Energieinformationstechnik
Teil 2.1 Ethernet

Dr. Leonhard Stiegler

www.dhbw-stuttgart.de

Kursinhalt

- Ethernet Übersicht und Protokolle
- Ethernet Schicht-1
- Ethernet Link Schicht
- Medium Access Control
- Logical Link Control – LLC
- Ergänzende LAN Protokolle

Definitionen

- Ein Computernetz ist eine Zusammenschaltung von Host-Rechnern, die Informationen austauschen über
  - Übertragungsverbindungen und
  - Netzknoten
- Ein **Lokales Netz** (**LAN**) umfasst in der Regel einen begrenzten geografischen Bereich, wie z.B. ein Gebäude, Stockwerk oder einen Campus
- **Ethernet** ist eine weit verbreitete LAN Technologie. Sie definiert
  - das Übertragungsmedium
  - den Zugang zum Medium
  - die physikalischen Übertragungseigensaften und Prozeduren
- Ethernet ist Teil der Standardisierungsfamilie 802

IEEE 802 Standardisierung

802.1 **LAN/MAN Architecture**
WGs: Interworking,
Security,
Audio/Video Bridging and
Congestion Management.

802.2 : **Logical Link Control (LLC)**

802.3 : **Ethernet**
Basic Ethernet 10 Mbit/s
Fast Ethernet 100 Mbit/s over copper or fibre
Gbit-Ethernet 1 Gbit/s over copper or fibre
10G-Ethernet 10 Gbit/s over optical fibres

802.11 : **WLAN**

802.16 : **WMAN**

802.17 : **Resilient Packet Ring**

IEEE 802.3 Standards

Section 1: Carrier sense multiple access with collision detection (CSMA/CD) Zugangsmethode und physikalische Schicht

Section 2: Einführung in 100 Mb/s Basisband Netze, 100BASE-T, FE

Section 3: Einführung in 1000 Mb/s Basisband Netze, GE

Section 4: Einführung in 10 Gb/s Basisband Netze

Section 5: Einführung in Ethernet für Teilnehmer-Zugangsnetze

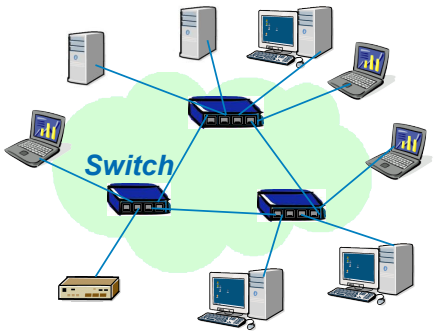
LAN Characteristika

- Führende Rolle in den Ethernet IEEE 802.3 Implementierungen
- Universelle IEEE 802.3 Medium Access Control Adressierung
- Hohe Datenrate: aktuell über 10 Gbit/s
- Möglichkeit der optischen Datenübertragung
- Entwicklung von Bus-Topologie (shared medium) zur Stern Topologie (dedicated media)
- Anwendungen:
  Private Netze, Zugangsnetze, Stadtnetze (Metropolitain Area Networks) Weitverkehrsnetze (Wide Area Networks)
- Diesteintegration: Echtzeit Sprache und Video
- Wireless LAN Implementierungen (IEEE 802.11, IEEE 802.16)

Netzwerke

Lokale Netze (Local Area Networks)

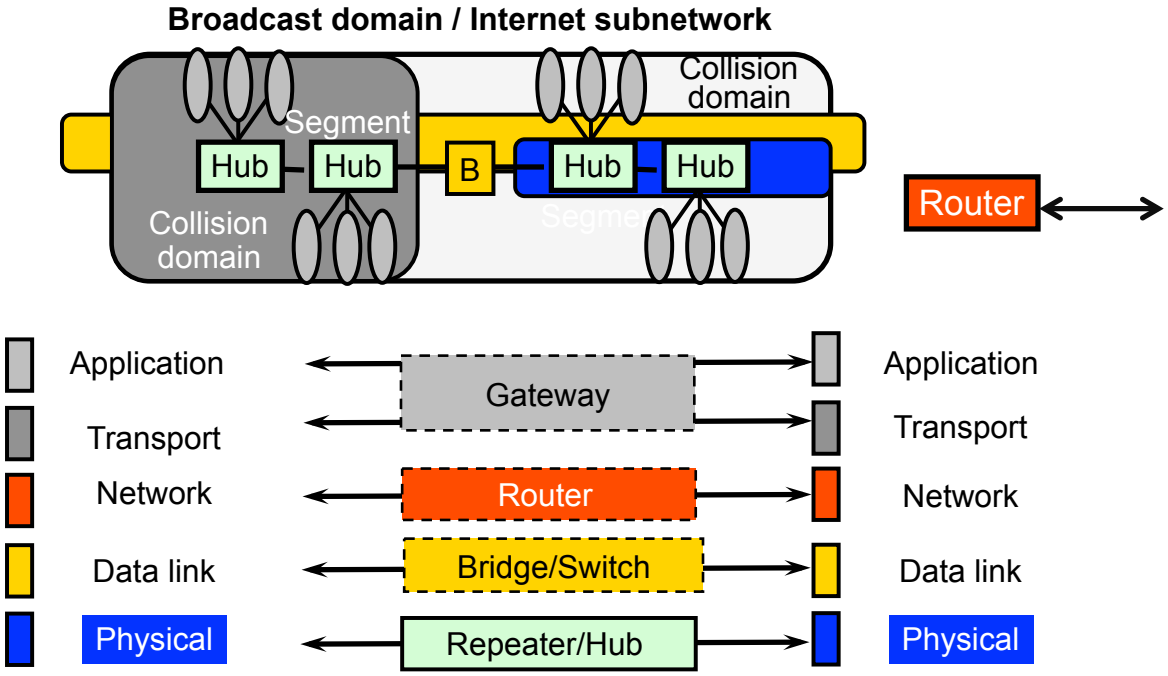
- Arbeitsplatz
- Zuhause
- Telekommunikationsnetze
- Automatisierungstechnik
- Transport (Schiene, Luft, Wasser)
- Medizintechnik



Ethernet Elemente

- Schicht-1 : Hub (wird nicht mehr verwendet)
- Switch / Bridge
  - Schicht-1 Funktion : Port
  - Schicht-2 Funktion :
    Verbindung von Eingangsport mit Ausgangsport

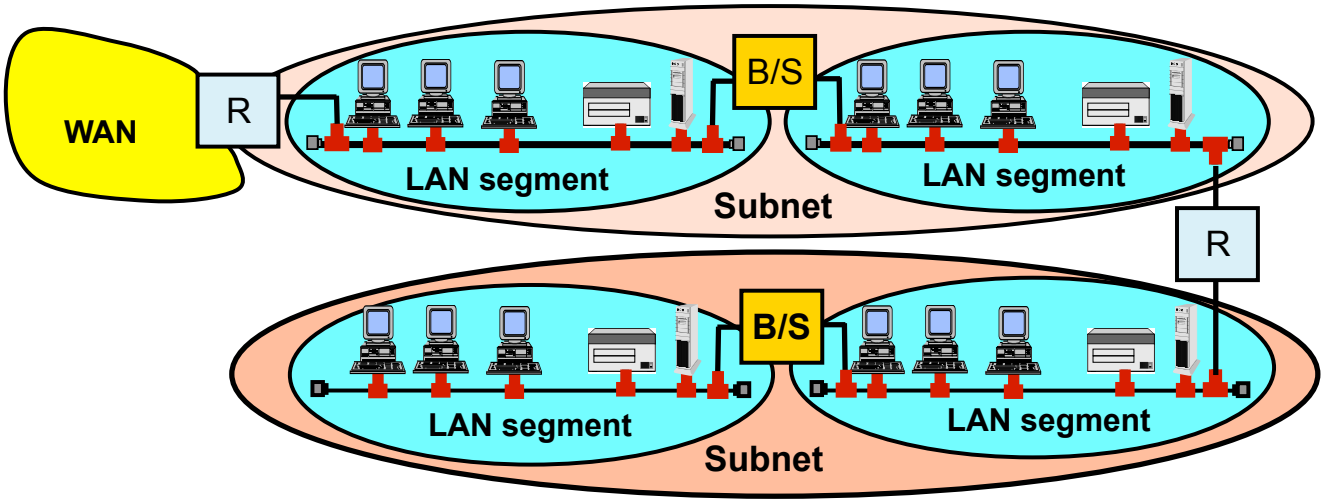
Netzelemente der Protokollschichten



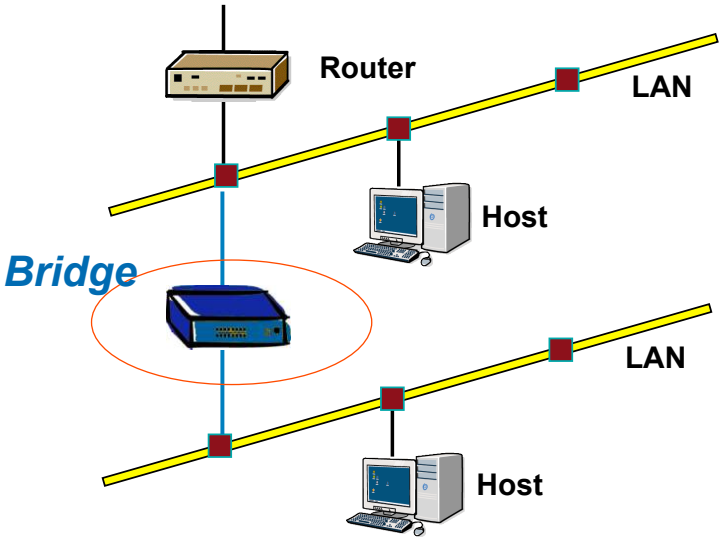
Bridge, Switch und Router

B/S • Bridge/Switch verbindet Schicht-2 LAN Segmente

R • Router verbindet Schicht-3 Netze



Netzelemente : vom Hub zur Bridge



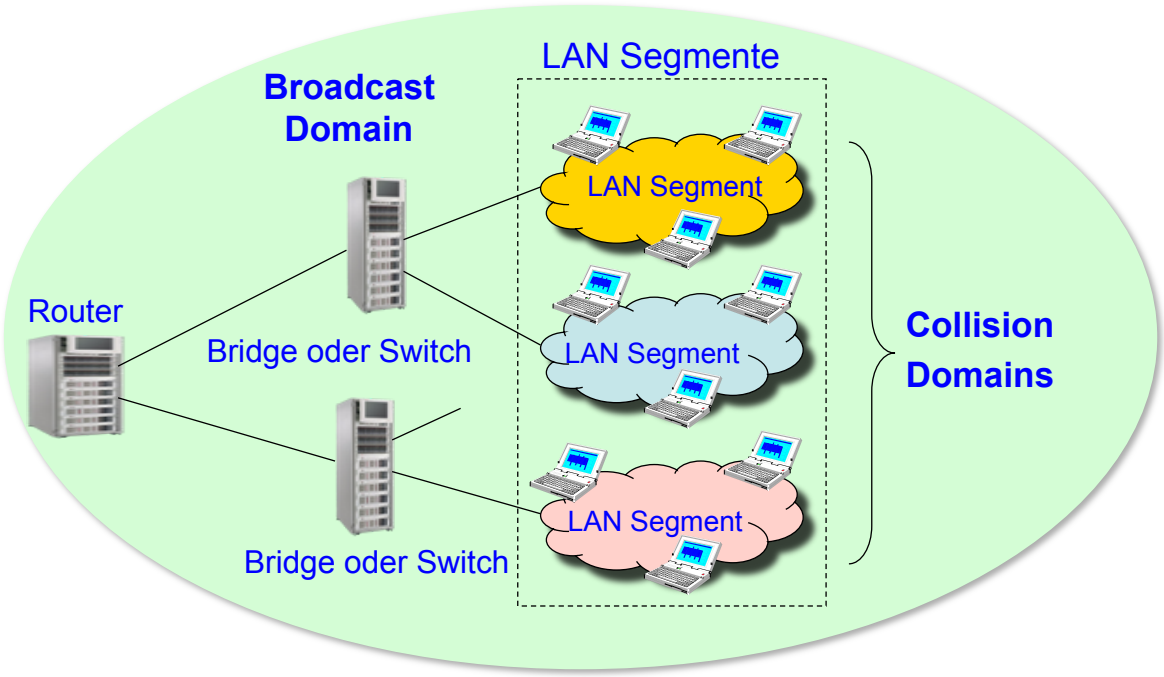
LAN Segment 1 (local traffic)

Traffic between segments

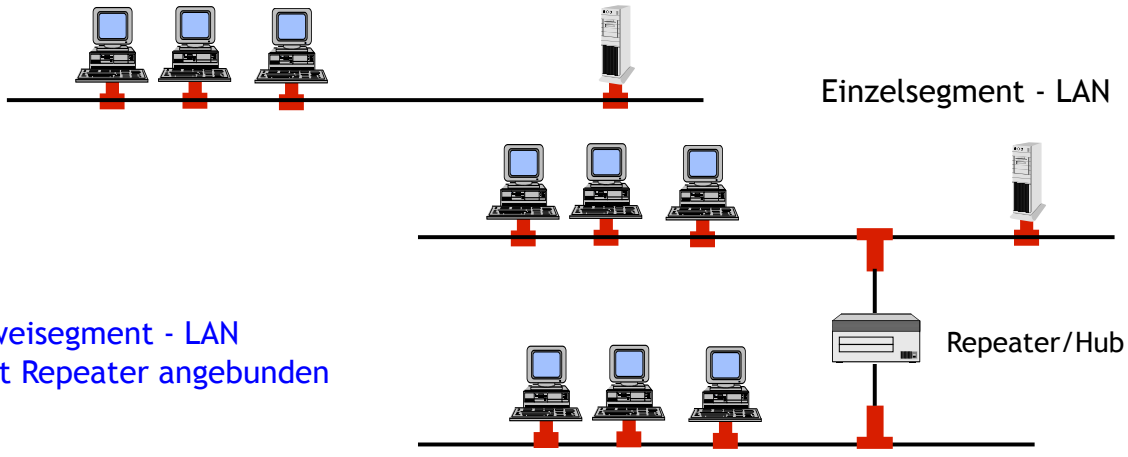
LAN Segment 2 (local traffic)

- Ein Hub “lötet” zwei LAN Segmente zusammen: jede Nachrícht wird an alle Ports weiter verteilt
- Eine Bridge “überspannt” zwei LAN Segmente: nur Nachrichten an Empfänger im jeweiligen Segment werden übermittelt

LAN Architekturbeispiel



LAN Segmentierung



- Heutige LAN Implementierungen verwenden keine Repeater, da diese Funktionen so genannte Collision domains bilden
- Die Übertragungskapazität in collision domains wird durch das geteilte Medium reduziert

Kursinhalt

- Ethernet Übersicht und Protokolle
- Ethernet Schicht-1
- Ethernet Link Schicht
- Medium Access Control
- Logical Link Control – LLC
- Ergänzende LAN Protokolle

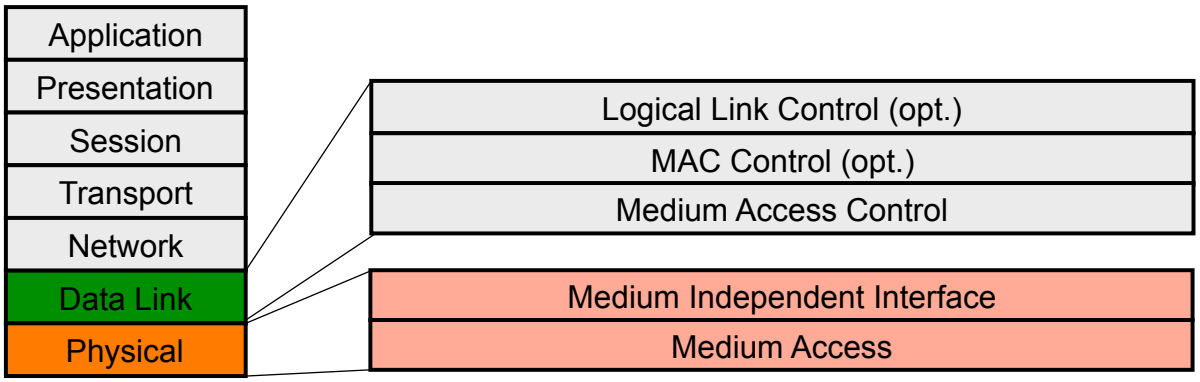
Ethernet Protokollschichten

Schicht-1 Funktionen

- Medium Access — **Medium Independent Interface**, **Medium Interface**

Schicht-2 Funktionen

- Zugang zum Übertragungsmedium — **Mediaum Access Control**
- Protokollsteuerung — **MAC Control**
- Link Verbindungssteuerung — **Logical Link Control**

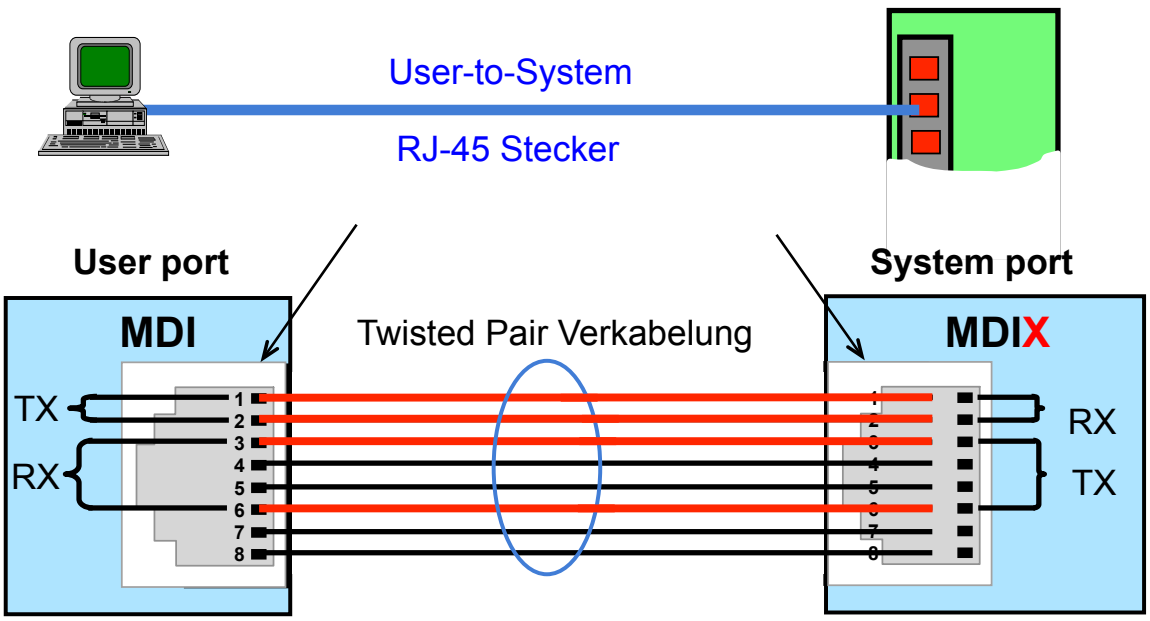


LAN Architektur

Ethernet (10Mbit/s)		Fast Ethernet - FE	Gigabit Ethernet	
	MAC User (e.g. LLC)			LLC
MAC Control (opt.)				MAC
Medium Access Control (MAC)				MAC
PLS	Reconciliation	Reconciliation	Reconciliation	PHY
AUI	MII	GMII	GMII	PHY
	PLS	PCS	PCS	PHY
	AUI	PMA	PMA	PHY
PMA	PMA	PMD	PMD	PHY
MDI				PHY
Medium				PHY

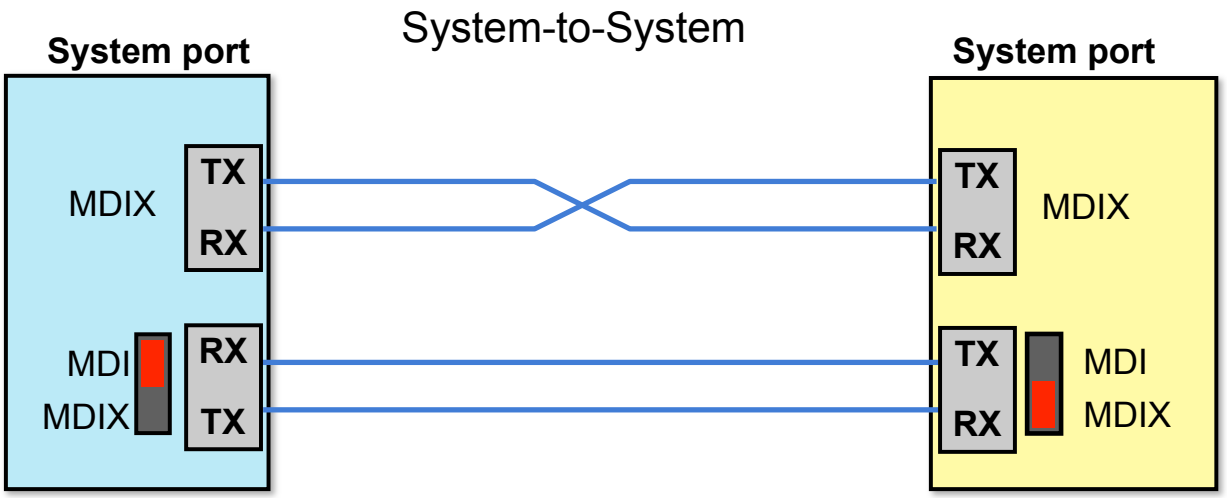
PLS: Physical Layer Signalling
AUI: Attachment User Interface
PMA: Physical Medium Access
MDI: Media Dependent Interface
MII: Medium Independent Interface
PCS: Physical Coding Sublayer
PMD: Physical Media Dependent Sublayer
LLC: Logical Link Control

LAN Verkabelung: Twisted Pair Link



Bei einer 1:1 Verkabelung müssen die Ports einer Seite getauscht werden (MDIX).

LAN Verkabelung: Twisted Pair Link



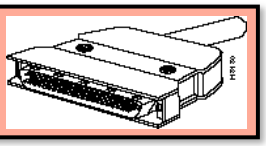
Ethernet BASE Übersicht

Variant Cable specification (min.)		Maximum Distance	
Ethernet			
10BASE-T	Class C, 2 x UTP, 16 MHz	100 m	HD/FD
Fast Ethernet			
100BASE-TX	Class D, 2 x UTP, 100 MHz	100 m	HD/FD
100BASE-T4	Class C, 4 x UTP, 100 MHz	100 m	HD
100BASE-FX	2 x 62,5/50 µm, MMF, 1310 nm	400 m 2 km	HD FD
Gigabit Ethernet			
1000BASE-T	Class D, 4 x UTP, 100MHz	100 m	HD
1000BASE-CX	STP 150 Ohm,	25 m	HD
1000BASE-SX	50 µm, MMF, 850 nm 62,5 µm, MMF, 850 nm	550 m 260 m	FD FD
1000BASE-LX	50 µm, MMF, 1310 nm 62,5 µm, MMF, 1310 nm 9 µm, SMF, 1310 nm	550 m 440 m 3 km	FD FD FD

Fast Ethernet

100Mbit/s Media Access Control Protocol (MAC)
802.3u CSMA/CD

Media Independent
Interface (MII)



100BaseT4	100BaseTX	100BaseFX

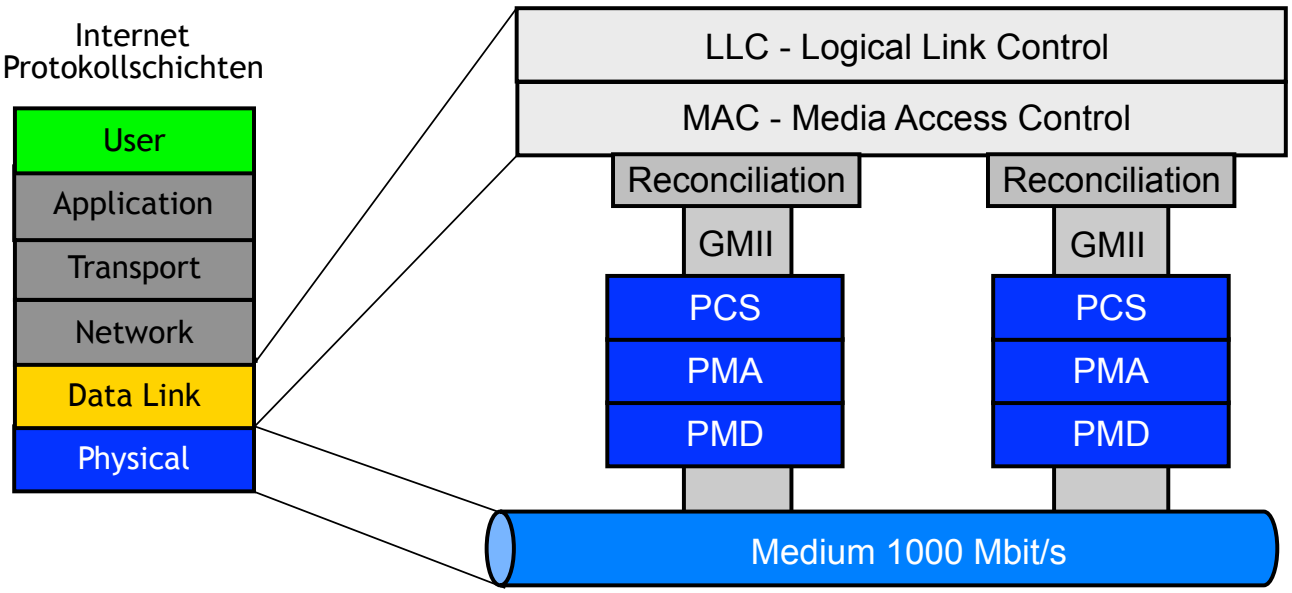
Gigabit Ethernet

1000MBit/s Media Access Control Protocol (MAC)
802.3z CSMA/CD

Gigabit Media Independent
Interface (GMII)
1000BaseCX

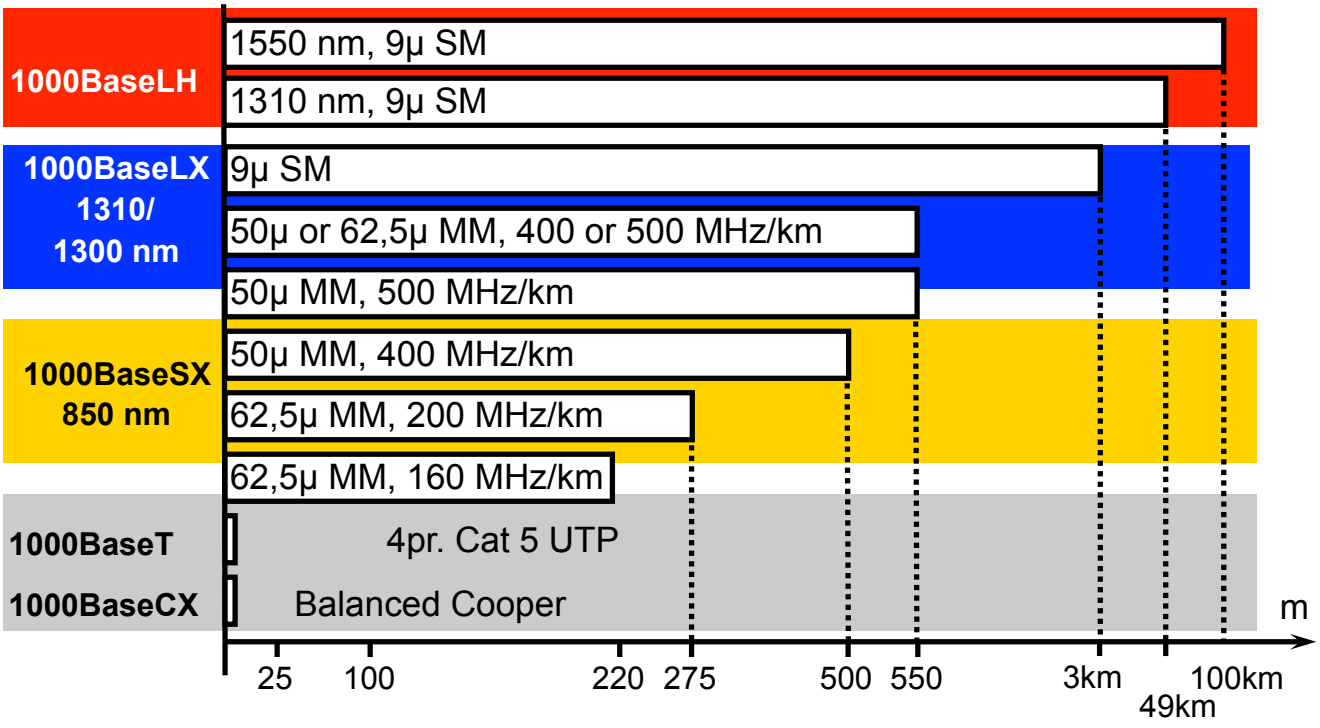
1000BASE LX	1000BASE SX	1000 BASE CX	802.3ab 1000BaseT

Gigabit Ethernet Architektur



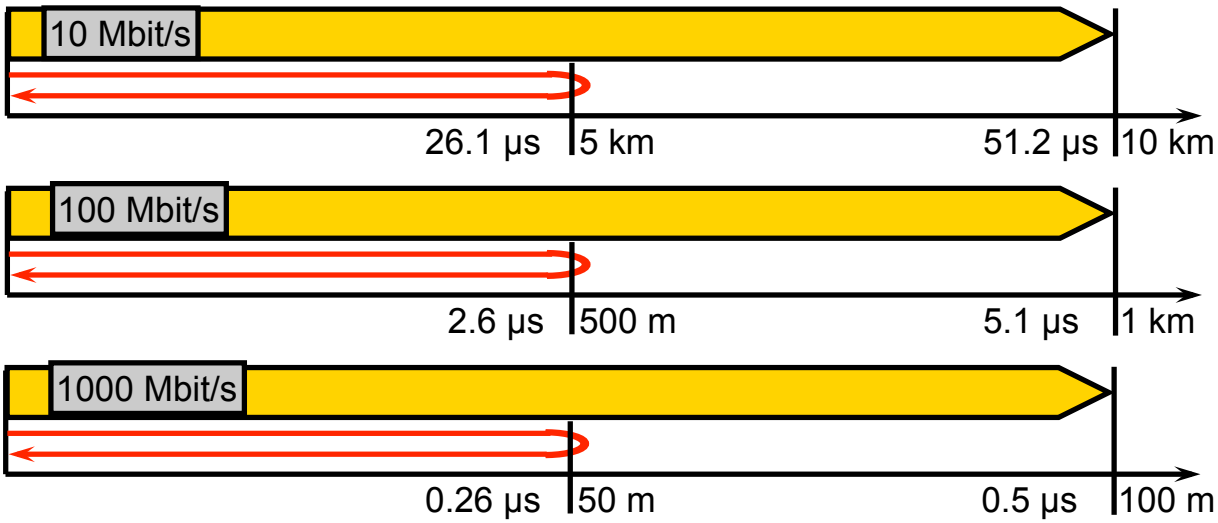
PCS: Physical Coding Sublayer
PMA: Physical Medium Attachment
PMD: Physical Medium Dependent

Medium und Übertragungsdistanz



Gigabit Ethernet und CSMA/CD

Roundtrip Delay und Übertragungsdistanz



Bedingungen:

- Rahmengröße = 64 bytes = 512 bits
- Signal-Ausbreitungsgeschwindigkeit = 200 000 km/s

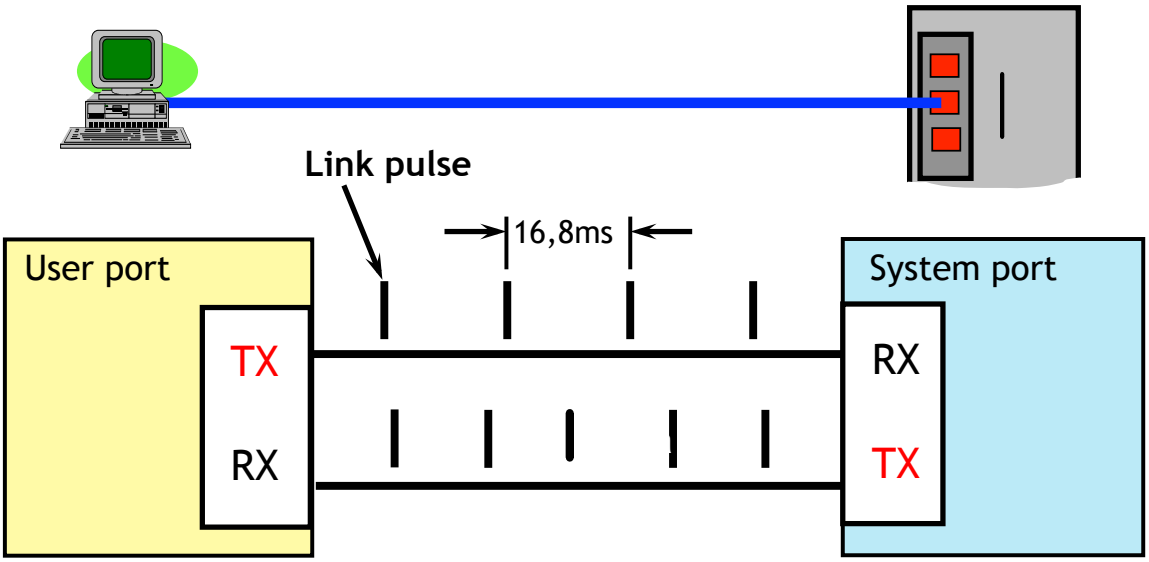
Auto-Negotiation

- Auto-Negotiation heißt die Prozedur, die zur Bestimmung einer gemeinsamen Übertragungsart (Mode) verwendet wird
- Modes: 10BASE, 100BASE (FE), 1000BASE (GE)
- Am Ende der Prozedur wird mit der Betriebsart auch die maximale Übertragungs-Datenrate festgelegt

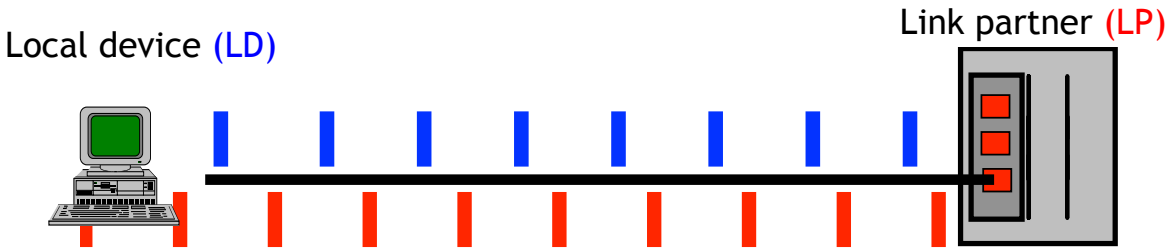
Basisfunktionen

- Falls nur ein Port Auto-Negotiation unterstützt (nicht üblich):
  - Verwendung von 10BaseT Mode.
- Beide Ports unterstützen Auto-Negotiation.
  - Verhandlung der Betriebsart (Geschwindigkeit)

Synchronisation: Link Pulse



Auto-Negotiation : Link Handshake

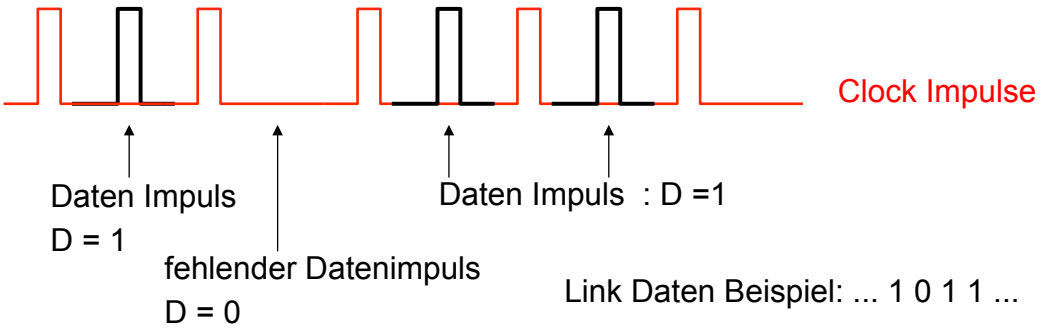


1. LCW kontinuierlich senden (LD) mit Ack=0
   (Info to LP: I do not yet know about you.)
2. Empfang 3 aufeinander folgender, gleicher LCWs (LP) mit Ack=x
   (LD now recognizes the LCW of LP.)
3. LCW (LD) mit Ack=1 senden
   (Info to LP: I received your LCW.)
4. Empfang 3 aufeinander folgender, gleicher LCWs (LP) mit Ack=1
   (Info from LP to LD: I received your LCW.)
5. Senden weiterer 6-8 LCWs (LD) mit Ack=1
   (To be certain that the handshake is complete.)

