

WIRELESS LOCAL AREA NETWORK (WLAN)

Aynishet Alemu

WLAN Overview

- A wireless local area network (WLAN) is a data communications system that allows devices to connect to each other wirelessly.
- WLANs are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards.
- WLANs can be used to connect devices such as computers, printers, and smartphones to each

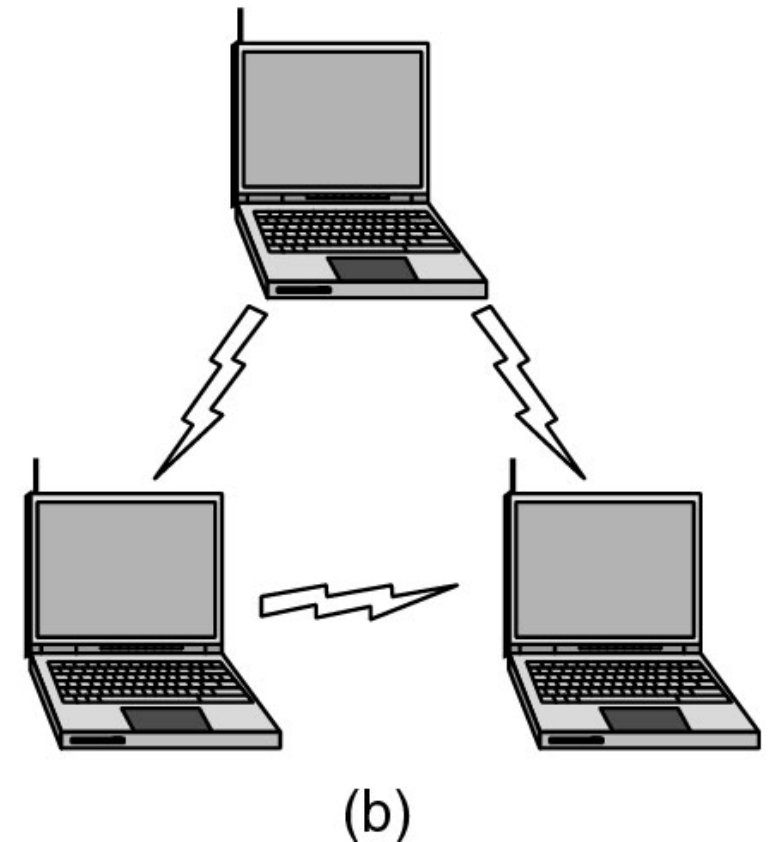
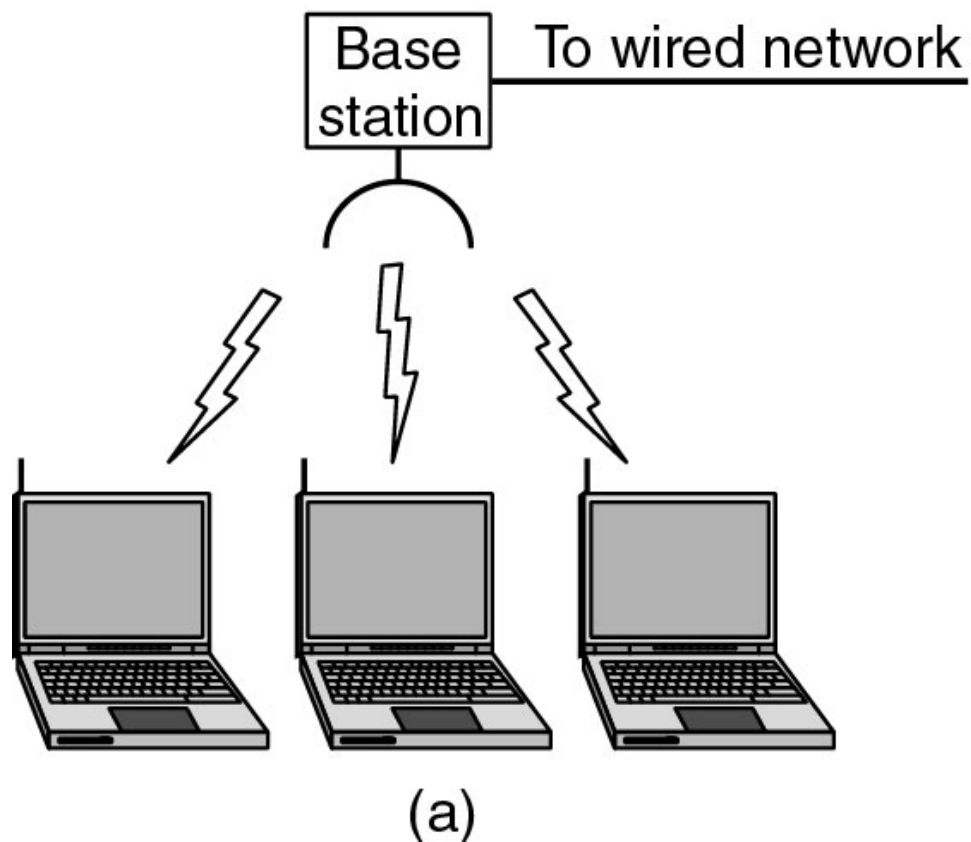
WLAN Overview

- A wireless local area network (WLAN) is a flexible data communications system implemented as an extension to, or as an alternative for, a wired LAN.
- Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections.
- The radio waves are typically in the 2.4 GHz or 5 GHz frequency bands.

WLAN Overview

- WLANs can be set up in a variety of ways.
 - The most common type of WLAN is an **infrastructure network**.
 - In an infrastructure network, devices connect to a central device called an access point.
 - The access point then connects the devices to each other and to the Internet.
 - **Another type of WLAN is an ad hoc network.** In an ad hoc network, devices connect to each other directly without the need for an access point. Ad hoc networks are often used for temporary purposes, such as when a group of people are working together on a project.

Wireless LANs

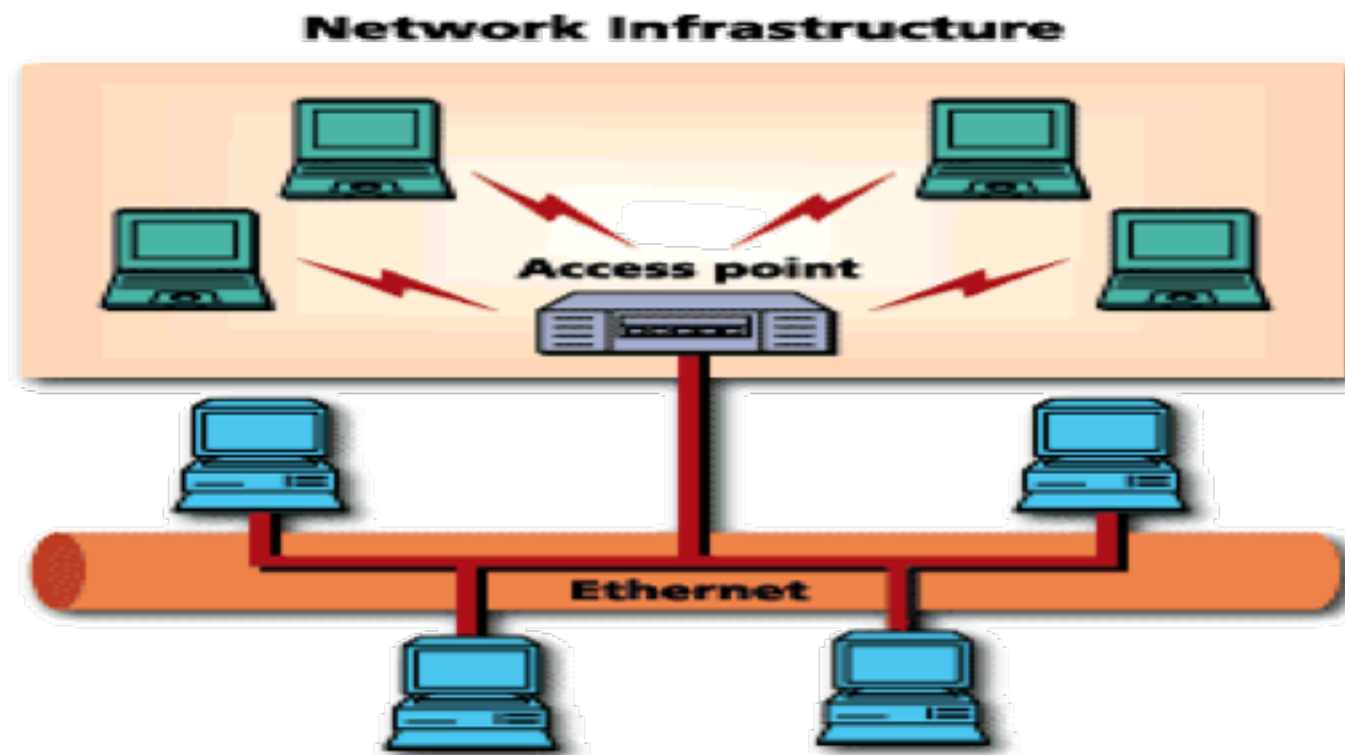


(a) Wireless networking with a base station. (b) Ad hoc networking.

Common Topologies

The wireless LAN connects to a wired LAN

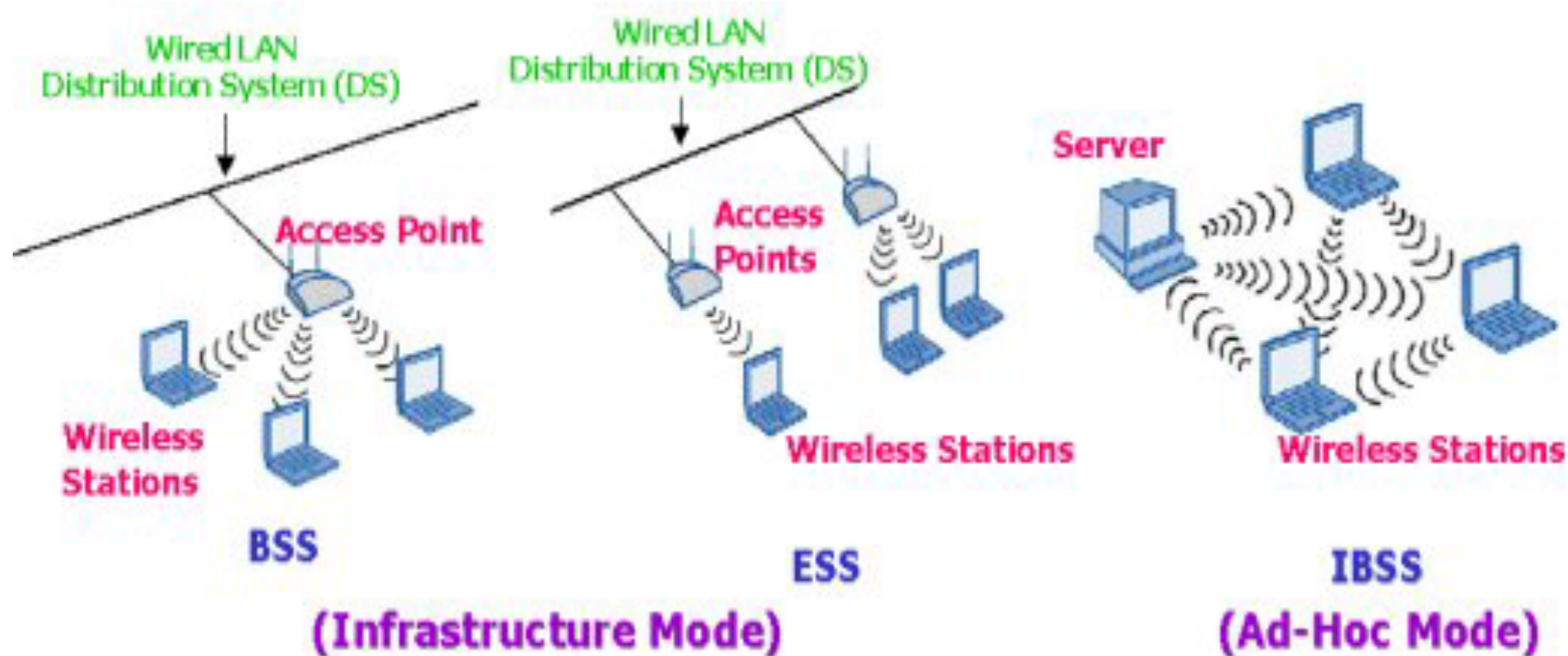
- There is a need of an access point that bridges wireless LAN traffic into the wired LAN.
- The access point (AP) can also act as a repeater for wireless nodes, effectively doubling the maximum possible distance between nodes.



