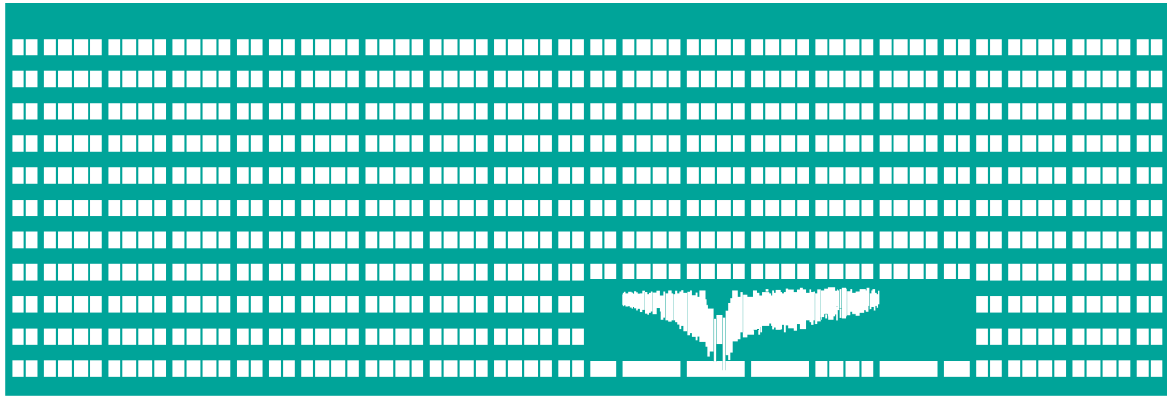
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

IEEE 802.11 Networks (WiFi)



Computer Networks
Lecture 10

What are IEEE 802.11 Networks ?

- Wireless networks operating in a license-free Instrumental-Scientific-Medicine (ISM) band
  - 2.4 GHz
  - 5 GHz
    - In European environment, ETSI requires dynamic channel selection and automatic transmit power adaptation
- Optimized for indoor usage
  - Outdoor use is also common in CZ
    - connection of multiple separated buildings, P2P connections
- Defines link and physical layer
  - Multiple options of physical layer implementation

Spread-Spectrum Transmission

- Standardization bodies require to spread the transmitted power over a wide frequency range
  - Max transmitted power is 100 mW
- The wider frequency range than is really necessary is used
  - The information is transmitted on multiple frequencies (redundancy)
    - Signal may be reconstructed even if the noise is present
    - Coexistence of multiple (uncoordinated) systems

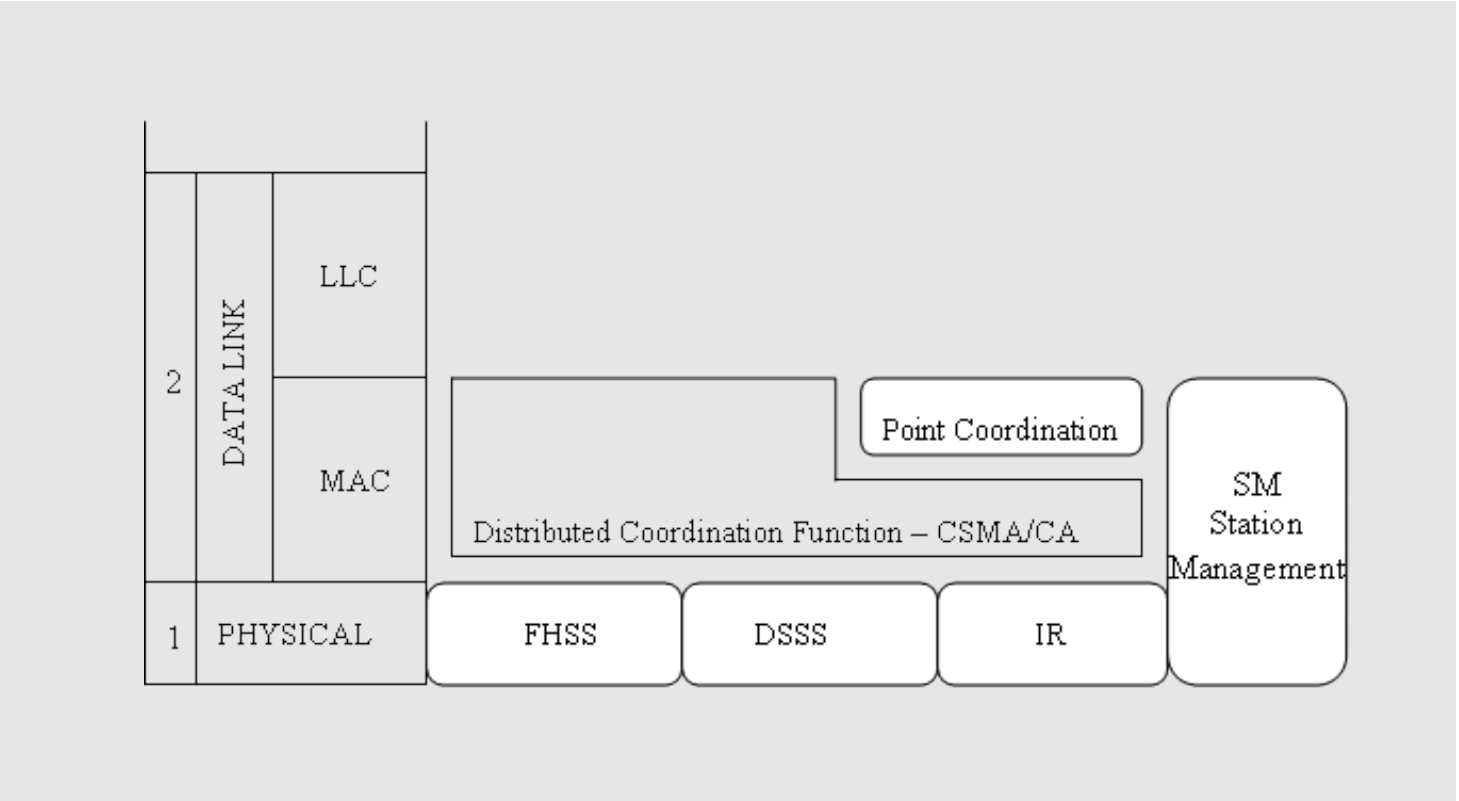
Channels of the 2.4 GHz ISM Band

- Europe: channels 1-13, USA: channels 1-11
- Adjacent-channel spacing 5 MHz, channel bandwidth 22 MHz
  - Every channel overlaps with 4 neighboring channels
- To completely avoid overlaps, we need to choose channels that provide 25 MHz spacing
  - Only 3 channels may be utilized simultaneously without interference

Channels of the 5 GHz ISM Band

- Non-overlapping channels
- Different for various countries/regions
- Europe (ETSI) – 11 non-overlapping channels