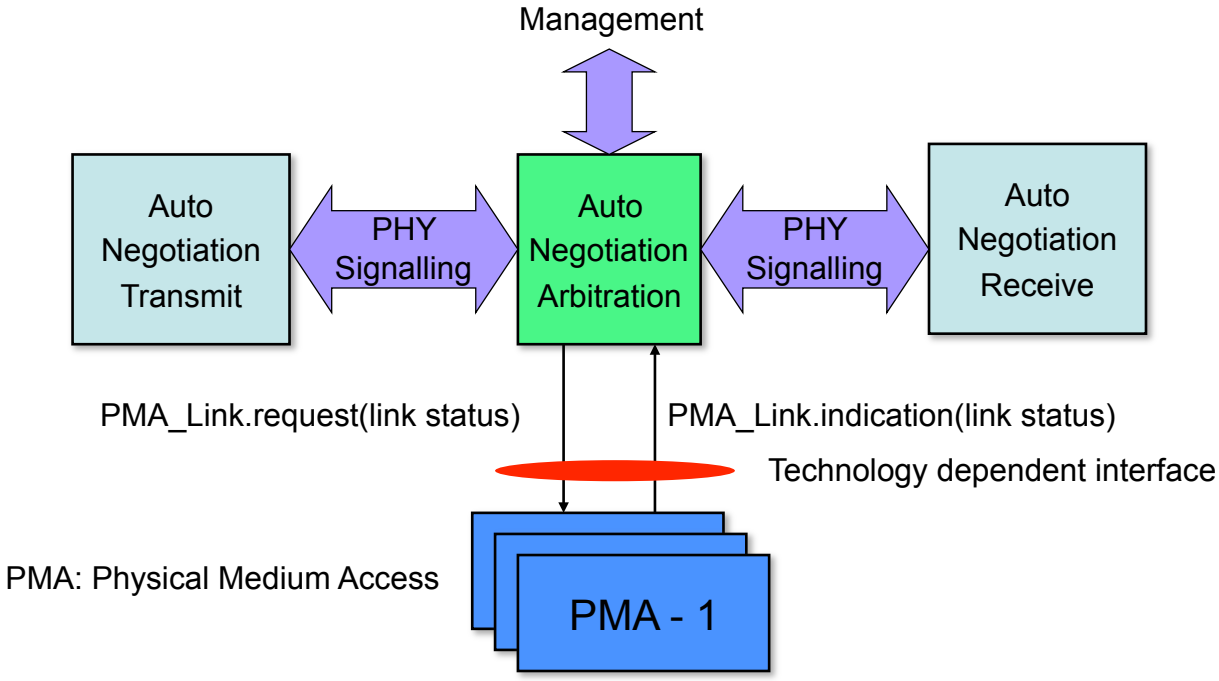
LCW: Link Control Word

Auto Negotiation : Signalisierung

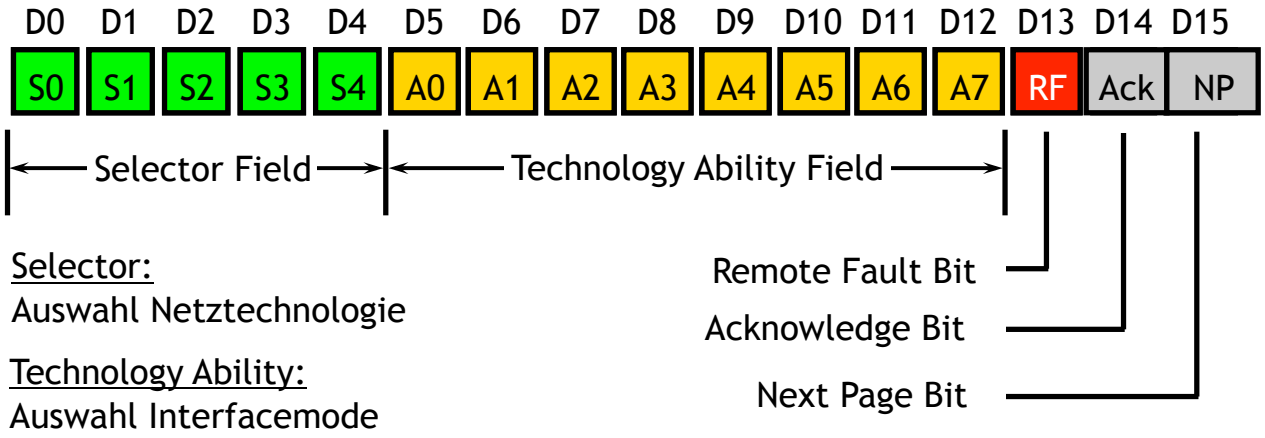
- PHY-Layer Primitive: PMA_Link.Request
  Funktion: Link Control, Auto-negotiation.
- Der Link Control Parameter kann die Werte: SCAN_FOR_CARRIER, DISABLE, oder ENABLE einnehmen
- Der Fast Link Pulse (FLP) Burst besteht aus einer Gruppe 17 – 33 10BASE-T kömpatiblen Link Integrity Test Pulsen.
- Jeder FLP Burst kodiert 16 Datenbits mittels alternierender Takt- und Daten-Impulsfolge.



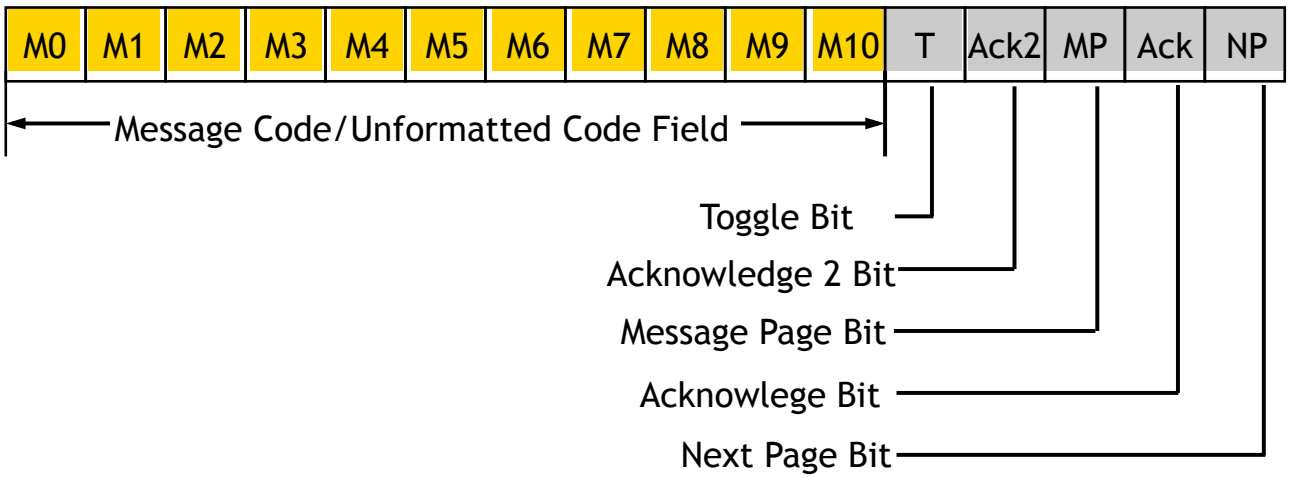
Arbitration Funktion



Base Link Codeword Format



Next Page Link Codeword Format



Kursinhalt

- Ethernet Übersicht und Protokolle
- Ethernet Schicht-1
- Ethernet Link Schicht
- Medium Access Control
- Logical Link Control – LLC
- Ergänzende LAN Protokolle

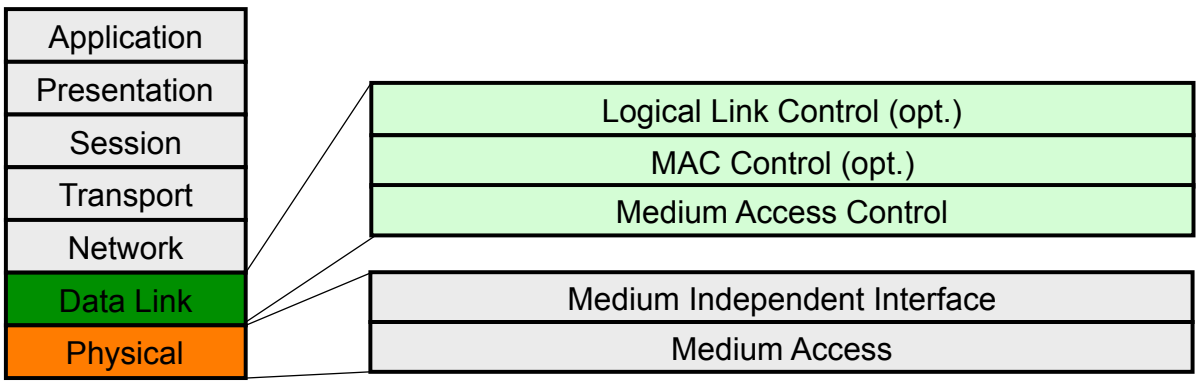
Ethernet Protokollschichten

Schicht-1 Funktionen

- Medium Access — **Medium Independent Interface**
  Medium Interface

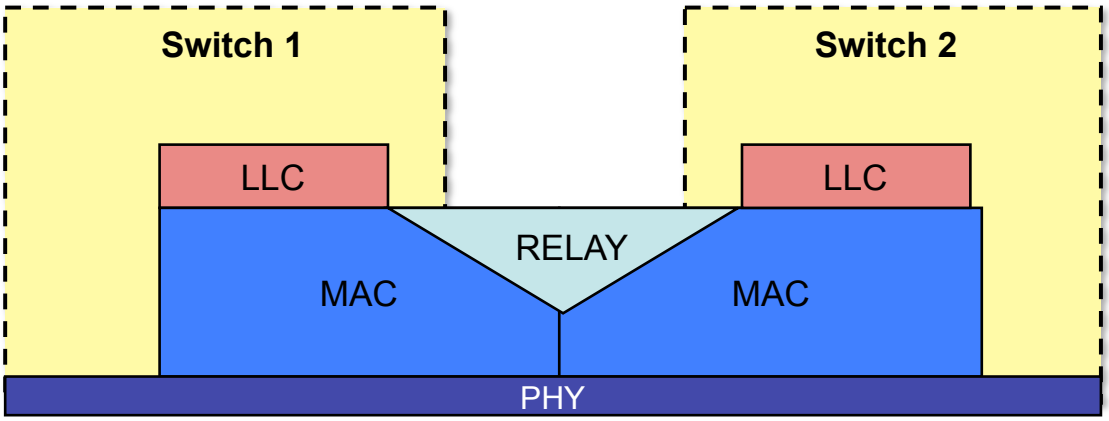
Schicht-2 Funktionen

- Zugang zum Übertragungsmedium — **Mediaum Access Control**
- Protokollsteuerung — **MAC Control**
- Link Verbindungssteuerung — **Logical Link Control**

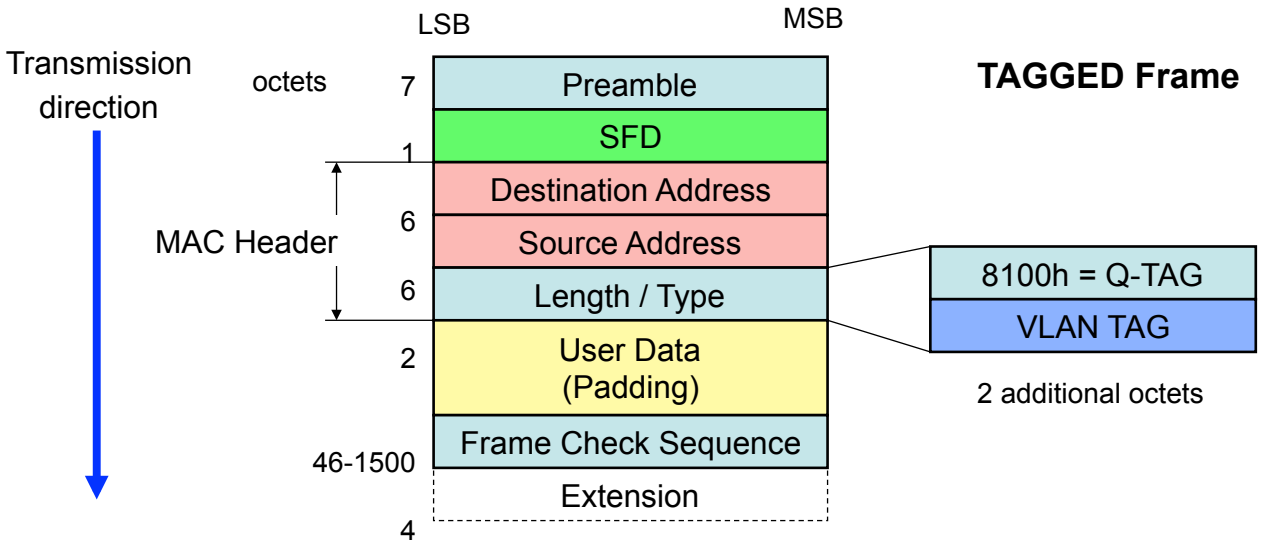


Layer-2 Bridge/Switch

Rahmen übertragen : Eingangsport -> Ausgangsport
Fehlerhafte Rahmen beseitigen
Rahmen zwischenspeichern und filtern
Durchführung von Management Funktionen
Durchführung von Quality of Service (priority, traffic class) Aufgaben



MAC Rahmen



SFD: Start Frame Delimitter

Aufgabe

- Aktivieren Sie Ihren Raspberry PI
- Laden Sie die GUI
- Verbinden Sie sich mit dem lokalen Kurs-WLAN
- Laden Sie das Trace-Programm Wireshark
  im shell-Fenster: sudo wireshark
- Aktivieren Sie einen Wireshark trace auf der WLAN0 – Schnittstelle
- Analysieren Sie die Ethernet Schicht

MAC Addressen Format

Beispiele:

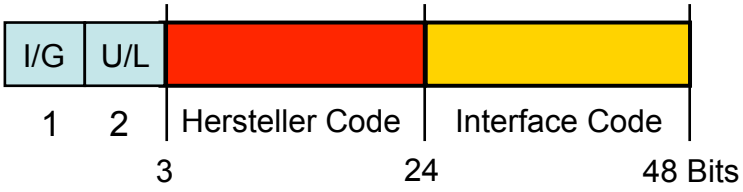
Unicast: 00-01-68-50-23-45

Broadcast: FF-FF-FF-FF-FF-FF

Multicast: **01**-**80**-C2-00-00-00

Multicast

Bridge Management

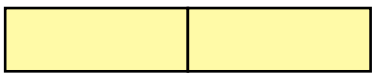


I/G: 0 = Individuelle Addresse;
1 = Gruppenaddresse (Broadcast = FFh)

U/L: 0 = Globale Addresse;
1 = Lokale Addresse

Type / Length Field:

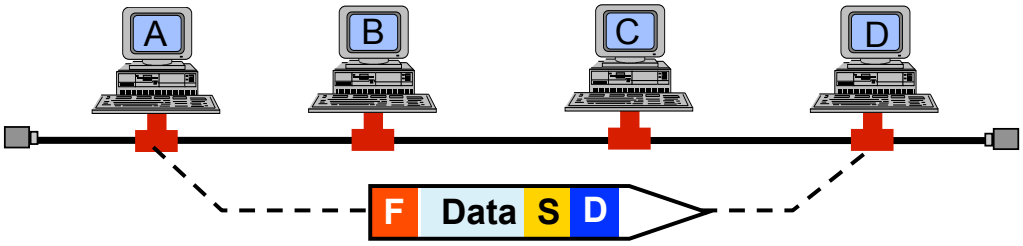
2 Octets



Beispiele: 0800 (2048): IP
0806 (2054): ARP

Falls Paket > = 1536 (0600h) TYPE - Interpretation : Protokoll - ID

MAC Adressierungsmethode



Nachricht (höhere Schichten): Data

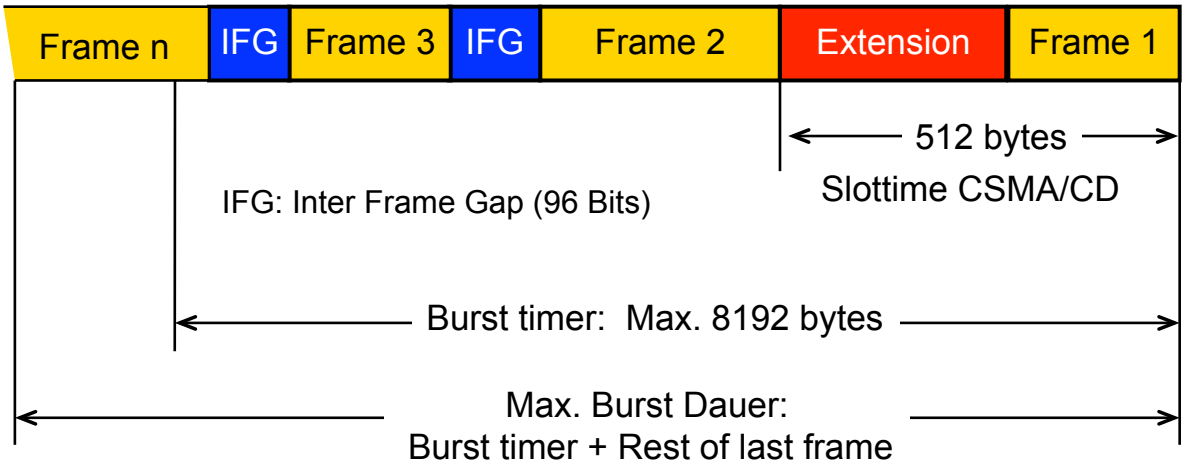
+ Dest. address D

+ Source address S

+ Error checking F

= Frame (packet) F Data S D

Frame Bursting

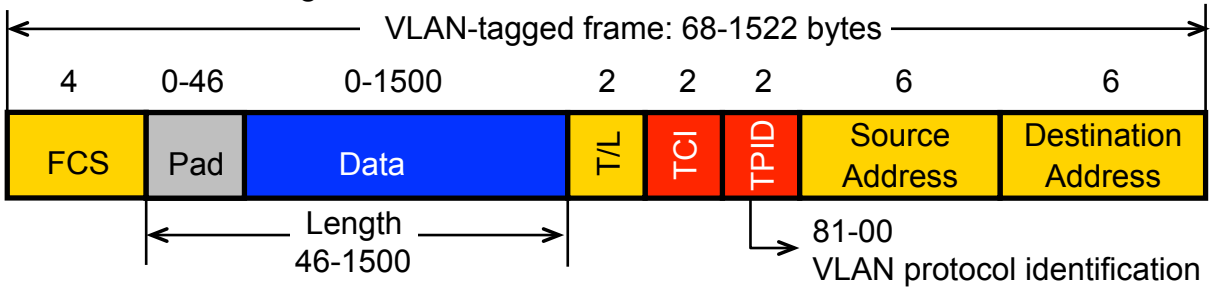


Kursinhalt

- Ethernet Übersicht und Protokolle
- Ethernet Schicht-1
- Ethernet Link Schicht
- Medium Access Control
- Logical Link Control – LLC
- Ergänzende LAN Protokolle

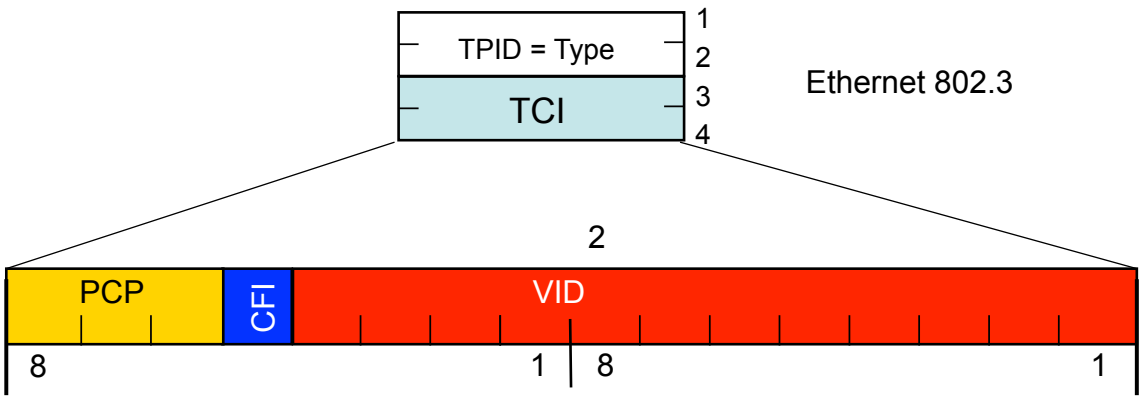
Virtual Local Area Network (VLAN)

- VLANs gruppieren Ethernet Hosts zu einem gemeinsamen LAN
- VLANs ermöglichen die Trennung der Ethernet Dienste
- Durch VLANs werden logische und physikalische Strukturen getrennt
- VLAN forwarding ermöglicht die Implementierung von Ethernet-basierten QoS Diensten
- Der Ethernet Header besitzt zusätzlich 2 Bytes für die VLAN Adressierung



TPID : TAG Protocol Identifier TCI: TAG Control Information

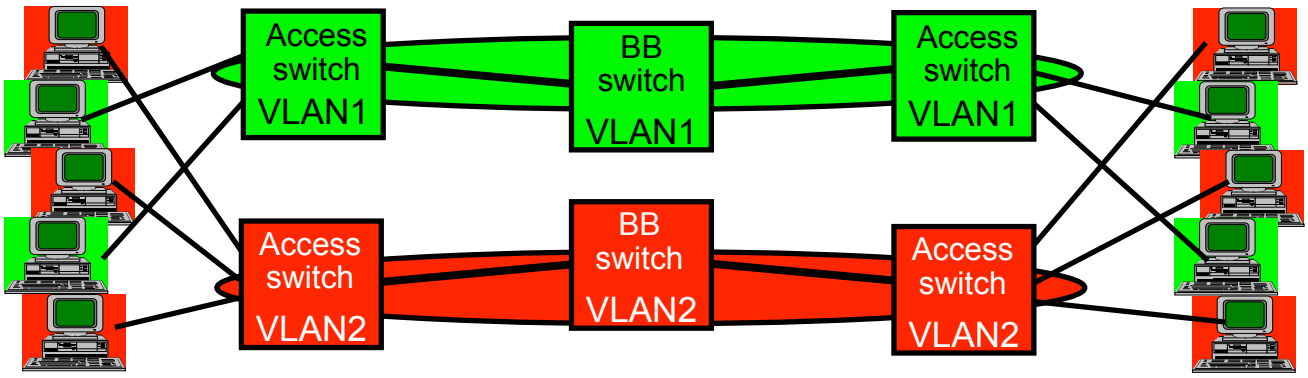
VLAN Tag Control Information (TCI)



CFI: Canonical format identifier
VID: VLAN identifier
TPID: TAG protocol ID
PCP: Priority Code Point
TCI: TAG control information

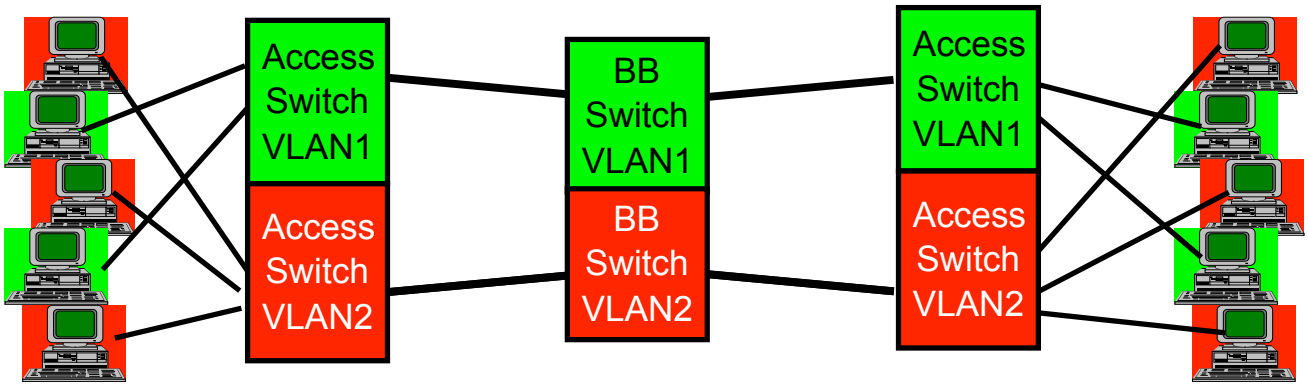
Virtual LAN Prinzipien (1)

- Virtual LAN Standard: IEEE 802.1Q
- VLAN Definition auf Port-Ebene
- Jedes VLAN kann als unabhängiges LAN betrachtet werden

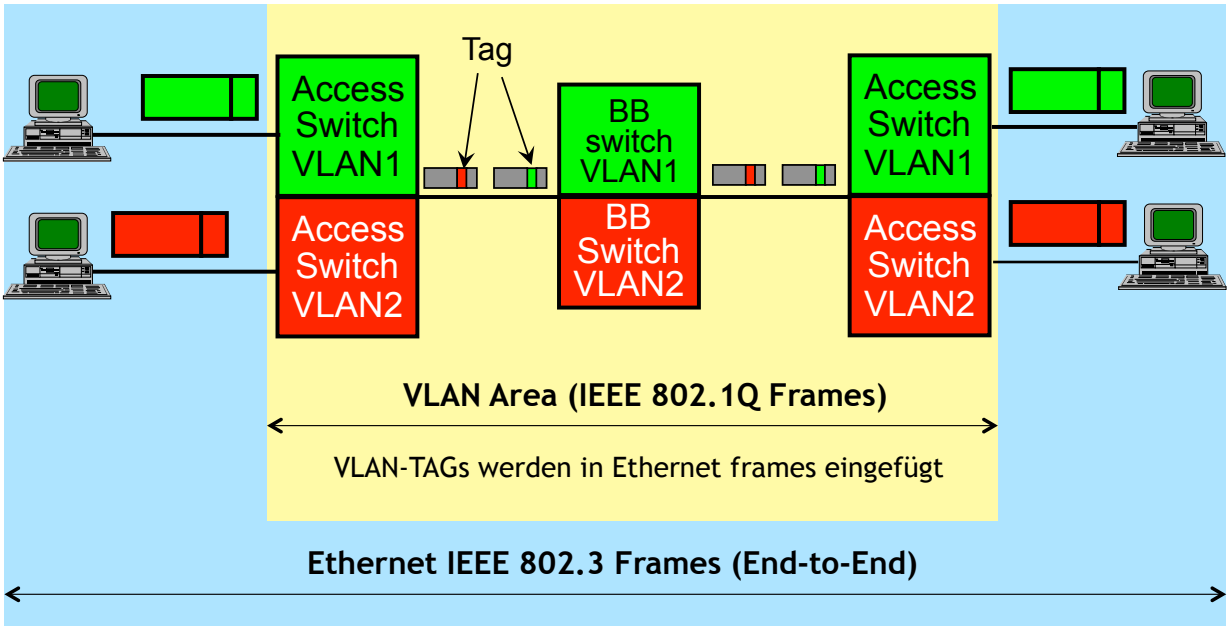


Virtual LAN Principles (2)

- Eine Netz-Infrastruktur für beide LANs



Virtual LAN Principles (3)



Ethernet Frame with VLAN Tag

```
IEEE 802.3/Ethernet DIX V2 Header
Frame Length : 68
Destination Address :  00-80-16-00-80-C0,
Source Address :               00-80-16-00-00-00,
802.1q Tag Type ID :   0x8100
Frame Checksum :               Good,
Frame Check Sequence :         01 4B 34 07
IEEE 802.1q - Virtual Bridged LAN
Tag Control Information :      0x2800
1.... .... .... =              Priority = 1
...0 .... .... .... =  RIF Field is Not Present
.... 1000 0000 0000 =  VLAN ID = 2048
Frame Format :                 Ethernet DIX V2
Ethertype :                    0x800 (IP)
IP - Internet Protocol
    Version :          4,
    Header length :            20
    Type of Service :  0x00
```


VLAN Arten (1)

Schicht-1 VLAN:

- LAN Switch Port abhängig
- unabhängig vom Schicht-2 Protokoll

Schicht-2 VLAN:

- Abhängig von der MAC-Addresse
- unabhängig vom Schicht-3 Protokoll

Schicht-3 VLAN:

- Abhängig von der IP-Adresse
- Definiert ein logisches Subnetz

Anwendungsschicht VLAN:

- Anwendungs-spezifisch z.B.VoIP

VLAN Arten (2)

Port-VLAN

Port	VLAN
1	1
2	1
3	2
4	1

Schicht-2 VLAN

MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

Protokoll-VLAN

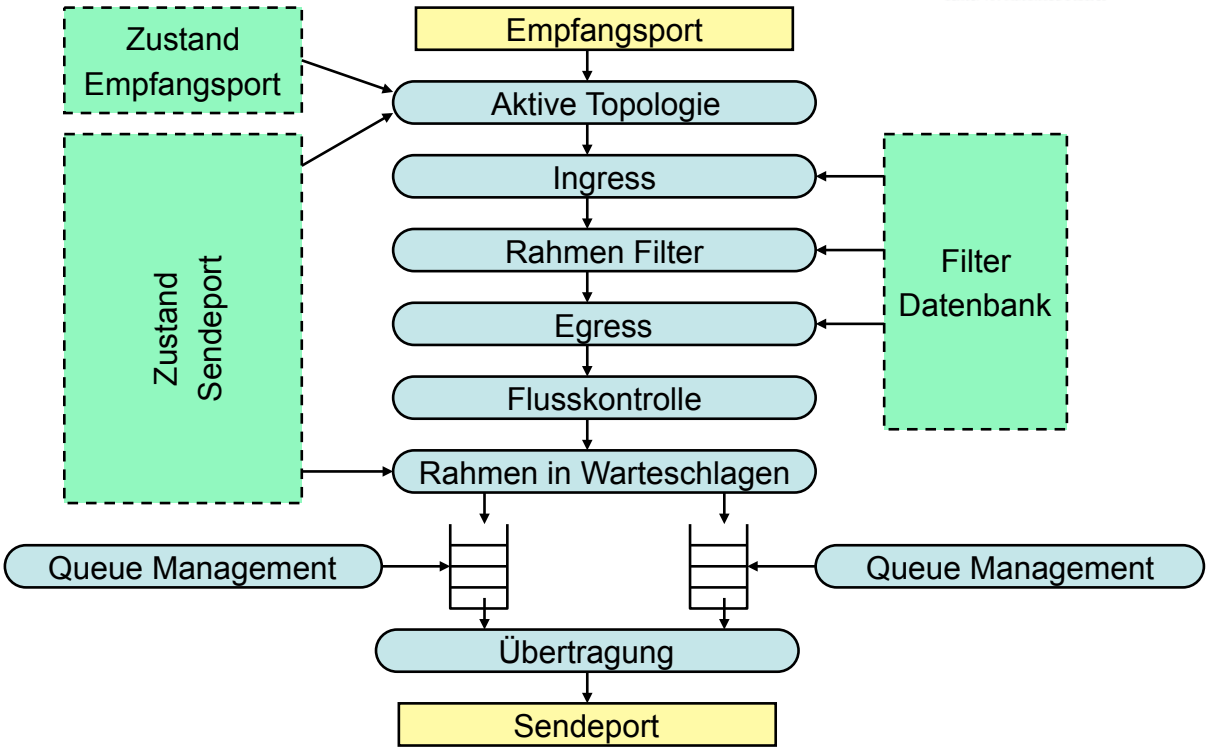
Protocol	VLAN
IP	1
IPX	2

Schicht-3 VLAN

IP Subnet	VLAN
23.2.24	1
26.21.35	2

802.1Q unterstützt Paketfilter für höhere Protokollschichten
unterschiedliche Anwendungen können dadurch
mit spezifischen QoS – Anforderungen transportiert werden

Forwarding Prozess



Traffic Priorisierung (IEEE 802.1D/p)

IEEE 802.1D/p

- Spezifiziert die dienstabhängige Verteilung und Priorisierung der LAN-Bandbreite
- 8 Prioritäts-Levels (0 – 7)
- Priorität wird durch die p-Bits im VLAN-Tag spezifiziert
- Möglichkeiten für das Management von :
  - Latenzzeit
  - Durchsatz

Prioritätsklassen

Network Control:
garantierte Zustellung der Rahmen mit höchster Priorität

Internetwork Control:
getrennte administrative Domains in großen Netzen

Sprache:
Verzögerung ≤ 10 ms, max Jitter nur durch die LAN Infrastruktur vorgegeben

Video:
Verzögerung ≤ 100 ms als primäre QoS Anforderung.

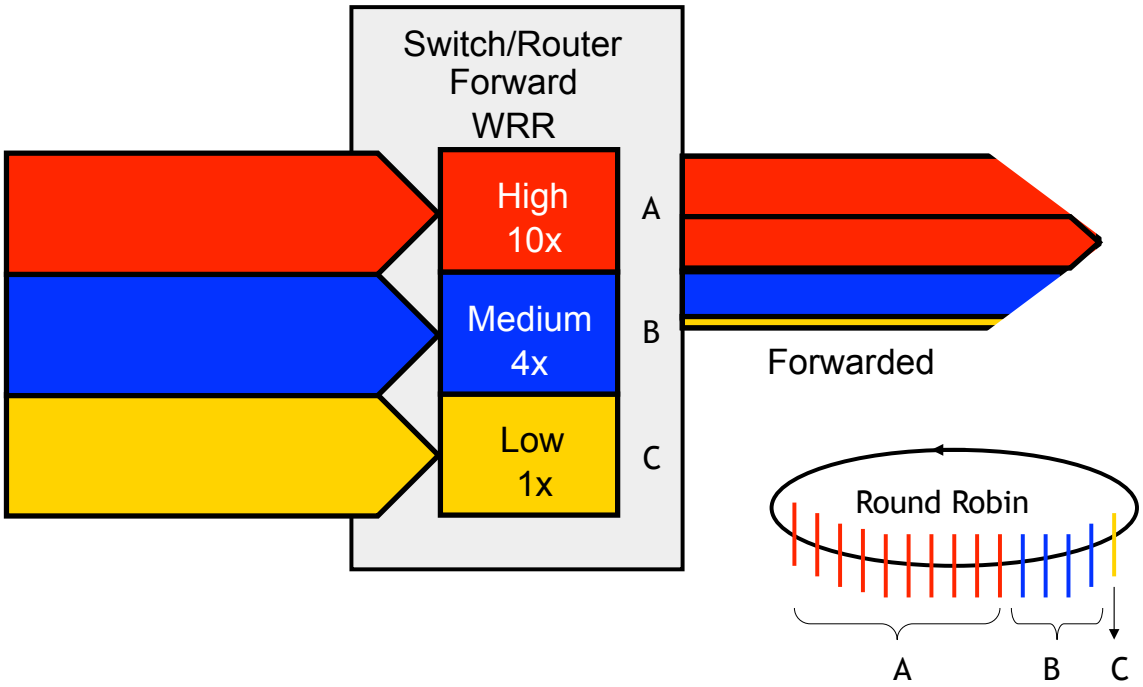
Kritische Anwendung:
garantierte min. Datenrate als primäre QoS Anforderung

Excellent Effort:
best-effort Service-Typ für Prime-users.

