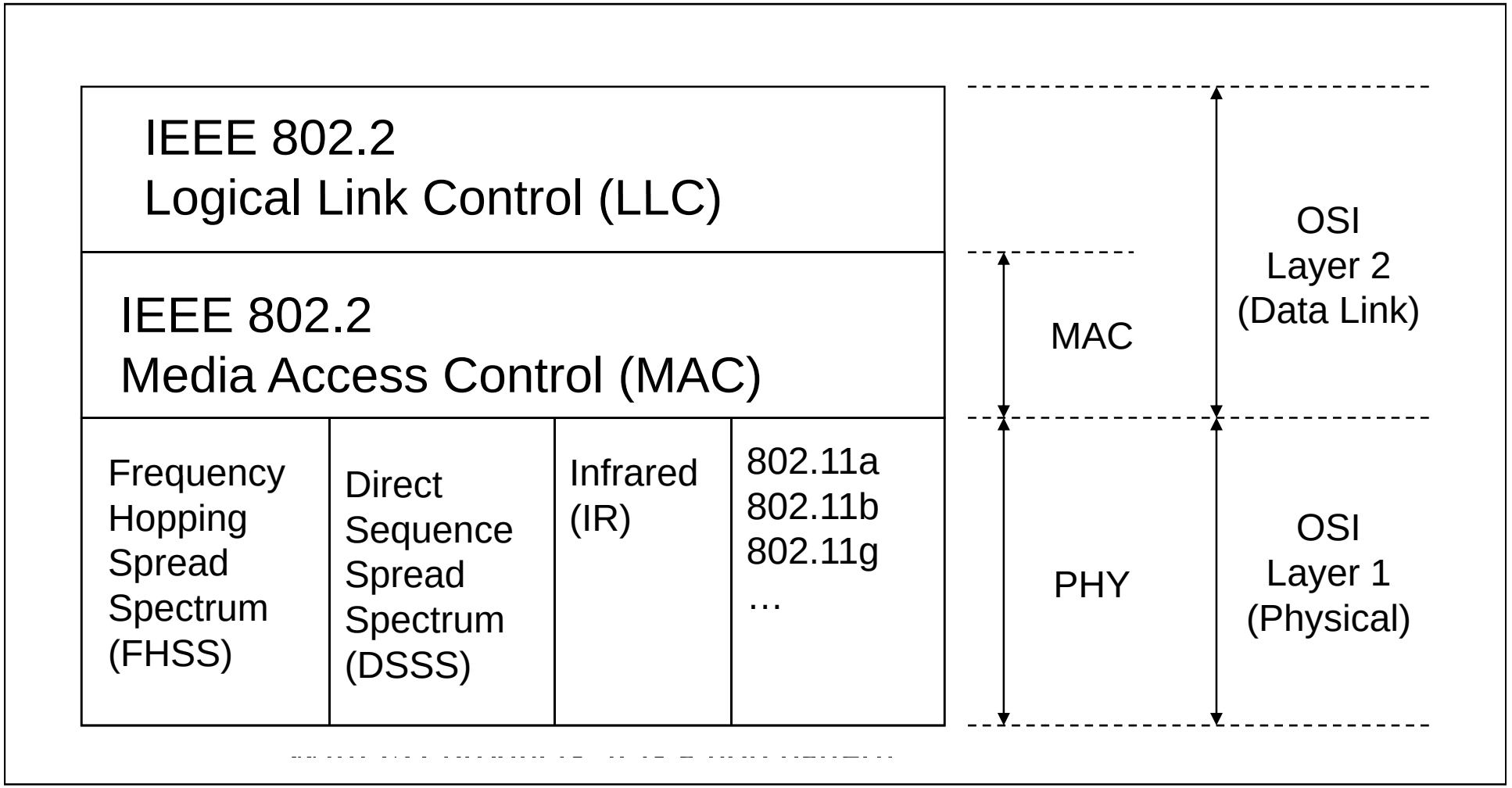
Relationship between management entities and components of 802.11 specification

- MLME: MAC layer management entity
- PLME: PHY layer management entity
- SME: Station management entity
- MIB: Management information base

How to join an existing cell

- Scanning
- Authentication
- Association

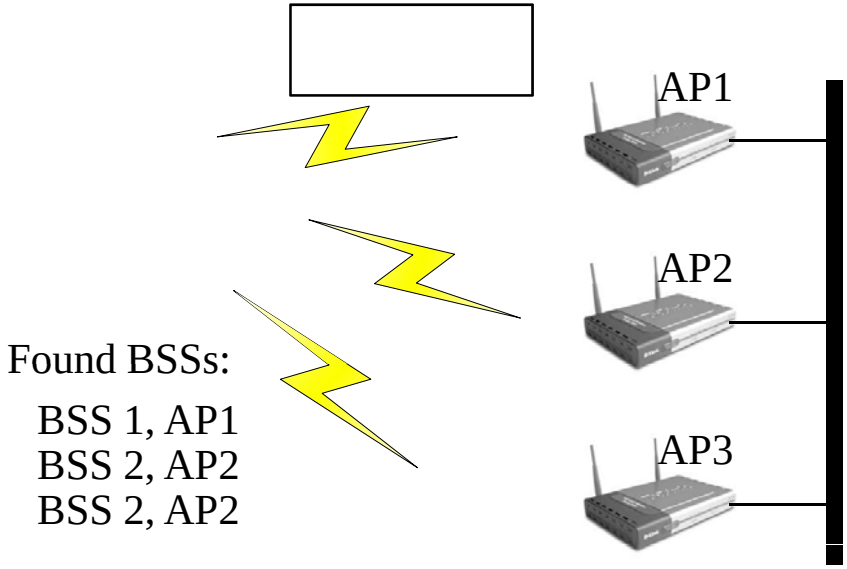
Scanning


IEEE 802.2
Logical Link Control (LLC)
IEEE 802.2
Media Access Control (MAC)
Frequency Hopping Spread Spectrum (FHSS)
Direct Sequence Spread Spectrum (DSSS)
Infrared (IR)
802.11a
802.11b
802.11g
…
MAC
PHY
OSI Layer 2 (Data Link)
OSI Layer 1 (Physical)

- ProbeDelay
- MinChannelTime
  - The minimum time to spend on each channel when scanning.
  - $\geqq$ ProbeDelay
- MaxChannelTime
  - The maximum time to spend on each channel when scanning.
  - $\geqq$ MinChannelTime

