Wireless Networks

ITS 413 – Internet Technologies and Applications

Contents

- Wireless Communications
  - Characteristics and Challenges
- Wireless Technologies
  - Telephony, PANs, LANs, MANs, …
- Case Study: IEEE 802.11 Wireless LANs
  - Details of how wireless LANs work

Wireless Communications

- Benefits
  - Untethered communications (no wires)
    - In some cases, can enable quick installation
  - Mobility of users and devices
- Challenges
  - Wireless channel is not as robust as wires
    - More errors, higher delays, varying conditions
  - Radio spectrum is limited (cannot just add more wires)
  - Many Internet protocols designed assuming a “perfect channel”
  - Broadcast nature – need to share access efficiently among users
  - Physical security is difficult; hence good network security is needed

Radio Frequency Spectrum

- Radio Frequency (RF) is part of electromagnetic spectrum where waves generated from AC into antenna
- Divided into bands, for example, VHF, UHF, Infrared, …
- Bandwidth in each band is limited
  - **Licensed**: controlled access but expensive (e.g. GSM, 3G – €50billion spent in Germany)
  - **Unlicensed**: cheap but congested (e.g. WLAN – more users means less throughput per user)
- Need efficient ways to share the bandwidth amongst users

RF Spectrum

Band	Frequency Range	Free-Space Wavelength Range	Propagation Characteristics	Typical Use
ELF (extremely low frequency)	30 to 300 Hz	10,000 to 1000 km	GW	Power line frequencies; used by some home control systems.
VF (voice frequency)	300 to 3000 Hz	1000 to 100 km	GW	Used by the telephone system for analog subscriber lines.
VLF (very low frequency)	3 to 30 kHz	100 to 10 km	GW; low attenuation day and night; high atmospheric noise level	Long-range navigation; submarine communication
LF (low frequency)	30 to 300 kHz	10 to 1 km	GW; slightly less reliable than VLF; absorption in daytime	Long-range navigation; marine communication radio beacons
MF (medium frequency)	300 to 3000 kHz	1,000 to 100 m	GW and night SW; attenuation low at night, high in day; atmospheric noise	Maritime radio; direction finding; AM broadcasting.
HF (high frequency)	3 to 30 MHz	100 to 10 m	SW; quality varies with time of day, season, and frequency.	Amateur radio; international broadcasting, military communication; long-distance aircraft and ship communication
VHF (very high frequency)	30 to 300 MHz	10 to 1 m	LOS; scattering because of temperature inversion; cosmic noise	VHF television; FM broadcast and two-way radio, AM aircraft communication; aircraft navigational aids
UHF (ultra high frequency)	300 to 3000 MHz	100 to 10 cm	LOS; cosmic noise	UHF television; cellular telephone; radar; microwave links; personal communications systems
SHF (super high frequency)	3 to 30 GHz	10 to 1 cm	LOS; rainfall attenuation above 10 GHz; atmospheric attenuation due to oxygen and water vapor	Satellite communication; radar; terrestrial microwave links; wireless local loop
EHF (extremely high frequency)	30 to 300 GHz	10 to 1 mm	LOS; atmospheric attenuation due to oxygen and water vapor	Experimental; wireless local loop
Infrared	300 GHz to 400 THz	1 mm to 770 nm	LOS	Infrared LANs; consumer electronic applications
Visible light	400 THz to 900 THz	770 nm to 330 nm	LOS	Optical communication

Stallings: Data and Computer Communications, Prentice Hall 2006.

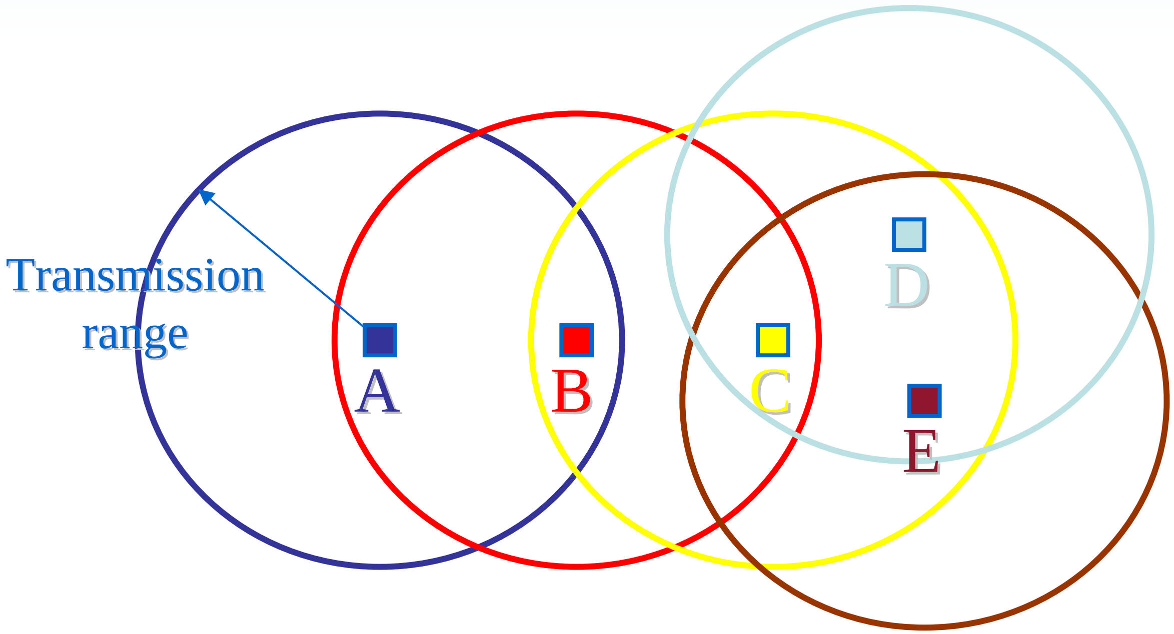
Wireless Transmission Systems

- Terrestrial Microwave
  - Directional antenna
  - Applications:
    - Long haul telecommunications: 4-6GHz
    - Building-to-building: 22GHz
    - TV: 12GHz
- Satellite Microwave
  - Directional antenna
  - Bent-pipe: satellite acts as repeater between two ground stations
  - Broadcast: satellite broadcasts to many ground stations
- Infrared
  - Directional transmission of infrared light
  - Short distances, no penetration of objects
- Broadcast Radio
  - Omnidirectional antenna (transmit in all directions)
  - Non line-of-sight (can go through walls)
  - Data network applications: WLAN, Bluetooth, …

Broadcast Nature of Radio

- Important characteristics:
  - Receiving signals from more than one transmitter usually mean the receiver cannot decode (understand) the signal
    - Other transmitters cause interference
  - Transmitters/receivers (transceivers) such that difficult to transmit and receive at same time
  - With omnidirectional antennas, all receivers within range of transmitter receiver (or hear) the signal
- We want to avoid interference at the receiver
- But we also want to make efficient use of spectrum!

Broadcast Nature of Radio



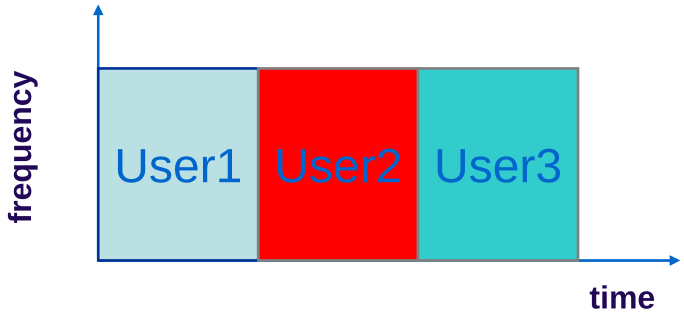
- All nodes within a transmitting node's range hear (receive) the transmission
- Assume receivers cannot decipher two transmissions
  - A node receiving two or more transmissions at once leads to interference (Layer 1 perspective)
  - In other words, a node receiving two or more frames at once leads to a collision (Layer 2 perspective)
    - Collision results in none of the frames being successfully received (i.e. all frames are discarded)
- Therefore, we use multiple access techniques to "separate" the transmissions…

Multiple Access

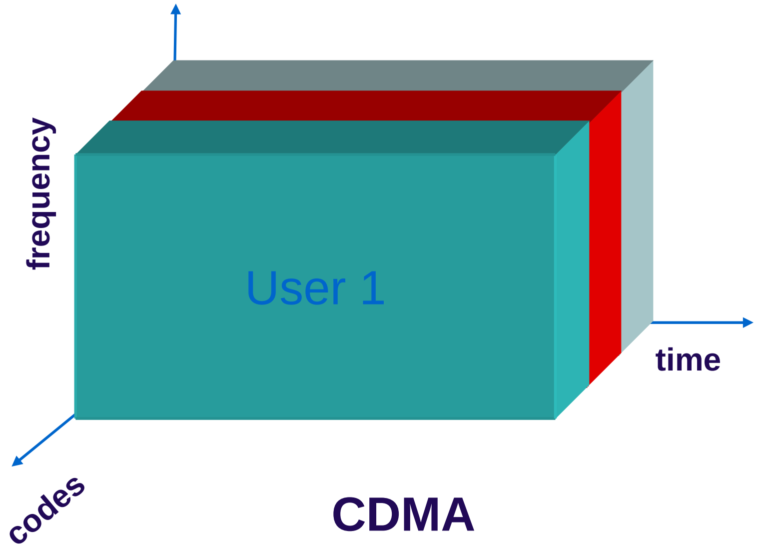
- Many users need to share the same channel. How do they do it?
- Frequency Division Multiple Access (FDMA)
  - Give each user a separate frequency to transmit on
  - If frequencies are far enough apart, then they won't interfere
- Time Division Multiple Access (TDMA)
  - Give each user a time slot to transmit in
  - Only one user transmits at any time instant
- Code Division Multiple Access (CDMA)
  - Spread signal across wider bandwidth than normally needed
  - Allocate code to each user; Receiver separates signals based on expected code
- Trade-offs amongst all approaches

Multiple Access

FDMA



TDMA

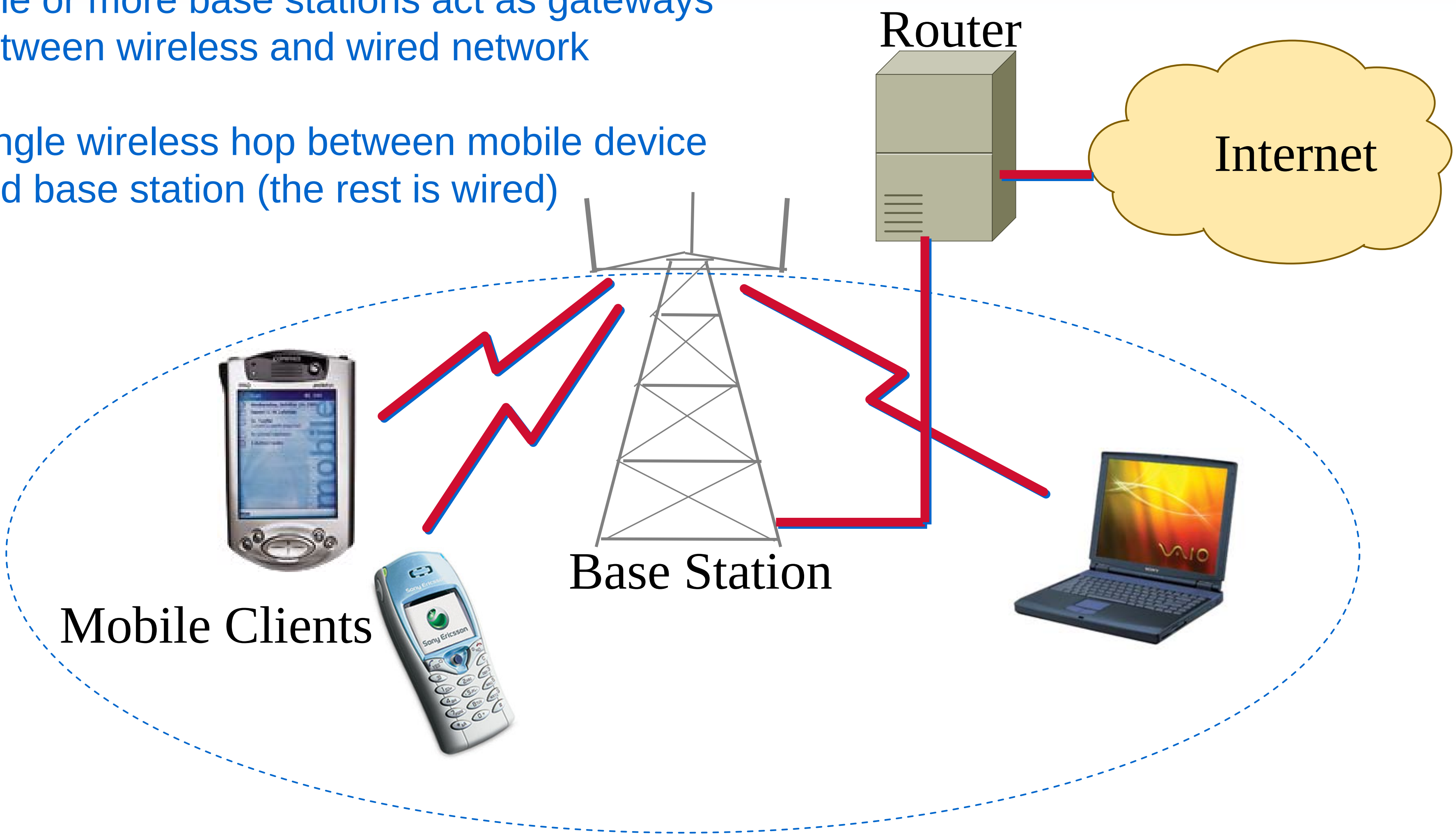


CDMA

Centralised Network Architecture

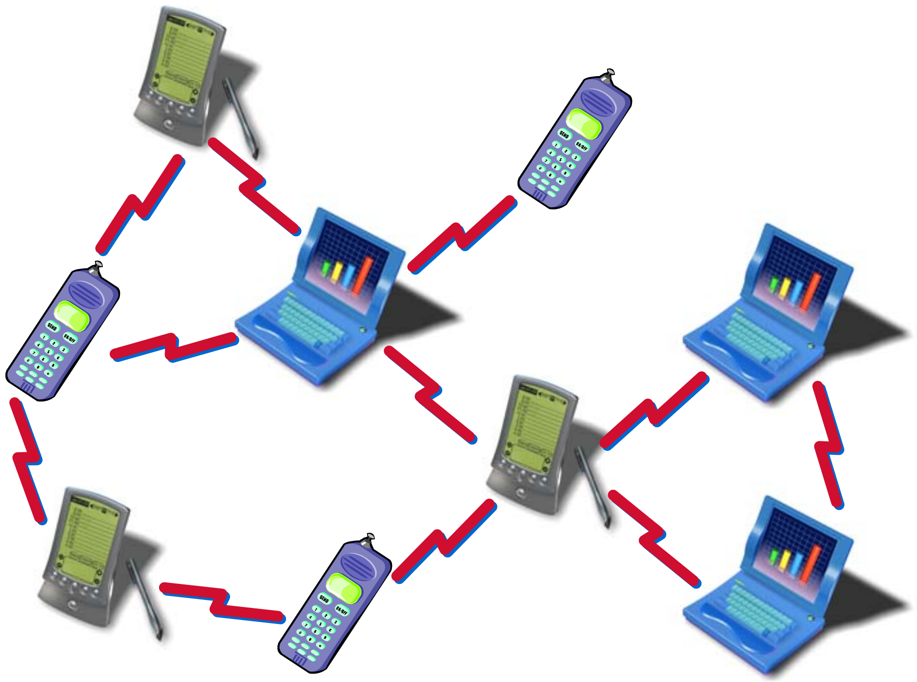
One or more base stations act as gateways between wireless and wired network