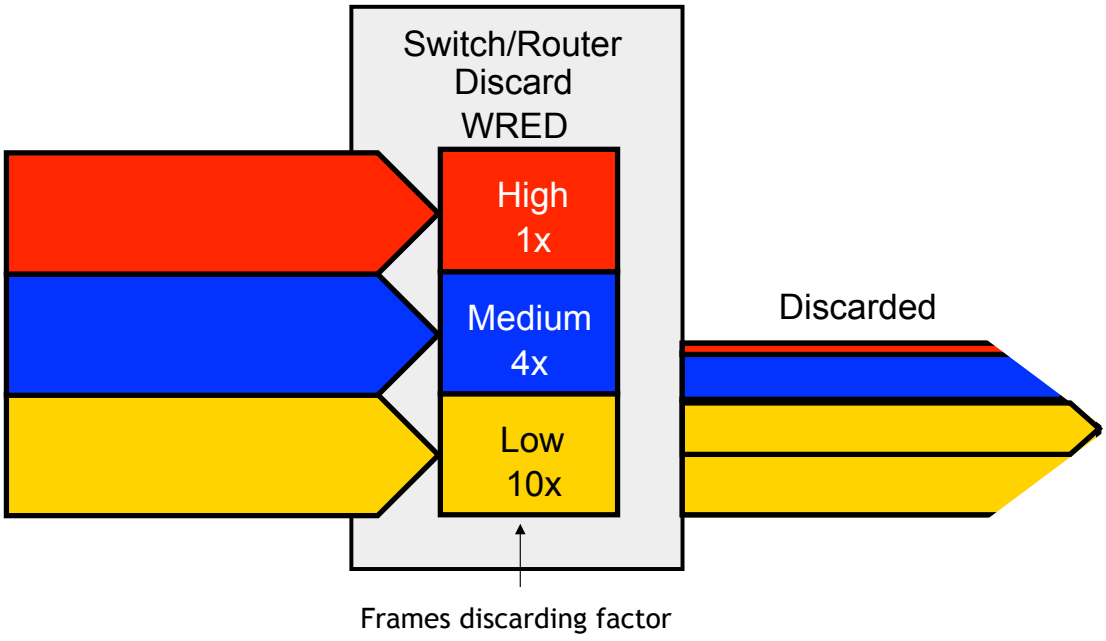
Best Effort:
Standard Verkehrsart für unpriorisierte Anwendungen

Background:
für Massendaten-Anwendungen ohne Auswirkungen auf die Netzgüte

Priorisierung: Weighted Round Robin (WRR)

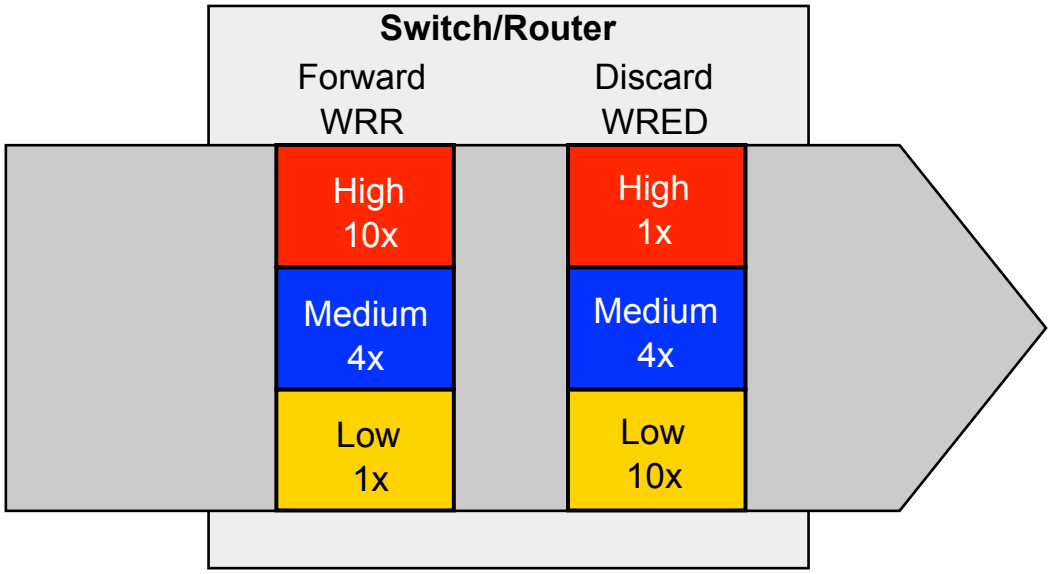


Weighted Random Early Discard



Scheduling Methoden: WRR und WED

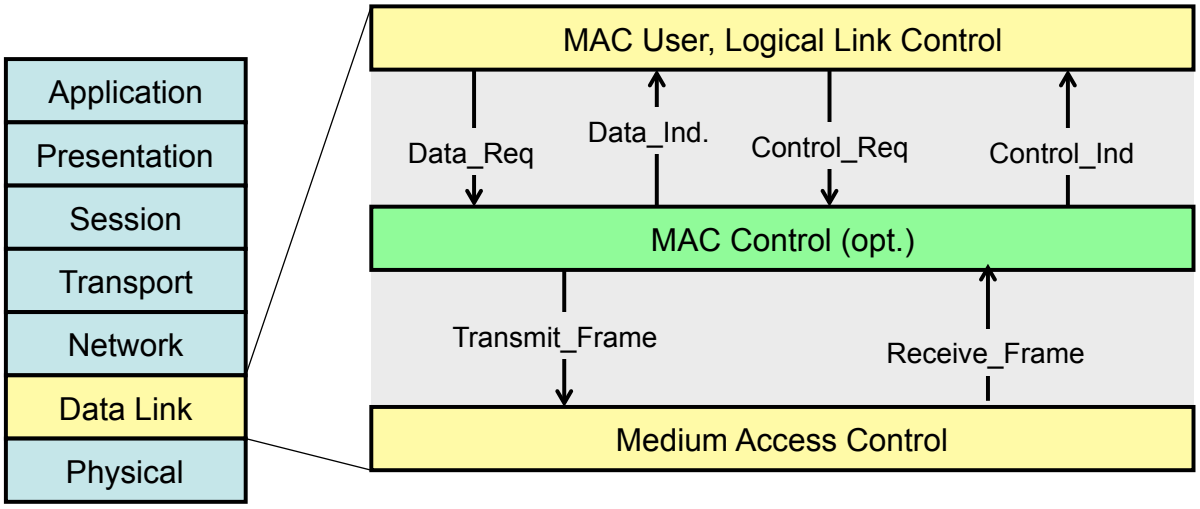
WRR: Weighted Round Robin
WED: Weighted Early Discard



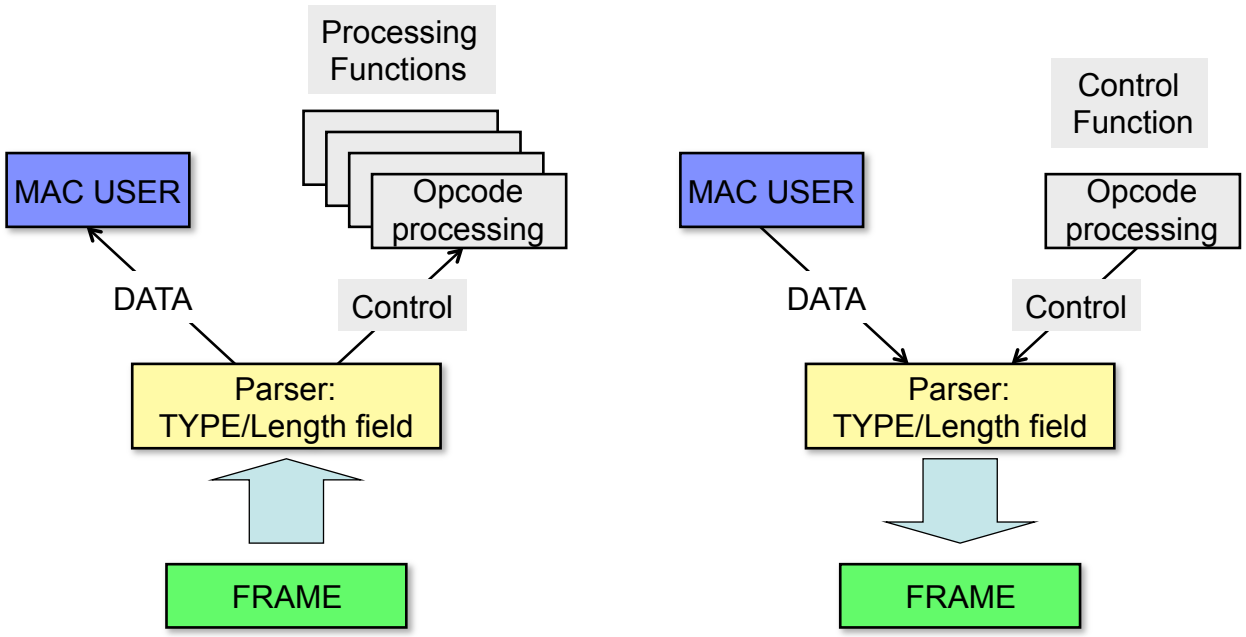
Kursinhalt

- Ethernet Übersicht und Protokolle
- Ethernet Schicht-1
- Ethernet Link Schicht
- Medium Access Control
- Logical Link Control – LLC
- Ergänzende LAN Protokolle

MAC Management Sublayer



Datentransport



MAC Operation

Data Encapsulation (Senden und Empfangen)

- Rahmenbildung
  frame boundary delimitation, frame synchronization
- Adressierung
  source address und destination address
- Fehler Erkennung
  Physical Medium Transmission Errors mittels FCS Berechnung

Media Access Management

- Medium Belegung
  collision avoidance
- Bewerbung um das Medium
  contention resolution, collision handling

Definitionen

Slot Time
Min. Übertragungszeit für einen Rahmen. **Berechnung**: Lmin * Übertragungsrate Lmin = 512. Für 10Mbit/s : Slot time = 512 * 10Mbit/s = 51.2 µs (1000Mbit/s: 0.512 µs)

Interframe Gap
Zeitintervall zwischen aufeinanderfolgenden Rahmen. Das Interframe Gap dauert 96 Bits. Bei 10 Mbit/s beträgt das Interframe Gap 9.6 µs (100Mbit/s: 0.96 µs)

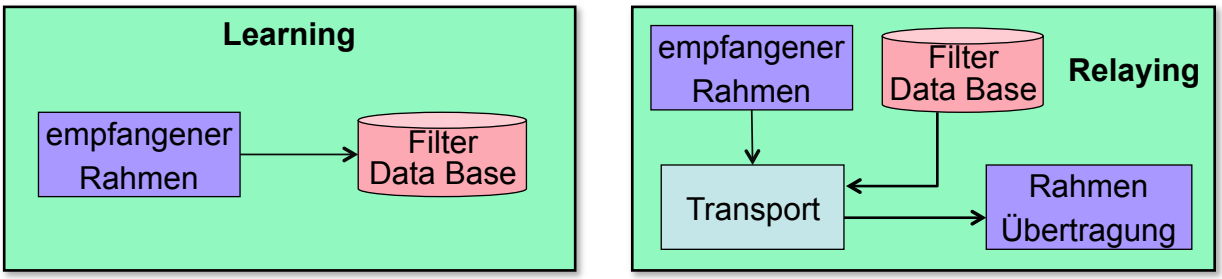
Roundtrip Delay
Beträgt die doppelte Signalverzögerungszeit zweischen Sender und Empfänger. Regel: Roundtrip Delay < Slot Time

Backoff Time
Wartezeit nach einer Kollisieonserkennung. Backoff time = N * Slot Time. N ist eine Zufallszahl zwischen 1 und 1023. Maximalwert: 52377.6 µs.

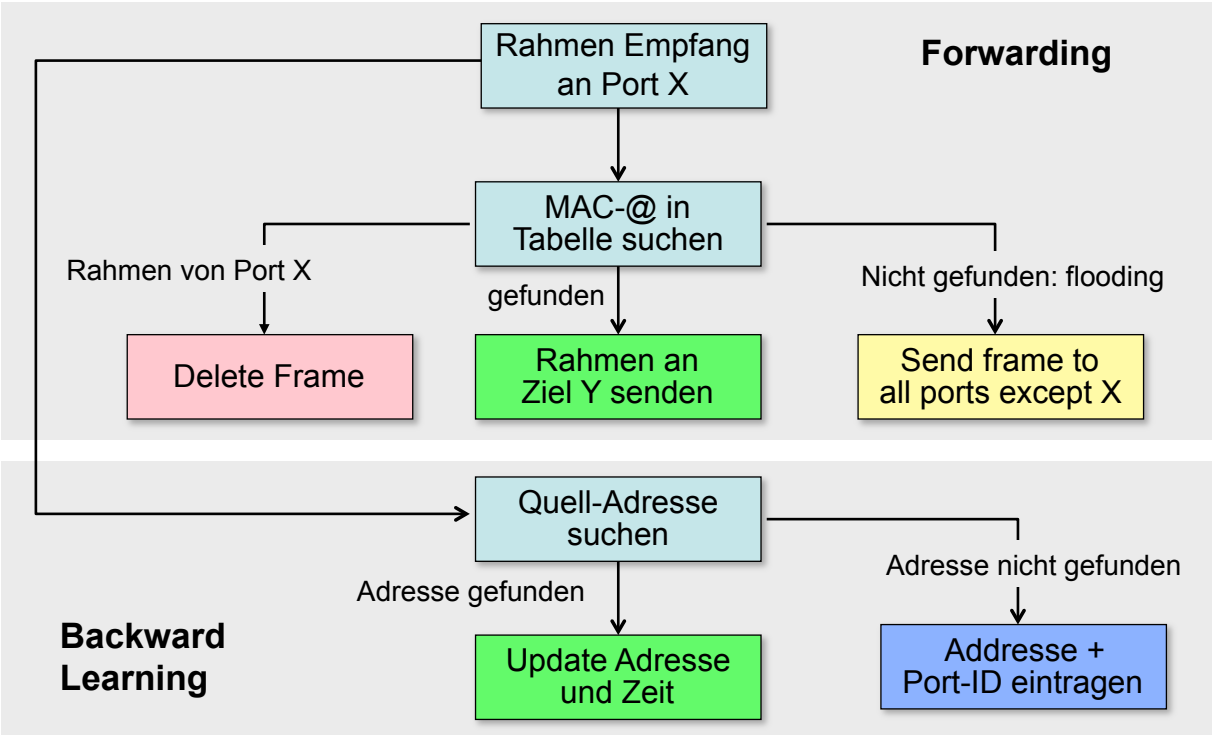
Frame Bursting
Zusammenfassung mehrerer Rahmen zu einem Burst mit einer max. Dauer von 65.536 µs .

Daten Filter

- Daten Filter ermöglichen die Kontrolle über spezielle Quell- und Zieladressen in bestimmten Netzsegmenten.
- Diese Funktion erlaubt den Aufbau von Verwaltungsgrenzen über welche bestimmte MAC-Adressen nicht weitergegeben werden
- Filter-Regeln und Filter-Entscheidungen werden bezüglich der MAC-Adressen durchgeführt

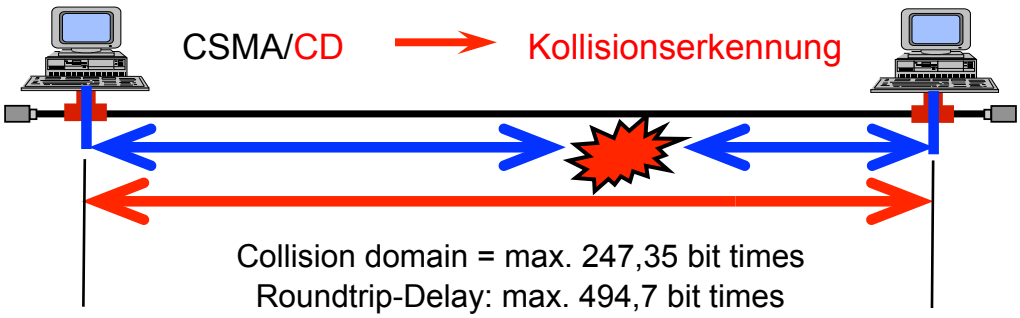


Rahmen Übertragung : Frame Forwarding

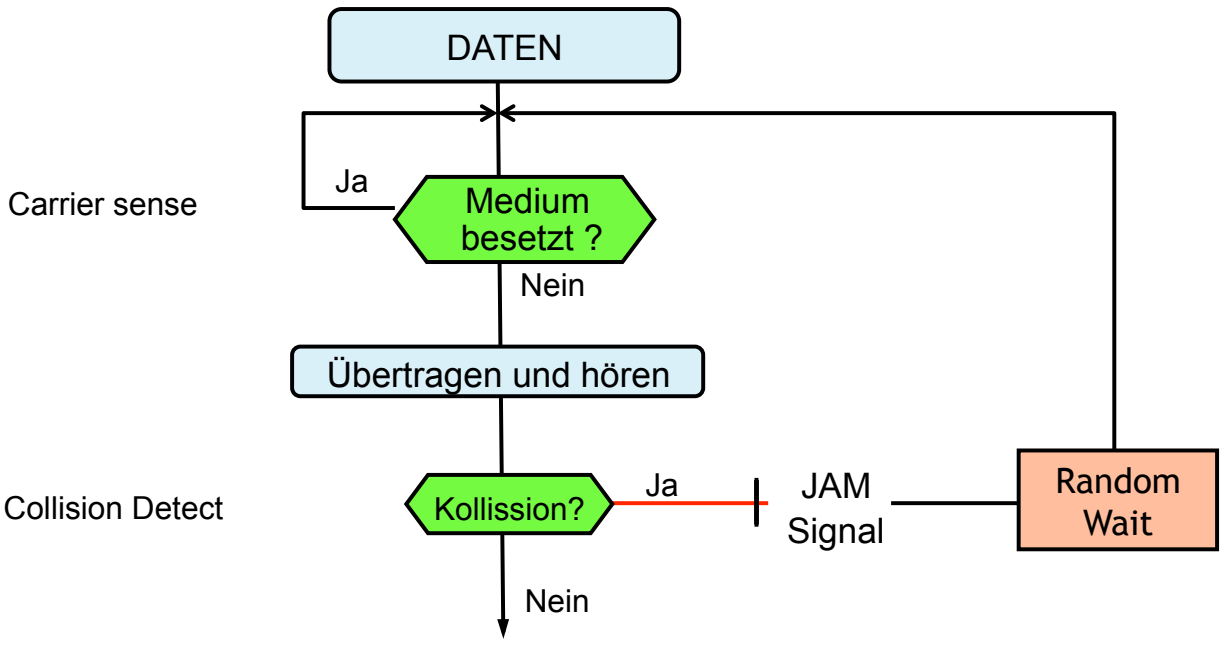


Kollisionen

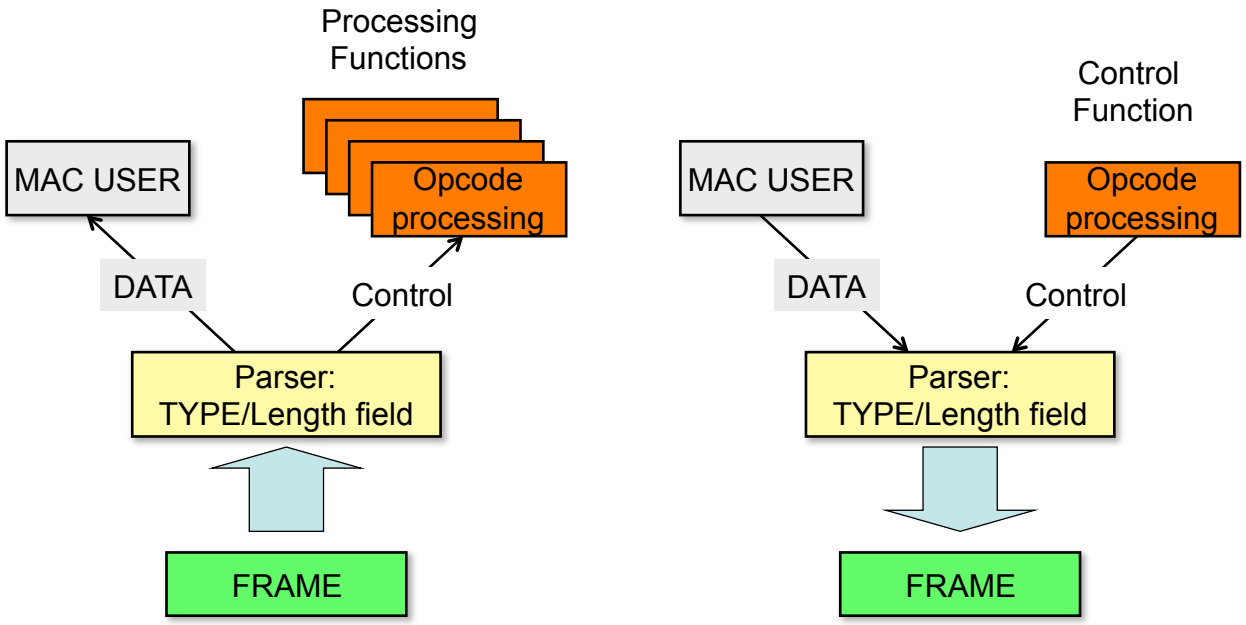
- Moderne Ethernet LANs vermeiden Kollisionen durch Punkt-zu-Punkt Topologie
- Eine Collision Domain ist ein Netzsegment in dem Datenkollisionen auftreten können, wenn zwei Stationen gleichzeitig den Bus belegen.
- Zur Vermeidung von Kollissionen dient CSMA-Zugangsmethode, bei der der the Medium-Zustand überwacht wird.



CSMA/CD Prozedur



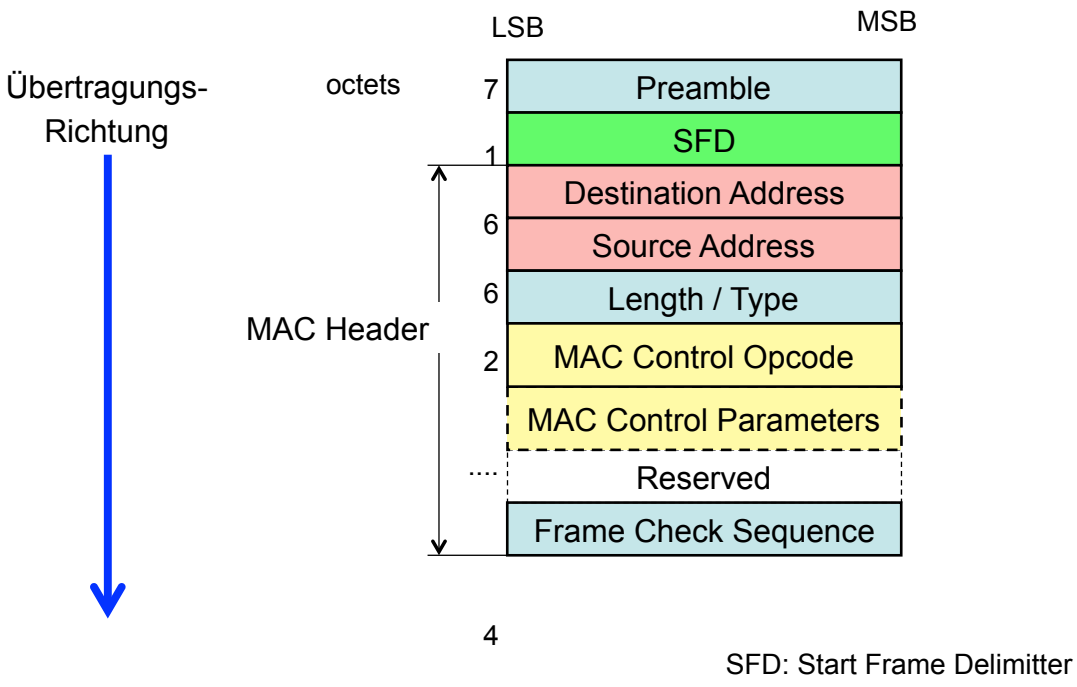
MAC-Schicht : Management Operationen



MAC Control Operations

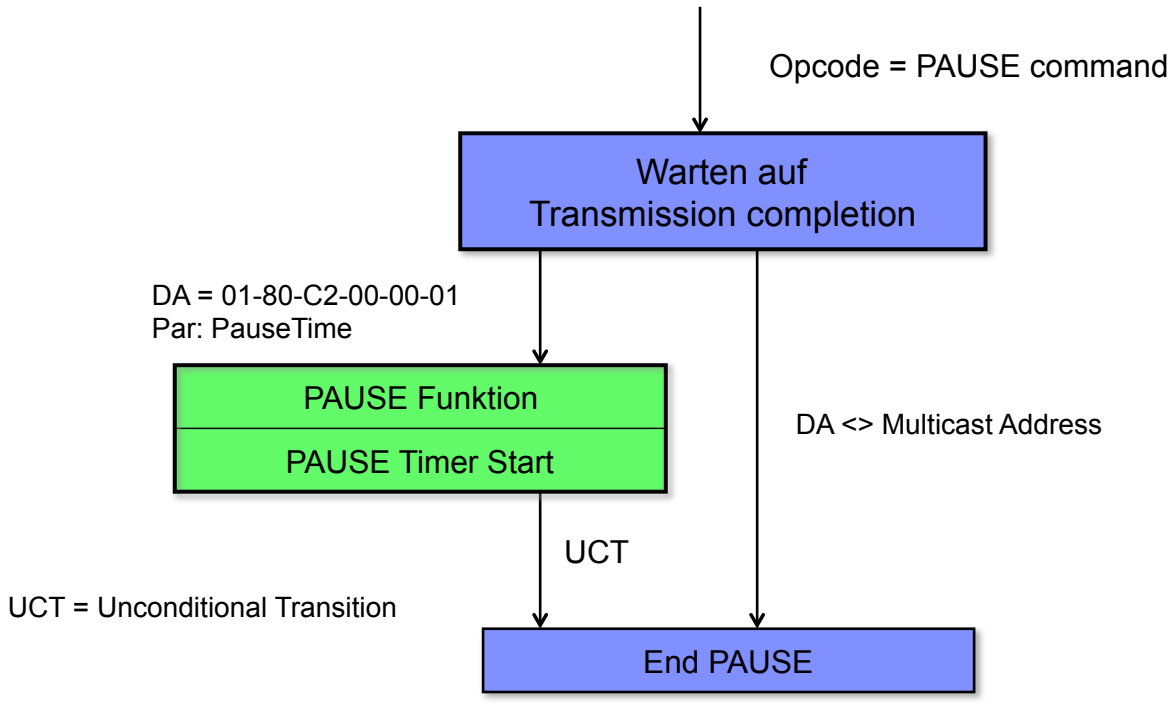
Code	Function Name	Comment
00 00	Reserved	
00 01	PAUSE	Flow Control: stop transmission
00 02	GATE	Flow Control: start transmission
00 03	REPORT	Pending transmission requests
00 04	REGISTER_REQ	Flow Control: registration request
00 05	REGISTER	Flow Control: registration
00 06	REGISTER_ACK	Flow Control: registration acknowledged
00 07-FF FF	Reserved	

MAC Control Frame

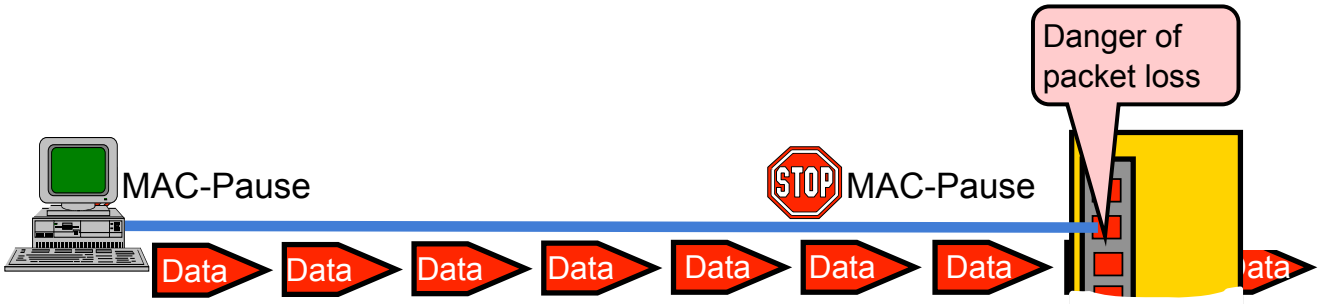


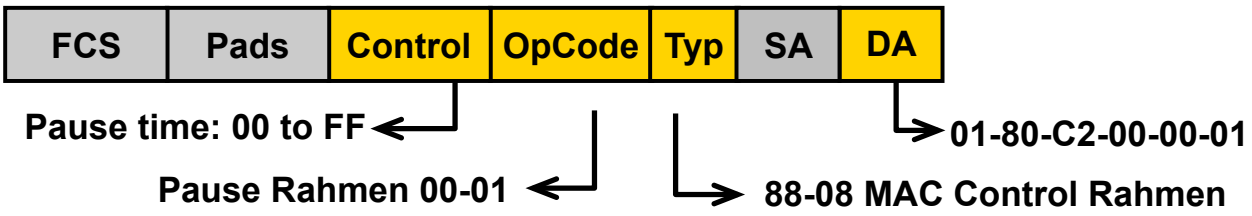
SFD: Start Frame Delimitter

PAUSE Operation



Full Duplex Flusskontrolle

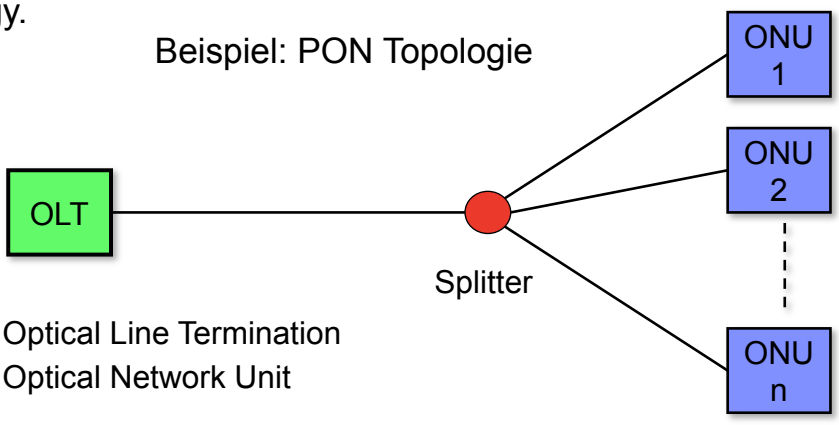




Multipoint MAC Control

- Multipoint MAC Control deals with mechanism and control protocols required in order to reconcile the P2MP topology into the Ethernet framework.
- When combined with the Ethernet protocol, such a network is referred to as Ethernet passive optical network (EPON).
- P2MP is an asymmetrical medium based on a tree (or tree-and-branch) topology.

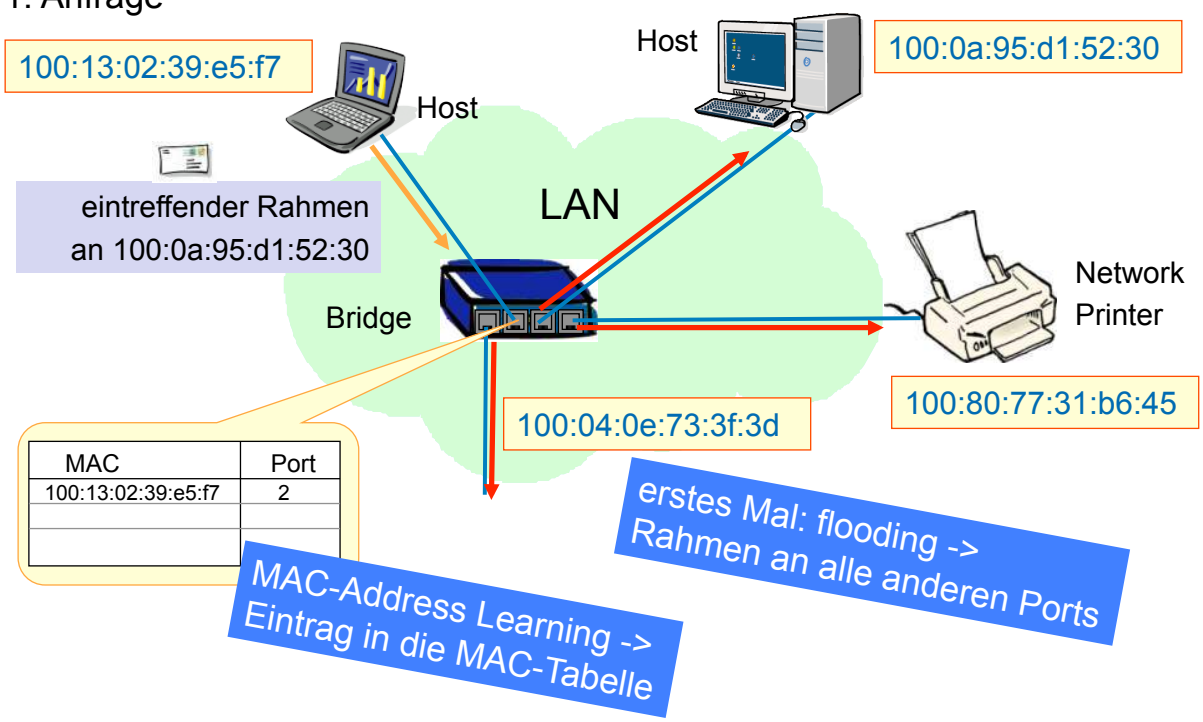
Beispiel: PON Topologie



OLT: Optical Line Termination
ONU: Optical Network Unit

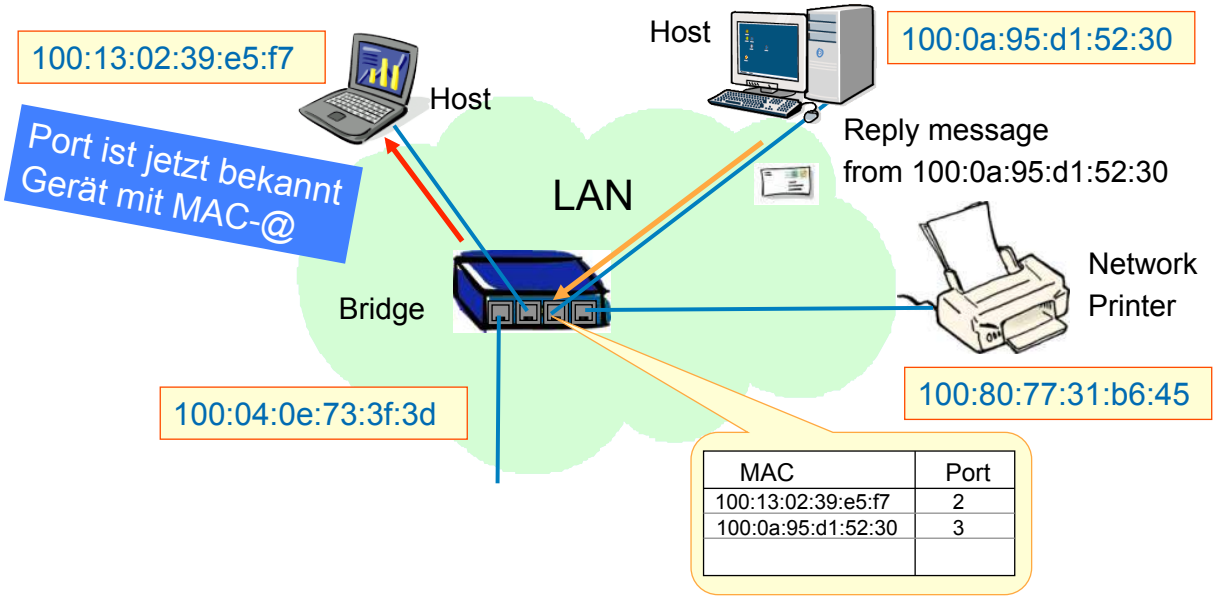
MAC-Prozedur: Paketweiterleitung (1)

1. Anfrage



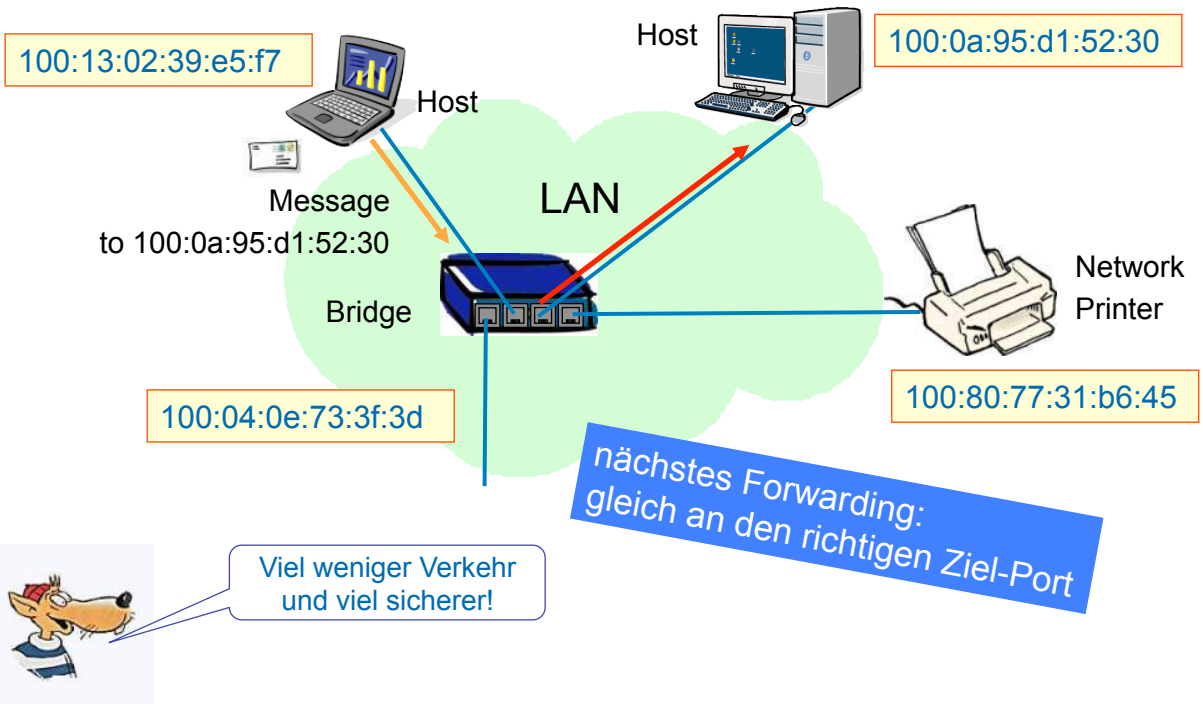
MAC-Prozedur: Paketweiterleitung (2)

2. Antwort



MAC-Prozedur: Paketweiterleitung (3)

3. nachfolgende Pakete

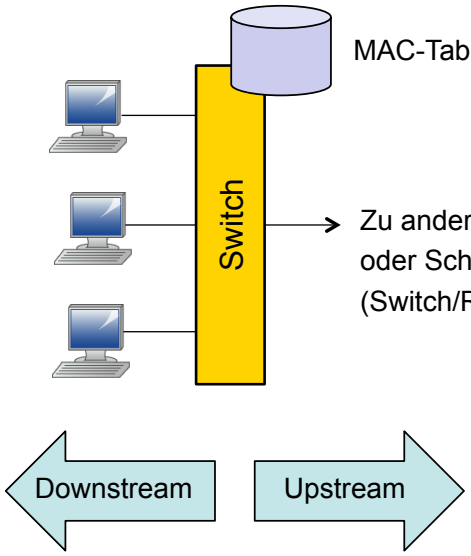


Viel weniger Verkehr
und viel sicherer!

