Part I Syllabus

Week	Subject
Week 1 Week 2 Week 3	Introduction
	Network layers & physical resilience
	Data link layer – Flow control
	Data link layer – Error control
	Local area network – Introduction
Week 4 Week 6 Week 7 * No lecture in Week 5 due to Students' Union Day	Local area network – Medium access control
	Local area network – Wired
	Local area network – WLAN
	Mobile access networks: From 1G to 5G
	Network paradigms
Recess Week (e-learning)	Review and examples

What is the problem with the guy?

CE3005/CZ3006 Computer Networks

Lecture 8
Wireless LAN: IEEE 802.11

NANYANG TECHNOLOGICAL UNIVERSITY

Contents

- **WLAN Overview**
  - WLAN Standard
  - WLAN Architecture
  - WLAN Protocol Stack
- **802.11 Physical Layer**
- **802.11 MAC Layer**
  - Hidden and Exposed Terminal Problems
  - CSMA/CA Protocol
  - MAC Management
- **Multi-Access Reservation Protocol**
  - Scheme
  - Throughput Calculation

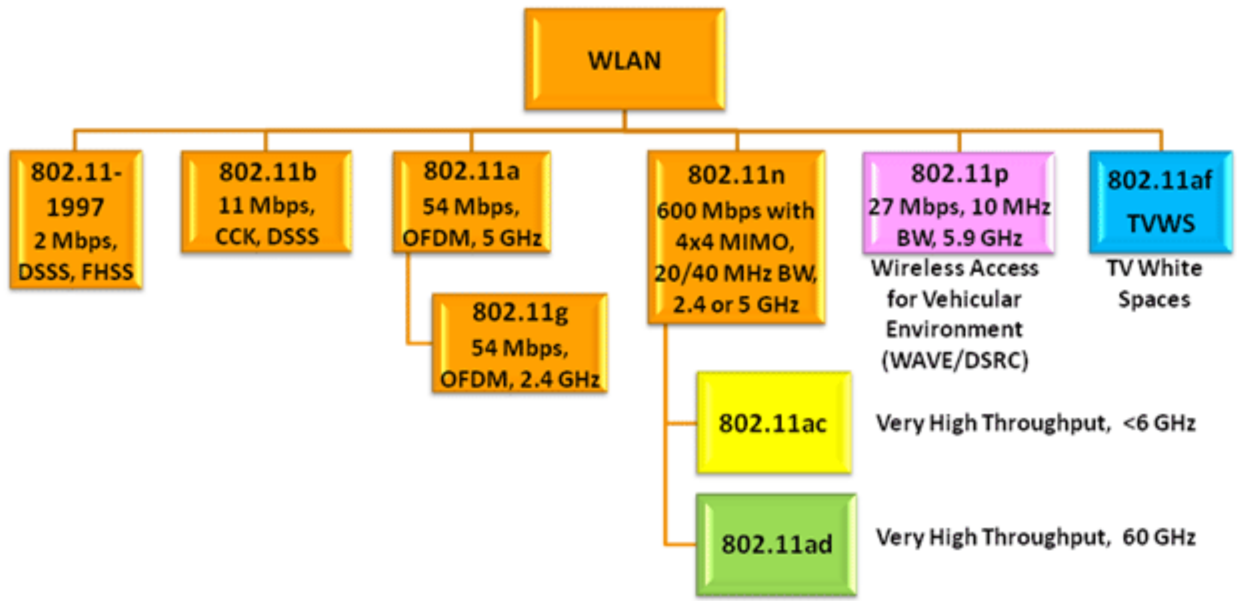
WLAN Overview

LAN/WLAN World

- **LANs provide connectivity for interconnecting computing resources at local levels of an organization**
- **Wired LANs**
  - Limitations because of physical, hard-wired infrastructure
- **Wireless LANs**
  - Flexibility
  - Portability
  - Mobility
  - Ease of Installation

IEEE 802.11 WLAN Standard

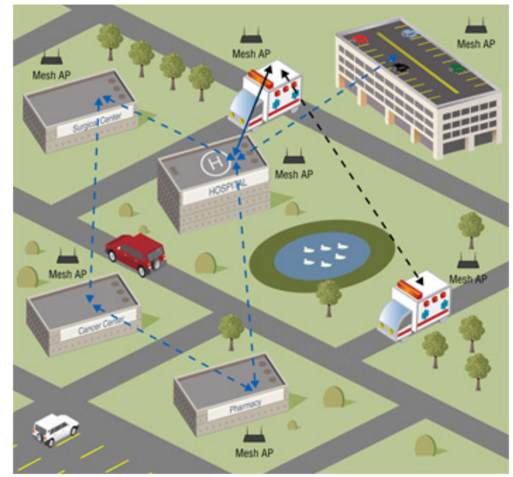
- In response to lacking standards, IEEE developed the first internationally recognized wireless LAN standard – IEEE 802.11
- IEEE published 802.11 in 1997, after seven years of work
- Most prominent specification for WLANs
- Scope of IEEE 802.11 is limited to Physical and Data Link Layers



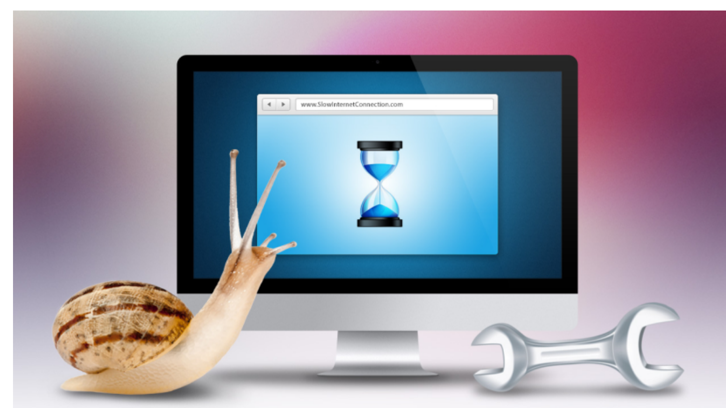
DSRC = Dedicated Short-Range Communications

Wireless LANs: Characteristics

- **Advantages**
  - Flexible deployment
  - Minimal wiring difficulties
  - More robust against disasters (earthquake, etc)
  - Historic buildings, conferences, trade shows,…

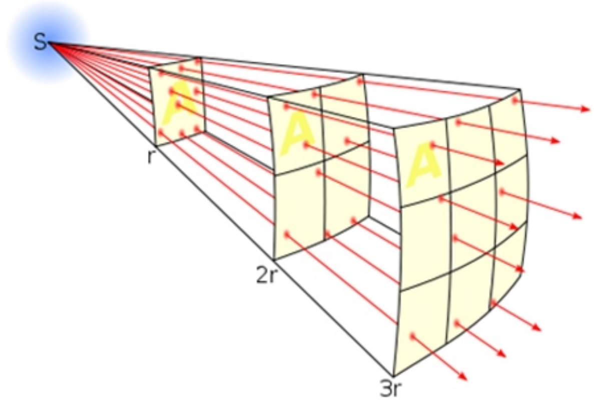


- **Disadvantages**
  - Low bandwidth compared to wired networks (1-10 Mbit/s)
  - Proprietary solutions
  - Need to follow wireless spectrum regulations



Wireless Link Characteristics

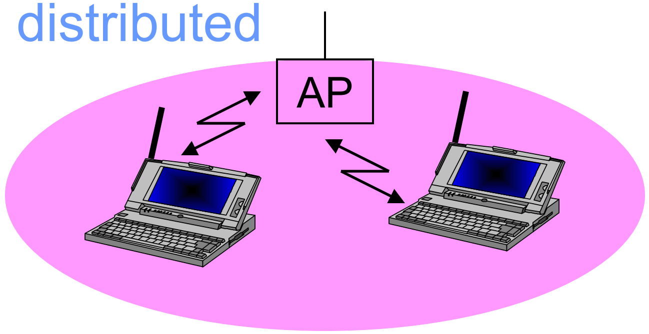
- **Different from wired link …**
  - Decreased signal strength: radio signal attenuates as it propagates through air (path loss)
  - Interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone)
  - Multipath propagation: radio signal reflects off objects ground, arriving at destination at slightly different times