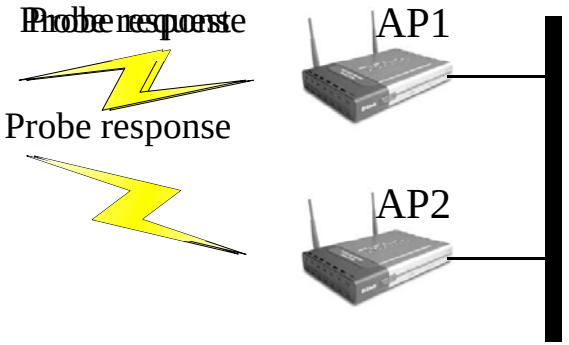
Passive Scanning

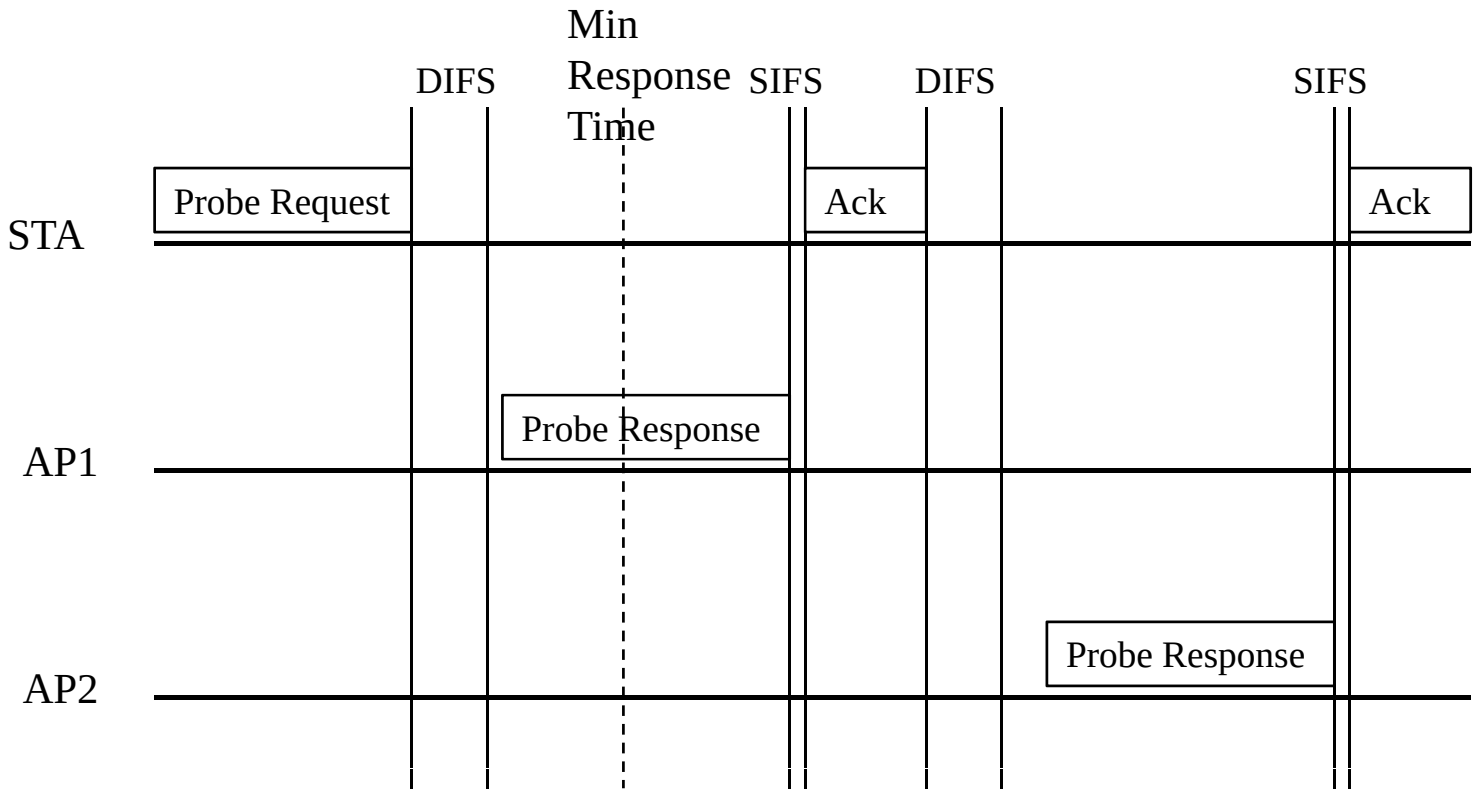
- Passive scanning saves battery power.
- In passive scanning, a station moves to each channel on the channel list and waits for Beacon frames.



Active Scanning

- For each channel to be scanned,
  - Move to the channel and wait for either an indication of incoming frame or for the ProbeDelay timer to expire.
    - If an incoming frame is detected, the channel is in use and can be probed.
    - The timer prevents an empty channel from blocking the entire procedure.
  - Send Prove Request frame.
  - Wait for MinChannelTime and check if channel is busy
    - If idle, there is no network. Move to next channel.
    - If busy, wait until MaxChannelTime and process any Probe Response frames.


Probe response
Probe response
AP1
Probe response
AP2


Min
Response
Time
DIFS
SIFS
DIFS
SIFS
Probe Request
Ack
Ack
STA
Probe Response
AP1
Probe Response
AP2

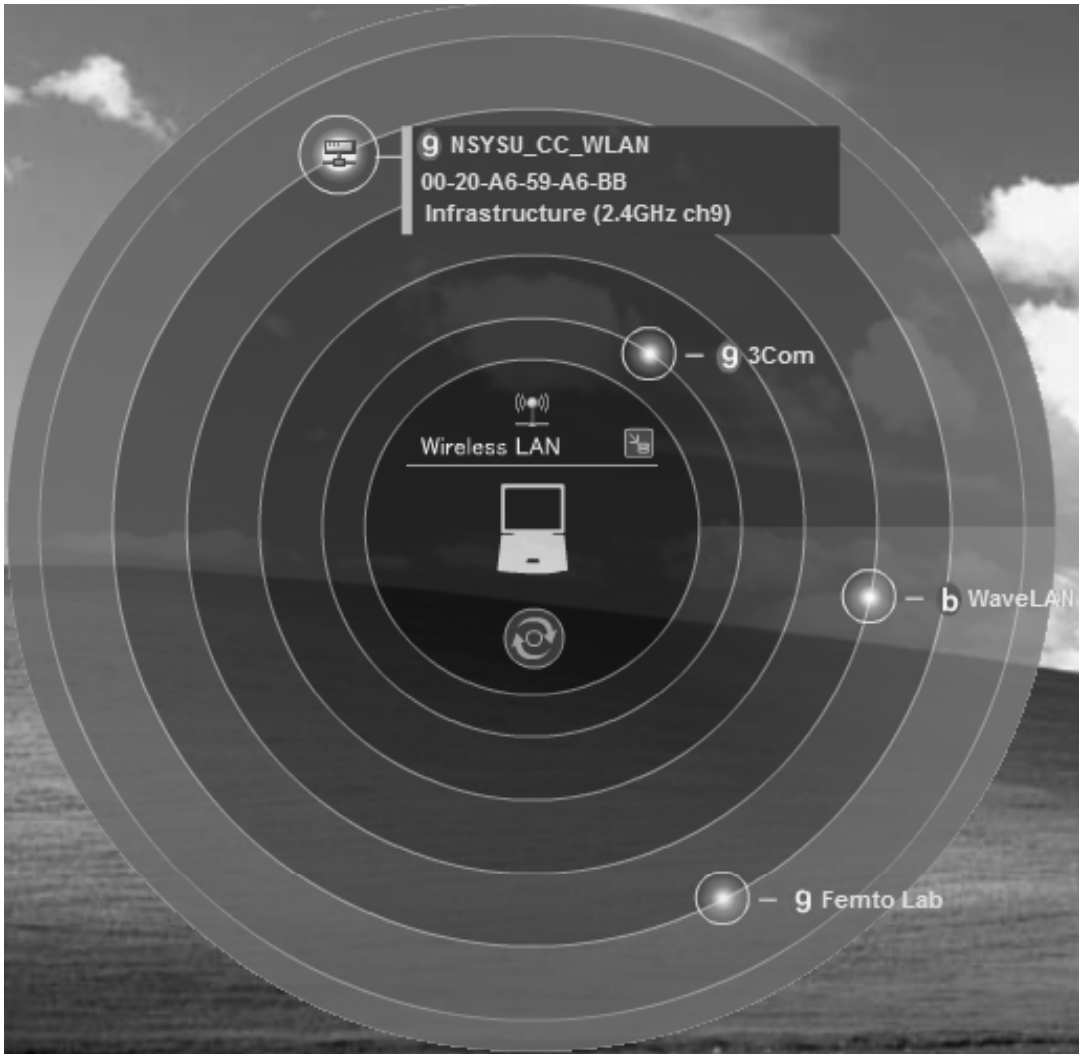
Scan Report

- The report lists all the BSSs that the scan discovered and their parameters.
  - BSSID
  - BSStype
  - SSID
  - Beacon intervals (integer)
  - DTIM period
  - Timing parameters: Timestamp, an offset
  - PHY, CF, IBSS parameters
  - BSSBasicRateSet: Stations must be able to receive data at all the rates listed in the set.