Wireless Local Area Network - WLAN

WLAN Architecture

- **Infrastructured Wireless LAN**



- **Ad-Hoc LAN**

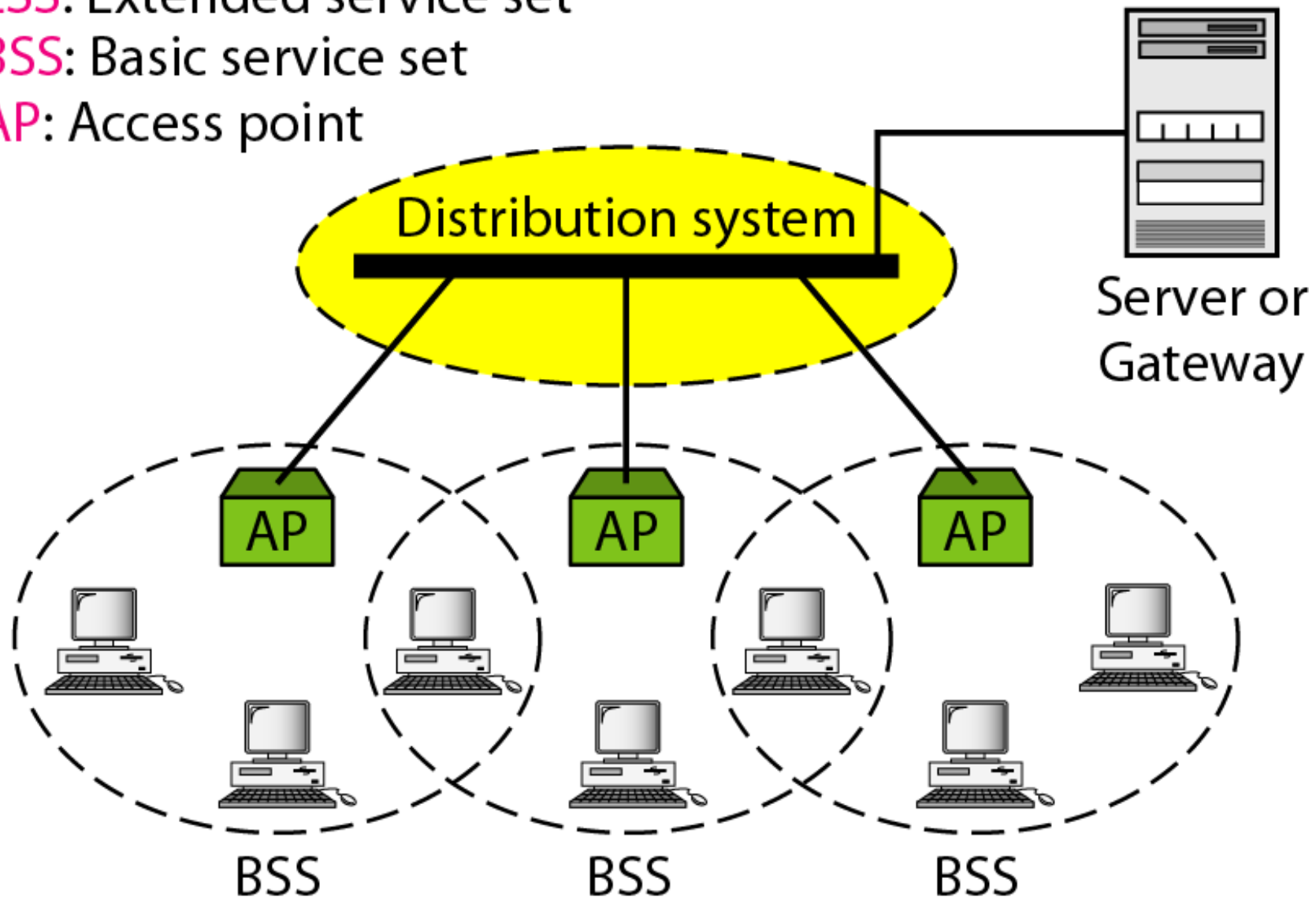
Independent Basic Service Set Network

Extended Service Sets (ESSs)

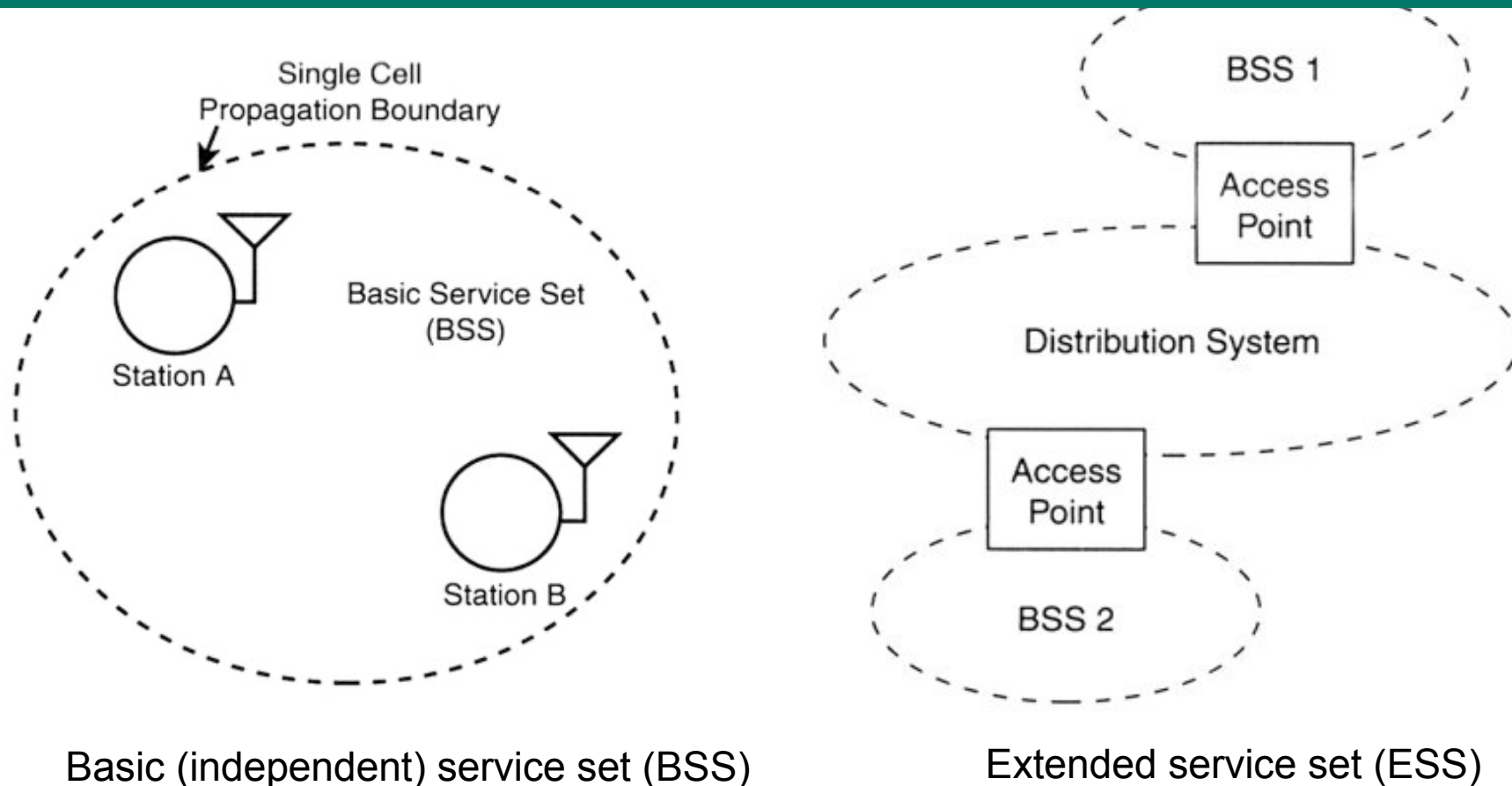
ESS: Extended service set

BSS: Basic service set

AP: Access point



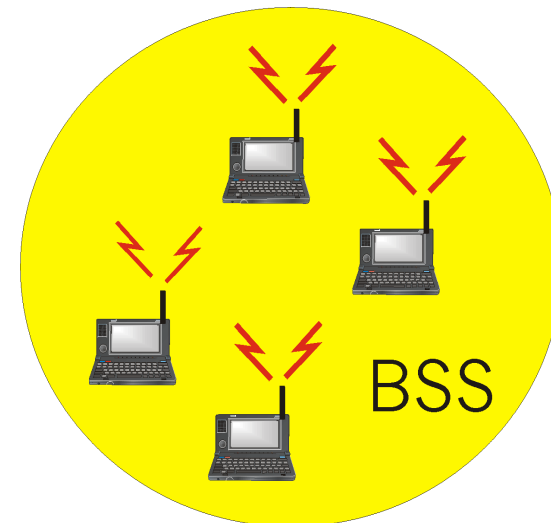
BSS and ESS



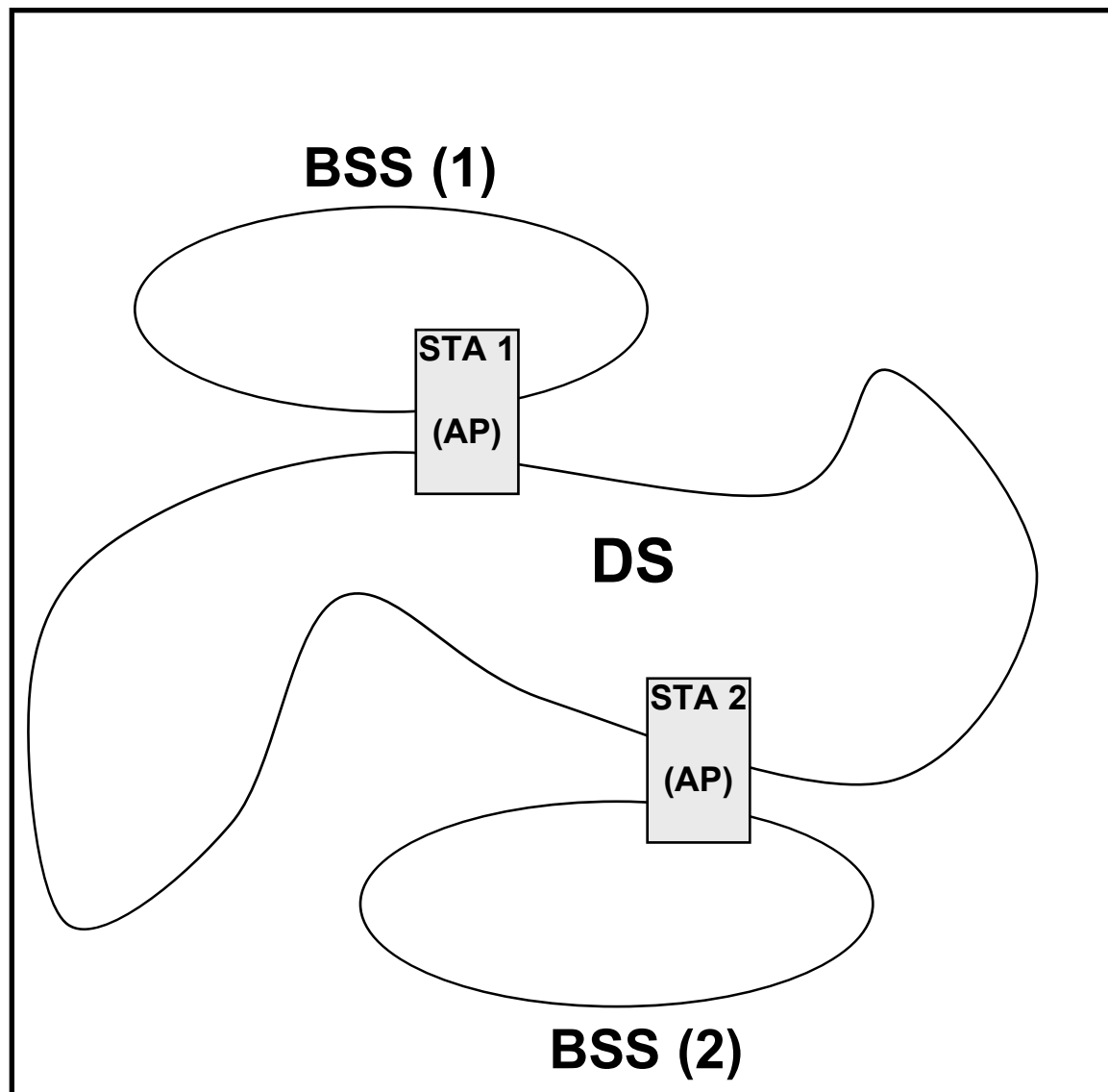
- In ESS multiple access points connected by access points and a distribution system as Ethernet
 - BSSs partially overlap
 - Physically disjoint BSSs
 - Physically collocated BSSs (several antennas)