Single wireless hop between mobile device and base station (the rest is wired)



Decentralised Network Architecture

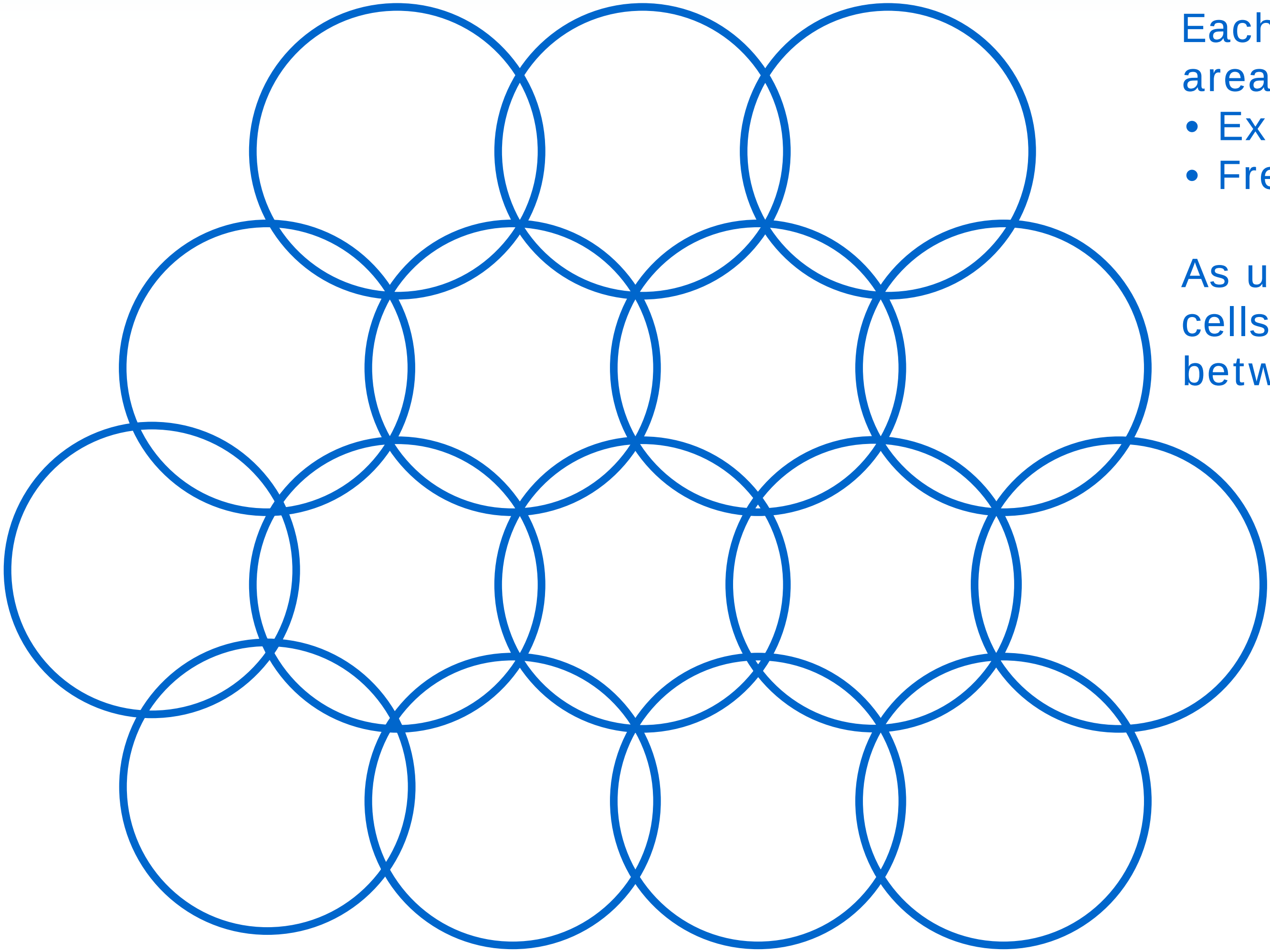
- Wireless devices connect between themselves
- If destination device is outside of range of source, then intermediate devices forward on source's behalf
- Require no or little pre-installed infrastructure (base stations, cables, servers)
  - Cheap and quick to build
- Highly dynamic network; topology changes often
- Hard to build efficient and secure networks



Coverage

- The distance a RF signal travels depends on transmit power, antennas, frequency and interference (e.g. from objects)
- Many systems have a nominal range, for example:
  - Bluetooth, WPANs: metres to 10’s of metres
  - IEEE 802.11: 10’s of metres indoors, 100’s of metres outdoors (further if point to point)
  - GSM/3G: 100’s of metres to kilometres
  - Satellites: 100’s to 1000’s of kilometres
- How do we extend the coverage?
  - Add more cells (base stations)

Cellular Architecture



Each cell is the coverage area of 1 base station

- Extend coverage
- Frequency re-use

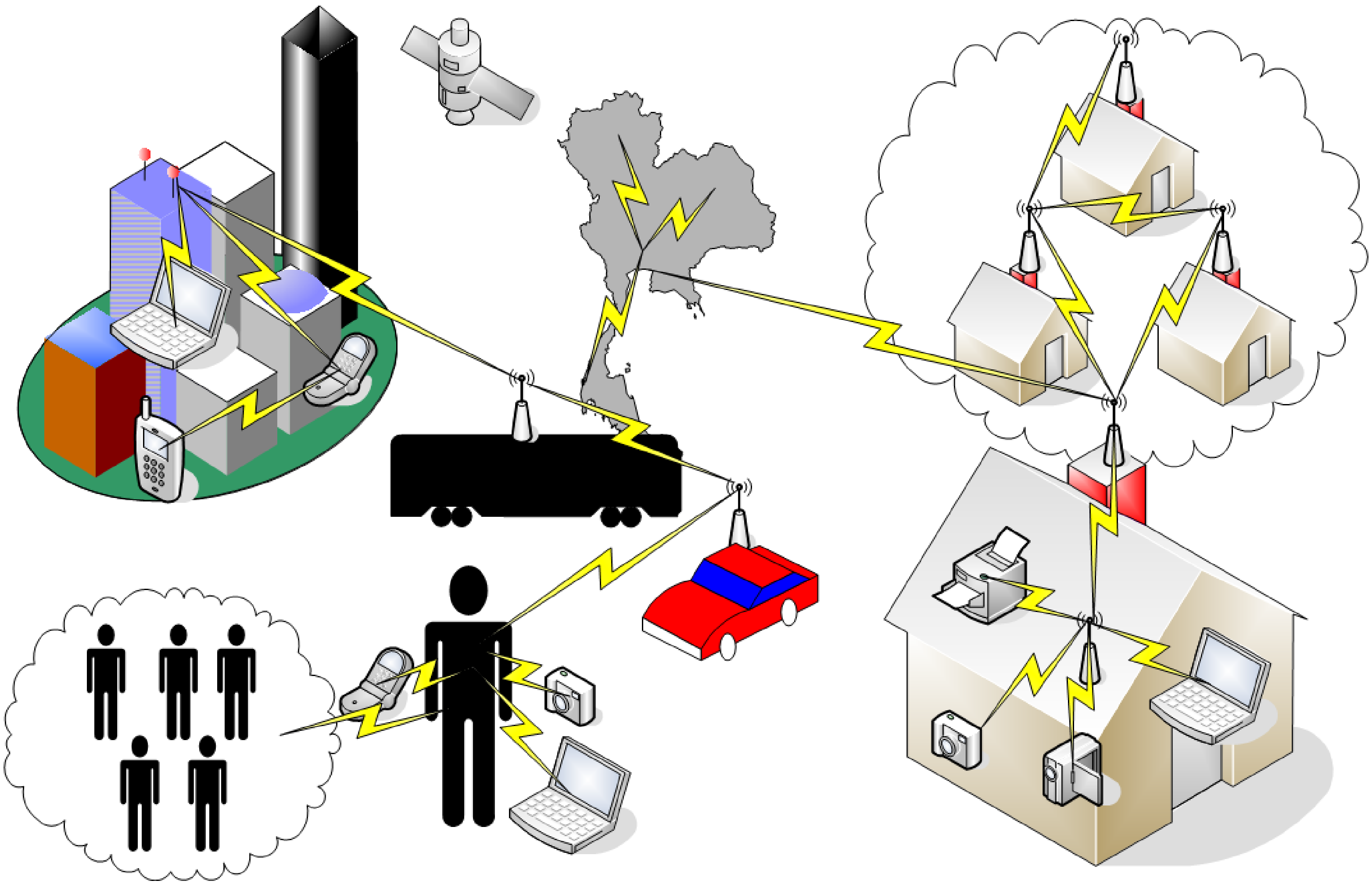
As users move between cells, must **handover** between base stations

Overview of Wireless Technologies

Wireless Networks

Next Generation Wireless Networks

Ubiquitous mobile access to Internet



Enabling Technologies

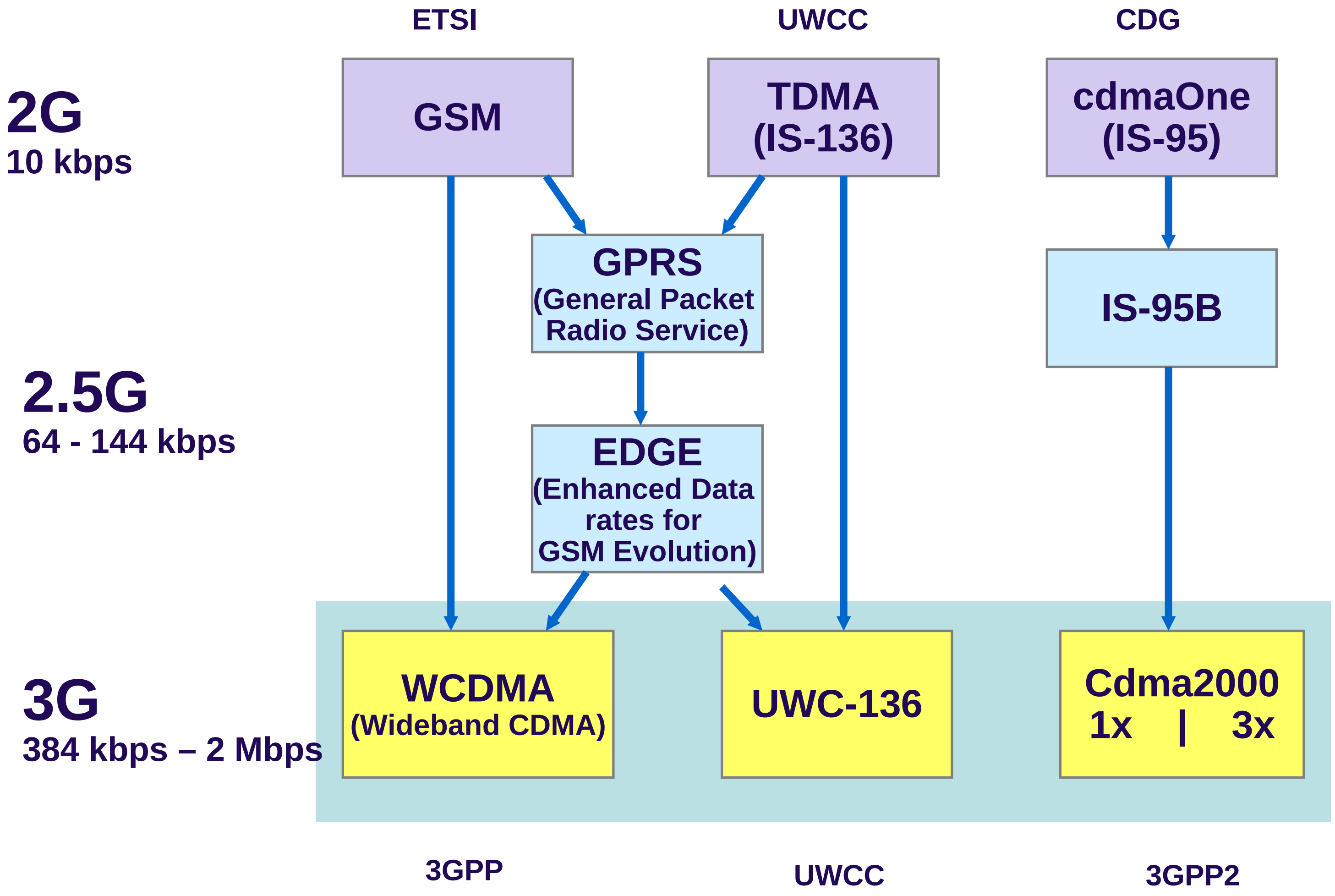
- Wireless Data Access
  - Protocols and standards for providing the wireless access
    - 3G, WiFi, WiMax, Bluetooth, Satellite, …
  - Usually layers 1 (Physical) and 2 (Data Link/MAC)
- Internet Mobility Support
  - Mobile users can access Internet from any location and network
    - Mobile IP
  - Layer 3 (Network)
- Infrastructure-less Networks
  - No longer rely on fixed (expensive) base stations with wired connections
  - Wireless connections between users for dynamic networks
    - Mesh networks, Mobile Ad Hoc Networks, Sensor Networks
  - Usually layers 3 and above
- Efficient Transport and Application Protocols
  - Existing or new protocols work well over wireless
    - TCP, HTTP, Voice, …
  - Layers 4 (Transport) and 5 (Application)
- Applications and Support Environments
  - Make it easy for a mobile user to access network services

