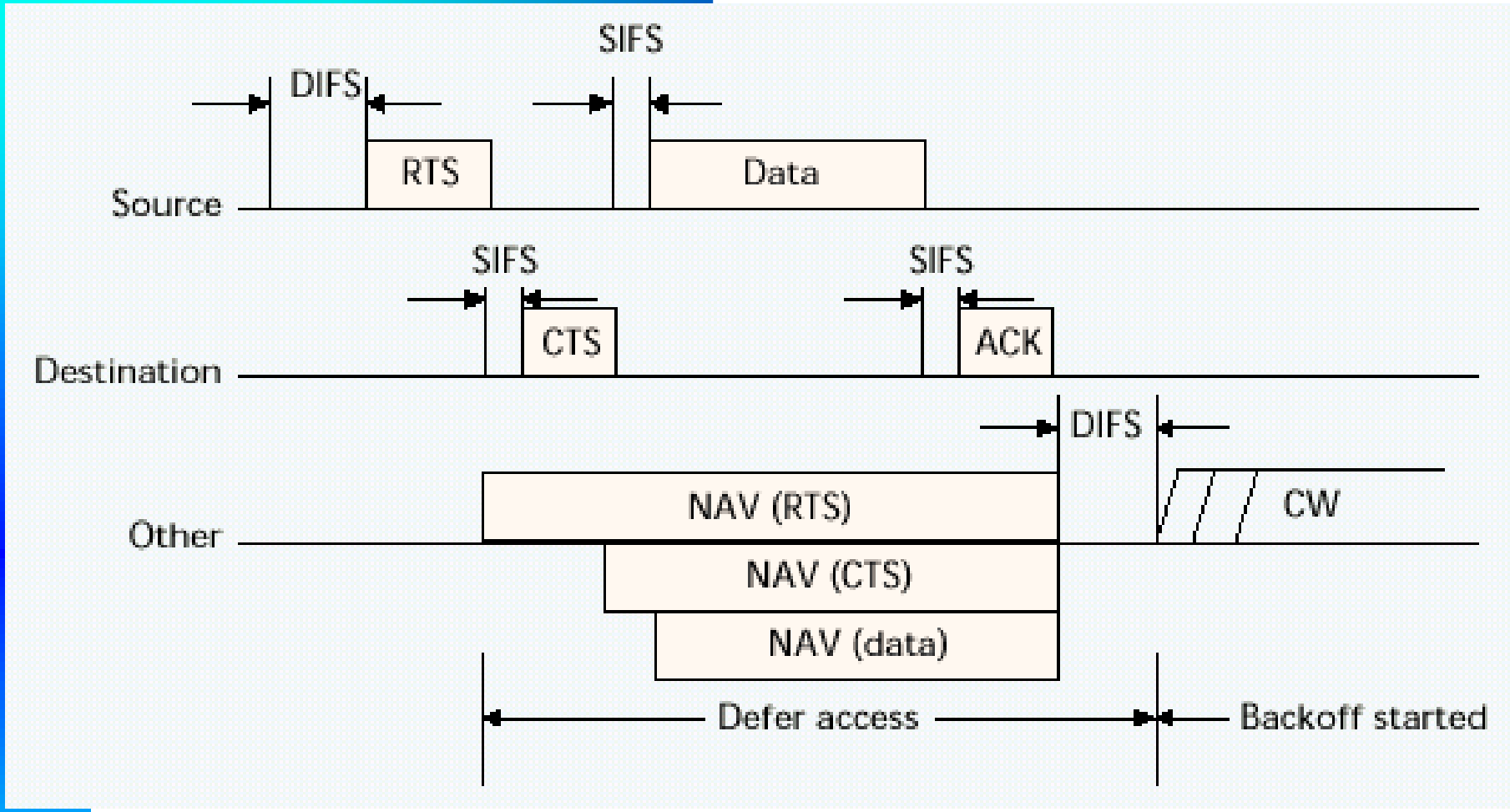
Mobile and Wireless Networks

Multiple Access Protocols and IEEE 802.11 Networks

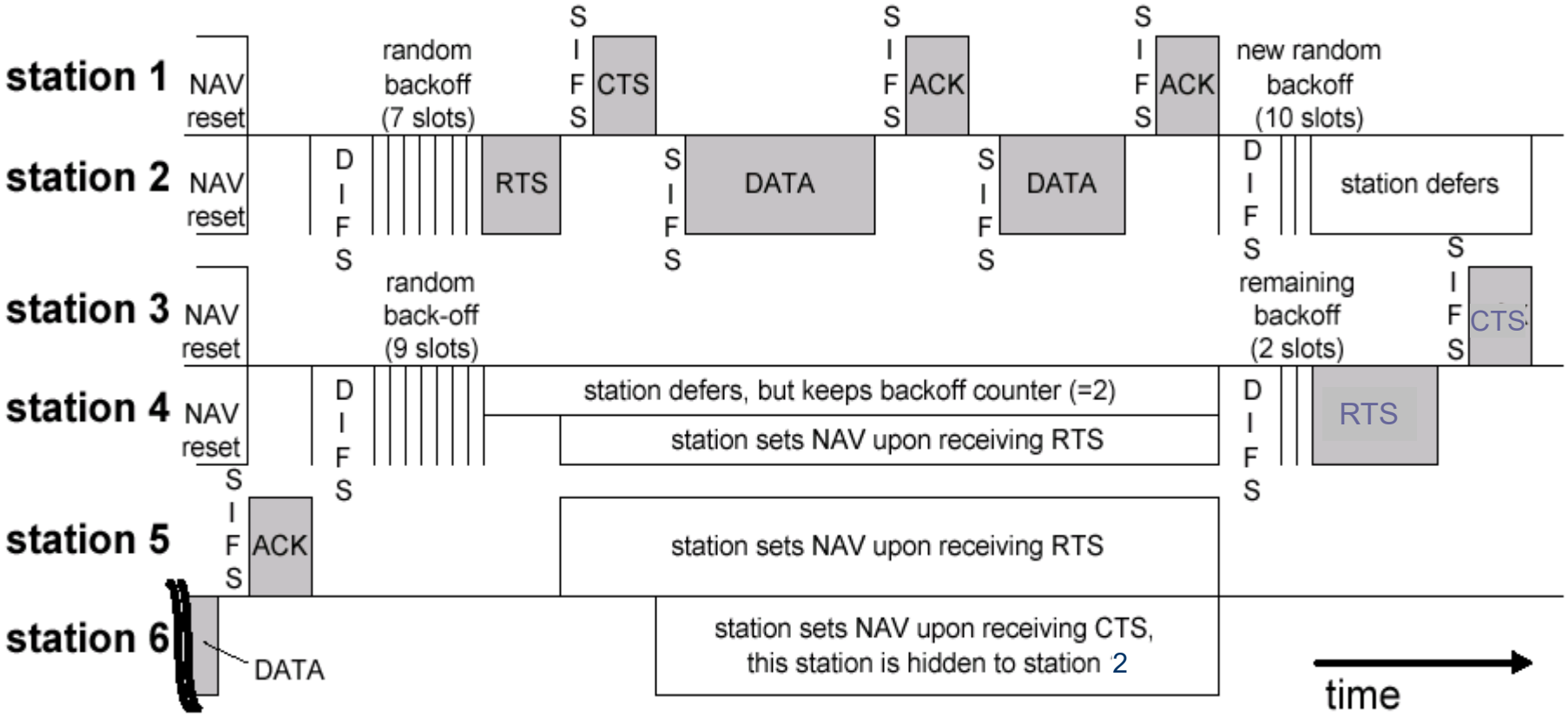
PART 2



- Always SIFS<DIFS

- Updating of NAVs (Network Allocation Vectors) very important through RTS/CTS/data packets to use power saving

Example of DCF transmission



CW doubles after each collision

- Initial CW -> 3 (backoff 0-3)
- CW after Collision 1 → 7 (backoff 0-7)
- CW after Collision 2 → 15 (backoff 0-15)
- CW after Collision 3 → 31 (backoff 0-31)
- CW after Collision 4 → 63 (backoff 0-63)