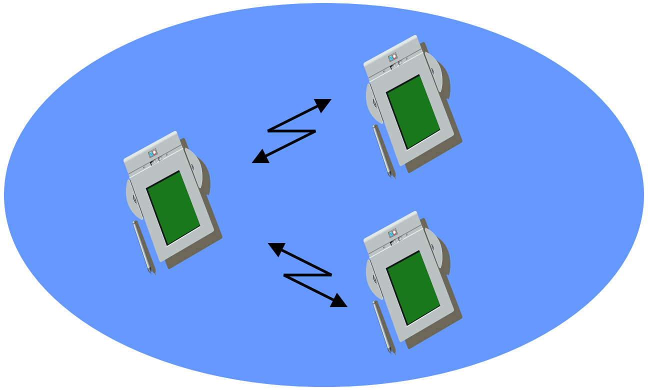
… make communications over wireless link much more "difficult"

WLAN Architecture

- **Building Modules**
  - Station (STA)
    - Mobile node
    - Smartphone, pad, laptop
  - Access Point (AP)
    - Stations are connected to access points.
- **Two Architectural Modes**
  - Infrastructure: centralized
  - Ad Hoc: distributed



Infrastructure

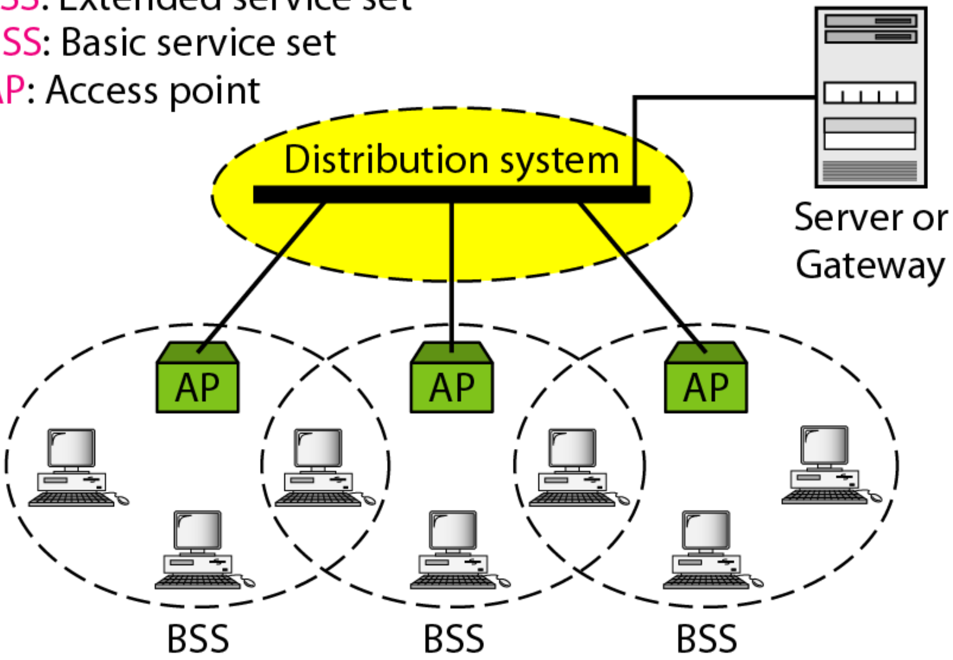


Ad Hoc

(Extended) Service Set

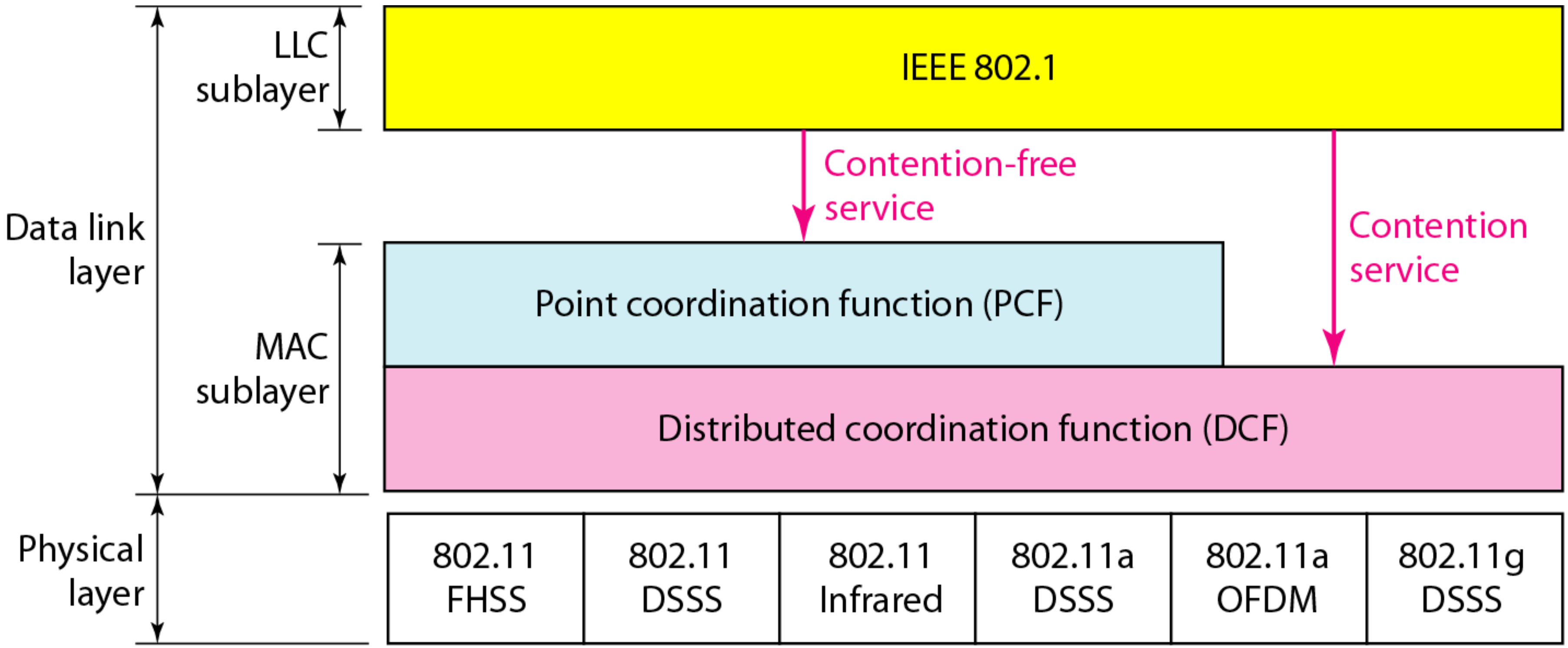
- **Basic Service Set (BSS)**
  - Stations and the AP within the same radio coverage form a BSS.
- **Extended Service Set (ESS)**
  - Several BSSs connected through APs form an ESS.