Joining

- After compiling the scan results, a station can elect one of the BSSs to join.
- Choosing which BSS to join is an implementation-specific decision and may even involve user intervention.
  - Common criteria: Power level, signal strength.
- The joining process involves matching local parameters to the parameters required by the selected BSS.
- One of the most important tasks is to synchronize timing information.

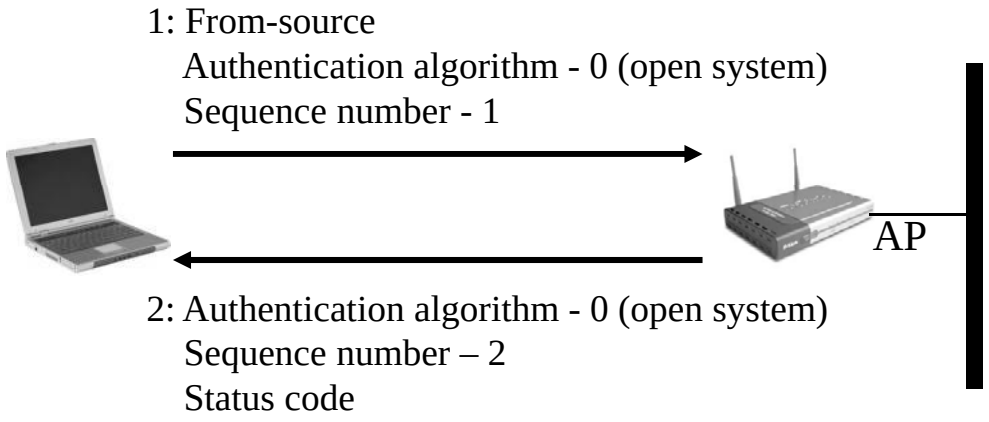

無線網路連線
網路工作
重新整理網路清單
爲住家或小型辦公室設定無線網路
相關的工作
了解有關無線網路
變更喜好網路的順序
變更進階設定
選擇一個無線網路
按下列清單中的一個項目來連線到範圍內的無線網路或取得其他資訊(W)
NSYSU_CC_WLAN
已連線
無安全性的無線網路
WaveLAN Network
自動
無安全性的無線網路
3Com
自動
無安全性的無線網路
連線(C)


g NSYSU_CC_WLAN
00-20-A6-59-A6-BB
Infrastructure (2.4GHz ch9)
g 3Com
Wireless LAN
b WaveLAN
g Femto Lab

Authentication

- Wireless networks are attractive in large part because physical access is not required to use network resources.
- The authentication process only proves the identity of one station (not mutual authentication).
- Network administrators may wish to authenticate mobile stations, but mobile stations can not authenticate the AP.
- One-way street: stations authenticate to network.
- A man-in-the-middle attack: a rogue AP could send Beacon frame to steal Authentication information.
- Two approaches: open-system and shared-key authentication.

Open-system authentication.



Open-system authentication exchange

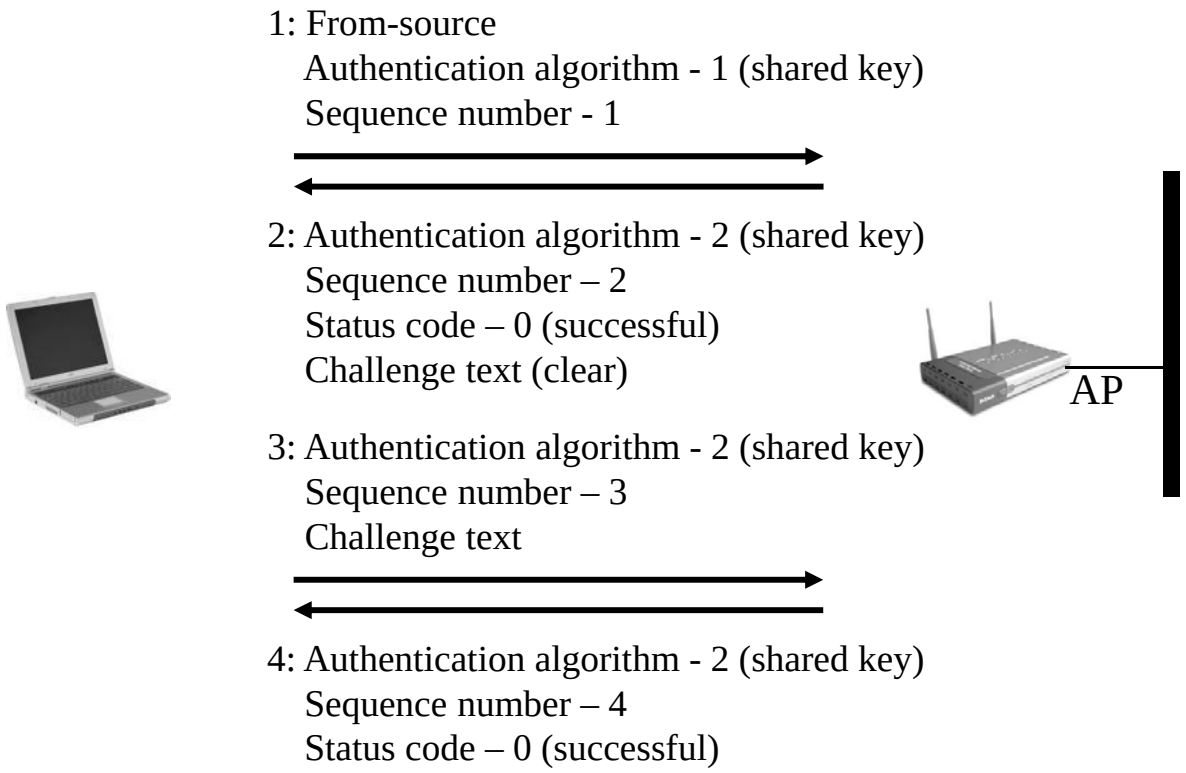
- The identity of any station is its MAC address.


無線 - 介面
SSID：
default
頻道：
Auto
無線模式：
Auto
54g Protection
授權方式：
Open System or Shared Key
WPA加密：
TKIP
WPA金鑰(WPA-PSK)：
WEP加密：
WEP-128bits
None
WEP-64bits
WEP-128bits
通行碼：
WEP金鑰1（10或26十六進位數）：
37DCEEEDD301E3
WEP金鑰2（10或26十六進位數）：
3B5D3C7D207E37DCEEEDD301E3
WEP金鑰3（10或26十六進位數）：
3B5D3C7D207E37DCEEEDD301E3
WEP金鑰4（10或26十六進位數）：
3B5D3C7D207E37DCEEEDD301E3


default 內容
關聯
驗證
連線
網路名稱 (SSID)(N):
default
無線網路金鑰
這個網路需要給下列一個金鑰:
網路驗證(A):
開放系統
資料加密(D):
WEP
網路金鑰(K):
****
確認網路金鑰(O):
****
金鑰索引 (進階)(X):
1
金鑰會自動地提供給我(H)
這是一個電腦對電腦 (臨機操作) 網路; 不使用無線存取點(C)

