DHBW Stuttgart

Rechnerkommunikation und Vernetzung
Teil 1: Ethernet Protokoll

Dr. Leonhard Stiegler
Nachrichtentechnik

www.dhbw-stuttgart.de

Inhalt

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

DHBW Stuttgart

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

DHBW Stuttgart

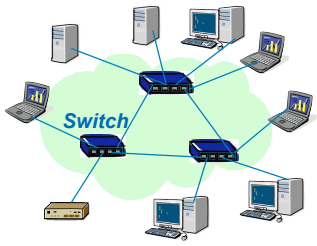
- Führende Rolle in den Ethernet IEEE 802.3 Implementierungen
- Universelle IEEE 802.3 Medium Access Control Adressierung
- Hohe Datenrate: aktuell über 10 Gbit/s
- Möglichkeit der optischen Datenübertragung
- Entwicklung von Bus-Topologie (shared medium) zur Stern Topologie (dedicated media)
- Anwendungen:
  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

DHBW Stuttgart

Lokale Netze (Local Area Networks)

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

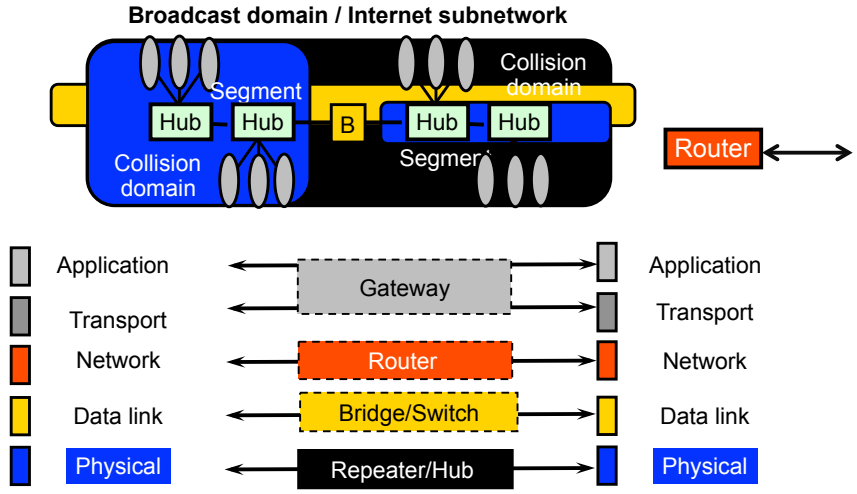


Ethernet Elemente

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

Netzelemente der Protokollschichten

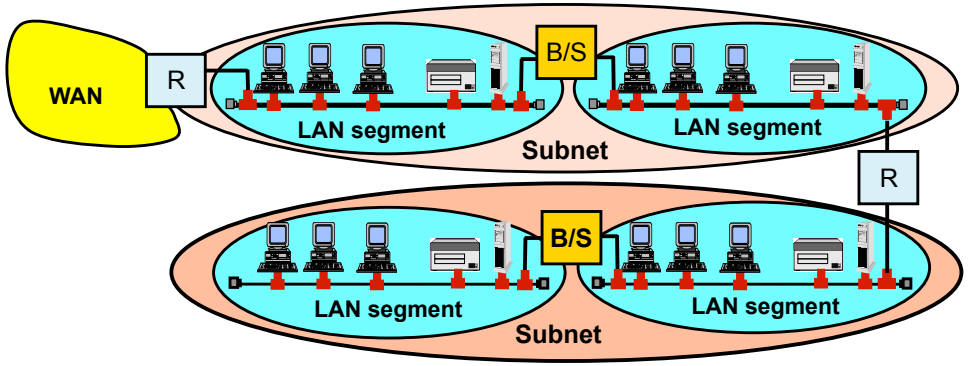
DHBW Stuttgart



Bridge, Switch und Router

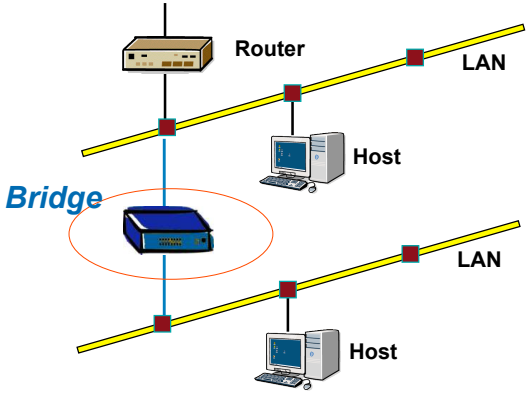
DHBW Stuttgart

- B/S • Bridge/Switch — verbindet Schicht-2 LAN Segmente
- R • Router — verbindet Schicht-3 Netze



Netzelemente : vom Hub zur Bridge

DHBW Stuttgart



LAN Segment 1 (local traffic)