ESS: Extended service set
BSS: Basic service set
AP: Access point



NANYANG TECHNOLOGICAL UNIVERSITY

802.11 Protocol Stack

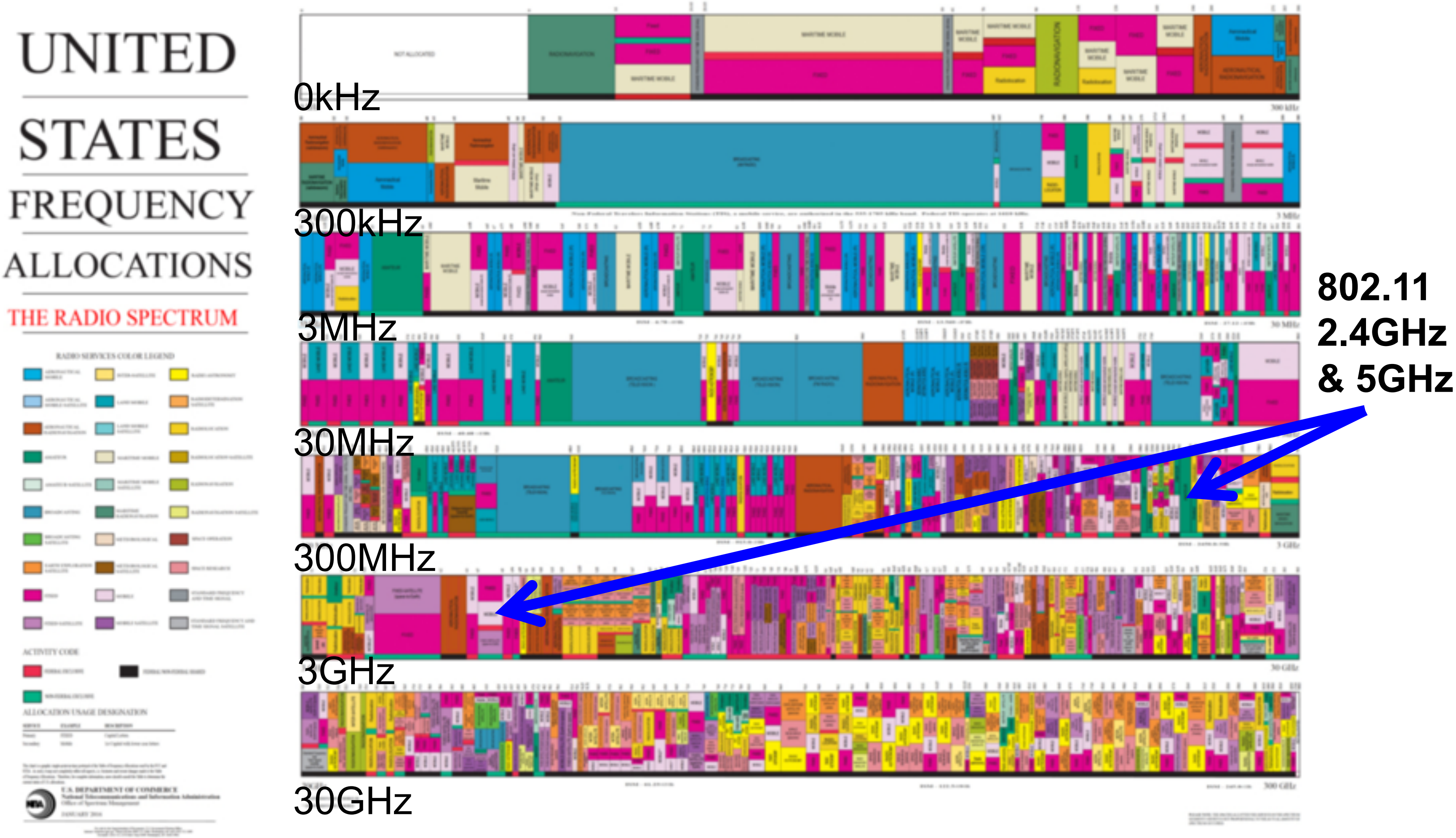


Wireless Physical Layer

Radio Spectrum

- **Radio frequency bands are allocated to different applications**
  - The use of most frequency bands needs licenses
  - IEEE 802.11 uses industrial, scientific and medical (ISM) bands that don’t require licenses if the radio transmissions follow the national/global regulations

Sub-THz Radio Spectrum



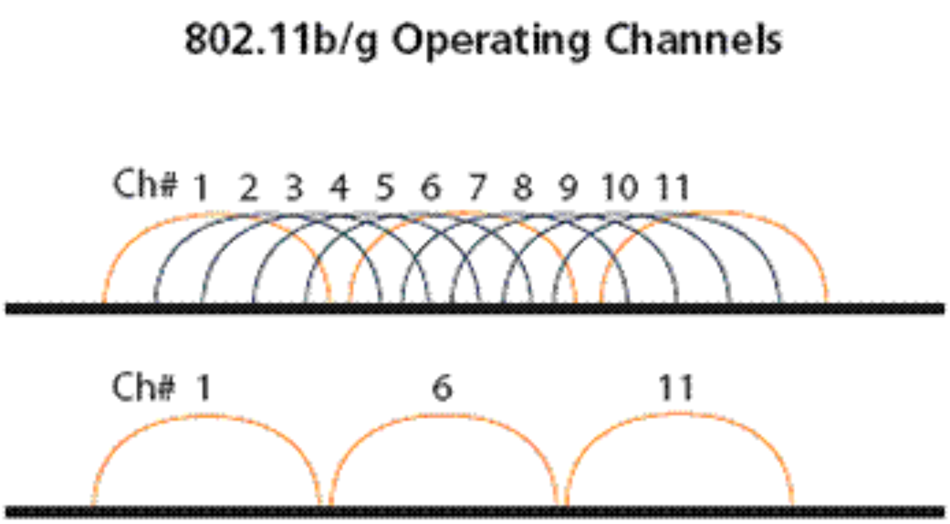
NANYANG TECHNOLOGICAL UNIVERSITY

IEEE 802.11 Physical Layer

	802.11b	802.11g	802.11a	802.11n	
Frequency Band	2.4GHz	5GHz	2.4GHz	2.4	5
Non-overlapping Channels	3	3	12	3	12
Baseline BW Per Channel	11Mbps	54Mbps	54Mbps	65	65
Max BW Per Channel	11Mbps	54Mbps	54Mbps	**130**	**270**
MIMO	1	1	1	4	4
Modulation	DSSS	DSSS/OFDM	OFDM	OFDM	

IEEE 802.11 Channels, Association

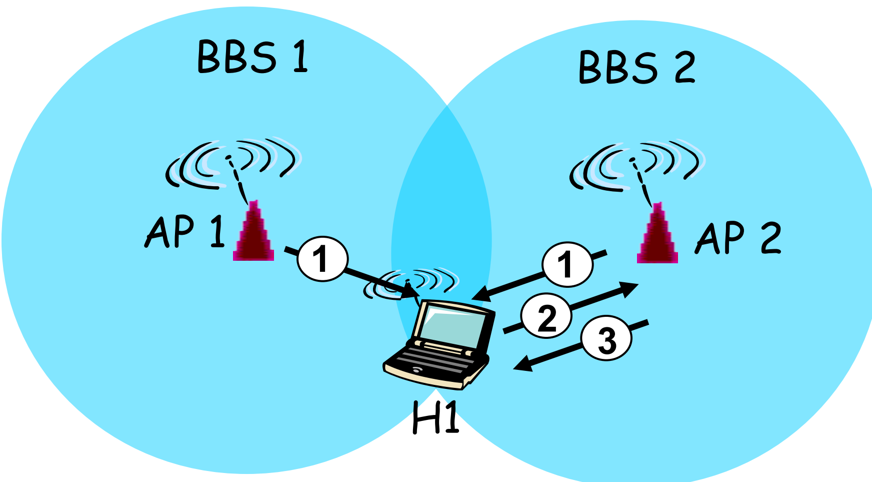
- **802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies**
  - AP admin chooses frequency for AP
  - Interference possible: channel can be same as that chosen by neighboring AP!

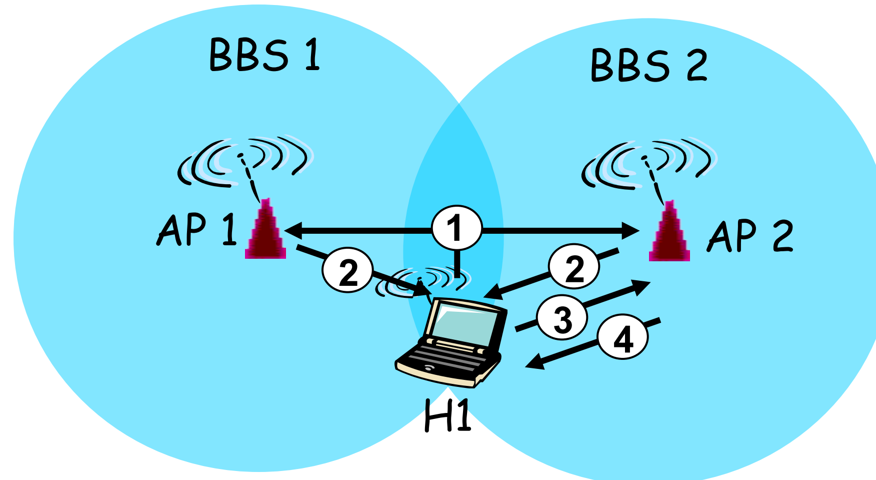


IEEE 802.11 Channels, Association

- **802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies**
  - AP admin chooses frequency for AP
  - Interference possible: channel can be same as that chosen by neighboring AP!
- **Host: must associate with an AP**
  - Scans channels, listening for beacon frames containing AP's name (SSID) and MAC address
  - Selects AP to associate with
  - May perform authentication (security purpose)
  - Will 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: Selected AP to H1