How the Contention Window works

- Whenever a backoff occurs the backoff time is uniformly chosen in the range $[0, W-1]$
- After each unsuccessful transmission the backoff windows size is doubled, up to a maximum value
- Once the backoff window size reaches its maximum value it will stay at that value until it is reset
- The value of W will be reset after every successful transmission of a data or RTS packet, or when a retry counter reaches its limit

Disadvantages of DCF

- Unpredictable collision number
- Unpredictable delay of successful transmission
- Unpredictable throughput
- Uncontrolled selection of station to transmit

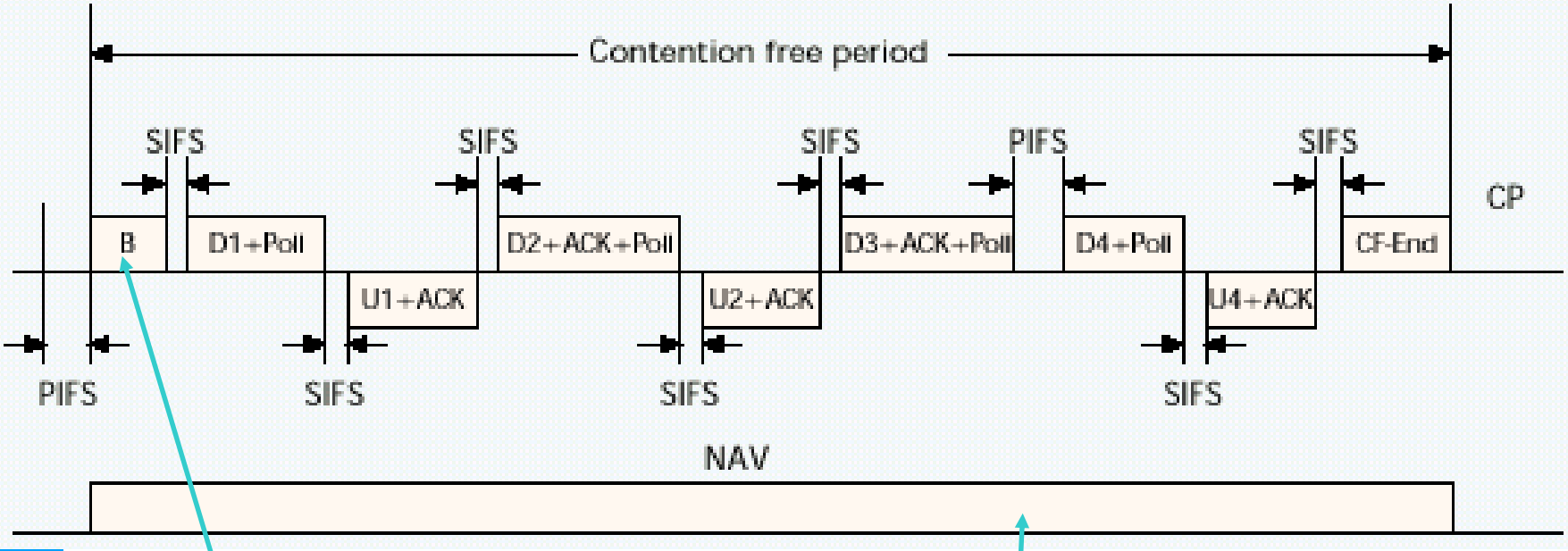
And one advantage:

- Low transmission delay and good performance for low traffic

Point Coordination Function (I)

- ✓ Activated by the AP whenever it decides to switch to contention-free period (e.g. when it observes large number of collisions)
- ✓ As a general rule, DCF for low traffic, PCF for high traffic
- ✓ In this mode the AP is referred to as Point Coordinator
- ✓ It has priority compared to DCF because it is activated for idle period PIFS<DIFS

Point Coordination Function (II)

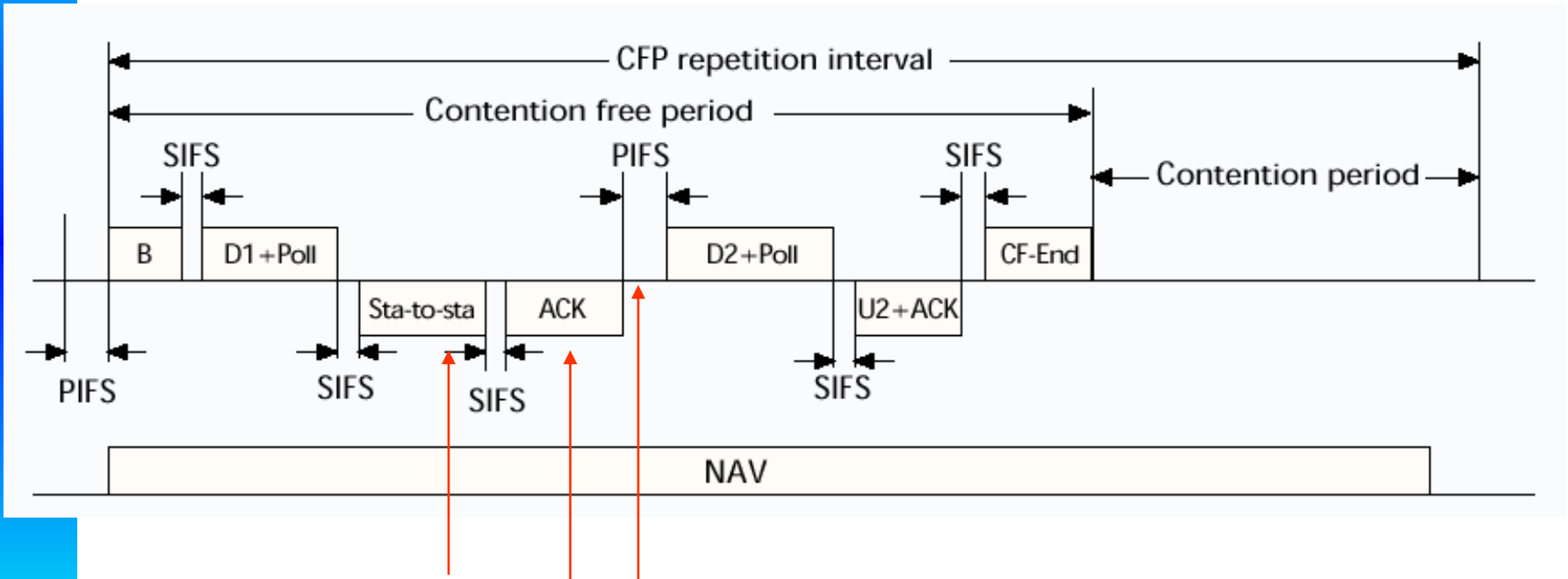


Synchronization beacon

Variable duration of
Contention Free Period

Point Coordination Function (III)

If a Station wants to transmit to another station during a CFP (contention-free period)