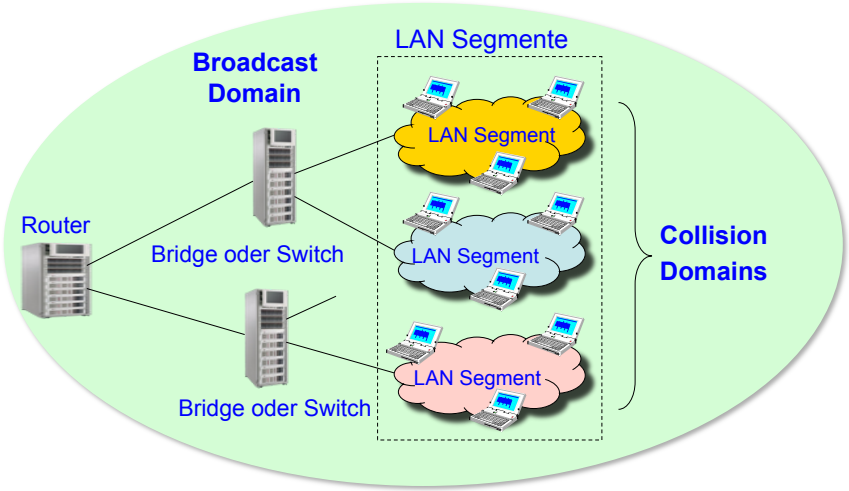
Traffic between segments

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

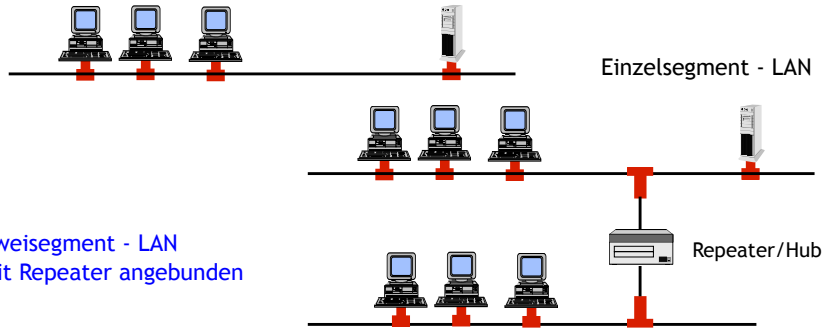
LAN Architekturbeispiel

DHBW Stuttgart



LAN Segmentierung

DHBW Stuttgart



- 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

Inhalt

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

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

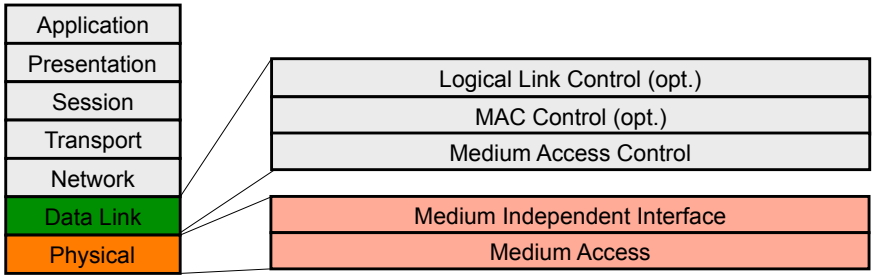
Ethernet Protokollschichten

Schicht-1 Funktionen

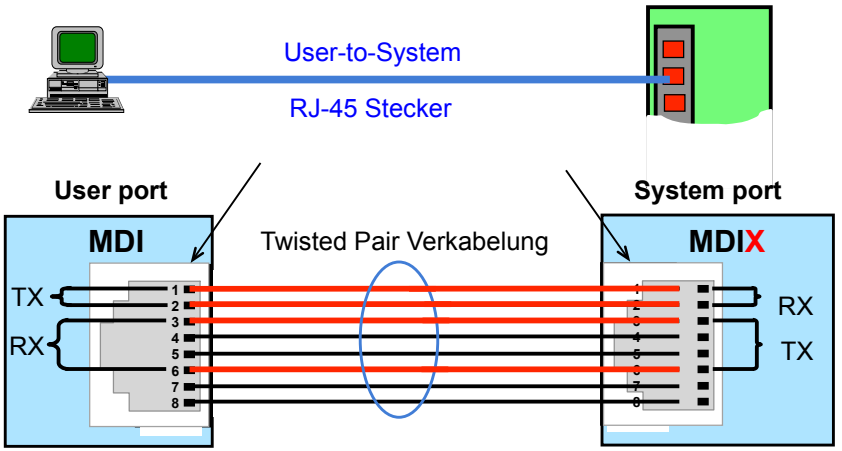
- Medium Access — **Medium Independent Interface**, **Medium Interface**