Structure of IEEE 802.11 Recommendations



Selected IEEE 802.11 Recommendations

- 802.11 (the core standard, current: 802.11-2016)
  - Original 802.11-1997 standard uses only 1 & 2 Mb/s
- Former 802.11a (802.11-2016, clause 17)
  - 5 GHz (USA), 6,9,12,18,24,36,48,54 Mb/s
- Former 802.11b (802.11-2016, clause 16)
  - 2.4 GHz (USA, Europe)
  - Extends 802.11 by DSSS 1,2,5.5 and 11 Mb/s
- Former 802.11g (802.11-2012, clause 18)
  - 2.4 GHz (USA, Europe)
  - Modulations similar to 802.11a (but 2.4GHz band)
- Former 802.11h (integrated to 802.11-2012)
  - 5 GHz (Europe)
  - Similar to 802.11a, but requires dynamic power adjustment and automatic channel selection

You may download 2016 standard at: https://standards.ieee.org/content/ieee-standards/en/standard/802_11-2016.html

Related 802.11-2012 Recommendations

- 802.11i – security+QoS (integrated in 802.11-2007)
  - QoS moved here from 802.11e
- 802.11f – fast roaming between APs. Superseded by 802.11k – Radio Resource Management & 802.11r – Fast roaming (integrated in 802.11-2012)
  - Avoids the need of reoccurring authentication during handover between APs
  - Useful for latency-critical mobile application (IP telephony, multimedia transfers, …)
- 802.11n – 2.4 & 5 GHz (802.11-2016, clause 19)
  - MIMO, wider bandwidth (20/40 MHz), speeds up to 144.4 Mb/s for 20 MHz & 300 Mb/s for 40 MHz.

Other Related Recommendations

- 802.11ac (802.11-2016, clause 21) – 5 GHz
  - Multi-station WLAN throughput >= 1 Gb/s, single station 500 Mb/s, 80/160 MHz range, up to 8 streams, up to QAM-256.
- 802.11ad (802.11-2016, clause 20, annexes Y,Z) – 60 GHz, WiGig
  - theoretical maximum throughput up to 7 Gbit/s.
  - will be used in a new wireless USB specification.
- 802.11af (802.11-2016, clause 22) – TV band 54-790 MHz on unused allocations
  - Cognitive technology for whitespaces in spectrum
  - illegal in CZ? In EU: 490-790MHz, 2h, closed loop
- 802.11ah – Wi-Fi HaLow – 900 MHz band, longer range, low power

WiFi

- „Wireless Fidelity“
- Logo provided by a consortium that focuses on 802.11 products interoperability testing
- Wi-Fi Alliance
  - Conformity testing
  - Relabeling of WiFi technologies
    - 802.11a – Wi-Fi 1
    - 802.11b – Wi-Fi 2
    - 802.11g – Wi-Fi 3
    - 802.11n – Wi-Fi 4
    - 802.11ac – Wi-Fi 5
    - 802.11ax – Wi-Fi 6

Components of IEEE 802.11 Wireless Network

- Access Point
- Wireless clients (stations)
- Distribution System
- Wireless medium (frequency band)

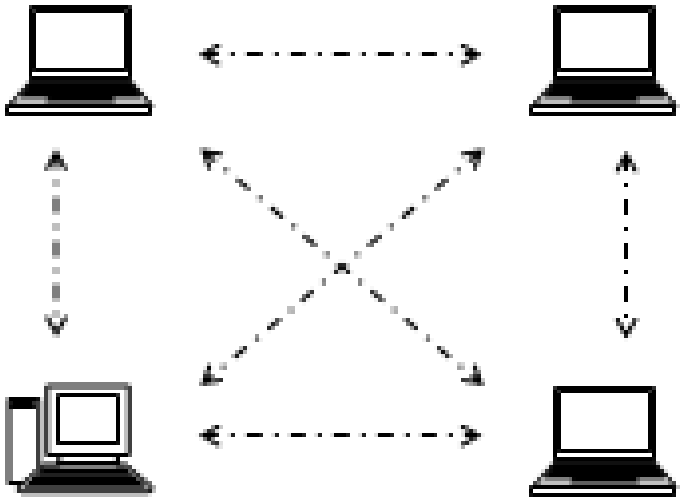
WiFi Usage Alternatives

- Ad-hoc
  - Used for temporary wireless interconnection of 2 or more nearby computers
  - Needs to be configured manually
- Infrastructure
  - Permanent wireless network infrastructure using access point (AP)
  - AP may act as a bridge to the wired network
    - Often also provides other functions, like DHCP server, NAT and other „PnP“ functions