Ad Hoc Wireless Networks

- IEEE 802.11 stations can dynamically form a group without AP
- Ad Hoc Network: **no pre-existing infrastructure**
- Applications: “laptop” meeting in conference room, car, airport; interconnection of “personal” devices (see bluetooth.com); battlefield; pervasive computing (smart spaces)
- IETF MANET
(**M**obile **A**d hoc **N**ETworks)
working group

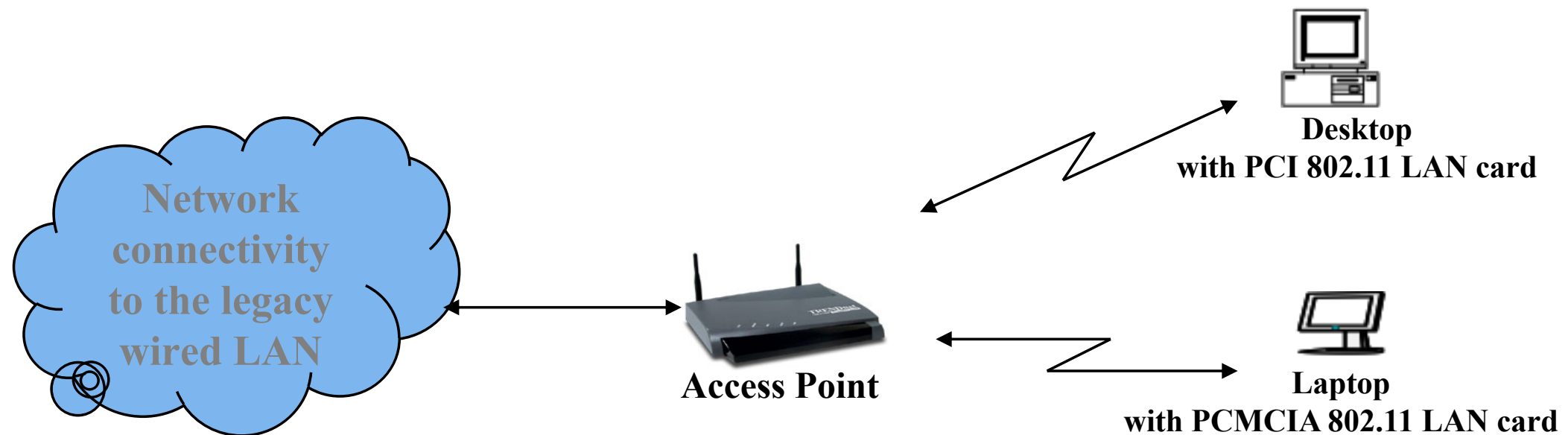


Components of 802.11



- A MAC, PHY layer specification
- Should serve *mobile* and *portable* devices
 - What is mobile?
 - What is portable?
- Should provide transparency of mobility
- Should appear as 802 LAN to LLC (“*messy MAC*”)
- Basic Service Set (BSS)
- Distribution System (DS)
- Station (STA)
- STA that is providing access to Distribution System Service (DSS) is an Access Point (AP)
- 802.11 supports Ad-hoc networking
- Provide “*link level security*”

802.11 Wireless LAN



- Provides network connectivity over wireless media

- An Access Point (AP) is installed to act as Bridge between Wireless and Wired Network

- The AP is connected to wired network and is

Wireless Local Area Network - WLAN

WLAN Standards

- The IEEE 802.11 standards define the physical layer and medium access control (MAC) layer protocols for WLANs.
- The physical layer defines the characteristics of the radio waves that are used to transmit data, such as the frequency band, modulation scheme, and data rate.
- The MAC layer defines the protocols that are used to control access to the wireless medium, such as

Physical Layer

- Medium: The physical medium over which the data is transmitted. This can be a wired medium, such as copper or fiber optic cable, or a wireless medium, such as radio waves.
- Signaling: The method used to encode the data into a signal that can be transmitted over the medium. This can be a digital signal, such as a series of bits, or an analog signal, such as a continuous wave.
- Data rate: The speed at which the data is transmitted. This is measured in bits per second

Data Link Layer

- Framing: The process of dividing the data into frames, which are the basic unit of data transmission.
- Each frame contains a header, which contains information such as the source and destination addresses, and a payload, which contains the actual data.
- Addressing: The process of assigning unique addresses to each device on the network. This allows devices to identify each other and

WLAN vs Ethernet

- WLAN (Wireless Local Area Network) and Ethernet are different in terms of their physical and data link layers. Let's compare them in these aspects:
- Physical Layer:
- **1. Medium:** Ethernet uses physical cables, such as twisted-pair copper cables (e.g., Cat5e or Cat6) or fiber optic cables, to transmit data. WLAN, on the other hand, uses wireless signals to transmit data over

WLAN vs Ethernet

- 3. Mobility: Ethernet connections are typically stationary and require physical connectivity to the network. WLAN allows mobility since it is wireless, enabling devices to connect and move within the coverage area.

WLAN vs Ethernet

- Data Link Layer:
- 1. Access Method: Ethernet typically uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the access method. It means devices listen to the network before transmitting and handle collisions if multiple devices transmit simultaneously. WLAN uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which includes mechanisms to avoid collisions in the wireless medium

WLAN vs Ethernet

- 2. Data Rate: Ethernet offers higher data rates, ranging from 10 Mbps (Ethernet) to 10 Gbps (10 Gigabit Ethernet), and even higher with newer standards. WLAN data rates vary depending on the specific wireless standard (e.g., 802.11b/g/n/ac/ax), ranging from a few Mbps to several Gbps.

WLAN vs Ethernet

- 3. Error Handling: Ethernet provides reliable communication by using error detection and correction mechanisms at the data link layer, such as the cyclic redundancy check (CRC). WLAN also employs error detection mechanisms, but the reliability may be affected by interference, signal attenuation, or environmental factors.

WLAN vs Ethernet

- 4. Security: Ethernet networks are typically considered more secure since physical access is required to intercept the communication. WLAN networks can be vulnerable to unauthorized access if not properly configured with encryption and authentication mechanisms, such as WPA2/WPA3.

WLAN vs Ethernet

- It's worth noting that both WLAN and Ethernet can coexist in the same network infrastructure, with WLAN access points connected to the wired Ethernet backbone to provide wireless connectivity to devices. The choice between WLAN and Ethernet depends on factors like mobility requirements, data rate needs, physical constraints, and security conside

Multiple Access with Collision Avoidance (CSMA/CA)

- Multiple Access with Collision Avoidance (CSMA/CA) is an access method used in wireless networks, particularly in WLANs (Wireless Local Area Networks). It is a protocol that helps regulate access to the shared wireless medium, minimizing the chances of collisions when multiple devices attempt to transmit data simultaneously.

Multiple Access with Collision Avoidance (CSMA/CA)

- In CSMA/CA, before a device transmits data, it performs a process called "carrier sense," where it listens to the wireless medium to check if it is idle. If the medium is idle, the device can proceed with transmission. However, if the medium is already in use by another device, the device defers its transmission and waits for the medium to become idle.

Multiple Access with Collision Avoidance (CSMA/CA)

- To further avoid collisions, CSMA/CA includes a "collision avoidance" mechanism. This mechanism involves the use of a "Request to Send" (RTS) and "Clear to Send" (CTS) exchange between the transmitting device and the receiving device. When a device wants to transmit data, it first sends an RTS frame to the intended receiver, requesting permission to transmit. The receiver responds with a CTS frame, granting permission to transmit. Other devices in the vicinity, upon

Multiple Access with Collision Avoidance (CSMA/CA)

- CSMA/CA also implements a random backoff mechanism to handle situations where multiple devices sense the medium as idle simultaneously. In such cases, each device waits for a random period of time before attempting to transmit again.
- Overall, CSMA/CA is designed to avoid collisions in wireless networks by listening to the medium, requesting permission to transmit, and using random backoff times. This protocol helps ensure more reliable and efficient data transmission in WLANs. This random backoff helps distribute the transmission attempts more evenly, reducing the likelihood of collisions.

Multiple Access with Collision Avoidance (CSMA/CA)

- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is a protocol used in wireless networks to manage access to the wireless medium and avoid collisions between multiple devices trying to transmit simultaneously. There are different types of CSMA/CA based on their specific characteristics and applications. Here are some examples:

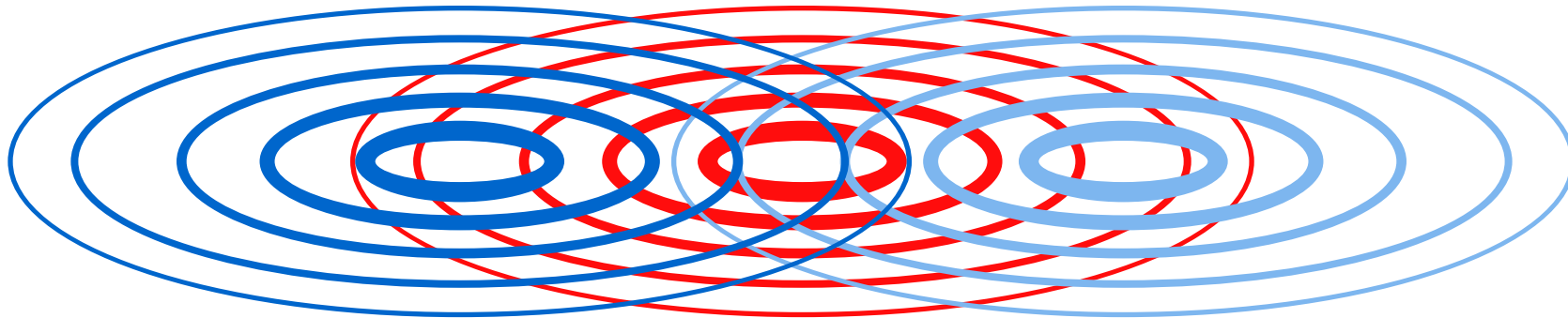
Multiple Access with Collision Avoidance (CSMA/CA)

- 1. Basic CSMA/CA: This is the fundamental form of CSMA/CA. In this type, a device listens to the wireless medium to check if it is idle before transmitting. If the medium is busy, the device waits for a random backoff period before attempting to transmit again. Basic CSMA/CA is used in various wireless standards, including 802.11b, 802.11g, and 802.11n.