Schicht-2 Funktionen

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

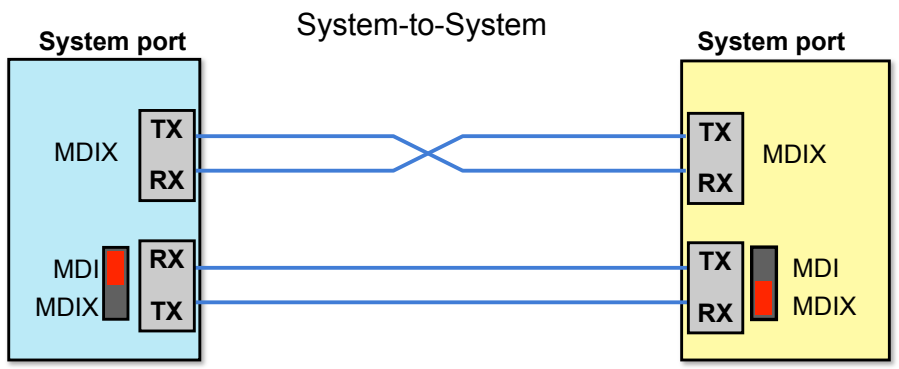


LAN Verkabelung: Twisted Pair Link



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

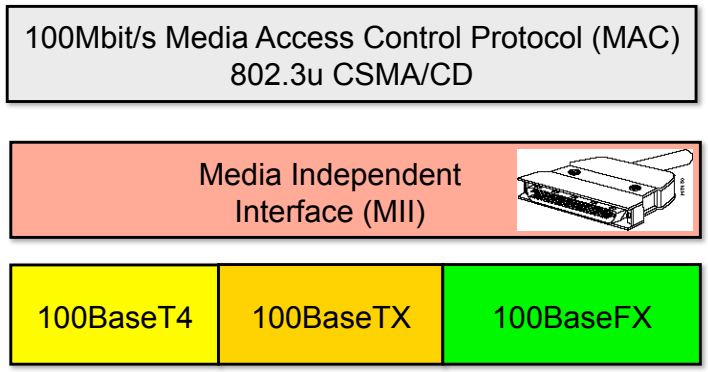
LAN Verkabelung: Twisted Pair Link



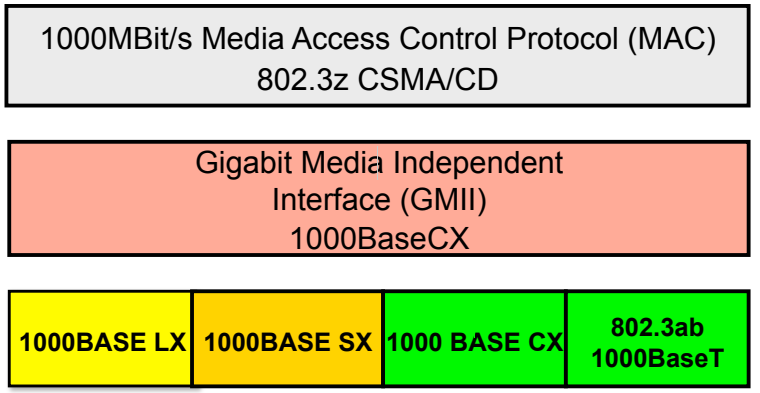
Ethernet BASE Übersicht

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

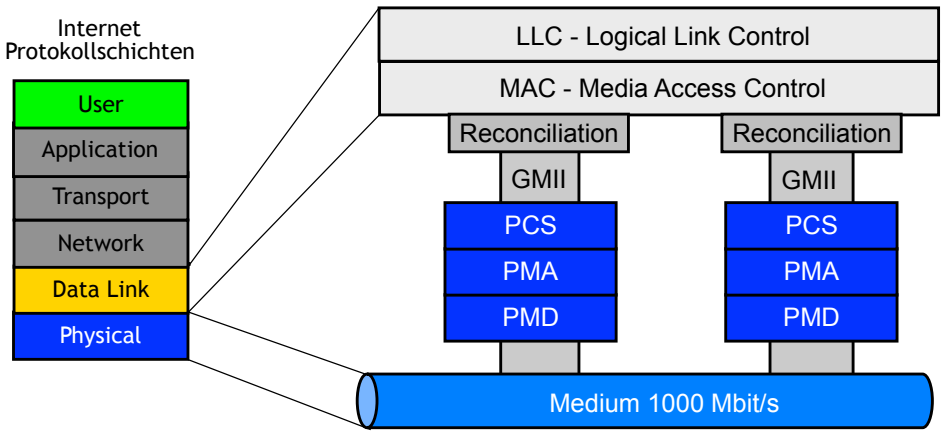
Fast Ethernet



Gigabit Ethernet

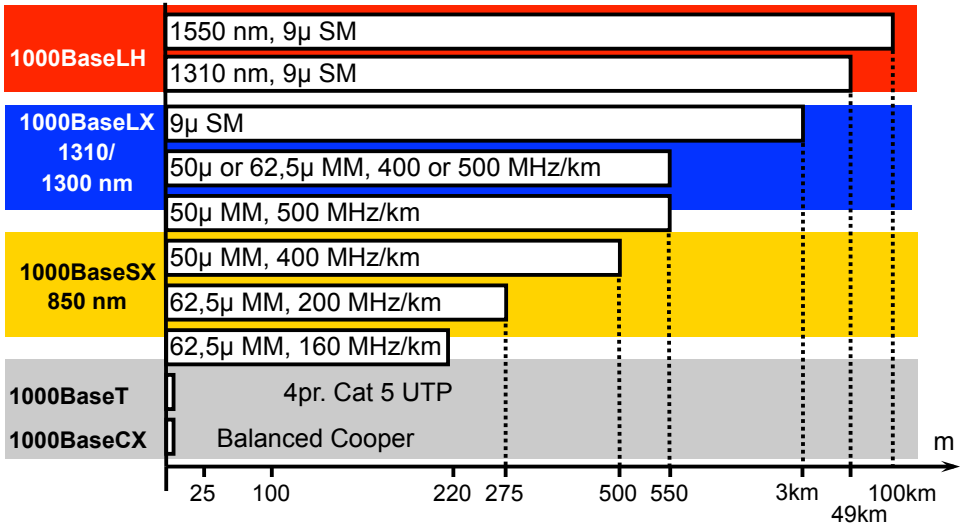


Gigabit Ethernet Architektur



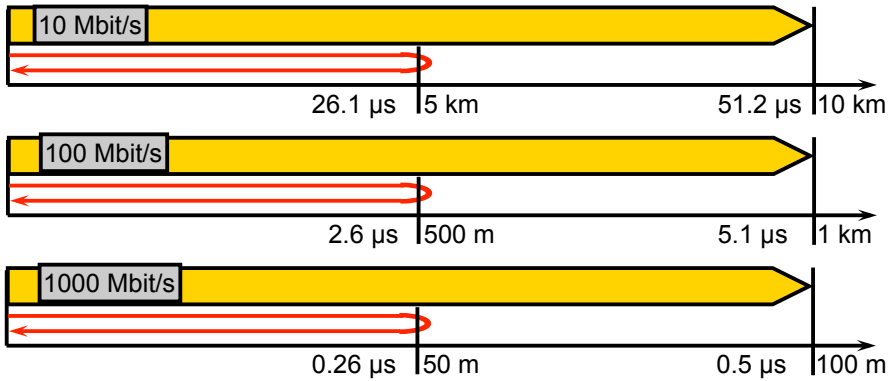
PCS: Physical Coding Sublayer
PMA: Physical Medium Attachment
PMD: Physical Medium Dependent

Medium und Übertragungsdistanz



Gigabit Ethernet und CSMA/CD

