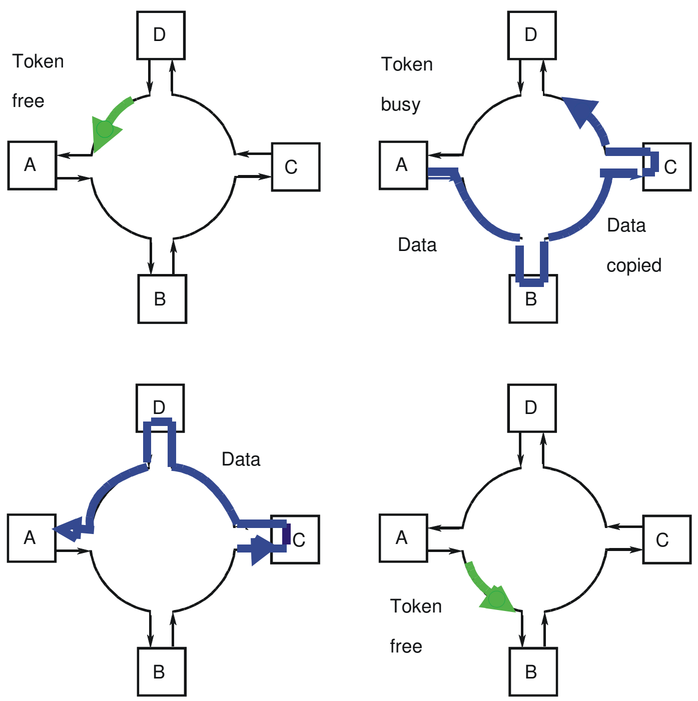
4.6 Token Ring

Standards

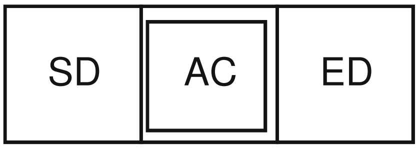
- IEEE 802.5
- ISO IS 8802/5

Mainly developed by IBM, approx. 1984 - 1992.

Media Access Control Protocol of the Token Ring

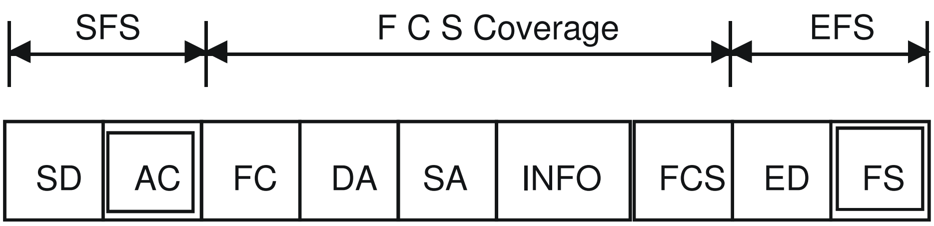


Token Ring: Format of the Token



SD = Starting Delimiter (1 Byte)
AC = Access Control (1 Byte)
ED = Ending Delimiter (1 Byte)

Token Ring: Format of the Data Frame



SFS = Start-of-Frame Sequence
SD = Starting Delimiter (1 byte)
AC = Access Control (1 byte)
FC = Frame Control (1 byte)
DA = Destination Address (2 or 6 bytes)
SA = Source Address (2 or 6 bytes)

INFO = Information (0 or more bytes)
FCS = Frame-Check Sequence (4 bytes)
EFS = End-of-Frame Sequence
ED = Ending Delimiter (1 byte)
FS = Frame Status (byte)

Token Ring: AC and FS Fields

Access Control (AC)

P P P	T	M	R R R

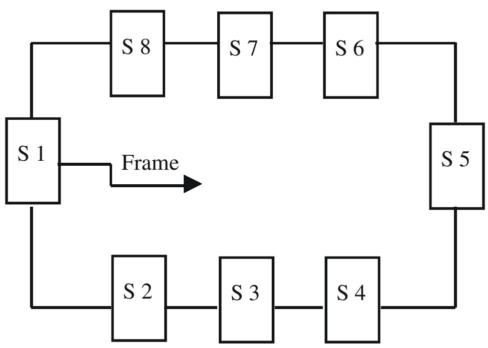
PPP = priority bits
T = token bit
M = monitor bit
RRR = reservation bits

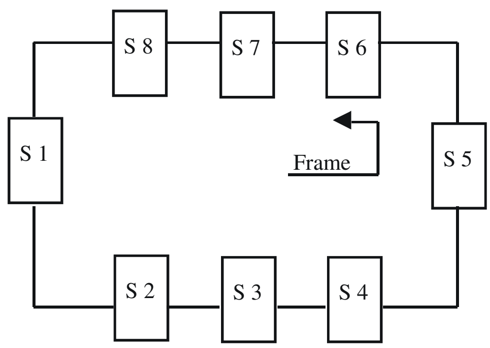
Frame Status (FS)

A C r r	A C r r

A = address-recognized bits
C = frame-copied bits
r = reserved bits

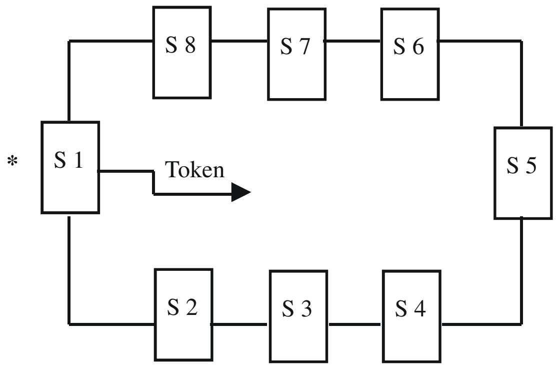
Token Ring: Priority Mechanism (1)

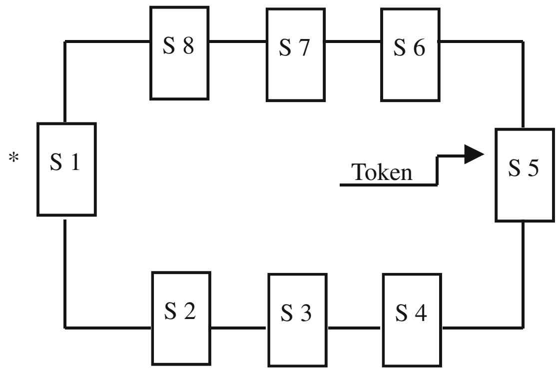




1. Station S1 receives the token and transfers its frame with normal priority.
2. S5 reserves a higher priority in the passing frame (RRR bit).

Token Ring: Priority Mechanism (2)

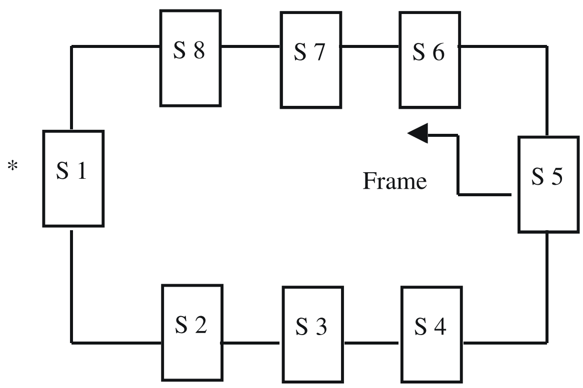


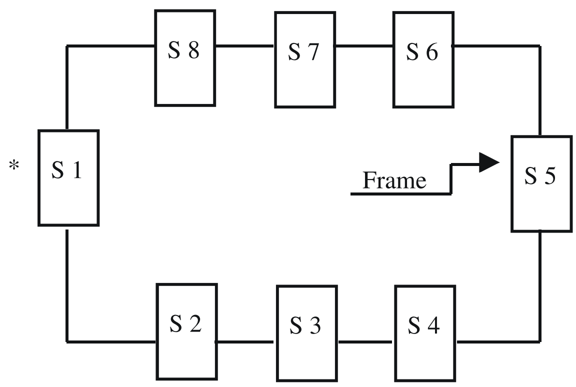


3. S1 removes its frame after transmission, creates a token with the priority reserved by S5 and changes into the "priority hold“ state.