Classifying Wireless Networks

Name	Abbrev.	Range	Applications	Examples
Wireless Personal Area Network	WPAN	Several metres	Connecting peripherals	Bluetooth, IrDA
Wireless Local Area Network	WLAN	10's to 1000's of metres	Office, home, street communications	IEEE 802.11
Wireless Metropolitan Area Network	WMAN	Km's	Inter-office and building connections,	IEEE 802.16, IEEE 802.20
Wireless Wide Area Network	WWAN	Km's to regional to global	City, nation wide telecommunications; connections between cities	3G(UMTS),GSM, Satellite

Mobile Telephony Networks

- Evolution of Technologies



GSM, GPRS and EDGE

- GSM
  - Dominant 2nd generation mobile telephony system
  - Technology used for most mobile phones for past 10-15 years
  - TDMA
  - Other alternatives: IS-136 (TDMA), IS-95 (CDMA) mainly in US
  - Data rate around 10kb/s
- GPRS and EDGE
  - Improved GSM data capabilities
    - 100-300kb/s
  - Make significant use of existing technology (networks, software, hardware)

3G: UMTS and CDMA2000

- Third Generation Networks (3G)
  - ITU developed a global vision for 3G in IMT-2000
  - Several implementations within IMT-2000
    - Require significant new technologies for deployment
  - Provide better voice and data capabilities
  - Move from circuit switching to packet switching
- UMTS/WCDMA
  - Evolved from GSM
  - 384kb/s
- CDMA2000
  - Evolved from CDMA (IS-95)
  - First step 1X: 144kb/s
  - Second step: 3X: 384kb/s
- Higher Speed Data Access
  - HSPDA: 10-15Mb/s download, 384kb/s uplink (trial deployments in place today)
  - HSUPA: extend HSPDA to include 5Mb/s uplink
  - 3G Release 7 – 10’s of Mb/s data rates

Comparison of Data Rates

Generation	Name	Data Rate	Spectrum	Switching
2G	GSM	14.4kb/s	200kHz	Circuit
2G	IS-136	9.6kb/s	30kHz	Circuit
2G	IS-95 (CDMA)	64kb/s	1.25MHz	Circuit
2.5G	HSCSD	56kb/s	200kHZ	Circuit/Packet
2.5G	GPRS	128kb/s	200kHz	Circuit/Packet
2.5G	EDGE	384kb/s	200kHz	Circuit/Packet
2.5G	CDMA2000 (1XRTT)	144kb/s	1.25MHz	Circuit/Packet
3G	WCDMA	144kb/s vehicle 384kb/s outdoor 2MB/s indoor	5MHz	Packet
3G	CMA2000 (3XRTT)	144kb/s vehicle 384kb/s outdoor 2MB/s indoor	5MHz	Packet

Wireless PANs

- Characteristics:
  - Short range networking between computers, peripherals and appliances
  - Cable replacement technology
  - Should be cheap, simple to use and energy efficient
  - Low (kb/s) to moderate (Mb/s) data rates
  - Range of several metres
- Standards:
  - Infrared (Infrared Data Association, IrDA)
  - Bluetooth
  - IEEE 802.15
    - Includes latest developments of Bluetooth
    - Also low data rate technology, e.g. for wireless toys

Bluetooth Characteristics

Parameter	Bluetooth v1.2
Range	10m @ 1mW 100m @ 100mW
Data Rates	723kb/s
Operating Frequency	2.4GHz ISM
Spread Spectrum/Modulation	Frequency Hopping
Media Access	TDMA
Applications	File transfer, headset, synchronisation, Internet bridge, network access, etc.
Commercial Status	Regularly available in laptops, PDAs, keyboards, phones, headsets etc.

Wireless LANs

- Aim to provide similar services as wired LANs to mobile users (laptops, PDAs, wireless desktops)
- Data rates are order of magnitude less than wired LANs
- Typical range of 10's to 100's of metres
- Standards:
  - IEEE 802.11 and its many amendments

- We will cover in detail as a case study

IEEE 802.11 Characteristics

Parameter	**802.11b**	**802.11a**	**802.11g**	**802.11n**
Range[3]	20-300m	15-30m	25-75m	20-60m
Data Rates	11Mb/s	54Mb/s	54Mb/s	384Mb/s
Operating Frequency	2.4GHz ISM	5GHz	2.4GHz	5GHz
Spread Spectrum/Modulation	Direct Sequence Spread Spectrum	OFDM	OFDM	OFDM, MIMO
Media Access	CSMA/CA	CSMA/CA	CSMA/CA	CSMA/CA
Applications	Web, email, database, office, …	Same as 11b, but also multimedia capabilities	Same as 11b, but also multimedia capabilities	Same as 11a/g, but also high quality video
Commercial Status	Regularly available in laptops, PDAs etc. Large deployment of infrastructure	Available in new laptops, PDAs etc. Not as widespread as 11b/g.	Regularly available in new laptops, PDAs etc.	Standard incomplete; "pre-N" products (based on draft standard) are available

Wireless MANs

- Legacy Microwave Technologies
  - Point-to-point wireless links over km's – Fixed nodes
  - Similar data rates to leased lines, DSL, cable
  - Proprietary as well as standards based systems in use today
    - Usually do not interoperate with each other
- IEEE 802.16 and IEE 802.20
  - 802.16 aimed to solve interoperability problems of legacy systems
  - WiMax is a consortium-led standard to agree on unspecified parts of 802.16
  - WiBro: South Korean led development of 802.16
  - 802.20: add user mobility, data rates up to 250Mb/s
  - Similar in expense and complexity as 3G equipment and networks

IEEE 802.16 Characteristics

Parameter	**802.16**
Range	30-50km LOS 8km NLOS
Data Rates	72Mb/s (per channel)
Operating Frequency	10-66GHz, Sub-11GHz, 5-6GHz unlicensed
Spread Spectrum/Modulation	OFDM
Media Access	TDMA/TDM
Applications	Interconnecting offices, last-mile services, ..
Commercial Status	Chips in development, becoming available; Products becoming available

Multi-hop Wireless Networks

- Infrastructure-less networks
  - Wireless nodes communicate amongst each other
  - No need for base stations, wired connections, servers, …
    - Cheap, quick to deploy, dynamic, survivable
  - Difficult to do: routing, security, high performance, QoS, …
- Mobile Ad Hoc Networks
  - Network formed amongst all wireless, mobile nodes
  - Examples:
    - Spontaneous network between group of friends
    - Military battlefield network amongst soldiers and vehicles
- Mesh Networks
  - Some fixed wireless nodes, e.g. to form a backhaul network
  - Network is not as dynamic as “pure” MANET
  - Examples:
    - Mobile broadband access for emergency services
    - Low cost network deployment in rural/remote areas
    - Community-based wireless networks

Relevance for Internet Protocols and Applications

- Characteristics of wireless networks and consequences:
  - Low bandwidth, the RF spectrum is limited
    - Need efficient protocol and application design
    - Need to manage access to spectrum
  - Large and/or varying delays (hard to predict delay)
    - Need Internet protocols that consider this
    - Relying on timeouts is difficult – how long should you wait?
  - Small devices
    - Applications must be tailored to device, or consider limitations
    - New GUI and user interaction methods are needed
  - Mobile users
    - Need to be able to locate users, and manage their network access
    - Enable new applications and services, e.g. location services

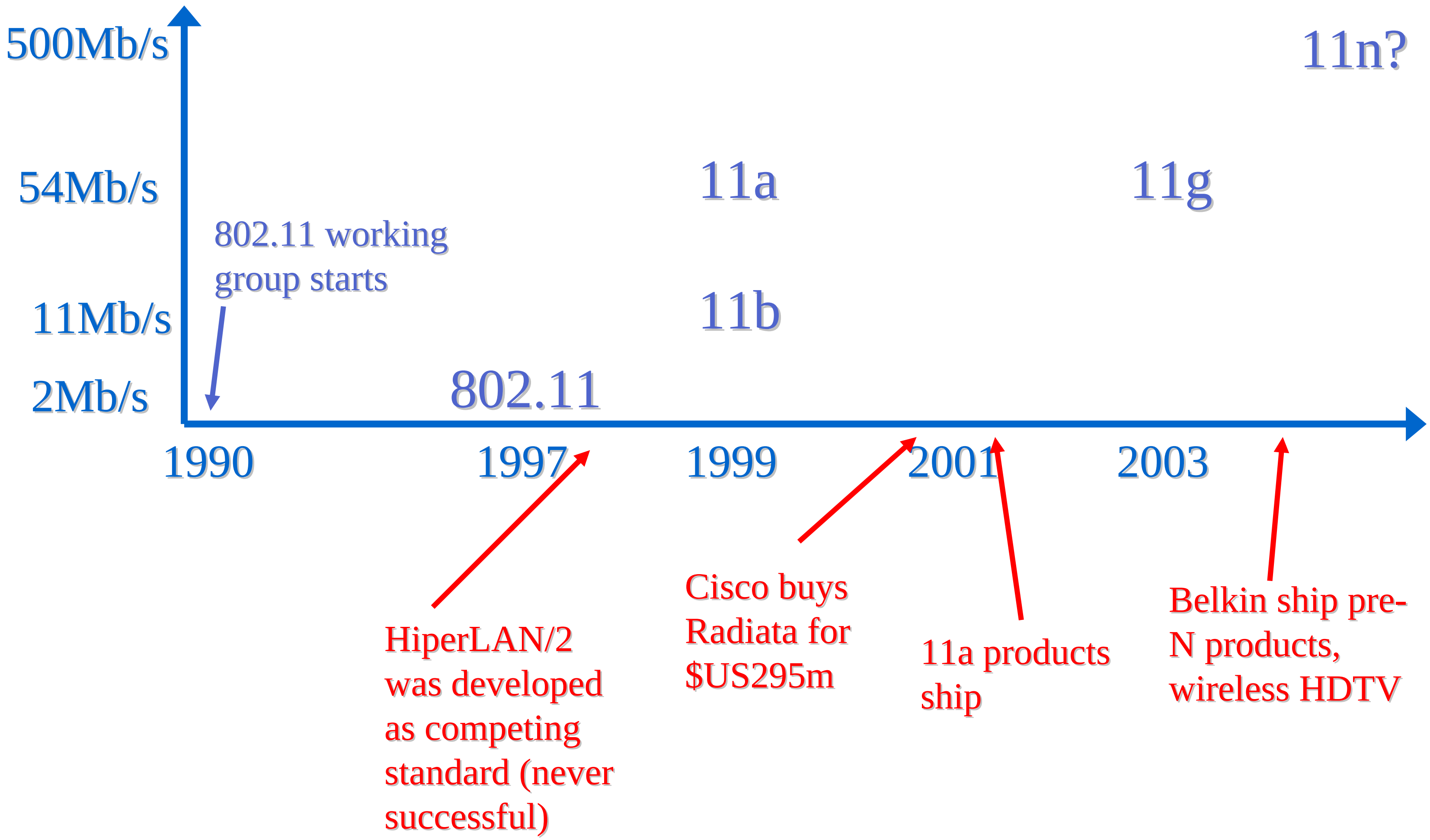
Wireless LANs

Wireless Networks

Aim of Wireless LANs

- Provide similar network capabilities to computers as on wired LANs
  - Support for mobile users (laptops, PDAs)
  - Provide LAN access when it is too expensive or too difficult to provide wires
    - Existing buildings with no network, historical buildings
    - Outdoors
- Usually only single-hop wireless
  - From user to base station (Access Point); the rest is wired