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: selected AP to H1

NANYANG TECHNOLOGICAL UNIVERSITY

802.11 MAC

802.11 MAC Sublayer

- **New challenges caused by the nature of wireless communications**
  - Broadcast
  - Signal attenuation
  - Pervasive electromagnetic noise
- **Three functional areas**
  - Access control (random access vs controlled access)
  - Reliable data delivery (against noises and collisions)
  - Security (authentication, packet injection, …)
- **Two additional problems:**
  - Hidden Terminal Problem
  - Exposed Terminal Problem

Access Control

- **Distributed Coordination Function (DCF)**
  - Distributed access protocol
  - Contention-based
  - Makes use of CSMA/CA
  - Suited for ad-hoc network and asynchronous traffic
- **Point Coordination Function (PCF)**
  - Alternative access method on top of DCF
  - Centralized access protocol
  - Contention-free, and works like polling
  - Suited for time-bound services like voice and multimedia

Reliable Data Delivery

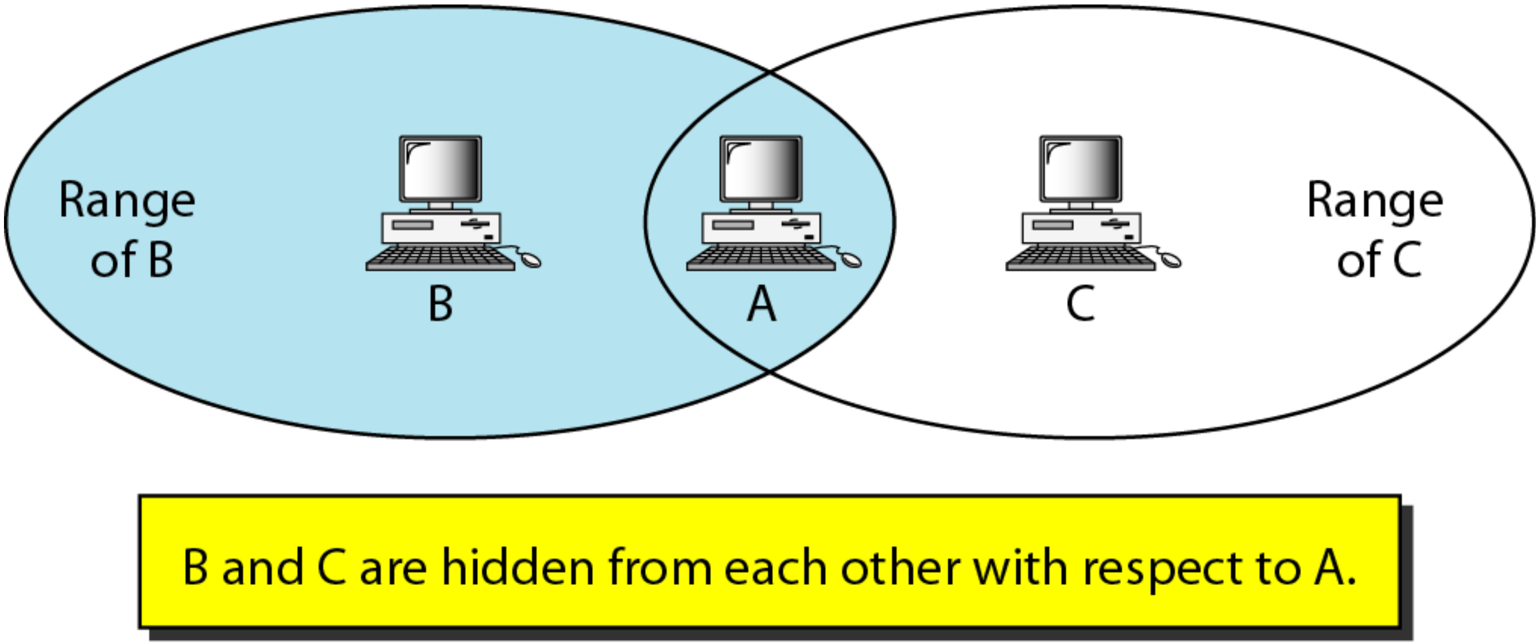
- **Loss of frames due to noise, interference and propagation effects**
- **Frame exchange protocol**
  - Sender broadcasts data
  - Receiver responds with acknowledgement (ACK)
  - If sender does not receive ACK, it retransmits frame
- **Four frame exchange for enhanced reliability**
  - Sender issues request-to-send (RTS)
  - Receiver responds with clear-to-send (CTS)
  - Sender transmits data
  - Receiver responds with ACK

802.11 Multi-Access

- **Collision**
  - A receiver hears transmissions from 2$^+$ nodes at the same time
- **802.11: CSMA - sense before transmitting**
  - Don't collide with ongoing transmission by other node
- **802.11: *no* collision detection!**
  - Difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - Can't sense all carriers & collisions in any case: hidden terminal problem
- **802.11: avoid collisions**
  - CSMA/C(ollision)A(voidance)

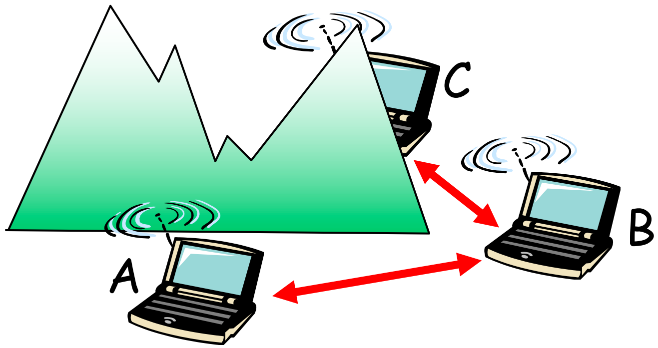
Hidden Terminal Problem

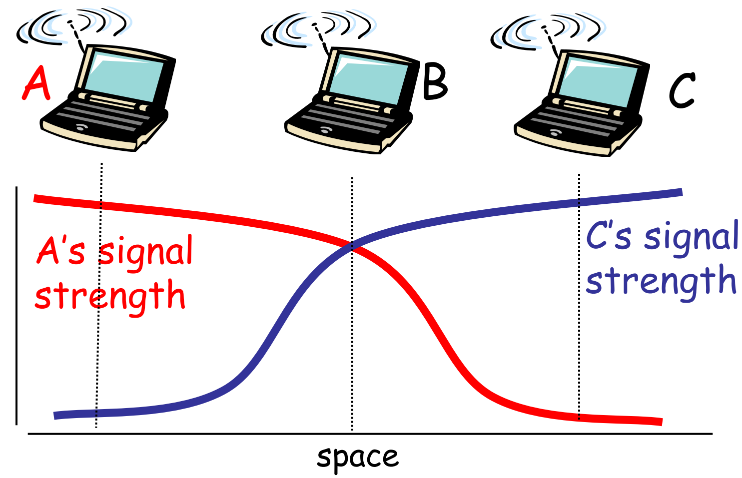
- **Signal decay causes collision**



Simultaneous transmissions from B, C to A will collide.
But, both B and C are unaware of the collision,
because they cannot hear each other!

Examples of Hidden Terminals





Caused by barrier

- B, A hear each other
- B, C hear each other
- A, C can not hear each other
  - A, C unaware of their interference at B
  - A is a hidden terminal to C, vice versa

Caused by signal attenuation

- B, A hear each other
- B, C hear each other
- A, C can not hear each other
  - A, C unaware of their interference at B

Q: Does Ethernet have hidden terminal problem?