Roundtrip Delay und Übertragungsdistanz



Bedingungen:

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

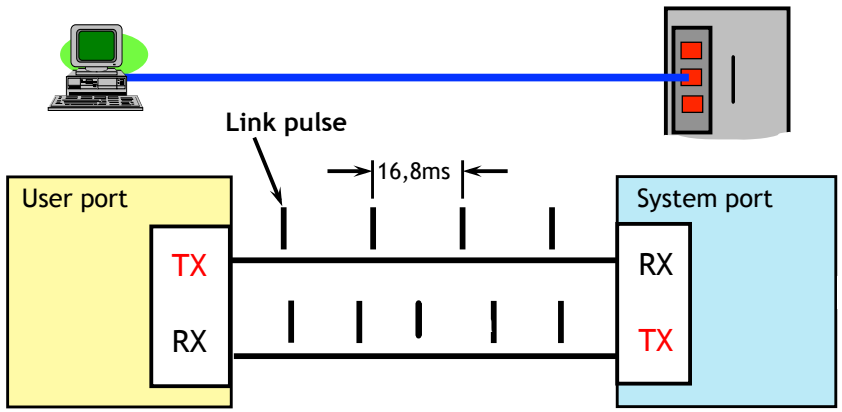
Auto-Negotiation

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

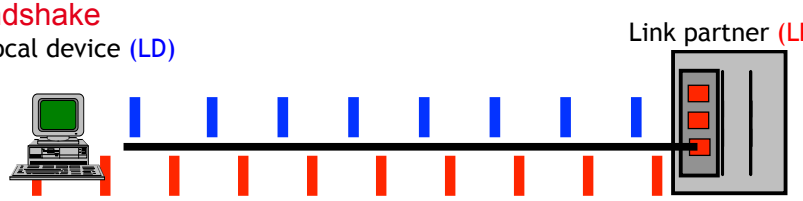
Basisfunktionen

- 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 Synchronization : Link Handshake

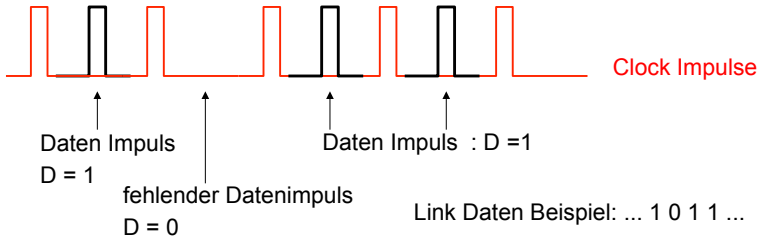


1. LCW kontinuierlich senden (LD) mit Ack=0
   (Info to LP: I do not yet know about you.)
2. Empfang 3 aufeinander folgender, gleicher LCWs (LP) mit Ack=x
   (LD now recognizes the LCW of LP.)
3. LCW (LD) mit Ack=1 senden
   (Info to LP: I received your LCW.)
4. Empfang 3 aufeinander folgender, gleicher 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.)