Shared-key Authentication

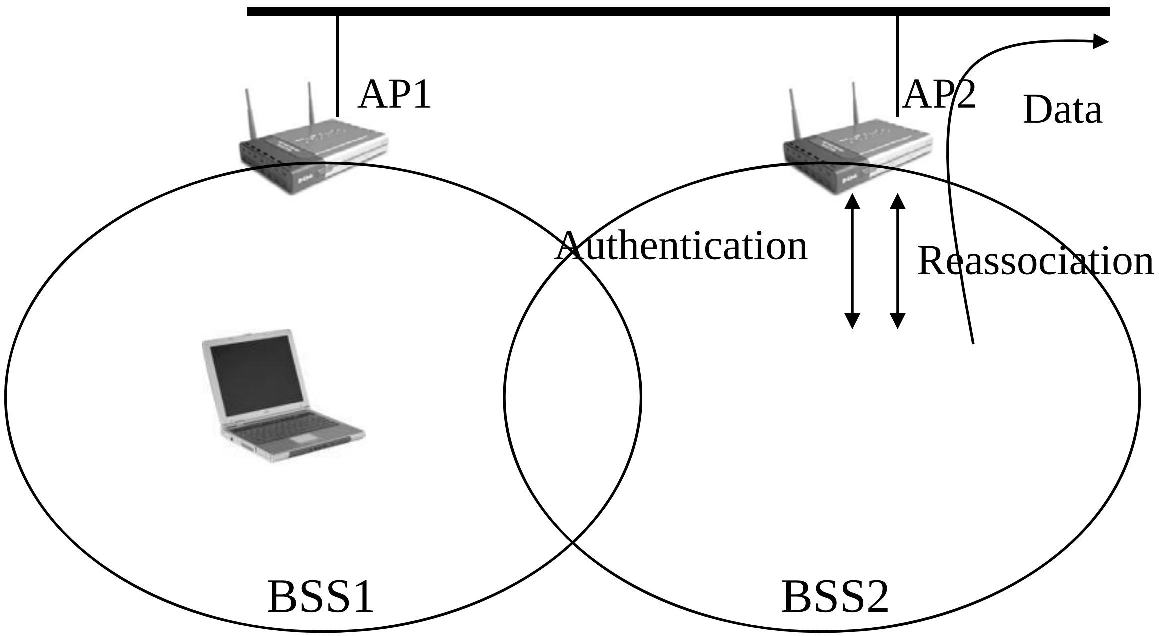
- Shared-key authentication makes use of WEP (Wired Equivalent Privacy).
- It requires that a shared key be distributed to stations before attempting authentication.
- The challenge text is composed of 128 bytes generated using the WEP keystream generator with a random key and IV.



Shared-key authentication exchange

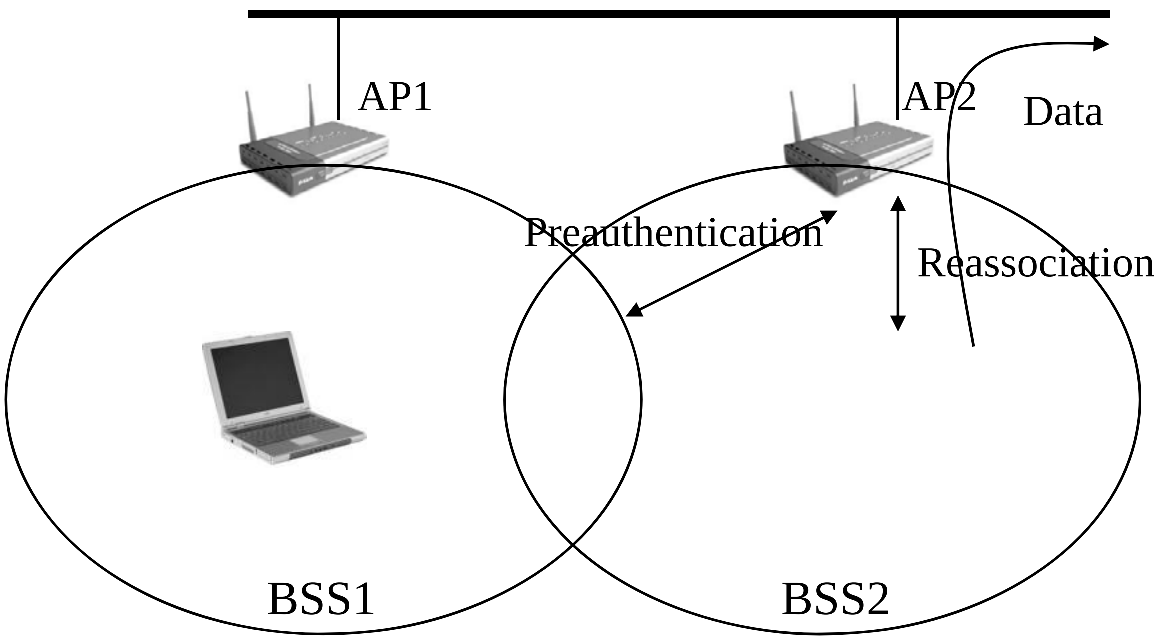
- The challenge text is composed of 128 bytes generated using the WEP keysteam generator with a random key and IV.

Preauthentication



Station begins to get close to the overlap
Between BSS1 and BSS2

AP2's signal is higher, the Station
decides to move and reassociation to AP2



Station [illegible] overlap between BSS1 and BSS2 and detects the presence of AP2

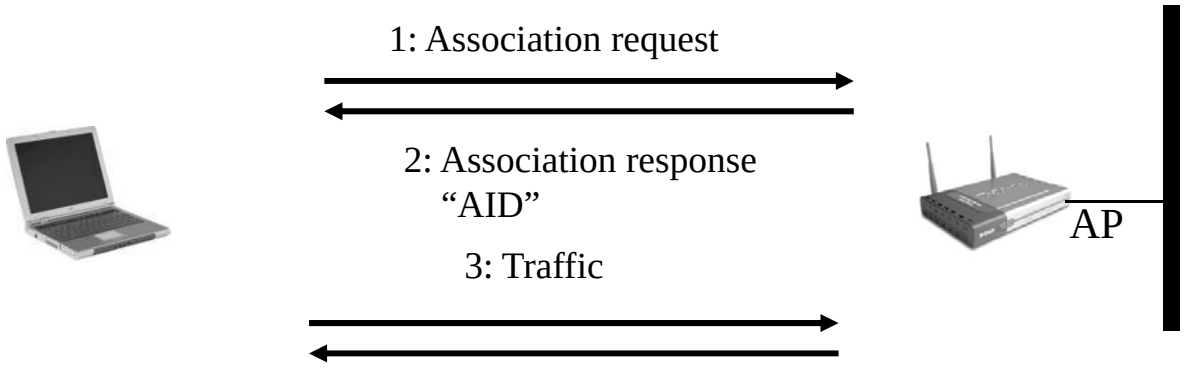
AP2's signal is getting stronger, [illegible]