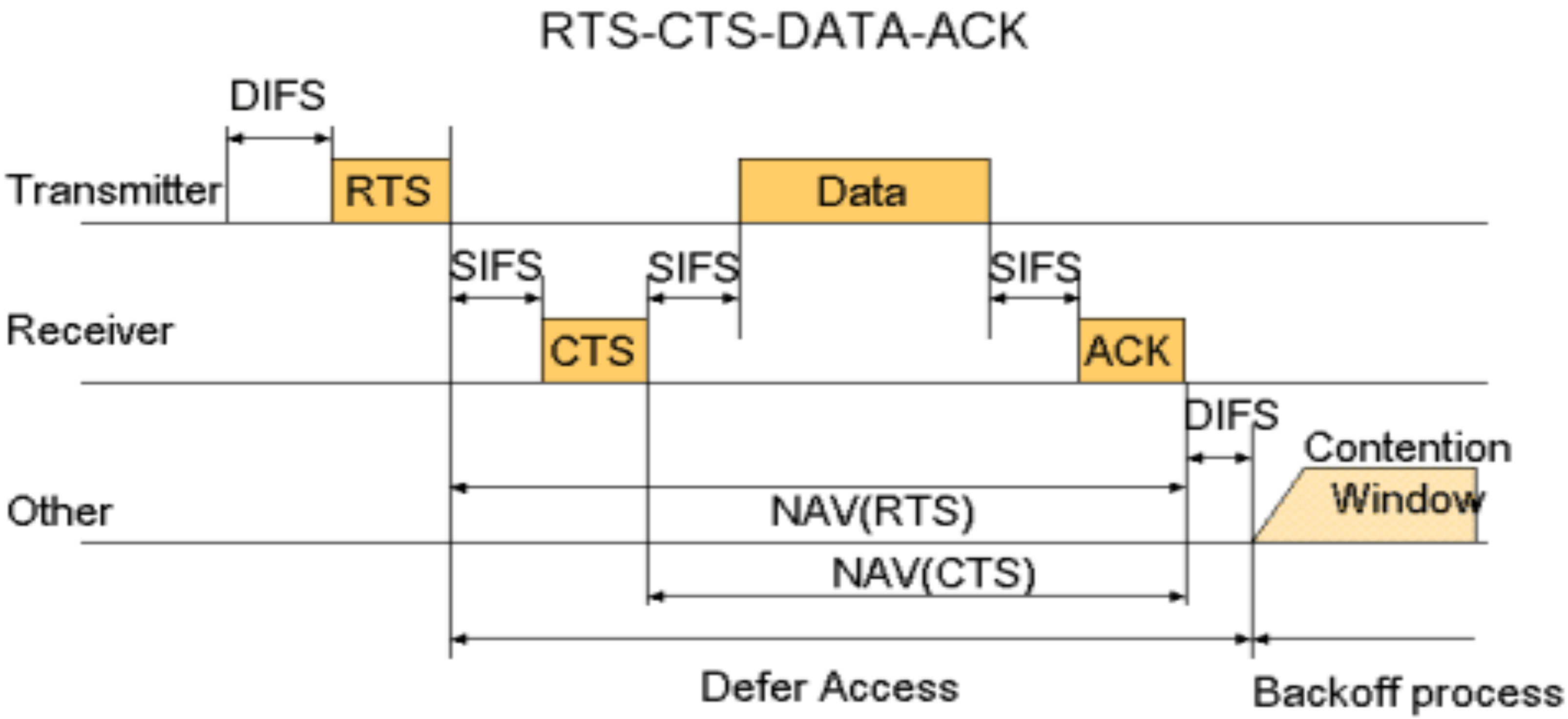
Collision Avoidance

idea: **Sender to "reserve" channel for a long data frame**

- **Sender first transmits a *small* request-to-send (RTS) packet to receiver using CSMA**
  - RTSs may still collide with each other, or an RTS may collide with an ongoing data frame
  - but they're short
- **Receiver broadcasts clear-to-send (CTS) in response to RTS**
- **CTS heard by all nodes**
  - Sender transmits data frame
  - Other stations defer transmissions

Avoid data frame collisions completely using small reservation packets!

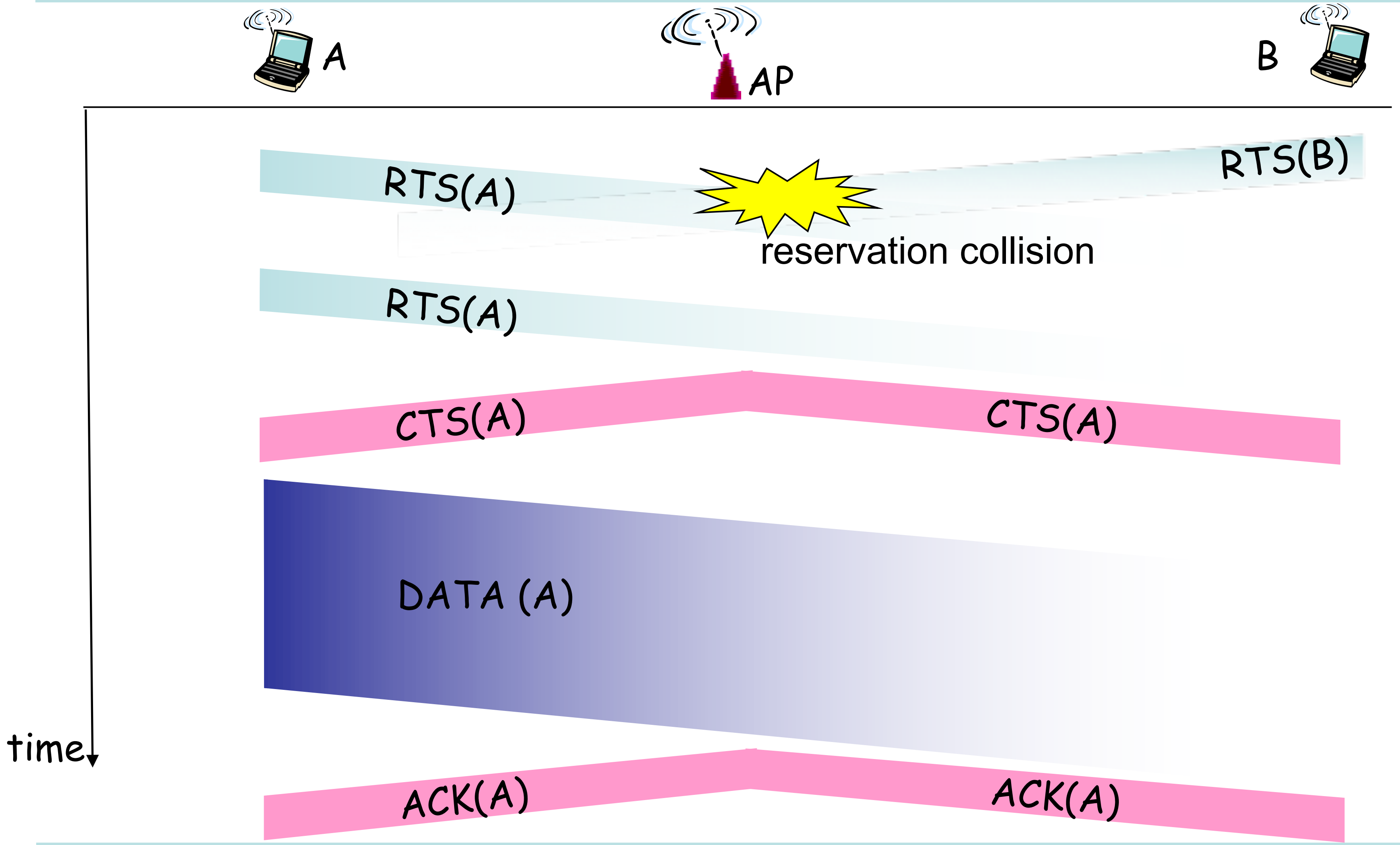
RTS-CTS-DATA-ACK



DIFS: Distributed IFS (Inter-frame Space) **for carrier sense**
RTS: Request-To-Send
SIFS: Short IFS