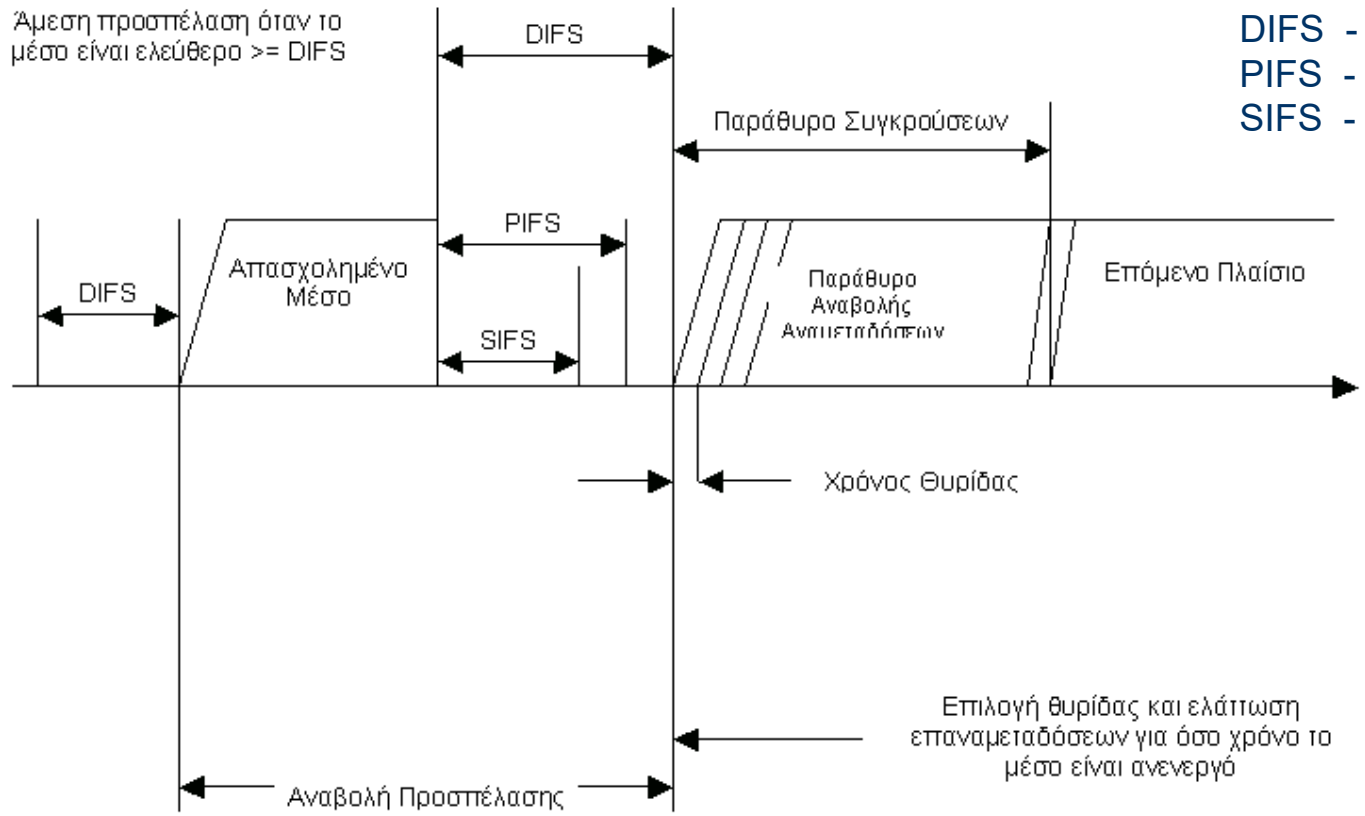
- When it is time to transmit, a STA chooses to transmit to aniother STA in the same BSS
- When the other STA receives data, replies with DCF Ack to the first STA
- AP waits for time equal to PIFS before continuing to the next STA (why?)

Main restrictions of PCF regarding QoS

- ✓ Terminals cannot send their requirements to PCF
- ✓ AP has no way to interrupt an ongoing transmission to send the synchronization beacon* and pass to PCF mode
- ✓ Poll does not set the time the channel is given to a STA, which means that the STA can keep the channel for the maximum allowed time*

* Maximum packet (MPDU) allowed 4095 bytes = 32760 bits = 32,76 msec (for a 1Mbps channel)

Inter-Frame Spaces



DIFS - 34 μsec
PIFS - 25 μsec
SIFS - 16 μsec

- Inter frame spacing required for MAC protocol traffic
  - SIFS = Short interframe space
  - PIFS = PCF interframe space
  - DIFS = DCF interframe space
- Back-off timer expressed in terms of number of time slots

Security in 802.11

When encryption and/or authentication is required, there things are important

- The actual needs of the user and how they cost

- Easy to use mechanisms

- And governmental restrictions in encryption methods, especially for exported products

Wired Equivalent Privacy (WEP) Protocol

- Reasonably efficient, compared to cost and actual needs it covers
- «Auto-synchronized» (STAs in and out easily)
- Low computing needs
- Optional in implementation
- Covers both encryption and authentication
- Use of the same key for both encryption and authentication (disadvantage)

Encryption

- Based on a secret key of 40 bits, statically stored in all stations
- The key passes through a bit generator to produce a bit sequence based on this
- The bit sequence is XORed with the data to be transmitted
- The output of the XOR is transmitted to the channel

Encryption example

Let binary 2 (00000010) to be the encryption key.
The key is XORed with the text we want to transmit, in our case the simple "HI"

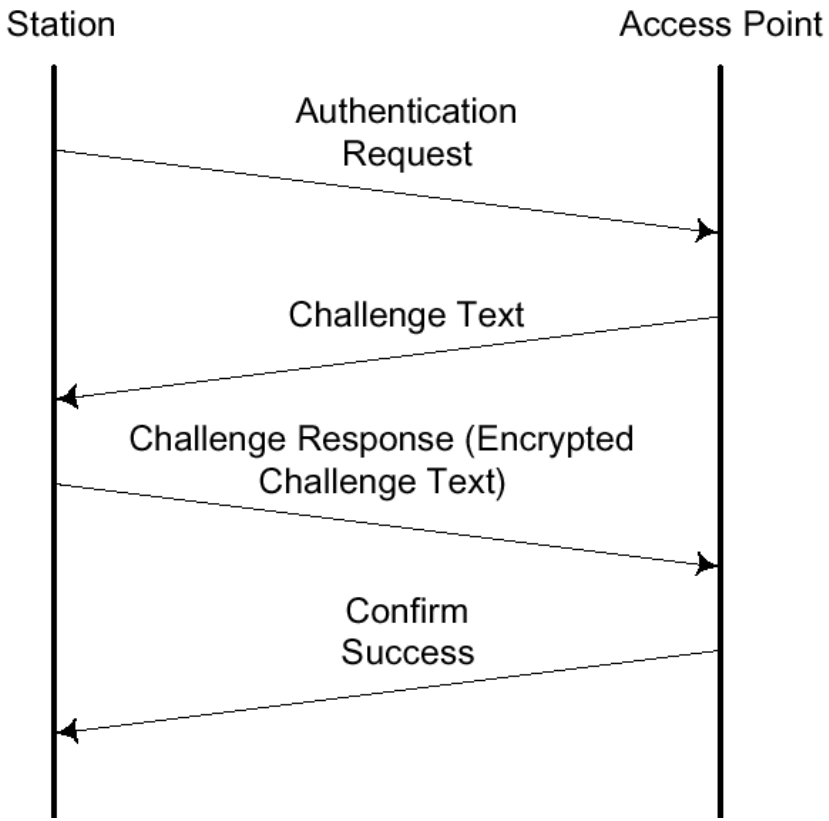
	H	I	Initial text
	0 1 0 0 1 0 0 0	0 1 0 0 1 0 0 1	
XOR	0 0 0 0 0 0 1 0	0 0 0 0 0 0 1 0	Encryption key
	0 1 0 0 1 0 1 0	0 1 0 0 1 0 1 1	Encrypted text

When the encrypted text reaches the receiver, it passes through the XOR again with the same key to recover the initial text

	0 1 0 0 1 0 1 0	0 1 0 0 1 0 1 1	Encrypted text
XOR	0 0 0 0 0 0 1 0	0 0 0 0 0 0 1 0	Encryption key
	0 1 0 0 1 0 0 0	0 1 0 0 1 0 0 1	
	H	I	Initial text