4. S2, S3 and S4 do not have priority frames to send, and the token travels on to S5.

Token Ring: Priority Mechanism (3)

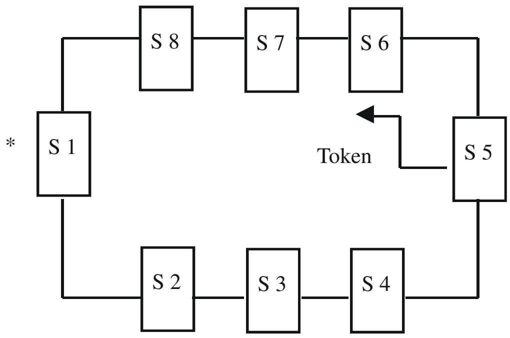


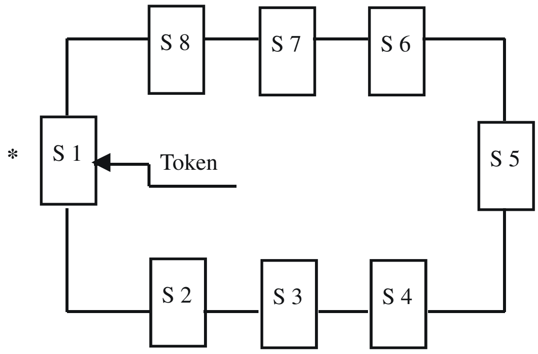


5. Station S5 transmits its priority frame.

6. The frame returns to S5.

Token Ring: Priority Mechanism (4)

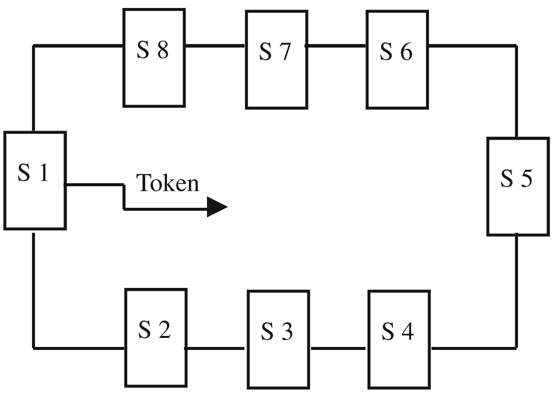




7. S5 terminates its transmission and creates a token with the priority that it has just used (the higher priority). S1, still in "priority hold", waits for a free token with this priority.

8. S1 receives the free token from S5 and recognizes the priority initiated by itself.

Token Ring: Priority Mechanism (5)



9. S1 leaves the "priority hold“ state (provided that no new priority reservation has arrived) and creates a token with normal priority. If S2 has been waiting for a token with normal priority, it can now send.

Functions for Correction Ring Failures

- Exactly one **active monitor** per ring for efficient failure correction.
- The monitor function is implemented in every station. All monitors except one are in **standby mode** for higher reliability and availability.
- The error correction functions use **ring management frames**:
  - Claim Token
  - Duplicate Address Test
  - Active Monitor Present
  - Standby Monitor Present
  - Beacon
  - Purge

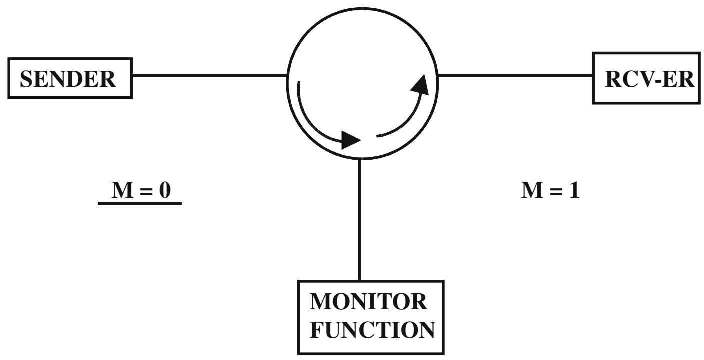
Active Monitor

Each station on the ring can play the role of the active monitor. A distributed election algorithm is used to elect exactly one to become the active monitor.

The active monitor protects against the following error conditions:

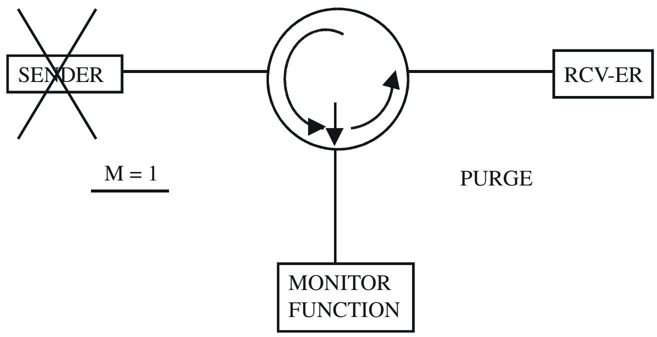
- circulating frame
- circulating token with high priority
- lost token
- more than one active monitor.

Circulating Frame (1)



- The sender produces a frame with the monitor bit M set to 0.
- The transmitter crashes.
- The active monitor sets the monitor bit M to 1 as the frame passes the station.

Circulating Frame (2)



If the active monitor sees a frame with M = 1, it deletes all traffic on the ring (purhes the ring) and initializes it again. It then creates a new token.

Lost Token

- The active monitor uses a timer to detect the loss of a token or a frame.
- The timer is started each time a frame delimiter is regenerated in the monitor station.
- If the timer rings before the next frame delimiter is recognized the active monitor purges the ring and creates a new token

More Than One Active Monitor

An active monitor falls back into standby mode if it receives a

- Purge Frame or
- Active Monitor Present Frame

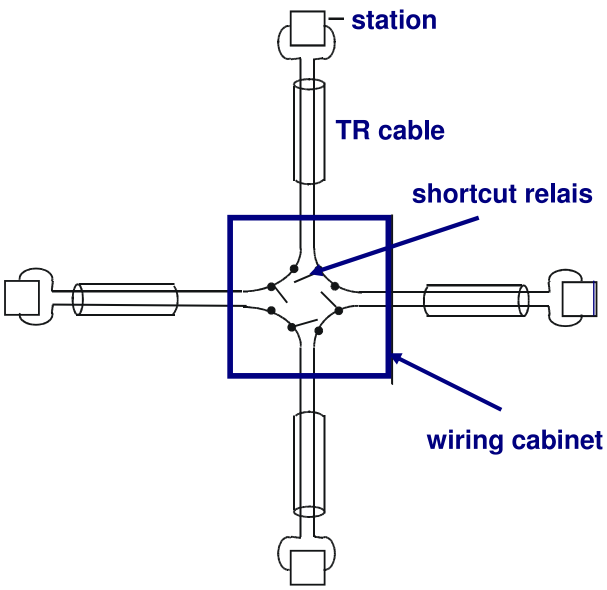
which it did not produce.