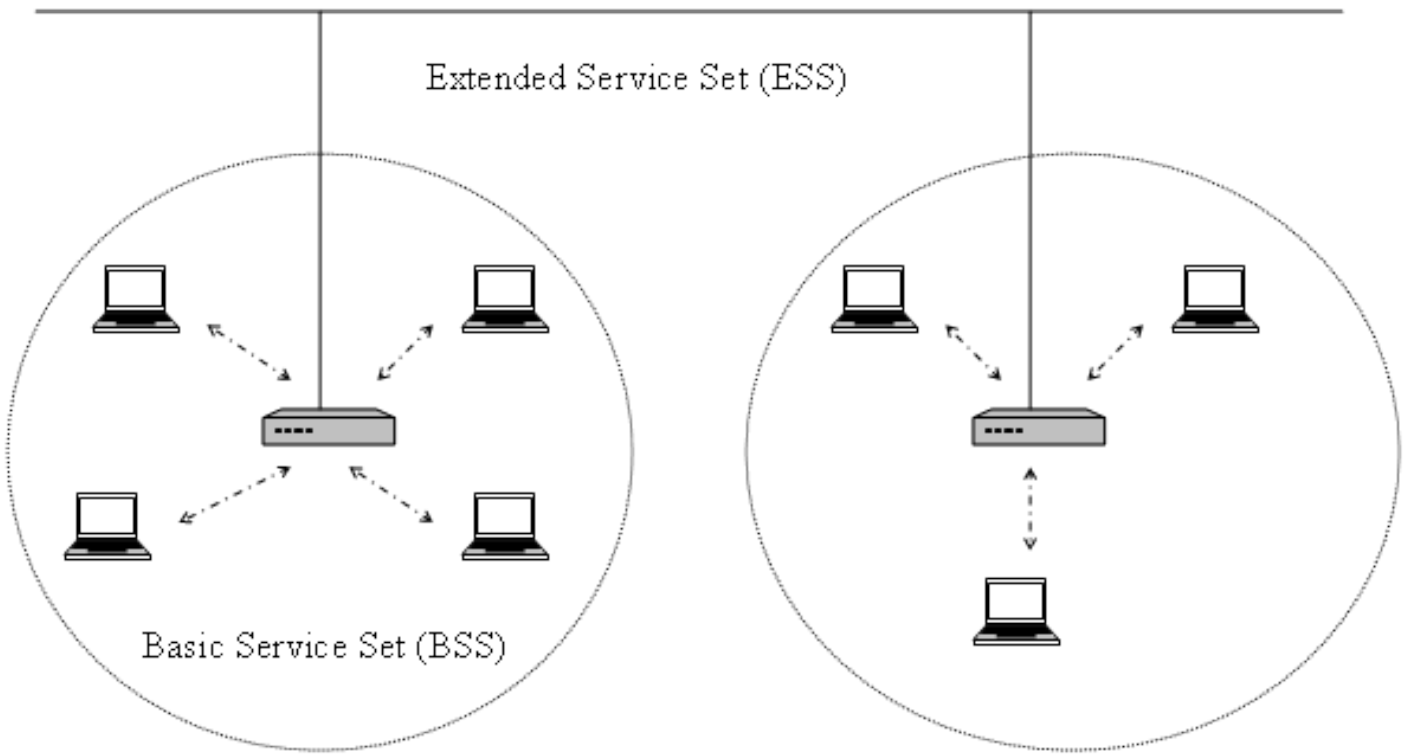
Architectures of WiFi Networks

- Independent Basic Service Set (IBSS)
  - A group of directly communicating stations
    - No frame relaying
  - Not interconnected with a wired network
- Basic Service Set (BSS)
  - Utilizes access point, stations communicate using AP
- Extended Service Set (ESS)
  - Interconnects multiple BSS using the distribution system
  - The distribution system is out of scope of the IEEE 802.11 standard
    - Ethernet
    - Various (proprietary) solutions of Wireless Distribution Systems (WDS)

IBSS



BSS, ESS

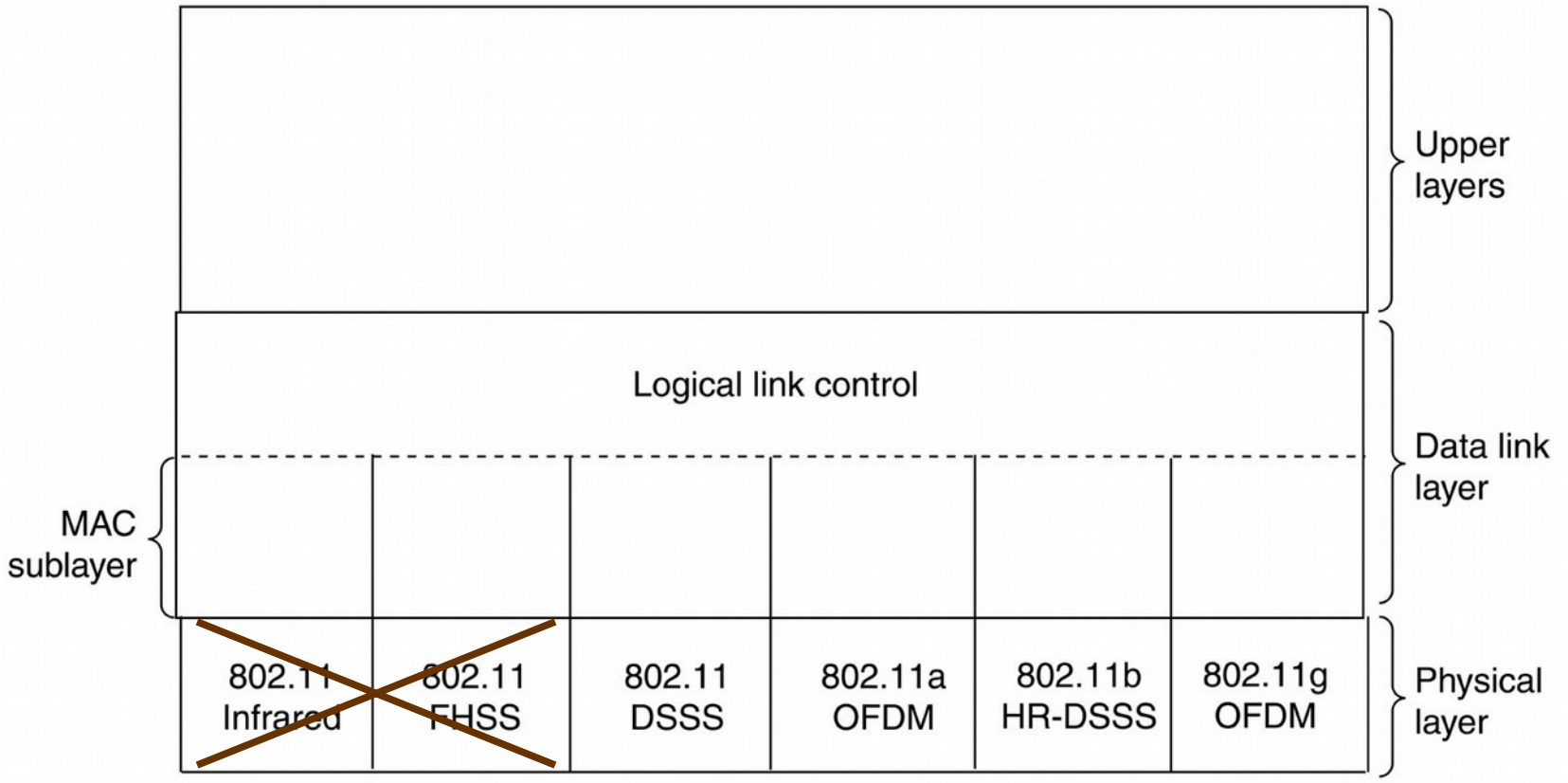


Terminology

- Service Set = logical group of stations
  - BSS=Basic Service Set
- SSID = Service Set Identifier
- BSS ID = BSS Identifier = AP MAC address

Physical Layer

Relations between IEEE 802.11 Recommendations (original)



Sublayers of IEEE 802.11 Physical Layer

- **Physical Layer Convergence Procedure (PLCP)**
  - appends its own header to L2 frames
    - specifies the particular modulation method
  - Detects the state of the channel for MAC sublayer of the link layer
    - busy/free
- **Physical Medium Dependent (PMD)**
  - Takes care of the physical transmission

Physical Layer Convergence Procedure Sublayer

- Different for various modulation methods
- Long (128b) and optional short (56b) preamble (for real-time transfers)
- PLCP frame format (differs for various PMD):
  - Preamble: synchronization sequence + Start Frame Delimiter (different for individual PMDs)
  - PLCP header
  - Data Rate (8b)
  - MAC PDU length: 16b
  - Header CRC (16b)
- For backward compatibility, PLCP frames are always transmitted using 1Mb/s BPSK

  => increases overhead

Functional Blocks of the Physical Layer

- Scrambling – „randomizes“ transmitted data (random data are supposed by transmission facilities)
  - XOR with pseudo-random sequence at transmitter and receiver side
- Encoding (Flyby)
- Interleaving – protects against impulse noise
- Mapping of groups of bits into modulation symbols