Decides to move [illegible] reassociation to AP2

Association

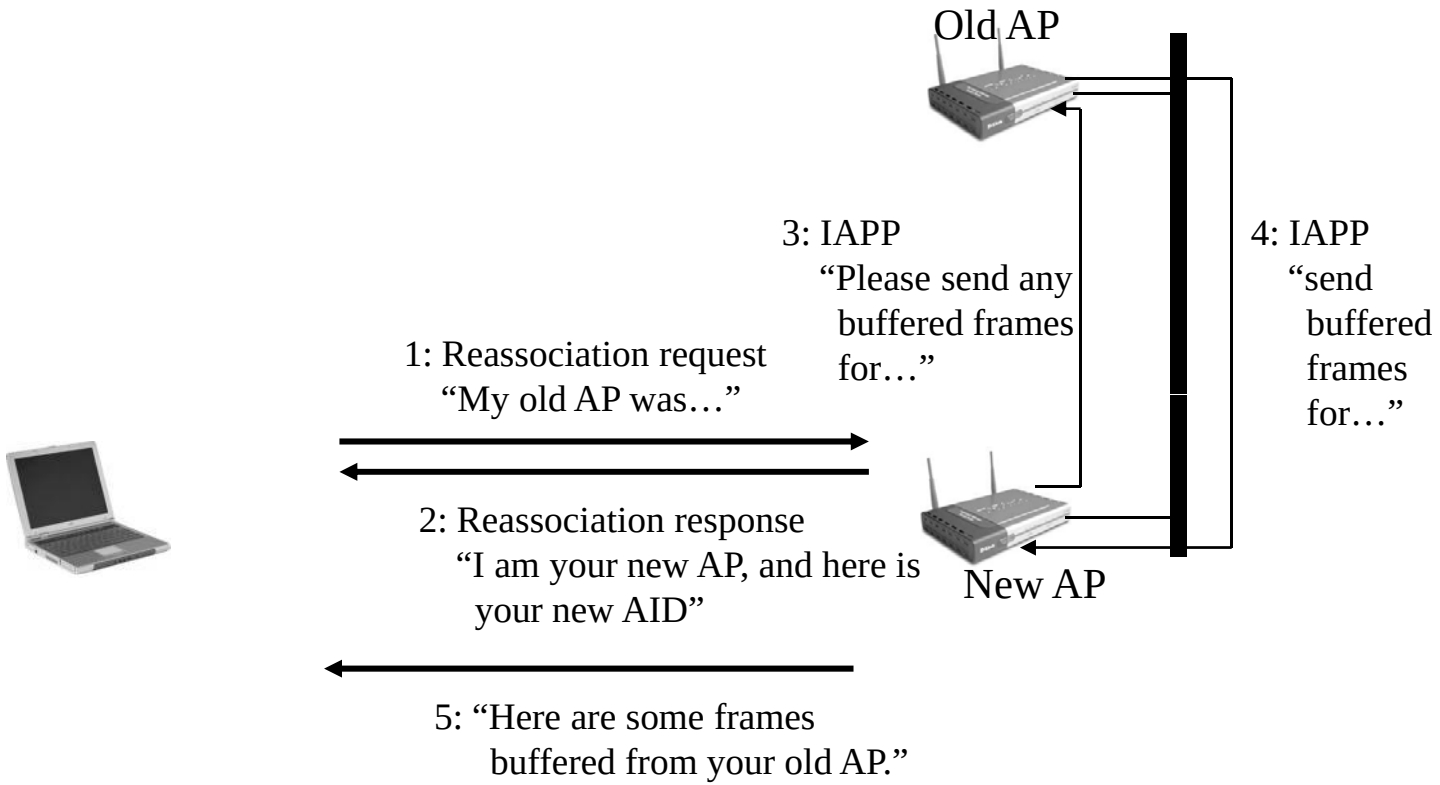
- Association is recordkeeping procedure that allows the distribution system to track the location of each mobile station.
- After association completes, an AP must register the mobile STA on the network so frames for the mobile STA are delivered to the AP.
- One method of registering is to send a gratuitous ARP.
- 802.11 explicitly forbids associating with more than one AP.

Associated procedure

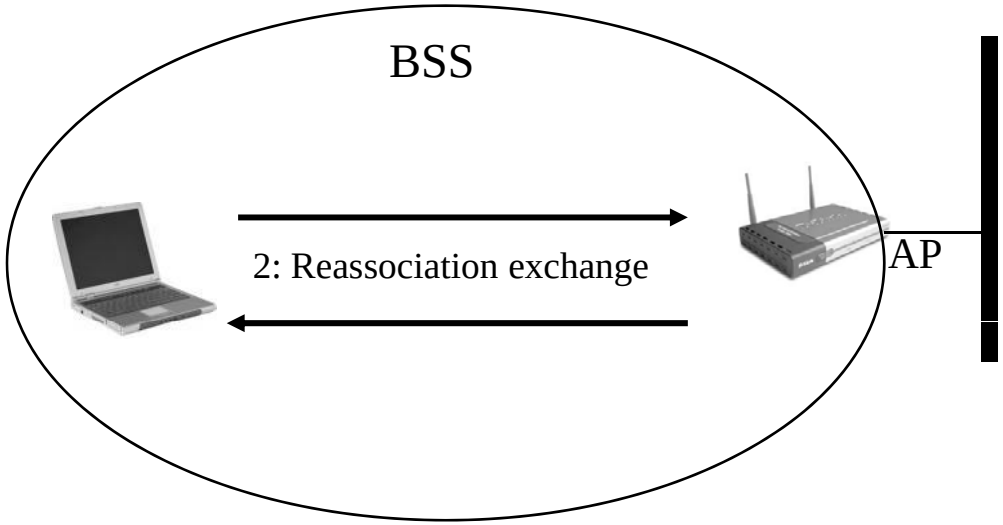


- Association request & reply are unicast frames. (ACK is required)