Token Ring: Bit Encoding

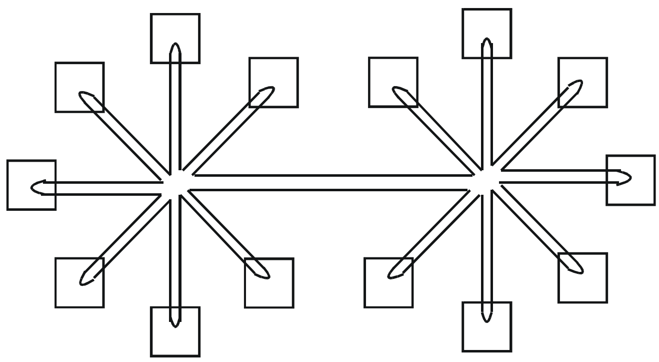
The token ring uses **Differential Manchester Encoding** in layer 1:

- A 0-bit changes the voltage level at the beginning of the bit interval.
- A 1-bit keeps the previous voltage level at the beginning of the bit interval.
- There is always a voltage transition in the middle of the bit interval.

Star Topology for the Token Ring



Structured Wiring

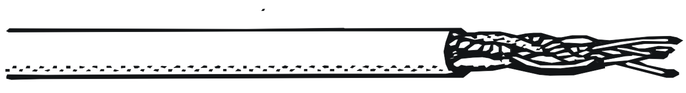


Logical ring Physical star

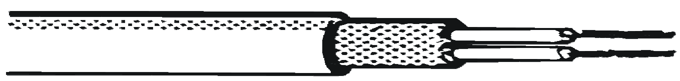
Ring wiring in form of a physical star topology facilitates error handling and allows more flexible wiring of new stations.

Cables for the Token Ring

Two twisted pairs of copper wire with a shield



Cable with two fiber optics conductors



Token Ring LAN Summary

- Physical ring topology
- Regeneration of the electrical pulses in each station. Thus low sensitivity to noise. Large rings with many stations possible.
- Natural topology for optical fiber since the signals are generated and read only at the ends of the cables (unlike with a bus topology).
- Ring management is quite complicated. If the token does not circulate properly, the entire ring is in trouble. Switching off a station requires a shortcut of the cable and re-initialization of the entire ring, etc.
- Stations that crash or operate incorrectly must be isolated and excluded from the ring.

4.7 Wireless LAN (IEEE 802.11)

Design goals

- Wireless local area network with 802 MAC layer and physical layer functionality
- Fits under the same LLC layer (802.2, Logical Link Control). Thus compatible with all higher layers in particular IP.
- Support for stationary wireless stations and mobile wireless stations (”roaming”)
- Can operate with an infrastructure (access points) or without an infrastructure (ad-hoc)

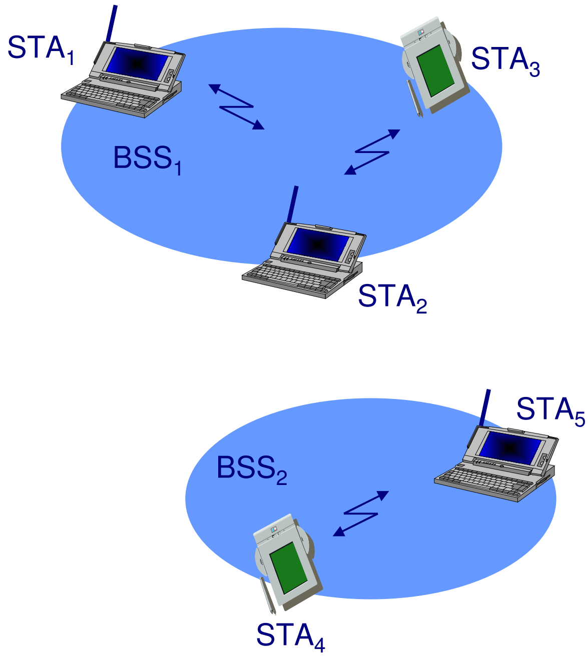
Many transparencies of this chapter were originally provided by Dres. Martin Mauve and Hannes Hartenstein. Their support is gratefully acknowledged.

IEEE 802.11 - System Architecture (1)

Independent Basic Service Set (IBSS)

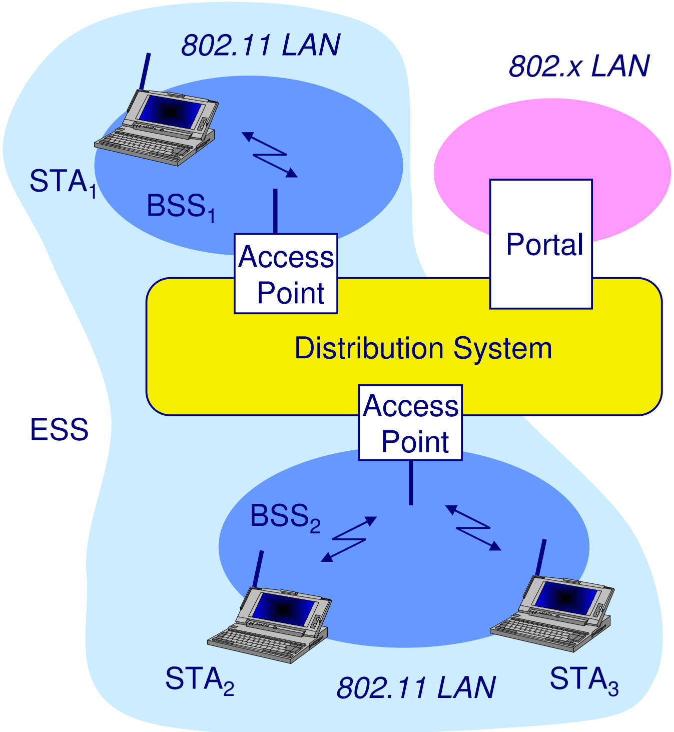
Set of mobile stations that are able to communicate directly with each other, without connection to a wired network.

The stations do not have “forward-ing” functionality. The IBSS only permits a 1-hop-communication (1-hop ad-hoc).



IEEE 802.11 - System Architecture (2)

IEEE 802.11 defines **access point, distribution system, portal** and **distribution ser-vices.**



IEEE 802.11 - System Architecture (3)

An **access point** is a station that offers **distribution services**.

The **distribution system** connects access points with each other.

Distribution services cover:

- association
- reassociation
- disassociation
- distribution
- integration

IEEE 802.11 - System Architecture (4)

Distribution Services

Association service

Establishes a logical connection between a mobile station and an access point.

Reassociation service

Similar to the association service, containes additional information about the previous access point.

Disassociation service

Terminates a logical connection.

IEEE 802.11 - System Architecture (5)

Integration Service

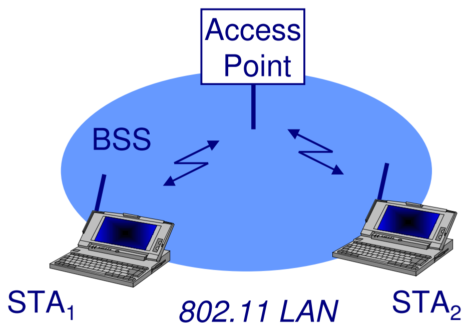
The integration service connects an IEEE 802.11 WLAN to other LANs. A **portal** implements the integration service.

IEEE 802.11 - System Architecture (6)

Infrastructure Basic Service Set

Communication is always between a mobile station and the access point.