History of Wireless LAN Standards

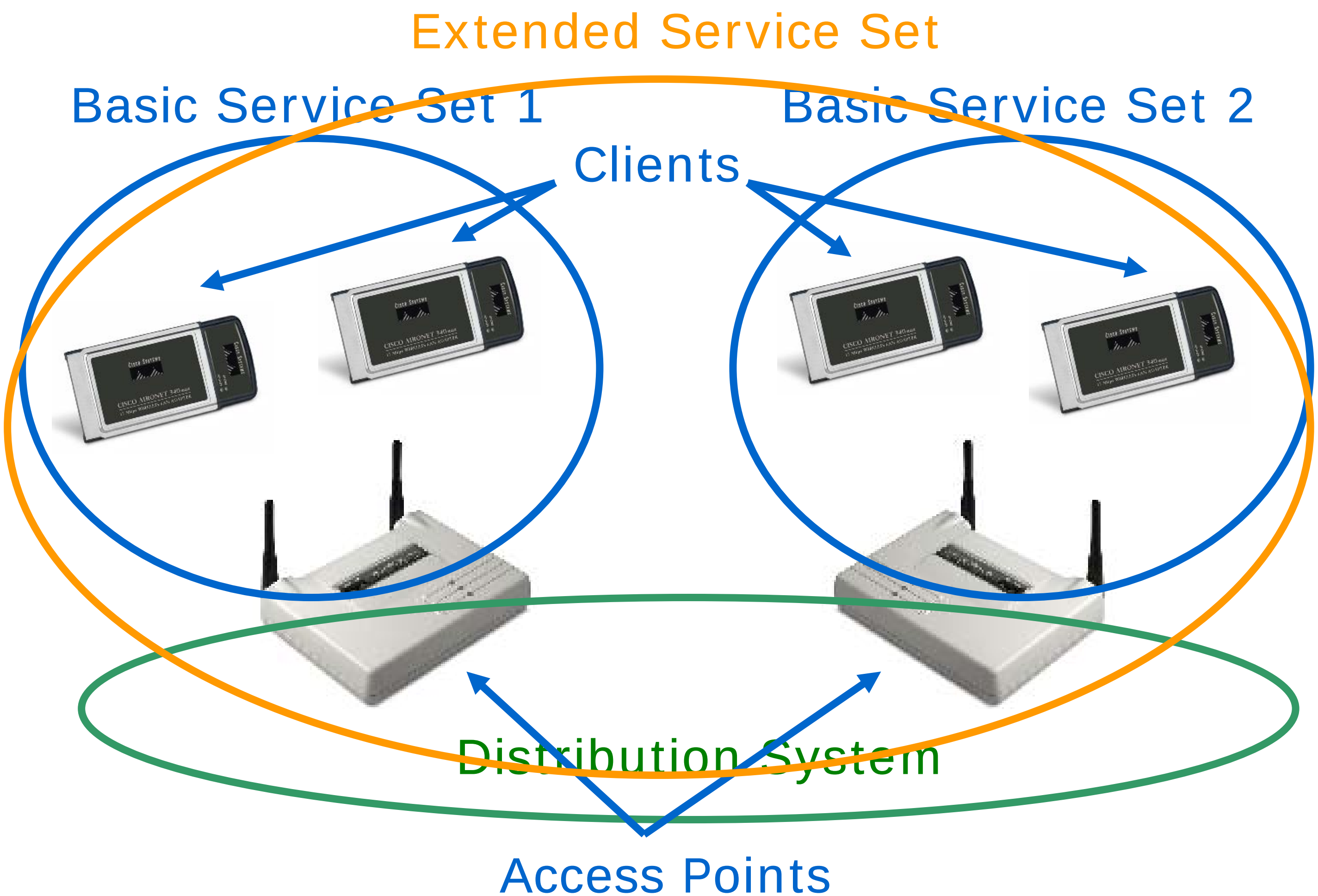


Standardisation Efforts

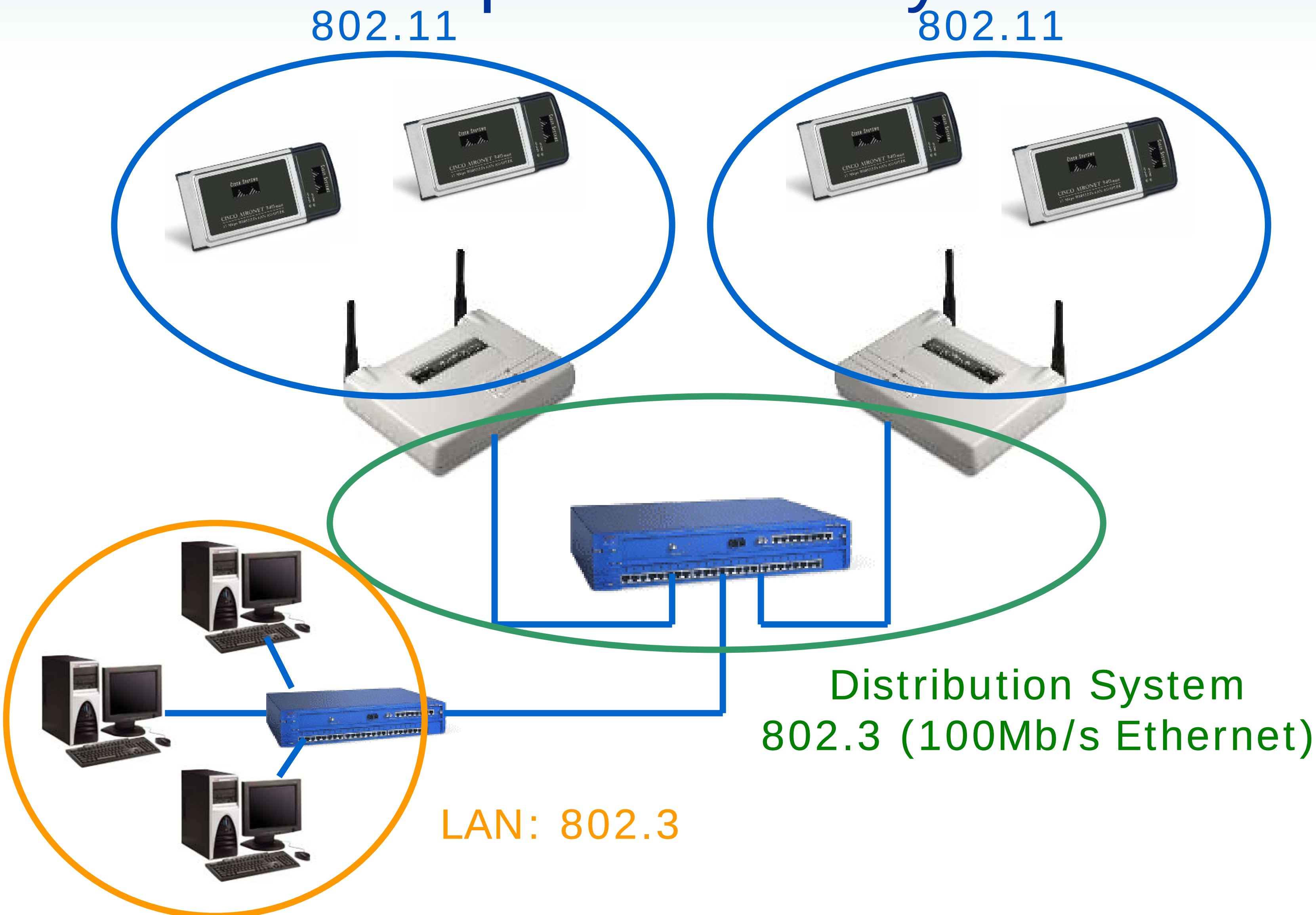
- IEEE 802 Working Group 11 sets the standards
  - Original standard fro 802.11 released in 1997
  - Since then, 802.11 Task Groups have developed amendments (denoted by letters)
    - a, b, g – Physical layer changes to improve data rates
    - e – quality of service
    - i – security
    - …
    - Currently up to Task Group Y
- Who is in the Working/Task groups?
  - Anyone (providing you attend meetings on regular basis)
  - Representatives of network hardware and software companies play significant role in influencing direction (hence many commercial, political pressures)
  - Some companies implement drafts of the standard before they are finalised, for example, “pre-N” products
- Compliance organisations
  - There are often different ways to implement that meets the standard
  - Companies get together and agree on how to implement so interoperable products
  - WiFi Alliance, Enhanced Wireless Consortium, …
- Non-standard modifications
  - Some companies enhance their implementations using proprietary techniques
  - Lead to performance improvements when using only their products, but not others
  - Often degrades performance of other networks!

Components of 802.11 System

Infrastructure Mode

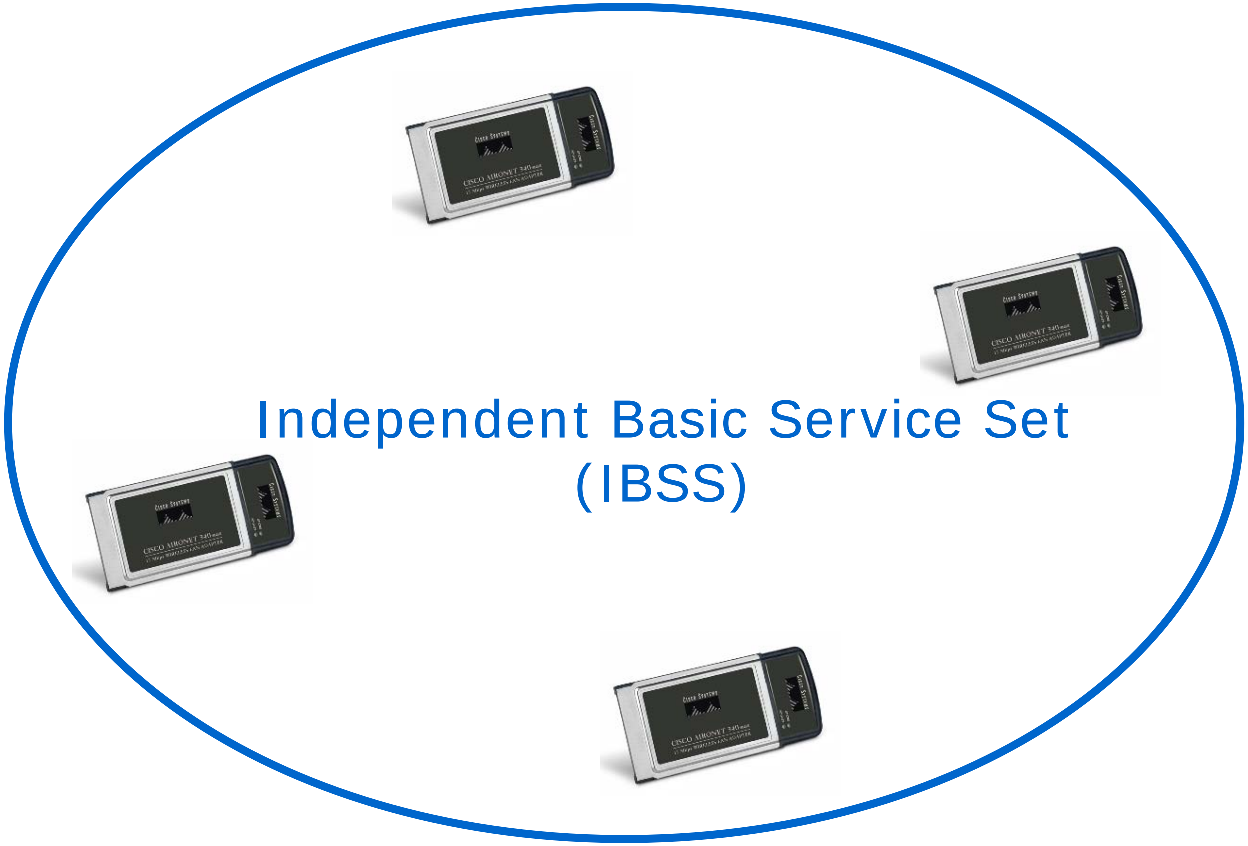


Example 802.11 System

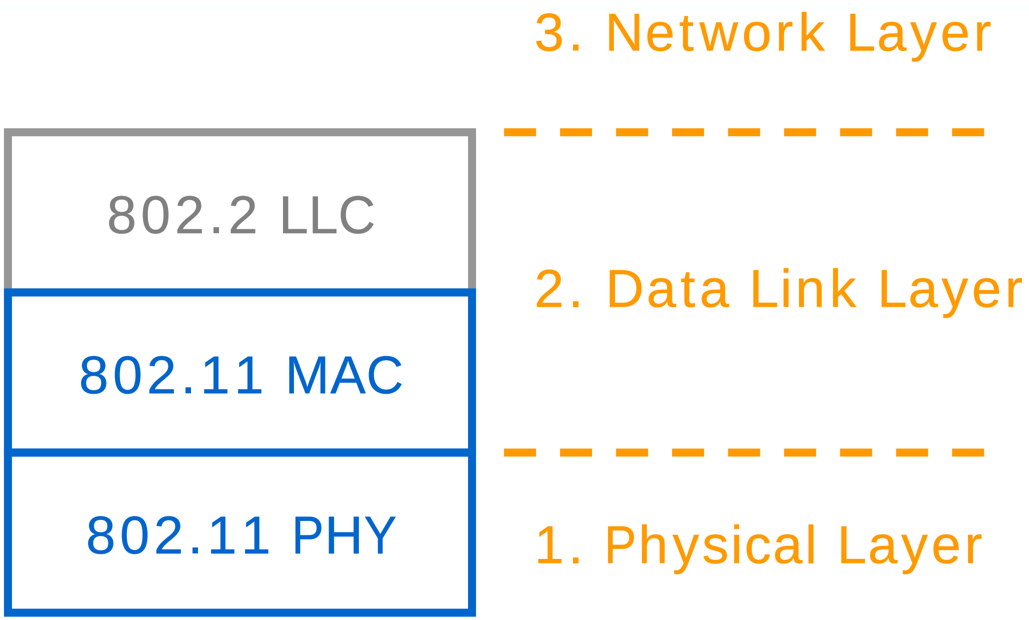


Ad hoc Mode

- Ad hoc mode: peer to peer communications between stations (or clients); No access points required