PMD Sublayer Options

Frequency Hopping Spread Spectrum

- Developed for military purposes (concealment of tr.)
  - Frequency band is divided into 75 1-MHz channels
- Transmitter alters channels (max 400 ms per channel)
  - Every station has a unique channel hopping pattern
    - Hopping patterns assigned by AP
    - 3 alternative hopping patterns are defined in Europe
- Allows coexistence of multiple independent systems in the same frequency band
  - According to 802.11, 26 systems may theoretically coexist in 2.4 GHz frequency band
- Simpler manufacturing
  - Does not use sophisticated calculations
    - Less power consumption
- Problem: as the hopping patterns are fixed, even the noised channels are used for transmission
- 802.11 defines 12Mbps and 2 Mb/s FHSS scheme

Direct Sequence Spread Spectrum

- Defined in 802.11 for 1Mb/s and 2 Mb/s
- The transmitted information is encoded so that it is spread into 22 MHz band
  - Three 22MHz bands are available
  - Spreading is accomplished using s chip sequence
    - Binary 1= chip sequence is transmitted, binary 0 bit=negation of chip sequence is transmitted
    - Individual stations use unique chip sequences
      - Mutually orthogonal, expressed in +1, -1 values
    - Knowing the chip sequence of a particular transmitter, the receiver may reconstruct just that transmitter's data from the signal that is a mixture of multiple transmissions
      - inner product of the received signal with the transmitter chip sequence
  - A 1MHz bit stream is converted to a 11MHz chip sequence (1b=11 chips).

High-Rate DSSS

- Enhanced DSSS
- Defined in 802.11b for 5.5 and 11 Mb/s

Orthogonal Frequency Division Multiplexing (OFDM)

- A frequency band is divided into multiple narrow-band channels with smaller bitrates (similar to ADSL)
  - Signal of each single low-speed channel is more immune
  - max. 54 Mb/s
- All channels use the same number of bits expressed by a modulation symbol
  - As the initial media measurement does not make sense on the wireless media – propagation conditions may change very rapidly
- Shorter reach
  - especially in the rugged terrain
- Originally utilized in 802.11a standard (5 GHz), later also in 802.11g (2.4 GHz)

Data rates in OFDM

- Defined by modulation & coding scheme index (MCS)
  - 802.11g/802.11n
    - OFDM is used with
      - 20 MHz channel - 52+4 subcarriers
      - 40 MHz channel
    - Modulation: BPSK, QPSK, 16-QAM, 64-QAM
    - Coding rate – the forward error correction (how much bits encode data): 1/2, 2/3, 3/4, 5/6
    - Guard interval: 400/800 ns
    - Number of parallel spatial streams: 1-4
  - Combination 802.11a/g – more MCS streams
  - 802.11ac
    - Adds 256-QAM (FEC 3/4 and 5/6)
    - 80/160 MHz channels

Signal Propagation Problems

- Multi-path reflections
  - Multiple reflected signals that traveled along different paths sum up on the receiver
  - Delay differences may not exceed 500 ns
- Hidden node problem
  - Station S detects a free channel in its neighborhood, but it is not free in the receiver's neighborhood (typically AP) – the source of the signal is not visible from station S
    - Caused by a limited signal reach and obstacles in the signal path
    - May be solved by RTS-CTS mechanism

Wireless Media Access Methods

- Distributed Coordination Function (DCF)
  - CSMA/CA
- Point Coordination Function (PCF)
  - for real-time applications (QoS may be implemented)
  - AP assigns the bandwidth to individual stations (polling)
  - Commonly combined together with DCF
    - Contention-Free Period and Contention Period (superframe)
  - Not implemented and utilized very often today
- IEEE 802.11e (802.11i)
  - 8 priorities, IFS has to be proportional to the priority value
  - admission control (distributed/centralized)
    - Timeslot reservation

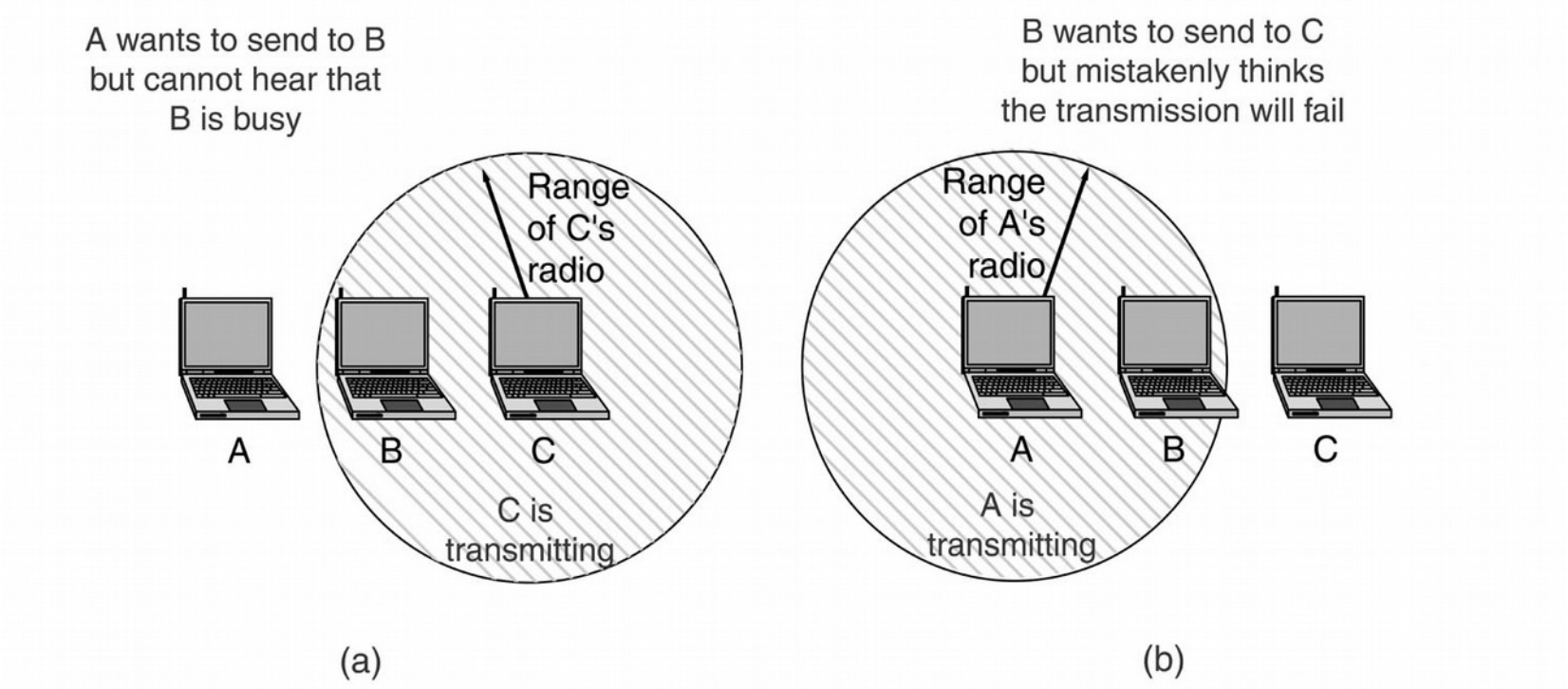
Collisions on the Wireless Media

- The detection of the collision is problematic on the wireless media
  - The same antenna cannot be utilized for transmission and reception at the same time
  - Station may not hear all the other stations well
    - Hidden node problem
- We may detect the free medium, but not the collision
- A solution is to acknowledge all received frames