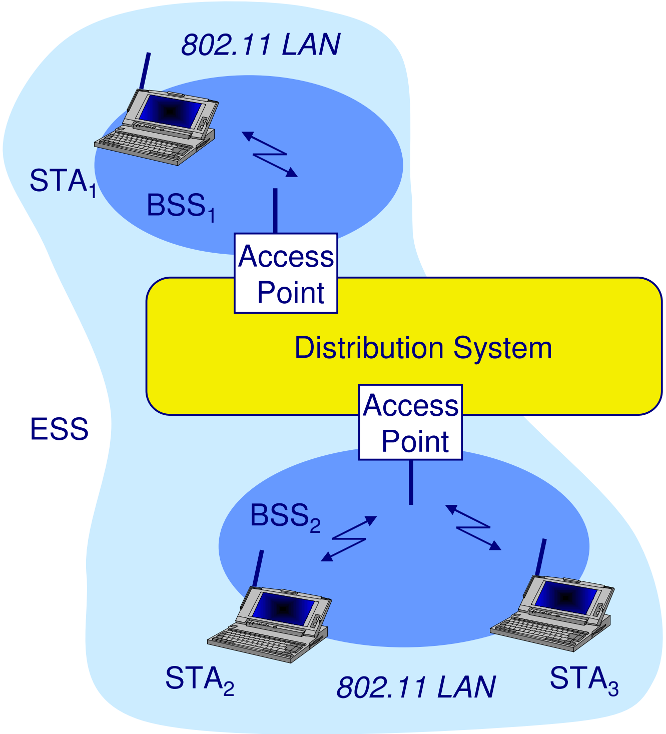
Extended communication possibilities, but frames between mobile stations are sent twice over the air.



IEEE 802.11 - System Architecture (7)

Extended Service Set

Set of Infrastructure BSSs that are connected by a distribution system.



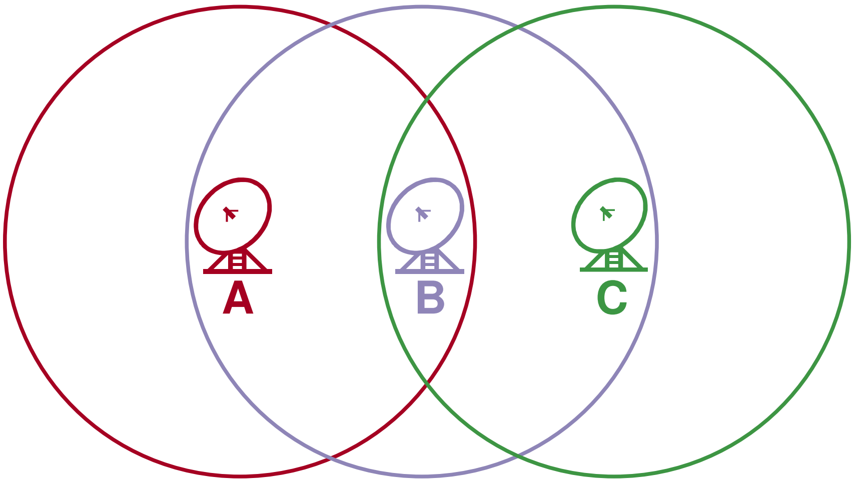
Media Access Control (MAC) in 802.11

Traffic Classes

- **Asynchronous data service** (standard)
  - Exchange of data packets on a "best effort" basis
  - Supports broadcast and multicast
  - Available in both modes, infrastructure mode and ad-hoc mode
- **Service with QoS guarantees** (optional)
  - implemented by the so-called Point Coordination Function (PCF)

Why are New MAC Algorithms Needed?

In wireless communication new problems arise because the physical layer operates differently from cable-based physical layers. For example, unlike in an Ethernet segment, not every station can hear every other station directly. In particular: From “A hears B” and “B hears C” we cannot always conclude that “A hears C”! A cannot sense if C is sending, and vice versa.



The Problem of the “Hidden Terminal”

- A and C both want to send to B.
- A senses the medium and states that it is free. A begins to send.
- At the same time, C senses the medium and sees that it is free (the signal of A does not reach C). C also begins to send.
- The signals collide in B, B receives none of the two messages correctly.
- **Neither A nor C can determine the collision since they do not hear each other.**

We conclude: CSMA/**CD** will not work.

IEEE 802.11 MAC (1)

DFWMAC: Distributed Foundation Wireless Medium Access Control

Three variants are standardized:

- **DFWMAC-DCF CSMA/CA** (mandatory in all WLANs)
  - Distributed Coordination Function – Carrier Sensing Multiple Access with Collision Avoidance
  - "listen before talk"
  - Collision reduction when "busy" by a "random backoff timer"
  - Acknowledgment of receipt through ACK (in unicast mode only)
  - The problem of the "hidden terminal" is not solved!
- **DFWMAC-DCF with RTS/CTS** (optional)
  - Basic function like DFWMAC-DCF CSMA/CA
  - In addition, avoidance of the hidden terminal problem by a Request-to-Send / Clear-to-Send mechanism (**RTS/CTS**).

IEEE 802.11 MAC (2)

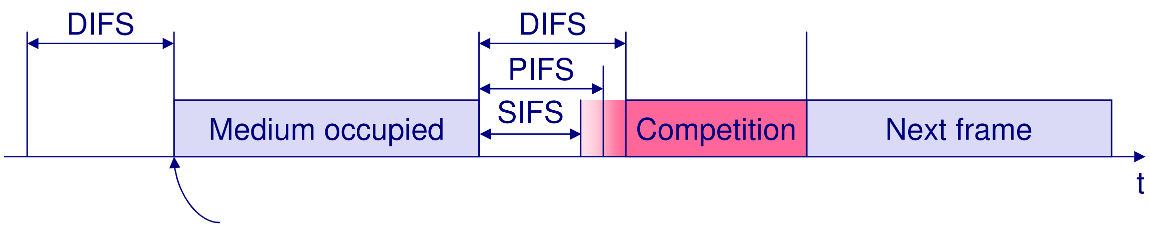
- **DFWMAC-PCF** (optional)
  - PCF = Point Coordination Function
  - collision-free, centralized access control procedure for services with time guarantees
  - Basic idea: the access point polls the stations in a round-robin fashion

Priorities by Three Waiting Periods (1)

IFS = Inter-Frame Spacing

- **SIFS** (Short Inter-Frame Spacing)
  - Highest priority, for ACK, CTS, answer to polling
- **PIFS** (PCF IFS)
  - Intermediate priority, for time-guaranteed services by the PCF (Point Coordination Function). The access point waits the PIFS time before using the medium for control purposes (in particular for polling).
- **DIFS** (DCF IFS)
  - Lowest priority, for asynchronous (best effort) data services

Priorities by Three Waiting Periods (2)

