The Ethernet Evolution

From 10Mbit/s to 10Gigabit/s Ethernet Technology
From Bridging to L2 Ethernet Switching and VLANs
Primer to Wireless LAN Technology

Agenda

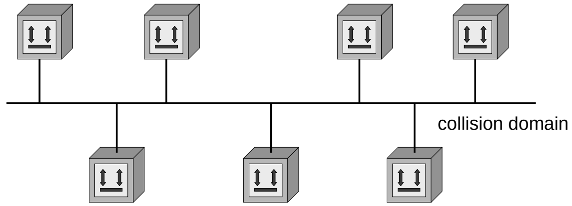
- **<u>Ethernet Evolution</u>**
- **VLAN**
- **High Speed Ethernet**
  - Introduction
  - Fast Ethernet
  - Gigabit Ethernet
  - 10 Gigabit Ethernet
- **Introduction to WLAN**

Datenkommunikation 384.081 - SS 2008

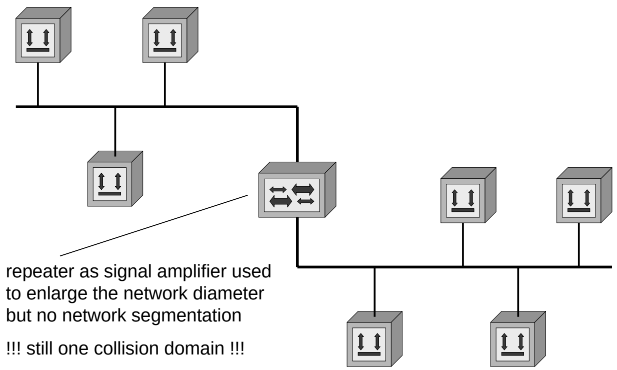
L07 - Ethernet Evolution and Wireless LAN Primer

The Beginning

- **initial idea: shared media LAN**
  - bus structure, CSMA/CD was access method
  - coax cable, transmission rate up to 10 Mbit/s
  - half-duplex transmission (two physical wires e.g. coax)



Enlarging the Network

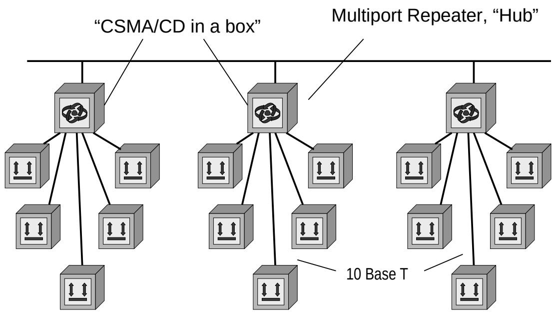


© 2008, D.I. Manfred Lindner

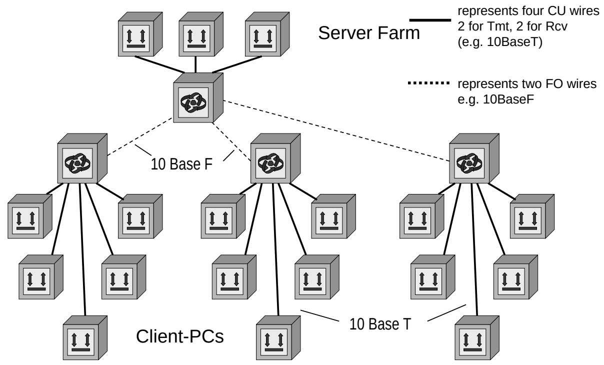
Multiport Repeater

- **demand for telephony-like point-to-point cabling using Twisted Pair wires**
  - based on structured cabling standard
  - 10BaseT as new Ethernet type to support this demand
  - four physical wires (2 for tmt, 2 for rcv)
- **network stations are connected star-like to a multiport repeater**
  - multiport repeater is called “hub”
- **hub simulates the bus: "CSMA/CD in a box"**
- **only half-duplex**
  - only one network station can use the network at a given time, all others have to wait

Structured Cabling (1)



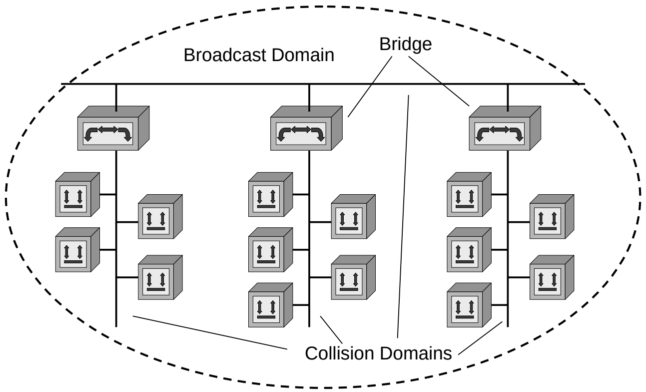
Structured Cabling (2)



Bridging

- **simple physical amplification with repeaters became insufficient**
  - with repeaters all nodes share the given bandwidth
  - the whole network is still one collision domain
  - -> technology moved toward layer 2
- **bridges segment a network into smaller collision domains**
  - store and forward technology (packet switching)
  - the whole network is still a broadcast domain
  - Spanning Tree provides a unique path between each two devices and avoids broadcast storms

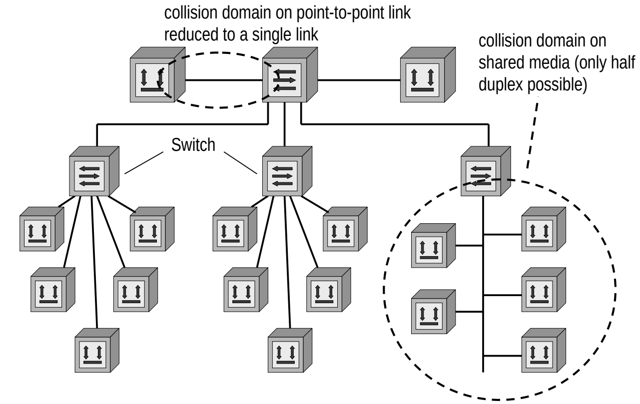
Network Segmentation with Bridges



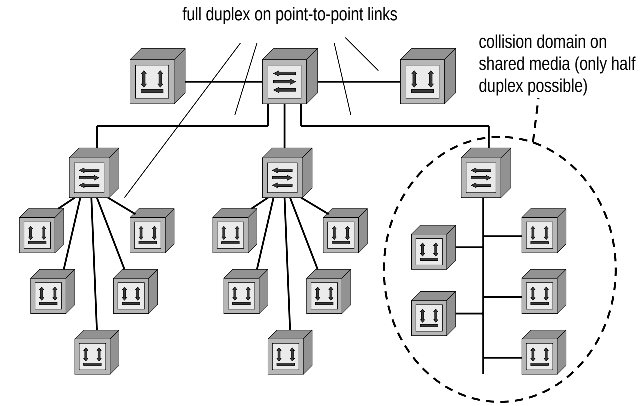
Switching (1)

- **"switching" means fast transparent bridging**
  - implemented in hardware
  - also called Layer 2 (L2) switching or Ethernet switching
- **multiport switches allow full duplex operation on point-to-point links**
  - no need for collision detection (media access control) on a link which is shared by two devices only
    - network station <-> switch port
    - switch <-> switch
- **multiport switches replaces multiport repeaters**
  - a collision free Ethernet can be built, if network consists of point-to-point links only

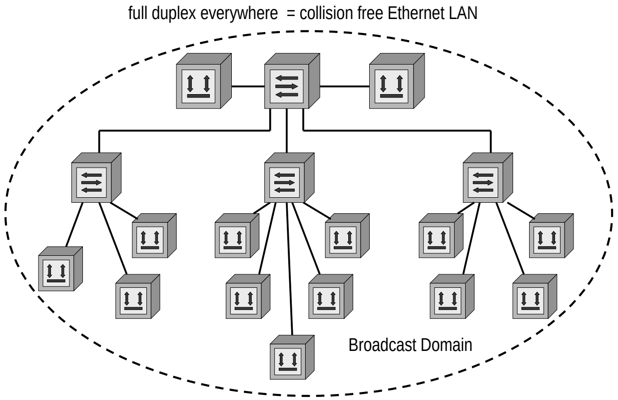
Switching (2)



Switching (3)



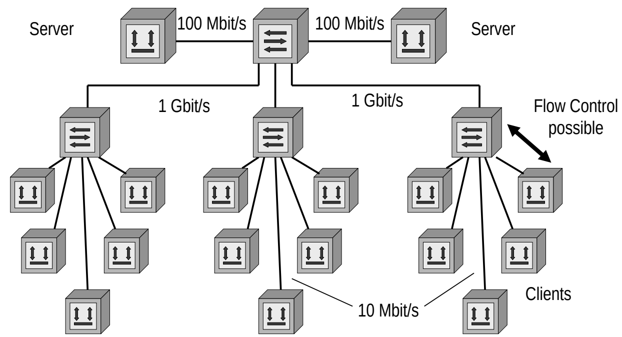
Switching (4)



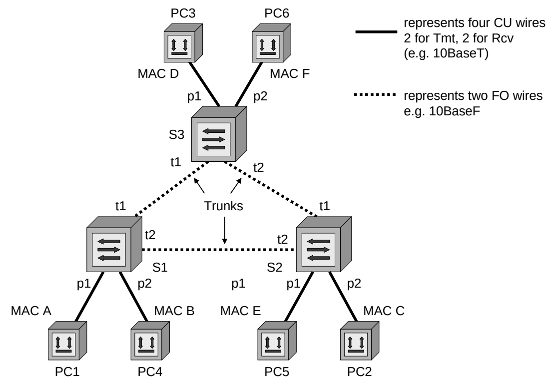
Switching (5)

- **L2 switches can connect Ethernets with 10 Mbit/s, 100 Mbit/s or 1000 Mbit/s for example**
  - clients using 10 Mbit/s either half duplex on shared media or full duplex on point-to-point connection with switch
  - server uses 100 Mbit/s, full duplex, point-to-point connection with switch
  - note: multiport repeater is not able to do this !
- **L2 switch as packet switch operates with asynchronous TDM**
  - congestion can be avoided by using a new MAC based flow control (pause command)