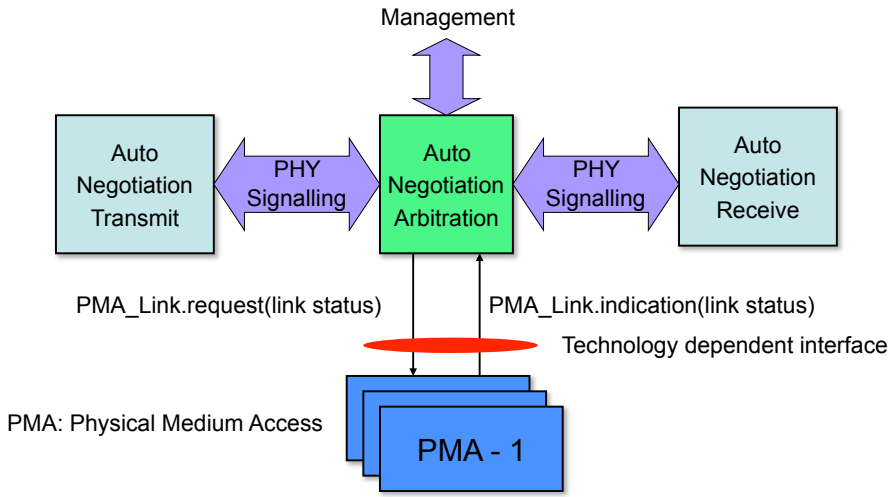
LCW: Link Control Word

Signalisierung bei der Auto Negotiation

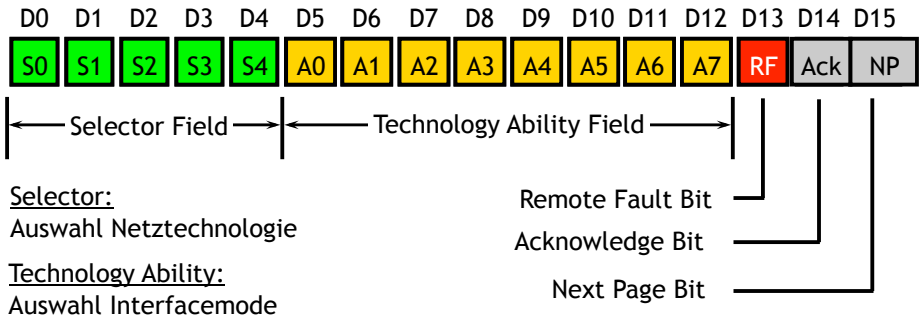
- PHY-Layer Primitive: PMA_Link.Request
  Funktion: Link Control, Auto-negotiation.
- Der Link Control Parameter kann die Werte: SCAN_FOR_CARRIER, DISABLE, oder ENABLE einnehmen
- Der Fast Link Pulse (FLP) Burst besteht aus einer Gruppe 17 – 33 10BASE-T kömpatiblen Link Integrity Test Pulsen.
- Jeder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