Authentication

- Uses the same secret key as in the case of encryption



Shared Key Authentication

Node

Access Point

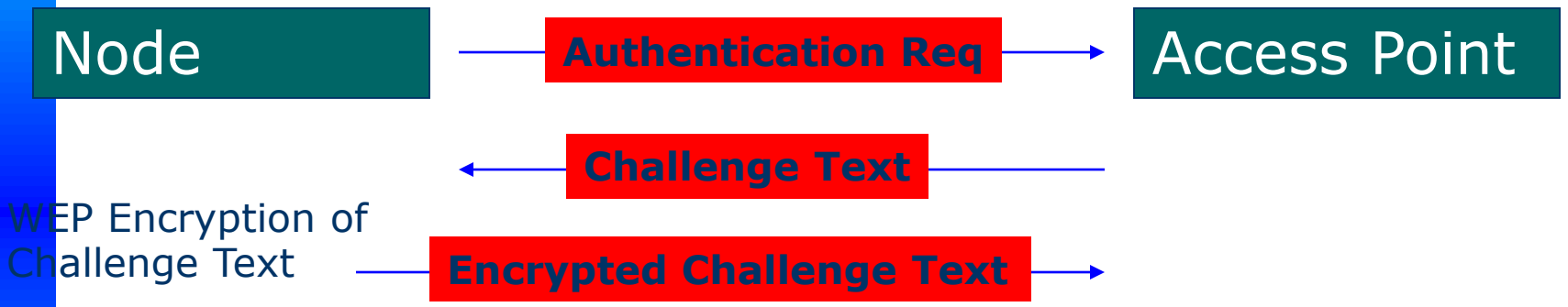
Shared Key Authentication

Shared Key Authentication

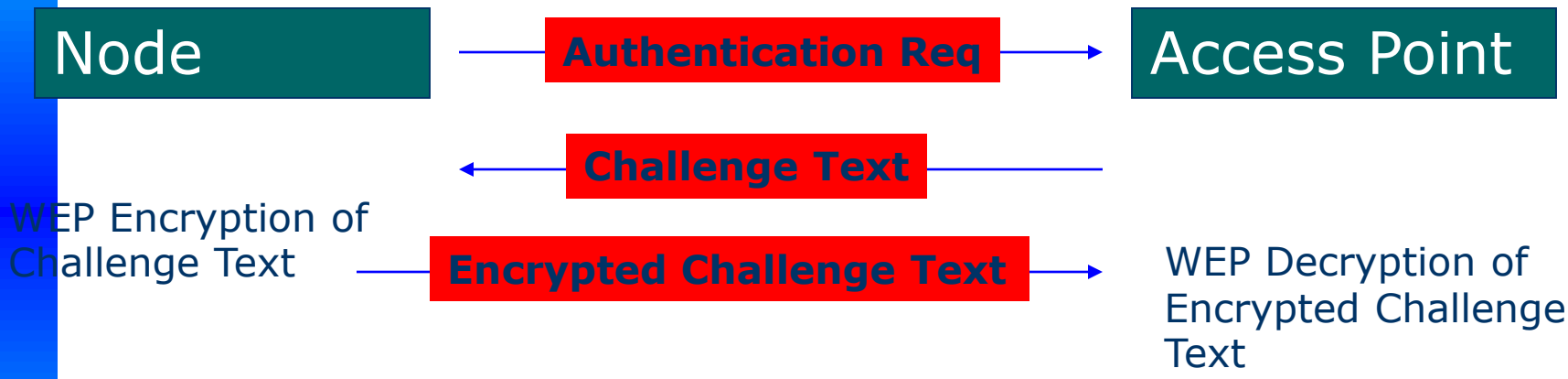
Shared Key Authentication

WEP Encryption of
Challenge Text

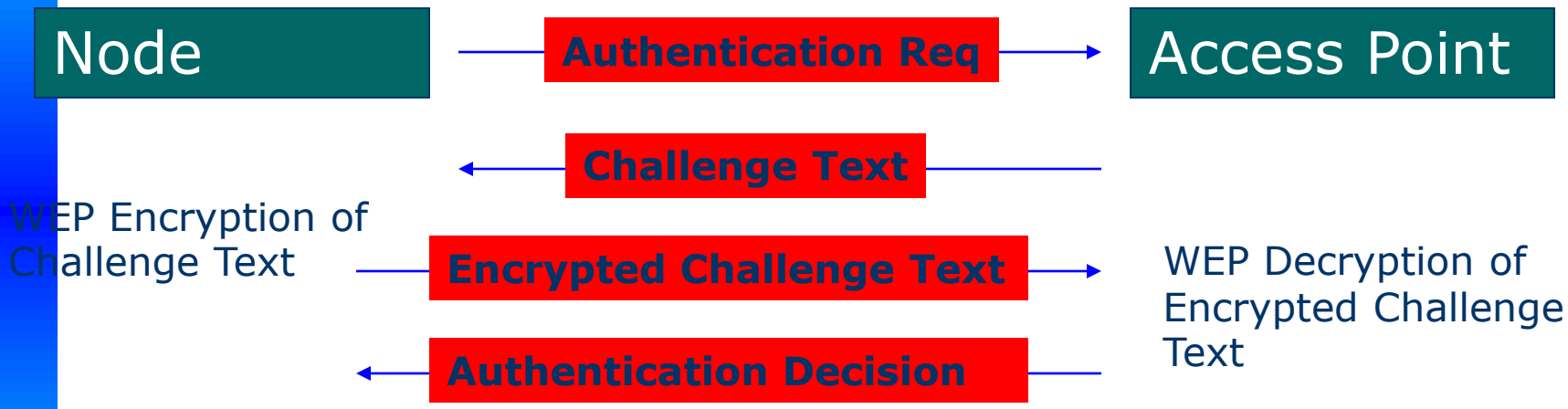
Shared Key Authentication



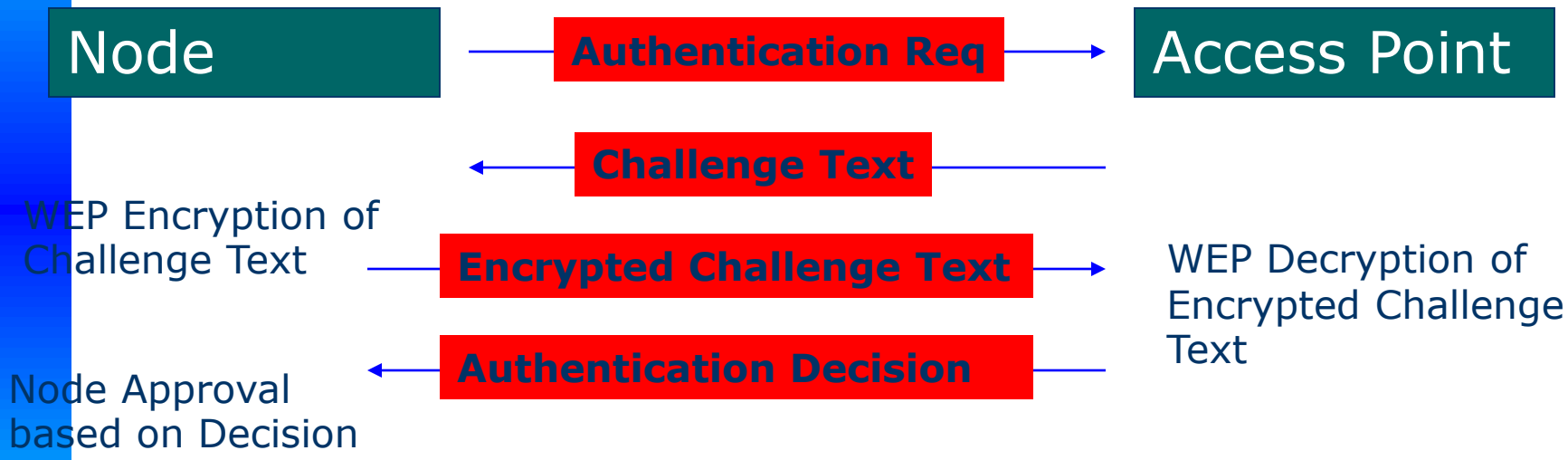
Shared Key Authentication



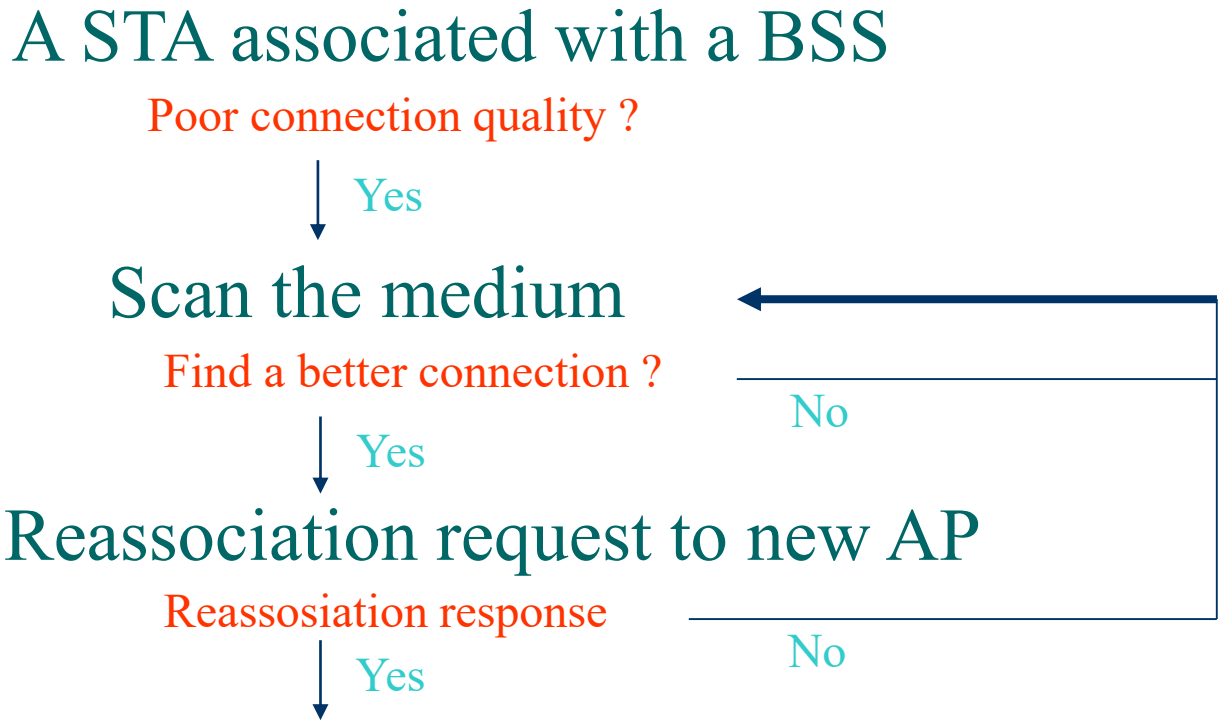
Shared Key Authentication



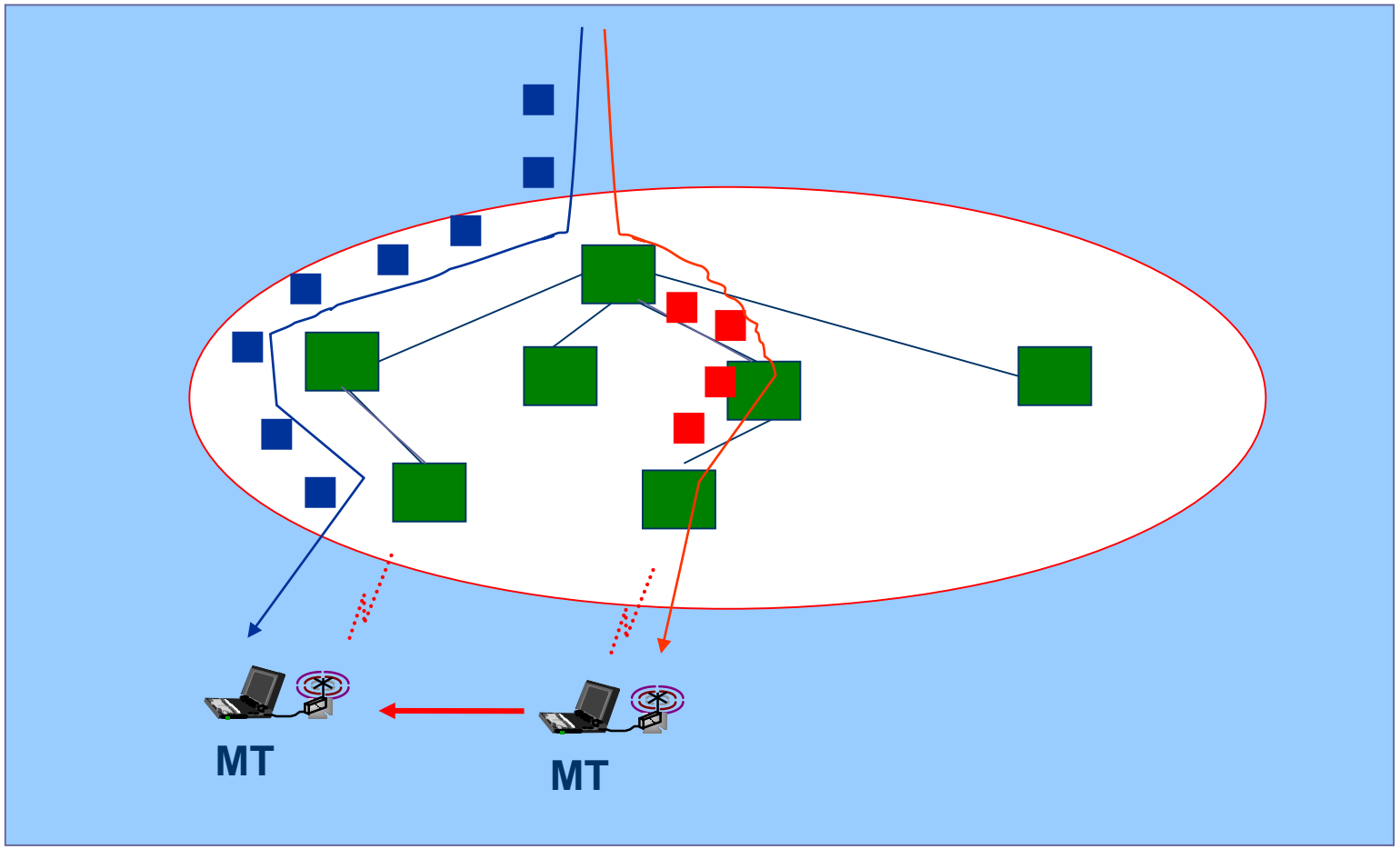
Shared Key Authentication



Mobility support



- No support for the packets that are lost during handover



Extensions of IEEE 802.11

IEEE 802.11 Group Standards

IEEE 802.11	The original 1 Mbit/s and 2 Mbit/s , 2.4 GHz RF and IR standard (1999)
IEEE 802.11a	54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
IEEE 802.11b	Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
IEEE 802.11c	Bridge operation procedures; included in the IEEE 802.1D standard (2001)
IEEE 802.11d	International (country-to-country) roaming extensions (2001)
IEEE 802.11e	Enhancements: QoS, including packet bursting (2005)
IEEE 802.11f	Inter-Access Point Protocol (2003) Withdrawn February 2006
IEEE 802.11g	54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
IEEE 802.11h	Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
IEEE 802.11i	Enhanced security (2004)
IEEE 802.11j	Extensions for Japan (2004)

IEEE 802.11 Group Standards Cont.

IEEE 802.11k	Radio resource measurement enhancements
IEEE 802.11l	(reserved and will not be used)
IEEE 802.11m	Maintenance of the standard; odds and ends.
IEEE 802.11n	Higher throughput improvements using MIMO (multiple input, multiple output antennas)
IEEE 802.11o	(reserved and will not be used)
IEEE 802.11p	WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
IEEE 802.11q	(reserved and will not be used, can be confused with 802.1Q VLAN trunking)
IEEE 802.11r	Fast roaming Working "Task Group r"
IEEE 802.11s	ESS Mesh Networking
IEEE 802.11T	Wireless Performance Prediction (WPP) - test methods and metrics Recommendation
IEEE 802.11u	Interworking with non-802 networks (for example, cellular)
IEEE 802.11v	Wireless network management
IEEE 802.11w	Protected Management Frames
IEEE 802.11x	(reserved and will not be used)
IEEE 802.11y	3650-3700 Operation in the U.S.