Reassociated procedure

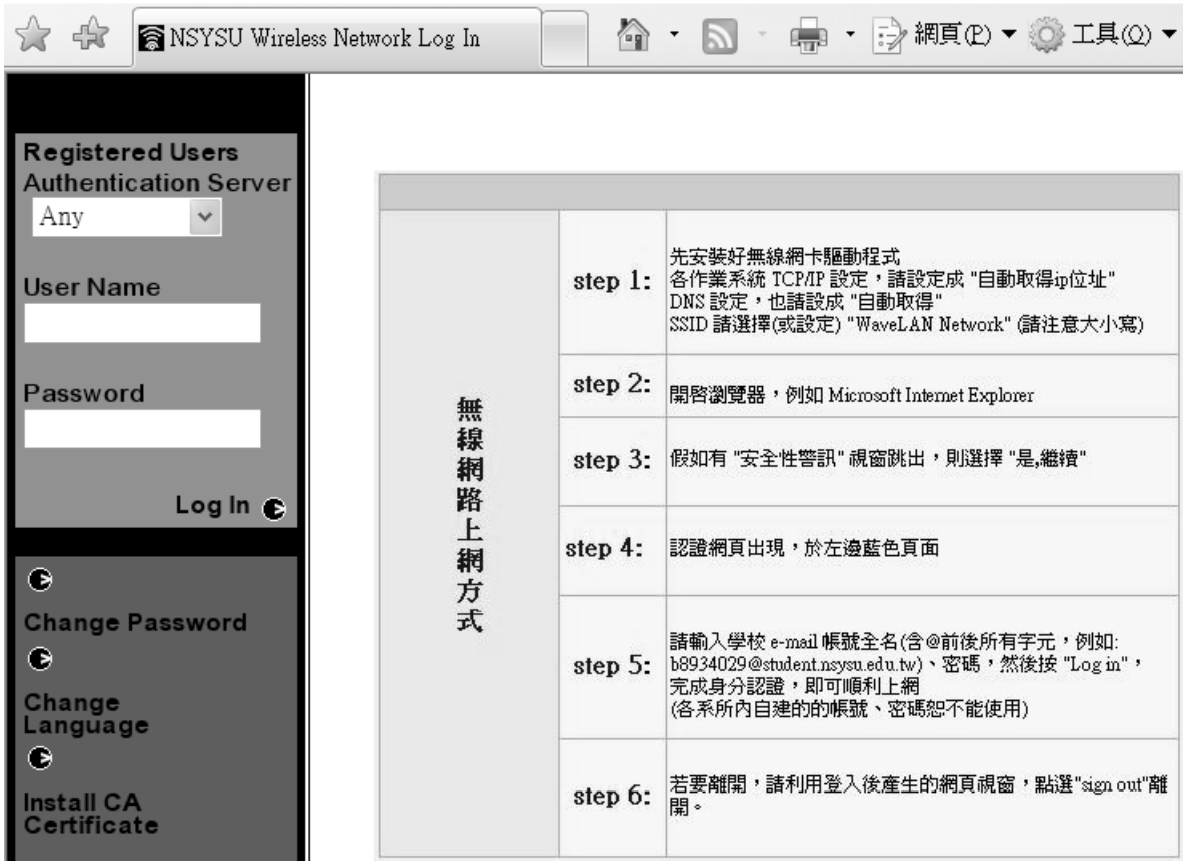


Reassociation with the same AP



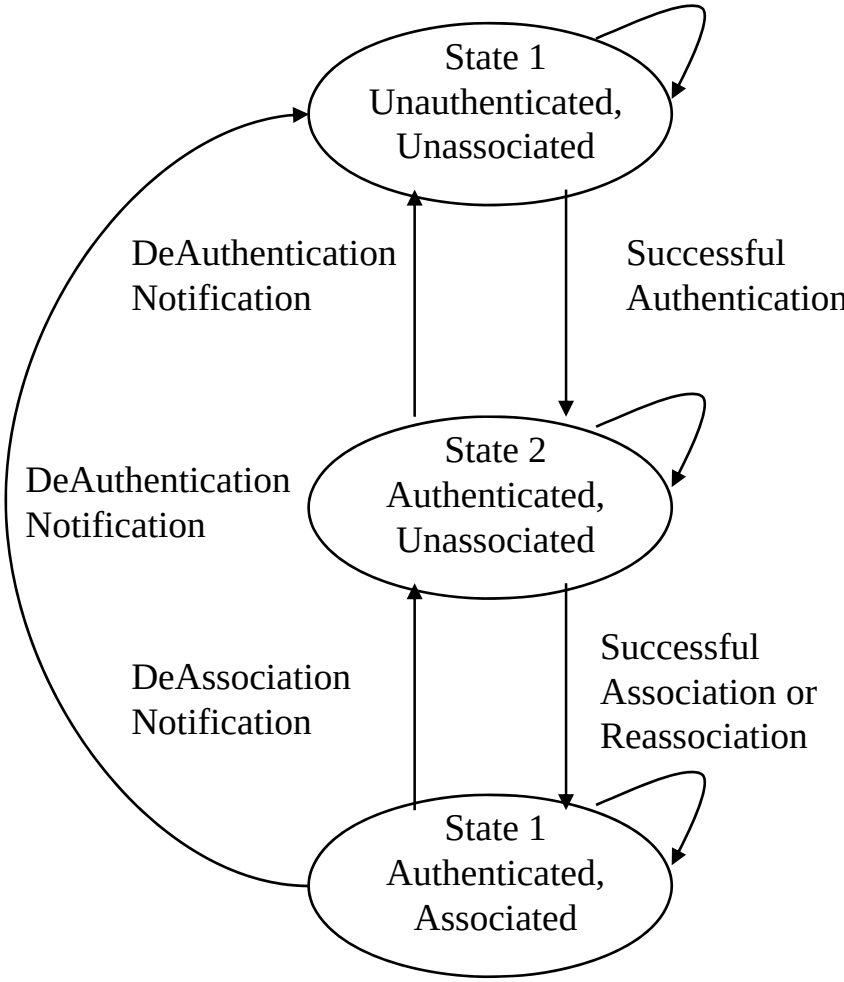
Other Authentication Methods

- RADIUS (Remote Authentication Dial In User Service)
  - Account/Password
- Registration of MAC address of mobile station
- 802.1x (WIRE1x)



無線網路上網方式		
	step 1:	先安裝好無線網卡驅動程式 各作業系統 TCP/IP 設定，請設定成 "自動取得ip位址" DNS 設定，也請設成 "自動取得" SSID 請選擇(或設定) "WaveLAN Network" (請注意大小寫)
	step 2:	開啓瀏覽器，例如 Microsoft Internet Explorer
	step 3:	假如有 "安全性警訊" 視窗跳出，則選擇 "是,繼續"
	step 4:	認證網頁出現，於左邊藍色頁面
	step 5:	請輸入學校 e-mail 帳號全名(含@前後所有字元，例如: b8934029@student.nsysu.edu.tw)、密碼，然後按 "Log in"，完成身分認證，即可順利上網 (各系所內自建的的帳號、密碼恕不能使用)
	step 6:	若要離開，請利用登入後產生的網頁視窗，點選"sign out"離開。

States of Authentication and Association



- Unauthenticated and unassociated
  - The node is disconnected from the network and not associated to an access point.
- Authenticated and unassociated
  - The node has been authenticated on the network but has not yet associated with the access point.
- Authenticated and associated
  - The node is connected to the network and able to transmit and receive data through the access point.

Power Conservation

- Powering down the transceiver can lead to great power savings in wireless networks.
- sleeping, dozing, PS mode vs. awake, active, on
- Power conservation
  - Minimizing the time spent in the awake stage.
  - Maximizing the time in the PS mode.

Power Management in Infrastructure Networks

- In infrastructure networks:
  - APs remain active at all time.
  - APs are aware of the location of mobile STAs.
  - STA can communicate its power management state to its AP.
  - All traffic must go through APs.
    - APs are an ideal location to buffer traffic.
- APs play a key role on power management in infrastructure networks.

Power Management in Infrastructure Networks (cont)

- AP have two power management-related task:
  - Buffering frames
    - AP can determine whether a frame should be delivered to the wireless network.
    - Frames should be buffered if the station is asleep.
  - Periodic announce buffer status
    - AP should periodically announce which stations have frames waiting form them.
    - A station only needs to power up the transmitter to transmit polling frames when there are buffered frames for it.

Power Management in Infrastructure Networks (cont)

- Listen Interval is the number of beacon periods for which the mobile station may choose to sleep.
  - Longer listen intervals require more buffer space on the access point.
- AP must agree to wait for at least the listen interval before discarding frames.
  - If a mobile station fails to check for waiting frames after each listen interval, they may be discarded without notification.

Unicast frame buffering and delivery

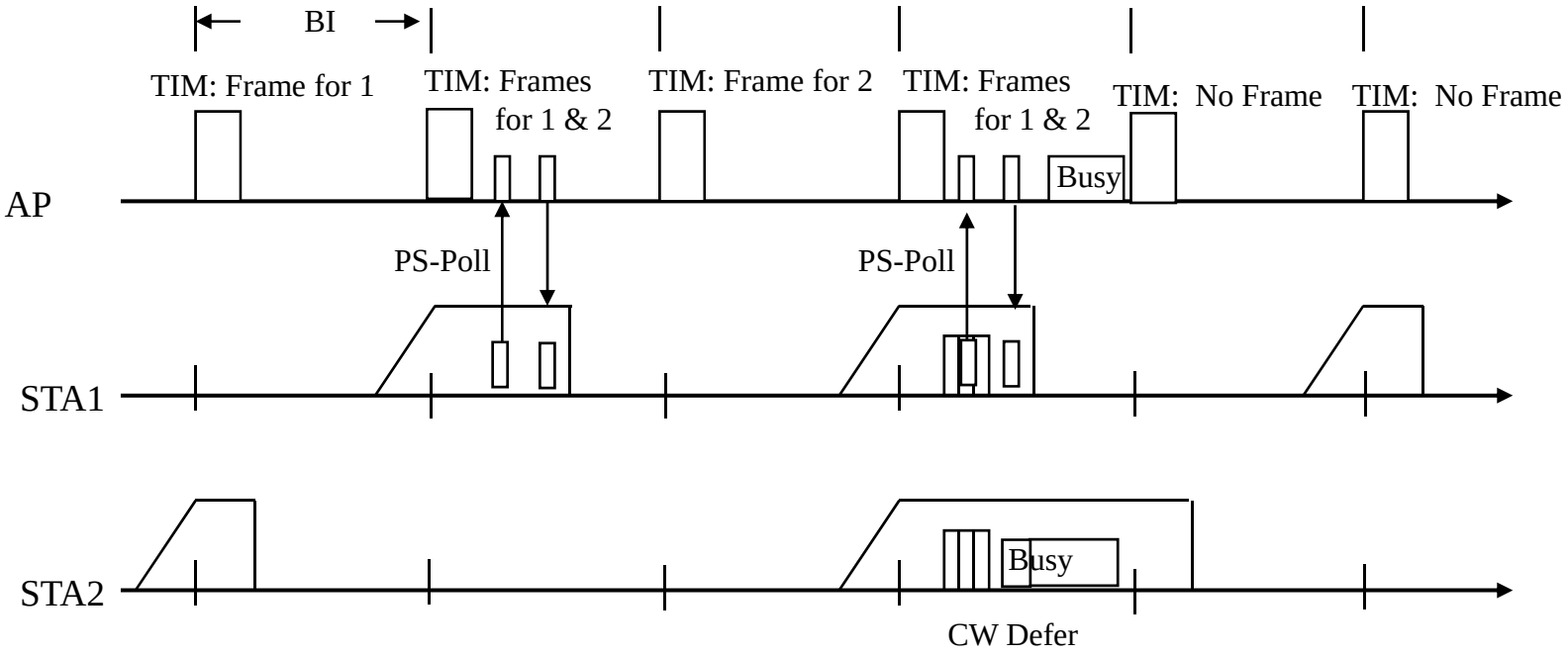
- When frames are buffered, the destination node's AID provides the logic link between the frame and its destination. (Multicast or Broadcast: AID = 0)
- APs assemble a TIM and transmit it in Beacon frames.
- TIM is a virtual bitmap composed of 2008 bits (251 B).
- Offsets are used so only a small portion of the virtual bitmap needs to be transmitted. Each bit corresponds to a particular AID.