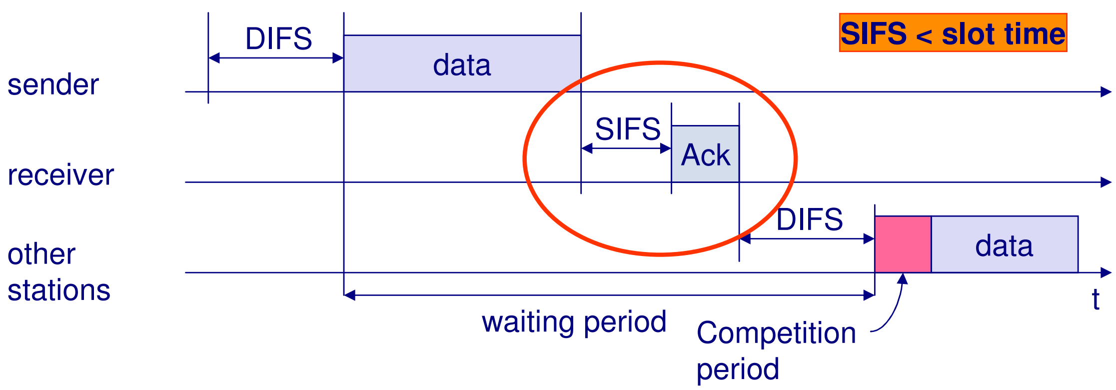


DFWMAC-DCF CSMA/CA: Concept

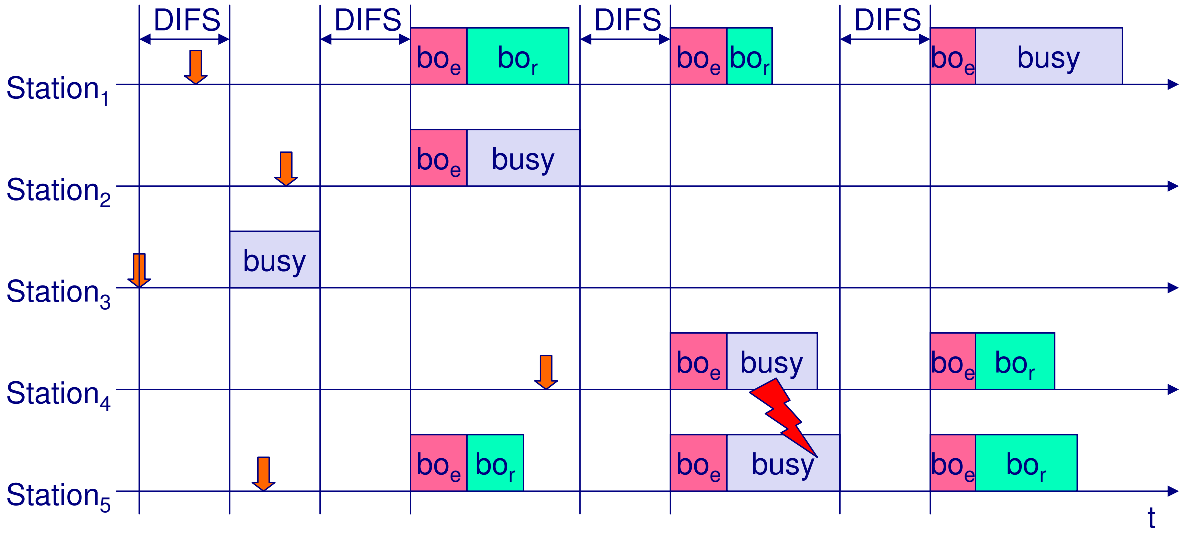
- “Listen-before-talk”: stations ready to send sense the medium (carrier sensing).
- If the medium is free for the duration of an appropriate Inter-Frame Spacing (IFS), the station sends immediately.
- If the medium is busy, the station waits for a free IFS and then waits for an additional random back-off time in order to reduce the probability of a collision.
- If the medium is accessed by another station during the back-off time, and the other station can be heard before the own backoff timer rings, the own back-off timer is stopped until the next transmission attempt. It is not reset; thus the backoff time will be shorter after every unsuccessful attempt. This increases the priority of stations that have waited before.
- Note: Collisions are still possible, although not very probable.

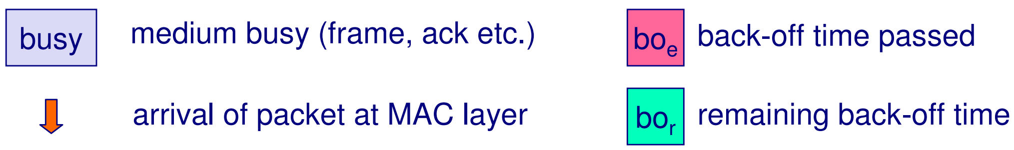
Acknowledgements (Unicast Case)

Problem: Collision detection to recognize a successful transmission on the sender side (like in the Ethernet) does not work! Therefore explicit acknowledgments are needed. If the sender does not receive an acknowledgment, a retransmission takes place **in the MAC layer**.



Comprehensive Example

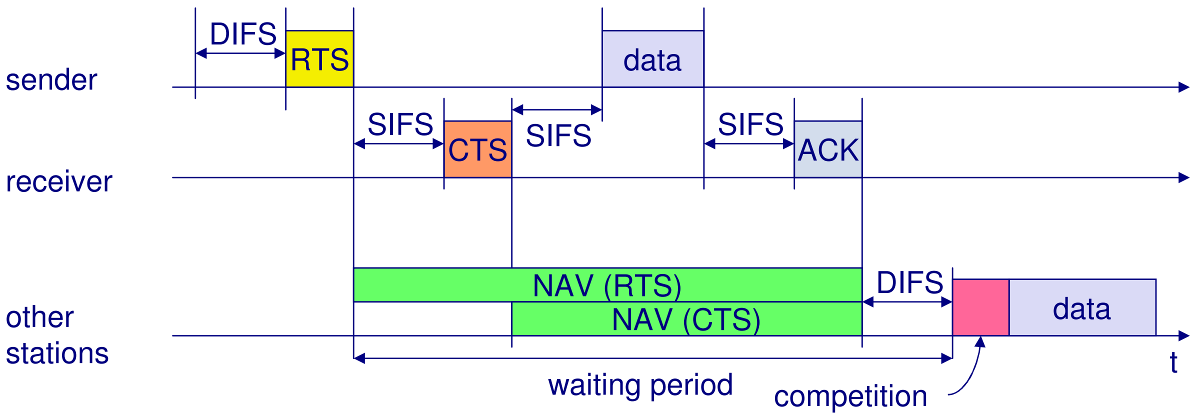




DFWMAC-DCF with RTS/CTS

Optional. Only available for unicast transmission. Usually not advisable for short packets. Basically a method by which the **receiver** informs all stations in his radio range to shut up. Solves the hidden terminal problem.

Extension of the access procedure by a **Network Allocation Vector NAV** for the reservation of future slots for the same pair of transmitter and receiver. RTS = Request To Send, CTS = Clear To Send.



DFWMAC-PCF (with Point Coordination Function)

The point coordinator is always an access point. PCF not available in ad-hoc mode.

PCF is an extension (additional function); PCF and DCF can be used at the same time.