Multiple Access with Collision Avoidance (CSMA/CA)

- 2. CSMA/CA with RTS/CTS (Request to Send/Clear to Send): In this type, an additional handshake mechanism is used to reduce collisions. Before transmitting, a device sends a Request to Send (RTS) frame to the intended recipient. The recipient responds with a Clear to Send (CTS) frame, reserving the medium for the duration of the transmission. Other devices in the vicinity defer their transmissions during this reservation period. CSMA/CA with RTS/CTS is employed in

Hidden Terminal Problem



A

B

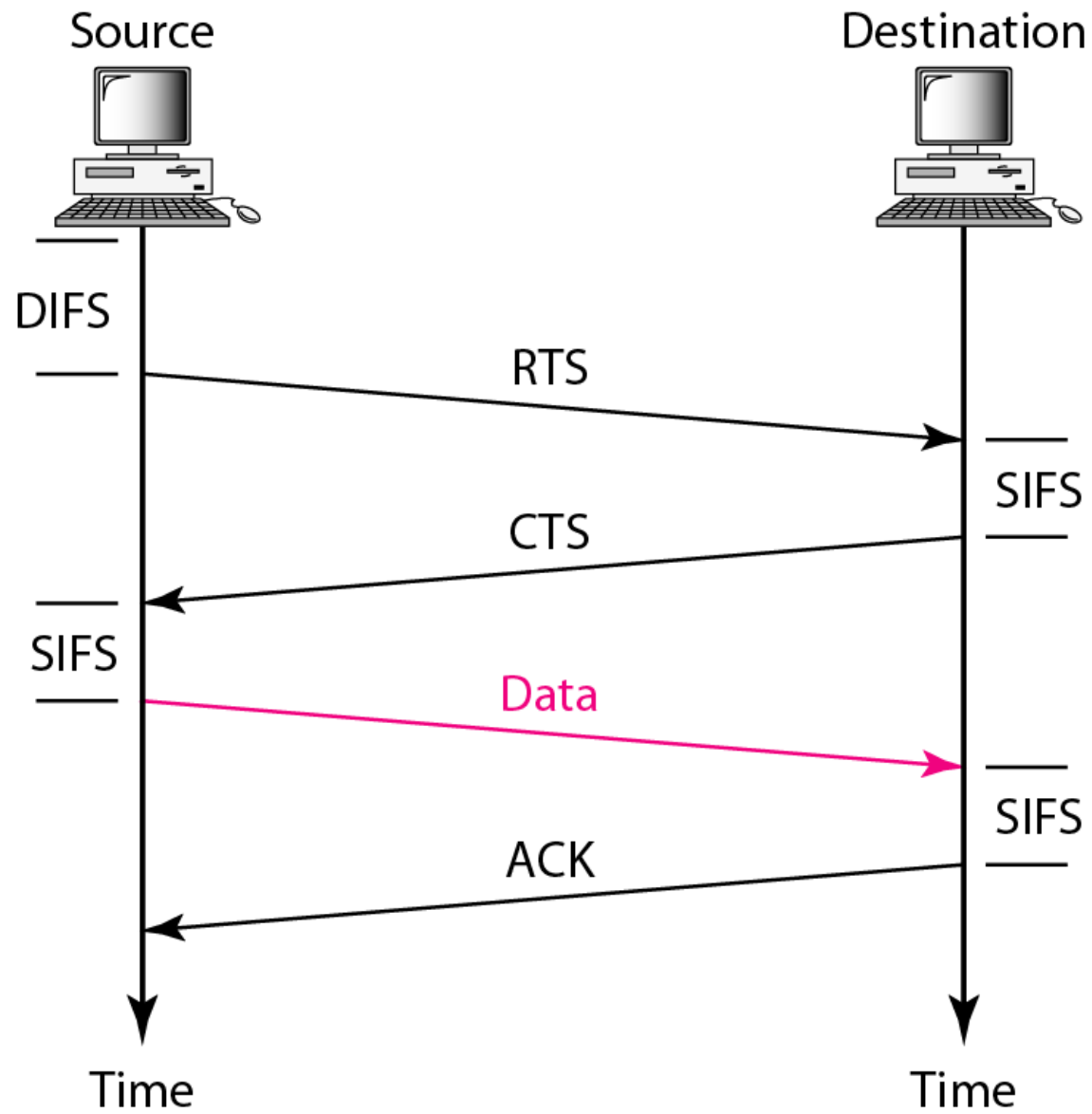
C

- A and C cannot hear each other.
- A sends to B, C cannot receive A.
- C wants to send to B, C senses a “free” medium
- Collision occurs at B.
- A cannot receive the collision (CD fails).
- A is “hidden” for C.

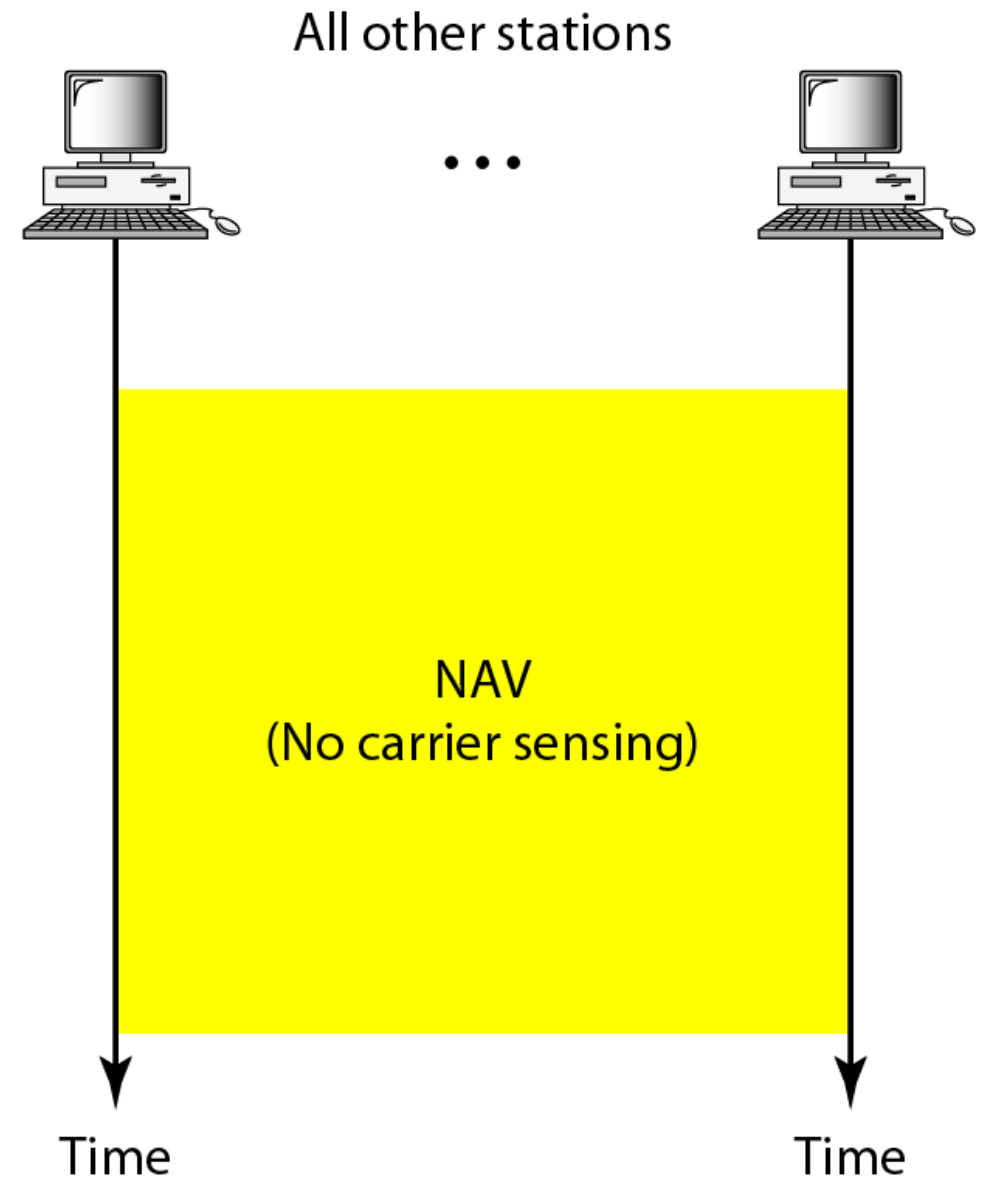
Multiple Access with Collision Avoidance (CSMA/CA)

- 3. Distributed Coordination Function (DCF):
DCF is a type of CSMA/CA used in the 802.11 standard. It employs a two-way handshake mechanism for collision avoidance. Before transmitting, a device listens to the medium for a Distributed Inter-Frame Space (DIFS). If the medium is idle for the DIFS duration, the device transmits. However, if the medium becomes busy during the DIFS, the device defers its transmission and waits for a random backoff period.

CSMA/CA



NAV (Network allocation vector)



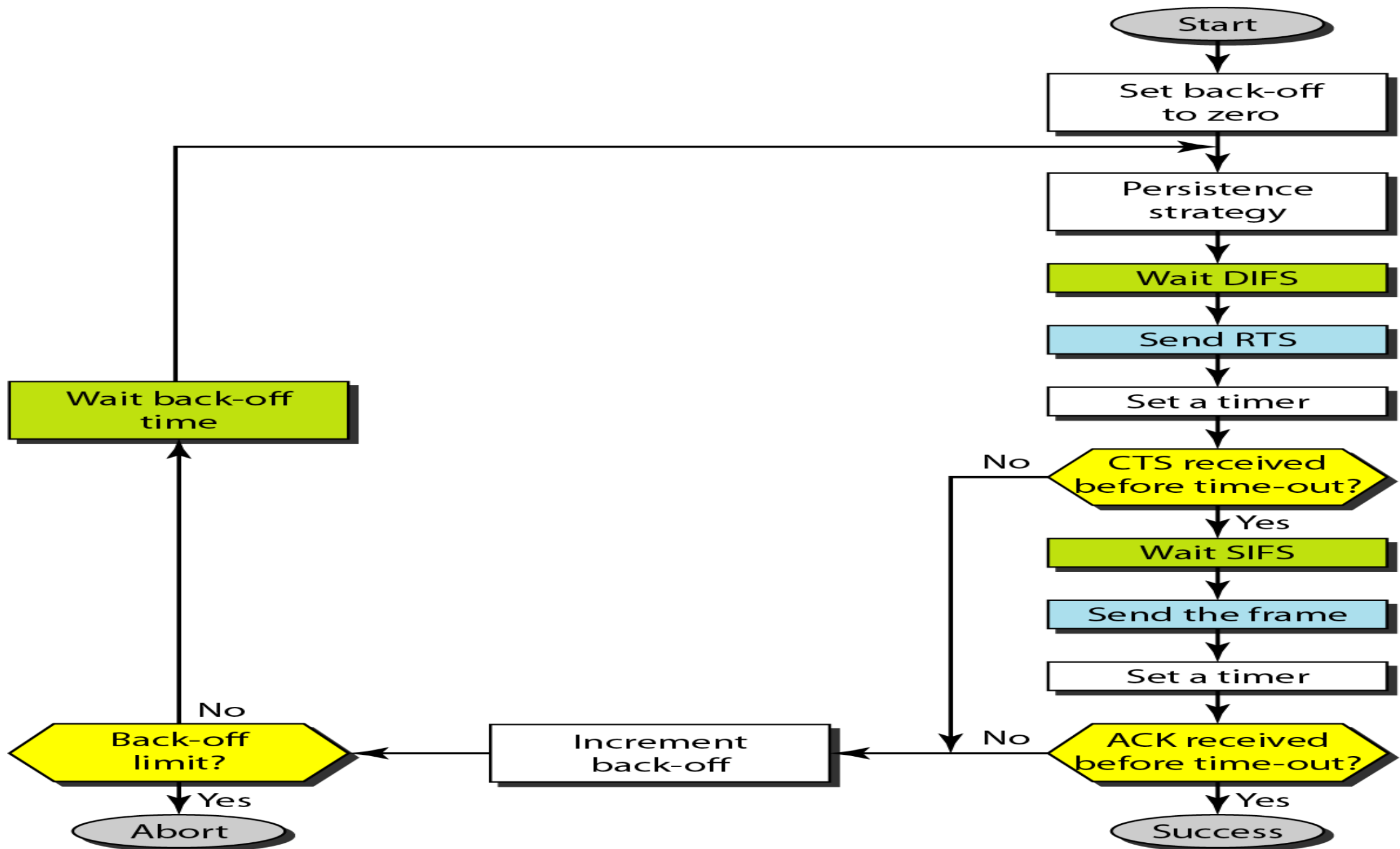
Multiple Access with Collision Avoidance (CSMA/CA)

- 4. Enhanced Distributed Channel Access (EDCA):
EDCA is a variant of CSMA/CA used in the 802.11e standard, which provides Quality of Service (QoS) support for wireless networks. EDCA introduces different access categories with different priorities, allowing devices with higher priority to have shorter backoff periods and higher chances of accessing the medium.