Unicast frame buffering and delivery (cont)

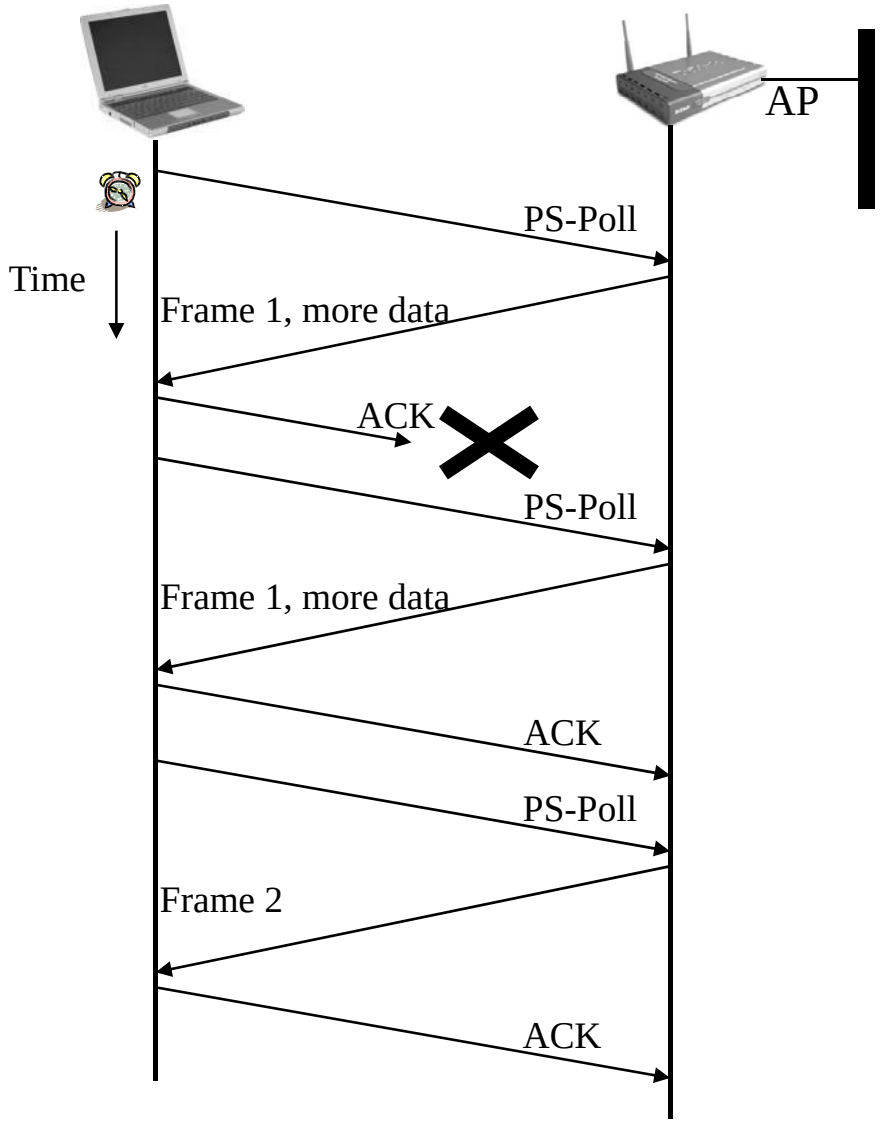
- To retrieve buffered frames, mobile STA use PS-Poll Control frame.
- When multiple stations have buffered frames, all STAs with buffered data must use random backoff algorithm to transmit the PS-poll.
- Each PS-Poll is used to retrieve one buffered frames. ACK is required.

Buffered frame retrieval process

Listen Intervals: 2 for STA1, 3 for STA2



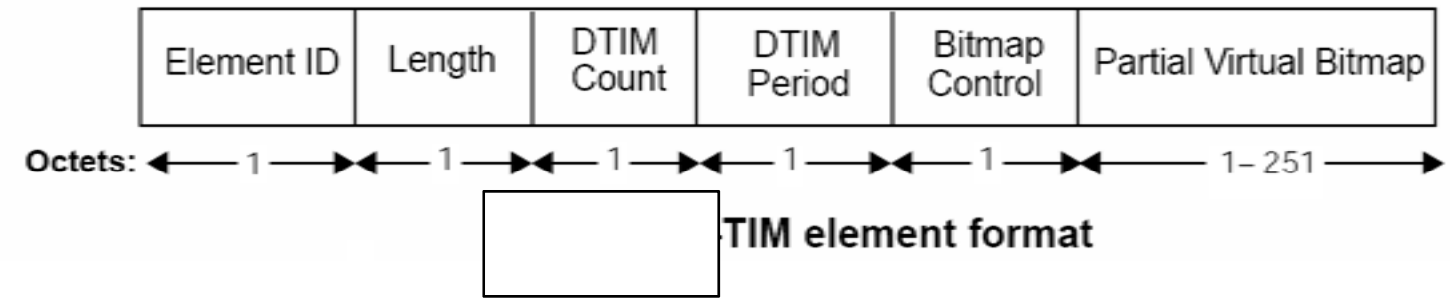
PS-Poll frame retrieval



- STAs may switch from a PS mode to active mode at any time.
- If a STA switches to active mode, frames can be transmitted without waiting for a PS-Poll.
- APs use an aging function to determine when buffered frames are old enough to be discarded.
- Aging function should not discard frames before he listen interval has elapsed.

Delivering multicast and broadcast frame: DTIM

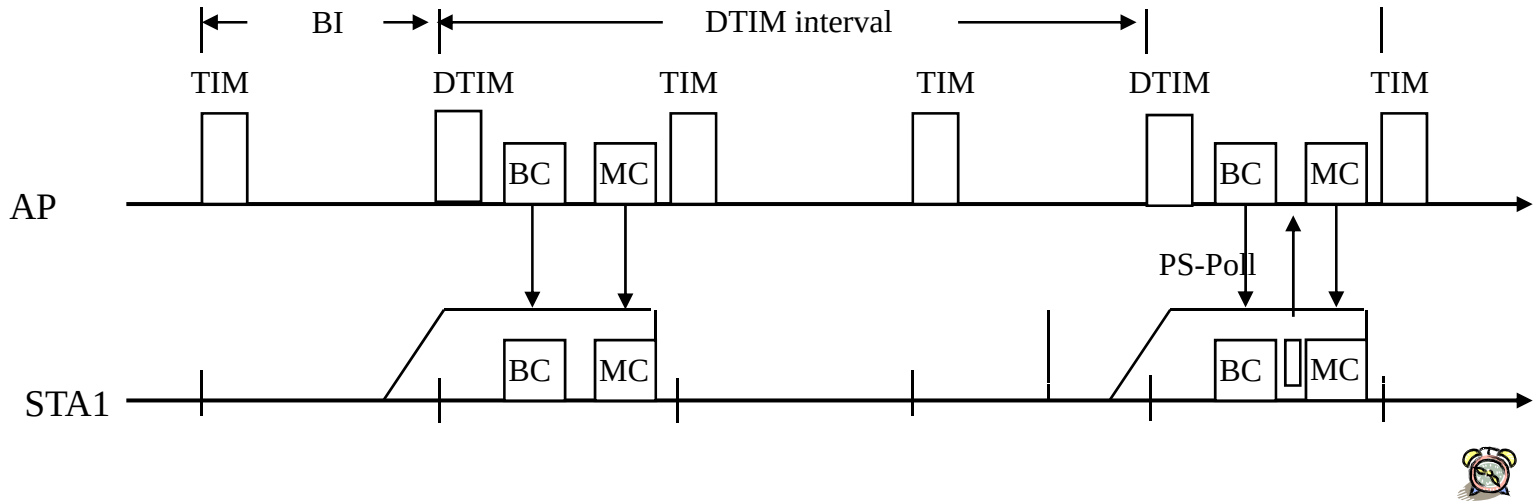
- Buffered broadcast and multicast frames are saved using AID 0.
- DTIM period
- Buffered broadcast and multicast traffic is transmitted after DTIM beacon.
- The AP may choose to defer the processing of incoming PS-Poll frames.