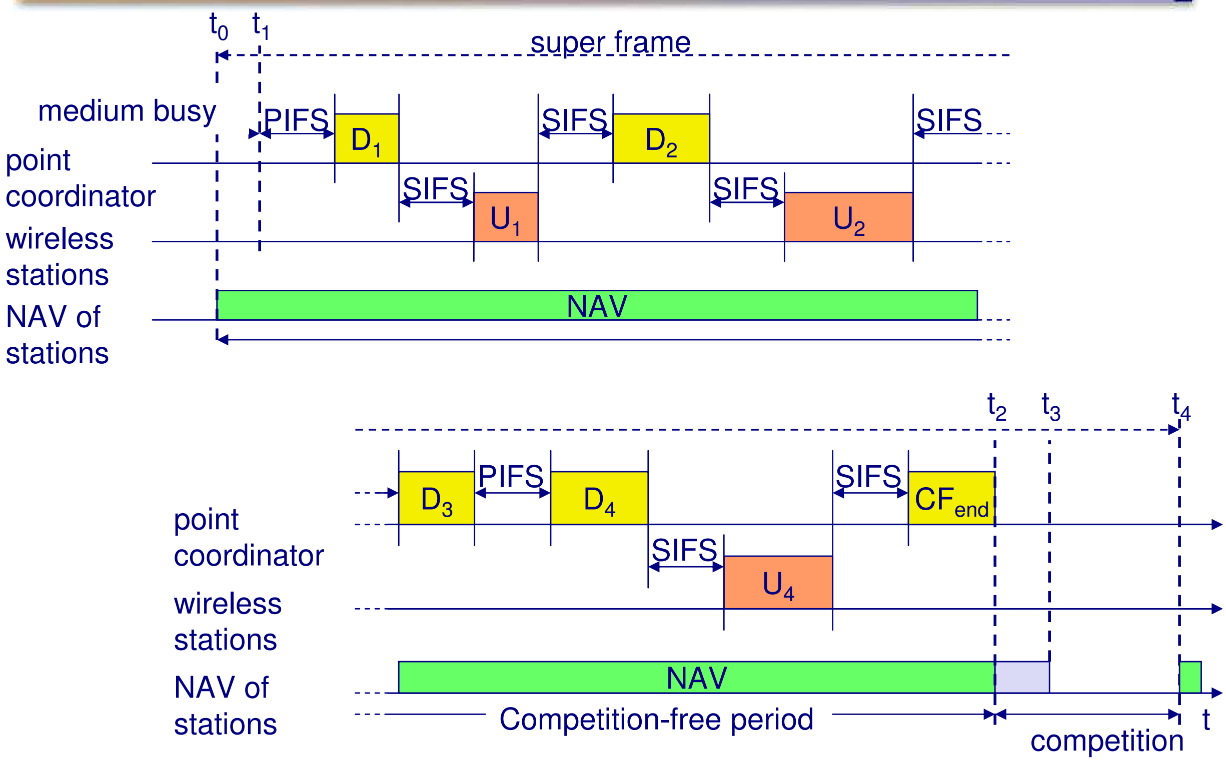
There is now a “Contention-Free Period” (CFP), in which the PCF coordinates the access to the medium without competition with other stations.

PCF uses PIFS (the intermediate IFS) in order to control the medium.

The NAV is used to communicate the CFP to the stations (to make the reservation).

The assignment of guaranteed sending periods to the stations is achieved by **polling**. A guaranteed sending period per round leads to a guranteed minimum bandwidth and a guaraneed maximum delay to access the medium.

PCF Example with Polling



IEEE 802.11 - Frame Structure

Frame Types

- Control Frame, Management Frame, Data Frame

Sequence numbers (Sequence Control)

- important for detecting duplicate packets after lost ACKs

Four Addresses

- Receiver, transmitter (physical), BSS Identifier, transmitter (logical)

Other

- Transmission duration, data, check sum (CRC)

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

Frame Control: Version, type, fragmenting, security...

Not all fields exist in all frames

Addressing: Four Addresses in the Frame

Packet type	to DS	from DS	Address 1	Address 2	Address 3	Address 4
Ad-hoc Network	0	0	DA	SA	BSSID	-
Infrastructure-Network, from AP	0	1	DA	BSSID	SA	-
Infrastructure-Network, to AP	1	0	BSSID	SA	DA	-
Infrastructure-Network, in DS	1	1	RA	TA	DA	SA

Two bits in the Frame Control field decide how the four addresses are interpreted.
The addresses usually are 48-Bit-MAC addresses.

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

Roaming (Better: Hand-over or Hand-off)

What happens when a station is moving, and the radio link gets weak or is lost?

Scanning

- Scanning of the environment (listen for beacons of APs or send a probe into the medium and wait for an answer).

Reassociation Request

- Contains information about the past AP and asks for a new association.

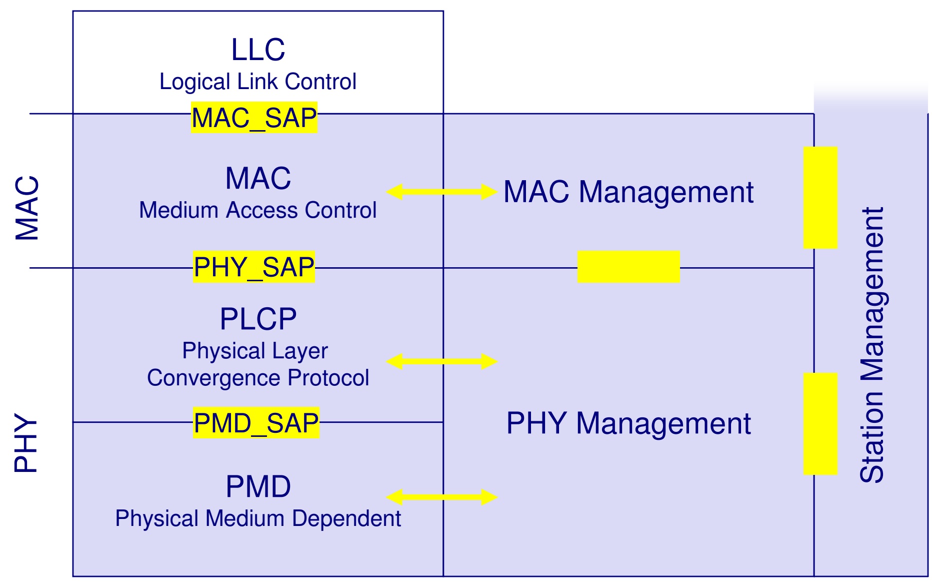
Reassociation Response

- Success: i.e. an AP answers, the station is physically connected again
- Failure: continue to scan

AP accepts Reassociation Request

- Registration of the new station with the distribution system
- The old AP is informed by the distribution system to release the connection to this station.

IEEE 802.11 – Physical Layer (1)



IEEE 802.11 – Physical Layer (2)

PLCP (Physical Layer Convergence Protocol)

- clear channel assessment

PMD (Physical Medium Dependent)

- line coding, modulation

PHY Management

- PHY MIB, choice of channel

Station Management

- control of bridge functions, interaction with distribution system

PHY- Options

IEEE 802.11 supports three PHY options, each with 1 and 2 Mbit/s:

- Frequency Hopping Spread Spectrum (2,4 GHz)
- Direct Sequence Spread Spectrum (2,4 GHz)
- Infrared (850 - 950 nm)

802.11a: 6 - 54 Mbit/s

- Frequency Division Multiplexing, (5 GHz)

802.11b: 5.5 and 11 Mbit/s

- High-rate **DSSS**

802.11g: 54 Mbit/s

PHY: Why 2.4 GHz?