Zusammenfassung

Schicht-2 Netzelement : Switch

- Die **MAC-Tabelle** enthält die Schicht-2 Adressen (MAC-Adressen) der angeschlossenen Geräte und deren Port-Nummer.
- **Paketzustellung**
  Packet Forwarding durch die Switch Software mit dieser Tabelle.
- Lebensdauer der MAC-Tabellen-Einträge ca. 300 sek.
- Eintrag wird gelöscht, wenn kein Paket übertragen wird.



Kursinhalt

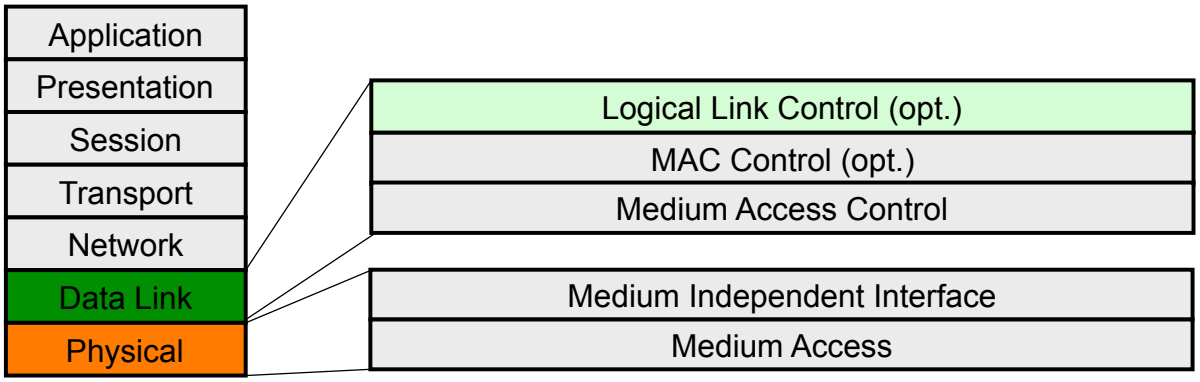
- Ethernet Übersicht und Protokolle
- Ethernet Schicht-1
- Ethernet Link Schicht
- Medium Access Control
- Logical Link Control – LLC
- Ergänzende LAN Protokolle

Ethernet Protokollschichten

Schicht-2 Funktion

- Link Verbindungssteuerung **Logical Link Control**

LLC bildet die Schnittstelle zur Netz-Schicht (Schicht-3) wie z.B. das Internet Protokoll (IP)



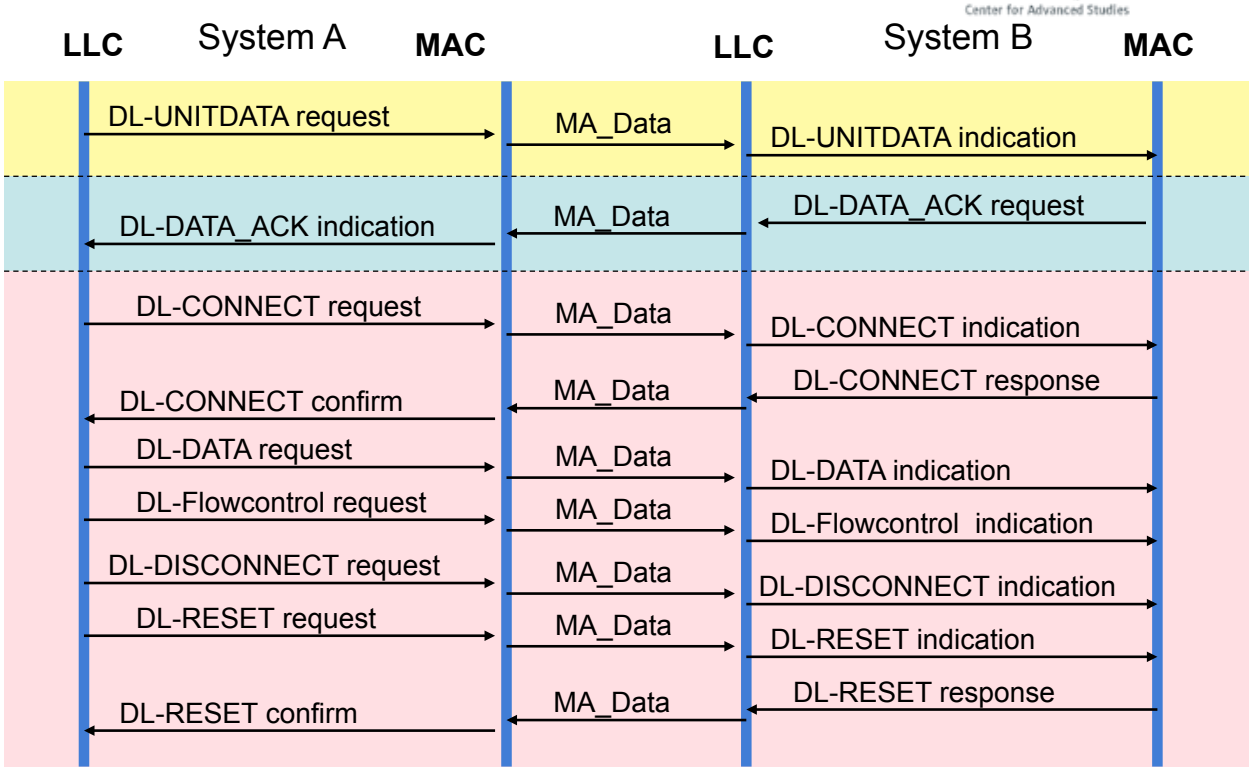
LLC Dienste

- Logical Link Control stellt der übergeordneten Schicht Dienste zur Verfügung, die durch **Service Access Point Addresses** (SAP) aktiviert werden.
- Ein SAP adressiert Prozeduren für spezifische Dienste der Protokollschicht
- SAPs werden z.B. für Signalisierung, Management und Datentransfer verwendet.
- LLC Dienste werden durch **LLC Dienstprimitive aktiviert**

LLC Service-Arten:

Verbindungslos - unquittiert	Type-1 Operationen
Verbindungsoritentiert	Type-2 Operationen
Verbindungslos - quittiert	Type-3 Operationen

LLC Nachrichtenablauf



LLC Nachrichten

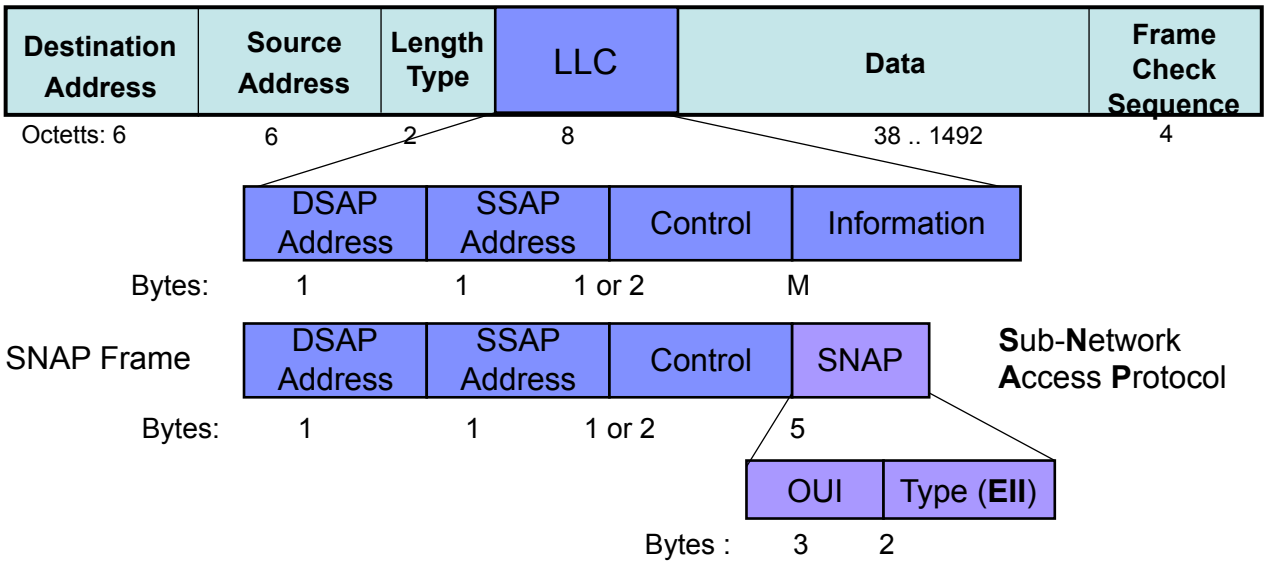
Symbol	Name	C/R
I	Information	C/R
RR	Receive Ready	C/R
RNR	Receive not Ready	C/R
REJ	Reject	C/R
FRMR	Frame Reject	R
UI	Unnumbered Information	C
UA	Unnumbered Ack	R
DISC	Disconnect	C
DM	Disconnect Mode	R
SABME	Set Asynchronous Balaced Mode extended	C

HDLC Messages

Symbol	Name	C/R
XID	Exchange Identification	C/R
TEST	Test message	C/R
AC0	Acknowledged CL Information Seq. 0	C/R
AC1	Acknowledged CL Information Seq. 1	C/R

non-HDLC Messages

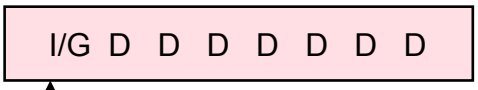
LLC Rahmenformat



DSAP: Destination Service Access Point Address
SSAP: Source Service Access Point Address
Control: Command/Response function (16 bit format includes numbering)
Information: Protocol Parameter field

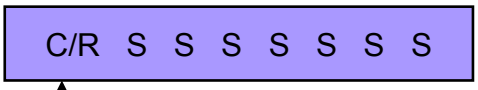
LLC Adresse und Control Format

DSAP



I/G = 0: individual DSAP
I/G = 1: Group DSAP

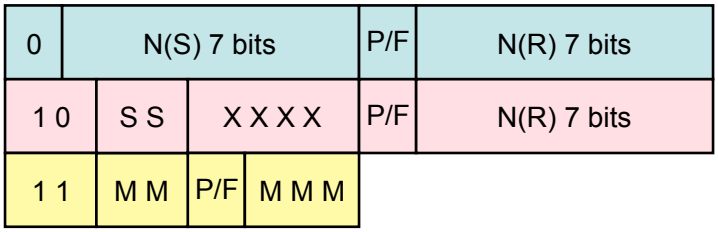
SSAP



C/R = 0: Command
C/R = 1: Response

Example:
DSAP = 1 1 1 1 1 1 1 1 (FFh) : Global DSAP Address

Control fileld formats:



Kursinhalt

- Ethernet Übersicht und Protokolle
- Ethernet Schicht-1
- Ethernet Link Schicht
- Medium Access Control
- Logical Link Control – LLC
- Ergänzende LAN Protokolle
  - Spanning Tree Protocol – STP , RSTP
  - Link Aggregation Control Protocol - LACP

Spanning Tree Protocol – STP und RSTP

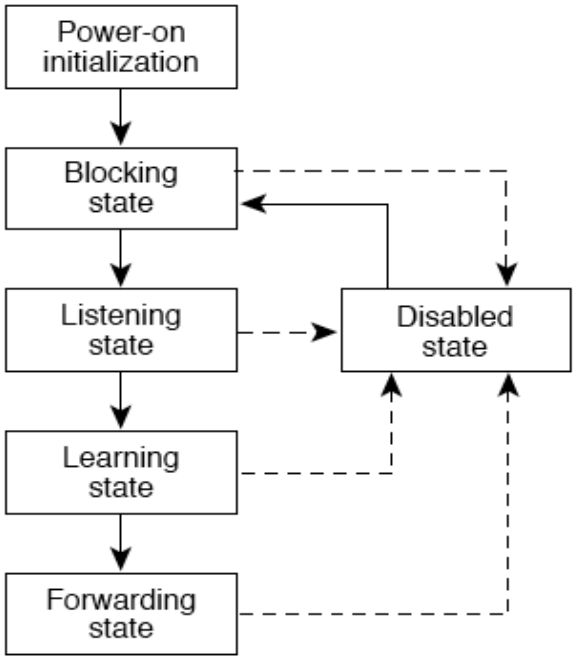
- Das Spanning Tree Protocol (STP) ist durch IEEE 802.1D spezifiziert
- STP wird durch das Rapid STP ersetzt
- RSTP kommuniziert mit STP
- RSTP ist wie STP ein Link Management Protokoll
- RSTP wird für die Ermittling redundanter Links verwendet.
- Redundate Links führen zu ungewünschten Transport-Schleifen in lokalen Netzen.
- In einem Ethernet LAN kann zwischen zwei Stationen nur ein aktiver Pfad bestehen.
- RSTP definiert eine hierarchische Kommunikationsverbindung, das alle beteiligten Schicht-2 Netzelemente (Switches) einschließt
- RSTP blockiert alle redundanten Pfade

Spanning Tree Prozedur

- Alle RSTP Switche sammeln mit Hilfe des Rapid Spanning Tree Protokolls Information über die existierenden Verbindungsleitungen
- Man nennt diese Nachrichten: Bridge Protocol Data Units (BPDUs)
- Die RSTP-Procedur liefert:
  - Die Festlegung eines eindeutigen **Root Switches** als Ausgangspunkt für eine Spanning-Tree Netztopologie.
  - Die Festlegung eines **Designated Switches** für jedes LAN Segment.
  - Die Identifizierung von Schleifen (loops) im LAN-Netz und und Blockierung der redundanten Switch Ports

STP Port-Zustände

Jeder Port besitzt ein Status Register, das den aktuellen Port-Zustand enthält

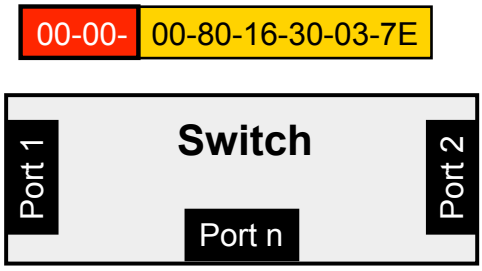


Spanning Tree Adressen

- Multicast address: 01-80-C2-00-00-00
- Bridge ID (BID): Priority | MAC-Adresse
  2 bytes 6 Bytes
- Port ID:
  Port 1; Port 2; Port n

Spanning Tree Prozedur

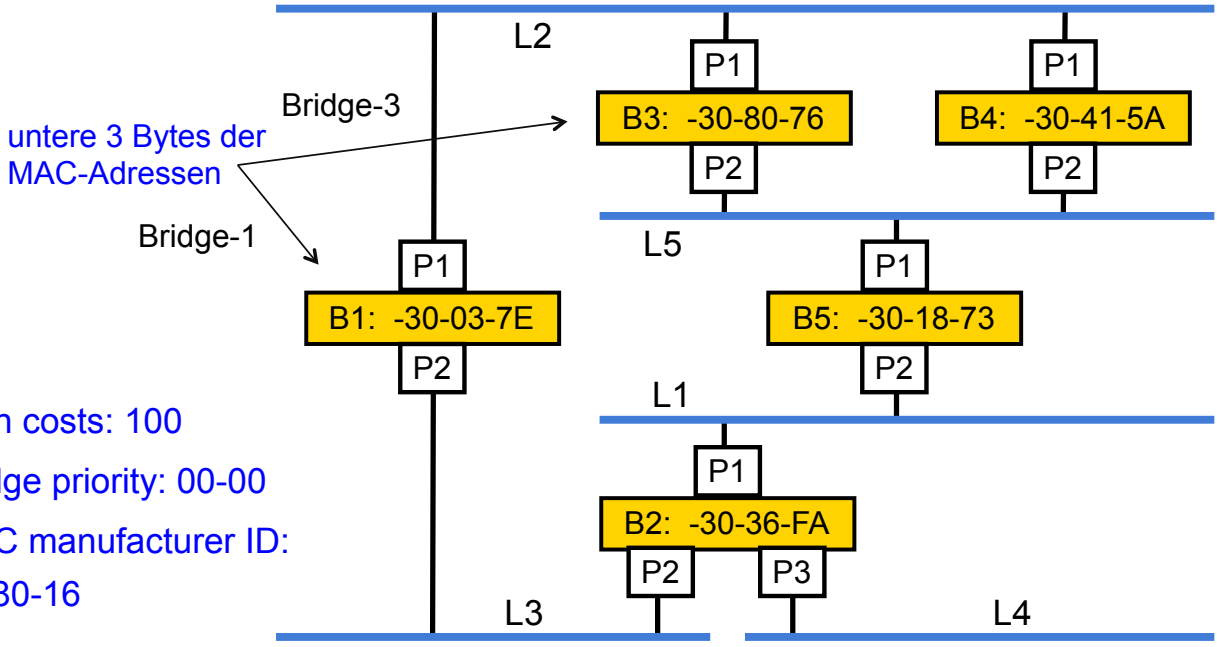
1. Jeder Switch erhält eine relative Prioritätszahl. Die **BID = Prioritätszahl + MAC-Adresse** definieren die Bridge-Priorität
2. Die Bridge mit der niedrigsten BID wird die **Root Bridge**
3. Jede Bridge bestimmt einen **Root Port = niedrigste Path Cost + geringste Entfernung** zur Root Bridge.
   Path Cost = 1000/line Kapazität in Mbit/s



RSTP Zustände

- **Listening**.
  Aufnahme von RSTP-Nachrichten (BPDUs) und Ermitteln der Netzkonfiguration
- **Learning**.
  In diesem Zustand wird die Tabelle der angeschlossenen Geräte (MAC table) aufgebaut, die Ethernet-Rahmen aber noch nicht weitergeleitet.
- **Forwarding**.
  Normalbetrieb des Bridge-Ports. Im Normalbetrieb leitet der Port LAN-Pakete weiter oder er befindet sich im blockierten Zustand.
- **Blocking**.
  In diesem Zustand sendet/empfängt der Port nur BPDUs. Andere LAN-Pakete werden nicht bearbeitet.
  Bei der Inbetriebnahme eines RSTP-Switches befinden sich alle Ports idn diesem Zustand

Root Bridge und Root Port (Beispiel)



Path costs: 100

Bridge priority: 00-00

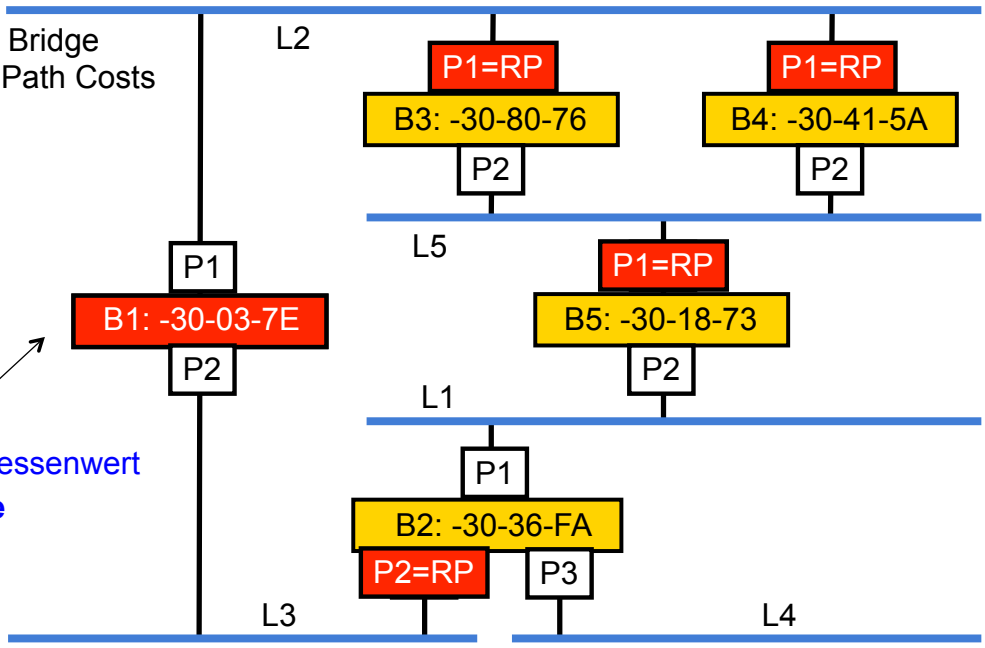
MAC manufacturer ID: 00-80-16

Root Bridge und Root Port Festlegung

Der Root Port in jeder Bridge besitzt die geringsten Path Costs zur Root Bridge.

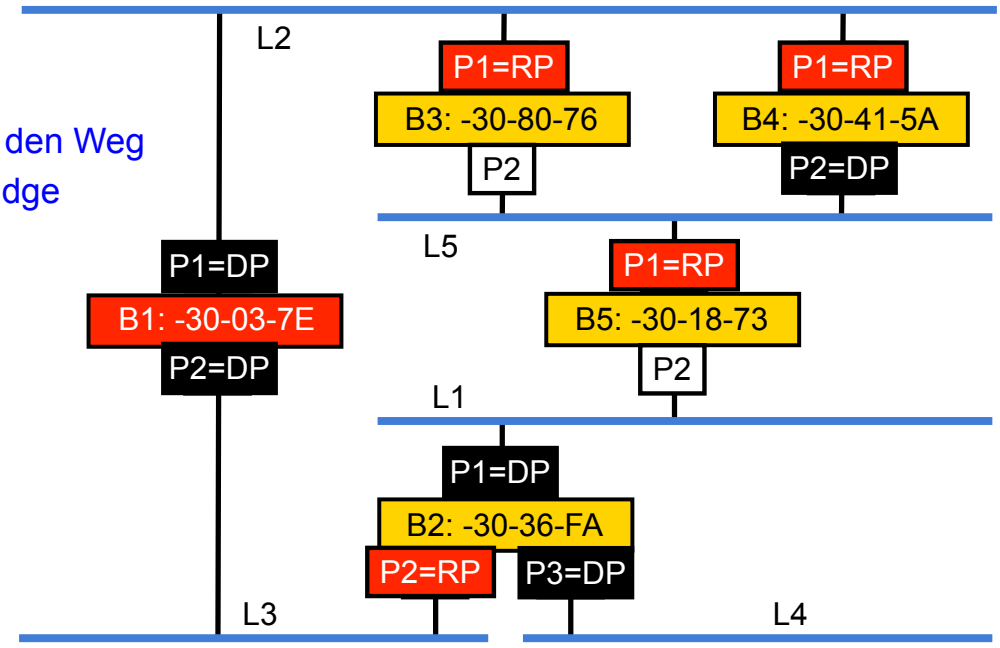
Falls es mehrere Ports mit den selben Path Costs zur Root Bridge gibt entscheidet die Port-Id.

Niedrigster Adressenwert
-> **Root Bridge**



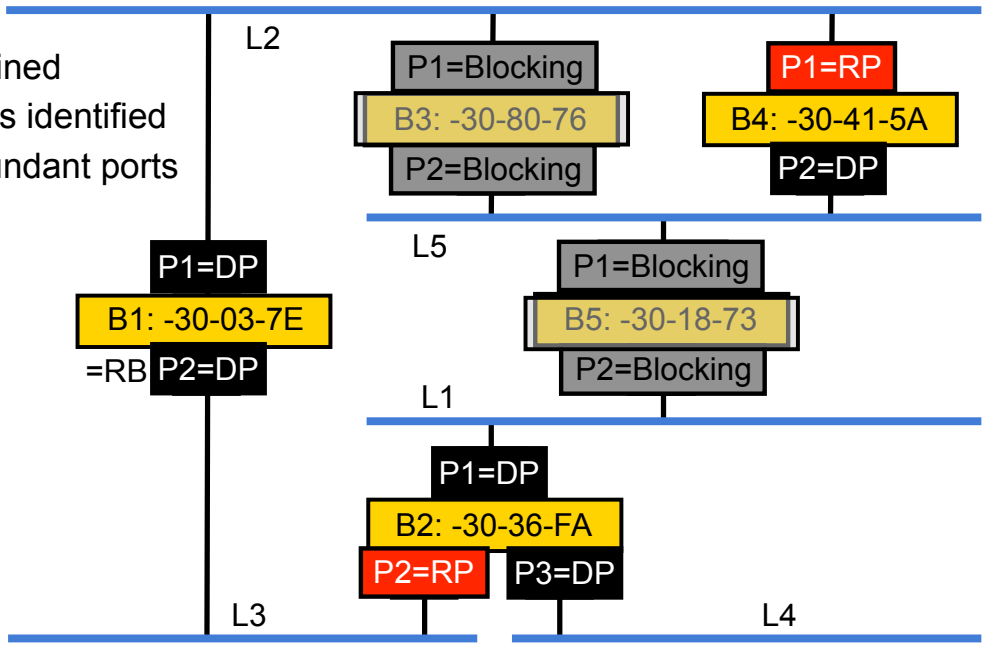
Designated Bridge Port Festlegung

DP markiert den Weg
zur Root bridge



Ergebnis der Spanning Tree Prozedur

1. Root Bridge defined
2. Designated ports identified
3. Blocking of redundant ports



Bridge Protocol Data Unit (BPDU)

PID	V	T	F	Root ID	Root Path Cost	Sender BID	PortID	M-Age	Max-A	Hello	FD

Field Name	Length (Bytes)
Protocol ID (PID)	2
Version (V)	1
Type (T)	1
Flags (F)	1
Rood ID	8
Root Path Cost	4
Sender BID	8
Port ID	2
Message Age (M-Age)	2
Max-Age (Max-A)	2
Hello	2
Forward Delay	2

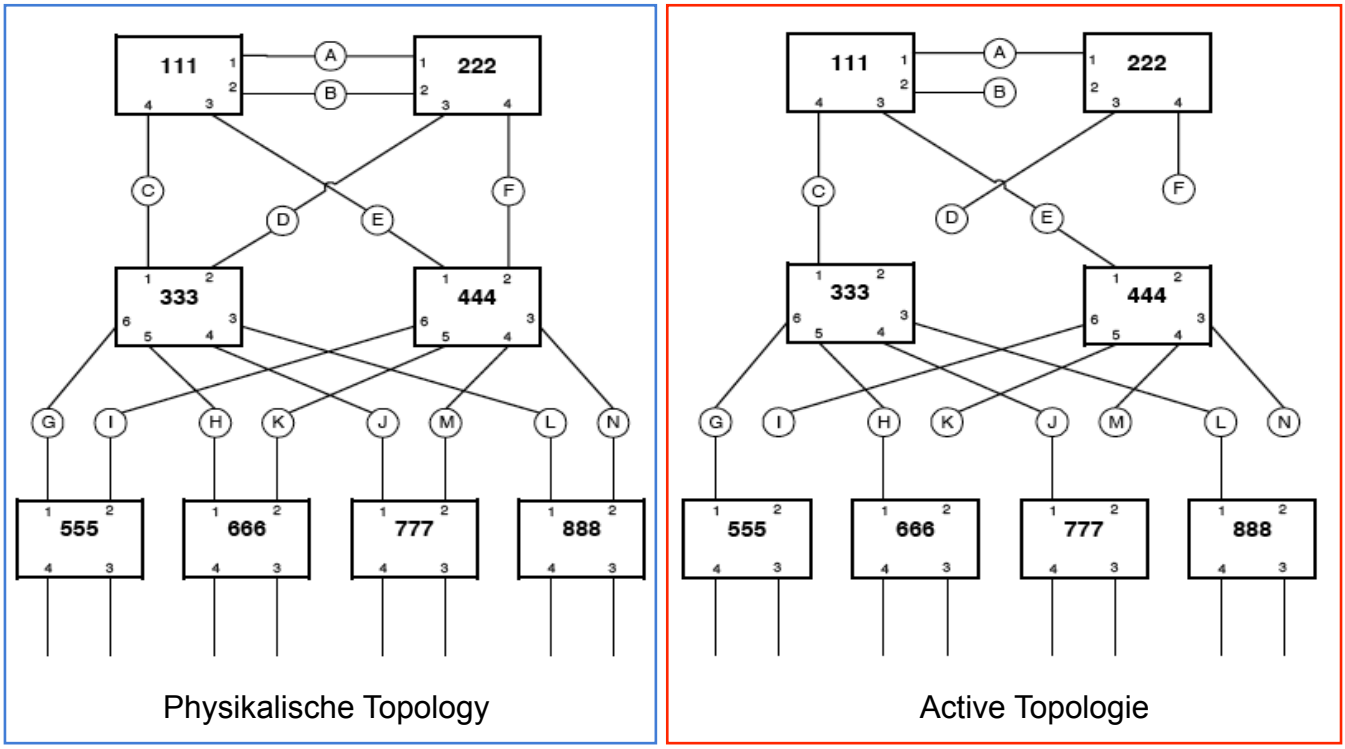
Priority Vector

- Rapid Spanning Tree Protocol (RSTP) Bridges tauschen Informationen (BPDUs) aus zur Ermittlung der **Root Bridge** und der **kürzesten Entfernung** (shortest path) von jedem LAN und allen anderen Bridges.
- Diese Information heißt: *Spanning Tree Priority Vector*.