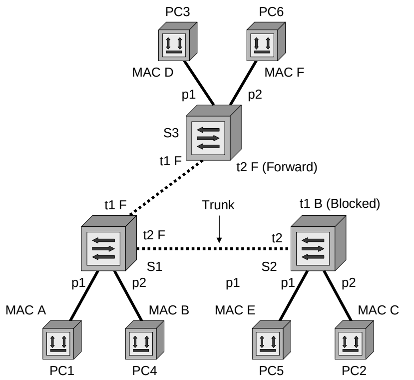
Switching (6)



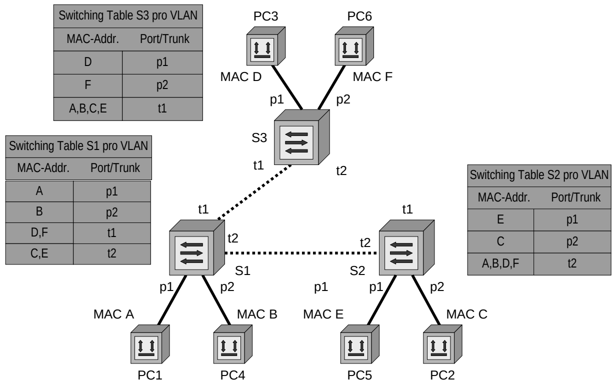
Redundant Topology L2 Switching



Spanning Tree Applied



Switching Table (L2)



Switching Table S3 pro VLAN

MAC-Addr.	Port/Trunk
D	p1
F	p2
A,B,C,E	t1

Switching Table S1 pro VLAN

MAC-Addr.	Port/Trunk
A	p1
B	p2
D,F	t1
C,E	t2

Switching Table S2 pro VLAN

MAC-Addr.	Port/Trunk
E	p1
C	p2
A,B,D,F	t2

Agenda

- **Ethernet Evolution**
- **VLAN**
- **High Speed Ethernet**
  - Introduction
  - Fast Ethernet
  - Gigabit Ethernet
  - 10 Gigabit Ethernet
- **Introduction to WLAN**

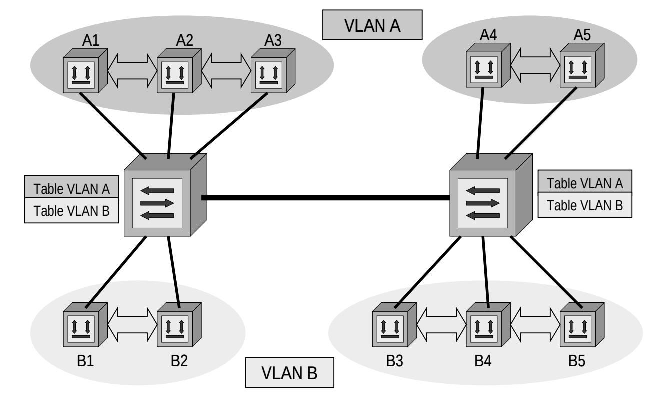
Virtual LANs (1)

- **today's work-groups are expanding over the whole campus in case of local environment**
- **users of one workgroup should be kept separated from other workgroups**
  - because of security reasons they should see there necessary working environment only
- **end-systems of one workgroup should see broadcasts only from stations of same workgroup**
- **the network must be flexible**
  - to adapt continuous location changes of the end-systems/users

Virtual LANs (2)

- **base idea of VLAN:**
  - multiplexing of several LANs via same infrastructure (switches and connection between switches)
- **today's switches got the ability to combine several network-stations to so-called "Virtual LANs"**
  - separate bridging/switching table maintained for every single VLAN
  - separate broadcast handling for every single VLAN
    - each Virtual LAN is its own broadcast domain
  - separate Spanning Tree for every single VLAN
    - note: IEEE 802.1w specifies a method to share one Rapid Spanning Tree among all VLANs

VLAN Example



VLAN Assignment

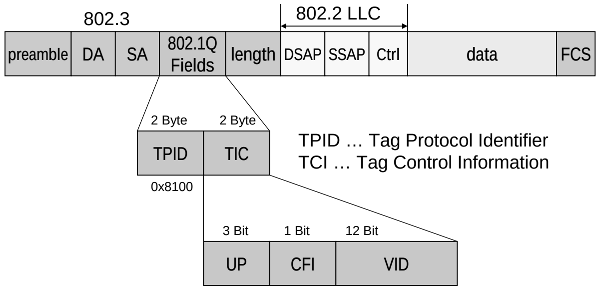
- **a station may be assigned to a VLAN**
  - port-based
    - fixed assignment port 4 -> VLAN x
    - most common approach
    - a station is member of one specific VLAN only
  - MAC-based
    - MAC A -> VLAN x
    - allows integration of older shared-media components and automatic location change support
    - a station is member of one specific VLAN only

Virtual Trunks - VLAN tagging

- **switches must be connected via VLAN-trunks on which each particular VLAN-frame is "tagged" (marked) with an identifier**
  - examples for tagging standards:
    - IEEE 802.10 (pre 802.1Q temporary solution)
    - ISL (Cisco)
    - IEEE 802.1Q
- **so switches can distinguish between several VLANs and manage their respective traffic**

© 2008, D.I. Manfred Lindner

802.1Q VLAN Tagging 1

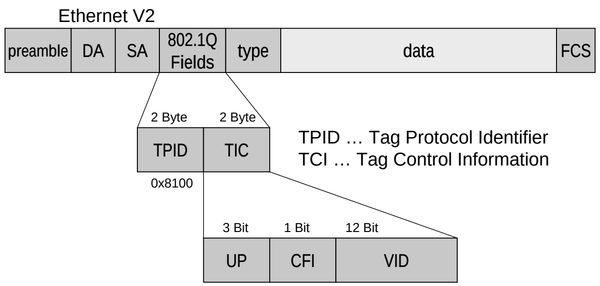


TPID … Tag Protocol Identifier
TCI … Tag Control Information

UP … User Priority
CFI … Canonical Format Identifier
VID … VLAN Identifier

note: With tagging Ethernets maximal frame length = 1522, minimal frame length = 68

802.1Q VLAN Tagging 2

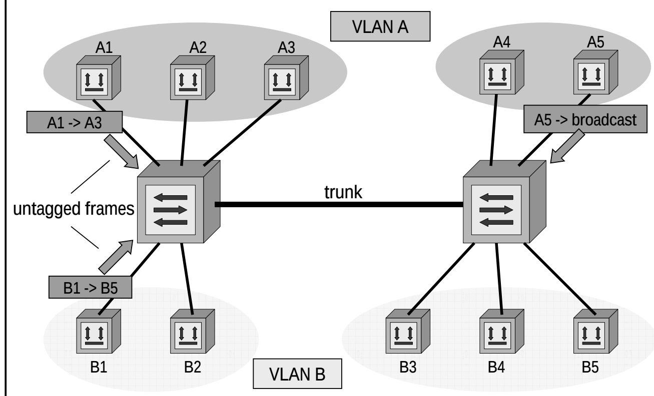


TPID … Tag Protocol Identifier
TCI … Tag Control Information

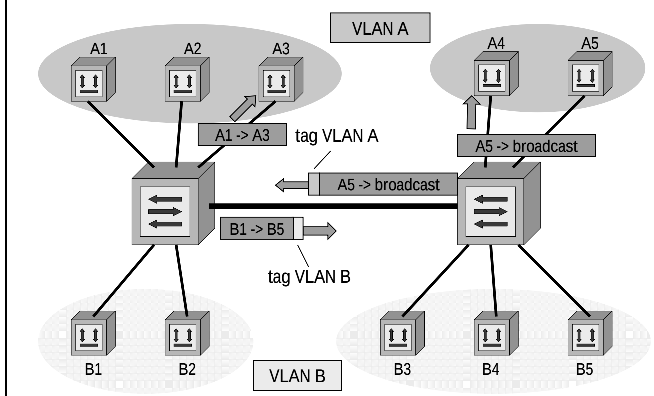
UP … User Priority
CFI … Canonical Format Identifier
VID … VLAN Identifier

note: With tagging Ethernets maximal frame length = 1522, minimal frame length = 68

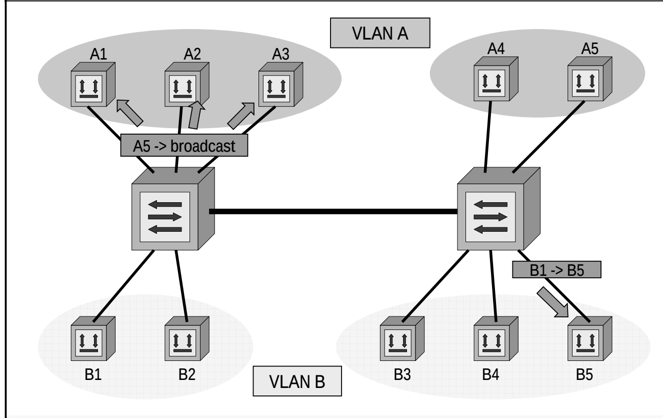
VLAN Operation (1)



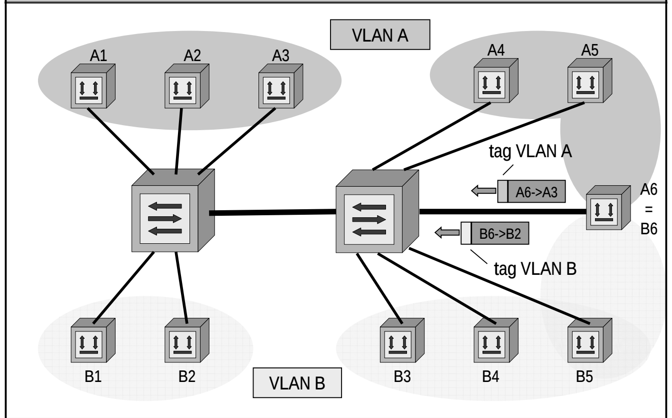
VLAN Operation (2)