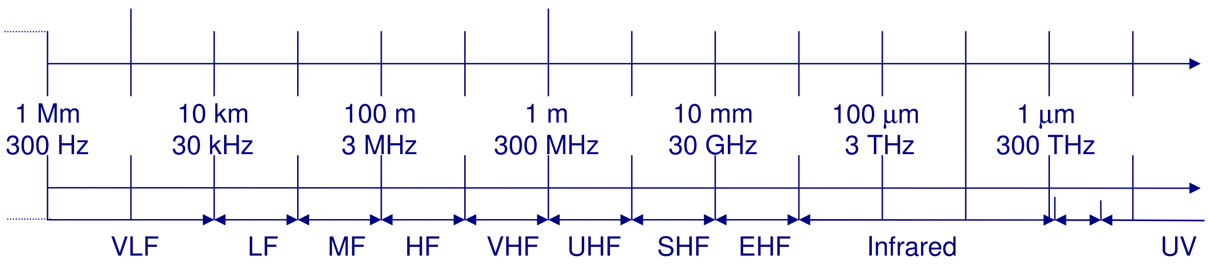
Unlicensed ISM band (Industrial, Scientific, Medical)

Advantage: usage free of charge, no permission required

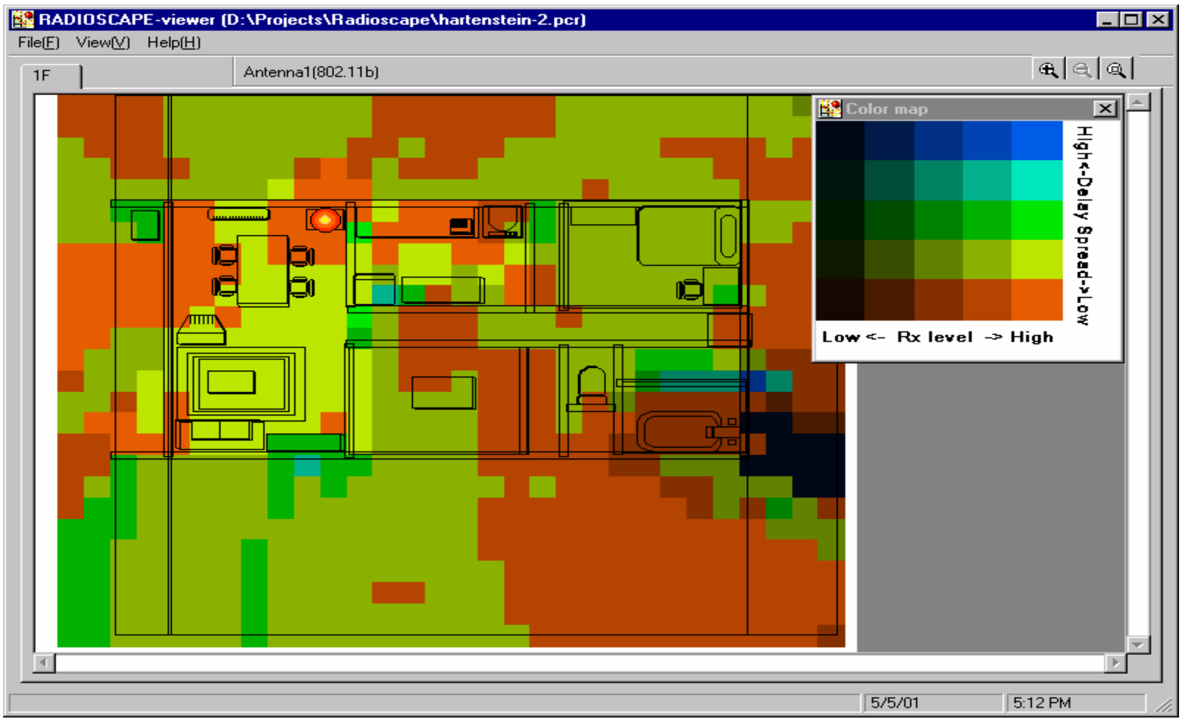
Problem: non-exclusive use (e.g., garage door openers and microwave ovens work at 2.4 GHz) = > a very noisy frequency band

Solution: use spread-spectrum technology

Frequency ranges and wavelengths:



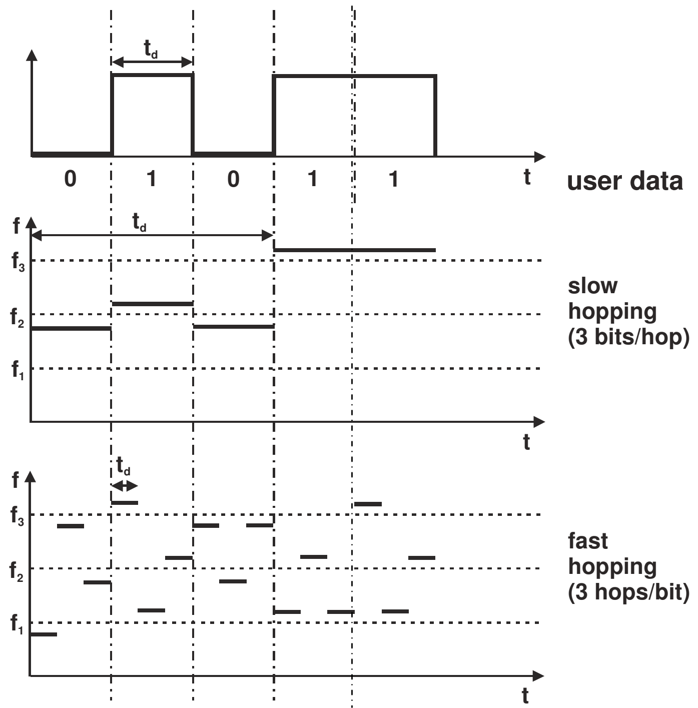
Radioscape (NEC-J @ Cebit 2001)



Frequency Hopping Spread Spectrum (1)

Several channels from the entire frequency band are used in parallel. Senders and receivers rapidly jump between the channels in an agreed sequence. In this way, narrow-band noise has less effect.

Frequency Hopping Spread Spectrum (2)

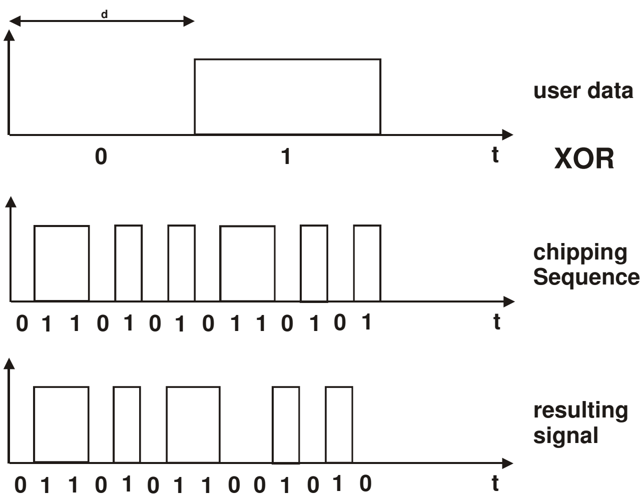


Frequencies in the 2.4 GHz Band

CHNL_ID	FCC Channel Frequencies	ETSI Channel Frequencies	Japan Frequency
1	2412 MHz	N/A	N/A
2	2417 MHz	N/A	N/A
3	2422 MHz	2422 MHz	N/A
4	2427 MHz	2427 MHz	N/A
5	2432 MHz	2432 MHz	N/A
6	2437 MHz	2437 MHz	N/A
7	2442 MHz	2442 MHz	N/A
8	2447 MHz	2447 MHz	N/A
9	2452 MHz	2452 MHz	N/A
10	2457 MHz	2457 MHz	N/A
11	2462 MHz	2462 MHz	N/A
12	N/A	N/A	2484 MHz

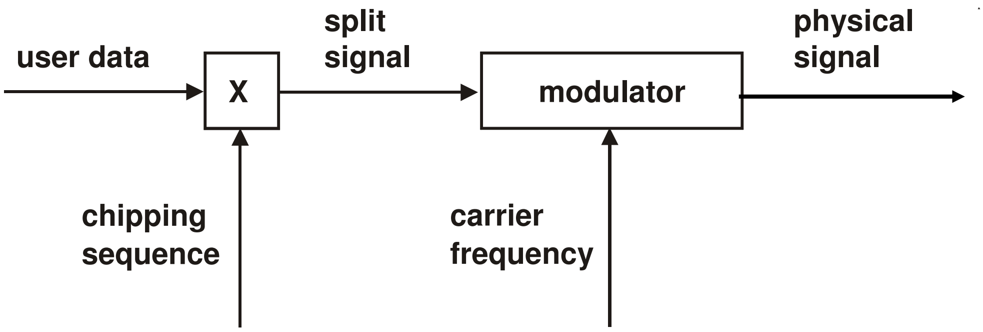
Direct Sequence Spread Spectrum (DSSS) (1)

Sender and receiver agree on a **chipping sequence** (a fast binary pattern). This is folded with the signal by XOR. The range thereby becomes significantly higher, but the signal becomes more easily recognizable in a noisy channel.