Arbitration Funktion



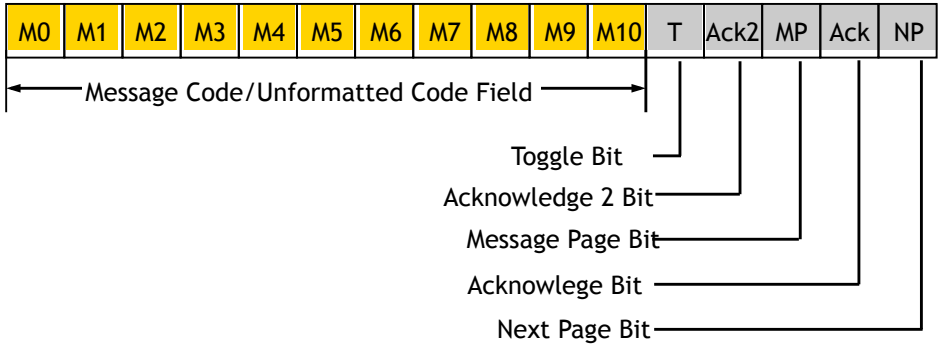
Base Link Codeword Format



Selector:
Auswahl Netztechnologie

Technology Ability:
Auswahl Interfacemode

Next Page Link Codeword Format



Inhalt

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

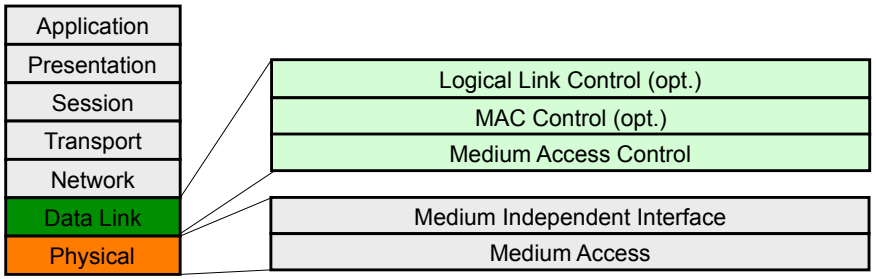
Ethernet Protokollschichten

Schicht-1 Funktionen

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

Schicht-2 Funktionen

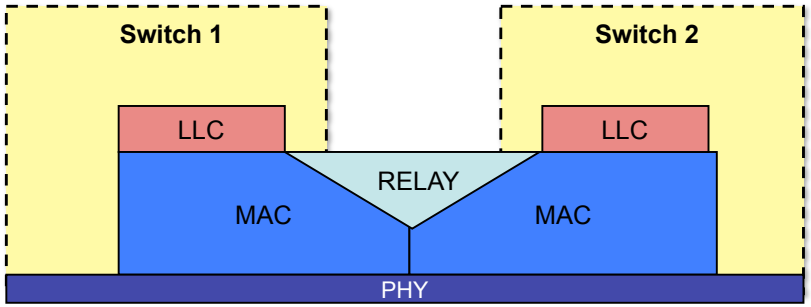
- Zugang zum Übertragungsmedium — **Mediaum Access Control**
- Protokollsteuerung — **MAC Control**
- Link Verbindungssteuerung — **Logical Link Control**



Layer-2 Bridge/Switch

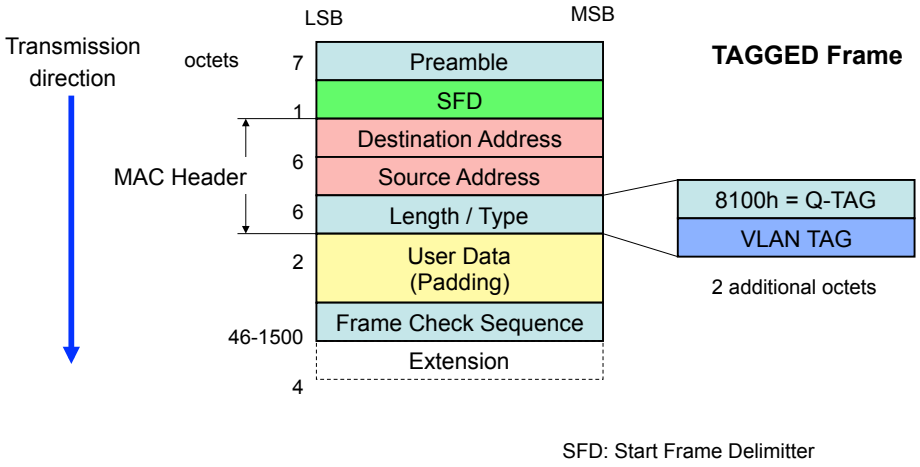
DHBW Stuttgart

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

DHBW Stuttgart



SFD: Start Frame Delimitter

Aufgabe

DHBW Stuttgart

- 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

DHBW Stuttgart

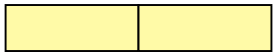
Beispiele:
Unicast: 00-01-68-50-23-45
Broadcast: FF-FF-FF-FF-FF-FF
Multicast: 01-80-C2-00-00-00

Multicast
Bridge Management

I/G: 0 = Individuelle Addresse;
1 = Gruppenaddresse (Broadcast = FFh)
U/L: 0 = Globale Addresse;
1 = Lokale Addresse

Type / Length Field:

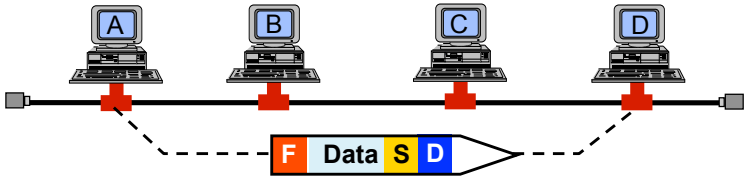
2 Octets



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

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

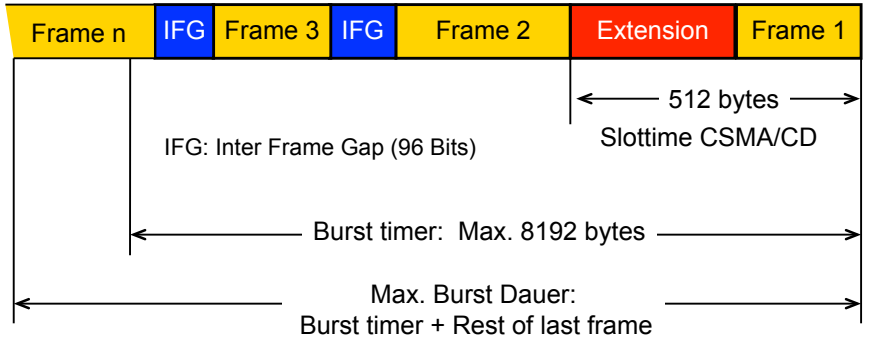
MAC Adressierungsmethode



Nachricht (höhere Schichten): Data

+ Dest. address D
+ Source address S
+ Error checking F
= Frame (packet) F Data S D