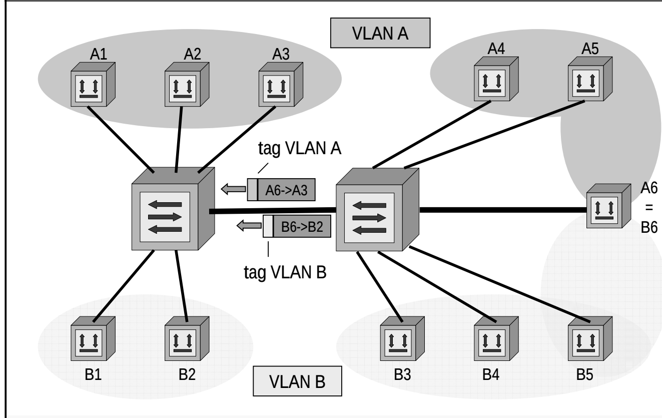
VLAN Operation (3)



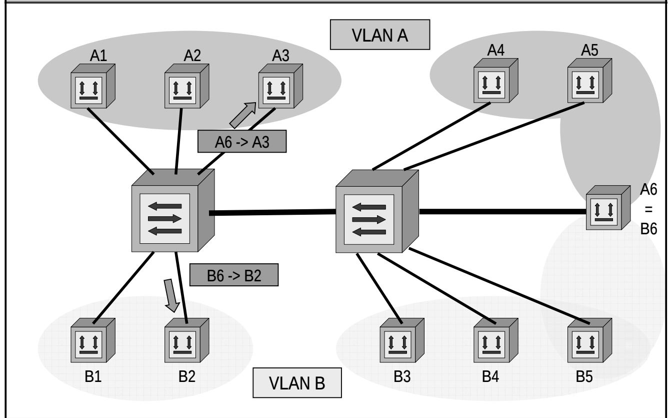
Multihomed VLAN 1



Multihomed VLAN 2



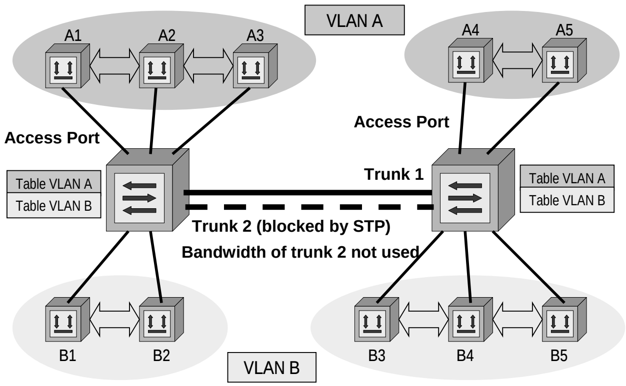
Multihomed VLAN 3



Trunking between L2 Switches

- **on trunks between multiport switches full duplex operation is possible**
  - hence "200 Mbit/s" with Fast Ethernet
  - hence "2 Gbit/s" with Gigabit Ethernet
- **on trunks <u>bundling</u> (aggregation) <u>of physical links</u> to <u>one logical link</u> is possible**
  - Fast Ethernet Channeling (Cisco)
    - 400 / 800 Mbit/s
  - Gigabit Ethernet Channeling (Cisco)
    - 4 / 8 Gbit/s
  - IEEE 802.3 (2002) LACP (Link Aggregation Control Protocol

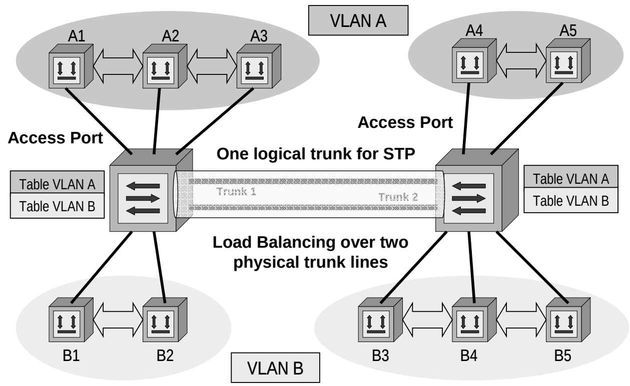
Trunking without LCAP / FEC / GEC



Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

Trunking with LCAP / FEC / GEC



Communication between VLANs

- **switches do not allow traffic between (different) VLANs**
- **end-systems have to make use of routers**
- **routers can be either part of several VLANs (via multiple physical ports), or**
- **routers provide VLAN-trunk capabilities -> router must be able to recognize and change VLAN tags**

Agenda

- **Ethernet Evolution**
- **VLAN**
- **High Speed Ethernet**
  - Introduction
  - Fast Ethernet
  - Gigabit Ethernet
  - 10 Gigabit Ethernet
- **Introduction to WLAN**

IEEE 802.3

- **the latest version of IEEE 802.3 (2005) specifies**
  - operation for 10 Mbit/s, 100 Mbit/s, Gigabit/s and 10Gigabit/sEthernet
  - full duplex Ethernet
  - auto-negotiation
  - flow control
- **it is still backward compatible to the old times of Ethernet**
  - CSMA/CD (half-duplex) operation in 100 and 1000 Mbit/s Ethernets with multiport repeater possible
  - frame bursting or carrier extension for ensuring slot-time demands in 1000 Mbit/s Ethernet
- **IEEE 802.3ak (2006)**
  - operation for 10 Gigabit/s Ethernet over copper

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

Collision Window / Slot Time

Technology	Bit-Time (sec)	Collision Window (sec)	Slot Time (bit-times)		Minimum Frame (bit-times / byte)	Distance (m)
10Mbit/s	100ns	51,2µs	512	=	512 / 64	2000-3000
100Mbit/s	10ns	5,12µs	512	=	512 / 64	~200
1000Mbit/s	1ns	0,512µs	512		512 / 64	~10-20
1000Mbit/s	1ns	4,096µs	4096*	≠	512 / 64	200

* by the usage of carrier extension / frame bursting

Full-Duplex Mode

- **full-duplex mode is possible on point-to-point links**
  - except 100BaseT4 (Cat 3 cable), 100BaseVG which can work in half duplex mode only
  - note: 10Base2 and 10Base5 are shared links and by default half duplex medias
- **if a network station is connected to an Ethernet switch via point-to-point link**
  - CSMA/CD is not in necessary and can be switched off
- **now a network station can**
  - send frames immediately (without CS) using the transmission-line of the cable and simultaneously receive data on the other line

Flow Control

- **speed-requirements for switches are very high**
  - especially in full duplex operation
  - also powerful switches can't avoid buffer overflow
  - earlier, high traffic caused collisions and CSMA/CD interrupted the transmission in these situations, now high traffic is normal
- **L4 flow control (e.g. TCP) between end-systems is not efficient enough for a LAN**
  - switches should be involved to avoid buffer overflow
- **therefore a MAC based (L2) flow control is specified**
  - MAC-control-protocol and the Pause command

MAC-Control Frame

- **identified among other frames by setting length field = 8808 hex**

always 64 octets

8 octets	6	6	2	2	44	4
preamble	DA	SA	8808h (Length)	MAC-ctrl opcode	MAC-ctrl parameters	FCS

MAC-ctrl opcode .... defines function of control frame

MAC-ctrl parameters .... control parameter data; always filled up to 44 bytes, by using zero bytes if necessary

- **currently only the "pause" function is available (opcode 0x0001)**

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

The Pause Command 1

- **on receiving the pause command**
  - station stops sending normal frames for a given time which is specified in the MAC-control parameter field
- **this pause time is a multiple of the slot time**
  - 4096 bit-times when using Gigabit Ethernet or 512 bit-times with conventional 802.3
- **paused station waits**
  - until pause time expires or an additional MAC-control frame arrives with pause time = 0
  - note: paused stations are still allowed to send MAC-control-frames (to avoid blocking of LAN)

The Pause Command 2

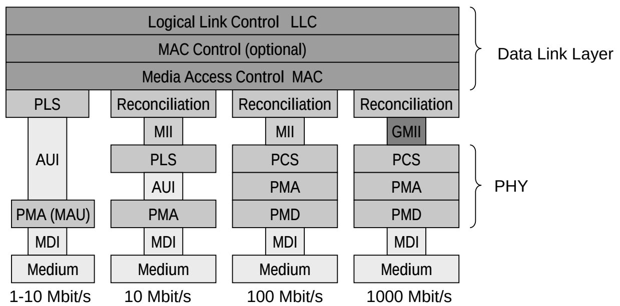
- **destination address is either**
  - address of destination station or
  - broadcast address or
  - special multicast address 01-80-C2-00-00-01
- **this special multicast address prevents bridges to transfer associated pause-frames to not concerned network segments**
- **hence flow-control (with pause commands) affects only the own segment**

Demand for Higher Speed

- **higher data rates need more sophisticated coding**
  - 10 Mbit/s Ethernet: Manchester coding
  - Fast Ethernet (100 Mbit/s): 4B/5B block code
  - Gigabit Ethernet 1000 Mbit/s): 8B/10B block code
- **new implementations should be backwards-compatible**
  - old physical layer signaling interface (PLS), represented by AUI, was not suitable for new coding technologies
- **AUI has been replaced**
  - MII (Media Independent Interface) for Fast Ethernet
  - GMII for Gigabit Ethernet

 Ethernet Evolution, v4.7 45

New Physical Sublayers



AUI...Attachment Unit Interface, PLS...Physical Layer Signaling, MDI...Medium Dependent Interface, PCS...Physical Coding Sublayer, MII...Media Independent Interface, GMII...Gigabit Media Independent Interface, PMA...Physical Medium Attachment, MAU...Medium Attachment Unit, PMD...Physical Medium Dependent

 Ethernet Evolution, v4.7 46

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

PHY Sublayers

- **Physical Layer Signaling (PLS) serves as abstraction layer between MAC and PHY**
- **PLS provides**
  - data encoding/decoding (Manchester)
  - translation between MAC and PHY
  - Attachment Unit Interface (AUI) to connect with PMA
- **several new coding techniques demands for a Media Independent Interface (MII)**
- **today coding is done through an media-dependent Physical Coding Sublayer (PCS) below the MII**