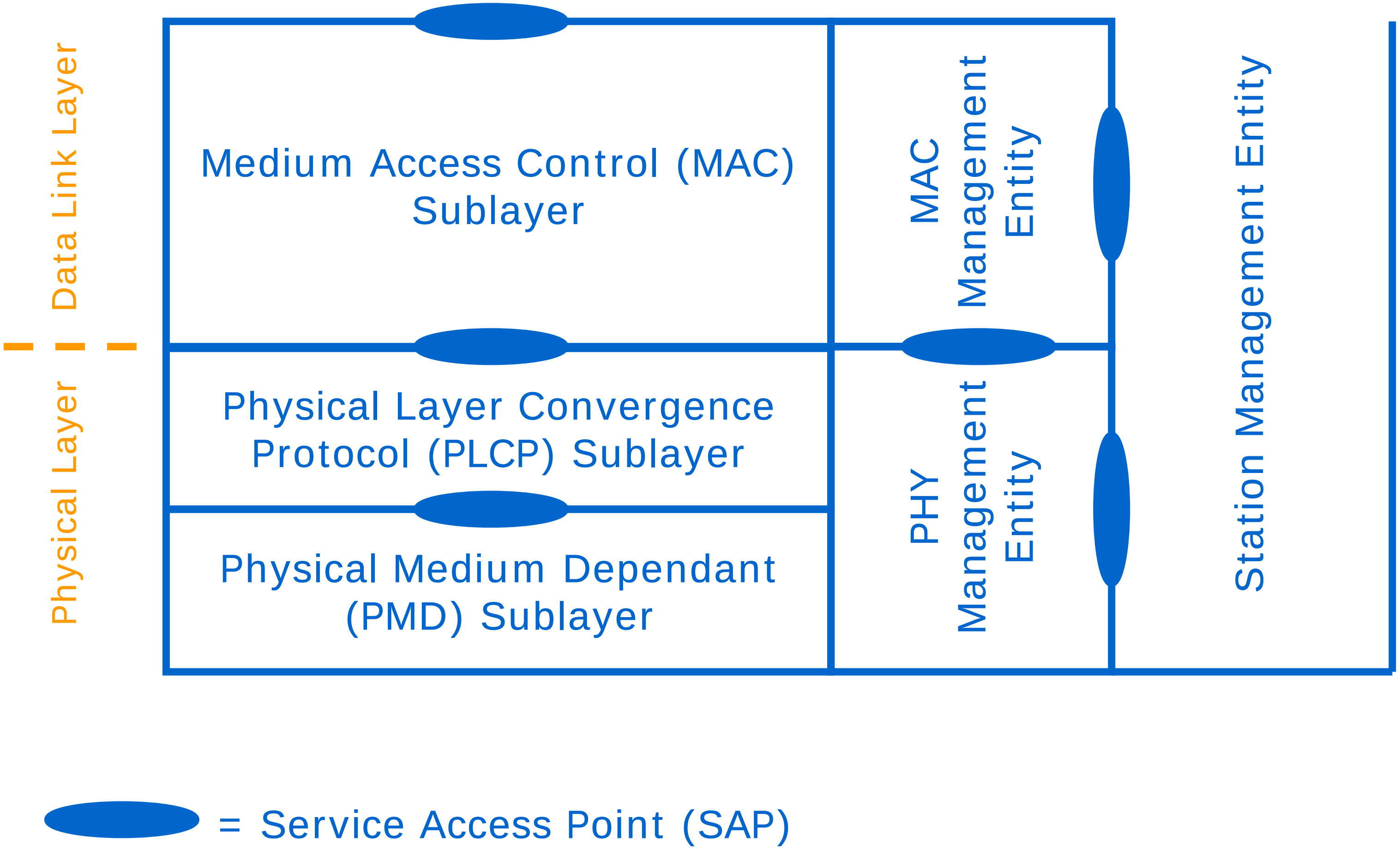


802.11 and OSI Reference Model



LLC = Logical Link Control
MAC = Medium Access Control
PHY = Physical

802.11 Layers and Interfaces



802.11 Physical Layer

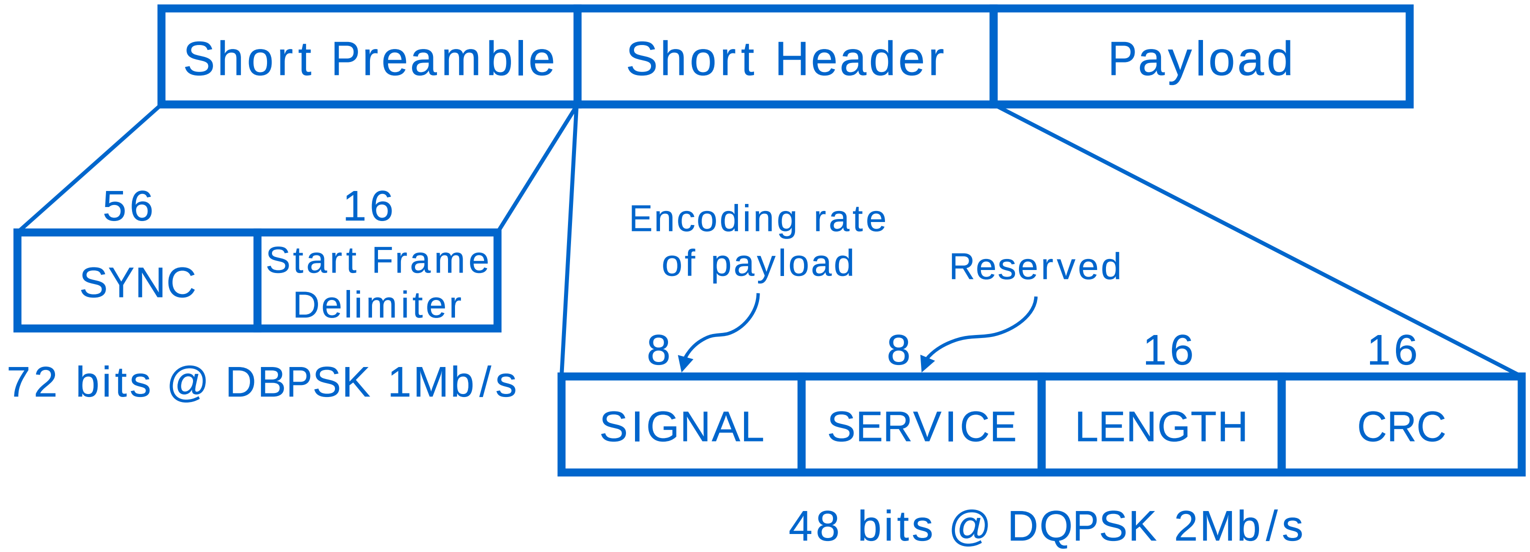
- Originally three physical layers in 802.11:
  1. Frequency Hopping Spread Spectrum (FHSS)
  2. Direct Sequence Spread Spectrum (DSSS)
  3. Infrared
- Radio transmission PHY layers operate in 2.4GHz ISM band
- Original data rates of 1Mb/s and 2Mb/s
- 1999: two new PHY layers standardised
  - 802.11a: OFDM at 5GHz, up to 54Mb/s
  - 802.11b: DSSS at 2.4GHz, up to 11Mb/s
- 2003: 11g - OFDM at 2.4Ghz, up to 54Mb/s, backwards compatible with 11b
- 2007?: 11n – Multiple Input Multiple Output (MIMO) antenna technology to reach speeds of 540Mb/s

- Note: 5GHz band is not officially approved for use in Thailand!

Radio Characteristics

	11b	11a	11g	11n
Rate	11Mb/s	54Mb/s	54Mb/s	540Mb/s
Frequency	2.4Ghz	5Ghz	2.4Ghz	5GHz
Physical	DSSS	OFDM	OFDM	OFDM, MIMO
Channels	11	12	11	?
Non-overlap	3	8	3	?
Range	20 – 300m	15 – 30m	25 – 75m	20-60m

Short 802.11b PHY Header

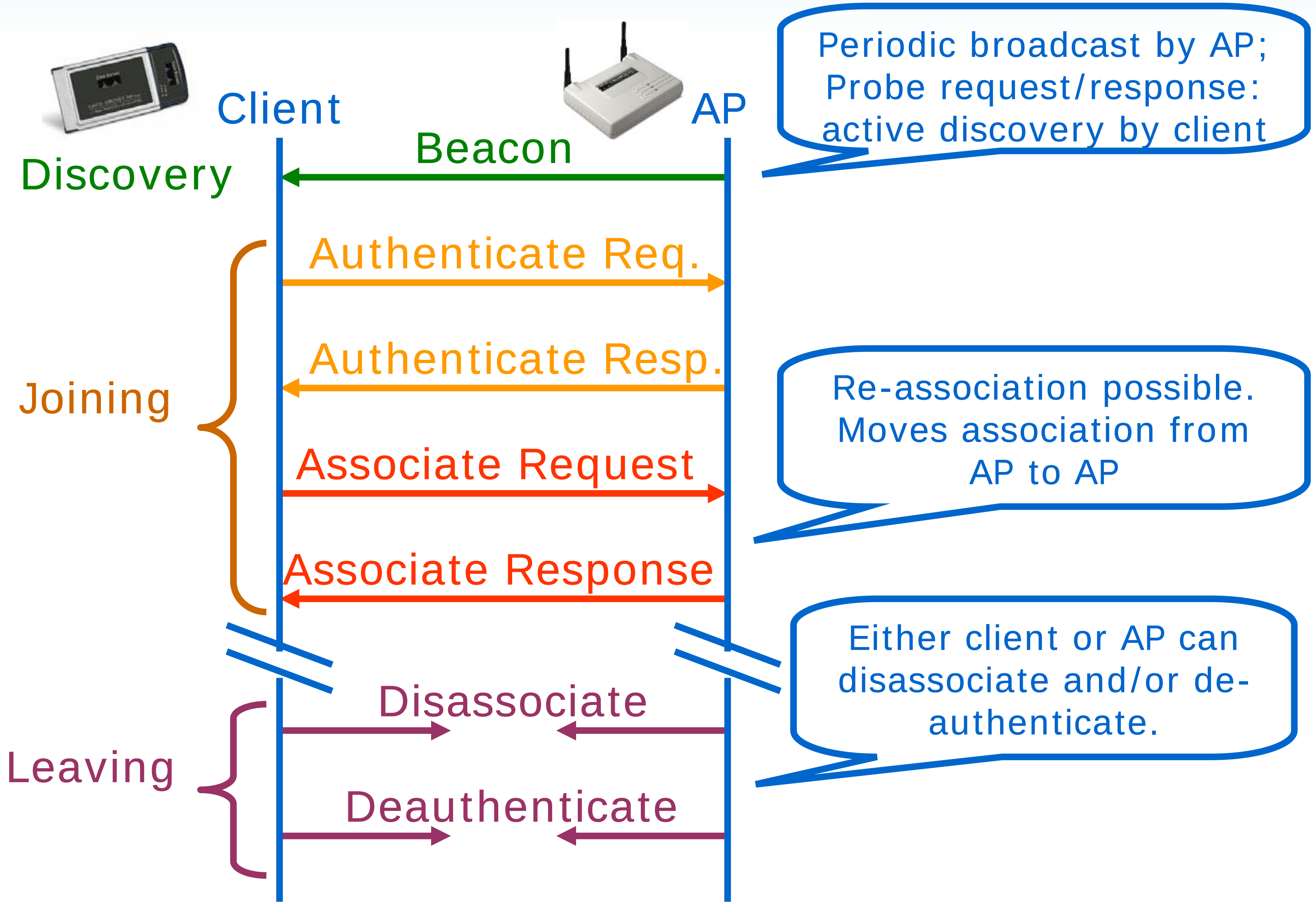


- Long preamble: 192μs overhead
- Short preamble option (802.11b): 96μs overhead
- Payload encoding at 1, 2, 5.5 or 11Mb/s
- Why are we interested in this detail?
  - Physical layer header introduces some overhead into frame

802.11 MAC Layer

- Defines management procedures for discovering, joining and leaving BSS/ESS
  - How does your laptop find an AP? How does it connect to the AP?
- Defines protocol for efficient and robust communication over wireless medium
  - How does your laptop share access with other surrounding laptops?
- Common across different physical layers
  - Same MAC used for 11a, 11b, 11g (although some parameter values change)

MAC Management



MAC Management Frames

- Discovery Frames
  - Beacon: periodic broadcast by AP (e.g. 10/sec)
  - Probe Request: active discovery by client
  - Probe Response: APs response to Probe Request
- Joining Frames
  - Authenticate Request (client) / Response (AP)
  - Associate Request (client) / Response (AP)
  - Reassociate Request (client) / Response (AP)
- Leaving Frames
  - De-authenticate (client or AP)
  - Disassociate (client or AP)
  - (these are notifications, not requests; no responses needed)

MAC Data Transfer

- Distributed Coordination Function (DCF)
  - Fair and efficient access for all clients
  - Carrier Sense Multiple Access (CSMA)
    - Clients contend for access to the medium
  - Collision Avoidance (CA)
  - DCF is mandatory in 802.11
- Point Coordination Function (PCF)
  - Contention (DCF) and contention-free periods
  - Contention-free period:
    - AP allocates radio resources to specific clients by polling stations currently on the polling list
  - Provide different levels of quality of service
  - PCF is optional in 802.11 (seldom implemented)

Distributed Coordination Function

- Two modes of operation:
  1. Basic Access mode
  2. RTS/CTS mode
- Basic access frames
  - DATA: user data passed from/to LLC
    - Header (+ tail) = 34 bytes
    - Payload: up to 2312 bytes (Ethernet max. 1500)
  - ACK: acknowledge receipt of DATA frame
    - Header ~ 14 bytes

802.11 DATA Frame

Octets:

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration	A1	A2	A3	Sequence Control	A4	Frame Body	FCS

Duration: Used to update NAV (see RTS/CTS)

Sequence Control: 12 bit sequence number, 4 bit fragment number

Addresses (A1-A4) depend on direction of frame

- Source Address, e.g. client address
- Destination Address, e.g. LAN client
- BSSID: AP address
- (A4 for wireless bridging)

Frame body: up to 2312 bytes (maximum for Ethernet 1500)