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

- CSMA
  - A free channel has to be detected before a transmission may start
  - A pause of the duration (DIFS+ random interval) follows
- Avoids collision of the acknowledgment frames
- After a frame is transmitted, a timeslot is reserved for transmission of an acknowledgment
  - The frame header carries the duration of the frame transmission (including time necessary for acknowledgment)
  - An acknowledgment is sent in short inter-frame space – SIFS
- If a transmitter does not receive frame acknowledgment in a specified timeout, it waits for a random time and makes a new attempt
- Broadcasts and multicasts are not acknowledged

Hidden Node Problem

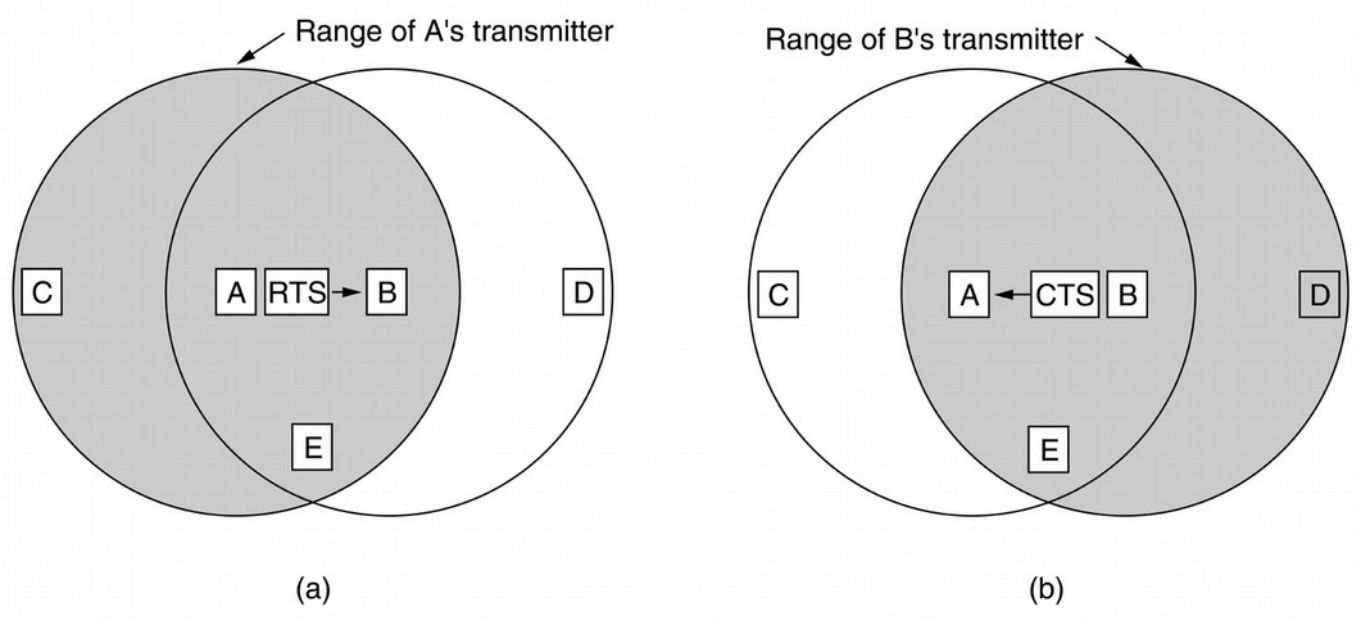


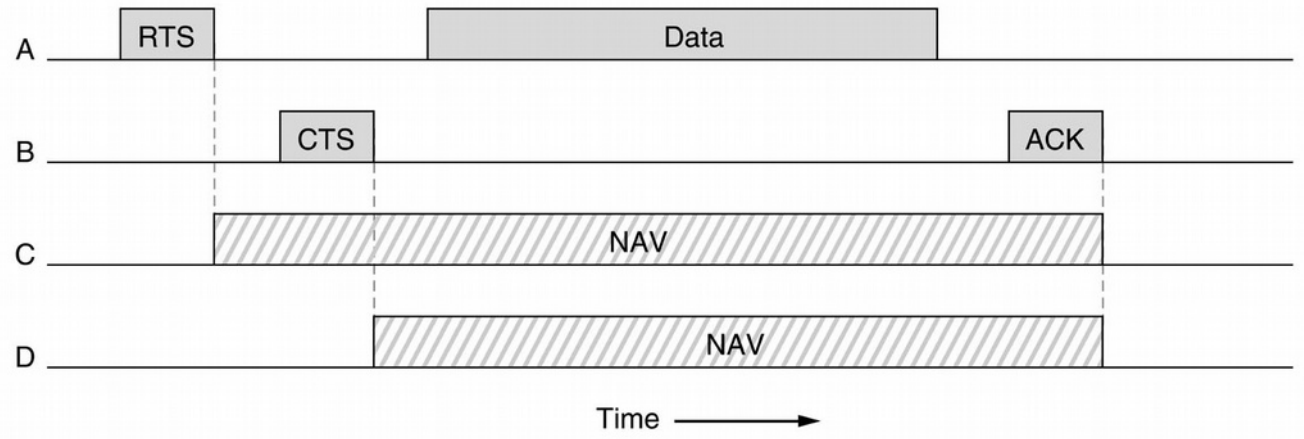
Solution of the Hidden Node Problem (1)

- A station that wants to transmit sends RTS frame first
  - RTS identifies source, destination and duration of the intended transmission
  - Duration of RTS+CTS+data+ACK, always with SIFS
- The destination station sends CTS with the intended transmission time copied
  - just the remaining part of the interaction
- All stations that hear RTS or CTS have to treat the medium as busy for the advertised transmission duration interval

The result is that all station in both the transmitter and receiver signal range are informed about the ongoing transmission

Solution of the Hidden Node Problem (2)