 Ethernet Evolution, v4.7 47

PHY Sublayers

- **PLS has been replaced with the Reconciliation sublayer**
  - Reconciliation layer transforms old MAC PLS-primitives into MII control signals
- **MII serves as an interface between MAC and PHY**
  - hides coding issues from the MAC layer
  - MII: often a mechanical connector for a wire; GMII is an interface specification between MAC-chip and PHY-chip upon a circuit board
  - one independent specification for all physical media
  - supports several data rates (10/100/1000 Mbits/s)
  - 4 bit (GMII: 8 bit) parallel transmission channels to the physical layer

 Ethernet Evolution, v4.7 48

PHY Sublayers

- **Physical Coding Sublayer (PCS)**
  - encapsulates MAC-frame between special PCS delimiters
  - 4B/5B or 8B/10B encoding respectively
  - appends idle symbols
- **Physical Medium Attachment (PMA)**
  - interface between PCS and PMD
  - (de) serializes data for PMD (PCS)
- **Physical Medium Dependent (PMD)**
  - serial transmission of the code groups
  - specification of the various connectors (MDI)

Bridging Aspects

- **new PHY-sublayers preserves old Ethernet MAC frame format**
  - bridging from 10 Mbit/s Ethernet to 100 Mbit/s Ethernet does not require a bridge to change the frame format
    - Remark: bridging from 10 Mbit/s Ethernet to FDDI (100 Mbit/s Token ring) requires frame format changing -> slower !!
- **therefore Ethernet L2 switches**
  - can connect Ethernets with 10 Mbit/s, 100 Mbit/s or 1000 Mbit/s easily and fast

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

Today: Gigabit Ethernet

- **continues point-to-point and full-duplex idea**
- **also backward compatible with initial 10 Mbit/s shared media idea -> CSMA/CD capable**
- **but nobody uses it as shared media!**
  - multiport repeater with Gigabit Ethernet seems absurd because of small network diameter (20m)
    - 200m with carrier extension and burst mode
  - bandwidth sharing decreases performance; every collision domain produces an additional delay for a crossing packet
  - full duplex means exclusive, unshared, high performance point-to-point connections between two stations (total 2Gbit/s!)

Gigabit Ethernet becomes WAN

- **point-to-point full-duplex connections do not limit the maximal network diameter as CSMA/CD does**
  - Gigabit over fiber optic cables reach 70 km length (and even more)
- **trend moves towards layer 3 switching**
  - high amount of today's traffic goes beyond the border of the LAN
  - routing decisions enable load balancing and decrease network traffic
- **Gigabit Ethernet becomes WAN technology**

Agenda

- **Ethernet Evolution**
- **VLAN**
- **High Speed Ethernet**
  - Introduction
  - Fast Ethernet
  - Gigabit Ethernet
  - 10 Gigabit Ethernet
- **Introduction to WLAN**

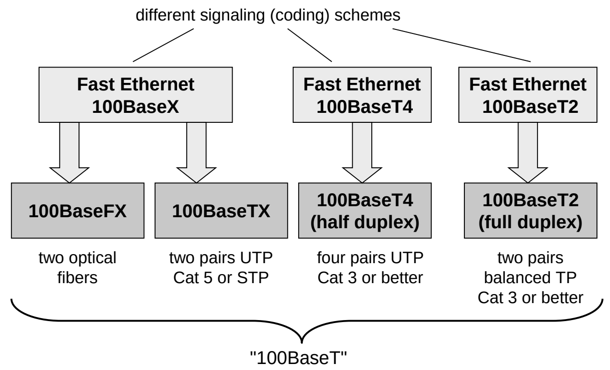
100 Mbit/s Ethernet

- **Access method disagreement split 100 Mbit/s LAN development into two branches:**
  - Fast Ethernet - IEEE-802.3u (today 802.3-2002)
  - 100VG-AnyLAN - IEEE-802.12 (disappeared)
- **Fast Ethernet was designed as 100 Mbit/s and backwards-compatible 10Mbit/s Ethernet**
  - CSMA/CD but also
  - Full-duplex connections (collision free)
- **Network diameter based on collision window requirement (512 bit times)**
  - reduced by factor 10
  - e.g. 250m compared with 2500m at 10 Mbit/s

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

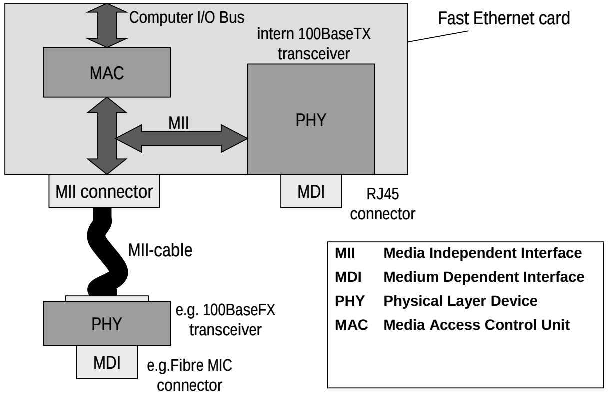
Implementation Overview



Fast Ethernet

- **AUI has been replaced with the Media Independent Interface (MII)**
  - New coding (4B/5B, 8B/6T, PAM 5x5) and bandwidth constrains demand for a redesigned abstraction layer
- **MII defines a generic 100BaseT interface**
  - Allows utilization of a 100BaseTX, 100BaseFX, 100BaseT4 or a 100BaseT2 transceiver
    - On-board or cable-connector with
    - 20 shielded, symmetrically twisted wire pairs -> 40 poles
    - One additional main-shield
    - 68 Ohm impedance; 2.5 ns maximal delay
    - 50 cm maximal length

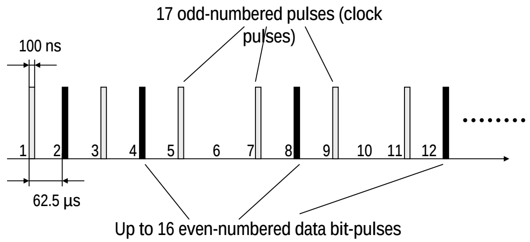
Typical Fashion



Autonegotiation

- **Autonegotiation support enables two 100BaseT devices (copper only) to exchange information about their capabilities**
  - signal rate, CSMA/CD or full-duplex
- **Achieved by Link-Integrity-Test-Pulse-Sequence**
  - Normal-Link-Pulse (NLP) technique is already available in 10BaseT to check the link state
  - 10 Mbit/s LAN devices send every 16 ms a 100ns lasting NLP -> no signal on the wire means disconnected
- **100BaseTX uses bursts of Fast-Link-Pulses (FLP) consisting of 17-33 NLPs**
  - Each representing a 16 bit word

FLP Burst Coding



= 1 1 0 1 0 1 ....

Autonegotiation

- **To avoid increase of traffic FLP-bursts are only sent on connection-establishments**
- **100BaseT stations recognizes 10 Mbit/s stations by receiving a single NLP only**
- **Two 100BaseT stations analyze their FLP-bursts and investigate their largest common set of features**
- **Last frames are sent 3 times -> other station responds with acknowledge-bit set**
- **Negotiated messages are sent 6-8 times**
  - FLP- session stops here

FLP-Session

- **The first FLP-burst contains the base-link codeword**
- **By setting the NP bit a sender can transmit several "next-pages"**
  - Next-pages contain additional information about the vendor, device-type and other technical data
- **Two kinds of next-pages**
  - Message-pages (predefined codewords)
  - Unformatted-pages (vendor-defined codewords)
- **After reaching the last acknowledgement of this FLP-session, the negotiated link-codeword is sent 6-8 times**

Base Page

S0	S1	S2	S3	S4	A0	A1	A2	A3	A4	A5	A6	A7	RF	Ack	NP

Selector field (S0–S4)   Technology ability field (A0–A7)

provides selection of up to 32 different message types; currently only 2 selector codes available:
10000....IEEE 802.3
01000....IEEE 802.9 (ISLAN-16T) (ISO-Ethernet)

Bit	Technology
A0	10BaseT
A1	10BaseT-full duplex
A2	100BaseTx
A3	100BaseTx-full duplex
A4	100BaseT4
A5	Pause operation for full duplex links
A6	reserved
A7	reserved

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

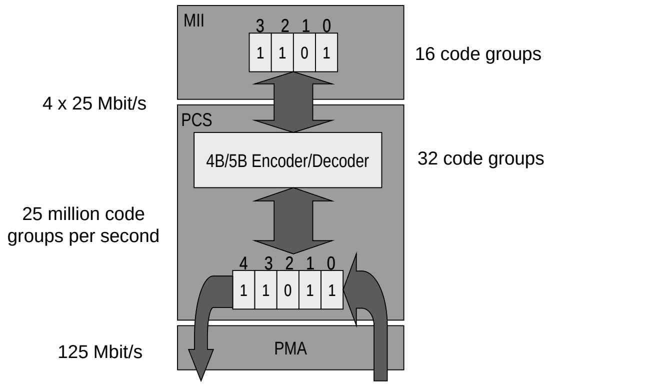
Base Page

- **Remote Fault (RF)**
  - Signals that the remote station has recognized an error
- **Next Page (NP)**
  - Signals following next-page(s) after the base-page
- **Acknowledge (Ack)**
  - Signals the receiving of the data (not the feasibility)
  - If the base-page has been received 3 times with the NP set to zero, the receiver station responds with the Ack bit set to 1
  - If next-pages are following, the receiver responds with Ack=1 after receiving 3 FLP-bursts

Coding

- **4B/5B block encoding: each 4-bit group encoded by a 5 bit run-length limited "code-group"**
  - Code groups lean upon FDDI-4B/5B codes
  - Some additional code groups are used for signaling purposes; remaining code groups are violation symbols -> easy error detection
  - Groups determinate maximal number of transmitted zeros or ones in a row -> easy clock synchronization
    - Keeps DC component below 10%
- **Code groups are transmitted using NRZI-encoding**
  - Code efficiency: 4/5 = 100/125 = 80% (Manchestercode only 50 %)