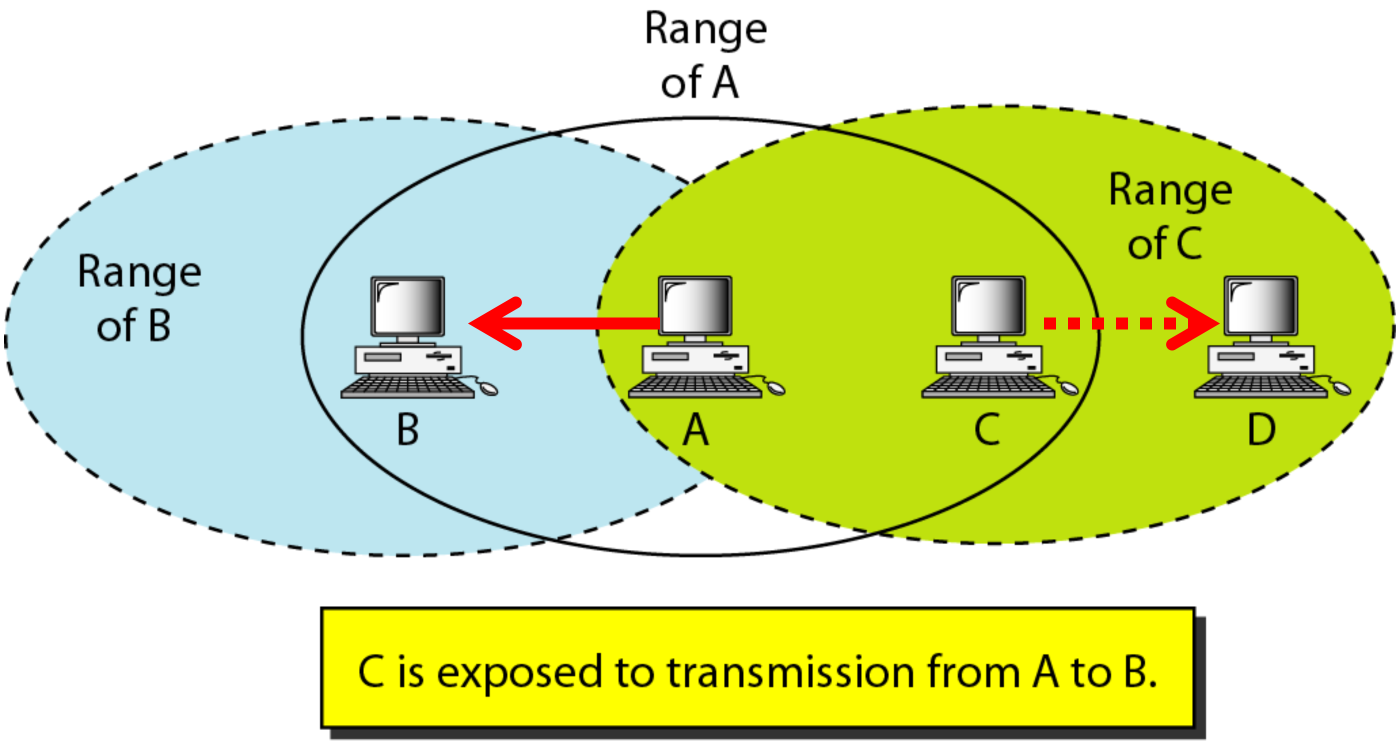
CTS: Clear-To-Send
ACK: Acknowledgement
NAV: Network Allocation Vector

Handshaking in Hidden Terminal Problem



Exposed Terminal Problem

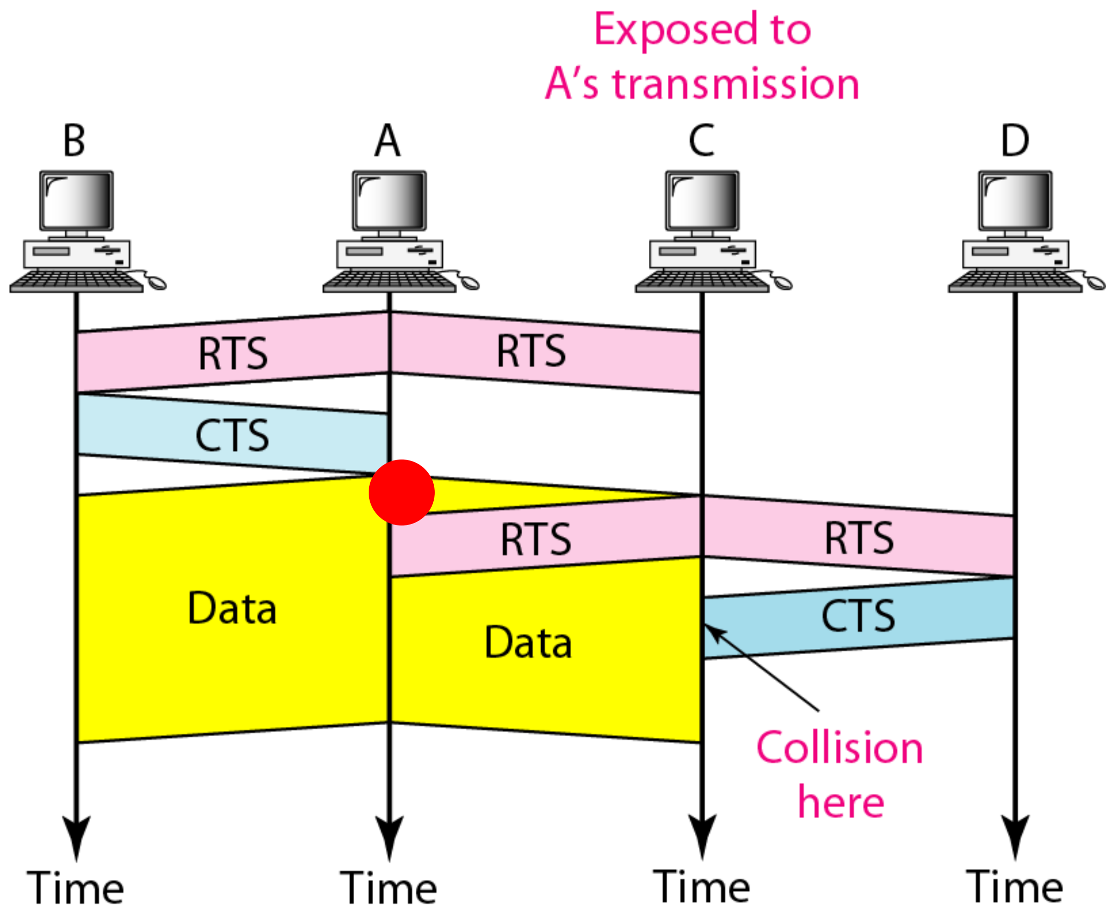
- **Signal decay causes Tx opportunity wasting**



The ongoing transmission from A to B will prevent C from transmitting to D, because C's carrier sense tells channel occupied.
However, in fact, C can transmit to D, because A's signal is weak at D!

Handshaking in Exposed Terminal Problem

- **RTS-CTS ensures no collision**
- **but doesn't solve the opportunity wasting problem**



802.11 Frame

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

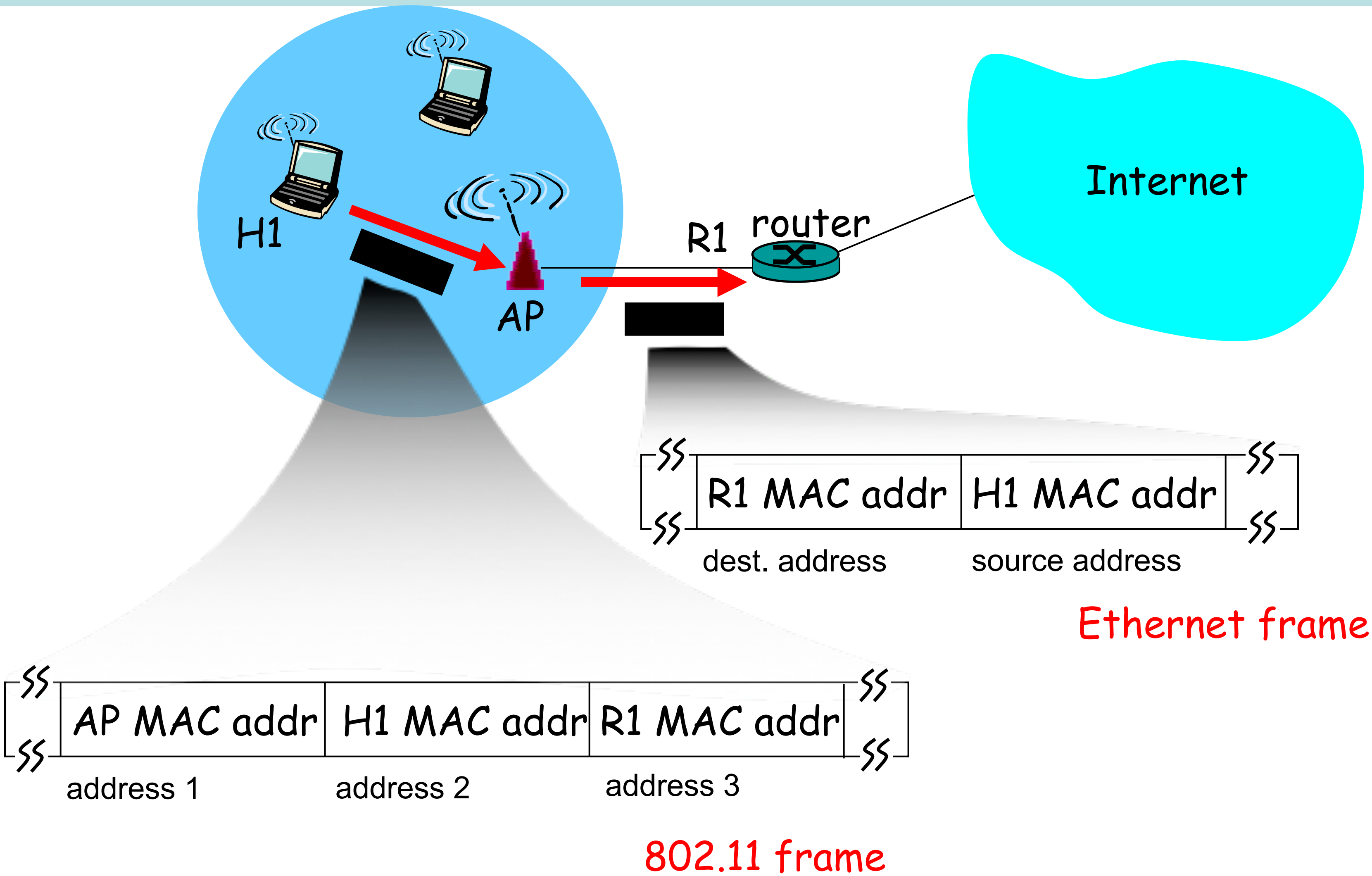
Address 1: MAC address of wireless host or AP to receive this frame