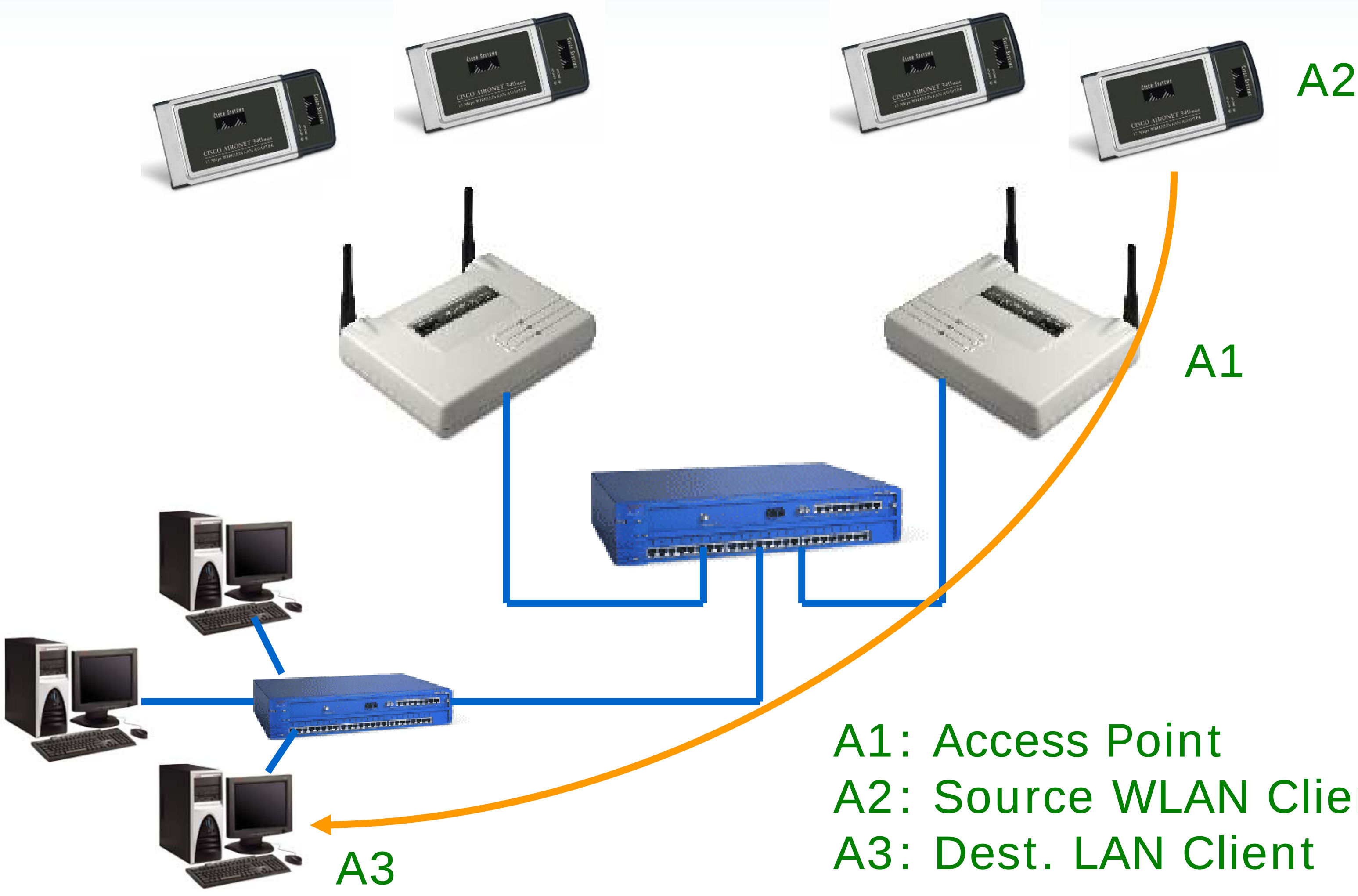
FCS: 32 bit CRC for error detection

DATA Frame Control field

Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order

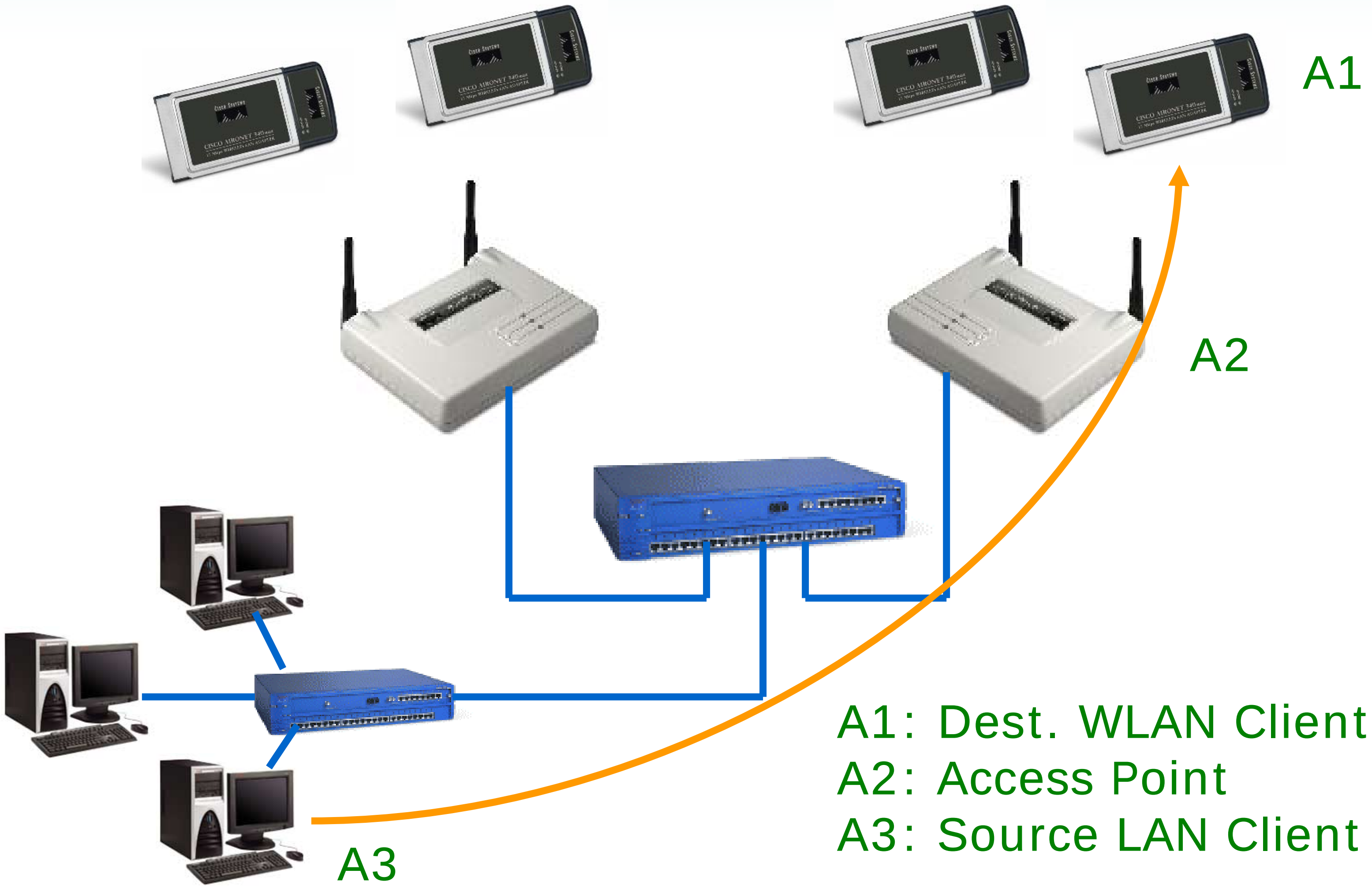
Field	Bits	Description
Protocol Version	2	Value: 0
Type	2	Control, data, management
Subtype	4	Probe Req., Data, Ack, …
To DS	1	00: Ad hoc; 10: Client to AP; 01: AP to client; 11: AP-AP (bridge)
From DS	1	
More Frag	1	More fragments to follow
Retry	1	Retransmission
Pwr Mgt	1	Power save mode
More Data	1	Power save or CFP
WEP	1	On or Off
Order	1	StrictlyOrdered/OrderableMulticast

Addressing in 802.11 – To LAN

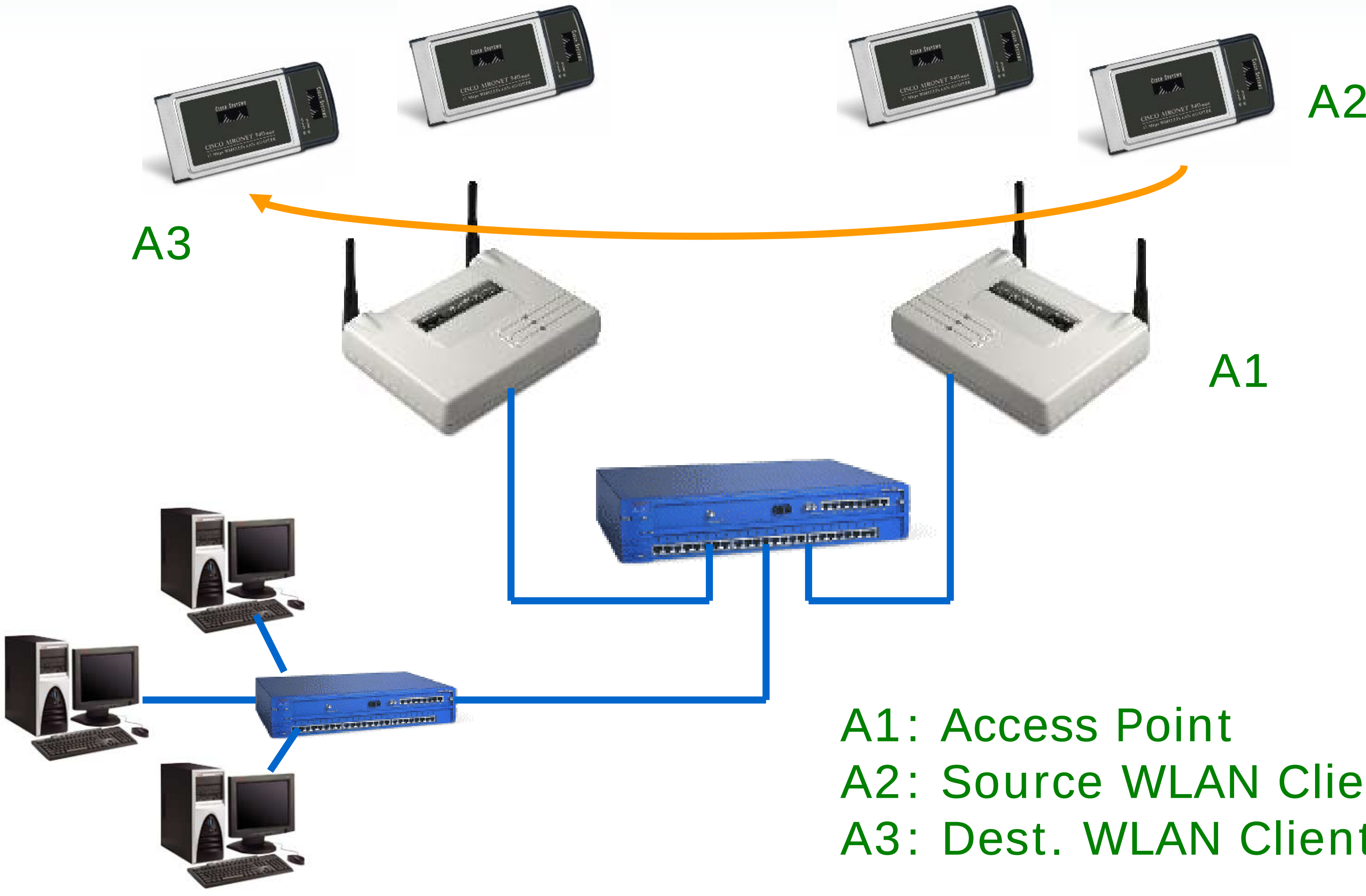


A1: Access Point
A2: Source WLAN Client
A3: Dest. LAN Client

Addressing in 802.11 – From LAN



Addressing in 802.11 – To WLAN



A1: Access Point
A2: Source WLAN Client
A3: Dest. WLAN Client

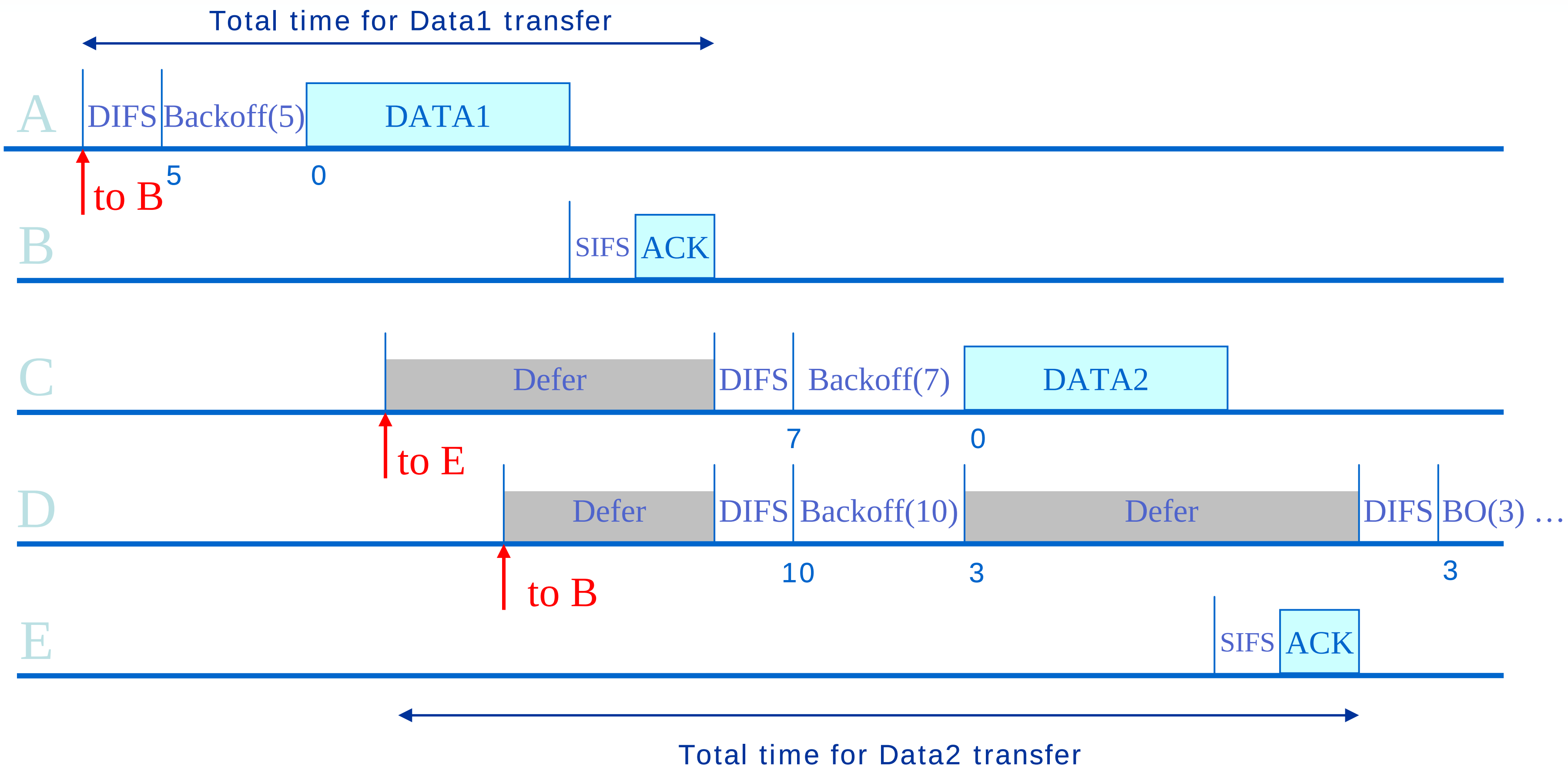
Basic Access Operation

- Clients and APs follow the same set of rules
  - Refer to them as stations
- When station has data ready to send:
  1. Medium must be idle for period of DCF Inter Frame Space (DIFS)
  2. After DIFS, medium must be idle for Backoff period
  3. When backoff complete, transmit DATA frame
  4. Upon receipt of ACK frame, data transfer is complete
- If medium becomes busy during DIFS:
  - Wait until idle, then restart from point 1 above
- If medium becomes busy during Backoff:
  - Suspend backoff counter, wait until idle, then restart from point 1 above
  - Continue backoff from where it was suspended