4B/5B Coding



Code Group Table

	PCS code-group	name	MII group	
DATA	11110	0	0000	
	01001	1	0001	
	10100	2	0010	
	10101	3	0011	
	01010	4	0100	
	01011	5	0101	
	01110	6	0110	
	01111	7	0111	
	10010	8	1000	
	10011	9	1001	
	10110	A	1010	
	10111	B	1011	
	11010	C	1100	
	11011	D	1101	
	11100	E	1110	
	11101	F	1111	
Control	11111	I	undefined	Idle pattern between streams
	11000	J	0101	Start of Stream Delimiter (1st part)
	10001	K	0101	Start of Stream Delimiter (2nd part)
	01101	T	undefined	End of Stream Delimiter (1st part)
	00111	R	undefined	End of Stream Delimiter (2nd part)
	00100	H	undefined	signals receiving errors

Remaining code groups are not valid (triggers error detection)

Signaling Types

- **Three signaling types :**
  - 100BaseX:
    - refers to either the 100BaseTX or 100BaseFX specification
  - 100BaseT4
  - 100BaseT2
- **100BaseX**
  - combines the CSMA/CD MAC with the FDDI Physical Medium Dependent layer (PMD)
  - allows full duplex operation on link

Signaling Types

- **100BaseT4**
  - allows half duplex operation only
  - 8B6T code
  - Uses 4 pairs of wires; one pair for collision detection, three pair for data transmission
  - One unidirectional pair is used for sending only and two bi-directional pairs for both sending and receiving
  - Same pinout as 10BaseT specification
  - Transmit on pin 1 and 2, receive on 3 and 6; bi-directional on 4 and 5; bi-directional on 7 and 8

100BaseTX and 100BaseFX

- **100BaseTX:**
  - 125 MBaud symbol rate, full duplex, binary encoding
  - 2 pair Cat 5 unshielded twisted pair (UTP) or 2 pair STP or type 1 STP
  - RJ45 connector; same pinout as in 10BaseT (transmit on 1 and 2, receive on 3 and 6)
- **100BaseFX:**
  - 125 MBaud symbol rate, full duplex, binary encoding
  - Two-strand (transmit and receive) 50/125 or 62.5/125-µm multimode fiber-optic cable
  - SC connector, straight-tip (ST) connector, or media independent connector (MIC)

100BaseT4 and 100BaseT2

- **100BaseT4:**
  - 25 MBaud, half duplex, ternary encoding
  - Cat3 or better, needs all 4 pairs installed
  - 200 m maximal network diameter
  - maximal 2 hubs
- **100BaseT2:**
  - 25 MBaud, full duplex, quinary encoding
  - 2 pairs Cat3 or better

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

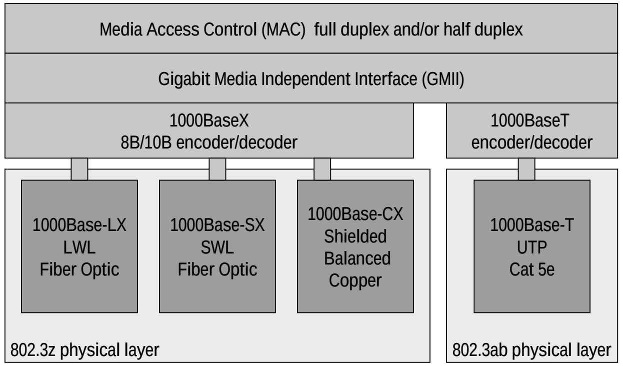
Agenda

- **Ethernet Evolution**
- **VLAN**
- **<u>High Speed Ethernet</u>**
  - Introduction
  - Fast Ethernet
  - <u>Gigabit Ethernet</u>
  - 10 Gigabit Ethernet
- **Introduction to WLAN**

Gigabit-Ethernet: IEEE-802.3z / IEEE802.3ab

- **Easy integration in existing 802.3 LAN configurations because backwards compatible**
  - Through integration of 3 different transceivers for 10, 100 and 1000 Mbit/s
  - No need to change existing equipment
  - Supports also 10 Mbit/s and 100 Mbit/s (not with fibre)
  - Access methods: CSMA/CD or full duplex
- **Backbone technology; has also WAN capabilities**
  - Reaches 70 km length using fibre optics
  - 1 Gbit/s data rate in both directions (full duplex mode, no collisions)
  - MAC based congestion avoidance (pause frame)

Implementation Overview



CSMA/CD Restrictions (Half Duplex Mode)

- **The conventional collision detection mechanism CSMA/CD**
  – Requires that stations have to listen (CS) twice the signal propagation time to detect collisions
  – Collision window of 512 bit times at a rate of 1Gbit/s limits the maximal net expansion to 20m !

CSMA/CD Restrictions (Half Duplex Mode)

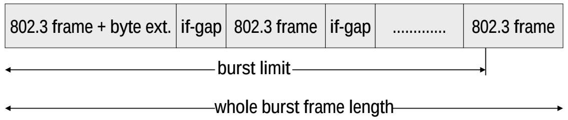
- **Solutions to increase the maximal net expansion:**
  – Carrier Extension:
    - extension bytes appended to (and removed from) the Ethernet frame by the physical layer
    - frame exists a longer period of time on the medium
  – Frame Bursting:
    - to minimize the extension bytes overhead, station may chain several frames together and transmit them at once ("burst").

Frame Bursting 1

- **With both methods the minimal frame length is increased from 512 to 4096 bits**
  – = 512 bytes
  – The corresponding time is called slottime
- **If a station decides to chain several frames to a burst frame, the first frame inside the burst frame must have a length of at least 512 bytes**
  – By using extension bytes if necessary
- **The next frames (inside the burst frame) can have normal length (i.e. at least 64 bytes)**

Frame Bursting 2

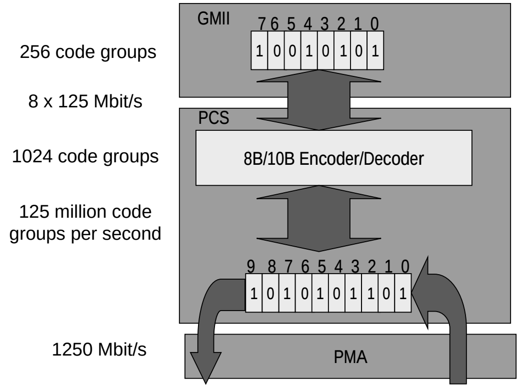
- **Station may chain frames up to 8192 bytes (=burst limit)**
  - Also may finish the transmission of the last frame even beyond the burst limit
- **So the whole burst frame length must not exceed 8192+1518 bytes**
  - Incl. interframe gap of 0.096 µs = 12 bytes



1000BaseX Coding

- **8B/10B block encoding: each 8-bit group encoded by a 10 bit "code-group" (symbol)**
  - Half of the code-group space is used for data transfer
  - Some code groups are used for signaling purposes
  - Remaining code groups are violation symbols
    - -> easy error detection
  - Groups determine the maximal number of transmitted zeros or ones in a 10 bit symbol
    - -> easy clock signal detection (bit synchronization)
  - No baselinewander (DC balanced)
    - lacking DC balance would result in data-dependent heating of lasers which increases the error rate
  - Code efficiency: 8/10 = 1000/1250 = 80%

8B/10B Coding



Implementations

- **actually 2 different wavelengths on fibre media, both full duplex, SC connector**
  - 1000Base-SX: short wave, 850 nm multimode (up to 550 m length)
  - 1000Base-LX: long wave, 1300 nm multimode or monomode (up to 5 km length)
- **1000Base-CX:**
  - Twinax Cable (high quality 150 Ohm balanced shielded copper cable)
  - About 25 m distance limit, DB-9 or the newer HSSDC connector

1000BaseT

- **1000Base-T defined by 802.3ab task force**
  - UTP uses all 4 line pairs simultaneously for duplex transmission!
    - Using echo-cancelling: receiver subtracts own signal
  - 5 level PAM coding
    - 4 levels encode 2 bits + extra level used for Forward Error Correction (FEC)
  - Signal rate: 4 x 125 Mbaud = 4 x 250Mbit/s data rate
    - Cat. 5 links, max 100 m; all 4pairs, cable must conform to the requirements of ANSI/TIA/EIA-568-A
  - Only 1 CSMA/CD repeater allowed in a collision domain
    - note: collision domains should be avoided

Autonegotiation

- **Both 1000Base-X and 1000Base-T provide autonegotiation functions to determinate the**
  - Access mode (full duplex - half duplex)
  - Flow control mode
- **Additionally 1000Base-T can resolve the data rate**
  - Backward-compatibility with 10 Mbit/s and 100 Mbit/s
  - Also using FLP-burst sessions

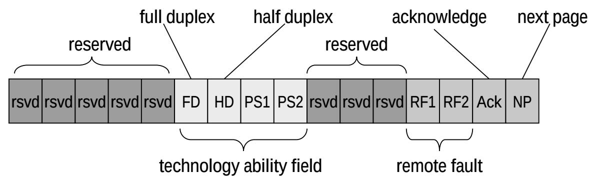
Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

1000BaseX Autonegotiation

- **1000Base-X autonegotiation uses normal (1000Base-X) signalling !**
  - Signaling part of the 8B/10B code groups
  - No fast link pulses !
    - Autonegotiation had never been specified for traditional fiber-based Ethernet
    - So there is no need for backwards-compatibility
- **1000Base-X does not negotiate the data rate !**
    - Only gigabit speeds possible
- **1000Base-X autonegotiation resolves**
  - Half-duplex versus full-duplex operation
  - Flow control

Base-Page



PS1	PS2	description
0	0	no pause
0	1	asymmetrical pause
1	0	symmetrical pause
1	1	symmetrical and asymmetrical pause

RF1	RF2	description
0	0	no error
0	1	offline
1	0	connection error
1	1	autonegotiation error (no common capabilities)

1000BaseT Autonegotiation

- **Autonegotiation is only triggered when the station is powered on**
- **At first the stations expects Gigabit-Ethernet negotiation packets (replies)**
- **If none of them can be received, the 100Base-T fast link pulse technique is tried**
- **At last the station tries to detect 10Base-T stations using normal link pulses**