Physical layer extensions

IEEE 802.11b

- compatible MAC as in 802.11
- larger data rates in 2.4 GHz (11Mbps)
- Direct Sequence Spread Specrtum (FDM)

IEEE 802.11a

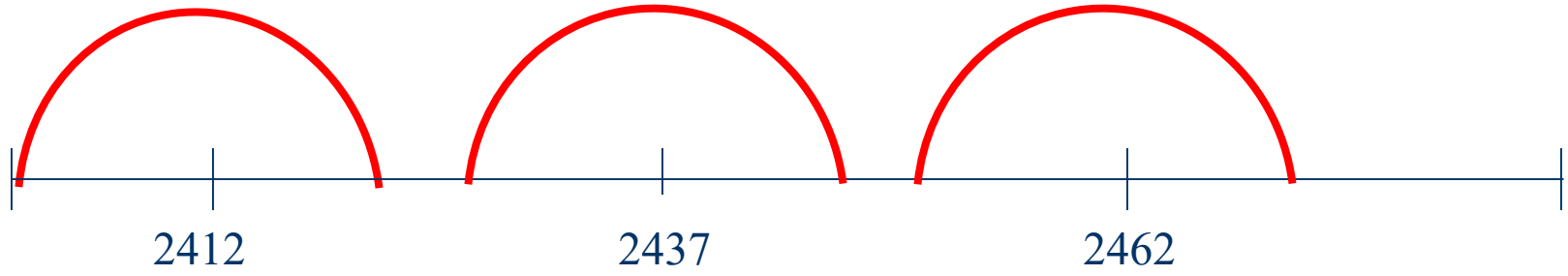
- compatible MAC as in 802.11
- 5 GHz band
- OFDM (Orthogonal Frequency Division Multiplexing)
- data rates up to 54 Mbps

IEEE 802.11g

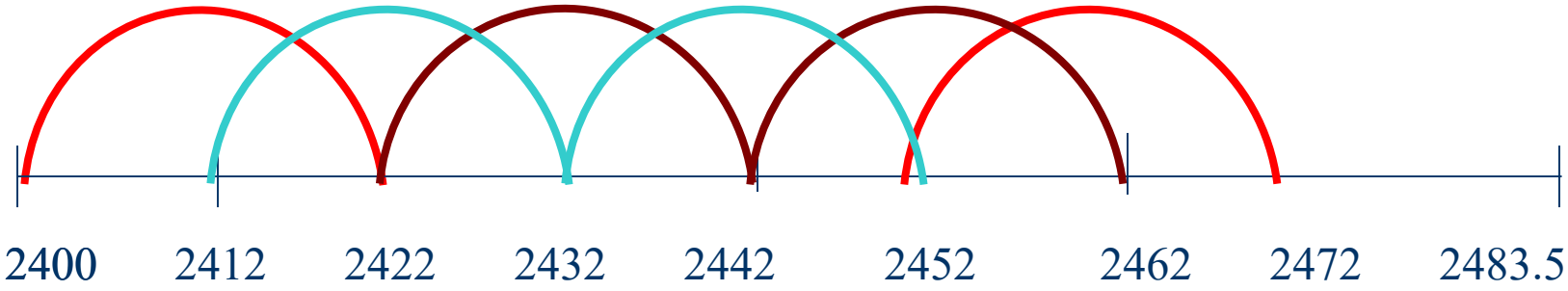
- compatible MAC as in 802.11
- larger data rates at 2.4 GHz (up to 54Mbps)
- OFDM (Orthogonal Frequency Division Multiplexing)