TIM element format

Delivering multicast and broadcast frame: DTIM

Listen Interval: 3 for STA1



Multicast and broadcast buffer transmission after DTIMs.

Timer synchronization

- Wireless network technologies depend a great deal on the distribution of timing information.
- Timing information is especially important in frequency-hopping networks.

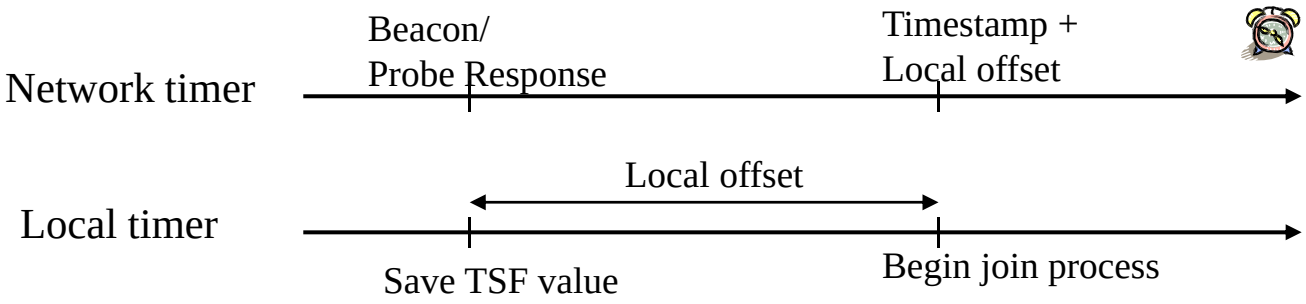
Timer synchronization

- Timing information is especially important in frequency-hopping networks
- Timing synchronization function (TSF) is based on a 1-MHZ clock.

  (one tick = 1 micro sec)

Infrastructure timing synchronization

- APs are responsible for maintaining the TSF time, and any STAs associated with an AP must simply accept the AP's TSF as valid.
  - Associated STAs maintain local TSF so that they can still remain roughly synchronized with the global TSF when missing a Beacon frame.



Matching the local timer to a network timer

Competing technologies

- Bluetooth

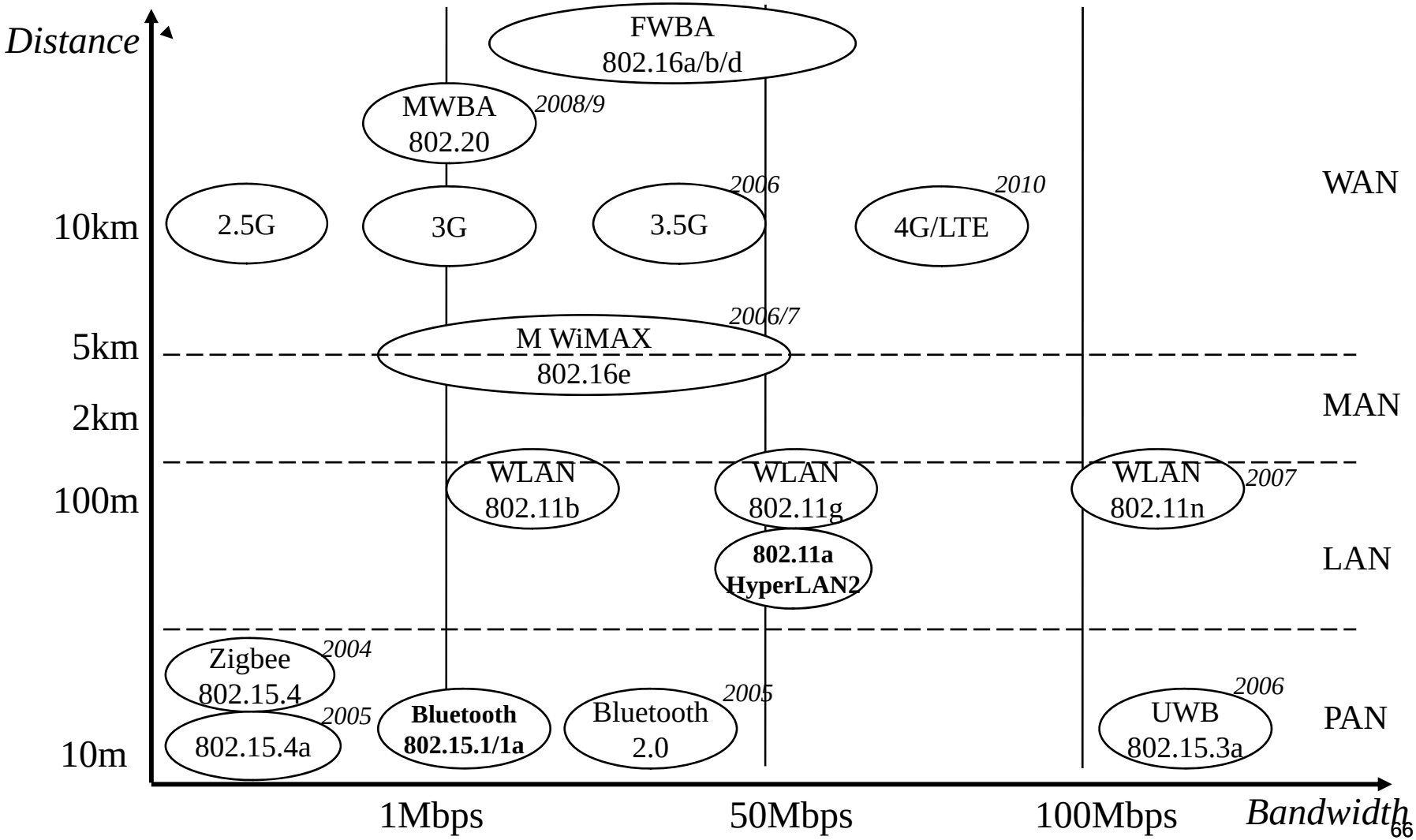
Version	Data Rate
Version 1	1 Mbps
Version 2.0 + EDR	3 Mbps
WiMedia Alliance (3.0?)	53 ~ 480 Mbps

- ZigBee
  - IEEE 802.15.4
  - operation in the unlicensed 2.4 GHz, 915 MHz and 868 MHz ISM bands
  - 250kbps

Competing technologies

- UWB
  - FCC authorizes the unlicensed use of UWB in 3.1–10.6 GHz.
  - 100 Mbps ~ 400 Mbps
- HomeRF
  - 2.4 GHz, WBFH (Wide band frequency hopping)
  - 10 Mbps, 150 ft.
- 3GPP
  - The 3rd Generation Partnership Project
  - 3.9G (HSDPA – 3.5G)
  - 100Mbps
- WiMAX

Road Map of Wireless Communication



- References
  - IEEE 802.11 standard
  - 802.11 Wireless Networks The Definitive Guide, Oreilly
  - Demystifying MIMO and 802.11n, Peter Reinders, Bluesocket, Inc
  - 802.11n: Next-Generation Wireless LAN Technology, Broadcom
  - 802.11 Technologies: Past, Present and Future, TROPOS networks