Agenda

- **Ethernet Evolution**
- **VLAN**
- **High Speed Ethernet**
  - Introduction
  - Fast Ethernet
  - Gigabit Ethernet
  - 10 Gigabit Ethernet
- **Introduction to WLAN**

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

10 Gigabit Ethernet (IEEE 802.3ae)

- **Preserves Ethernet framing**
- **Maintains the minimum and maximum frame size of the 802.3 standard**
- **Supports only full-duplex operation**
  - CSMA/CD protocol was dropped
- **Focus on defining the physical layer**
  - Four new optical interfaces (PMD)
    - To operate at various distances on both single-mode and multi-mode fibers
  - Two families of physical layer specifications (PHY) for LAN and WAN support
  - Properties of the PHY defined in corresponding PCS
    - Encoding and decoding functions

PMDs

- **10GBASE-L**
  - SM-fiber, 1300nm band, maximum distance 10km
- **10GBASE-E**
  - SM-fiber, 1550nm band, maximum distance 40km
- **10GBASE-S**
  - MM-fiber, 850nm band, maximum distance 26 – 82m
  - With laser-optimized MM up to 300m
- **10GBASE-L4**
  - For SM- and MM-fiber, 1300nm
  - Array of four lasers each transmitting 3,125 Gbit/s and four receivers arranged in WDM (Wavelength-Division Multiplexing) fashion
  - Maximum distance 300m for legacy FDDI-grade MM-fiber
  - Maximum distance 10km for SM-fiber

WAN PHY / LAN PHY and their PCS

- **LAN-PHY**
  - 10GBASE-X
  - 10GBASE-R
    - 64B/66B coding running at 10,3125 Gbit/s
- **WAN-PHY**
  - 10GBASE-W
    - 64B/66B encoded payload into SONET concatenated STS192c frame running at 9,953 Gbit/s
    - Adaptation of 10Gbit/s to run over traditional SDH links

IEEE 802.3ae PMDs, PHYs, PCSs

		PCS		
PMD	10GBASE-E	10GBASE-ER		10GBASE-EW
PMD	10GBASE-L	10GBASE-LR		10GBASE-LW
PMD	10GBASE-S	10GBASE-SR		10GBASE-SW
PMD	10GBASE-L4		10GBASE-LX4	
		LAN PHY		WAN PHY

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

10 Gigabit Ethernet over Copper

- **IEEE 802.3ak defined in 2004**
  - 10GBASE-CX4
  - Four pairs of twin-axial copper wiring with IBX4 connector
  - Maximum distance of 15m
- **IEEE 802.3an working group**
  - 10GBASE-T
  - CAT6 UTP cabling with maximum distance of 55m to 100m
  - CAT7 cabling with maximum distance of 100m
  - Standard ratification expected in July 2006

Agenda

- **Ethernet Evolution**
- **VLAN**
- **High Speed Ethernet**
  - Introduction
  - Fast Ethernet
  - Gigabit Ethernet
  - 10 Gigabit Ethernet
- **<u>Introduction to WLAN</u>**

- **Most of the now following slides are taken from the Wireless LAN section**
  - http://www.perihel.at/2/index.html
  - with the friendly permission of Dipl.Ing.Herbert Haas
- **Best WLAN lectures available on the Internet**
- **Have a close look if you are involved with WLAN in the future**

Wireless LAN

- **Again a <u>shared media</u> for a lot of stations**
  - like the original Ethernet bus on coax segment
  - located around a WLAN access point
    - in the so called "Infrastructure Mode"
  - sharing originally done by a combination of TDM, CSMA/CA and FDM techniques
    - TDM … Time Division Multiplexing
    - FDM … Frequency Division Multiplexing
    - CA … Collision Avoidance
- **Everybody equipped with the proper equipment (WLAN card)**
  - can listen to the traffic going on
  - can sent traffic to the access point
  - lead to new type of security problems

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

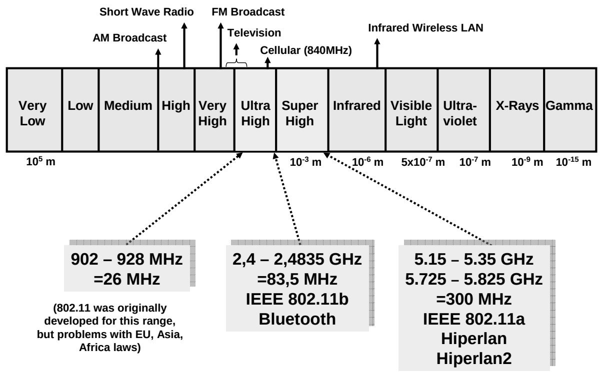
IEEE 802.11 Standard

- **Another IEEE working group**
- **Most successful WLAN standard**
  - Easy and robust wireless LAN
  - Infrared and radio transmission
  - Worldwide use (2,4 GHz)
  - "WIFI-Standard"
  - 1-54 Mbit/s
- **Infrastructure and Ad-hoc design**

IEEE Working Groups

802.1 Higher Layer LAN Protocols
802.2 Logical Link Control
802.3 Ethernet
802.4 Token Bus
802.5 Token Ring
802.6 Metropolitan Area Network
802.7 Broadband TAG
802.8 Fiber Optic TAG
802.9 Isochronous LAN
802.10 Security
802.11 Wireless LAN
802.12 Demand Priority
802.13 Not Used
802.14 Cable Modem
802.15 Wireless Personal Area Network
802.16 Broadband Wireless Access
802.17 Resilient Packet Ring

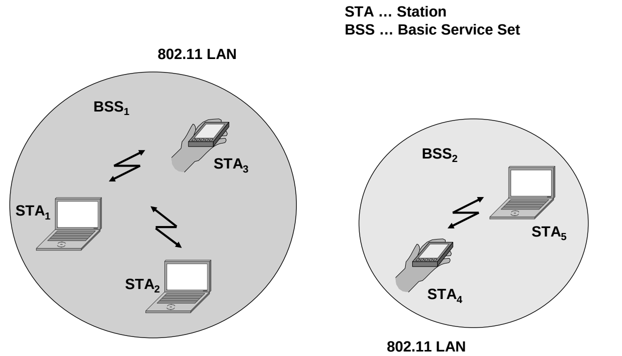
License Free ISM Band



802.11 Standard

- **802.11** **(oldest (1997), decommissioned, “legacy”)**
  - 1 and 2 Mbit/s in the 2,4 GHz-Band
  - FHSS (Frequency Hopping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum)
- **802.11a** **(2001, 2003)**
  - Up to 54 Mbit/s in the 5 GHz-Band
  - New OFDM (Orthogonal Frequency-Division Multiplexing) technology
- **802.11b** **(first (1999) and most widespread)**
  - 5,5 and 11 Mbit/s in the 2,4 GHz-Band
  - Using only DSSS
- **802.11g** **(newest, 2003)**
  - 20+ Mbit/s in the 2,4 GHz-Band (b-compatibility)
  - Vendors decided to use 54 Mbit/s, OFDM

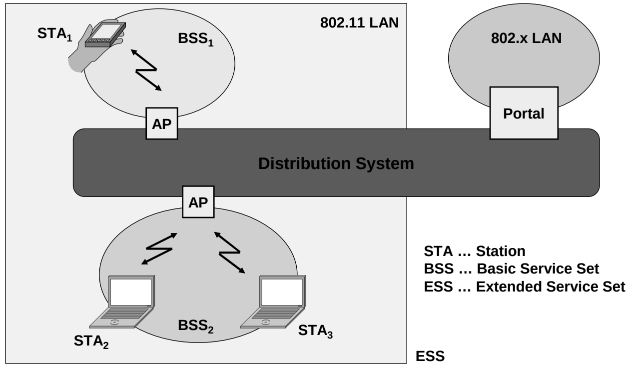
Ad-hoc Network



Datenkommunikation 384.081 - SS 2008

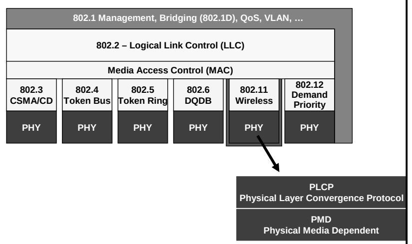
L07 - Ethernet Evolution and Wireless LAN Primer

Infrastructure Network



Protocol Layers

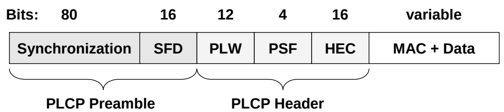
- **MAC layer**
  - Medium access control
  - Fragmentation
- **PHY layer = PLCP + PMD**
  - Established signal for controlling
  - Clear Channel Assessment (CCA)
  - Service access point
- **Physical Layer Convergence Protocol (PLCP)**
  - Synchronization and SFD
  - Header
- **Physical Medium Dependent (PMD)**
  - Modulation and coding



Clear Channel Assessment

- **CCA is an algorithm to determine if the channel is clear**
- **But what is *"clear"* ?**
  - Either measuring only WLAN carrier signal strengths
  - Or measuring the total power of both noise and carriers
- **Minimum RX signal power levels should be configured at receivers (APs & clients)**
  - CSMA would not allow to send any frames if the environmental noise level is too high
- **Part of PHY, used for MAC**

FHSS Frame Format

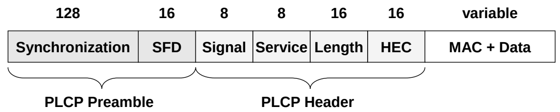


- **PLCP header runs always with 1 Mbit/s**
- **User data up to 2 Mbit/s**
- **Synchronization with 80 bit string “01010101…”**
- **All MAC data is scrambled by a $s_{(z)}=z^7+z^4+1$ polynomial to block any DC component**
- **Start Frame Delimiter (SFD)**
  - Start of the PLCP header
  - 0000110010111101 bit string
- **PLCP Length Word (PLW)**
  - Length of user data inclusive 32 bit CRC of the user data (value between 0 and 4095)
  - Protects user data
- **PLCP Signaling Field (PSF)**
  - Describe the data rate of the user data
- **Header Error Check (HEC)**
  - 16 bit CRC
  - Protect Header