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

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 Addressing



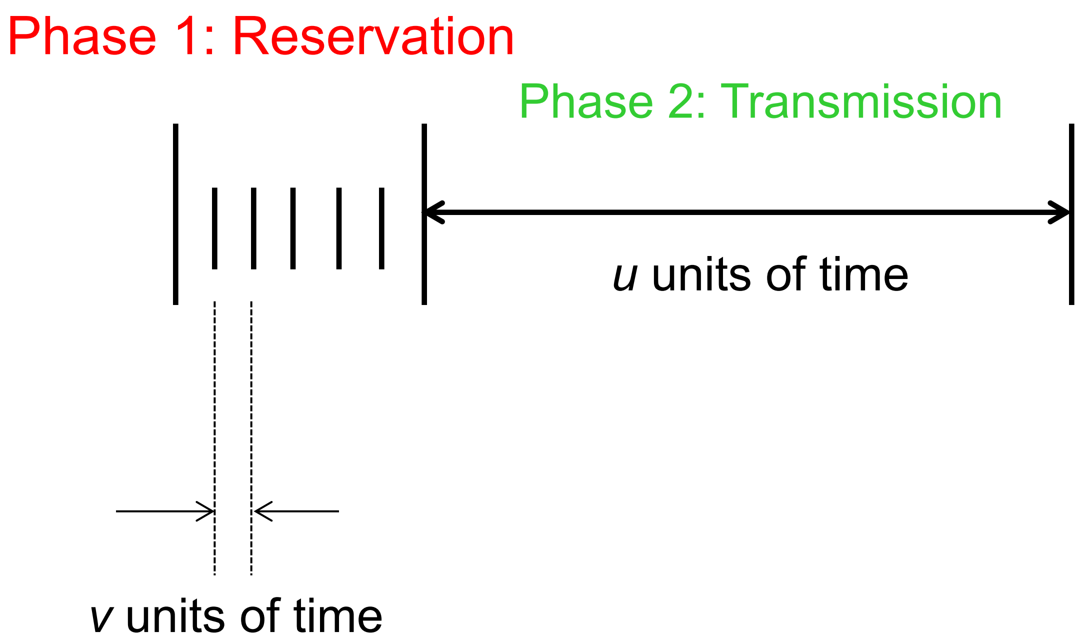
802.11 Advanced Capabilities

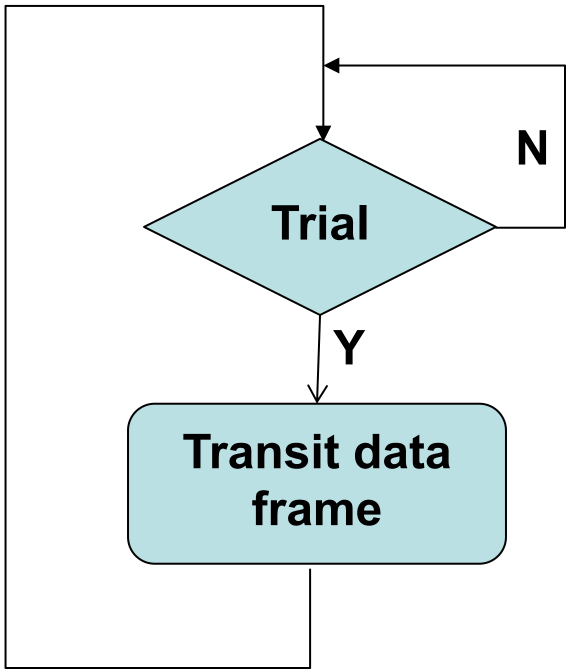
- **Synchronization**
  - finding and staying with a WLAN
  - synchronization functions
- **Power Management**
  - sleeping without missing any messages
  - power management functions
- **Roaming**
  - functions for joining a network
  - changing access points
  - scanning for access points
- **Management information base**

Multi-Access Reservation Protocol (MARP)

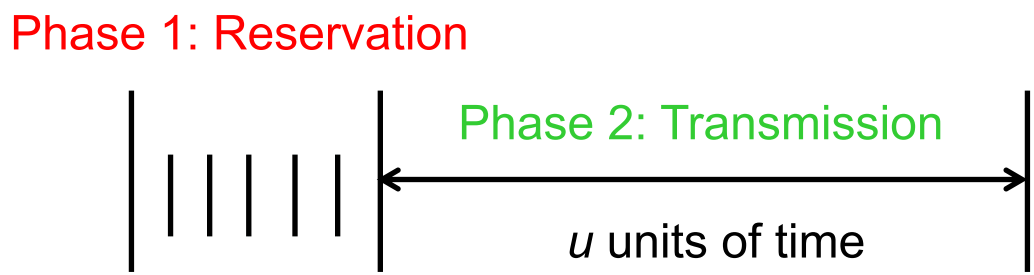
Multi-Access Reservation Protocol

- **Two-Phase Protocol**
  - Phase 1: Channel Reservation
  - Phase 2: Data Transmission



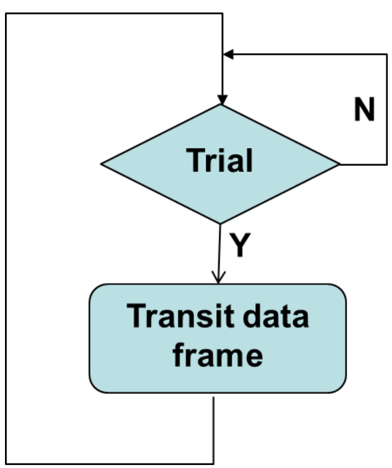


MARP Transmission Window



How many reservation trial frames?