Priority Vector Komponenten

Root Bridge Identifier, Root Path Cost zur Root Bridge von der sendenden Bridge	Netz
Bridge Identifier der sendenden Bridge Port Identifier von dem Port über den die Nachricht übertragen wurde	Lokal
Port Identifier von dem Port über den die Nachricht empfangen wurde	internal

Bridge Configuration Example



Priority Vector Berechnung

port priority vector = {RootBridgeID : RootPathCost : DesignatedBridgeID : DesignatedPortID : BridgePortID}

message priority vector = {RD : RPCD : D : PD : PB}

root path priority vector = {RD : RPCD + PPCPB : D : PD : PB }

Bedingungen für den Message Priority Vector als Ersatz für den Port Priority Vector:

A	((RD < RootBridgeID)) ||
B	((RD == RootBridgeID) && (RPCD < RootPathCost)) ||
C	((RD == RootBridgeID) && (RPCD == RootPathCost) && (D < DesignatedBridgeID)) ||
D	((RD == RootBridgeID) && (RPCD == RootPathCost) && (D == DesignatedBridgeID) && (PD < DesignatedPortID)) ||
E	((D == DesignatedBridgeID.BridgeAddress) && (PD == DesignatedPortID.PortNumber))

Kursinhalt

- Ethernet Übersicht und Protokolle
- Ethernet Schicht-1
- Ethernet Link Schicht
- Medium Access Control
- Logical Link Control – LLC
- Ergänzende LAN Protokolle
  - Spanning Tree Protocol – STP , RSTP
  - Link Aggregation Control Protocol - LACP

Link Aggregation - LACP

Definition

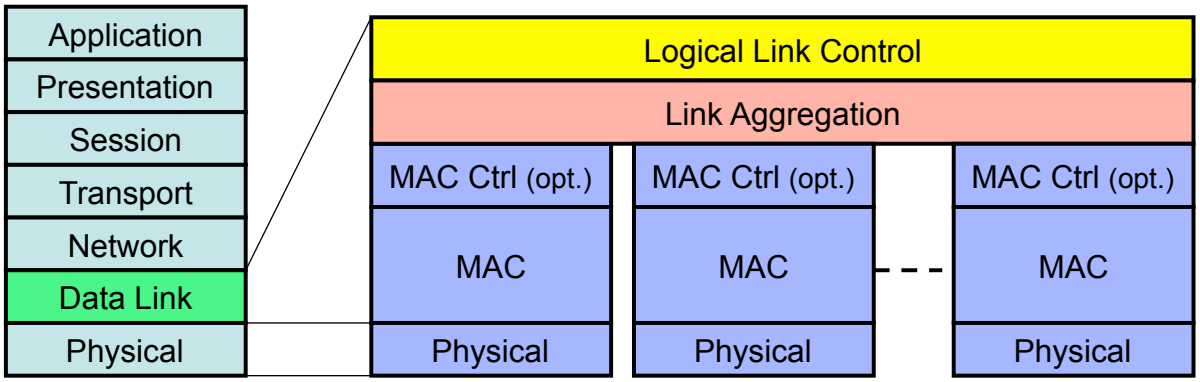
- Das Link Aggregation Control Protocol LACP unterstützt die Gruppierung von physikalischen Links zu einer logischen Einheit. Diese Link-Gruppe wird wie ein physikalischer Link behandelt

Eigenschaften:

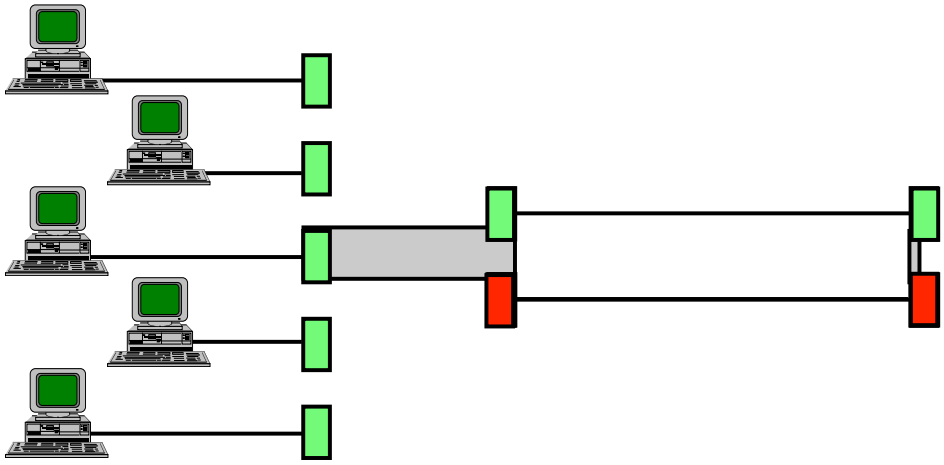
- **Erhöhung der** Datenrate:
  Die Kapazität mehrerer Ports addiert sich zu einem logischen Link
- **Load sharing**:
  Schicht-2 Verkehr wird über mehrere Links verteilt
- Keine Änderung im IEEE 802.3 Rahmenaufbau
- **Netzmanagement**:
  Link Aggregation Objecte sind im Standard Netzmanagement definiert
- Link Aggregation ist nur für **Punkt-zu-Punkt Verbindungen** im Full-duplex Mode verfügbar

Ethernet Protocol Layers

Link Aggregation umfasst einen optionalen Sublayer zwischen der MAC User und der MAC- oder optionalen MAC Control - Schicht



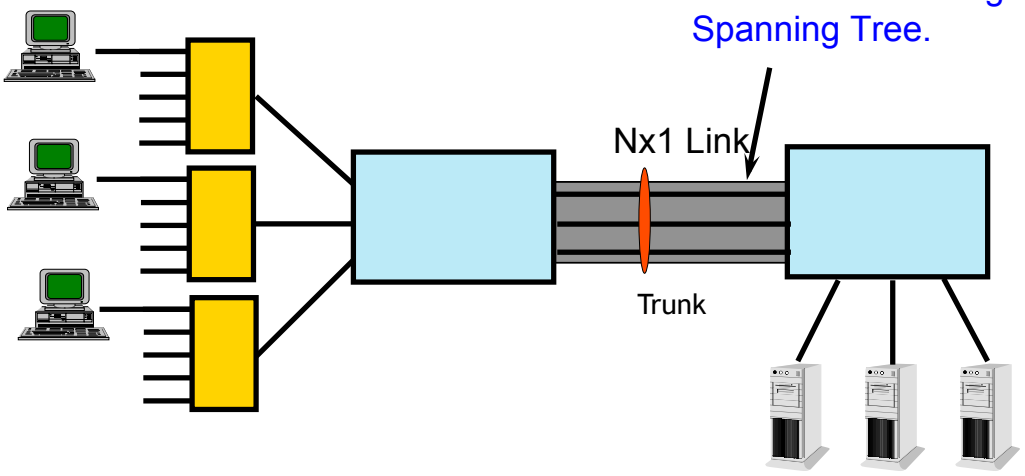
STP: Nachteile



- **Redundanz:** hohe Umschaltzeit aus dem Blockierungszustand
- **Lastverteilung:** ungeeignet
- **Skalierbarkeit**: 10M/100M/1G; nicht n x 100M

Link Aggregation (IEEE 802.3-Clause 43)

Sieht aus wie eine Verbindung im Spanning Tree.



Funktionsprinzip

Aggregator:

- verbindet einen oder mehrere Hardware-Ports in einem System.
- **verteilt** Rahmen vom MAC Client an die Ports
- **sammelt** empfangene Rahmen aus den Ports an den MAC Client

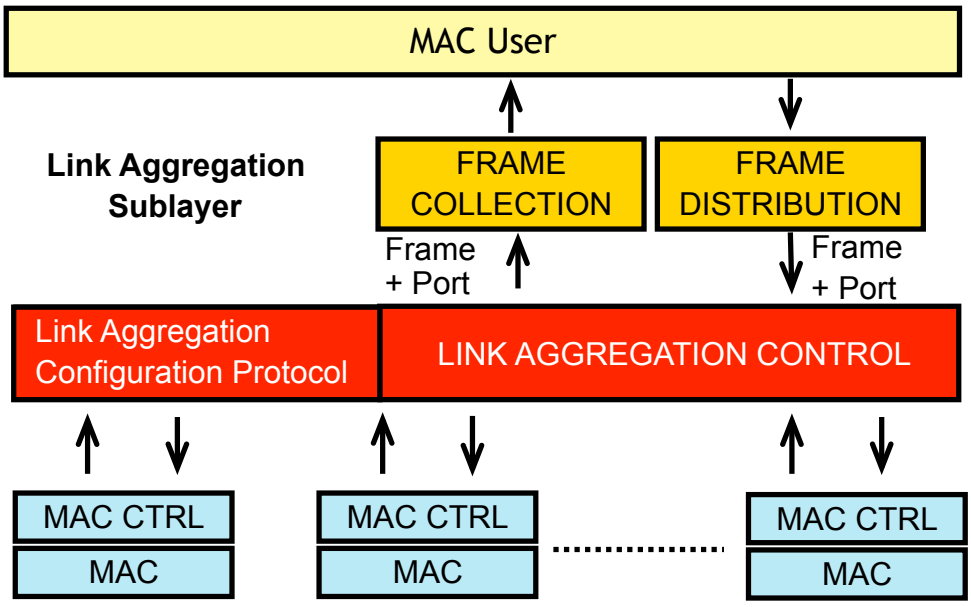
System:

- kann mehrere Aggregatoren für mehrere MAC Clients enthalten
- ein Port gehört zu einer bestimmten Zeit einem bestimmten Aggregator
- Ein MAC Client wird zu einer bestimmten Zeit von einem bestimmten Aggregator bedient

Link Aggregation Control Function (LAC):

- Die Port-Aggregation wird durch die Link Aggregation Control Function realisiert.

Referenzmodell



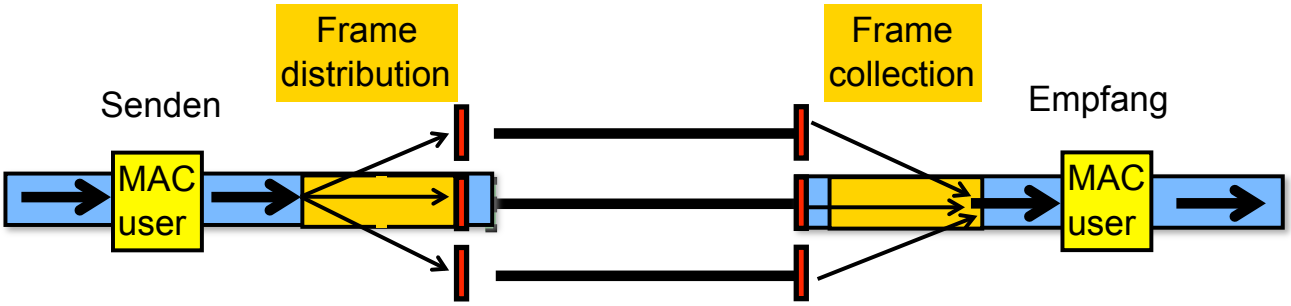
Frame Distribution / Frame Collection

Frame Distribution

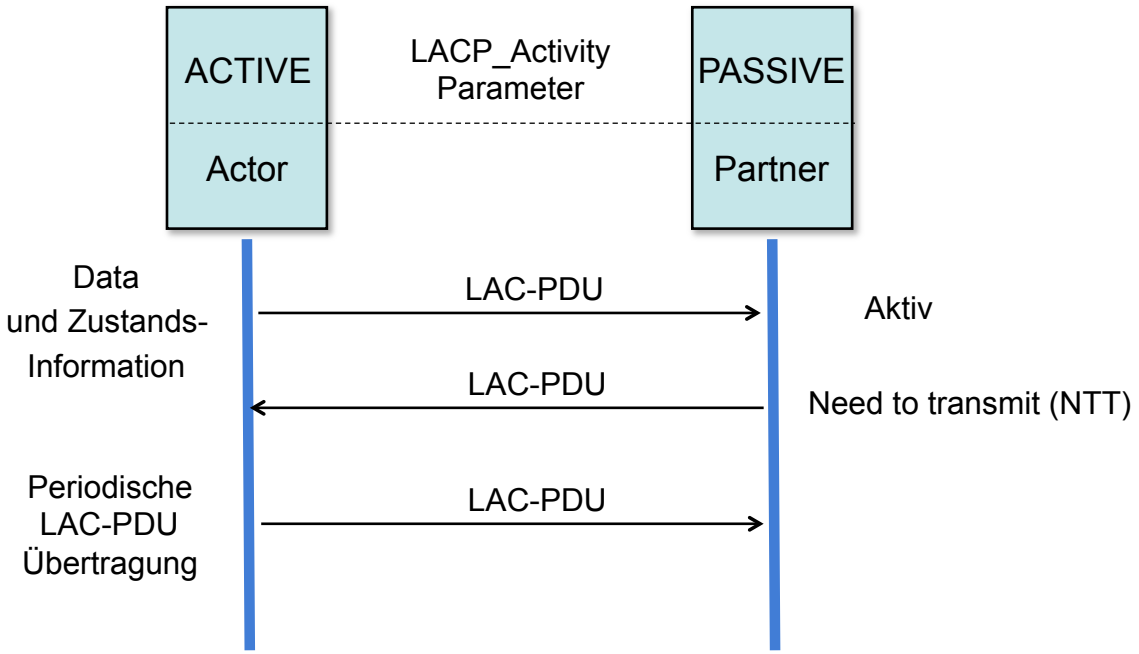
- Zuständig für die **Verteilung** der Frames über die physikalischen Links.
- Sicherstellung dass keine Frames verdoppelt wurden

Frame Collection

- Zustandig für die ursprüngle Wiederherstellung der Paket-Reihenfolge
- Ablieferung der Pakete an die **MAC Client** Funktion.



LACP Kommunikation

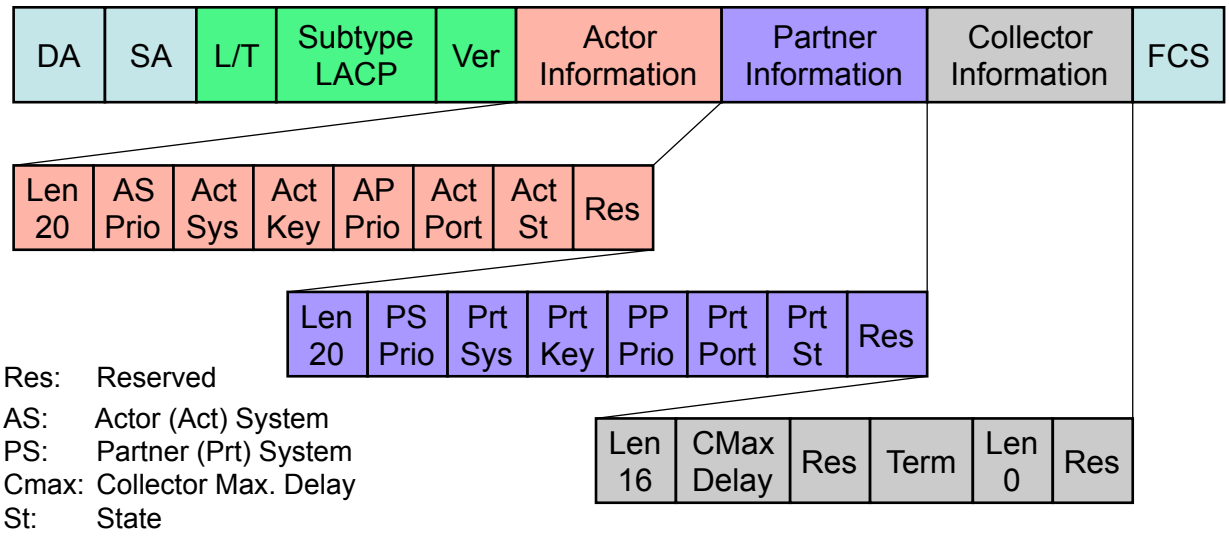


Im LACP gibt es keinen Frame Loss Detection und Retry Mechanismus

LACP Nachrichten

Link Aggregation Control konfiguriert und überwacht den Link Aggregation sublayer mittels statischer und dynamischer Informationen

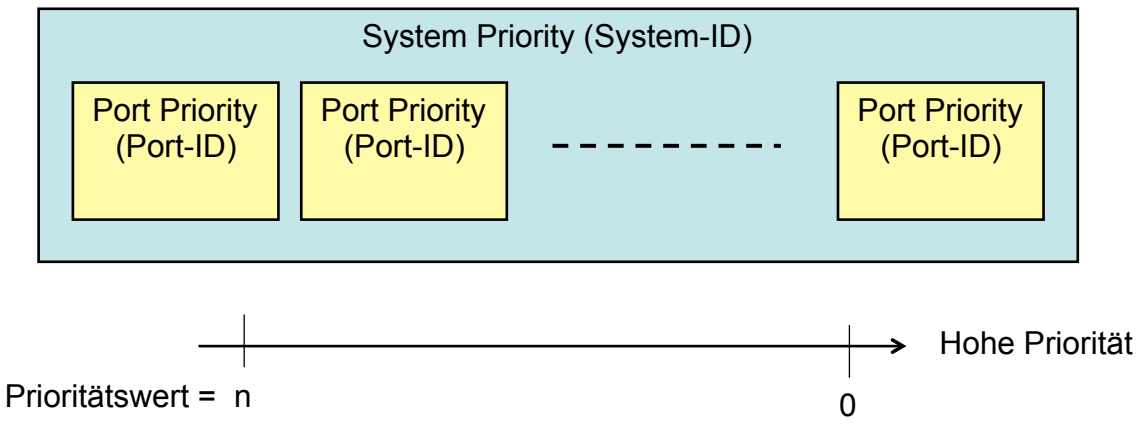
LACP Protocol Data Unit Format:



Res: Reserved
AS: Actor (Act) System
PS: Partner (Prt) System
Cmax: Collector Max. Delay
St: State

Link Priority

- Jedem LACP-Link ist eine eindeutige Priorität zugewiesen
- Prio-0 ist der höchste Prioritätswert.
- Ports werden gemäß ihrer lokalen **Priorität bezeichnet.**



Energieinformationstechnik
Teil 2.2 Internet

Dr. Leonhard Stiegler

www.dhbw-stuttgart.de

Kursinhalt

- Einführung: Telekommunikationsprotokolle
- Internet Protokollschichten
- IP Version 4
- Beziehung : MAC-Adresse – IP-Adresse
- IP Adressierung, Subnetze
- Übersicht : IP-Routing
- IP Transportschichten: TCP und UDP
- Internet Control Protocol ICMP

Definition: Kommunikationsprotokoll

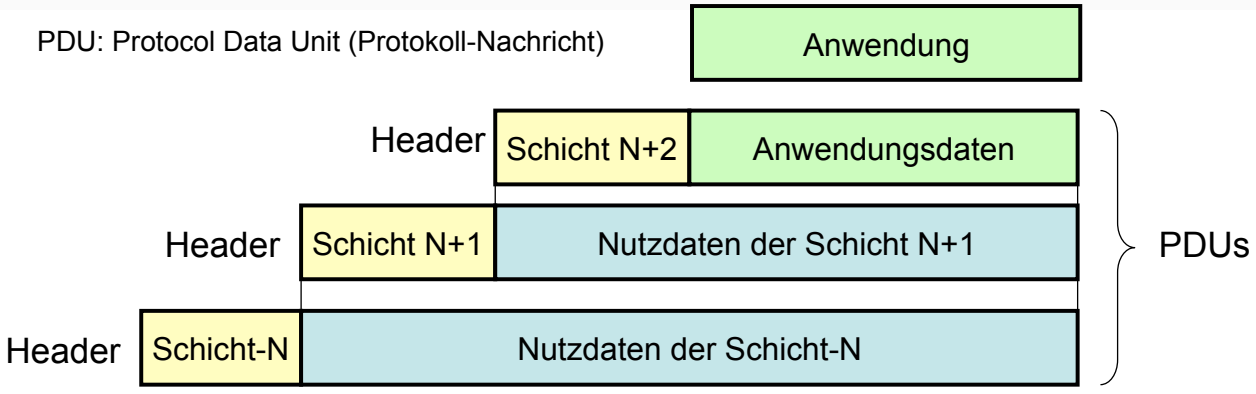
Kommunikationsprotokolle spezifizieren :

- Formate, Datentypen und Inhalte der Protokollnachrichten (PDUs)
- Protokollschichten, welche PDUs austauschen
- Zeitbedingungen für den PDU-Austausch
- Dienste, welche von unteren Schichten zur Verfügung gestellt werden
- Protokoll-Zustände und die erlaubten Zustandsübergänge *beschrieben durch Zustandsdiagramme*
- Fehlerbehandlung

Kommunikation der Protokollschichten

- Jede Protokollschicht besitzt einen Protokollheader, der die Funktionen der Protokollschicht realisiert.
- Jede Protokollschicht stellt ihren Header vor die Daten der darüber liegenden Schicht
- Eine Protokollnachricht der Schicht-N enthält alle darüber liegenden Protokollschichten.

PDU: Protocol Data Unit (Protokoll-Nachricht)



IETF Dokumente

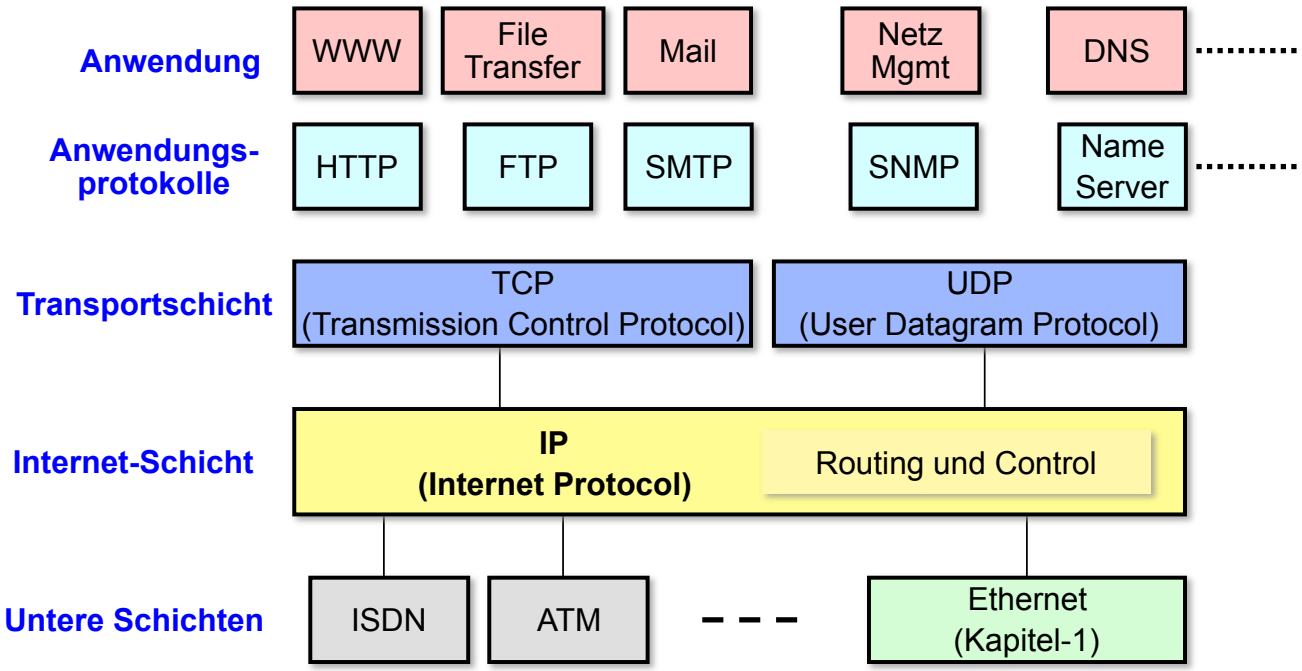
Request for Comments RFC: offizielle IETF Dokumente

Experimental RFC:	Versuchsstadium
Informal RFC:	zur Information und Koordination
Best Current Practice RFC:	Implementierungs-Hinweise
Standards Track RFC:	offizielle Standards (Standard-Vorschläge, Draft standard)
Internet Draft Documents (ID):	nicht-offizielle Arbeits- papiere, mögliche RFC-Vorläufer

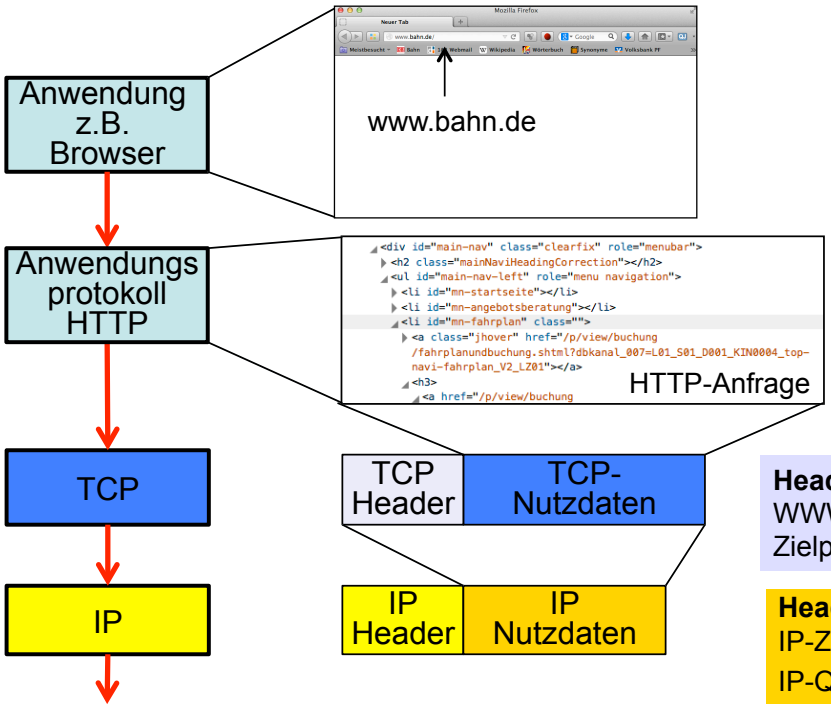
Kursinhalt

- Einführung: Telekommunikationsprotokolle
- Internet Protokollschichten
- IP Version 4
- Beziehung : MAC-Adresse – IP-Adresse
- IP Adressierung, Subnetze
- Übersicht : IP-Routing
- IP Transportschichten: TCP und UDP
- Internet Control Protocol ICMP

Internet-Protokollfamilie



Verarbeitung von IP-Paketen : Sender

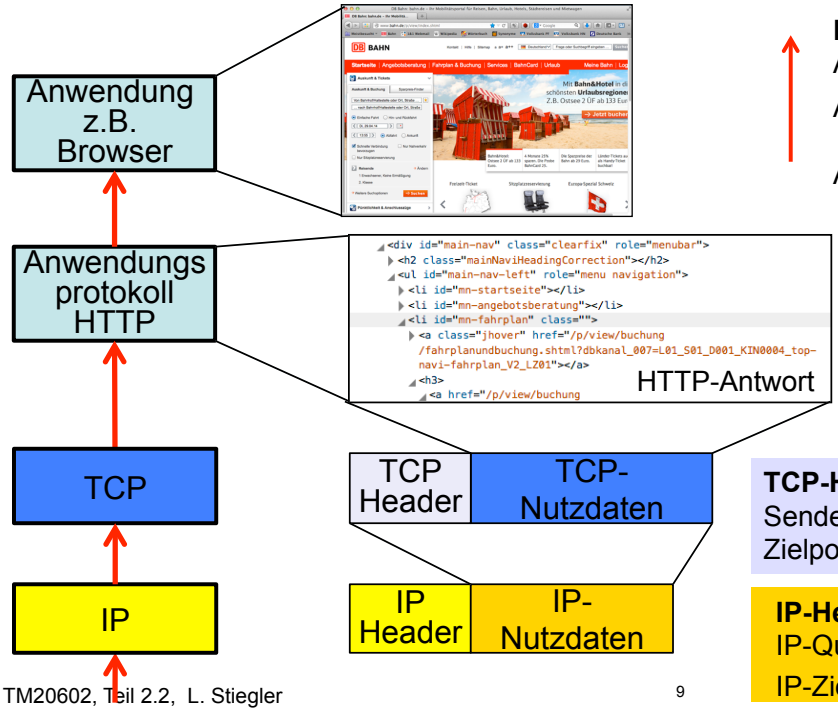


Transport der Daten erfolgt lokal durch das Betriebssystem

Header: Anwendungsadressen
WWW im Zielserver:
Zielport = 80 Sender-Port = z.B. 32550

Header: Geräteadressen
IP-Ziel: www.bahn.de (23.209.177.133)
IP-Quelle: z.B. 85.12.16.22

Verarbeitung von IP-Paketen : Empfänger



Betriebssystem ermittelt die richtige Anwendung (Port-Nr)

Anwendungsprotokoll ermittelt das richtige Anzeige-Fenster (Port-Nr)

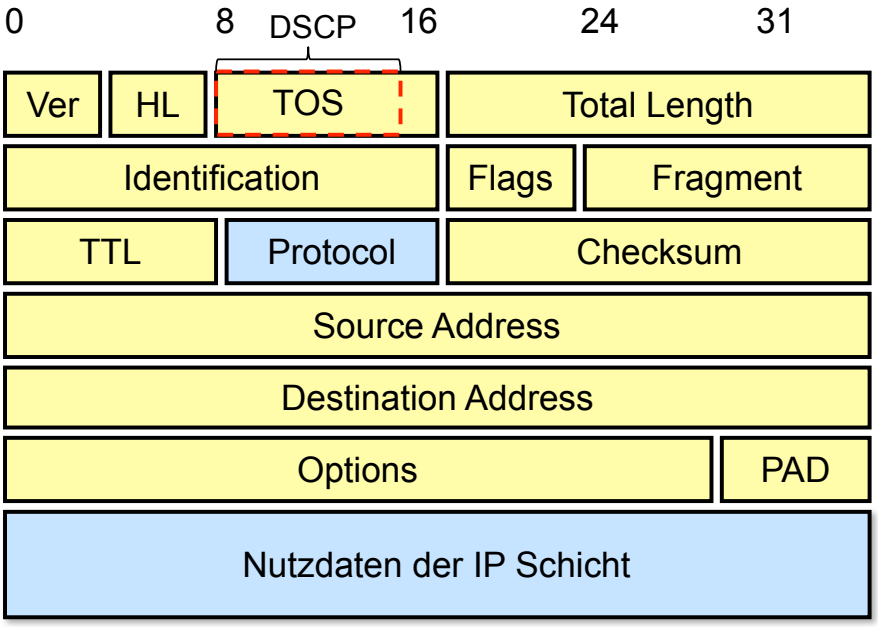
TCP-Header: Anwendungsadressen
Sender-Port = 80
Zielport = 32550

IP-Header: Geräteadressen
IP-Quelle: www.bahn.de (23.209.177.133)
IP-Ziel: z.B. 85.12.16.22

Kursinhalt

- Einführung: Telekommunikationsprotokolle
- Internet Protokollschichten
- IP Version 4
- Beziehung : MAC-Adresse – IP-Adresse
- IP Adressierung, Subnetze
- Übersicht : IP-Routing
- IP Transportschichten: TCP und UDP
- Internet Control Protocol ICMP

Internet Protokoll Schicht - IPv4 Header



DSCP: Differentiated Services Code Point

IP-Header Parameter (1)

Feldname	Länge [Bits]	Bedeutung
VER	4	IP Versionsnummer
HL	4	Header Länge in 32-Bit Einheiten
TOS	8	Type of Service Bits 0-5: DSCP (Differentiated Services Code Point) Bits 6-7: ECN (Explicit Congestion Notification – IP-Flusskontrolle)
Total Length	16	Paketlänge in Bytes
Identification	16	Steuerung der Fragmentierung
Flags	3	Bit 0 reserviert = 0Bit 0 Bit 1 DF Don't Fragment Bit 2 MF More Fragments
Fragment	13	Fragment Offset

IP-Header Parameter (2)

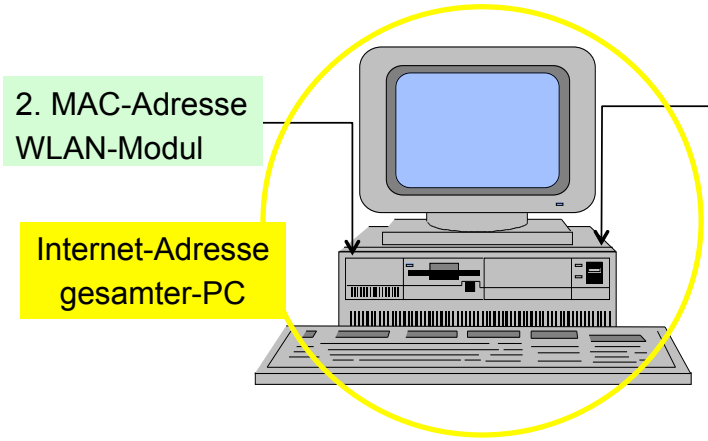
Feldname	Länge [Bits]	Bedeutung
TTL	8	Time to Live : Lebensdauer in Anzahl der Hops
Protocol	8	Protokollname der folgenden Schicht
Checksum	16	Header Prüfsumme
Source Address	32	Sender-Adresse
Destination Address	32	Ziel-Adresse
Options	Max. 32	Zusatzinformation für Routing und Transport-Sicherheitsmethoden
PAD	Variabel	Füllbits zu 32 Bit
Data	Variabel	Nutzdaten

Kursinhalt

- Einführung: Telekommunikationsprotokolle
- Internet Protokollschichten
- IP Version 4
- Beziehung : MAC-Adresse – IP-Adresse
- IP Adressierung, Subnetze
- Übersicht : IP-Routing
- IP Transportschichten: TCP und UDP
- Internet Control Protocol ICMP

MAC-Adressen und IP-Adressen

MAC-Adressen sind vom Hersteller **fest vorgegeben**



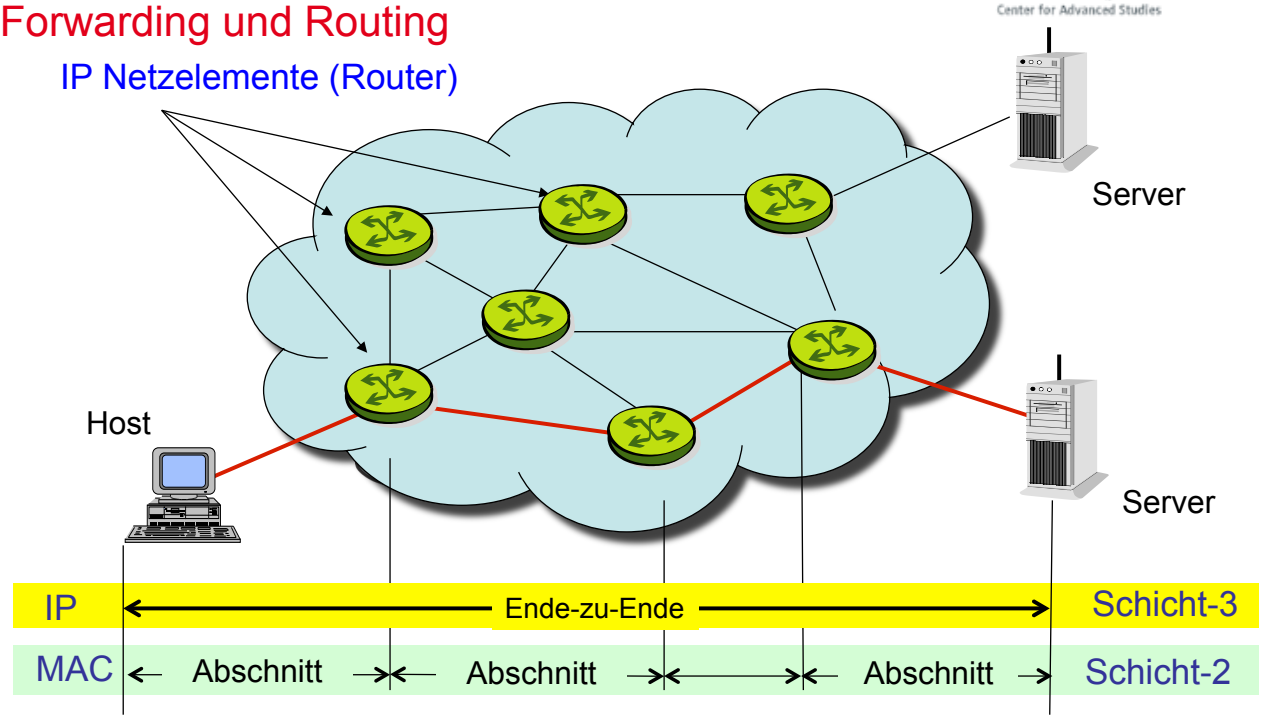
Lokal von PC zu PC, von PC zum Drucker, etc. werden IP-Pakete in **Ethernet-Rahmen** transportiert

Internet Adressen werden **zugeteilt**

Mittels der Internet Adresse wird ein Gerät (Host) eindeutig adressiert

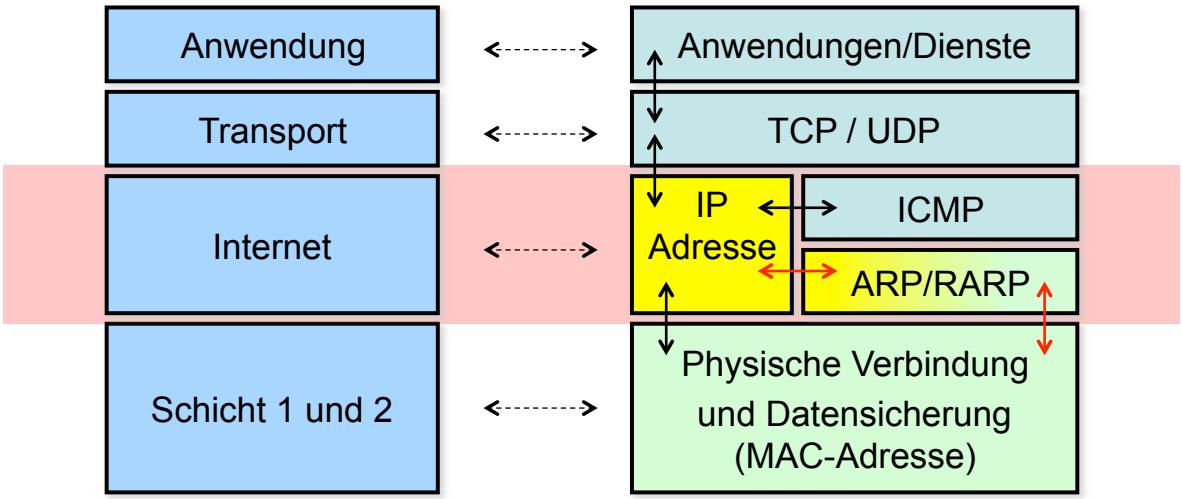
MAC-Adressen und IP-Adressen : Forwarding und Routing

IP Netzelemente (Router)



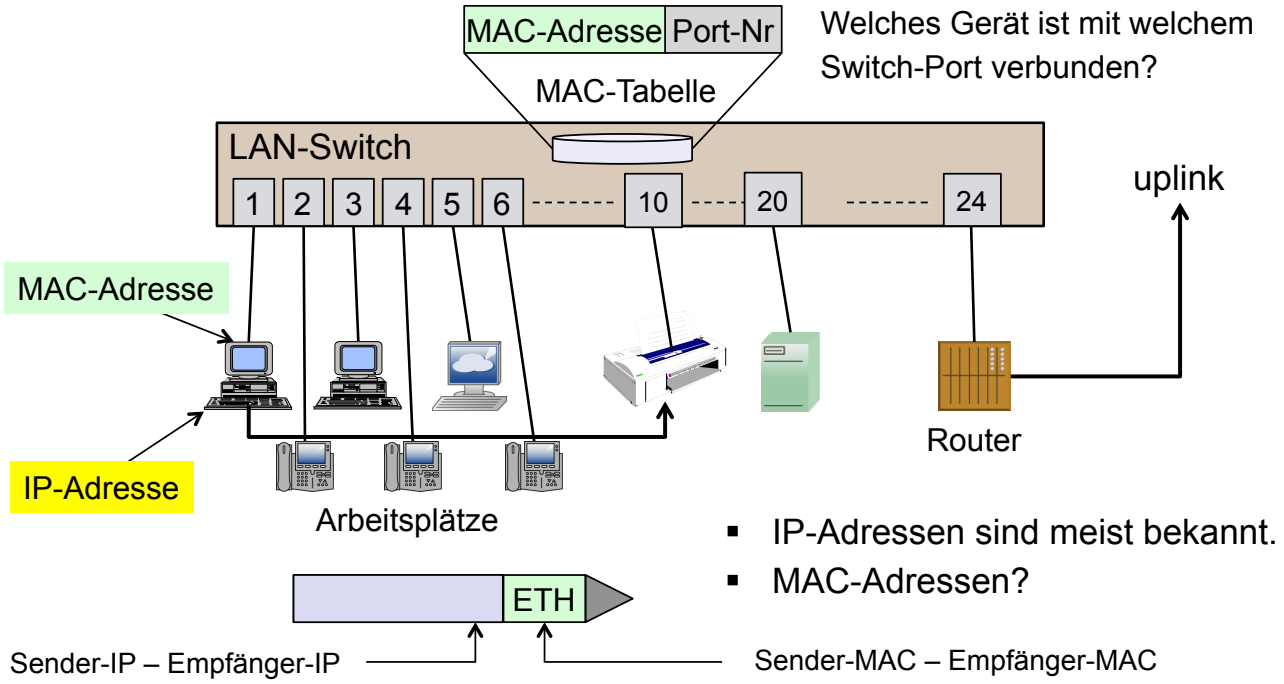
IP - MAC Adressenzuordnung

Die Kooperation zwischen Schicht-2 und Schicht-3 spielt
für die Kommunikation im Anschlussbereich eine entscheidende Rolle.