Direct Sequence Spread Spectrum (DSSS) (2)

Block diagram of a DSSS transmitter



4.8 Logical Link Control for LANs

Data Link Layer in LANs

Identical for CSMA/CD, Token Ring, WLAN, etc.!

Three types of service:

LLC Type 1: Unconfirmed connectionless service

- Unconfirmed transmission of data frames.
- The higher layers are responsible for the preservation of packet order, error control and flow control.

LLC Type 2: Connecting-oriented service (similar to HDLC)

- connection establishment and termination
- data transfer with acknowledgements (delivery guaranteed)
- packet sequence maintained by layer 2
- flow control

Logical Link Control

LLC Type 3: Confirmed connectionless service

- Each datagram is confirmed by exactly one acknowledgement in the opposite direction
- Application in real-time systems, such as process control, etc.

4.9 LAN Bridges

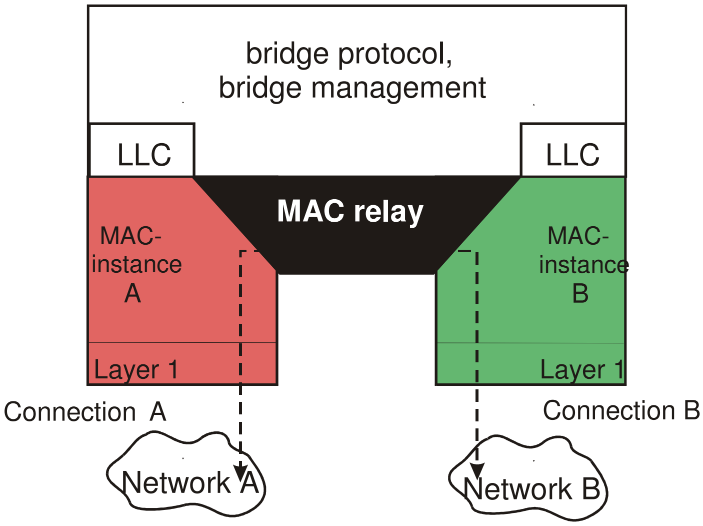
A **brigde** connects two or more LANs that may use different MACs (e.g., an Ethernet LAN with a Wireless LAN). It can be considered as a layer-2 gateway.

A bridge has a **frame filter.** It forwards only those frames to the neighbor LAN whose destination address is not on the local link.

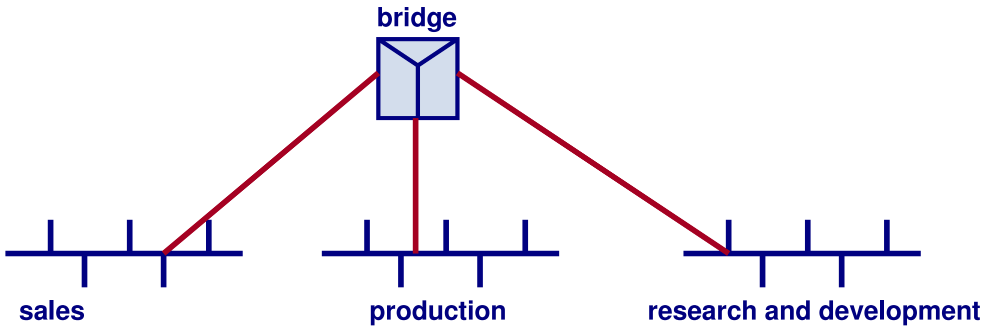
A bridge operates on layer 2 exclusively (on MAC frames). Protocols of the higher layers are not taken into consideration. In particular, a LAN bridge is quite different from an IP router.

Bridges are usually self-learning, i.e., they learn from the incoming frames which MAC addresses are located in which attached LANs.

Protocol Layers of a LAN Bridge



Example of a Bridge between Three LANs



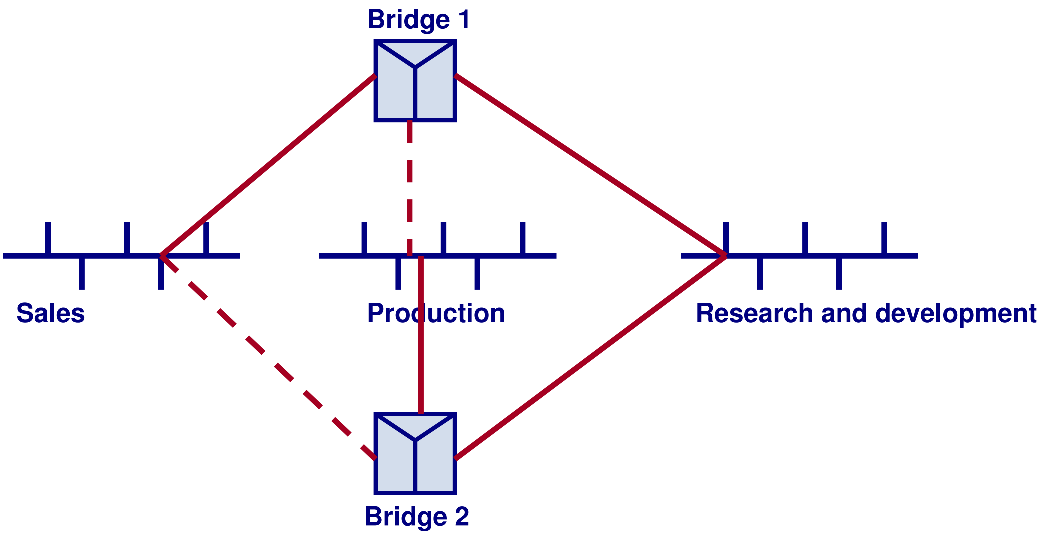
Entries in the Table of a Self-Learning Bridge

Example

destination address	output port	timer
0800201D8E8F	1	300 s
08002B32A945	2	180 s
08002B32A988	3	240 s

Spanning Trees

In order to make the interconnection of LANs more reliable, there are often several interconnection points (bridges). In order to avoid the cycling of frames in such a network, the bridges must agree on a **spanning tree** for the graph. This is done with a **spanning tree protocol**.



Bridges and the like...

- A **hub** operates on layer 1. It forwards each arriving frame to all outgoing links.It replaces a physical bus topology, implementing the MAC function inside the box. The number of frame collisions is not reduced by a hub.
- A **frame switch** forwards each arriving frame to exactly one outgoing link, leading directly to the destination. The decision is based on the destination address in the LAN frame. It functions like a packet switching device, but on layer 2. Compared to a hub, the number of collisions is reduced since incoming frames are buffered, and switching is done internally at a multiple of the line speed. There is no frame filter function.
- A **bridge** also operates on layer 2. It contains a self-learning filter and forwards only those packets that are not intended for stations on the local LAN.
- A **router** is a packet switching device, typically for IP packets, on layer 3.