WiFi Channels

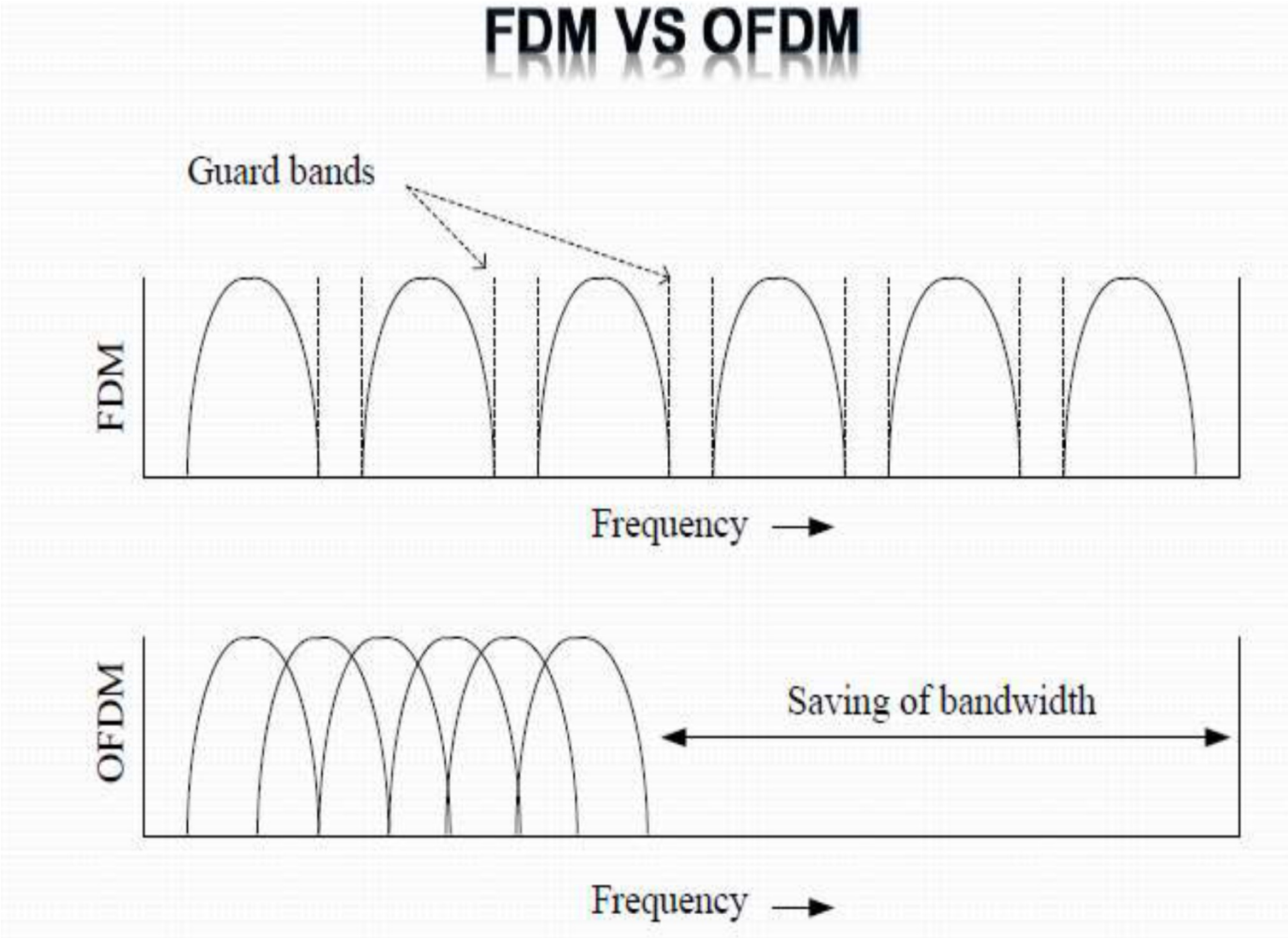
Non overlapping channels



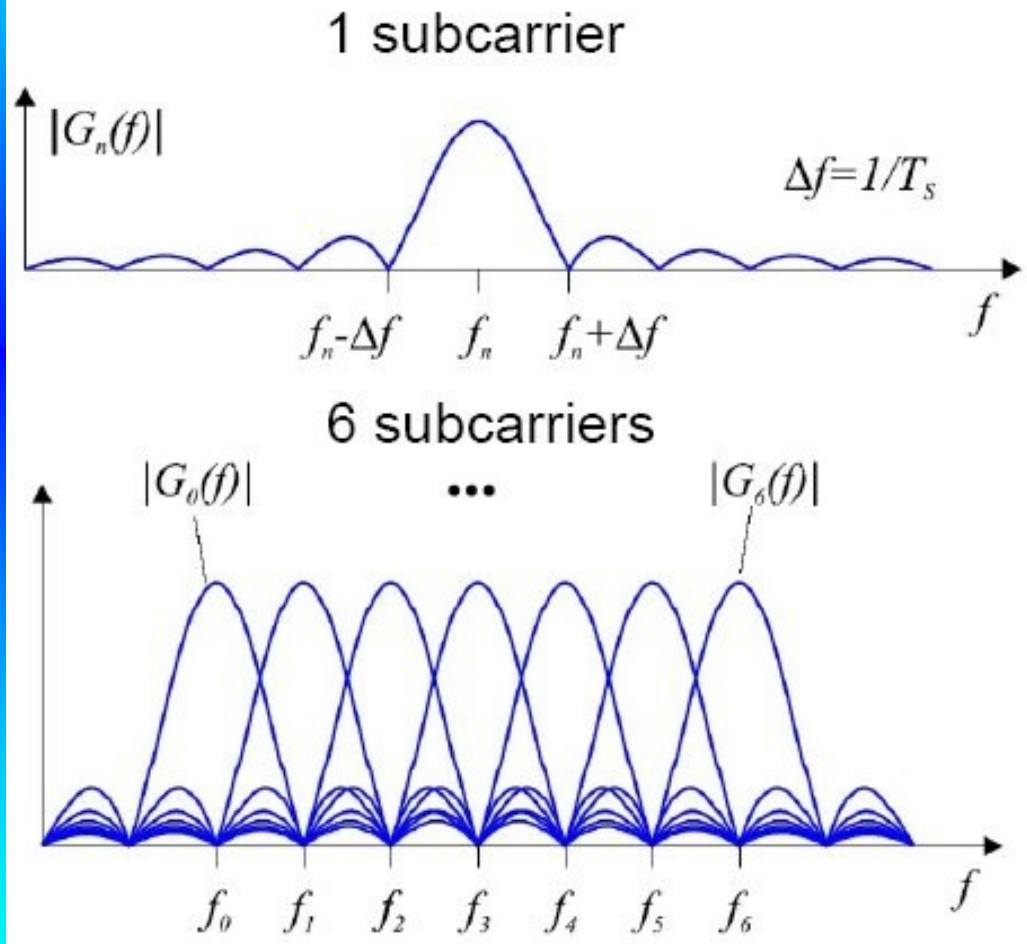
Overlapping channels



OFDM


FDM VS OFDM
Guard bands
FDM
Frequency
OFDM
Saving of bandwidth
Frequency

OFDM



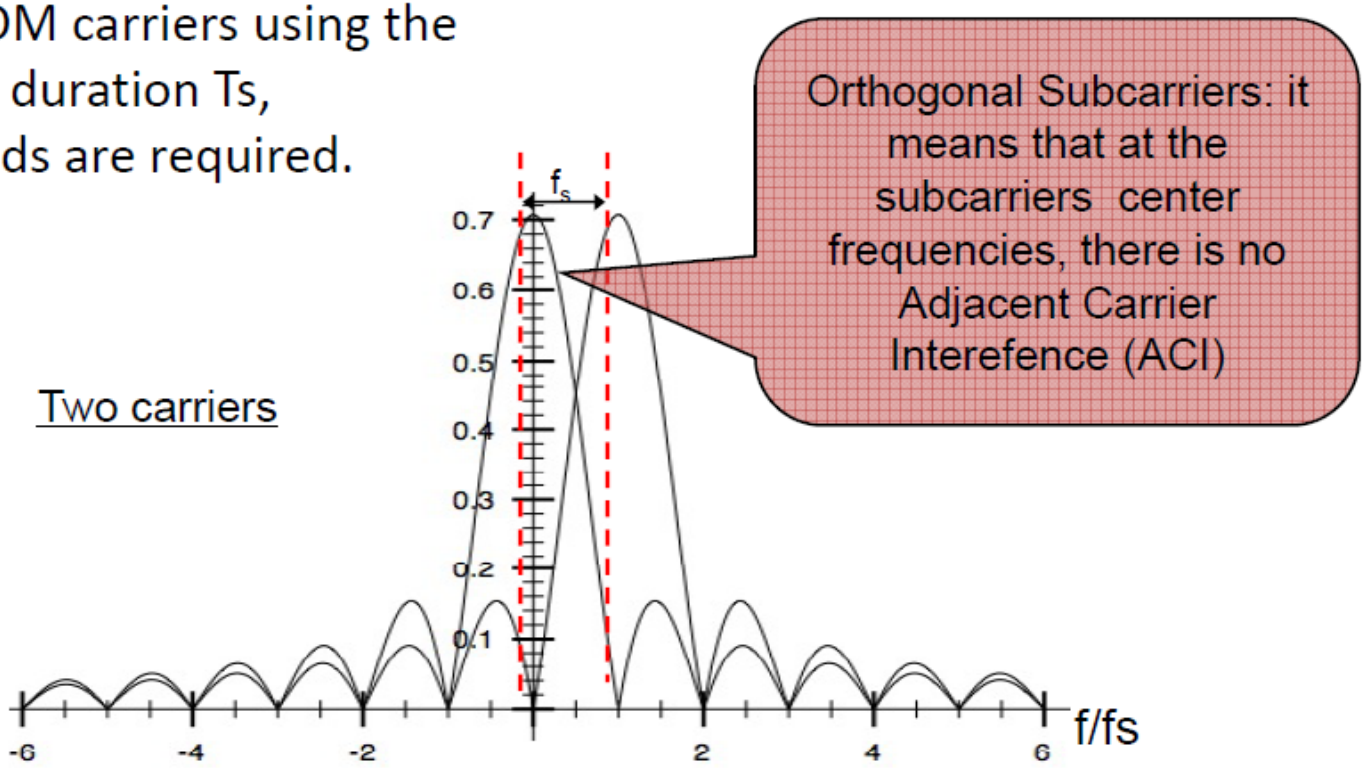
- Improved spectral efficiency
- Reduce ISI effect by multipath

OFDM: Orthogonal Frequency Division Multi-Carrier

Thus OFDM simply places the next carrier exactly in the first null point of the previous one.

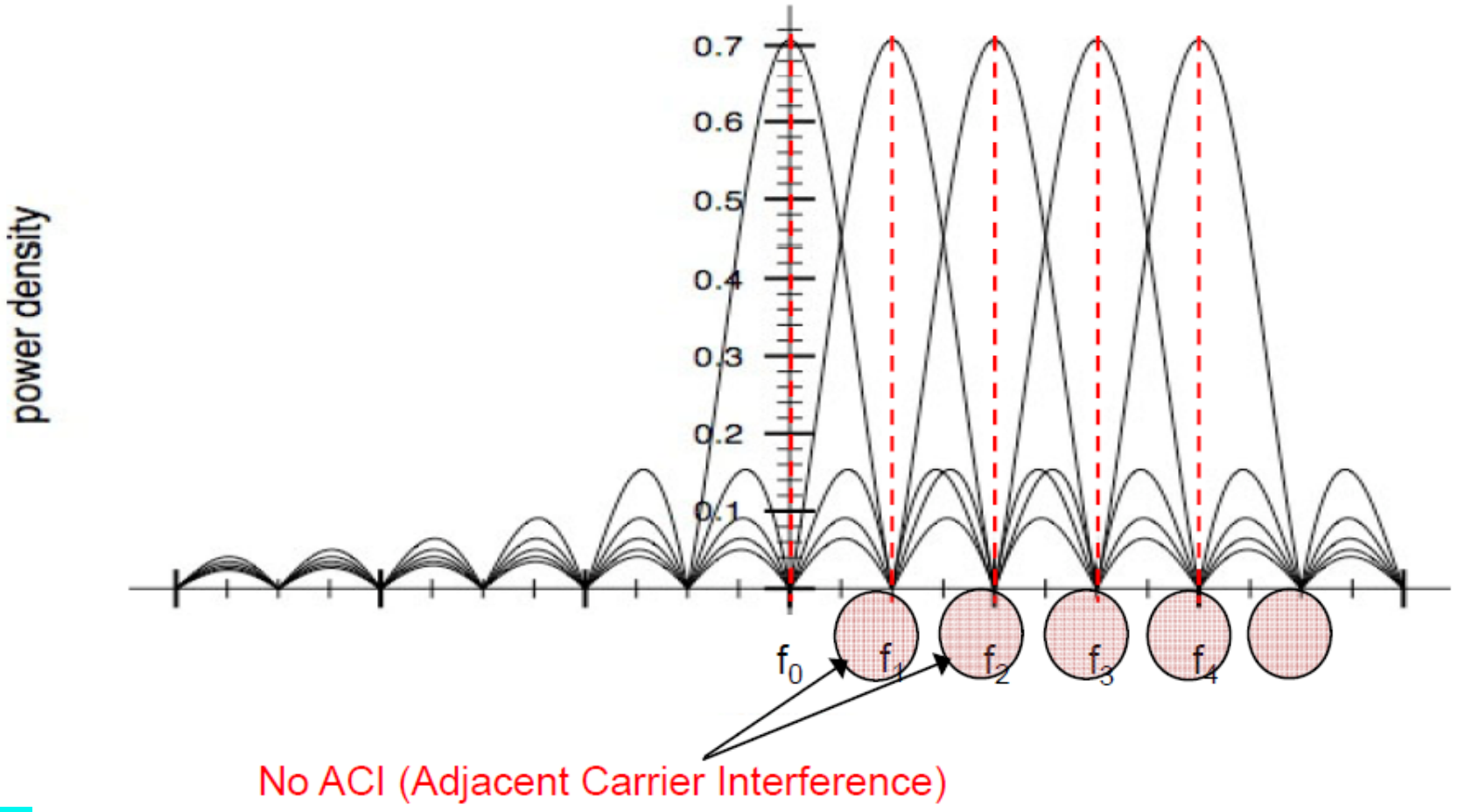
With this we don't need any pulse-shaping.