Frame Bursting

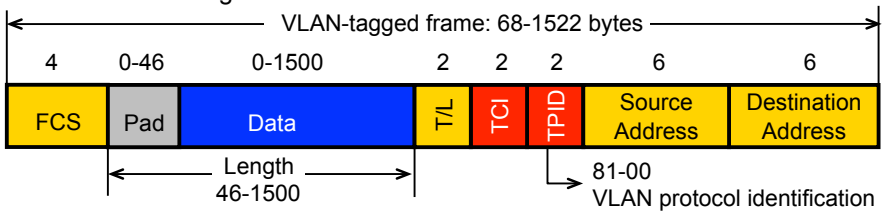


Inhalt

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

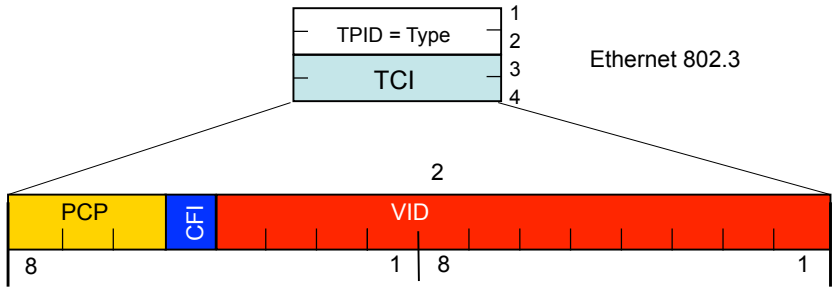
Virtual Local Area Network (VLAN)

- 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

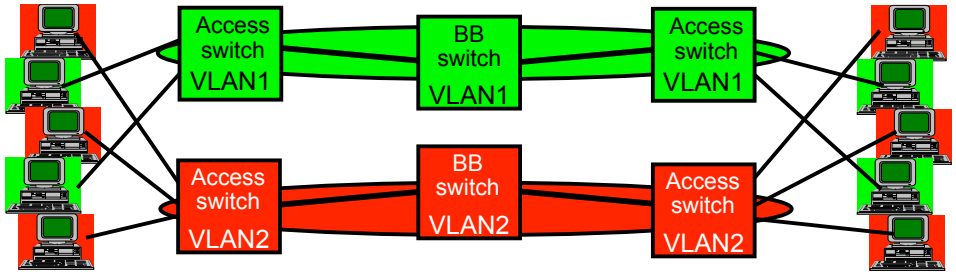
VLAN Tag Control Information (TCI)



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

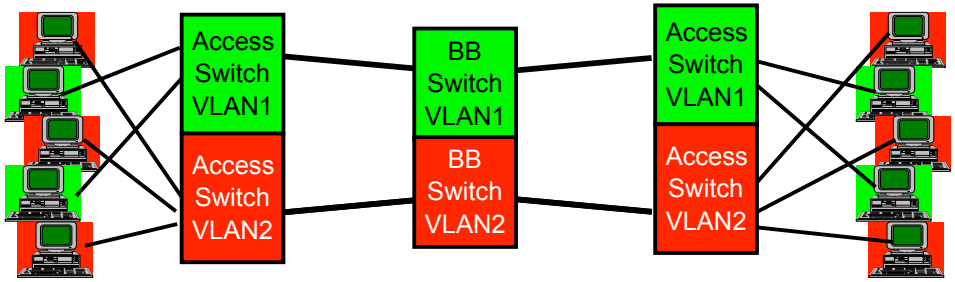
Virtual LAN Prinzipien (1)

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

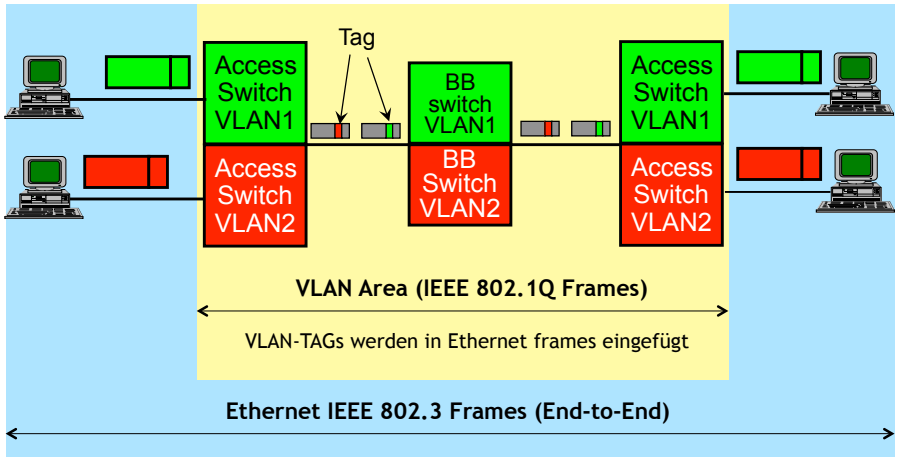


Virtual LAN Principles (2)