Drahtgebunden z. B. Ethernet oder drahlos z.B. WLAN

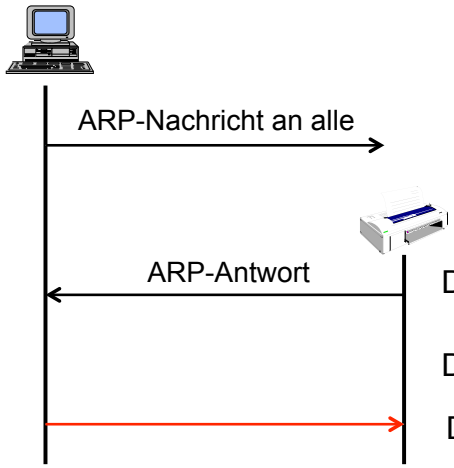
Adressierung im LAN



- IP-Adressen sind meist bekannt.
- MAC-Adressen?

Address Resolution Protocol – ARP Beispiel

- PC kennt die IP-Adresse des Druckers (z.B. 192.168.1.12 aus der Drucker-Konfiguration) aber nicht dessen MAC-Adresse
- PC benötigt die MAC-Adresse des Druckers um diesen ein Ethernet-Paket schicken zu können



Wer hat die IP-Adresse: 192.168.1.12 ?
MAC-Sender : PC
MAC-Empfänger : alle Bits = 1

Drucker antwortet: MAC-Sender : Drucker
MAC-Empfänger: PC

Damit erhält dieser die MAC-Adresse des Druckers

Druckdaten

Aufgabe

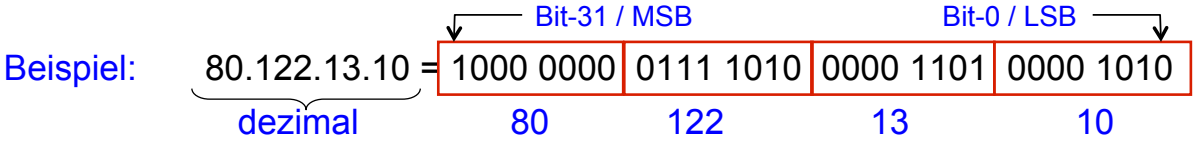
- Analysieren Sie mittels Wireshark das Protokollverhalten Ihres Raspberry PI sobald er mit dem WLAN Router verbunden ist.
- Auf welche Weise wird die MAC-Adresse des Routers ermittelt?

Kursinhalt

- Einführung: Telekommunikationsprotokolle
- Internet Protokollschichten
- IP Version 4
- Beziehung : MAC-Adresse – IP-Adresse
- IP Adressierung, Subnetze
- Übersicht : IP-Routing
- IP Transportschichten: TCP und UDP
- Internet Control Protocol ICMP

IP-Adressen Darstellung

- Internet Adressen des IPv4-Protokolls sind 32-Bit lang.
- Sie werden in vier Teile a‘ 8 Bit zerlegt und als Dezimalzahlen angegeben



- Die Internetadresse wird in zwei logische Teile zerlegt:
- Der vordere Teil (höherwertige Bits) benennt das **Netz**, zu dem die IP-Adresse angehört (**Netz-Teil**)
- Der hintere Teil (niederwertige Bits) adressiert alle Terminals (**Hosts**).
- Die **Netzmaske** legt die beiden Teile (Netz- und Host-Adresse) fest.

Adressklassen

IPv4 Adressen werden in Klassen und Spezialfunktionen eingeteilt.
Die Klasseneinteilung geschieht je nach Größe der Netz- bzw. Host-Anteile.

- **Klasse-A:** Prefix: **0** — **Bereich**: 0.0.0.0 bis 127.0.0.0
  8-bit Network (/8) — 8-Bit Netz + 24-Bit Host
- **Klasse-B:** Prefix: **1 0** — **Bereich**: 128.0.0.0 bis191.255.255.255
  16-bit Network (/16) — 16-Bit Netz + 16-Bit Host
- **Klasse-C:** Prefix: **1 1 0** — **Bereich**: 192.0.0.0 bis 223.255.255.255
  24-bit Network (/24) — 24-Bit Netz + 8-Bit Host
- **Klasse-D**: Prefix: **1 1 1 0** — **Bereich**: 224.0.0.0 bis 239.255.255.255
  Adressierung von Host-Gruppen (Multicast)
- **Klasse-E**: Prefix: **1 1 1 1** — **Bereich**: 240.0.0.0 bis 255.255.255.255
  reservierter Bereich

Subadressierung und Netzmasken

- Subadressierung durch Maskierung = Trennung von Netz- und Host-Adressen

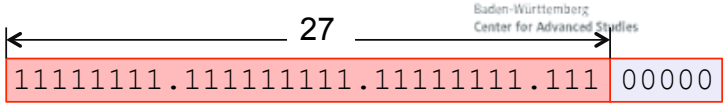
Klasse	NETZ	HOST			Netzmaske	
A	11111111	00000000	00000000		255. 0. 0. 0	/8
	11111111	1 0000000	00000000	00000000	255.128. 0. 0	/9
	11111111	11 000000	00000000	00000000	255.192. 0. 0	/10
	11111111	111 00000	00000000	00000000	255.224. 0. 0	/11
	11111111	1111 0000	00000000	00000000	255.240. 0. 0	/12
	11111111	11111 000	00000000	00000000	255.248. 0. 0	/13
	11111111	111111 00	00000000	00000000	255.252. 0. 0	/14
	11111111	1111111 0	00000000	00000000	255.254. 0. 0	
B	11111111	11111111	00000000	00000000		

Beispiel: IP-Adresse:	01010000	01111010	00011010	00001010	/ 24
AND-Funktion:	11111111	11111111	11111111	00000000	
Netz-Anteil:	01010000	01111010	00011010	00000000	

Auswertung durch den Router — Hostadressen

Subnetz-Berechnung

- Beispiel: Klasse-C Netz
  Berechnungstabelle:



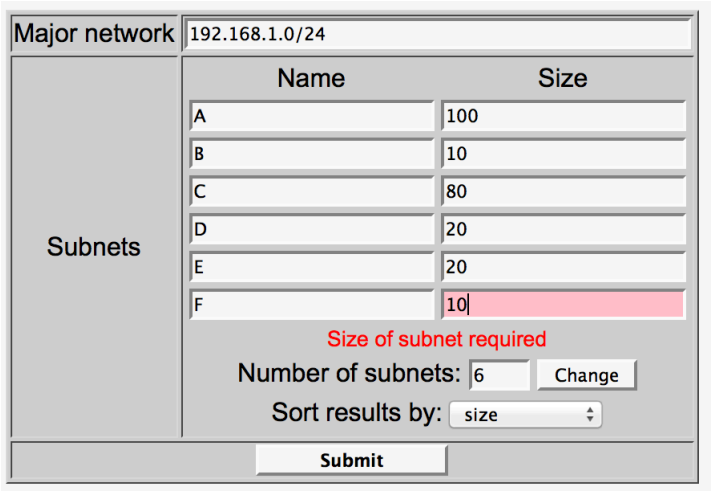
Bit-Wert	128	64	32	16	8	4	2	1
geborgte Bits	1	2	3	4	5	6	7	8
Maskenwert	128	192	224	240	248	252	255	256
Prefix	/25	/26	/27	/28	/29	/30		
Max. Anzahl an Hosts +1 (Broadcast) + 1(Netz)	126	62	30	14	6	2		

- **Beispiel: 192.168.10.40 /27 :**

Subnetz-Maske	255.255.255.224
3-Bits wurden vom Klasse-C Netz entnommen:	2^3 = 8 Subnetze
3-Bits entsprechend dem Bitwert	32
gehört zur Netzadresse:	192.168.10.**32**
gehört zur Broadcast-Adresse:	192.168.10.63
Nächstes Subnetz:	192.168.10.64

Dimensionierung von Sub-Netzen

- **Variable Length Subnet Masking** ist eine Methode, mit der Netz-Administratoren den verfügbaren Adressenraum in Subnetze von unterschiedlicher Größe einteilen können. URL: http://www.vlsm-calc.net/
- Beispiel: Adressenberechnung für 6 Subnetze



Ergebnis: (Auszug)

Address	Mask
192.168.1.0	/25
192.168.1.128	/25
192.168.2.0	/27
192.168.2.32	/27
192.168.2.64	/28
192.168.2.80	/28

Private Internet-Adressenbereiche

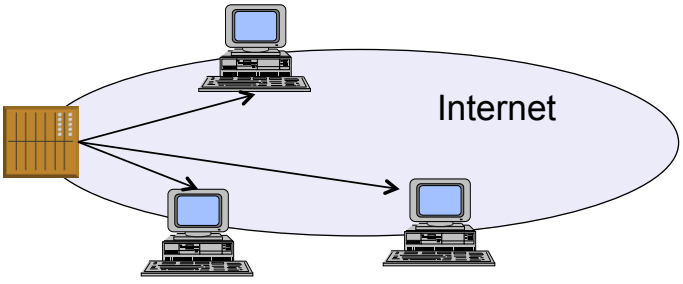
- Nicht-öffentliche Adressenbereiche
  - sind nicht eindeutige, mehrfach verwendbare Adressen
  - werden verwendet für effektive Verwendung des begrenzten Adressraumes
  - sind durch spezielle IETF-Standards definiert

- Als **nicht-öffentliche Adressbereiche** sind reserviert:
  - 10. 0. 0. 0 – 10.255.255.255 (/8)
  - 172.16. 0. 0 – 172. 31.255.255 (/12)
  - 192.168. 0. 0 – 192.168.255.255 (/16)
  - 100. 64. 0. 0 – 100. 64. 255. 255 (/10) für Internet Service Provider

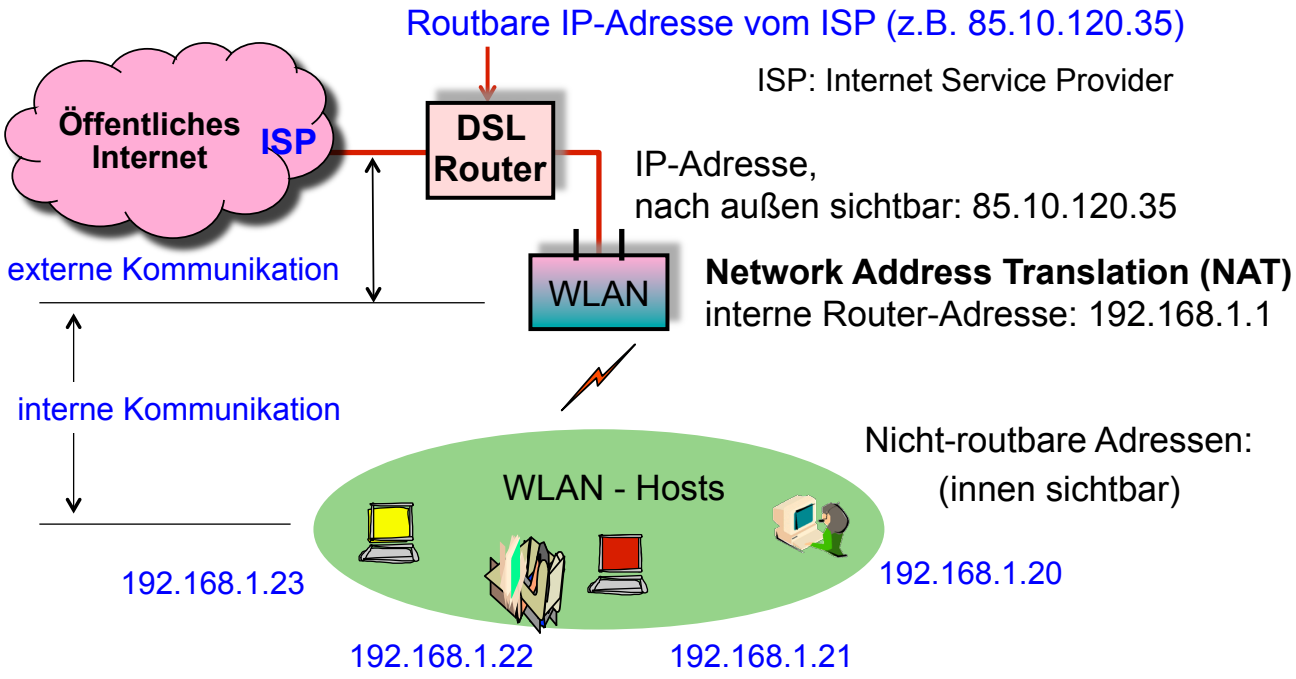
IP Adressenvergabe

- Jeder Internet-Host benötigt für die Kommunikation eine eigene Internet-Adresse
- Die Vergabe dieser IP-Adresse erfolgt entweder
  - automatisch (**dynamisch**) durch einen speziellen **DHCP-Server** oder
  - **statisch** durch den Administrator
- Die automatische / dynamische Adressenvergabe verwendet das **Dynmanic Host Configuration Protocol - DHCP**
- Die DHCP-Funktion kann auch von einem Router ausgeführt werden

DHCP-Server zur dynamischen Vergabe von IP-Adressen



Network Address Translation - NAT



Kursinhalt

- Einführung: Telekommunikationsprotokolle
- Internet Protokollschichten
- IP Version 4
- Beziehung : MAC-Adresse – IP-Adresse
- IP Adressierung, Subnetze
- Übersicht : IP-Routing
- IP Transportschichten: TCP und UDP
- Internet Control Protocol ICMP

Routing : Allgemeine Definition

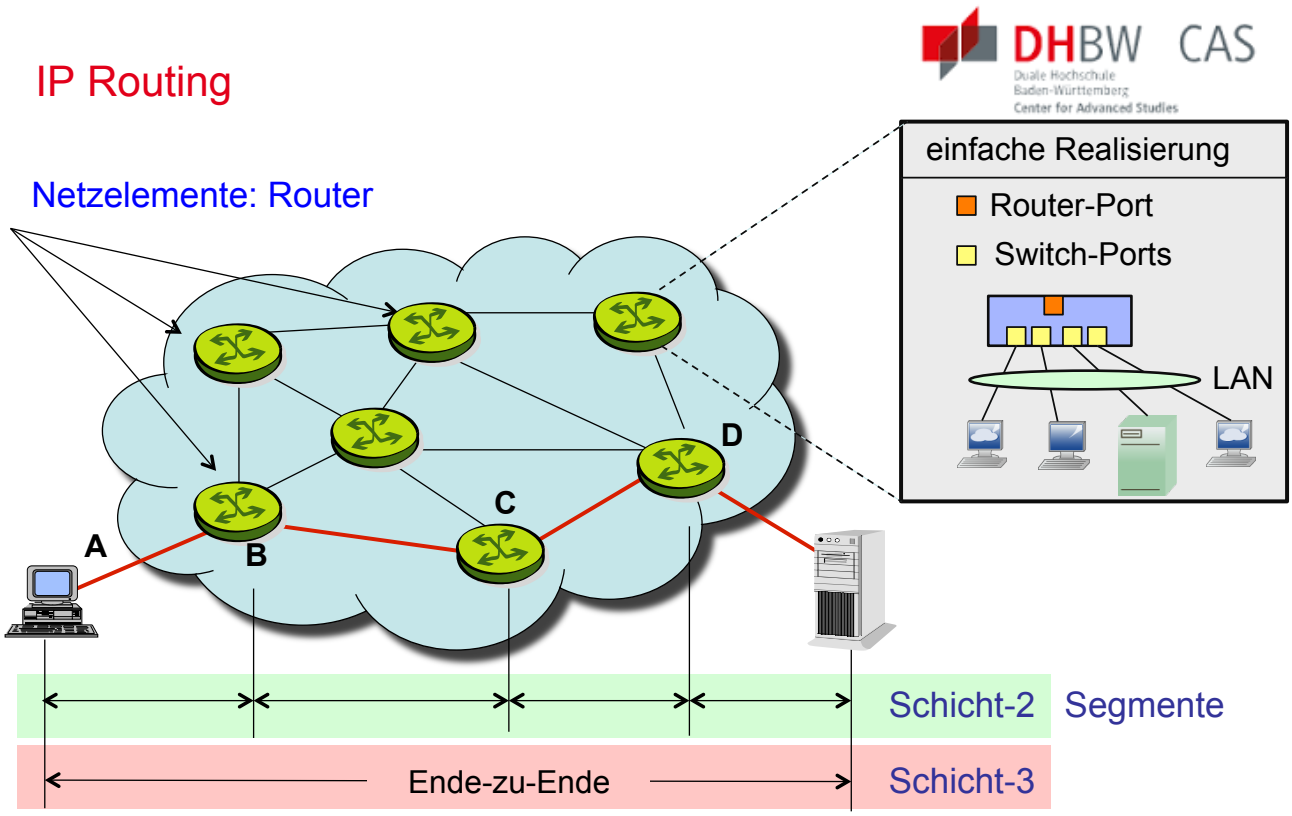
Grundlegender Prozess in allen Telekommunikations- Netzen

Routing-Aufgaben werden vom Router durchgeführt

Der Router

- leitet Information von der Quelle zum Ziel
- verwendet dafür spezielle Methoden, einschl. grafische Theorie
- verwendet spezielle Routing-Protokolle
- wertet die Ziel-Adressen aus um den optimalen Pfad durch das Netz zu finden
- bewertet spezielle Kriterien (Metrik) für die Wege-Auswahl
- behandelt Netzfehler bei der Weiterleitung von Informationen

IP Routing

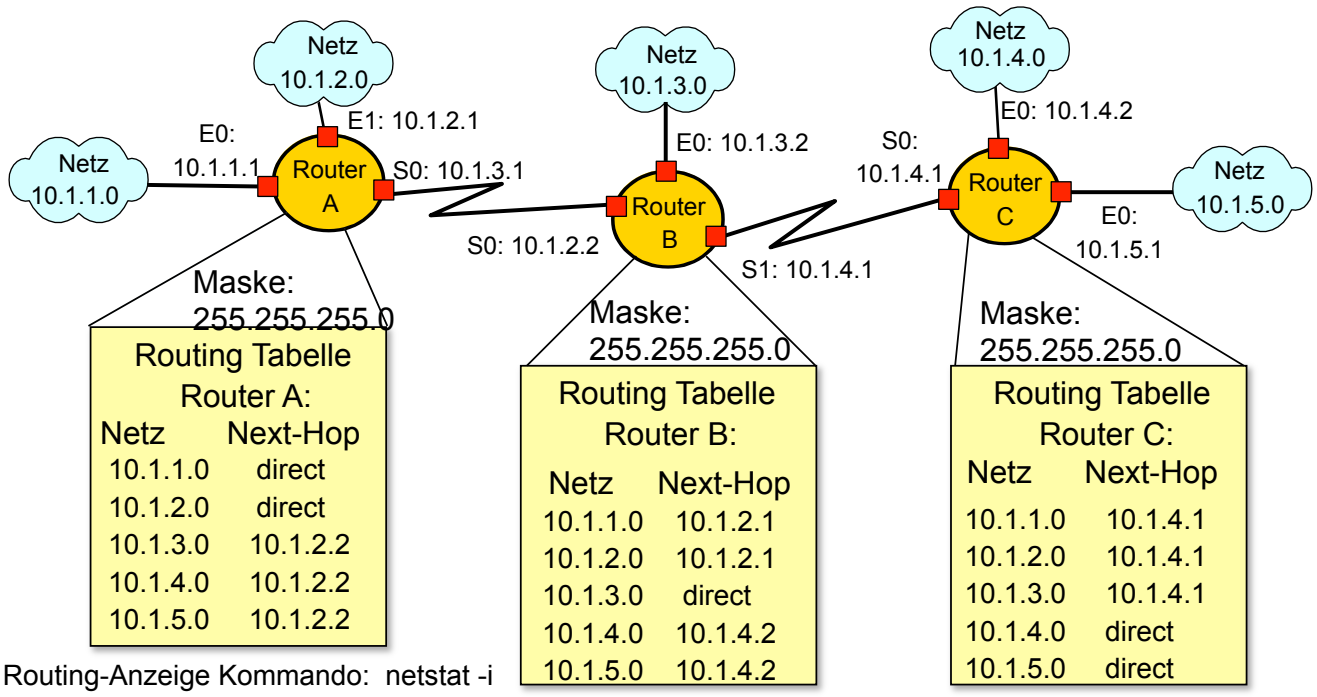


Routing-Tabelle

Inhalt einer Routing-Tabelle

- Zieladresse (erforderlich) : bestimmt das Zielnetz für den Router
- Zielführung (erforderlich) : markiert ein direkt verbundenes Netz oder einen Folge-Router (next-hop), welcher einen Schritt näher am Ziel liegt
- Angabe über das Routingprotokoll
- Art des verbundenen Netzes oder Netzabschnitts, z.B. Ethernet, serial link, usw.
- Standard Route (default route indication)

IP Routing - Prinzip



Routing-Anzeige Kommando: netstat -i

Routing Protokolle

Routing Prozeduren dienen

- dem Austausch von Erreichbarkeits-Informationen zwischen Routern
- der Erstellung einer Routing-Tabelle
- der Berücksichtigung von Netz-Topologie-Änderungen in der Routing-Tabelle
- der Bewertung von empfangener Erreichbarkeits-Information
- der Bestimmung optimaler Routes basierend auf der Erreichbarkeitsinformation

Routing Methode: Hierarchisches Routing

- wird bei großen Netzen verwendet
- Routing-Aufwände nehmen mit der Netzgröße zu: proportional zur Anzahl der Knoten
- Behandlung von Routing-Tabellen : langsam und umständlich in sehr großen Netzen
- Konsequenz : Strukturieren von Netzen in mehrere untereinander verbundene Domänen (z.B. Autonomous Systems AS im Internet)
- Hierarchisches Routing : intra-domain und inter-domain
- Verschieden Protokolle : Interior Gateway Protocols IGP (intra-domain) und Exterior Gateway Protocols EGP (inter-domain)

Routing Methode: Statisches Routing

Charakteristika und Optionen

- Definition und Bildung einer Routing-Tabelle für jeden Router im Netz
- Manuelle Eingaben fester Leitwege durch den Operator
- Exakte Kontrolle und Voraussage von Paket-Laufwegen
- Neu-Definition und manuelle Eingabe bei Konfigurationsänderung
- Summen (summary) Routes für die Bearbeitung spezifischer Adressen in der Routing-Tabelle : Definition von Adressmasken

Routing Methode: Dynamisches Routing

Charakteristika und Optionen

- Automatische Generierung von Routing-Tabellen bei der Inbetriebnahme des Netzes.
- Austausch von Erreichbarkeits-Information zwischen den Routern der angeschlossenen Netze
- Verwendung spezieller Routing-Protokolle, welche den Informationsaustausch regeln
- Verbreitung spezifischer Algorithmen zur Berechnung der optimalen Pfade durch das Netz und Generierung der Routing-Tabellen
- Flexible, dynamische Anpassung der Routing-Tabellen auch bei Netz-Topologieänderungen.

Metrik zur Routen-Bewertung

Aufgabe einer Metrik

- Es existieren i.a. mehrere alternativ-Routen zwischen Quelle und Ziel
- Aufgabe: Erkennen der am besten geeigneten Route unter verschieden Alternativen
- Definition einer Metrik als Maß für die optimale Eignung einer Route
- Eine oder mehrere Metriken werden ausgewählt für spezielle Routing-Protokolle
- Wichtige Metriken für dynamisches Routing:
  - hop count
  - Verkehr
  - Zuverlässigkeit (z.B. Fehlerrate)
  - Bandbreiten-Bedarf
  - Paket-Verzögerung
  - Kosten

Kursinhalt

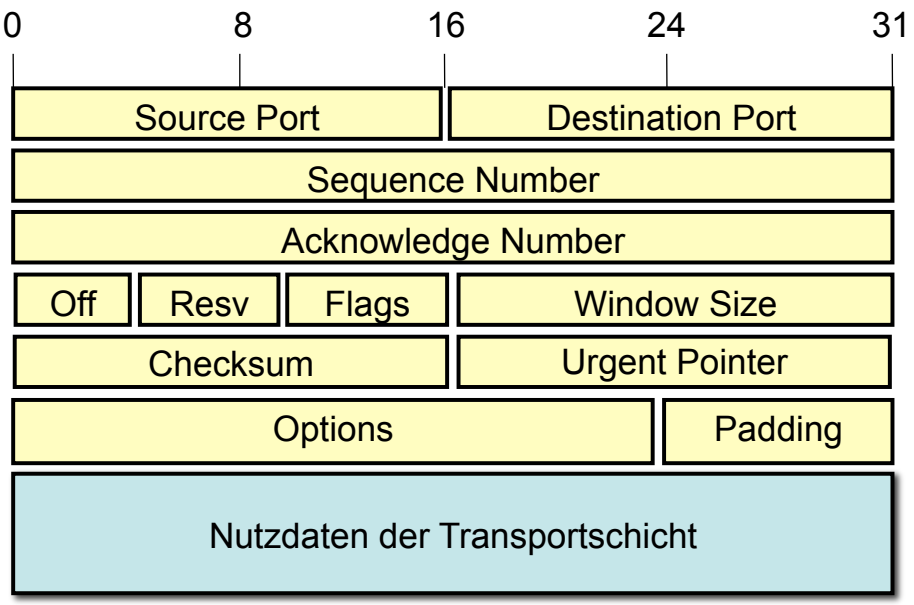
- Einführung: Telekommunikationsprotokolle
- Internet Protokollschichten
- IP Version 4
- Beziehung : MAC-Adresse – IP-Adresse
- IP Adressierung, Subnetze
- Übersicht : IP-Routing
- IP Transportschichten: TCP und UDP
- Internet Control Protocol ICMP

Transportschicht - TCP und UDP

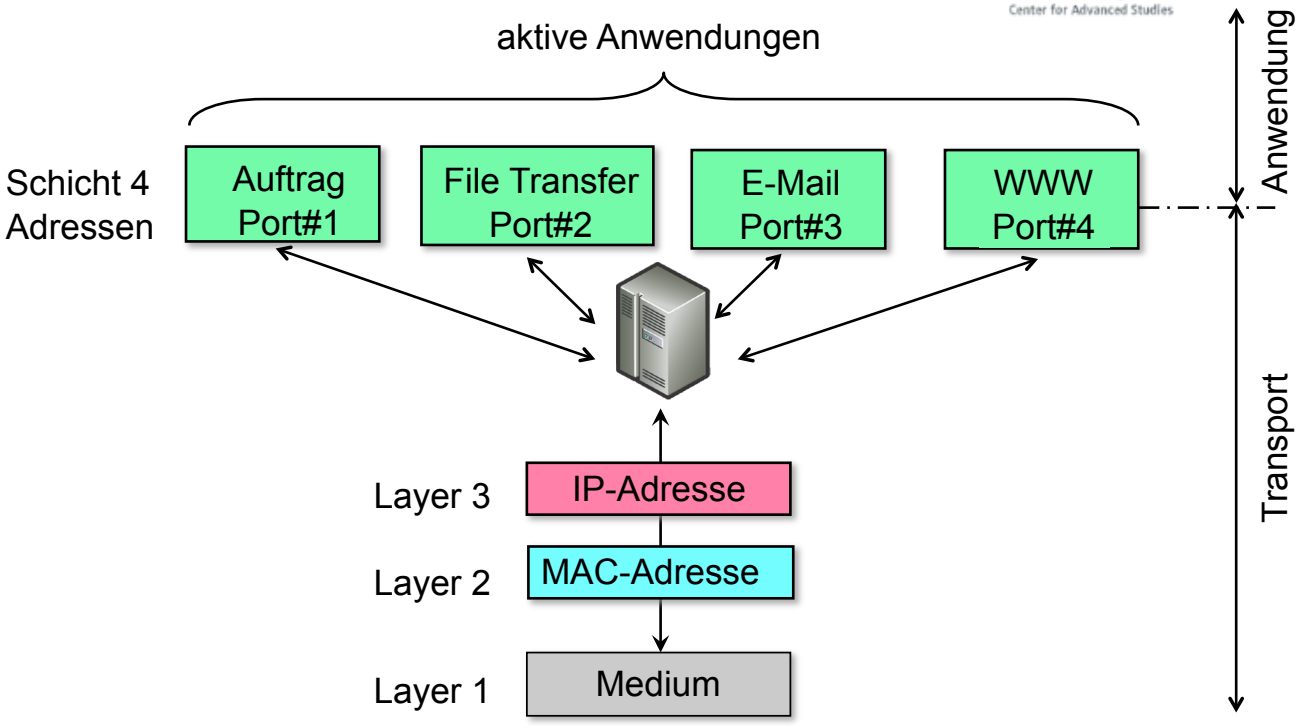
- Die IP-Protokoll-Architektur bietet auf der Transport-Ebene zwei grundsätzliche Transport-Verfahren
- Das **TCP - Transmission Control Protocol** unterstützt den **verbindungsorientierten** und gesicherten Transport von Daten
- Das **UDP - User Datagram Protocol** unterstützt den **verbindungslosen** und ungesicherten Transport von Daten

Transmission Control Protocol TCP

RFC 793



Transport-Adresse (Port)

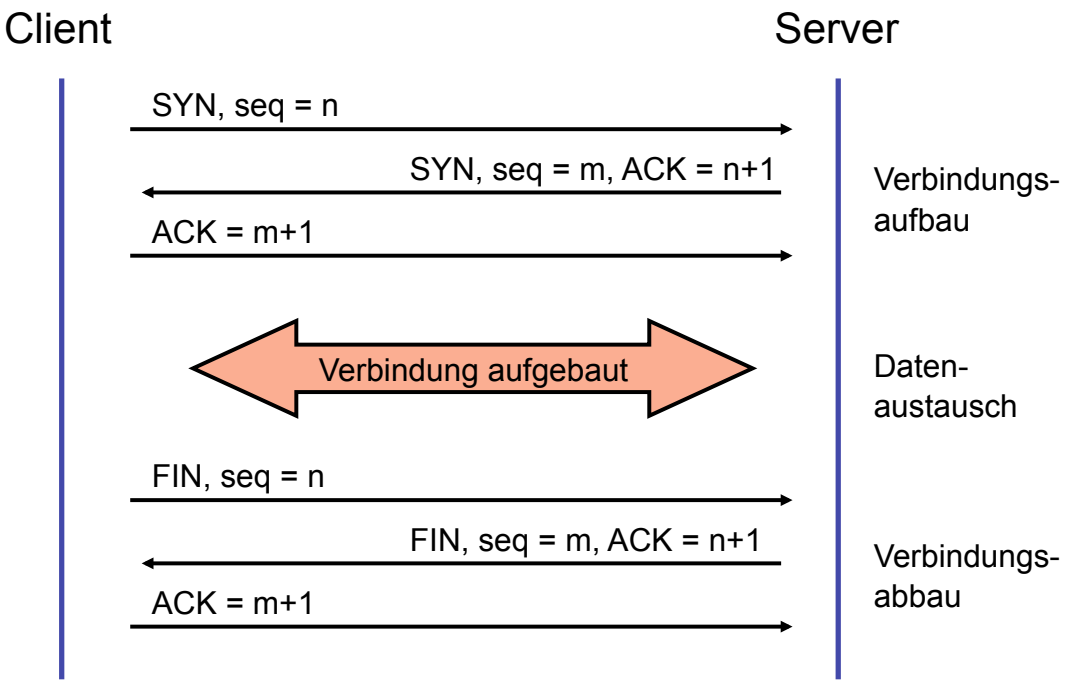


Standard Anwendungen

In einer UNIX-Umgebung werden die verfügbaren Standard-Anwendungen in der Datei: etc/services aufgelistet:

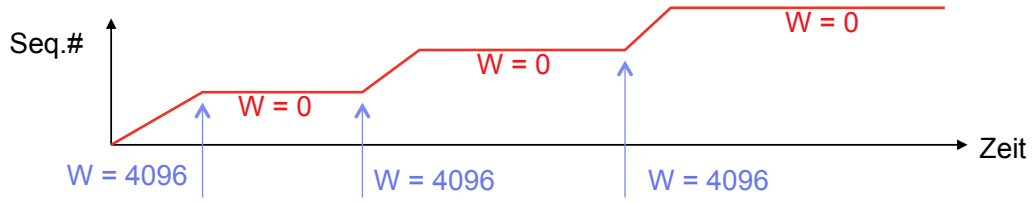
```
ftp-data        20/udp/tcp      # File Transfer [Default Data]
ftp             21/udp/tcp      # File Transfer [Control]
ssh             22/udp/tcp      # SSH Remote Login Protocol
telnet          23/udp/tcp      # Telnet
smtp            25/udp/tcp      # Simple Mail Transfer
tftp            69/udp/tcp      # Trivial File Transfer
www             80/tcp          #www, http
pop3            110/udp/tcp     # Post Office Protocol - Version 3
ntp             123/udp/tcp     # Network Time Protocol
snmp            161/udp/tcp     # SNMP
snmptrap        162/udp/tcp     # SNMPTRAP
ldap            389/udp/tcp     # Lightweight Directory Access Protocol
.....
```