Between OFDM carriers using the same symbol duration Ts, no guard bands are required.



Spectrum Overlapping of multiple OFDM carriers

$$f_n = f_0 + nf_s = f_0 + n\frac{1}{T_s} \qquad n = \ldots -1, 0, 1, 2 \ldots.$$



Characteristics	802.11	802.11b	802.11a	802.11g
Modulation	FH/DSSS	DSSS	OFDM	OFDM
Carrier Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz
Max Physical Rate	2 Mb/s	11 Mb/s	54 Mb/s	54 Mb/s
Max Data Rate, Layer 3	1.2 Mb/s	5 Mb/s	32 Mb/s	32 Mb/s
Medium Access Control / Media Sharing	CSMA/CA	CSMA/CA	CSMA/CA	CSMA/CA
Connectivity	Conn.-less	Conn.-less	Conn.-less	Conn.-less
Multicast	Yes	Yes	Yes	Yes

Other 802.11 extensions

802.11f
Allows communication between neighboring APs to reduce handover delay

802.11h
Allows coexistence with other standards at 5GHz (e.g., HiperLAN/2) (Dynamic Frequency Selection – DFS)

802.11i
Security extensions

802.11e
QoS improvements through new MAC capabilities

IEEE 802.11e

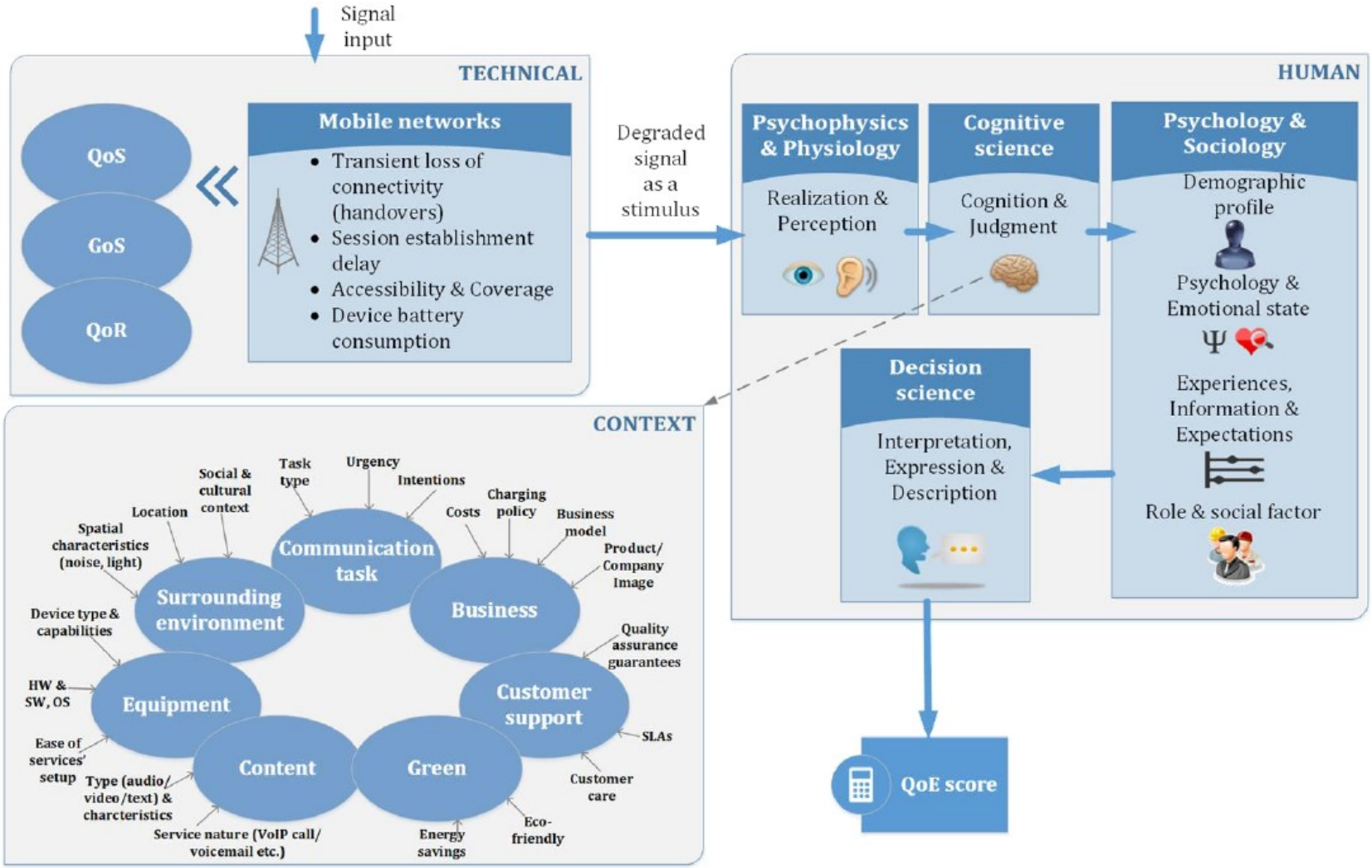
What QoS means

- Quality of Service – QoS: The «efficient» data transmission resulting «satisfactory» operation of a network application as it is perceived by the user
- What «satisfactory» operations means? Usually subjective and depends on the user preferences, and specific needs
- What «efficient» transmission means? Is the data transmission that satisfies specific quality of service parameters, extracted based on the «efficient» operation of a network application
- Typical QoS parameters:
  - mean end-to-end delay
  - maximum end-to-end delay
  - maximum delay jitter
  - mean packet error rate

QoS guarantees

- Based on the type of traffic, and user needs and preferences, QoS parameters are extracted.
- Real-time applications (voice, video) have strict requirements for low mean and max delay (100-200 msec end-to-end), and looser requirements for mean packet error rate (e.g., 10^{-3}).
- Non-real-time applications (email, file transfer) have strict requirements for packet errors, but looser requirements for delay (e.g., a few seconds).
- The target for QoS parameters are shared per link.
- The main target of the layer 2 (Data-Link) protocols is to guarantee the target values of the QoS parameters per data flow.
- So the MAC protocol at 802.11 has to guarantee the target QoS values in the WiFi radio interface.

Quality of experience - QoE



Quality of experience - QoE

Aspect	Quality Influence Factors	
Mobile networks	Vertical and horizontal handovers Battery consumption Session establishment delay	Accessibility Coverage
Service	Call setup success ratio Blocking probability Call setup time	Call cut-off ratio Availability & Reliability
Transport / Network	Round trip / one-way delay Jitter Packet loss ratio Delay burstiness distribution	Loss burstiness distribution Bottleneck bandwidth Congestion period
Physical	SNR / SIR / SINR Bit rate BLER Outage probability Packet / Symbol / Bit Error Probability Outage capacity	Ergodic capacity / rate Throughput Diversity order / coding gain Area spectral efficiency Energy efficiency

Quality of experience - QoE