Interframe Spacing

- **Interframe spaces (IFS):** Intervals between transmissions of data frames
 - **Short IFS (SIFS):** For immediate response actions such as ACK
 - **Point Coordination Function IFS (PIFS):** Time used by a device to access medium after it has been asked and then given approval to transmit
 - **Distributed Coordination Function IFS (DIFS):** Standard interval between transmission of data frames

CSMA/CA flowchart



What is IEEE 802.11?

- Standard for wireless local area networks (wireless LANs) developed in 1990 by IEEE
- Intended for home or office use (primarily indoor)
- 802.11 standard describes the MAC layer, while other sub-standards (802.11a, 802.11b) describe the physical layer
- Wireless version of the Ethernet (802.3) standard

WLAN standards

- The following are some of the most common WLAN standards
- * IEEE 802.11a: This standard uses the 5 GHz frequency band and supports data rates up to 54 Mbps.
- * IEEE 802.11b: This standard uses the 2.4 GHz frequency band and supports data rates up to 11 Mbps.
- * IEEE 802.11g: This standard uses the 2.4 GHz frequency band and supports data rates up to 54 Mbps.
- * IEEE 802.11n: This standard uses the 2.4 GHz and 5 GHz frequency bands and supports data rates up to 600 Mbps.
- * IEEE 802.11ac: This standard uses the 5 GHz frequency band and supports data rates up to 3.46 Gbps.
- *

IEEE 802.11a

- 802.11a is a wireless networking standard that operates in the 5 GHz frequency band. It was one of the earliest standards developed for wireless local area networks (WLANs) and was ratified by the Institute of Electrical and Electronics Engineers (IEEE) in 1999.

IEEE 802.11a

- Some key features of the 802.11a standard include:
- 1. Frequency Band: 802.11a operates in the 5 GHz frequency band, which provides several advantages over the 2.4 GHz band used by other standards like 802.11b and 802.11g. The 5 GHz band has more available channels, which means less interference from other devices like microwaves and cordless phones.
- 2. Data Rate: 802.11a supports data rates of up to

IEEE 802.11a

- 3. Modulation Scheme: 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM) as its modulation scheme. OFDM divides the available frequency spectrum into multiple subcarriers and transmits data simultaneously on these subcarriers, increasing the overall data throughput.
- 4. Channel Width: 802.11a uses a channel width of 20 MHz, allowing for higher data rates but also

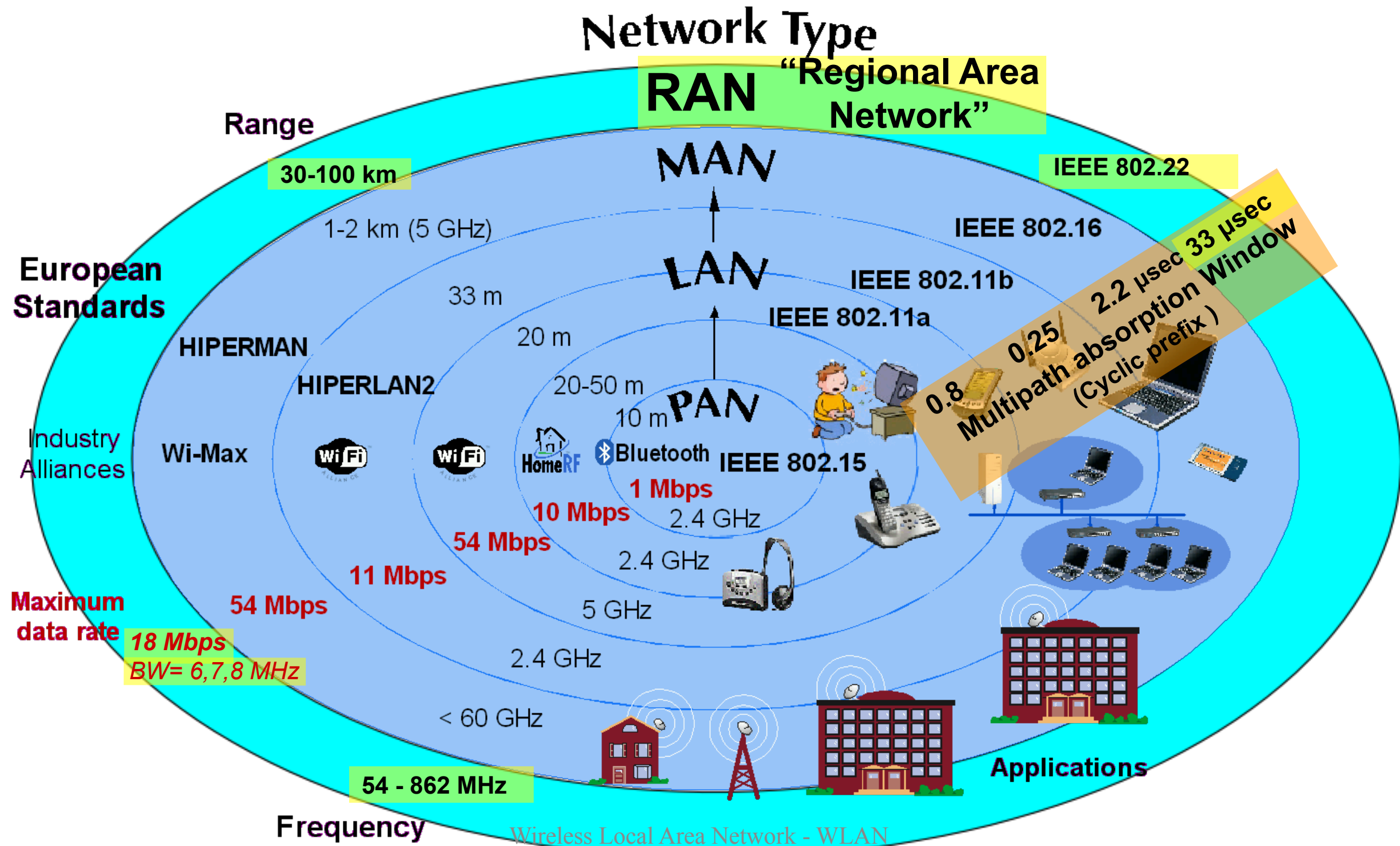
IEEE 802.11a

- 5. Range: One of the limitations of 802.11a is its reduced range compared to 802.11b and 802.11g. The higher frequency used by 802.11a leads to increased signal attenuation and reduced range, making it more suitable for indoor deployments or shorter-range applications.

WLAN standards

Standard	Frequency Band	Channel Width	Modulation Scheme	Range	Data Rate
802.11b	2.4 GHz	20 MHz	Direct Sequence Spread Spectrum (DSSS)	Medium to High	Up to 11 Mbps
802.11a	5 GHz	20 MHz	Orthogonal Frequency Division Multiplexing (OFDM)	Medium to Low	Up to 54 Mbps
802.11g	2.4 GHz	20 MHz	OFDM and DSSS	Medium to High	Up to 54 Mbps
802.11n	2.4 GHz/ 5 GHz	20 MHz/40 MHz	OFDM and Multiple Input Multiple Output (MIMO)	High	Up to 600 Mbps
802.11ac	5 GHz	20 MHz/40 MHz/ 80 MHz/160 MHz	OFDM and MIMO	High	Up to 6.77 Gbps
802.11ax	2.4 GHz/ 5 GHz	20 MHz/40 MHz/ 80 MHz/160 MHz	OFDM and MIMO	High	Up to 9.6 Gbps

IEEE Standards



WLAN standards

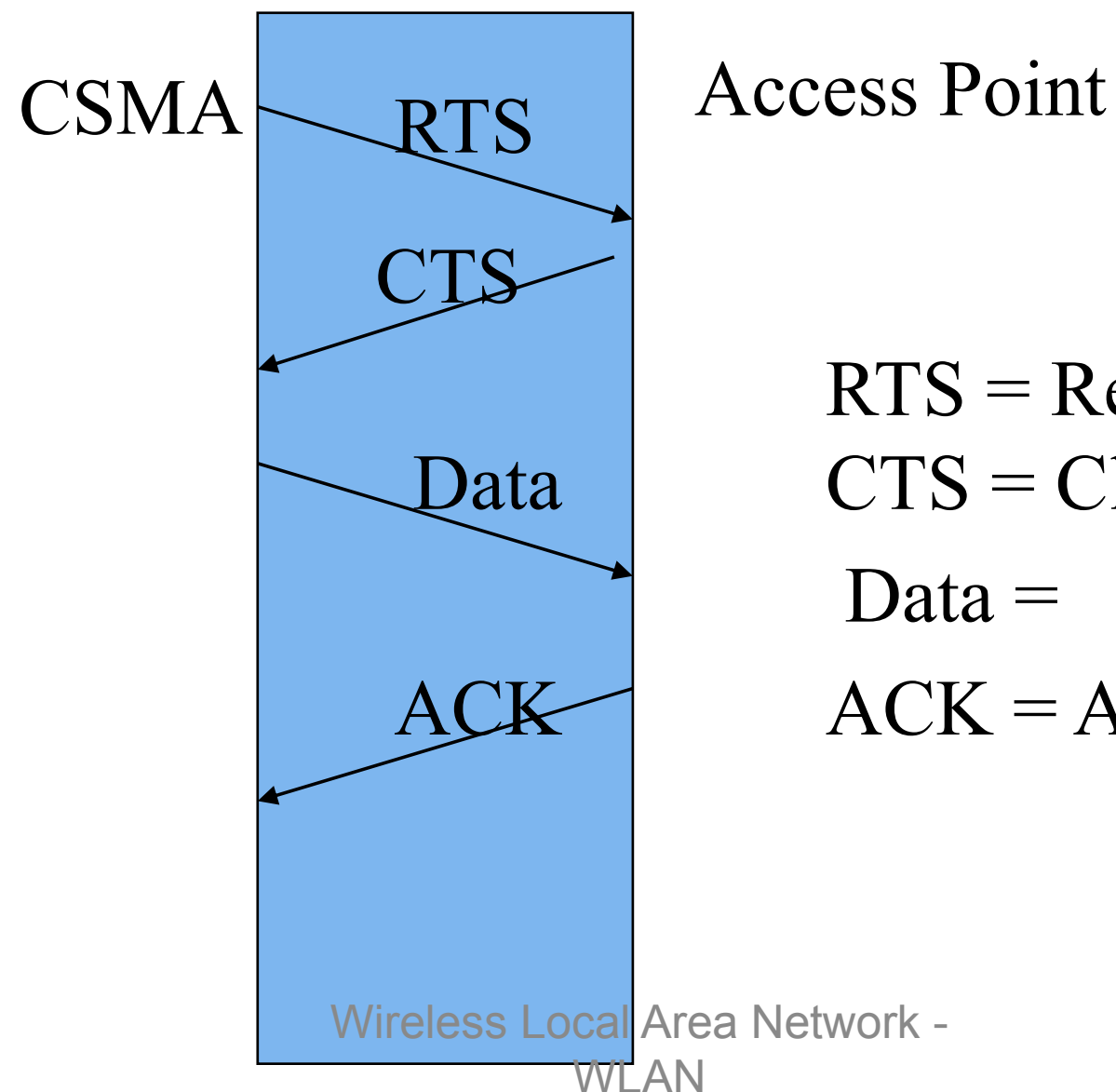
- While 802.11a was an important milestone in wireless networking, it was eventually superseded by newer standards like 802.11n, 802.11ac, and 802.11ax (Wi-Fi 6). These newer standards offered higher data rates, improved range, and backward compatibility with older standards. However, 802.11a is still used in some niche applications or in environments where the 5 GHz band is less crowded and interference is a concern.