Advantages of RTS-CTS Mechanism

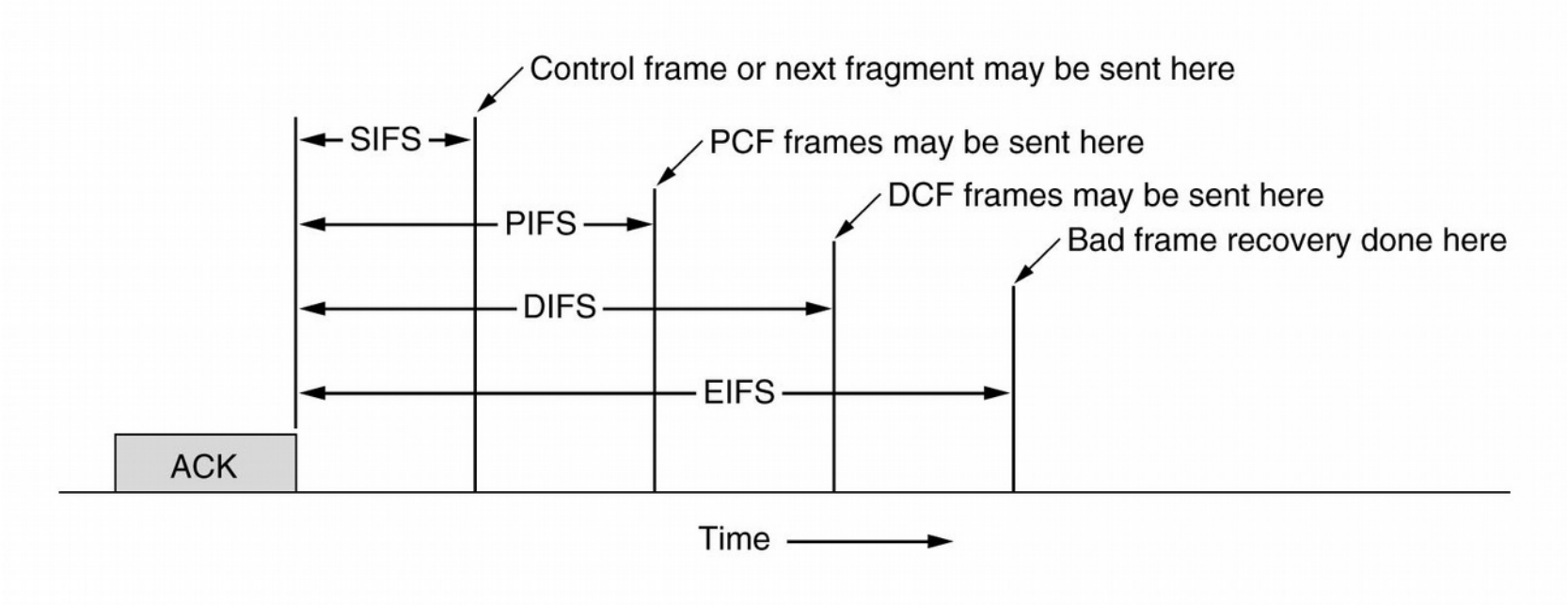
- Only RTS frames may collide
  - As RTS is very short, the impact to the efficiency is limited
- Efficient only for long data frames (much longer than RTS frames)
  - A threshold of the data frame length for usage of RTS-CTS mechanism may be configured
- Commonly switched off completely on point-to-point links
  - as there are no hidden nodes

Link Layer

Responsibilities of Link Layer

- CRC calculation and checking
- Fragmentation of frames
  - As there is a high probability of interference, sending a frame by a multiple shorter fragments decreases overhead in case of a retransmission
  - A threshold of a length of frame that will be fragmented may be defined
  - From MAC protocol perspective, all fragments of a frame are sent as a single burst
  - broadcast a multicast fragments are never fragmented
- Frame header informs about a modulation used to transmit (the rest of) the frame
  - Header is always sent on the basic bitrate
- Several lengths of interframe spaces are defined
  - Used in MAC protocol and traffic prioritization.

CSMA/CA Timing



IEEE 802.11 Frame Types

- Data frames
  - contains the useful information passed between transmitter and receiver
- Control frames
  - control information that accompanies the data frames
- Management frames
  - Connection into WLAN, authentication

Management Frames

- Association Request, Association Response, Reassociation Request, Reassociation Response, Disassociation
- Probe Request, Probe Response
- Authentication, Deauthentication
- Beacon (transmitted periodically by an AP or by a dedicated station in IBSS)
- Announcement Traffic Indication Frame (ATIM)

Management Frames contain the fixed parts (different for various frame types) and optional Information Elements (IE)

Examples of IEs

- SSID
- Supported Rates – multiplies of 500 kbps
- Frequency hopping parameter set
  - dwell time, hopping pattern
- Direct Sequencing (DS) parameter set
  - channel number
- Contention Free (CF) parameter set
  - CFPMaxDuration, CFPDurationRemaining, time to nearest CFP, interval between CFPs
- TIM (Traffic Indication Map)
  - informs about frames buffered for individual stations in power-save mode
- Interval between timeslots for sending of broadcast and multicast frames

Control Frames

- Request to Send (RTS), Clear to Send (CTS)
- Acknowledgment (ACK)
- PS-Poll (Power Save Poll)
- CF-End (Contention Free Period End)
- CF-End+CF-Ack (Contention Free Period End + ACK of last data frame)

Data Frames

- Data
- Data+CF-Ack
- Data+CF-Poll
- Data+CF-Ack+CF-Poll
- Null data
- CF-ACK (without data)
- CF-Poll (without data)
- CF-Ack+CF-Poll (without data)

Discovery of Access Point

Initiated by a station

- Active
  - Probe Request on all channels (involves station's SSID and all supported rates)
  - AP responds with Probe Response
    - contains SSID, supported rates, parameters of the physical layer assigned to a requesting station
      - (hopping pattern for FHSS, chip sequence for DSSS)
- Passive
  - Listening for beacon frames (on all channels)
  - Takes a longer time

Authentication

- One-way
  - Station authenticates to the AP
- Open and Shared Key Mode
  - Open = no authentication
  - Shared Key = authentication using the shared WEP key
    - challenge-response protocol
- Authentication frame
  - used for both request and response

Association with Access Point (1)

- During association, AP maps its logical port to a particular station
  - Association Request (from station)
    - involves SSID, supported rates, listen (wakeup) interval for frame reception from the AP (in power save mode)
  - Association Response (from AP)
    - status code, Association ID, supported rates
    - Association ID used for the future management of the communication on the radio channel