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

DSSS Frame Format



- **PLCP header runs always with 1 Mbit/s (802.11 standard)**
- **User data up to 11 Mbit/s (802.11b standard)**
- **Synchronization (128 bit)**
  - Also used for controlling the signal amplification
  - And compensation for frequency drifting
- **Start Frame Delimiter (SFD)**
  - 1111001110100000
- **Signal (Rate)**
  - 0x0A → 1 Mbit/s (DBPSK)
  - 0x14 → 2 Mbit/s (DQPSK)
  - Other values reserved for future use
    - 11 Mbit/s today with CCK
- **Service**
  - 0x00 → 802.11 frame
  - Other values reserved for future use
- **Length**
  - 16 bit instead of 12 bit in FHSS
- **Header Error Check (HEC)**
  - 16 bit CRC (ITU-T-CRC-16 Standardpolynom)

MAC Principles

- **Responsible for several tasks**
  - Medium access
  - Roaming
  - Authentication
  - Data services
  - Energy saving
- **Asynchronous data service**
  - Ad-hoc and infrastructure networks
- **Realtime service**
  - Only infrastructure networks

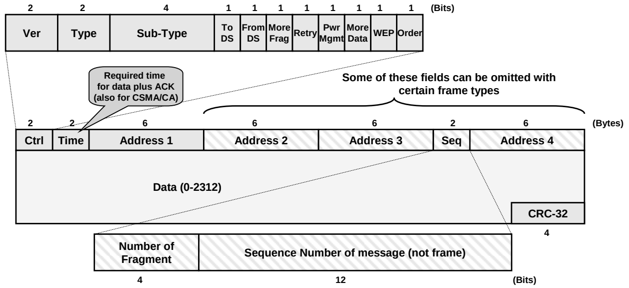
MAC Header – Overview

2	2	6	6	6	2	6	0-2312	4
FC	D-ID	Address 1	Address 2	Address 3	SC	Address 4	Data	CRC

MAC Header (FC through Address 4)

- **Frame Control (FC) includes**
  - Protocol version, frame type
  - Encryption information
  - 2 Distribution System Bits (DS)
- **Duration ID (D-ID) for virtual reservations**
  - Includes the RTS/CTS values
- **Addresses are interpreted according DS bits**
- **Sequence Control (SC) to avoid duplicates**

MAC Header – More Specific



- **Header length: 10-30 Bytes**
- **Total maximum length: 2346 Bytes (without CRC)**
- **Time field also used for power saving**

Header Details – Addresses

Ctrl: To DS	Ctrl: From DS	Address 1	Address 2	Address 3	Address 4	
0	0	Receiver	Sender	Cell	--	Used for all mgmt and ctrl frames. Used for data frames in Ad-hoc or broadcast situations.
0	1	Receiver	Cell	Sender	--	Communication inside BSS: Frame from AP to Receiver. Sender is originator. ACK must be sent to AP.
1	0	Cell	Sender	Receiver	--	Communication inside BSS: Frame from Sender to AP. Should be relayed to receiver.
1	1	Cell	Cell	Receiver	Sender	Communication between APs. Address1 is receiving AP, address2 is sending AP.

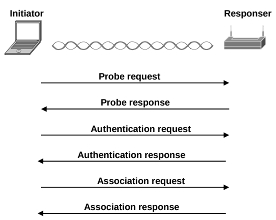
- **Infrastructure network:**
  Cell address = AP's MAC address

Note

- **If an AP is used, ANY traffic runs over the AP**
  - Because stations do not know whether receiver is associated to this AP or another AP
- **Cell address = AP‘s MAC address**
  - Always specified in header
  - Not *needed* in Ad-hoc network

Service Set Management Frames

- **Beacon frame**
  - Sent periodically by AP to announce its presence and relay information, such as timestamp, SSID, and other parameters
  - Radio NICs continually scan all 802.11 radio channels and listen to beacons as the basis for choosing which access point is best to associate with
- **Probe request frame**
  - Once a client becomes active, it searches for APs in range using probe request frames
  - Sent on every channel in an attempt to find all APs in range that match the SSID and client-requested data rates
- **Probe response frame**
  - Typically sent by APs
  - Contains synchronization and AP load information (also other capabilities)
  - Can be sent by any station (ad hoc)



Authentication and Association

- **Authentication frame**
  - AP either accepts or rejects the identity of a radio NIC
- **Deauthentication frame**
  - Send by any station that wishes to terminate the secure communication
- **Association request frame**
  - Used by client to specify: cell, supported data rates, and whether CFP is desired (then client is entered in a polling list)
- **Association response frame**
  - Send by AP, contains an acceptance or rejection notice to the radio NIC requesting association
- **Reassociation request frame**
  - To support reassociation to a new AP
  - The new AP then coordinates the forwarding of data frames that may still be in the buffer of the previous AP waiting for transmission to the radio NIC
- **Reassociation response frame**
  - Send by AP, contains an acceptance or rejection notice to the radio NIC requesting reassociation
  - Includes information regarding the association, such as association ID and supported data rates
- **Disassociation frame**
  - Sent by any station to terminate the association
  - E. g. a radio NIC that is shut down gracefully can send a disassociation frame to alert the AP that the NIC is powering off

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

Beacon Details

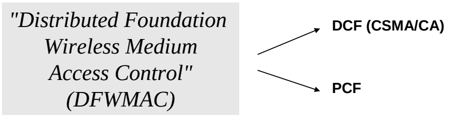
- **Clients verify their current cell by examine the beacon**
- **Beacon is typically sent 10 times per second**
- **Information carried by beacon:**
  - Timestamp (8 Bytes)
  - Beacon Interval (2 Bytes, time between two beacons)
  - Cell address (6 Bytes)
  - All supported data rates (3-8 Bytes)
  - Optional: FH parameter (7 Bytes, hopping sequenz, dwell time)
  - Optional: DS parameter (3 Bytes, channel number)
  - ATIM (4 Bytes, power saving in ad-hoc nets) or TIM (infrastructure nets)

SSID

- **32 bytes, case sensitive**
  - Spaces can be used, but be careful with *trailing* spaces
- **Multiple SSIDs can be active at the same time; assign the following to each SSID:**
  - VLAN number
  - Client authentication method
  - Maximum number of client associations using the SSID
  - Proxy mobile IP
  - RADIUS accounting for traffic using the SSID
  - Guest mode
  - Repeater mode, including authentication username and password
- **Only "Enterprise" APs support multiple SSIDs**
  - Cisco: 16
  - One broadcast-SSID, others kept secret
  - Repeater-mode SSID

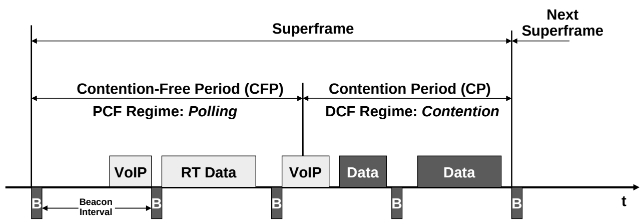
```
AP# configure terminal
AP(config)# configure interface dot11radio 0
AP(config-if)# ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# end
```

Access Methods - CSMA/CA



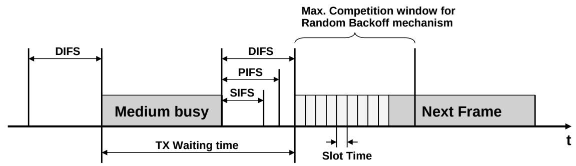
- **Distributed Coordination Function (DCF)**
  - Asynchronous data service
  - Optionally with RTS/CTS
- **Point Coordination Function (PCF)**
  - Intended for realtime service (e. g. VoIP)
  - Polling method
  - Optional

Superframe



- **Beacon is sent by "Point Coordinator" (PC=AP)**
- **Minimum CP period guaranteed**
  - To avoid starvation of non-realtime data
  - At least one frame can be sent
- **<u>Note:</u> Poll-Frames and ACKs omitted in this picture!**

CSMA Access Method



Basic Ideas

- **No standing waves in free space => no Ethernet-like collision detection possible**
- **Collision is detected by missing ACKs!**
- **Truncated Random Exponential Backoff like in Ethernet and 802.3**
- **Simple fragmentation mechanism**
  - Ethernet compatibility
  - Performance (interferences)
- **CCA to determine medium state**
- **CSMA: "Listen before talk“**
- **A safety Inter-frame Space (DIFS | PIFS | SIFS, plus Backoff) must be awaited before TX**

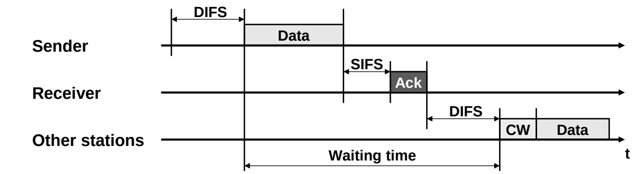
Details

- **CW is multiple of Ethernet slot time**
  - If medium is busy: Backoff
  - Slot time: 47 µs (9 µs)
- **DCF Inter-Frame Space (DIFS)**
  - Longest waiting time, 128 µs (34 µs)
  - Used for asynchronous data services
- **PCF Inter-Frame Space (PIFS)**
  - Used for APs to stop user communication, 78 µs (25 µs)
- **Short Inter-Frame Space (SIFS)**
  - Shortest waiting time, highest priority, 28 µs (16 µs)
  - Used for ACKs

Backoff Policies

- **Random backoff reduces collisions**
- **Competition window (CW)**
  - Start value of 7 slot times
  - After every collision → CW doubled
  - To a max of 255
- **Post-backoff**
  - After successful transmission
  - To avoid "channel-capture"
- **Exception: Long silent durations**
  - Station may send immediately after DIFS

CSMA/CA in Action

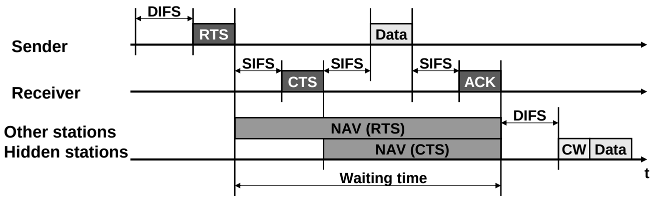


- **Point-to-point communication**
- **Acknowledgment is send after SIFS**
  - Before all other communications
  - Guaranteed collision free
- **Re-transmitted frames have no higher priority over other frames**