Wireless LANS

- Wireless Fidelity (Wi-Fi)
 - Operates
 - In the same manner as the Ethernet networks
 - A device waits for silence on the radio frequency
 - Carrier Sense Multiple Access (CSMA)
 - Operates in
 - AD-Hoc mode or
 - Uses a Access point (AP) to allow connection to wired infrastructure

Wireless LANS

- Wireless Fidelity (Wi-Fi)



RTS = Request to Send
CTS = Clear to Send
Data =
ACK = Acknowledgment

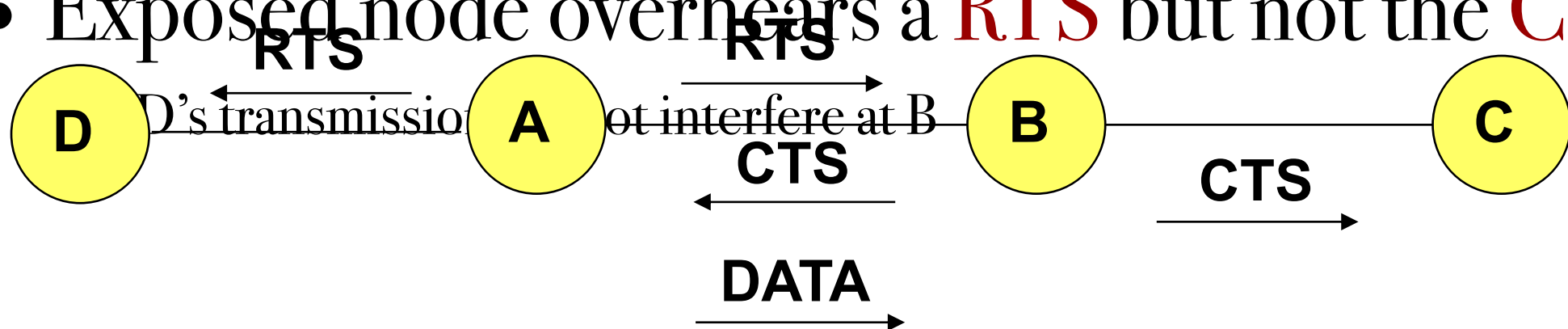


Wireless LAN Protocols

- **MACA** protocol solved hidden and exposed terminal problems. How?
 - Sender broadcasts a Request-to-Send (*RTS*) and the intended receiver sends a Clear-to-Send (*CTS*).
 - Upon receipt of a *CTS*, the sender begins transmission of the frame.
 - RTS, CTS helps determine who else is in range or busy (**C**ollision **A**voidance).

Solution for Hidden Terminals

- A first sends a *Request-to-Send (RTS)* to B
- On receiving **RTS**, B responds *Clear-to-Send (CTS)*
- Hidden node C overhears **CTS** and keeps quiet
 - Transfer duration is included in both RTS and CTS
- Exposed node overhears a **RTS** but not the **CTS**



WEP (Wired Equivalent Privacy)

k is the shared key

Message + checksum(message) = plaintext

$$E_k(\text{PlainText}) = \text{CipherText}$$

$$D_k(\text{CipherText}) = D_k(E_k(\text{PlainText})) = \text{PlainText}$$

WEP Process

- Integrity Check (IC): checksum of message
 - Message + checksum(message) = plaintext
- Encryption
 - Generates keystream (PseudoRandom string of bytes)
- XOR ($\oplus$) keystream and plaintext = ciphertext
- Send ciphertext over network

XOR		
	0	1
0	0	1
1	1	0

WEP at the receiver

- Sender and receiver use same key
 - Sender encrypts
- Receiver decrypts
 - Sender XOR keystream and plaintext to get ciphertext
 - Receiver XOR ciphertext with same key to get plaintext
 - ... $RC4(x) \oplus \text{keystream} = x$
 - RC4 (Rivest Cipher 4) is a simple & most widely used form of stream cipher. It encrypts messages one byte at a time.

WLAN Benefits

- Mobility
 - increases working efficiency and productivity
 - extends the On-line period
- Installation on difficult-to-wire areas
 - inside buildings
 - road crossings
- Increased reliability
 - Note: Pay attention to security!
- Reduced installation time
 - cabling time and convenient to users and difficult-to-wire cases

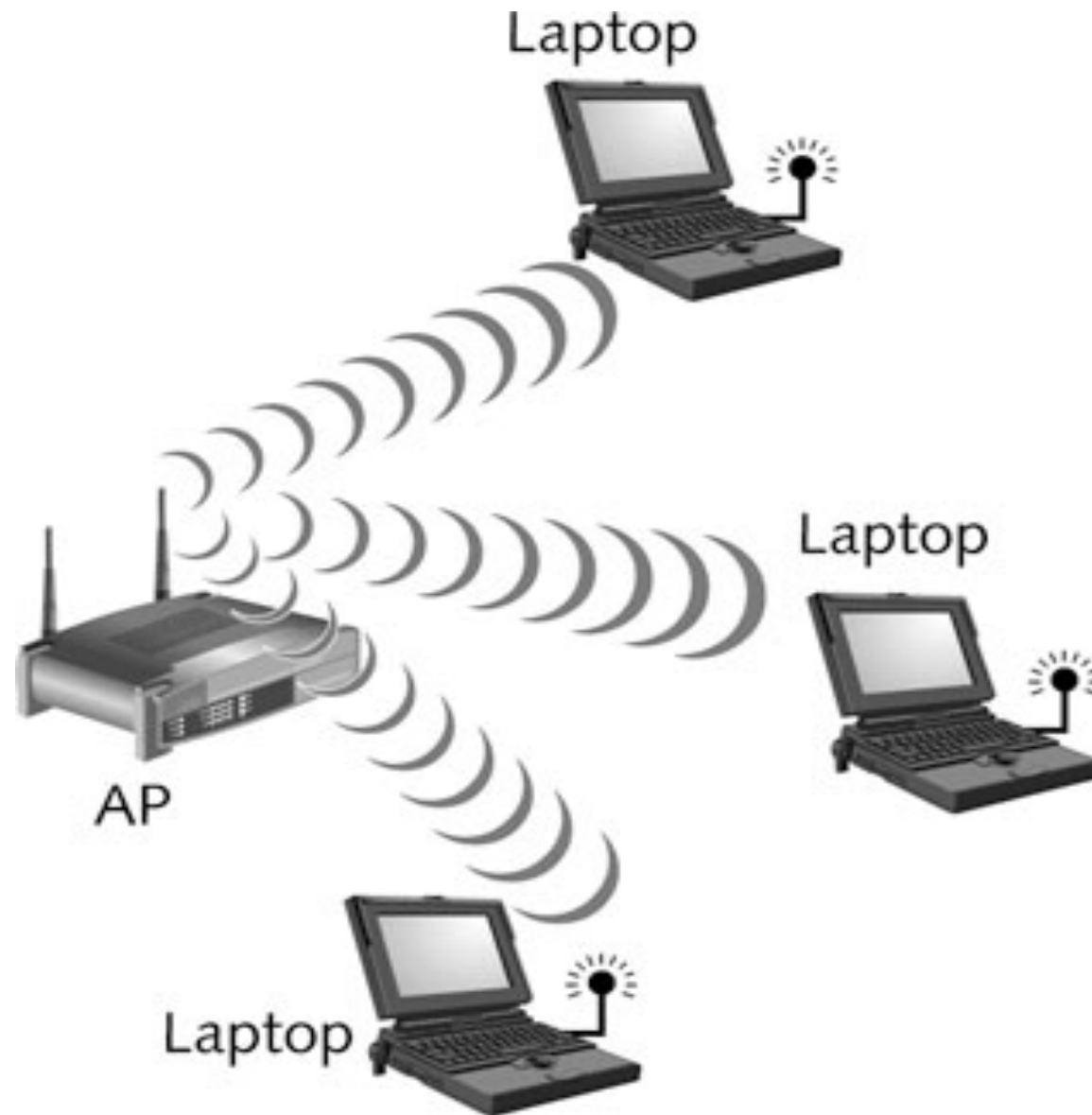
802.11 - MAC management

- Synchronization
 - try to find a LAN, try to stay within a LAN
 - timer etc.
- Power management
 - sleep-mode without missing a message
 - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
 - integration into a LAN
 - roaming, i.e. change networks by changing access points
 - scanning, i.e. active search for a network
- MIB - Management Information Base
 - managing, read, write

Discovering the WLAN: Beacons

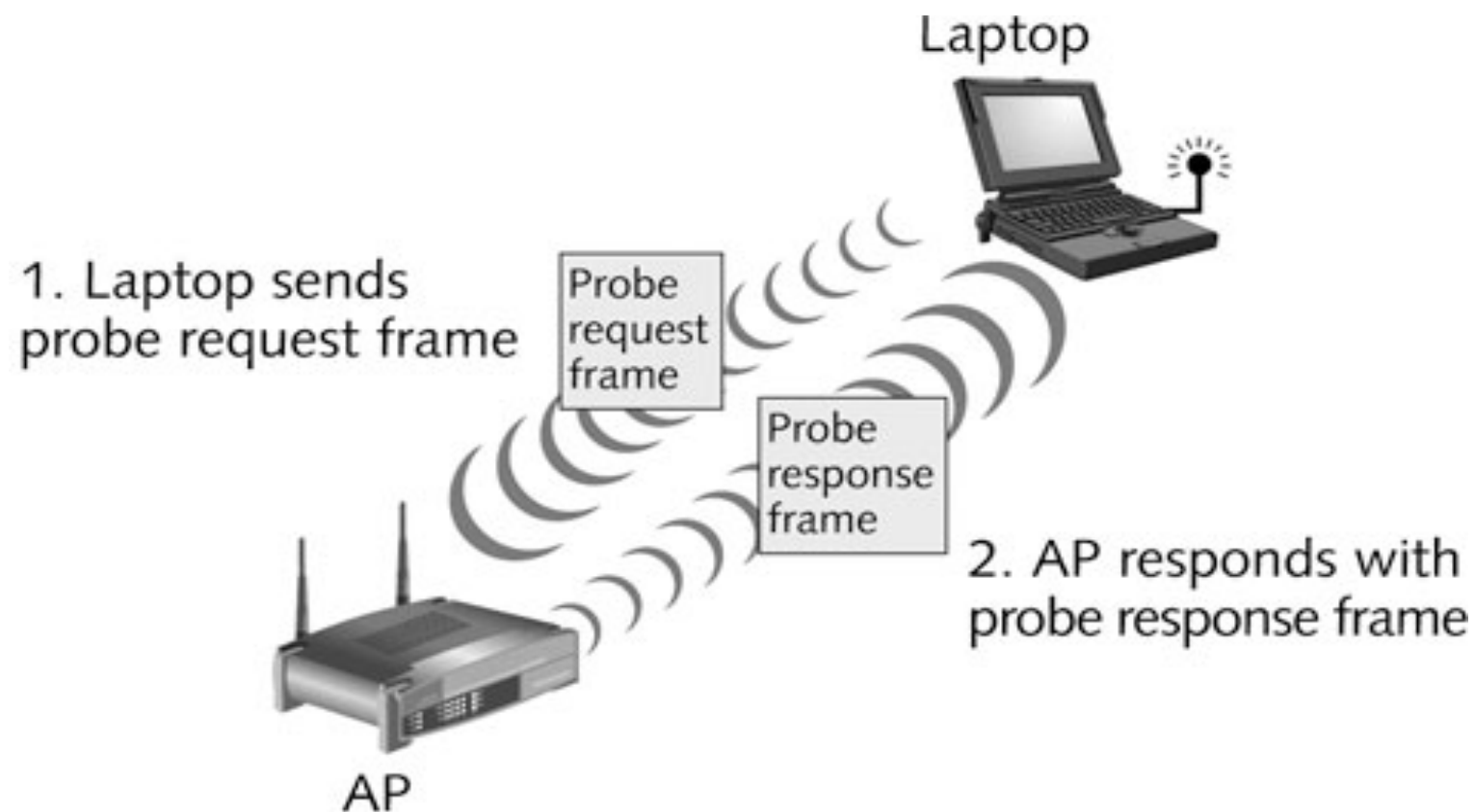
- At regular intervals, AP (infrastructure network) or wireless device (ad hoc network) sends beacon frame
 - Announce presence
 - Provide info for other devices to join network
- Beacon frame format follows standard structure of a management frame
 - Destination address always set to all ones
- Beacon frame body contains following fields:
 - Beacon interval
 - Timestamp
 - Service Set Identifier (SSID)
 - Supported rates
 - Parameter sets
 - Capability information
- In ad hoc networks, each wireless device assumes responsibility for beacons
- In infrastructure networks beacon interval normally 100 ms, but can be modified