Basic Access Operation

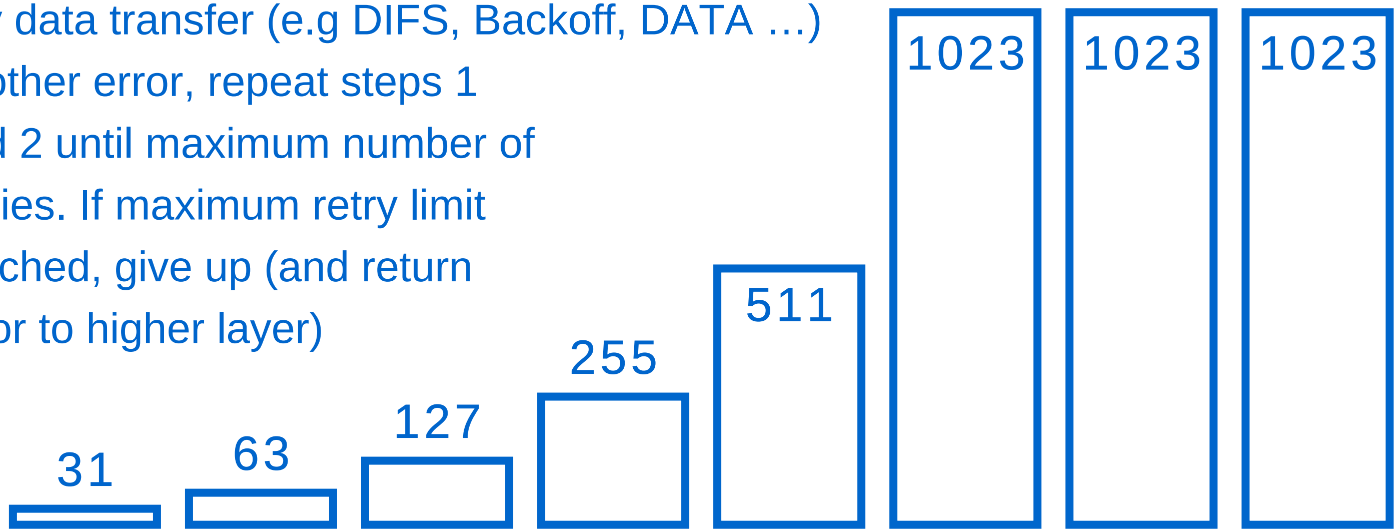
- Interframe Spaces
  - DCF IFS (DIFS): period that the medium must be sensed idle before starting backoff
  - Short IFS (SIFS): period to wait between frame transmissions during data transfer
    - E.g. Receiver waits SIFS before sending ACK
    - SIFS is always less than DIFS
- Backoff Period
  - R = random integer between 0 and CW
  - Backoff Period = R x SlotTime
  - CW: Contention Window size, initially CWmin
  - SlotTime: defined for PHY (e.g. 20 μs for 11b)
  - Choosing a random Backoff period minimises collisions after two or more stations defer
  - Provides fair access to all nodes (on average, every station gets same chance of winning access)

DCF Basic Access Timing Diagram



Collisions and Contention Window

- Collisions may still occur when random backoff is used
  - Two stations chose same random number of slots to backoff, therefore transmit at same time
  - Stations ready to transmit cannot hear each other (therefore will think medium is idle when its actually busy)
- If transmitting station doesn't receive ACK after ACKTimeout period, assume an error:
  - Double CW (until it reaches CWmax)
  - Retry data transfer (e.g DIFS, Backoff, DATA …)
  - If another error, repeat steps 1
  - and 2 until maximum number of
  - retries. If maximum retry limit
  - reached, give up (and return
  - error to higher layer)



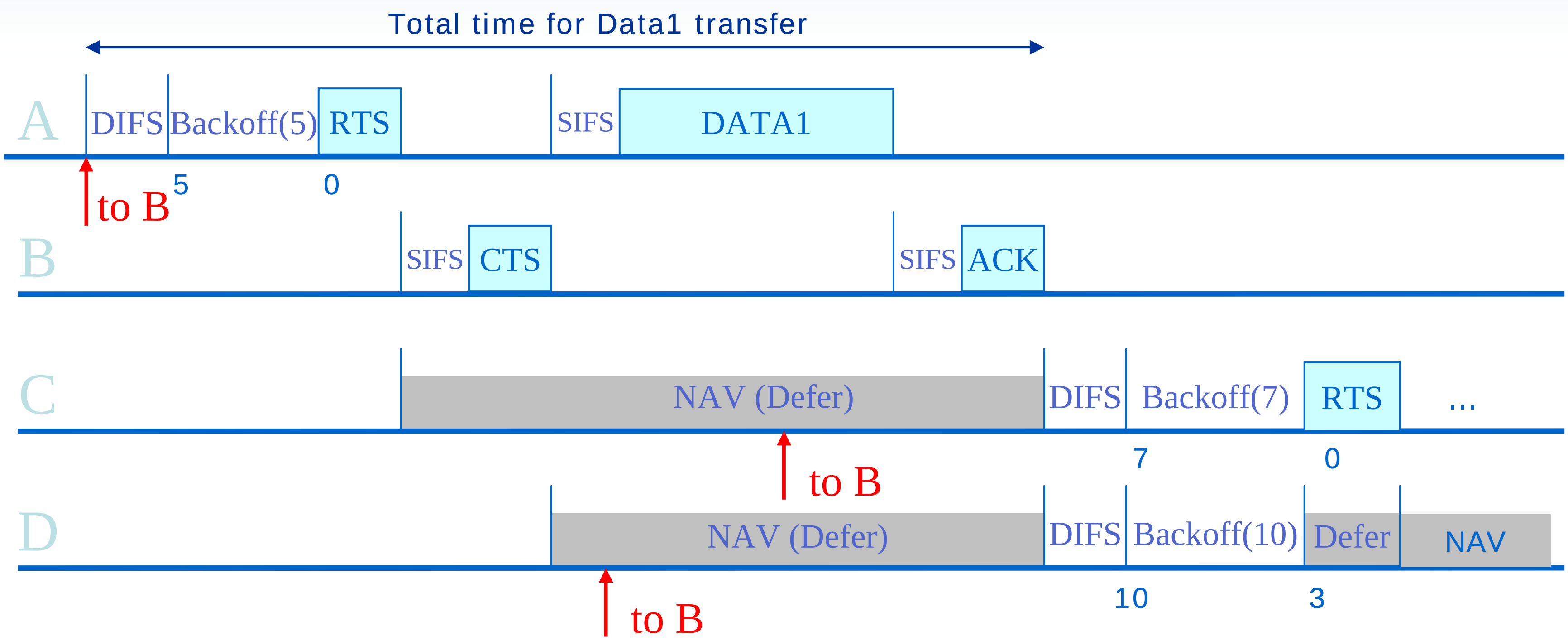
RTS/CTS Frames

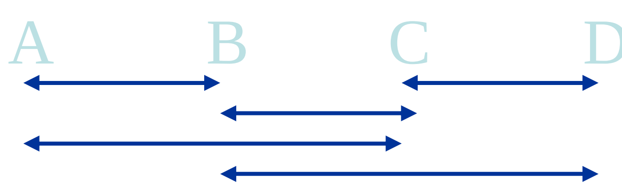
- RTS Frame
  - Request To Send
  - Sent to intended recipient of DATA
  - Notifies all stations of upcoming DATA frame
  - Size ~ 20 bytes
- CTS Frame
  - Clear To Send
  - Response from the recipient of RTS
  - Notifies all stations of upcoming DATA frame
  - Size ~ 14 bytes
- DATA and ACK also used

RTS/CTS Operation

- Normal access procedures applied to sending RTS frames
  - e.g. sense medium idle for DIFS then backoff
- All stations receiving RTS or CTS set their Network Allocation Vector (NAV) based on Duration field in the RTS or CTS frame
  - NAV keeps track of when the medium is in use
  - After the NAV period, other stations can attempt transmission (normal backoff rules apply)

RTS/CTS Timing Diagram





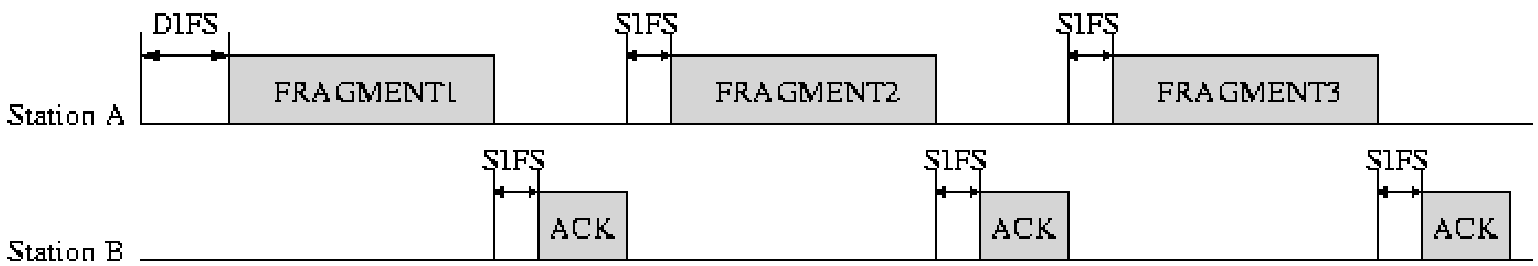
A and D are out of range!
Therefore D does not hear
RTS, but does hear CTS

Basic Access vs. RTS/CTS

- RTS Threshold: frames larger than this are sent using RTS/CTS
  - Overhead of RTS/CTS justified with large payloads
- In highly loaded networks, RTS/CTS also beneficial
  - Lower RTS Threshold
- With RTS/CTS, collisions nearly independent of the number of stations
  - Lower RTS Threshold when many stations, or varying numbers of stations
- With RTS/CTS, avoid collisions due to hidden terminals
  - However, may increase exposed terminals

Fragmentation

- Unicast frames are fragmented if their length exceeds Fragmentation Threshold
- All fragments are sent within one call of the access procedure (Basic or RTS/CTS)
- Each individual fragment is ACKed



MAC Performance

- Physical layer offers raw data rate (e.g. 11Mb/s in 802.11b)
- MAC introduces overheads to provide addressing, reliability and management:
  - Frame headers
  - Control frames: ACK, RTS, CTS, …
  - Interframe spaces
  - Backoffs
  - Collisions and retransmissions

IEEE 802.11 MAC Parameters

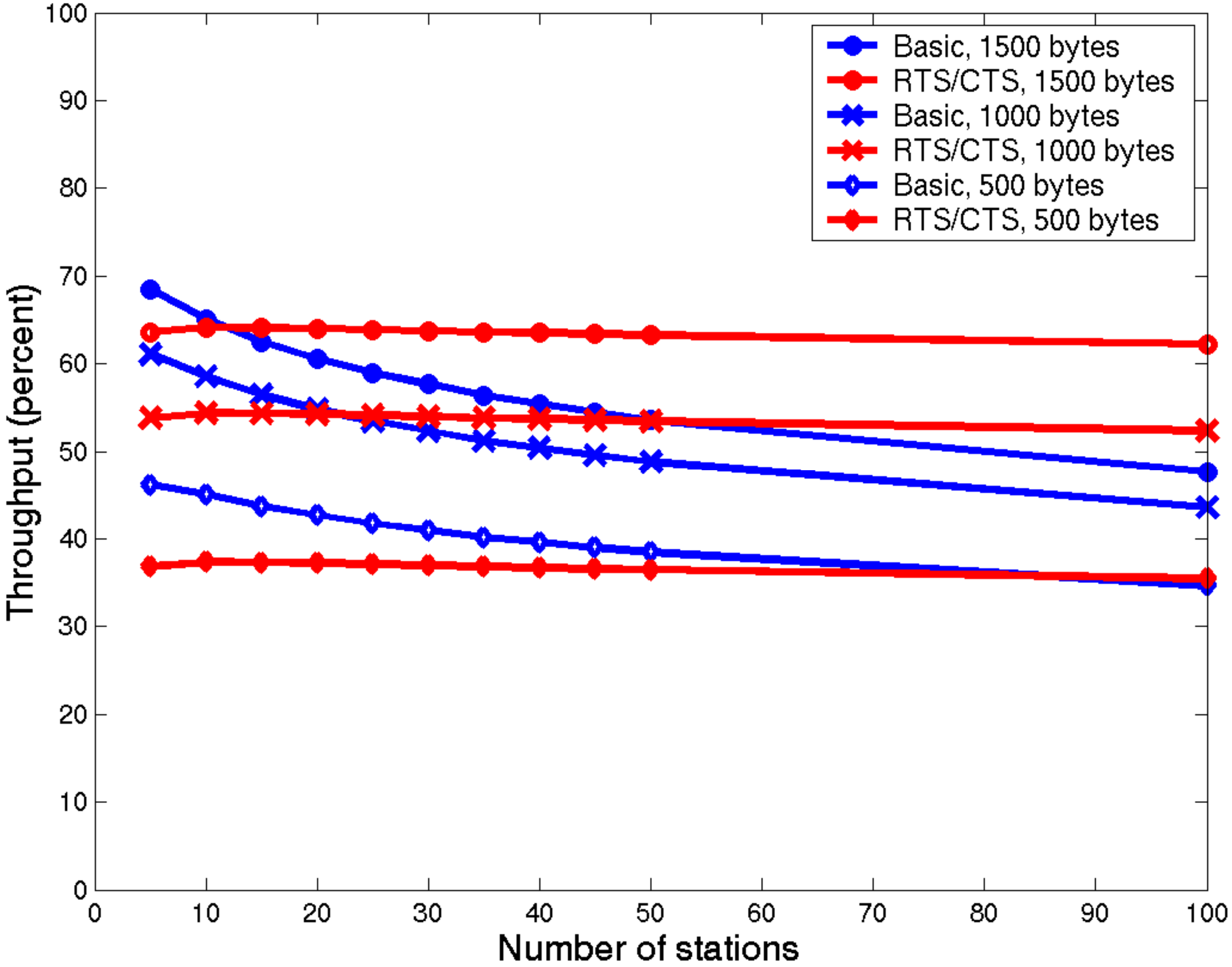
Parameter	802.11b	802.11a	802.11g
DIFS	50μs	34 μs	28 μs
SIFS	10 μs	16 μs	10 μs
SlotTime	20 μs	9 μs	9 μs
CWmin	31	15	15
CWmax	1023	1023	1023