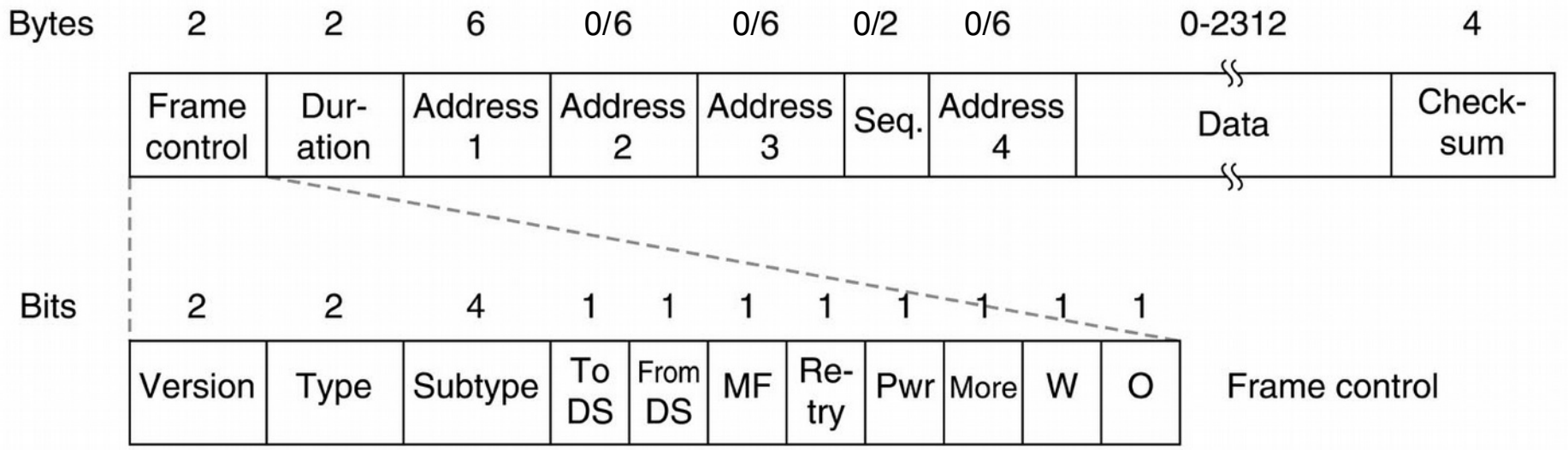
Association with Access Point (2)

- A station may be associated only to a single AP at the same time
  - If a station looses the signal, it tries to make a handover to different AP
  - The conditions that trigger the handover and the way the station chooses the new AP are dependent on the wireless card driver implementation
    - signal quality, number of collisions in the BSS-retry counters,…
- AP commonly supports tens of associations
  - Number of stations associated with AP is much more limited by the available bandwidth

Power-Save Mode

- Allows to save station's battery while maintaining the possibility of reception of frames destined for the station
- AP buffers unicast frames for stations in their sleeping interval
  - Station periodically awakes to receive the beacon frame from the AP (wakeup interval)
    - beacon frame informs which stations have the frame buffered on the AP (utilizes Association ID)
  - After an awaken station hears that AP has a frame buffered for it, it requests the frame using a Poll frame
- A wakeup interval is defined by AP administrator and propagated in beacon frames
  - Broadcast/multicast frames have to be buffered if there is at least one power-save station in the BSS

IEEE 802.11 Link Layer Frame



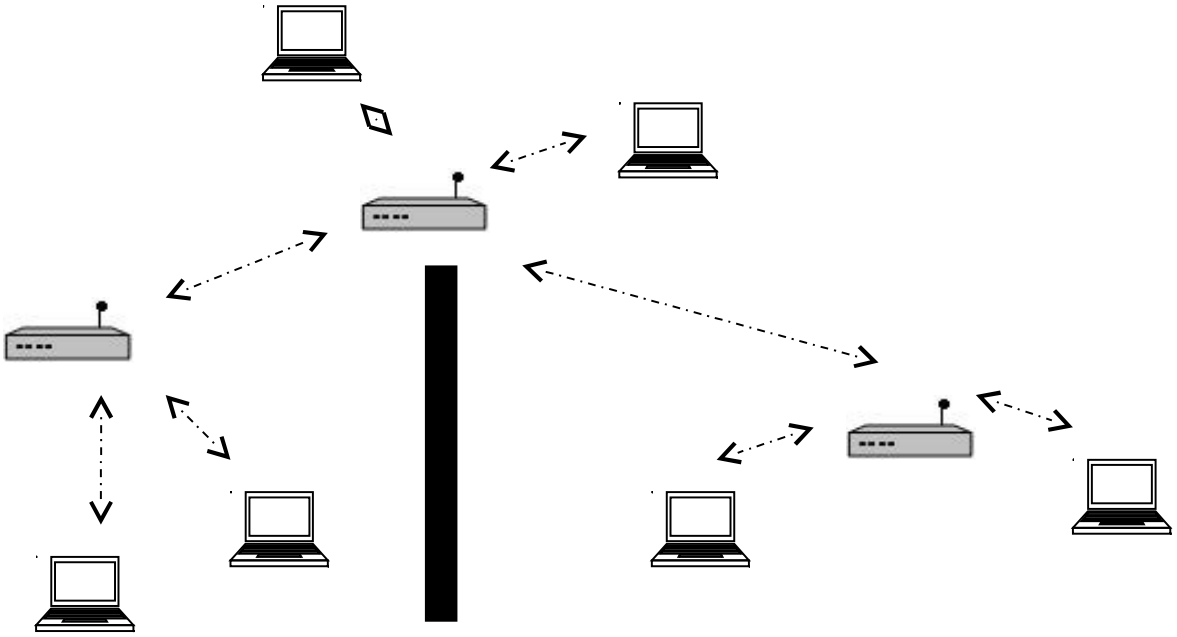
- Address 1 – receiver, Address 2 – transmitter
- Address 3 – mostly BSSID
  - But in Mesh also Address 3/4 destination/source STA
- QoS (0/2 bytes) field and High throughput control (0/4 bytes) field can be added before data portion