- Assume that the reservation success probability is S_r
- Number of reservation trial frames to reserve the channel: X
  - $X = 1$ (the first trial succeeds) with probability of S_r
  - $X = k$ (the first k-1 trials fail, the k^{th} trial succeeds) with probability of $S_r(1-S_r)^{k-1}$
  - This is a geometric distribution, so $E[X] = 1/Sr$
- The average transmission window is $u + v/S_r$ units of time

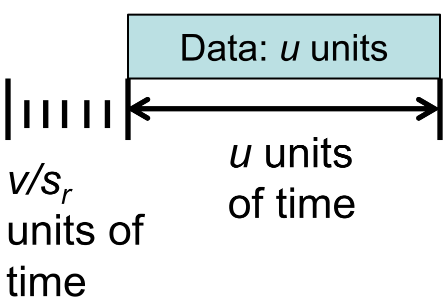


MARP Throughput

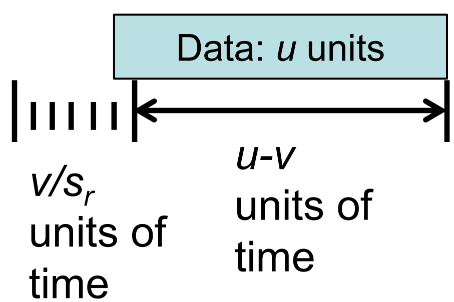
$$\text{Throughput } S = \frac{\text{Time for message transmission}}{\text{Transmission window}}$$

Case	Message Length	Reservation Phase Length	Throughput
(1) Reservation frame not used for message data bits	u	v/S_r	$S = \frac{u}{u + {}^{v}/_{S_r}}$
(2) Successful reservation frame used for message data bits	u	v/S_r	$S = \frac{u}{(u-v) + {}^{v}/_{S_r}}$
(3) Successful reservation frame used for message data bits	$u+v$	v/S_r	$S = \frac{u+v}{u + {}^{v}/_{S_r}}$

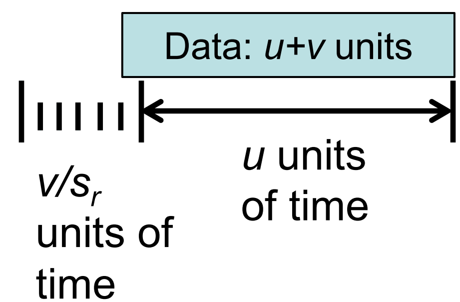
Case (1)



Case (2)



Case (3)



MARP Example

Consider an experimental LAN using an MARP for data transmission. The protocol consists of two phases. In phase 1, it adopts some MAC protocol for transmission stations to reserve the channel. In phase 2, when one station reserves the channel, it transmits one frame. The length of reservation frame is 5ms, and the length of the data frame is 1s. No information bit is carried in the reservation frame. If the reservation success probability is 0.5, what is the throughput of the multi-access reservation protocol?

CRACK Framework:

Context:	MARP with no data bits in reservation
fRamwork:	the throughput of MARP is S=1/(1+v/S_r)
Apply:	v=5ms, S_r=0.5
Calculation:	S = 1/(1+0.005/0.5)=1/1.01=0.99
checK:	S<=1

Local Area Network Summary

<table>
<tr><th colspan="2" rowspan="2">MAC Protocols</th><th colspan="3">Transmission Protocol</th><th rowspan="2">Throughput/ Utilization</th><th rowspan="2">Note</th></tr>
<tr><th>Carrier Sensing</th><th>Frame Transmission</th><th>Collision Detection</th></tr>
<tr><td rowspan="2">Aloha</td><td>Slotted</td><td rowspan="2">• None</td><td>• Each transmits in a slot immediately with probability p</td><td rowspan="6">• When a collision is detected, the colliding frames are transmitted up to their last bits.</td><td>$S = Np(1-p)^{(N-1)}$
$= Ge^{-G}$</td><td rowspan="2">Number of Stations: N
Probability of Attempt: p
Attempt Rate: $G = Np$</td></tr>
<tr><td>Pure</td><td>• Each transmits immediately with probability p</td><td>$S = Np(1-p)^{2(N-1)}$
$= Ge^{-2G}$</td></tr>
<tr><td rowspan="3">CSMA</td><td>Non-Persistent</td><td rowspan="3">• Must sense channel before transmission</td><td>• When a busy channel is sensed, a station defers for a random period of time before next sense</td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td>P-Persistent</td><td>• When a busy channel is sensed, a station continues to sense until the channel turns idle. Then, with probability p, it transmits, and with probability $1-p$, it defers to next time slot.</td></tr>
<tr><td>1-Persistent</td><td>• A special case of P-Persistent where $p = 1$</td></tr>
<tr><td colspan="2">CSMA/CD (Ethernet)</td><td>• Must sense channel before transmission</td><td>• The same as CSMA</td><td>• When a collision is detected, transmissions are aborted to reduce the channel wastage.</td><td>$S = \frac{1}{1 + 6.44a}$
$a = \frac{T_{Prop}}{T_{frame}}$
(not covered in lecture)</td><td>Minimum Frame Size
• $T_{frame} \geq 2\tau$
Binary Exponential Backoff
• In i-th retransmission, the slot is chosen from a uniformly distributed random variable R, in the range of $[0, 2^K - 1]$, where $K = \min(i, 10)$.</td></tr>
<tr><td colspan="2">CSMA/CA (802.11)</td><td>• Must sense channel before transmission</td><td>Sender:
• If sense channel idle for DIFS, then transmit entire frame (no CD).
• If sense channel busy, then start random backoff time. Transmits when timer expires.
• If no ACK, increase random backoff interval
Receiver:
• If frame received OK, return ACK after SIFS</td><td>• No collision detection due to hidden terminal</td><td colspan="2">Multi-Access Reservation
• Use random-access with mini-frame (v unit of time) to reserve the channel
• If reservation successful, transmit u unit of data frame
<table>
<tr><th></th><th>$\frac{u}{u + v/S_r}$</th><th>$\frac{u}{(u-v) + \frac{v}{S_r}}$</th><th>$\frac{u+v}{u + v/S_r}$</th></tr>
<tr><td>Total data length</td><td>u</td><td>u</td><td>$u + v$</td></tr>
<tr><td>Data bit in mini-frame</td><td>No</td><td>Yes</td><td>Yes</td></tr>
</table></td></tr>
</table>

NANYANG TECHNOLOGICAL UNIVERSITY

Learning Objectives

- **WLAN Overview**
  - Understand two alternative WLAN architectures
- **802.11 Physical Layer**
  - Understand different transmission schemes
- **802.11 MAC Layer**
  - Understand hidden and exposed terminal problems
  - Understand CSMA/CA protocol
- **Multi-Access Reservation Protocol (MARP)**
  - Understand the scheme of MARP
  - Calculate and maximize throughput for MARP

Reading Material

Wireless Physical Layer (I)

- **Physical layer conforms to OSI (five options)**
  - 1997: **802.11** infrared, FHSS, DHSS
  - 1999: **802.11a** OFDM and **802.11b** HR-DSSS
  - 2001: **802.11g** OFDM
- **802.11 *Infrared***
  - Two capacities 1 Mbps or 2 Mbps.
  - Range is 10 to 20 meters and cannot penetrate walls.
  - Does not work outdoors.
- **802.11 *FHSS* (*Frequency Hopping Spread Spectrum*)**
  - **The main issue is multipath fading.**
  - 79 non-overlapping channels, each 1 Mhz wide at low end of 2.4 GHz ISM band.
  - Same pseudo-random number generator used by all stations.
  - Dwell time: min. time on channel before hopping (400msec).

Wireless Physical Layer (II)

- **802.11 *DSSS* (*Direct Sequence Spread Spectrum*)**
  - Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA see Tanenbaum sec. 2.6.2).
  - Each bit transmitted using an 11 chips Barker sequence, PSK at 1Mbaud.
  - 1 or 2 Mbps.
- **802.11a *OFDM* (Orthogonal Frequency Divisional Multiplexing)**
  - Compatible with European HiperLan2.
  - 54Mbps in wider 5.5 GHz band ➔ transmission range is limited.
  - Uses 52 FDM channels (48 for data; 4 for synchronization).
  - Encoding is complex (PSM up to 18 Mbps and QAM above this capacity).
  - E.g., at 54Mbps 216 data bits encoded into 288-bit symbols.
  - More difficulty penetrating walls.

Wireless Physical Layer (III)

- **802.11b** ***HR-DSSS*** **(*****High Rate Direct Sequence Spread Spectrum*****)**
  - **11a and 11b** *shows a split in the standards committee.*
  - **11b** approved and hit the market before **11a.**
  - Up to 11 Mbps in 2.4 GHz band using 11 million chips/sec.
  - Note in this bandwidth all these protocols have to deal with interference from microwave ovens, cordless phones and garage door openers.
  - Range is 7 times greater than **11a.**
  - **11b and 11a are incompatible!!**
- **802.11g** ***OFDM*****(*****Orthogonal Frequency Division Multiplexing*****)**
  - **An attempt to combine the best of both 802.11a and 802.11b.**
  - Supports bandwidths up to 54 Mbps.
  - Uses 2.4 GHz frequency for greater range.
  - Is backward compatible with 802.11b.