Rough Throughput Calculation

- Assume 1500 byte payload using Basic Access, no collisions or deference!
- Best case (on average) for 802.11b (11Mbit/s)
  - Time = DIFS + AverageBackoff + DATA + SIFS + ACK
  - = 50 + 16*20 + (1500+34)*8/11 + 10 + 10
  - = 1506 usec
  - Throughput = 1500 bytes/1506usec
    - = 7.97Mbit/s
- Best case for 802.11a (54Mbit/s)
  - Time = 34 + 16*9 + (1500+34)*8/54 + 10 + 14*8/54
    - = 417 usec
  - Throughput = 1500bytes/417 usec
    - = 28.50Mbit/s
- RTS/CTS: need to add 2 x SIFS + RTS + CTS time
  - 11b throughput: 6.65Mb/s
  - 11g throughput: 24.69Mb/s

Theoretical Throughput

802.11b Example
10 clients per AP
Basic Access
1000 byte payload
600kb/s per client



Realistic Throughput

- Take into account:
  - Collisions, retransmissions
  - IP, TCP and other protocol overheads
  - Varying sizes of payload
  - About 10 nodes per AP
- All IEEE 802.11b clients; 11b AP
  - 3 to 5 Mb/s per cell
- Mixture of IEEE 802.11g and 11b clients; 11g AP
  - 10 to 15 Mb/s per cell

Security in Wireless LANs

- Original 802.11
  - Authentication
    - Ensure the client has permission to access the network
    - Originally used a shared secret key (Wired Equivalent Privacy, WEP)
      - Client and AP must be pre-configured with the same secret key
  - Confidentiality
    - Ensure the communications between client and AP cannot be overheard
      - WEP shared secret key also used for encryption
  - WEP has several limitations
    - In practice, if an attacker can collect several GB of traffic between a client and AP, it can discover the secret key
- Enhanced Wireless LAN Security
  - Wireless Protected Access (WPA): increase key size and solve WEP problems
  - IEEE 802.11i: complete security architecture tat can use other network security mechanisms

Wireless LAN Design Issues

- How many users per Access Point?
  - Performance per user drops as number of users increase
  - But we want to minimise number of APs
    - Costly devices, costly to install and manage
    - Handover between APs may become inefficient
- Basic Access versus RTS/CTS – What RTS threshold?
  - Basic Access is more efficient if few collisions (unless hidden terminals)
  - RTS/CTS helps avoid hidden terminals
- How to cover a large area?
  - Cellular coverage: many small cells or a few large cells?
  - Avoid interference between cells
    - Use different frequencies, but only 3 non-overlapping frequencies available

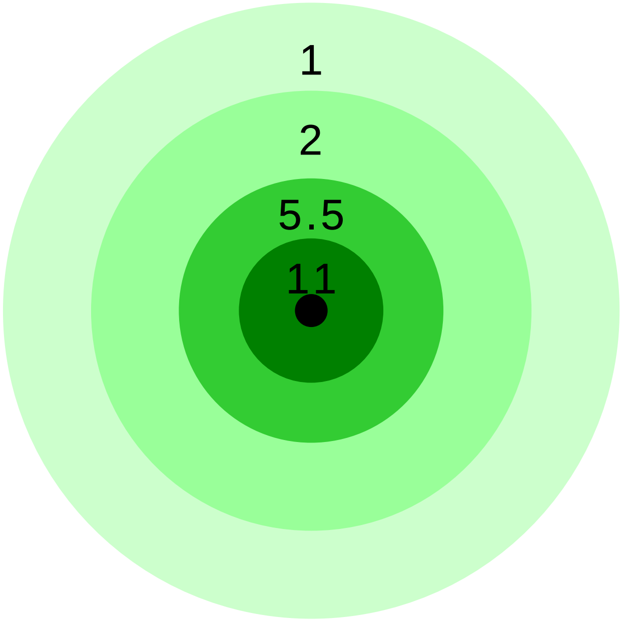
Wireless LAN Design Issues

- How do we secure the network?
  - Need to authenticate users (usually to a central network authentication server)
  - Need encryption: Layer 2 (802.11 WEP, WPA, 11i) or other layer (IPsec, VPN, …)
- How do we give priority to users and applications?
  - Voice calls get priority over data traffic
  - Quality of service management on APs; but what about network wide?

Wireless LAN Capacity Issues

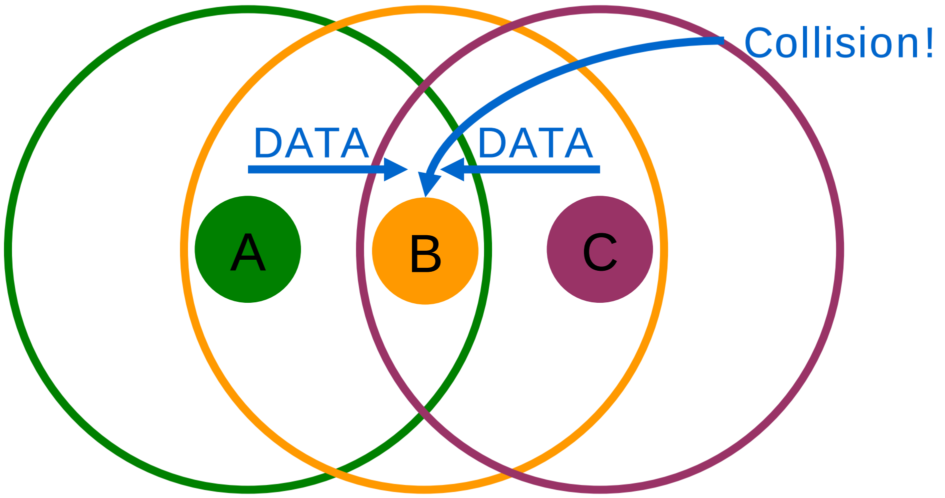
Data Rates

- Automatic Rate Fallback (ARF)
  - Devices switch between data rates based on signal quality
  - 1, 2, 5.5, 11 Mb/s
  - Further from AP, lower data rate

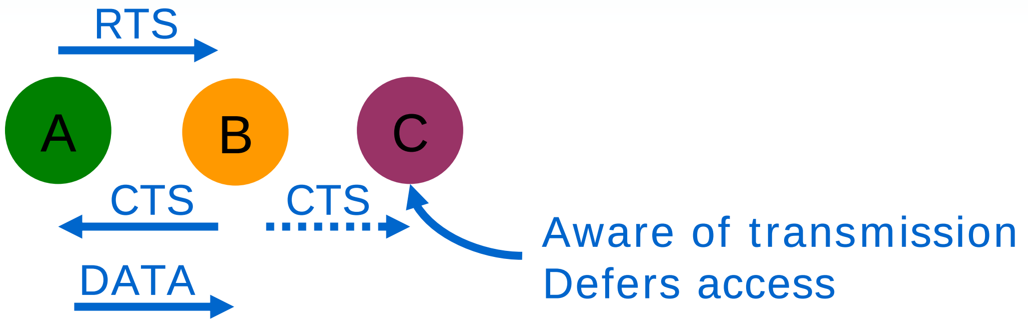


Hidden Terminal Problem

- A and C can't hear each other (C is hidden from A)
- Following MAC rules: A and C can transmit simultaneously
- Result: collisions at B
  - Significant capacity reduction



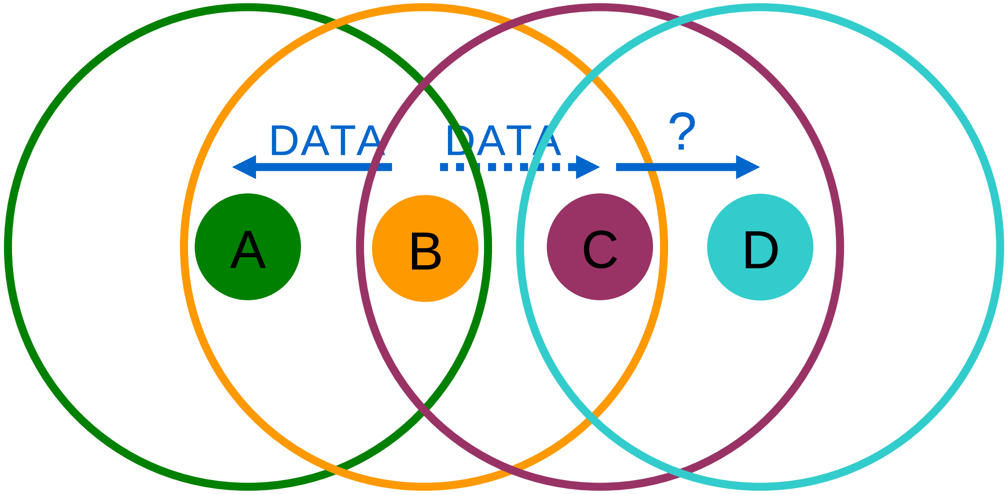
RTS/CTS and Hidden Stations



- Basic Access: collision probability depends on DATA size, 100’s – 1500 bytes
- RTS/CTS: collision probability depends on RTS size, ~ 14 bytes

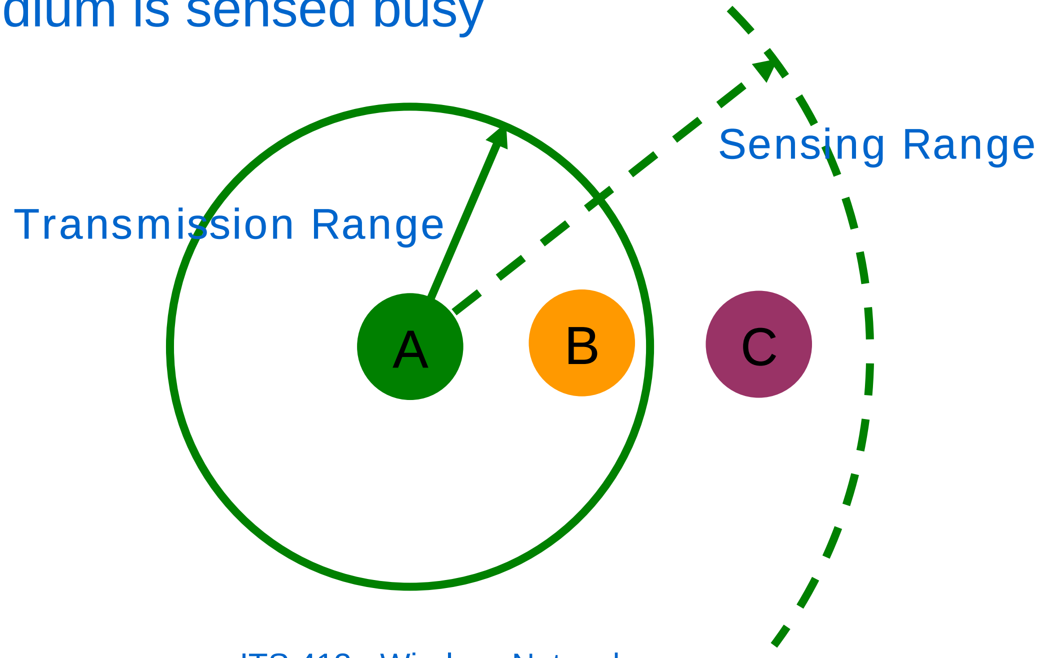
Exposed Terminal Problem

- A can only hear B; D can only hear C
- 802.11 MAC: If B sends to A, C withholds from sending
- BUT C could safely send to D
- Stations waste opportunities to send



Transmission & Sensing Ranges

- Transmission Range:
  - Maximum distance from a station at which successful data transmission can occur
- Sensing Range:
  - Maximum distance from a station at which signals can be heard, i.e. the medium is sensed busy



Device Characteristics and Options

- Transmit Power
  - Range from 1mW up to several hundred mW
  - May have regulatory (legal) limitations in some countries
  - Some devices you can control Tx power, others you cannot
- Receive Sensitivity
  - What is the lowest signal that a receiver can decode frames?
  - The lower value the better receiver
- Antenna Pattern
  - Clients are usually omni-directional (but not always)
  - APs may be controlled by network designer
- Data Rates
  - Fixed at a certain rate (e.g. 54Mb/s) or allow ARF
- Transmission Range
  - In the real world, very hard to control!