TCP Signalisierung

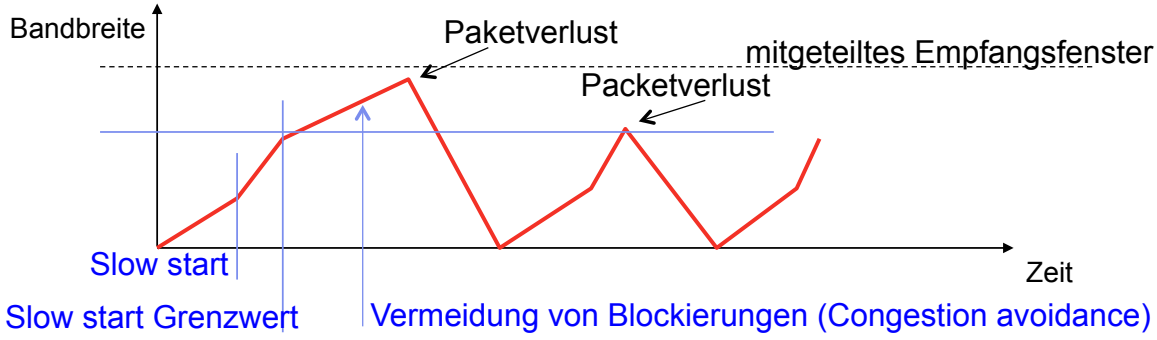


Flusskontrolle / Blockierungs-Kontrolle

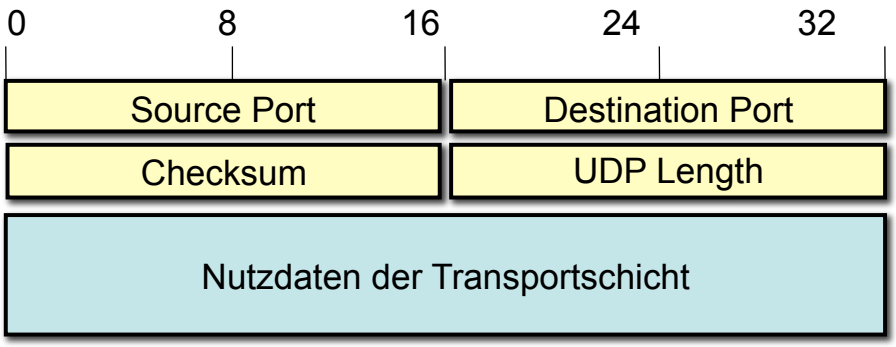
1. Der Empfänger bestimmt die Quittungs-Fenstergröße des Senders



2. Paketverlust:



User Datagram Protocol UDP



RFC 768

- Verbindungslose Kommunikation
- Ungesicherter Datentransport
- Keine Fehlererbehebung bei fehlerhaften Daten
- Für Echtzeitverbindungen geeignet

Kursinhalt

- Einführung: Telekommunikationsprotokolle
- Internet Protokollschichten
- IP Version 4
- Beziehung : MAC-Adresse – IP-Adresse
- IP Adressierung, Subnetze
- Übersicht : IP-Routing
- IP Transportschichten: TCP und UDP
- Internet Control Protocol ICMP

ICMP - Internet Control Message Protocol

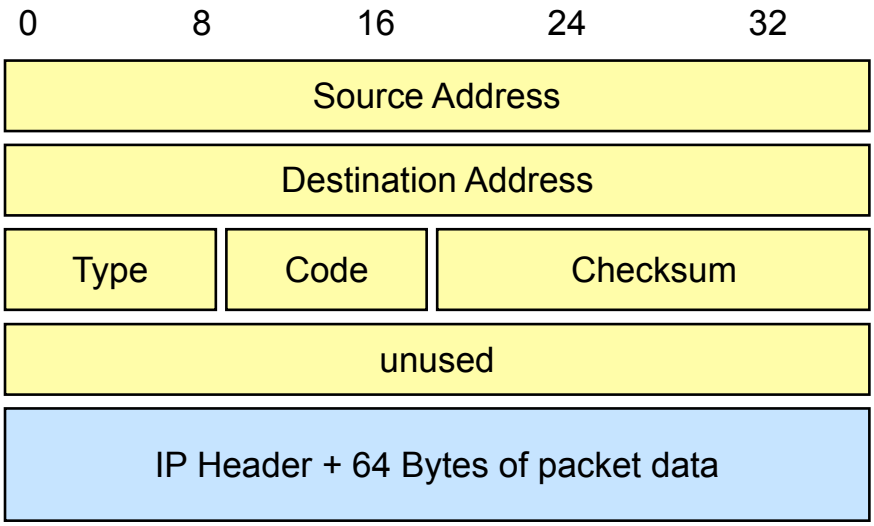
- ICMP ist ein integraler Bestandteil des Internet Protokolls, und muss in jedem IP-Modul implementiert sein. ICMP Protocol-Id = 1
- ICMP Nachrichten zeigen Protokollfehler bei der Verarbeitung von IP-Paketen an.
- ICMP Nachrichten werden in verschiedenen Umständen generiert:
  - wenn ein Paket sein Ziel nicht erreichen kann,
  - wenn ein Netzknoten nicht genug Speicherkapazität besitzt, um ein Paket weiterzuleiten
  - usw…

ICMP Nachrichten

Name der Nachricht		Nr
Destination Unreachable		3
Time exceeded	(TTL-Fehler)	11
Parameter Problem		12
Source Quench		4
Redirect		5
Echo	(z.B. ping)	8
Echo Reply	(z.B. ping)	0
Timestamp		13
Timestamp Reply		14
Information Request		15
Information Reply		16

ICMP Header Beispiel

Nachrichtenname: Destination unreachable (3):



DHBW CAS
Duale Hochschule
Baden-Württemberg
Center for Advanced Studies

Energieinformationstechnik
Teil 2.3 Anwendungsprotokolle

Dr. Leonhard Stiegler

www.dhbw-stuttgart.de

Kursinhalt

- Einführung
- Übersicht Protokolle
  - Stationsautomatisierung IEC 61850
  - Common Information Model IEC 61970
  - Sicherheit IEC 62351
- Anwendungsbeispiel
  - IEC 61850 Raspberry Pi Client – Server Implementierung

Aufgabe von Standards

Internationale Standards

- ermöglichen Interoperabilität und Integration unterschiedlicher Herstellersysteme
- sind hierarchisch und strukturiert aufgebaut und legen fest:
  - Datenstrukturen und Formate
  - Kommunikations-Methoden, Nachrichten und
  - Prozeduren
- erlauben eine effektive System-Konfiguration
- erlauben effektive effektive System-Kommunikation
- ermöglichen einfaches Modellieren von Geräten und Daten
- ermöglichen kostengünstige und skalierbare Lösungen

Normatives Umfeld

Übersicht - Themen der Arbeitsgruppen des IEC TC 57:

- IEC 61850:
  - netzwerkbasierter Feldbus für Schaltanlagen mit Datenmodell (Communications and Associated Data Models)

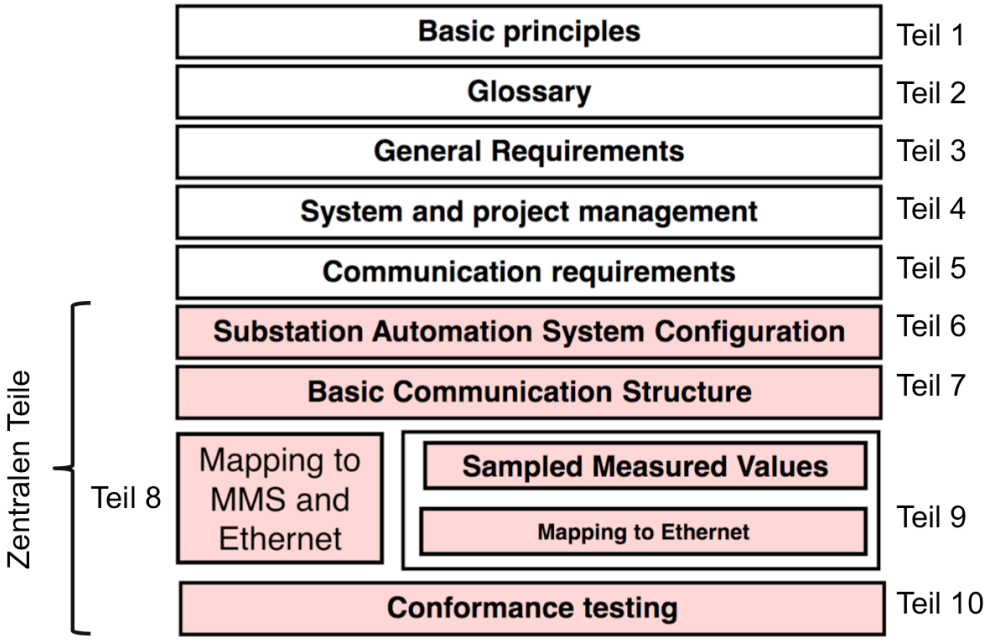
- IEC 61970 Common Information Model:
  - Datenmodelle für den Austausch von Informationen über primäre Betriebsmittel
  - Energy Management Systems – Application Programming Interfaces (API)

TC: Technical Comittee

Kursinhalt

- Einführung
- Übersicht der Protokolle
  - Stationsautomatisierung IEC 61850
  - Common Information ModelI IEC 61970
  - Sicherheit IEC 62351
- Anwendungsbeispiel
  - IEC 61850 Raspberry Pi Client – Server API

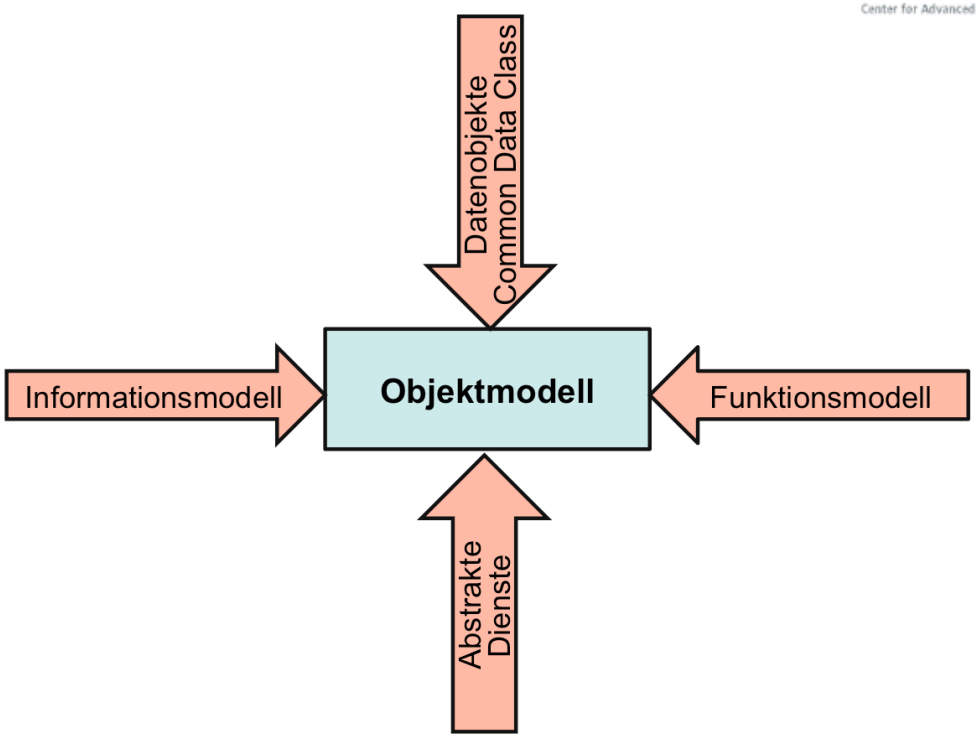
IEC61850 Aufbau des Standards



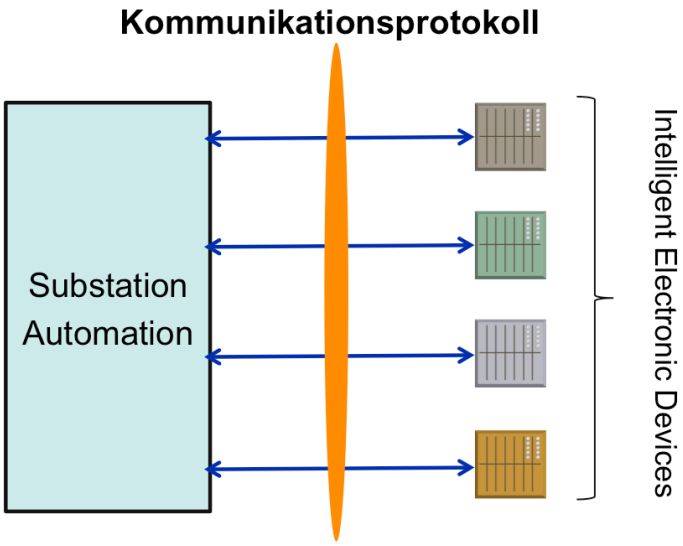
Zentrale Teile des IEC 61850 Standards

Part 6-1:	Substation Configuration Language (SCL)
Part 7-2:	Abstract Communications Service Interface (ACSI) and base types
Part 7-3:	Common Data Classes (CDC)
Part 7-4:	Logical Nodes
Part 8-1:	Specific Communications Service Mappings (SCSM) MMS & Ethernet
Part 9-2:	SCSM Sampled Values over Ethernet
Part 10-1:	Conformance Testing

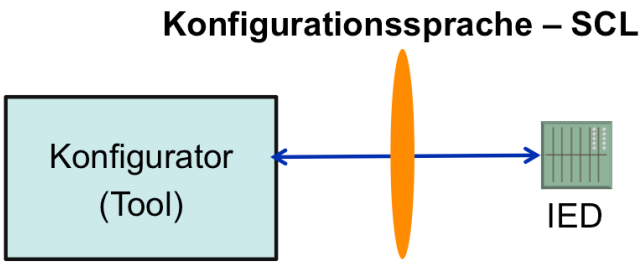
IEC 61850 Kernkomponenten (1)



IEC 61850 Kernkomponenten (2)



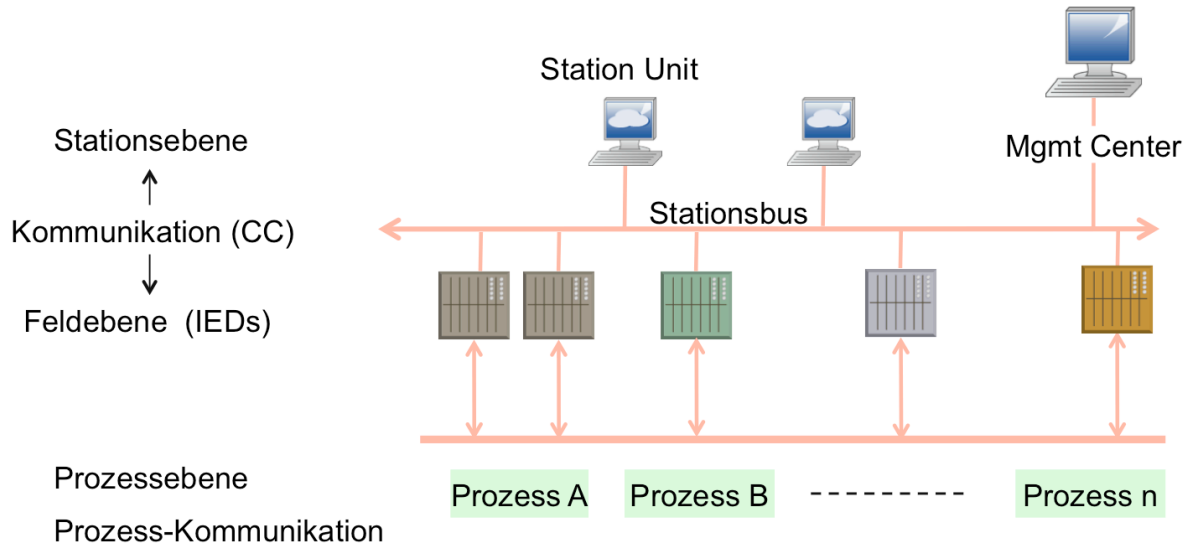
IEC 61850 Kernkomponenten (3)



IED = Intelligent Electronic Device

IEC 61850 Übersicht

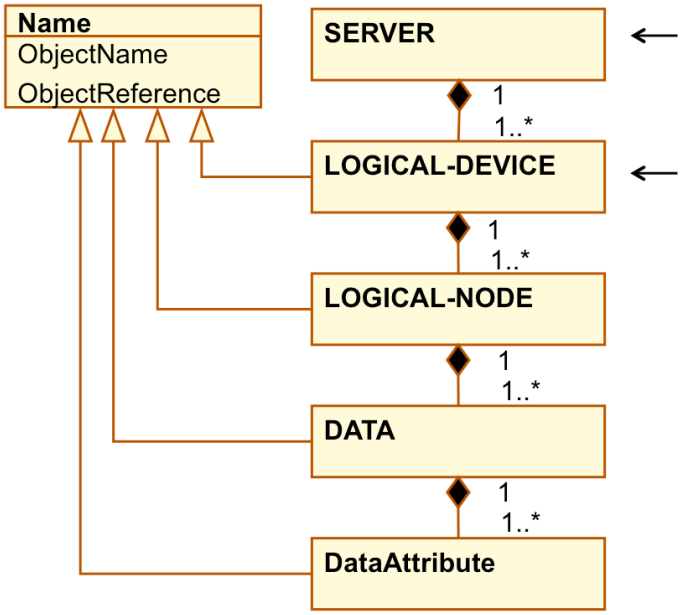
Die Norm IEC 61850 definiert die Kommunikation zwischen Geräten in der Stationsautomatisierung elektrischer Stromerzeuger



IEDs :

- sind Microprocessor-basierte Geräte, wie z.B. Leistungsschalter, Schutzrelais, etc.
- empfangen Daten z.B. von Sensoren oder Messeinrichtungen
- aktivieren Steuerungskommandos in geeigneten Situationen zur Aufrechterhaltung der gewünschten Systemzustände

IEC 61850 Objektmodell : Klassen



Physical Device:
Zugang über die Netzadresse

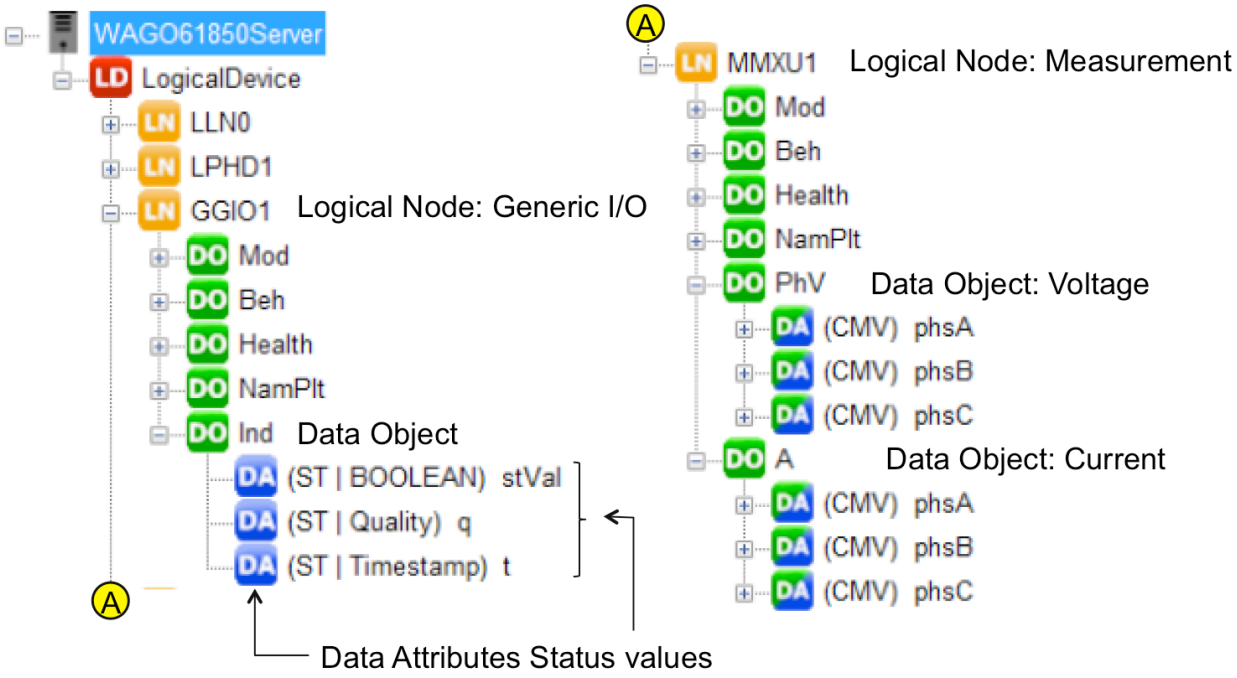
Daten mehrerer Logical Devices können in einem einzigen Physical Device zusammenfließen (data concentrator)

Notes:

Objektmodell : Logical Node Types

Name	Funktion
Axxx	Automatic Control (4). ATCC (tap changer), AVCO (volt. ctrl.), etc.
Cxxx	Supervisory Control (5). CILO (Interlocking), CSWI (switch ctrl), etc.
Gxxx	Generic Functions (3). GGIO (generic I/O), etc.
Ixxx	Interfacing/Archiving (4). IARC (archive), IHMI (HMI), etc.
Lxxx	System Logical Nodes (2). LLN0 (common), LPHD (Physical Device)
Mxxx	Metering & Measurement (8). MMXU (meas.), MMTR (meter.), etc.
Pxxx	Protection (28). PDIF, PIOC, PDIS, PTOV, PTOH, PTOC, etc.
Rxxx	Protection Related (10). RREC (auto reclosing), RDRE (disturbance)..
Sxxx	Sensors, Monitoring (4). SARC (archs), SPDC (partial discharge), etc.
Txxx	Instrument Transformer (2). TCTR (current), TVTR (voltage)
Xxxx	Switchgear (2). XCBR (breaker), XCSW (switch)
Yxxx	Power Transformer (4). YPTR (transformer), YPSH (shunt), etc.
Zxxx	Other Equipment (15). ZCAP (cap ctrl), ZMOT (motor), etc.
Wxxx	Wind (Set aside for other standards)
Oxxx	Solar (Set aside for other standards)
Hxxx	Hydropower (Set aside for other standards)
Nxxx	Power Plant (Set aside for other standards)
Bxxx	Battery (Set aside for other standards)
Fxxx	Fuel Cells (Set aside for other standards)

Datenobjekte - Beispiel

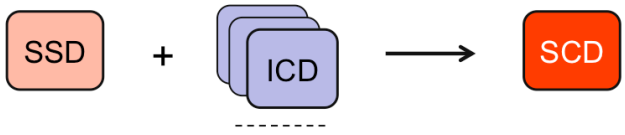


Substation Configuration Language – SCL

- IEC61850-6-1 **SCL**
- Beschreibungssprache für die IED Kommunikation
- XML basiert
- Erlaubt die formale Beschreibung eines:
  - Substation Automation System und die
  - Konfiguration eines IED

Substation Configuration – SCL

- Substations (IEDs) werden mittels der SCL – Sprache (Substation Configuration Language) beschrieben
- SCL ist durch IEC61870-6 spezifiziert
- SCL Dateiarten:
  - **ICD** (IED Capability Description)
    enthält die Systemkonfiguration eines IED, opt. Kommunikation
  - **SSD** (System Specification Description)
    logical nodes, data type templates
  - **SCD** (Substation Configuration Description)
    alle Informationen (data types, IED, communication, logical nodes



Configured IED Description (CID)

Instantiated IED Description (IID) file:

System Exchange Description (SED) file

Kommunikationsmodell : IEC 61850-7

Der Teil IEC 61850-7 (Basic Communication Structure) definiert und spezifiziert :

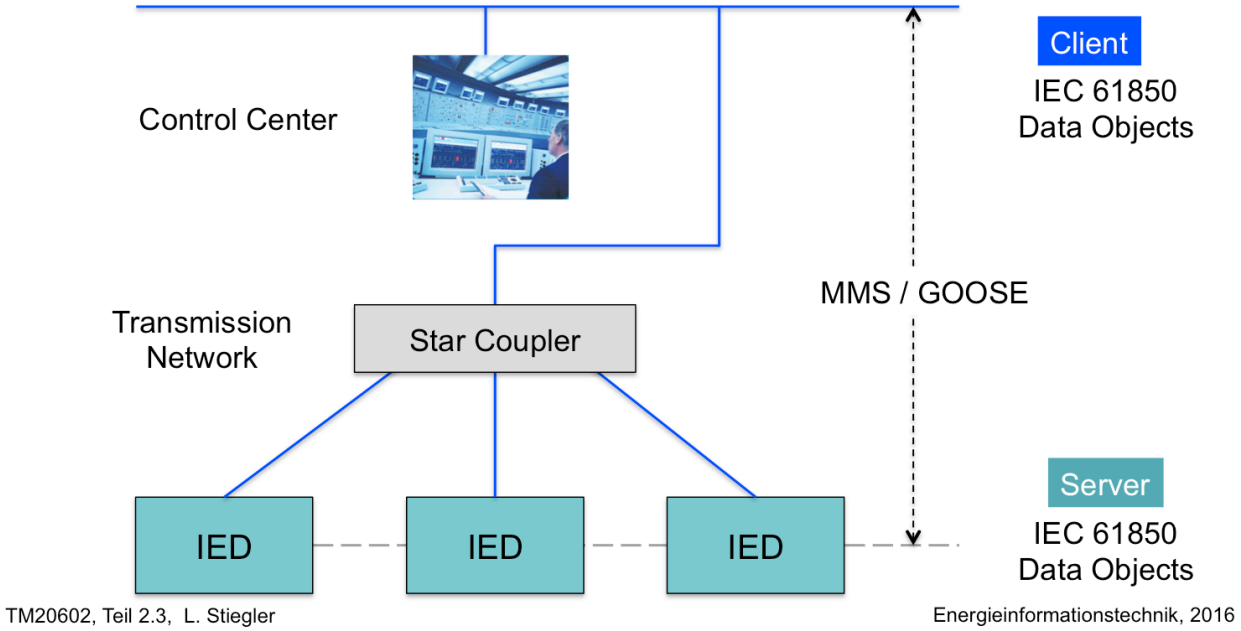
- die grundlegende Kommunikationsstruktur
- das grundlegende Objektmodell
- Kommunikationsprinzipien
- die abstrakte Schnittstelle (API) für Kommunikationsdienste
- die Kommunikationsdienste
- ein Modell der Server-Datenbank
- abstrakte gemeinsame Datenklassen
- das Konzept der logische Knoten (logical nodes)

Kommunikationsrollen

- **Client**
  - empfängt Daten vom Server (z.B. Mess- und Statistik-Daten, ...)
  - aktiviert Prozeduren (z.B. Steuerung, Abfragen, ...)
  - verarbeitet Mess- und Statistik-Daten
  - besitzt i.d.R. Management-Funktion
- **Server**
  - kontrolliert physikalische Schnittstellen
  - führt Steuerungskommandos durch
  - verarbeitet Messdaten (Umrechnungen, Grenzwertanalyse, ...)
  - besitzt i.d.R IED Funktion
- **API**
  - Programmierschnittstelle zwischen Client und Server
  - führt das Kommunikationsprotokoll durch
  - wird durch eine SCD-Datei beschrieben

IEC 61850 Kommunikationsmodell

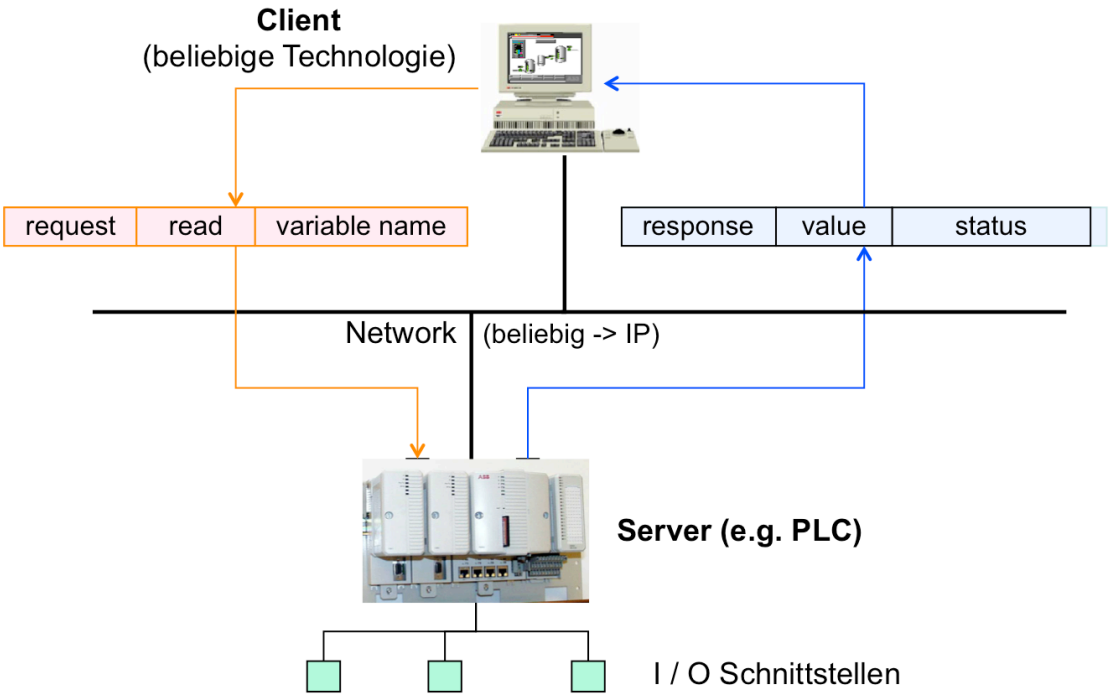
IEC 61850 Client – Server Kommunikation zwischen IED und Control Center



This system must have software that can interpret the IEC 60870-5-103 communication messages

IEC 60870-5-103 defines communication for a serial, unbalanced link only. Communication speeds are defined as either 9600 or 19200 baud

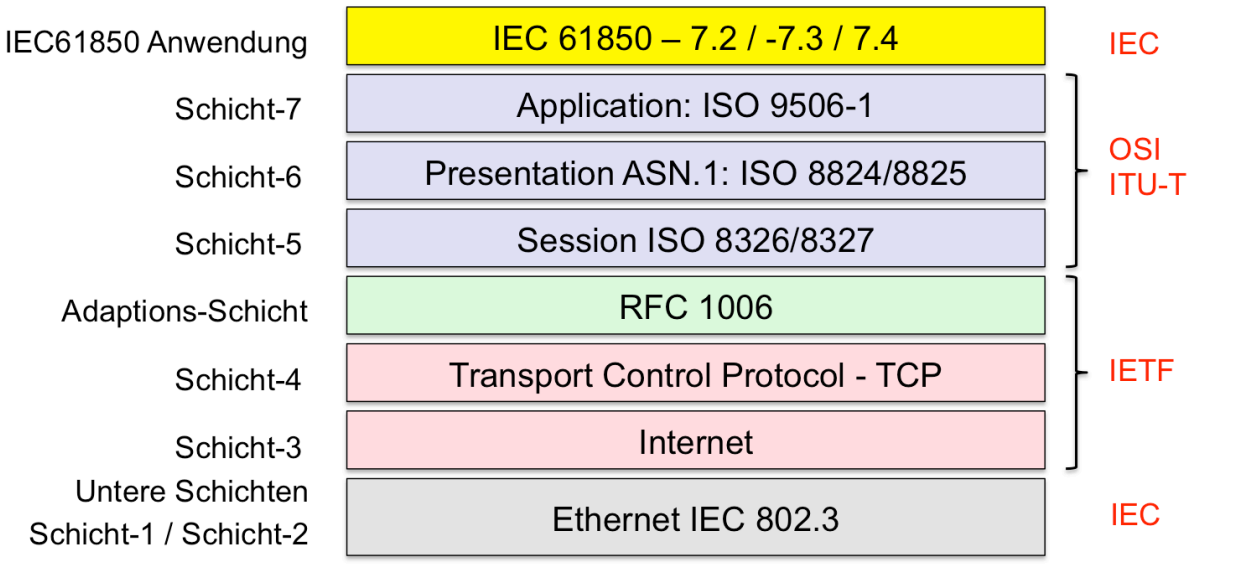
MMS – Kommunikation



PLC = Programmable Logical Controller
MMS: R/W Gerätevariablen mittels Standard-Nachrichten (Protocol Data Units = PDU)

MMS Protokollschichten

Spezifikation: IEC 61850 Part 8-1:
Specific communication service mapping (SCSM) – Mappings to **MMS** (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3



Developed 1980 (!) for the MAP project (General Motor's flexible manufacturing initiative)
Originally unluckily tied to the OSI communication stack and Token Bus (IEEE 802.4)
Reputed for being heavy, complicated and costly due to poor implementations.
Boeing adopted MMS as TOPs (MMS on Ethernet) - a wise step.
Adopted by the automobile industry, aerospace industry, and PLC manufacturers: Siemens, Schneider, Daimler, ABB.
Standardized since 1990 as: ISO/IEC 9506-1 (2003): Industrial Automation systems - Manufacturing Message Specification -
Part 1: Service Definition
Part 2: Protocol Specification

MMS has been during its 15 years of existence a reference model for industry rather than an actual implementation.
Its high complexity makes it very general, but the requested bandwidth and computing power were out of reach until few years ago.
It is - sometimes as a proprietary version - part of every PLC today.
It gave rise to several other "simpler" models (DLMS, BacNet, FMS....)
It is the base of IEC 61850 „Communication networks and systems in substations", which bases on TCP/IP/Ethernet.

Kursinhalt

- Einführung
- Übersicht Protokolle
  - Stationsautomatisierung IEC 61850
  - Common Information Model IEC 61970
  - Sicherheit IEC 62351
- Anwendungsbeispiel
  - IEC 61850 Raspberry Pi Client – Server Implementierung

Common Information Model – CIM

- CIM ist ein Satz von Standards, der eine Systemintegration und einen Informationsaustausch basierend auf einer gemeinsamen „Sprache“ ermöglicht.
- Hauptstandards:
  - IEC 61970
    EMS Application Program Interface (EMS-API)
  - IEC 61968
    System Interfaces for Distribution Management
  - IEC 62325
    Framework for Energy Market Communication
- Ziel:
  - gemeinsames Informationsmodell, welches das elektrische Netz definiert
- Schnittstellen werden über Profile definiert

Informationsmodell:
- Allgemeines Modell aller Objekte eines EVU und deren Beziehungen untereinander
- Anwnedungsunabhängig

Kontextabhängigkeit:
- legt fest, welche CIM-Teile für ein bestimmtes Profil benutzt werden
- besteht aus vorgeschriebenen und optionalen Informationen und Einschränkungen
- erzeugt jedoch keine zusätzlichen Informationen

Die **Syntax** beschreibt das Format für die Instanzdaten

Ein **Profil**
- ist eine kontextabhängige, auf einen konkreten Anwendungsfall bezogene Untermenge des darunterliegenden semantischen Modells.
- spezifiziert die Informationsstruktur der auszutauschenden Information
- betrifft in der Regel mehrere Schnittstellen
- wird als Funktionsmerkmale von Produkten unterstützt z.B. CIM/XML Import/Export, ESB Adapter

Profile bilden die Grundlage für Interoperabilitätstests (IOP)

CIM – Beschreibung

- CIM wurde entwickelt durch die Technical Committee TC 57 der IEC
- CIM ist durch den IEC-Standard 61970 spezifiziert
- CIM beschreibt die Programmierschnittstelle (API) für Energie-Managementsysteme
- CIM ist objekt-orientiert, UML-Objekte und Datenaustauschformate für
  - Übertragung,
  - Verteilung und
  - Erzeugung von Energie
- IEC TC 57 Arbeitsgruppen:
  - WG 13 : IEC 61970
    Energy management systems - Application Program Interfaces
  - WG10 : IEC 61850
    IED communications & associated data models in power systems

Klassen beschreiben :
- Objekte
- ihre Eigenschaft und
- ihre Beziehungen mit anderen Objekten

Beispiel: Transformator – in Unterstationen enthalten – besitzen eindeutige Namen – arbeiten unter Betriebsspannungen, etc.