Discovering the WLAN: Beaconing



Discovering the WLAN: Scanning

- Receiving wireless device must be looking for beacon frames
- **Passive scanning:** Wireless device simply listens for beacon frame
 - Typically, on each available channel for set period
- **Active scanning:** Wireless device first sends out a management probe request frame on each available channel
 - Then waits for probe response frame from all available APs



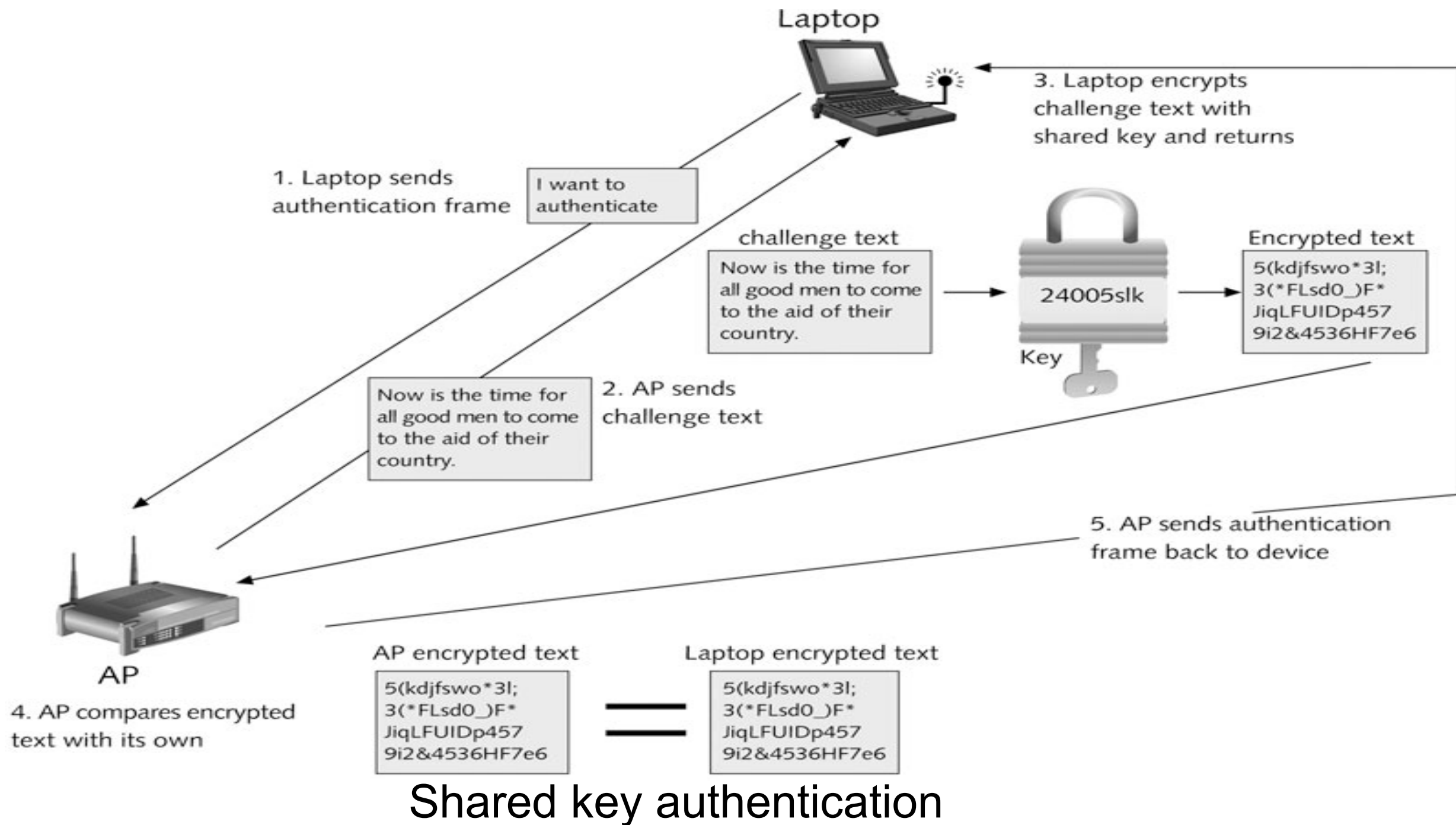
Joining the WLAN: Authentication

- Unlike standard wired LANS, **authentication** performed *before* user connected to network
 - Authentication of the *wireless device*, not the user
- **IEEE 802.11 authentication:** Process in which AP accepts or rejects a wireless device
- **Open system authentication:** Most basic, and default, authentication method
- **Shared key authentication:** Optional authentication method
 - Utilizes **challenge text**
- Open system and Shared key authentication techniques are weak
 - Open System: Only need SSID to connect
 - Shared Key: Key installed manually on devices
 - Can be discovered by examining the devices

Joining the WLAN: Authentication



Joining the WLAN: Authentication



Joining the WLAN: Association

- **Association:** Accepting a wireless device into a wireless network
 - Final step to join WLAN
- After authentication, AP responds with association response frame
 - Contains acceptance or rejection notice
- If AP accepts wireless device, reserves memory space in AP and establishes association ID
- Association response frame includes association ID and supported data rates

Remaining Connected to the WLAN: Reassociation

- **Reassociation:** Device drops connection with one AP and establish connection with another
 - Several reason why reassociation may occur:
 - Roaming
 - Weakened signal
 - When device determines link to current AP is poor, begins scanning to find another AP
 - Can use information from previous scans

WLAN Technology Problems

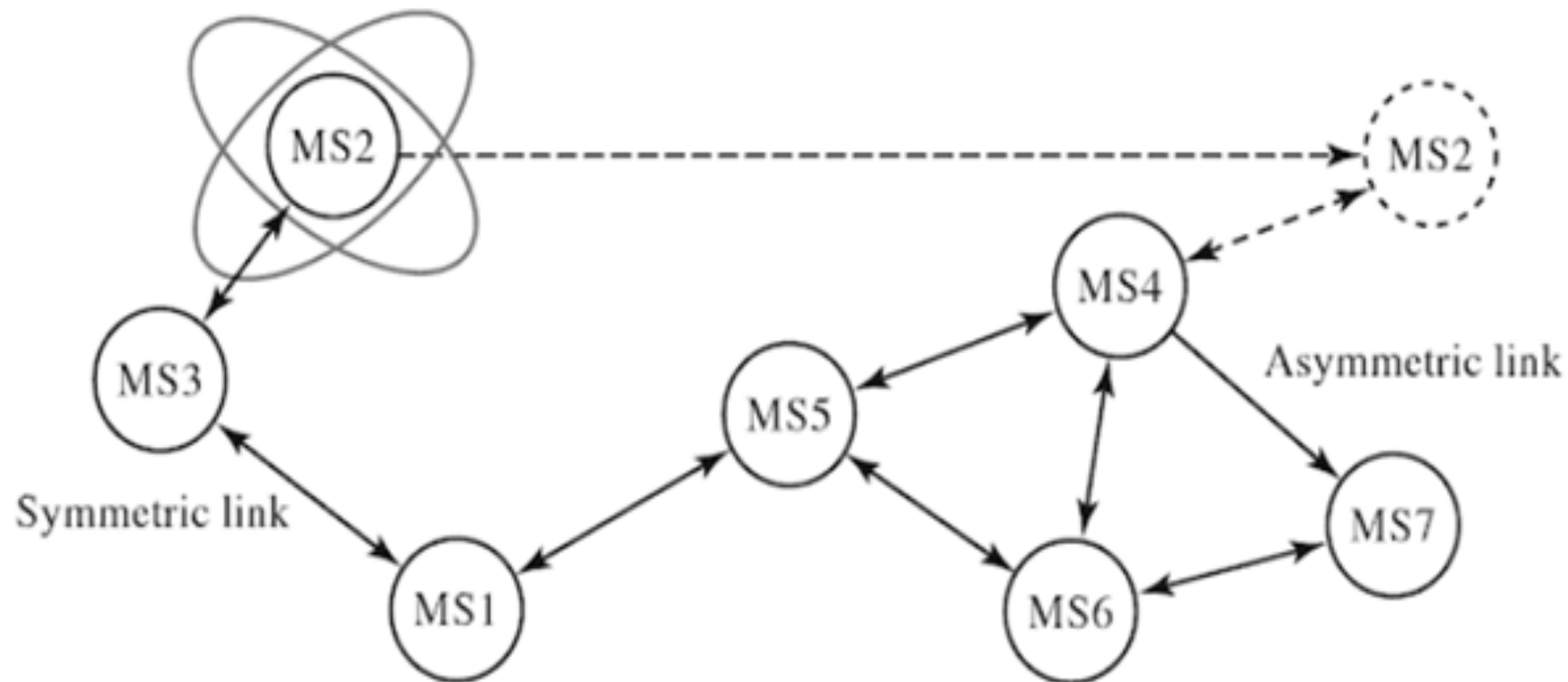
- Data Speed
 - IEEE 802.11b support up to 11 MBps, sometimes this is not enough - far lower than 100 Mbps fast Ethernet
- Interference
 - Share same frequency with microwave oven, Bluetooth, and others
- Security
 - Current WEP algorithm is weak - usually not ON!
- Roaming
 - No industry standard is available and propriety solution are not interoperable - especially with GSM
- Inter-operability
 - Only few basic functionality are interoperable, other vendor's features can't be used in a mixed network

MANETs

- **MANETs (Mobile Ad Hoc Networks)**
 - MANET is a **continuously self-configuring, self-organizing, infrastructure-less network of mobile devices connected without wires.**
 - It is sometimes known as "on-the-fly" networks or "spontaneous networks".