CSMA/CA with RTS/CTS Access Method

- **Avoid the problem of invisible devices or "Hidden Stations"**
  - Station receives data from two other devices
  - The two other devices didn't see each other
  - Each device thinks medium is free → Collision
- **2 special packets → RTS and CTS**
  - Every station must listen to this packets

Four-way handshake:
1. RTS
2. CTS
3. Data
4. ACK



Datenkommunikation 384.081 - SS 2008

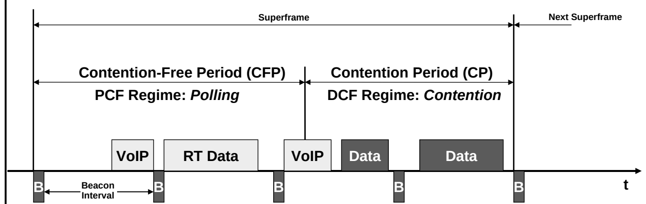
L07 - Ethernet Evolution and Wireless LAN Primer

RTS/CTS => "Virtual Reservation"

- **Collision can only occur at the begin or after a transmission**
- **Much more overhead**
  - RTS/CTS packets increase the total access-delay
- **Usage guidelines**
  - Only when longer frames are sent on average (> 500 Bytes)
  - When hidden stations are expected

PCF – Polling Principle

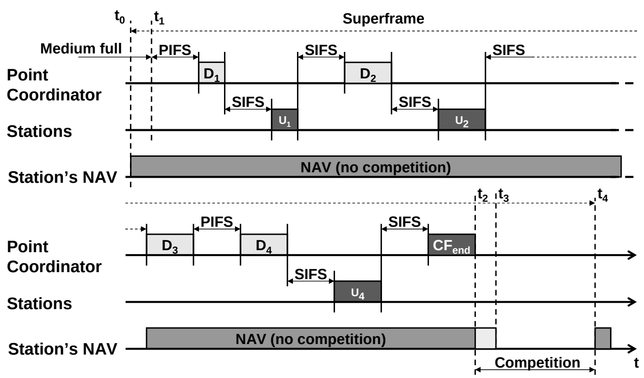
- **Guaranteed transmission parameters**
  - Minimum data rate
  - Maximum access-delay
- **AP necessary (!)**
  - For medium access control
  - Polling and time-keeping
  - Acts as "point coordinator"
- **Point Coordinator (PC) splits access time into a Superframe**
  - Contention-free period (PCF method)
  - Contention period (DCF method)
- **Target Beacon Transmission Time (TBTT) is announced in each beacon**



CFP Policy

- **Beacon starts CFP by announcing maximum duration of CFP**
  - Can be multiple of Beacon intervals
  - Intermediate Beacons indicate the remaining CFP duration
- **Between two successive CFPs there must be space to send at least on frame in the CP mode!**
- **The AP may finish the CFP earlier!**
  - Sending the CF-End Control Frame
- **CFP is *optional***
  - CSMA/CA-only clients must not interfere
  - CFP also relies on CSMA/CA

PCF Medium Access



PCF Algorithm

- **At t_0 starts the competition free zone**
- **Medium gets free at t_1**
- **After PIFS the PC can access the medium**
  - No other station can access because PIFS is smaller than DIFS
- **Now PC polls first station (D1)**
- **Stations may answer with user data after SIFS**
- **Stations must Ack within PIFS**
  - PIFS is shortest idle period within CFP
- **All frames are sent through AP !!!**
- **AP maintains list of all stations that should be polled**
  - Announced by association process
  - PC continuously polls listed stations
- **PC can send data together with beacon (piggy-back)**
- **By sending a CF_{end} frame the PC starts the CP**

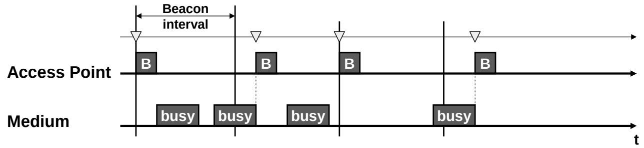
802.11g/b Compatibility

- **"b" expects CCK preamble and cannot detect OFDM signals**
  - Therefore collisions with legacy "b"
- **Compatibility mode**
  - g-devices only use RTS/CTS
    - Always 1 Mbit/s and BPSK
    - Newer "g" sends a CCK-based CTS before each OFDM-based data frame
  - "g" suffers from reduced throughput
    - 8-14 Mbit/s instead of 22 Mbit/s
- **"g" reaches longer distances (=>OFDM)**
  - Cell design must consider b-only clients
  - Only when same power level used !

Synchronization

- **Timing Synchronization Function (TSF)**
  - Used to synchronize all clocks
  - Established by *timestamps* in periodic beacon
- **Important for**
  - Energy saving mechanism
  - Roaming
  - PCF coordination(!)
  - Synchronization with FHSS systems
- **Note: Beacon-frame are not strictly sent periodically**
  - Medium might be busy

Synchronization via AP

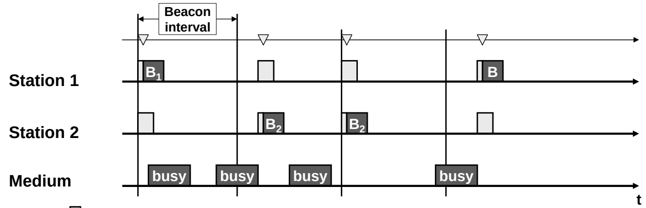


- ▽ - **Time stamp**
- B - **Beacon Frame**
- **Infrastructure networks**
  - Access point cares for synchronization

Datenkommunikation 384.081 - SS 2008

L07 - Ethernet Evolution and Wireless LAN Primer

Synchronization with Ad-hoc



- ▯ - **Random delay**
- **Each station tries to send beacon frame after each interval**

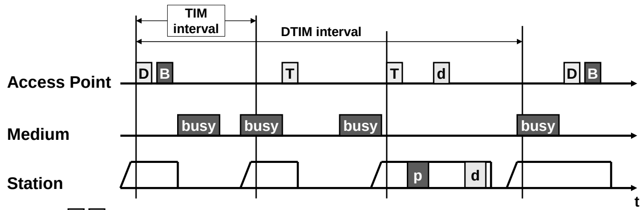
Power Management

- **Many devices use batteries: energy saving mechanisms are essential for acceptance**
- **Typical consumptions (at 100 mW)**
  - TX: 450 mA
  - RX: 270 mA
  - Sleep: 15 mA
- **IEEE 802.11 standard**
  - Transition between modes always initiated by station
- **Two system modes**
  - 1) Active (power save after configured idle period possible)
  - 2) Power (power save after TX/RX event)
- **Two power states**
  - 1) Awake
  - 2) Doze
- **TSF necessary**

Power Management

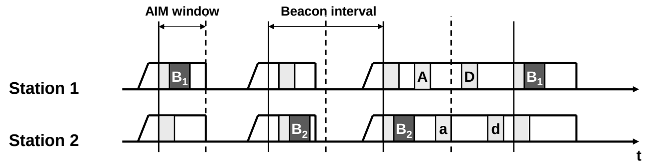
- **Traffic Indication Map (TIM)**
  - Sent with every beacon
  - Indicates for which stations frames are buffered
- **Delivery Traffic Indication Map (DTIM)**
  - List for broadcast/multicast receivers
- **Every TIM interval the station wakes up and listens for a TIM packet**
- **If there is data available, the station first emits the PS packet, then receives the data**

Power Management via AP



- **T D TIM/DTIM frames**
- **B Broadcast**
- **p Power Saving (PS) frame = "I am awake, send me data"**

Power Management with Ad-hoc



- **A a ATIM packet and ATIM-Ack**
- **D d Data and data-Ack**
- **B Beacon packet**
- **Random delay**

Power Management

- **Every Beacon interval all stations wake up**
- **If a station has data for another one, the station sends out an Ad-hoc Traffic Indication Map (ATIM)**
- **After the right station received this packet, this station sends back an acknowledgment**
- **Now the station remains in the awake modus**

Attacks on WLANs

- **Classical shared media**
  - Network sniffing is easily possible and can not be prevented
  - You need no physical access to it
  - Distance of reachability (range) can not exactly be determined
    - Power of sender
    - Sensitivity of receiver (antenna)
    - Location conditions
- **Dangers**
  - Getting sensitive information (username, passwords) in order to impersonate legitimate users
  - Using IP infrastructure (Internet access) on behalf of legitimate users
  - "Pluy and Play" mode of wireless components is very "helpful" to provide instant open access

Wireless LAN – Security 1

- **Protection achievable only by crypto-graphical methods**
- **Following possibilities:**
  - Encryption for privacy
    - WEP (Wired Equivalent Privacy, shared secret-key)
      - part of the original 802.11 standard
      - Very insecure, "DESASTER"
    - TKIP (Wi-Fi, Temporal Key Integrity Protocol, shared secret-key)
      - Still WEP based but avoids known WEP vulnerabilities
    - AES (Advanced Encryption Standard)
  - Authentication
    - Open (WEP)
    - Shared (WEP)
    - WPA (Wi-Fi Protected Access)
      - Together with 802.1x / EAP / AAA infrastructure (Radius)
      - Dynamic WEP keys
    - WPA PSK (Pre Shared Key)
      - SOHO area

Wireless LAN – Security 2

- **Following possibilities (cont.:**
  - Real strong solutions still on the way
    - IEEE 802.11i end of 2004 released
    - WPA-2
      - WPA2-Personal (PSK)
      - WPA2-Enterprise (EAP, AAA Server)
- **Even with crypto-graphical methods**
  - Discovery of WLAN infrastructure is possible
    - WLAN management frames
      - Beacons, Probe Request/Response
      - Authentication Request/Response
      - Association Request/Response
    - SSID, MAC in clear-text, L3 maybe secured
  - Denial of Service (DoS) is possible
    - E.g. high power RF signal generator