Instanzen beschreiben die spezifischen Objekte einer Klasse, die im System existiert

IEC 61850 und IEC 61970 CIM

IEC 61850

- Einheitliche Darstellung der Sekundärtechnik (Schutz, Regler, Überwachung)
- Schwerpunkt: Schaltanlagen (Feldebene)
- Datenmodell als Dokument verfügbar (IEC Standard)

IEC 61970 Common Information Model (CIM)

- Einheitliche Darstellung der Primärtechnik (IEC 61970-301 definiert CIM)
- Schwerpunkt: Leittechnik (Betrieb) und Pflege der Betriebsmittel
- Datenmodell direkt im UML-Format verfügbar (IEC Standard)

Kursinhalt

- Einführung
- Übersicht Protokolle
  - Stationsautomatisierung IEC 61850
  - Common Information Model IEC 61970
  - Sicherheit IEC 62351
- Anwendungsbeispiel
  - IEC 61850 Raspberry Pi Client – Server Implementierung

Sicherheit in Energiemanagementsystemen

- **IEC 62351** wurde von der WG 15 der IEC TC 57 entwickelt
- **IEC 62351** behandelt die Sicherheit der TC 57 Standards
- **IEC 62351** ist der aktuellste Standard für Sicherheit in Energiemanagementsystemen
- **IEC 62351** umfasst auch die Datenkommunikation
- **IEC 62351** beschreibt Maßnahmen zur Erfüllung der Grundforderungen an sichere Datenkommunikation / Datenverarbeitung:
  - Vertraulichkeit
  - Datenintegrität
  - Authentifizierung und
  - Unleugbarkeit (non-Repudiation)
- **IEC** 62351 definiert Rollenprofile mit unterschiedlichen Zugriffsrechten

IEC 62351 schließt die Standard-Serien: IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 und IEC 61968 ein.

IEC 62351 Aufbau des Standards (1)

- Teil-1
  - Übersicht über das Gesamtdokument **IEC 62351** und Einführung in die informationstechnischen Sicherheitsaspekte für den Betrieb von Stromversorgungsanlagen
- Teil-2:
  - Glossar
- Teil-3:
  - Ende-zu-Ende Absicherung des Datenverkehrs für TCP/IP-basierte Verbindungen
  - Verwendung von TLS [RFC5246]
  - Client und Server Authentifizierung auf Basis von X.509-Zertifikaten

IEC 62351 Aufbau des Standards (2)

- Teil-4
  - Sicherheitsmaßnahme für MMS-basierte Protokolle (z.B. IEC 60870-6, IEC 61850)
  - Absicherung der Transportschicht gemäß IEC 62351-3
  - Definition eines Authentifizierungsmechanismus "SECURE" auf der Anwenderschicht für MMS-Assoziationen unter Verwendung von X. 509-Zertifikaten
- Teil-5:
  - Sicherheit für IEC 60870-5 und abgeleitete Protokolle (z.B. IEC 60870-5-104 / IEC 60870-5-101 / DNP 3.0) auf der Anwenderschicht
  - Zugriffsberechtigung auf kritische Ressourcen einer Unterstation
  - Rollen-basierten Zugriffsbeschränkungen (RBAC) und Erfassung sicherheitsrelevanter Ereignisse in Statistiken.

IEC 62351 Aufbau des Standards (3)

- Teil-6
  - Sicherheit für das IEC61850-Protokoll
  - Einsatz von VLAN-Markierungen und X.509-Signaturen bei GOOSE- und SMV-Telegrammen
- Teil-7
  - Sicherheit durch Einsatz von Tools zur Netzwerk- und Systemverwaltung, um eine
  - Überwachung der Stromnetz-Infrastruktur
  - Verwendung von MIB-Definitionen für IEDs
  - herstellerunabhängige relevante Systeminformationen bezüglich des Gerätes und der Kommunikationslinien
  - Verwendung des SNMP-Protokolls zum Austausch von MIB-Objekten

MIB: Management Information Base

IEC 62351 Aufbau des Standards (3)

- Teil-8
  - IEC 62351-8
    Definition von Methoden zur Verarbeitung und Verwaltung von Zugriffsrechten für Benutzer und Dienste
  - Rollen-basierten Zugriffskontrollsystems (RBAC)
  - vordefinierte Standard-Rollen und die Zugriffsrechte im Kontext von IEC 61850 (z.B. Auflistung aller Objekte in einem "Logischen Gerät")
  - Austausch von Identitätsinformation und Rollenname als ASN.1 Zugriff-Token
  - zentrale Verwaltung der Zugangsdaten über ein LDAP-System
  - Zugriff (PUSH- / PULL-Mechanismus) auf die Identitätsinformation des Kommunikationspartners

Die Identitätsinformation sowie der Rollenname wird in einem Zugriff-Token (ASN. 1-Syntax) abgelegt, der mit Hilfe verschiedener Transportmechanismen (X.509-Zertifikate, X.509-Attribut-Zertifikate, Software-Token) auf eine kryptographisch sichere Art zwischen den Systemen ausgetauscht

IEC 62351 Vordefinierte Rollen und Rechte

Value	Role \ Right	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTING GROUP	SECURITY
<0>	VIEWER	X			X							
<1>	OPERATOR	X	X		X				X			
<2>	ENGINEER	X	X	X	X		X	X		X		
<3>	INSTALLER	X	X		X		X			X		
<4>	SECADM	X	X	X			X	X	X	X	X	X
<5>	SECAUD	X	X		X	X						
<6>	RBACMNT	X	X					X		X	X	
<7 ... 32767>	Reserved	For future use of IEC defined roles.										
<32768 ... -1>	Private	Defined by external agreement. Not guaranteed to be interoperable.										

IEC 62351 Aufbau des Standards (4)

- Teil-9 : „Cyber Security“
  - Schlüssel-Management für Stromversorgungsanlagen,
  - korrekten und sicheren Umgang mit sicherheitskritischen Parametern, z.B. Passwörter, Verschlüsselungsschlüssel
  - Lebenszyklus von kryptografischer Information: Anmeldung, Erstellung, Verbreitung, Installation, Verwendung, Lagerung und die Entfernung
  - Umgang mit digitalen Zertifikaten (öffentlicher / privater Schlüssel)
  - Infrastruktur (PKI, X.509-Zertifikate) für asymmetrische Verschlüsselungsverfahren
  - Mechanismen bezüglich:
    - Zertifikatsanforderung (SCEP, CMP)
    - Zertifikatssperrung (CRL, OCSP)

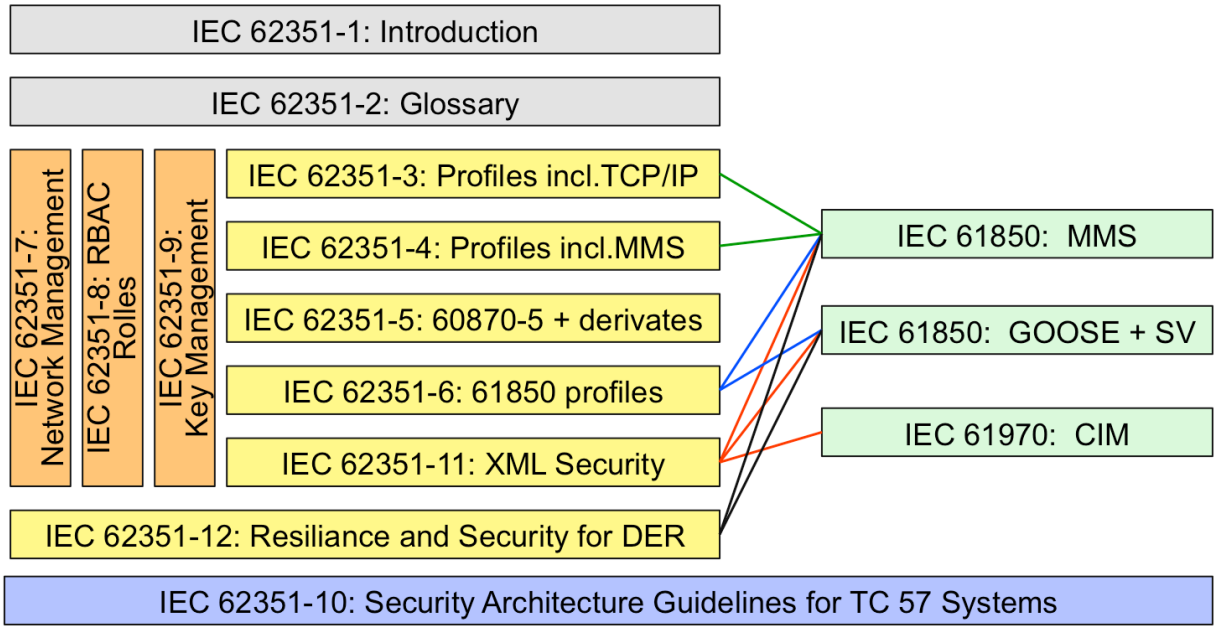
Bei Verwendung von symmetrischen Schlüsseln (z.B. Sitzungsschlüssel) wird ein Mechanismus zur sicheren Verteilung basierend auf GDOI [RFC6407] und IKEv2 [RFC7427] vorgestellt.

IEC 62351 Aufbau des Standards (5)

- Teil-10 : Sicherheitsarchitekturen
  - Sicherheits-Architekturen für die gesamte IT-Infrastruktur,
  - spezielle Sicherheitsanforderungen aus dem Umfeld der Stromerzeugung.
  - Identifizierung kritischer Stellen in der Kommunikationsarchitektur (z.B. Leitstelle zum Umspannwerk, Umspannwerk-Automatisierung)
  - geeignete Sicherheitsmechanismen (z.B. Datenverschlüsselung, Benutzerauthentifizierung)
  - Anwendung des Mechanismus' aus **IEC 62351** und bewährte Standards aus dem IT-Bereich (z.B. VPN Tunnel, Secure FTP, HTTPS)
- Teil-11
  - Sicherheit für XML-Dateien
  - Einbettung des originalen XML-Inhalts in einen XML-Container

Der XML Container ermöglicht wahlweise Verschlüsselung, X.509-Signatur für die Authentizität der XML-Daten

IEC 62351 Zuordnung



DER: Distributed Energy Resources

Weitere IEC 62391 Technical Reports und Standards:

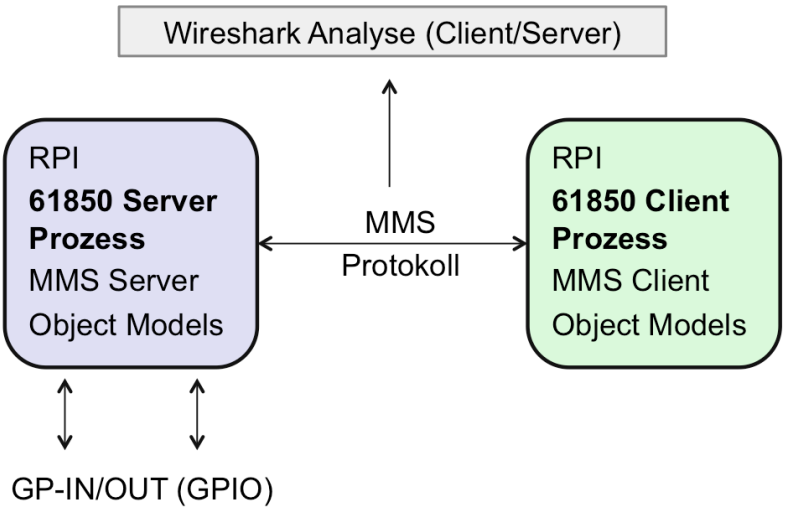
- IEC/TR 62351-13: Guidelines on What Security Topics Should Be Covered in Standards and Specifications
- IEC/TR 62351-90-1: Guidelines for Using Part 8 Roles
- IEC 62351-100-1: Conformance test cases for IEC 62351-5 and companion standards
- IEC 62351-14 Security Event Logging and Reporting
- IEC/TR 62351-90-2 Deep Packet Inspection

Kursinhalt

- Einführung
- Übersicht Protokolle
  - Stationsautomatisierung IEC 61850
  - Common Information Model IEC 61970
  - Sicherheit IEC 62351
- Anwendungsbeispiel
  - IEC 61850 Raspberry Pi Client – Server Implementierung

Open Source Bibliothek : libIEC61850

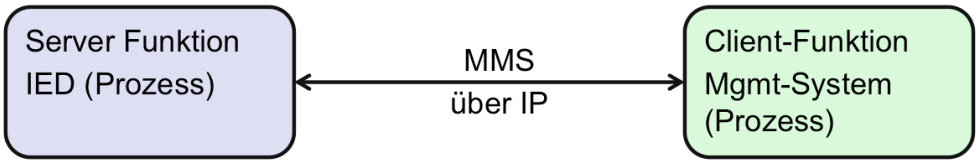
- IEC 61850 Client API mit MMS-client API
- IEC 61850 Server API mit MMS-server API



Notizen:

libice61850 Software

- API für Raspberry PI
- Application Programming Interface – API Implementierung
  - Client – Server Impelentierung für IEC 61850 Anwendungen
  - MMS Protokollstack für TCP/IP und GOOSE
  - Substation Configuration Description (SCD-File) wird bei der Software Produktion (nicht während der Kommunikation) verarbeitet



- Client / Server – Beispielprogramme
- Automatische Generierung des Server-Modell Codes static_model.c und static_model.h aus der icd - Datei

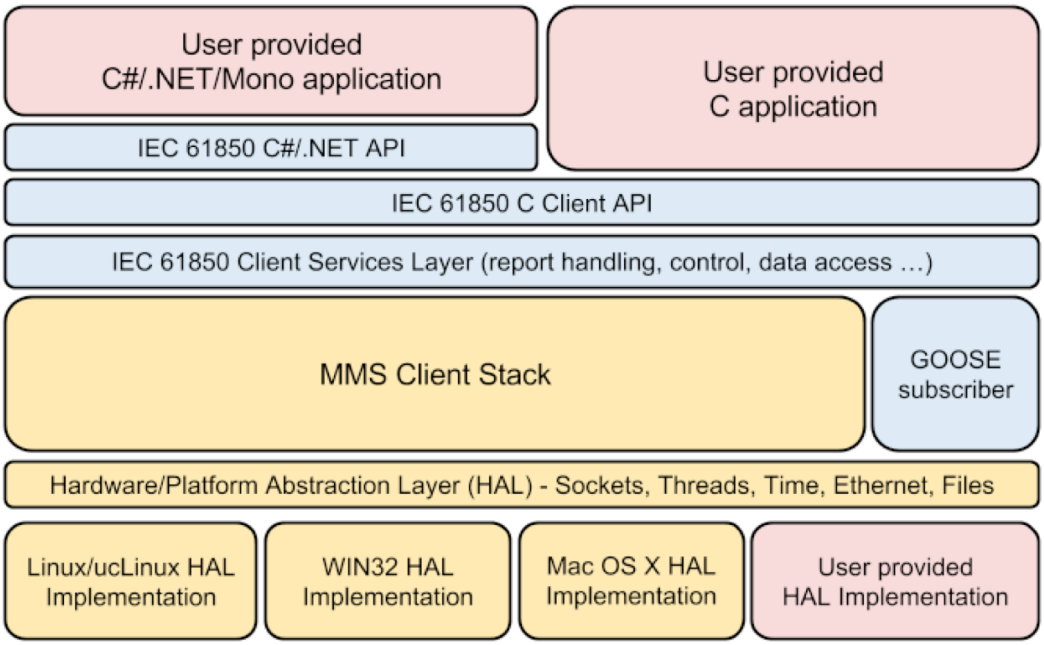
Für die Software gibt es verschiedene Testbeispiele:

- iec61850_client_example1
- iec61850_client_example2
- iec61850_client_example3 <- kann für alle Server-Beispiele verwendet werden
- iec61850_client_example4
- iec61850_client_example5

- server_example1
- server_example2
- server_example3
- server_example4
- server_example5

} IED Funktion / Konfiguration

Client Protokollstack

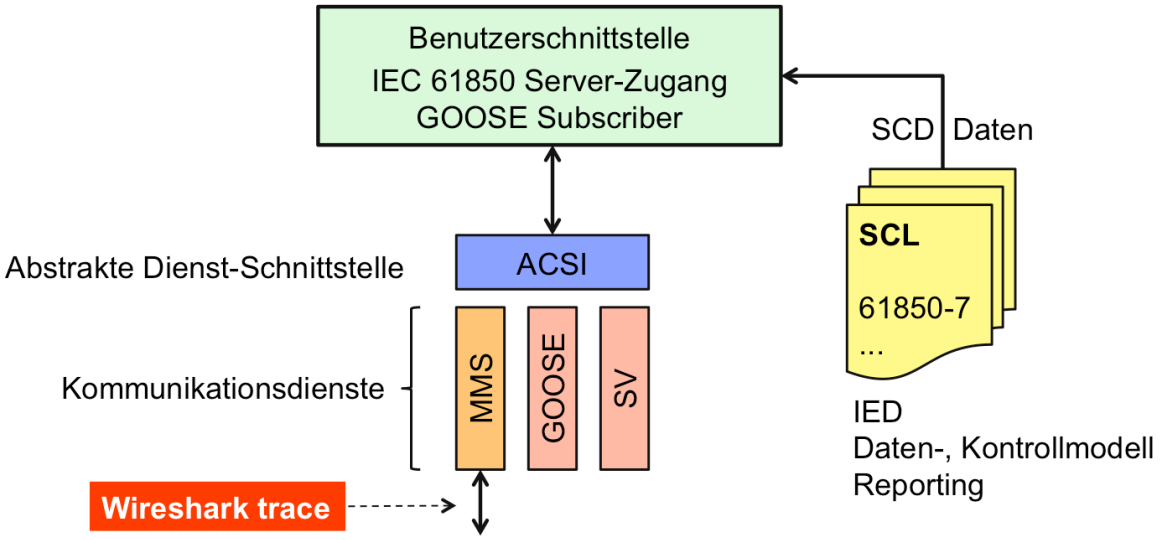


HAL-Schichten: Hardware Abstraction Layer
Anpassungsschicht an die jeweils verwendeten Betriebssysteme

MMS Server Stack: MMS-Protokollschichten

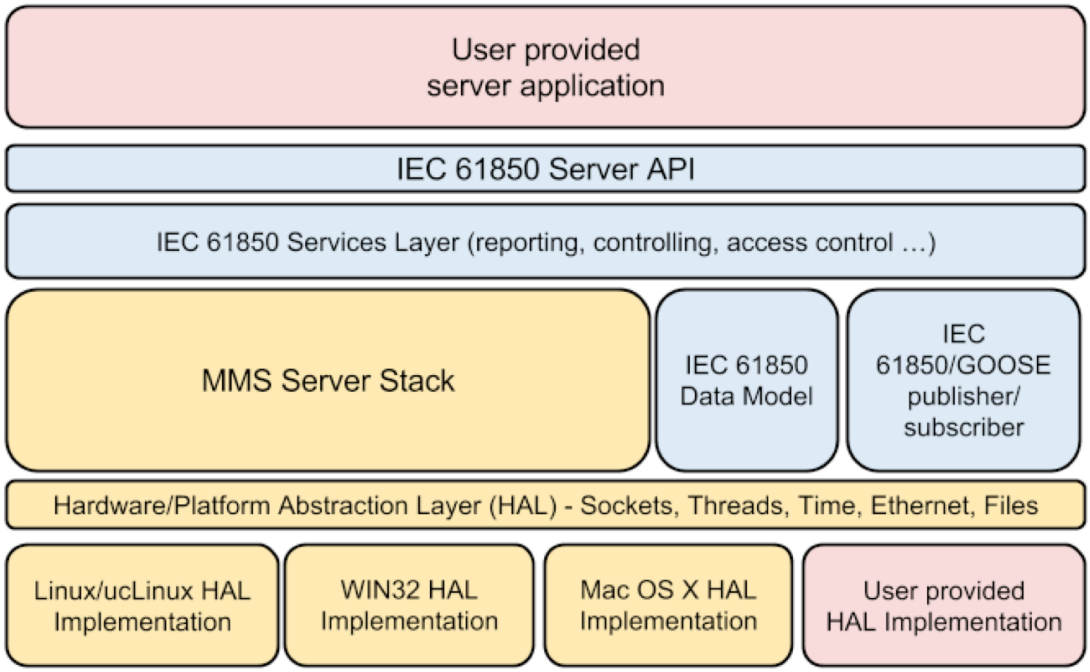
Client Anwendung

- Client API gemäß IEC 61850 ACSI (Abstract Communication Service Interface IEC 61850-7-2)
  - Kommunikationsmethoden: MMS, GOOSE, SV



Als Benutzerschnittstelle wird während des Tests die Unix-Shell verwendet.
Client und Server befinden sich auf der selben Raspberry Hardware und kommunizieren intern über das Loopback-Interface (127.0.0.1).
Die Kommunikation wird mittels Wireshark überprüft.

Server Protokollstack

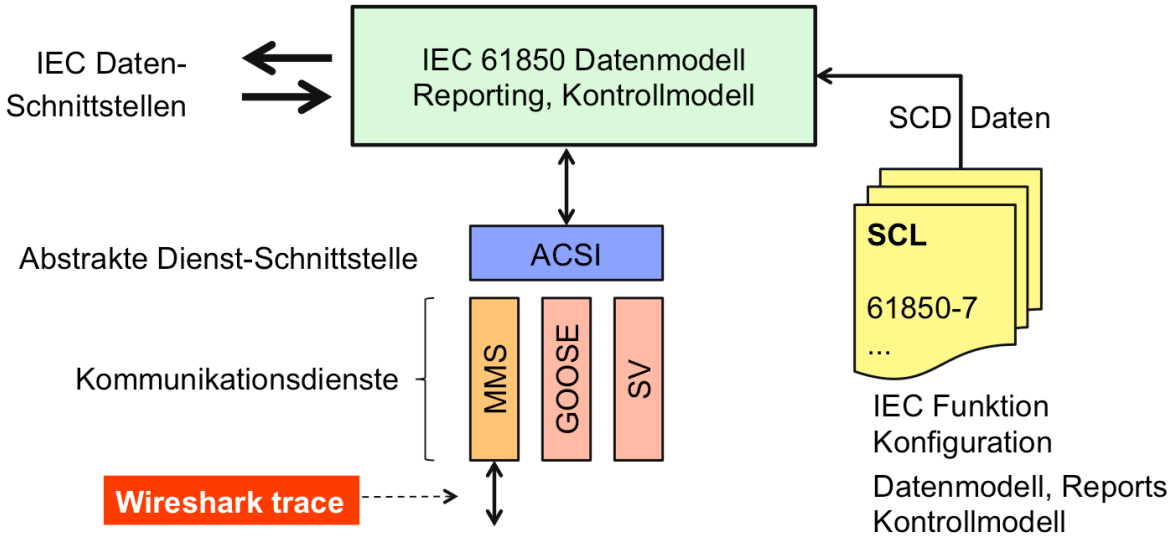


HAL-Schichten: Hardware Abstraction Layer unterstützt die Portierung auf unterschiedliche Hardware Plattformen
Anpassungsschicht an die jeweils verwendeten Betriebssysteme

MMS Server Stack: MMS-Protokollschichten
IEC 61850 Datenmodell: wird durch Konfigurationsdateien (SCD, ICD, CID) beschrieben

Server Anwendung (IDE)

- Server API gemäß IEC 61850 ACSI (Abstract Communication Service Interface IEC 61850-7-2)
  - Kommunikationsmethoden: MMS, GOOSE, SV



Die Server-Anwendung bildet die IED-Funktionen ab.
Client und Server befinden sich auf der selben Raspberry Hardware und kommunizieren intern über das Loopback-Interface (127.0.0.1).
Die Kommunikation wird mittels Wireshark überprüft.

Die IED-Testbeispiele verwenden keine Raspberry – Ressourcen, wie z.B. GPIO-Pins Systemdaten, etc. Die Testbeispiele können durch die Implementierung entsprechender Software-Funktionen erweitert werden.

Zugang zum Raspberry Pi

- Zugang über **Putty** (ssh) oder über ein Linux **shell-Fenster**
  - ssh pi@<IP-Adresse des Raspberry Pi>
  - Passwort: raspi
  - Raspberry Pi Kommando-Promt

  } ssh remote access
- Alternativ: über eine Remote Desktop (xrdp) Verbindung
- **Protokollanalyse – Tool für MMS-Nachrichten**
  - Analysetool: wireshark
    - Raspberry – Version kann MMS (noch) nicht dekodieren
  - **Workaround**:
    - Verwendung der dumpcap – Trace-Funktion:
      Programmaufruf ohne Parameter: **sudo dumpcap - i lo**
      erzeugt ein pcap-Dateiformat im /tmp-Verzeichnis
    - kopieren der pcap-Datei auf den PC (mit mc etc.)
      Analyse auf dem lokalen PC mit Wireshark

Verwendung der libice61850 Beispiele

- Verzeichnis auf dem Raspberry Pi:
  - /home/pi/IEC61850/libiec61850-0.9.2.1
- Verzeichnis der **Beispiele:**
  - libiec61850-0.9.2.1/examples
- Die Beispiele bestehen aus Client – Server Programmen die auch auf einem Raspberry (IP = 127.0.0.1 localhost) gegeneinander ablaufen können
  - **Client-Dateien**: Iec61850_client_example1 ... 5
  - **Server-Dateien**: server_example1 ... 5
  - **MMS-Utility**: (Client-Funktion): examples/mms_utility

iec61850 Beispiele

- Inhalt der Verzeichnisse
  - **Client** :

Verzeichnis:	z.B. *iec61850_client_example2*
ausführbare Datei:	client_example2
C-Code:	client_example2.c
Compiler-Dateien:	Makefile und CMakeLists

  - **Server**:

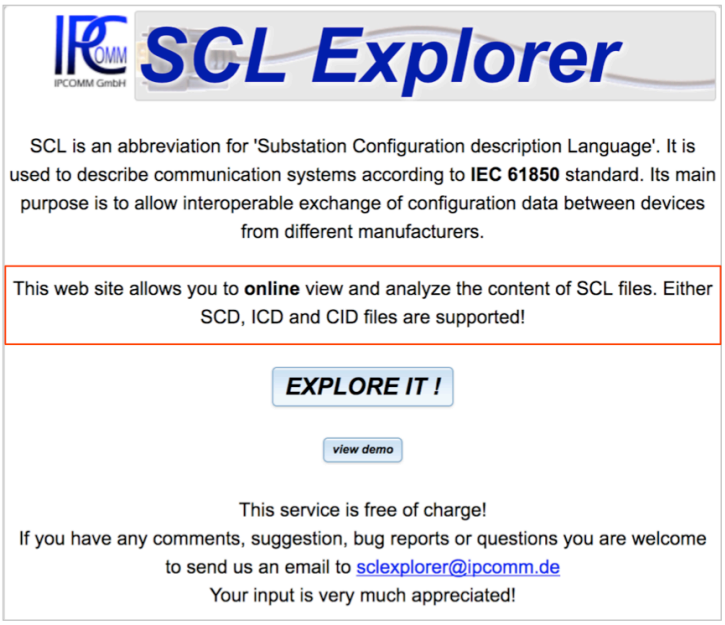
Verzeichnis:	z.B. *server_example3*
ausführbare Datei:	server_example3
C-Code:	server_example3.c
Datenmodell-Beschreibung:	static_model.h, static_model.c
ICD-Datei:	simpleIO_direct_control.icd
Compiler-Dateien:	Makefile und CMakeLists

- Auswertung / Analyse der ICD-Datei mit Hilfe von Tools wie z.B. IEDScout oder der Online-Analyse von IPComm.

Darstellung der ICD – Struktur

Auswertung von SCL-Dateien (alternativ auch über IEDScout):

- http://www.scl61850.com/-XbgiB-3_View



ICD Analyse:

- Analysieren Sie die Struktur der ICD-Datei von Server3:
  - Datenobjekte in LLN0
  - Kommunikations-Parameter
  - LN-Types
  - Data Type Templates

Die verwendeten IED-Funktionen können mittels SCD-, ICD-, oder CID-File beschrieben werden. Die vorliegenden Beispiele verwenden das ICD-Fileformat.

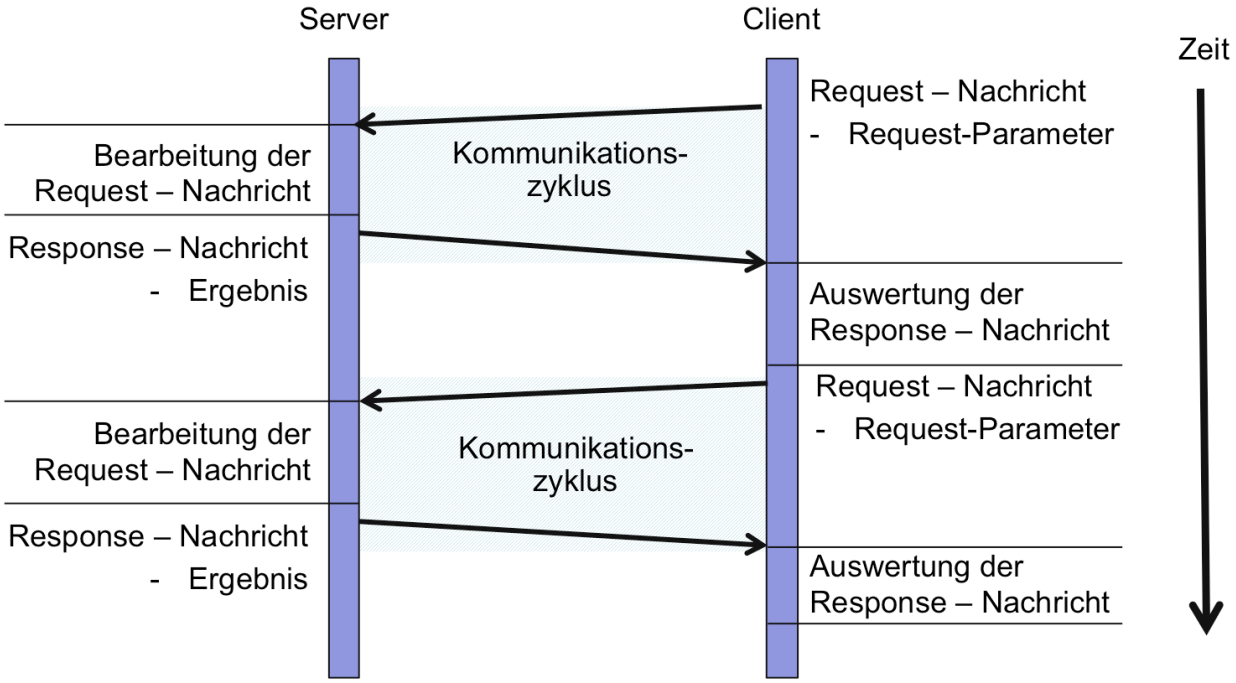
Änderungen können mittels geeigneter Tools (IEDScout) durchgeführt werden. Kleinere Anpassungen manuell in der XML-Datei.

MMS – Analyse (1)

- Mit dem Raspberry verbinden über ssh oder remote desktop
  3 Verbindungen: Fenster1: **client** Fenster2: **server** Fenster3: **wireshark**
- Wechseln Sie zum **Server-Fenster** in das Verzeichnis:
  cd /home/pi/IEC61850/libiec61850-0.9.2.1/examples/server_example3
- Wechseln Sie zum **Client-Fenster** in das Verzeichnis:
  cd /home/pi/IEC61850/libiec61850-0.9.2.1/examples/iec61850_client_example2
- Aktivieren Sie zunächst den Server:
  sudo ./server_example3 -> Ausgabe: *Using libIEC61850 version 0.9.2*
- Wechseln Sie zum **WiresharkFenster:**
  dumpcap -i lo
- Wechseln Sie zum Client Fenster und aktivieren Sie den Client:
  sudo ./client_example2
- Wechseln Sie zum **wireshark-Fenster**:
  Beenden Sie den Prozess mit *Ctr-C*

Die Eingaben sind kursiv dargestellt.
Alle Programme müssen mit Root-Rechten ausgeführt werden den Kommandos immer ein „sudo“ vorangestellt.

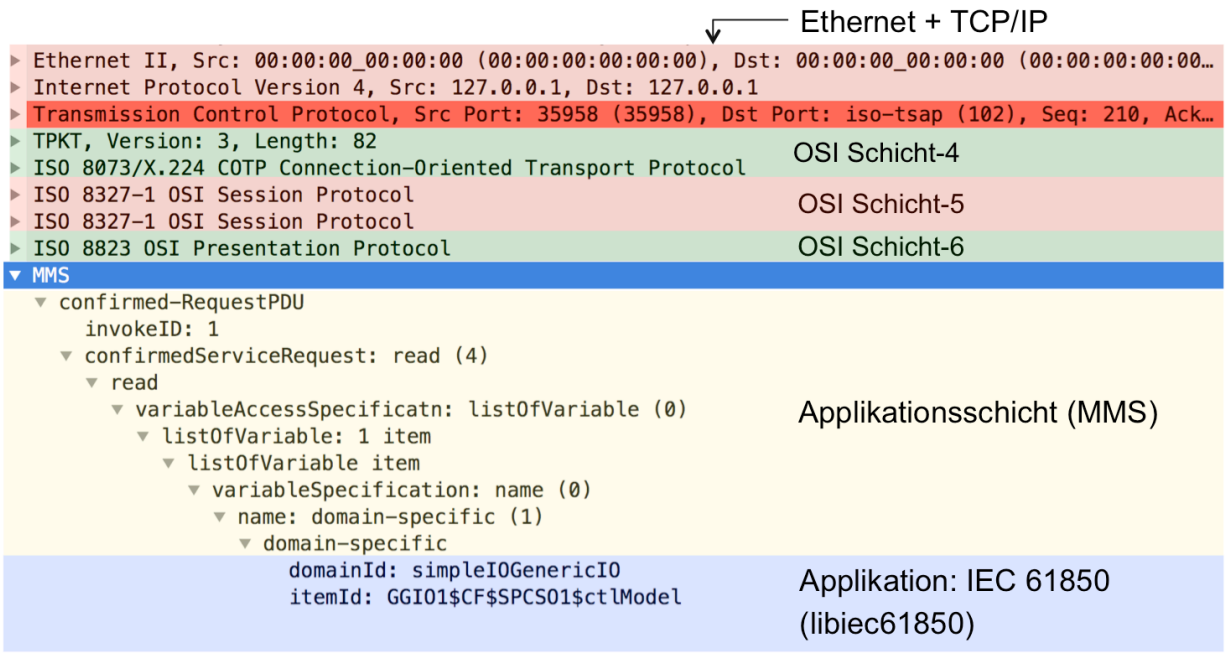
Client – Server Kommunikation



MMS – Analyse (2)

- Kopieren Sie die wireshark Trace-Datei auf einen USB-Stick:
  - USB-Stick lokalisieren: *ls - l /media/pi* -> USB-Stick Verzeichnis z.B.: B2E7-2AD3
  - *cp tmp/wireshark* /media/pi/B2E7-2AD3*
  - Wireshark auf dem PC öffnen und Trace-Datei auswählen z.B: *wireshark_pcapng_Loopback_20160909204456_ENtGPg*
- Identifizieren Sie den MMS-Verbindungsaufbau
  - Welche Protokollschichten werden dargestellt ?
- Identifizieren Sie die MMS-Kommunikation
  - Welche Protokoll-Operationen sind im Trace dargestellt?

Wireshark Trace Beispiel



Protokollschichten:

Schicht-1 und Schicht-2:	Ethernet Protokoll: IEEE 802.3
Schicht-3:	Internet
Schicht-4:	TCP (IETF Transportschicht)
Schicht-4: Adaption	ISO Transport Service on Top of TCP RFC 2126 (Weiterentwicklung von RFC 1006)
Schicht-4: Adressierung	ISO 8073 (TSAP-adressing <-> Port addressing) X.224 (OSI Transport-Schicht)
Schicht-5:	Session Protocol (connection oriented)
Schicht-6:	Presentation Protocol (connection oriented)
Schicht-7:	MMS (Applikationsschicht = IEC 61850-8-1)
Applikation:	IEC 61850

MMS – Analyse (3)

- Weitere Client – Server Kommunikationsbeispiele:
  - server_example3 mit:
    - Iec61850:client_example2
      Welche MMS-Funktion wird aktiviert?
    - Iec61850:client_example4
      Welche MMS-Funktion wird aktiviert?
    - mms_utility
      Pogrammaufruf mit Parameter: -h
      zeigt die Liste der verfügbaren Funktionsaufrufe
    - Probieren Sie die Funktionen aus und erstellen Sie für jede einen Wireshark Trace