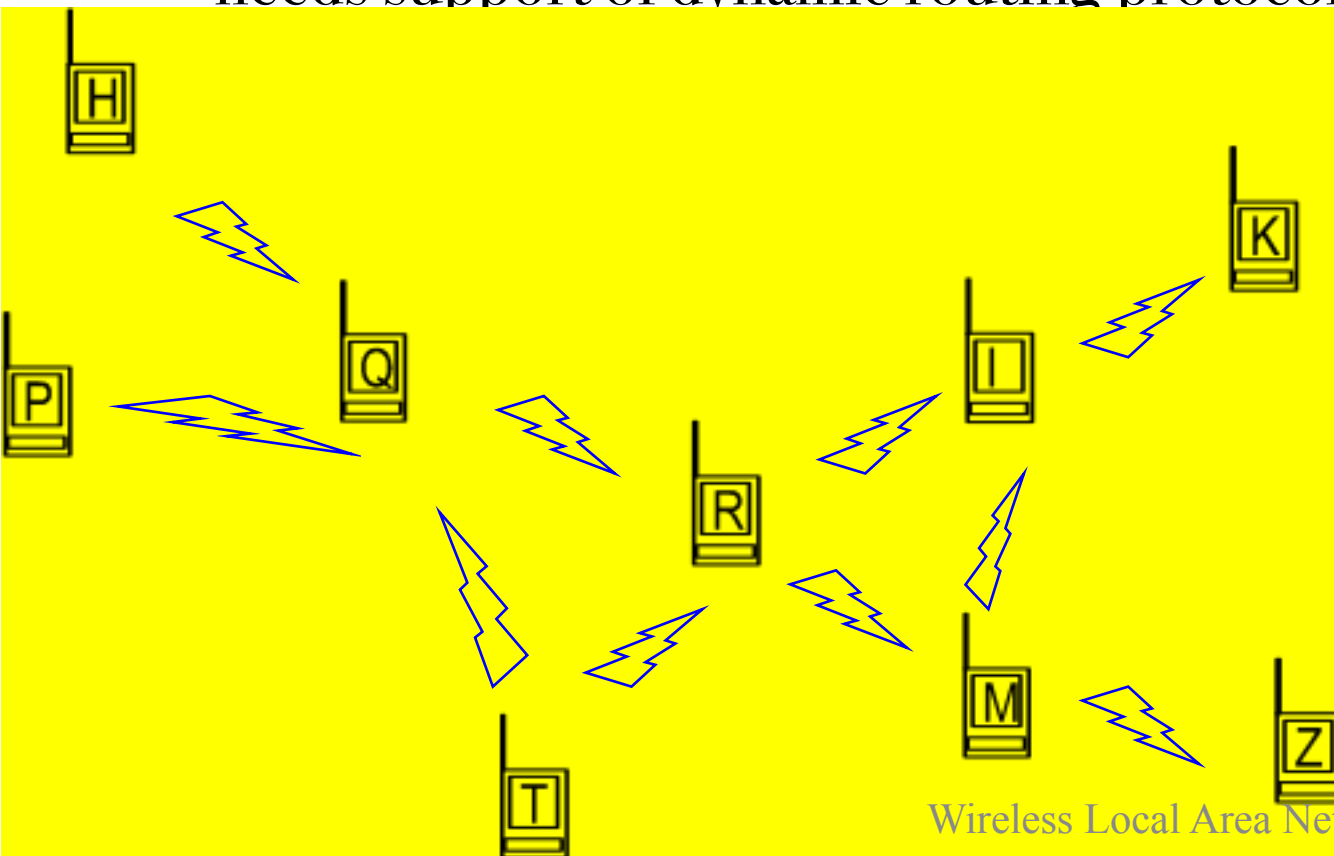
MANETs

- MANET is autonomous system of nodes or MSs(serving as routers) connected by wireless links, union of which forms a communication network



MANETs

- MANET = Mobile Ad Hoc Networks
 - multi-hop communication
 - Coverage area is larger than radio range of single nodes
 - Therefore, to reach some destination a node can use other nodes as relays.
 - needs support of dynamic routing protocols (discover routes, adapt to changes)



Characteristics Interface of MANET



- ❑ **Dynamic Topology:** Node in MANET has a dynamic nature, which can be moved anywhere.
- ❑ **Autonomy:** Each node in MANET role as **end-user** as well as a router which calculates its own route-path which will subsequently be selected.
- ❑ **Bandwidth limitations:** Link on wireless networks tend to have low capacity when compared to a wired network.
- ❑ **Limitations of energy:** All nodes in MANET are mobile, so it is ascertained that node uses battery power to operate. So it is necessary to optimize the design of energy.
- ❑ **Limitations Security:** Wireless networks tend to be more vulnerable to security than wired networks.

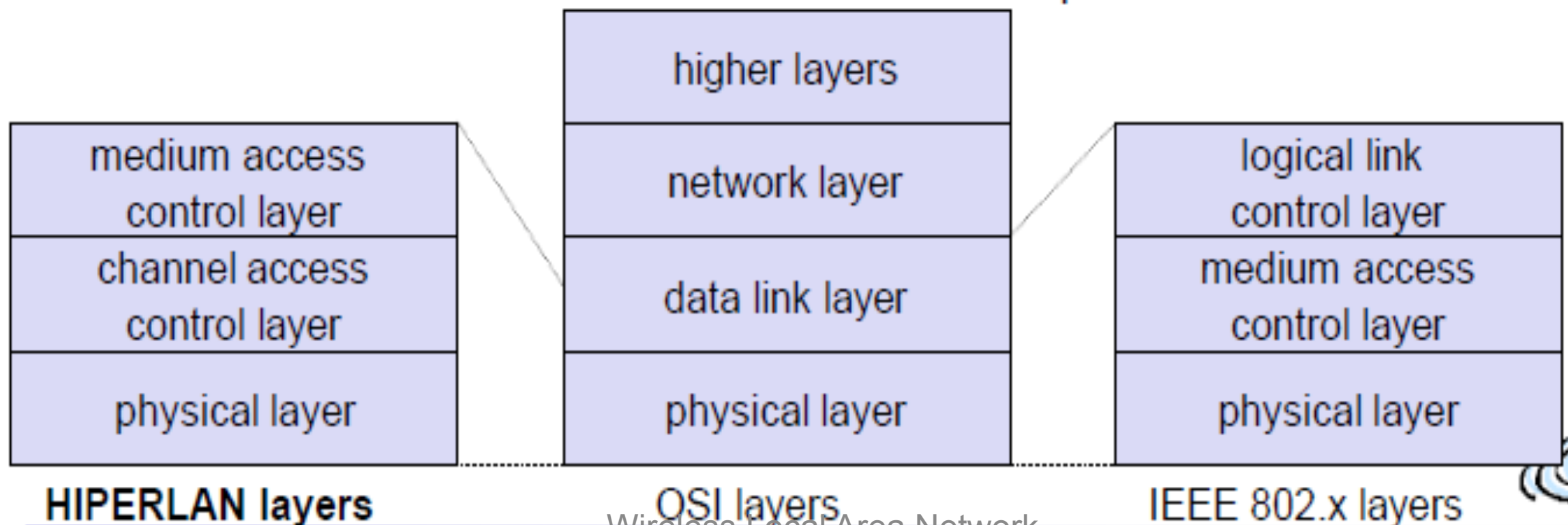
What is HIPERLAN/2?

- European standard developed by ETSI/BRAN (European Telecommunications Standards Institute/Broadband Radio Access Networks)
- Physical Layer is very similar to 802.11a
- Standard based on Wireless ATM (Asynchronous Transfer Mode)
- ATM asynchronous time-division multiplexing to encode data into small, fixed-sized cells.

HIPERLAN PROTOCOL

HIPERLAN family

- ❑ one standard cannot satisfy all requirements
 - range, bandwidth, QoS support
 - commercial constraints
- ❑ HIPERLAN 1 standardized since 1996 – no products!



Overview: original HIPERLAN protocol family

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	

HIPERLAN 1 never reached product status,
the other standards have been renamed/modifed !

Wireless Local Area Network -
WLAN



HiperLAN2

- IEEE 802.11 is a widely accepted standard in the United States for wireless LANs
 - Primarily a “cellular” random access scheme with ad hoc networking and contention free access
 - 802.11b products are available now, but 802.11a are better
- HIPERLAN/2 is being pushed in Europe
 - Wireless ATM solution for real-time traffic
 - Standard reflects the network topology
- There is an effort to agree on one world-wide standard, keep your fingers crossed

Wireless Sensor Networks:

- **sensor**

- A **transducer** – convert physical quantity, such as pressure or brightness, into an electrical signal, or vice versa.
- converts physical phenomenon e.g. heat, light, motion, vibration, and sound into electrical signals

- **sensor node**

- basic unit in sensor network
- contains on-board sensors, processor, memory, transceiver, and power supply

- **sensor network**

- consists of a large number of sensor nodes
- nodes deployed either inside or very close to the sensed

Wireless Sensor Networks Applications

Military Applications

- Monitoring friendly forces, equipment, and ammunition
- Battlefield surveillance
- Reconnaissance of opposing forces and terrain
- Targeting
- Battle damage assessment
- Nuclear, biological, and chemical attack detection

Wireless Sensor Networks Applications

Environmental Applications

- Forest fire detection
- Bio-complexity mapping of environment
- Flood detection
- Precision Agriculture
- Air and water pollution

Wireless Sensor Networks Applications

Health Applications

- Telemonitoring of human physiological data
- Tracking and monitoring doctors and patients inside a hospital
- Drug administration in hospitals

Home and Office Applications

- Home and office automation
- Smart environment

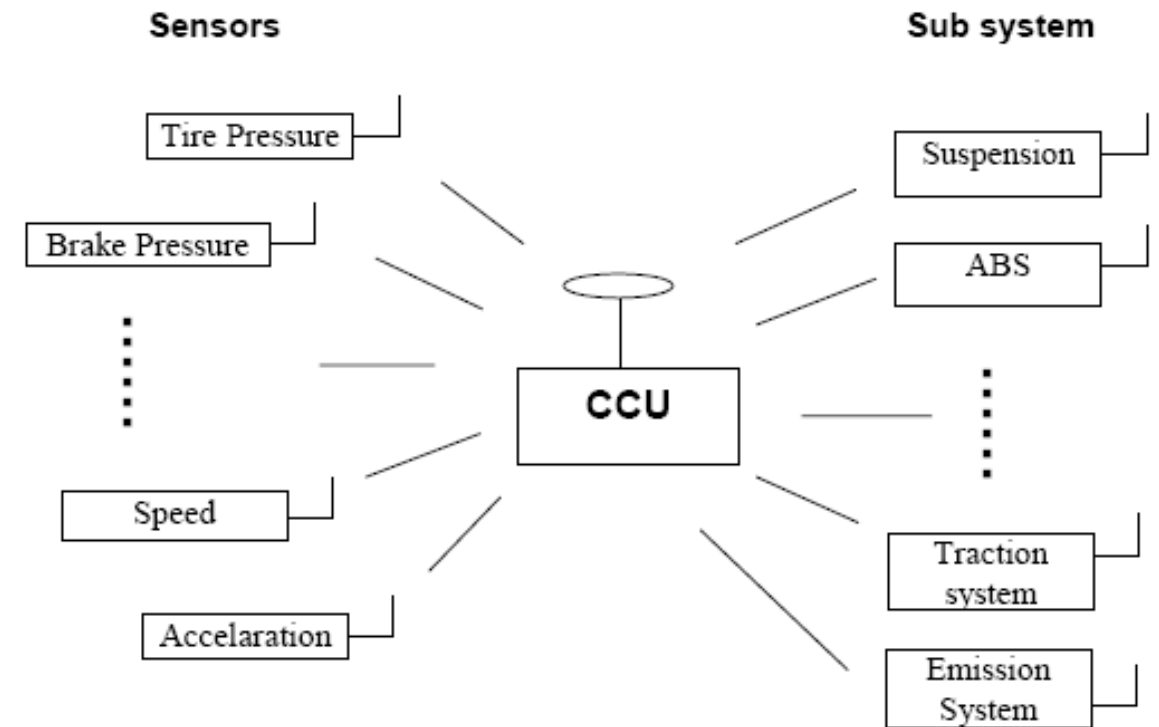
Wireless Sensor Networks Applications

Automotive Applications

- Reduces wiring effects
- Measurements in chambers and rotating parts
- Remote technical inspections
- Conditions monitoring e.g. at a bearing

Wireless Sensor Networks Applications

Automotive Applications



Thank You!