Special Networking Devices of the Wireless Infrastructure

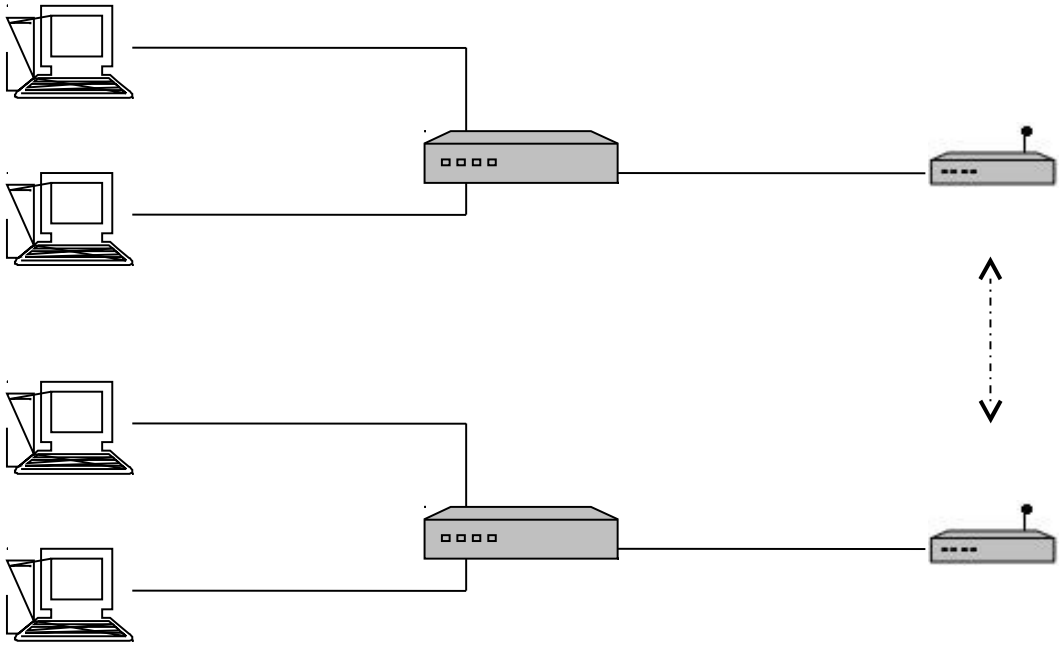
Repeater, Bridge

- Repeater AP
  - Purely wireless bridge (not connected to a wired network)
  - Sends and receives on the same channel – divides the throughput by 2
  - Repeater is associated as a client of another AP
- Workgroup Bridge
  - Connect a working group of stations equipped with Ethernet NIC to a wireless network
    - acts as Ethernet switch/hub with WiFi NIC
  - Encapsulates Ethernet frames into WiFi frames, the receiving AP has to decapsulate them accordingly
- Wireless Bridge
  - A variation of the workgroup bridge
  - Provides a point-to-point wireless interconnection of two LANs

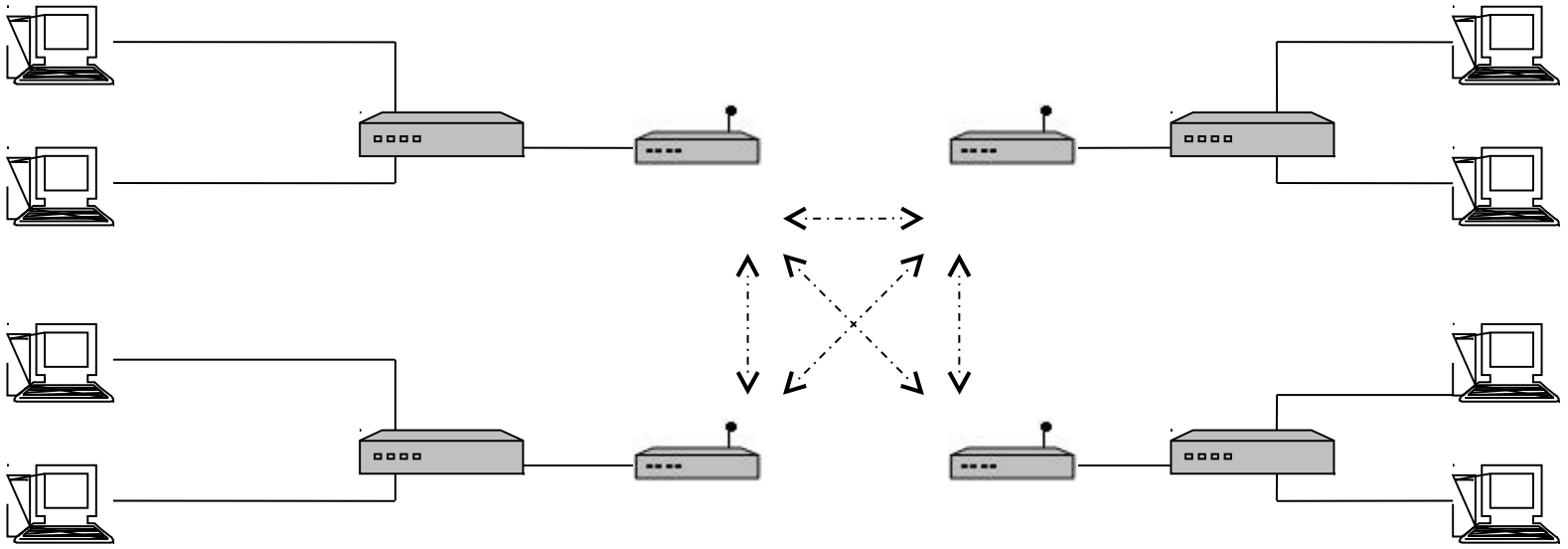
Usage of the Repeater



Usage of the Point-to-Point Bridge



Usage of the Point-to-Multipoint Bridge



Interoperability of Special Wireless Infrastructure Devices

The functionality of special devices is NOT standardized

- Nomenclature is not unified
- Uncertain interoperability between vendors
- Not all APs support the „client mode“, i.e. the ability of being a client of another AP

WiFi Security (1)

- Authentication
  - Open + Shared key
- Encryption
  - WEP – Wired-Equivalent Privacy
    - Shared key (64/128B), used simultaneously for encryption and authentication
    - Easy to crack (if the attacker has enough time and sufficient traffic on the channel)
      - Matter of tens of minutes
      - Freely available cracking software
    - It is recommended to use together with a mechanism of periodic change of encryption keys

WiFi Security (2)

- WiFi Protected Access – WPA
  - Repairs main WEP drawbacks
  - Problems of the initialization vector
  - Temporal Key Integrity Protocol (TKIP)
- WPA2=802.11i
  - better encryption algorithm (AES)
  - Still not implemented in some old WiFi devices

Intelligent Wireless Networks and Wireless Mesh Networks

Basic Features of Intelligent WiFi Networks (1)

- Centralized WLAN management
  - WLAN Controller
- A coverage by a wireless signal is accomplished using „lightweight“ APs managed by a WLAN controller
  - AP download their configuration from WLAN controller
    - Increases security, easier centralized management
  - L2/L3 traffic tunneling to WLAN controller (LWAPP)
    - Secure operation of multiple different kinds of users on a shared wireless infrastructure
  - Support for L2 and L3 roaming

Basic Features of Intelligent WiFi Networks (2)

- Coordinated physical layer management
  - Dynamic channel assignment (according to noise conditions, AP interferences, load on individual channels)
  - Control of the transmission power (compensation of AP outages)
  - Detection of rogue APs + enforcing of client reassociation to the authorized AP
  - Balancing of client association to individual APs

Wireless Mesh

- Outdoor wireless network solution
- Combines 2.4 and 5 GHz bands
  - 5 GHz Wireless distribution system -
  - 2.4 GHz hot-spots
  - Roof APs (RAP) and Mesh APs (MAP)
- Traffic may be bridged into wired infrastructure by RAP or tunneled to a WLAN controller
- Path over the wireless mesh is determined using a special protocol
  - Adaptive Wireless Path protocol
  - Hybrid Wireless Mesh Protocol
  - Some other protocol, e.g. OLSR or B.A.T.M.A.N