- 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

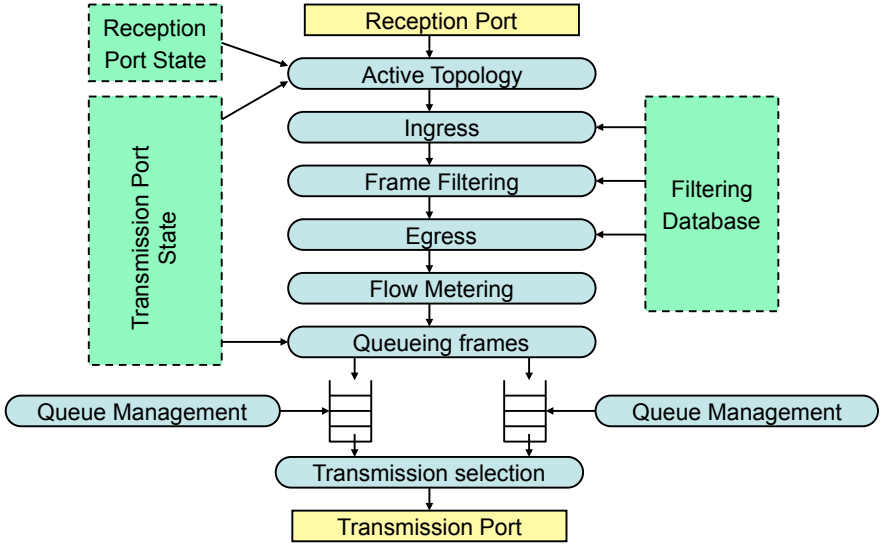
Protocol	VLAN
IP	1
IPX	2

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)

DHBW Stuttgart

IEEE 802.1D/p

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

Prioritätsklassen

DHBW Stuttgart

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

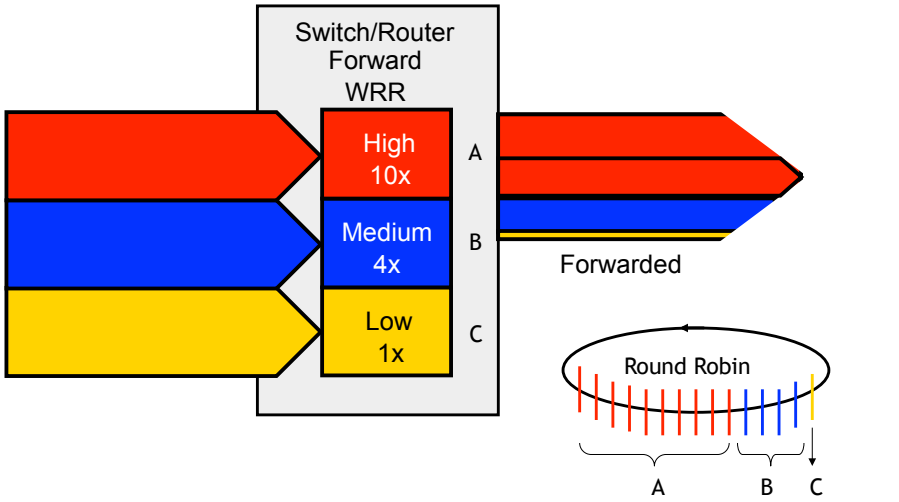
Excellent Effort:
best-effort Service-Typ für Prime-users.

Best Effort:
Standard Verkehrsart für unpriorisierte Anwendungen

Background:
für Massendaten-Anwendungen ohne Auswirkungen auf die Netzgüte

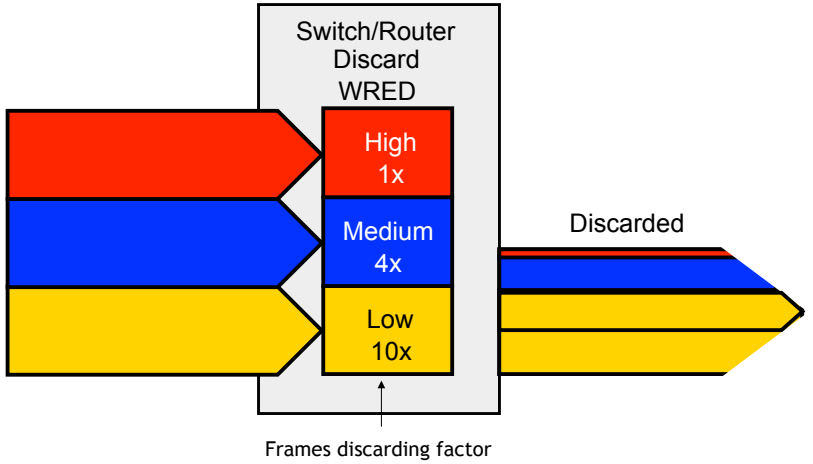
Priorisation: Weighted Round Robin (WRR)

DHBW Stuttgart



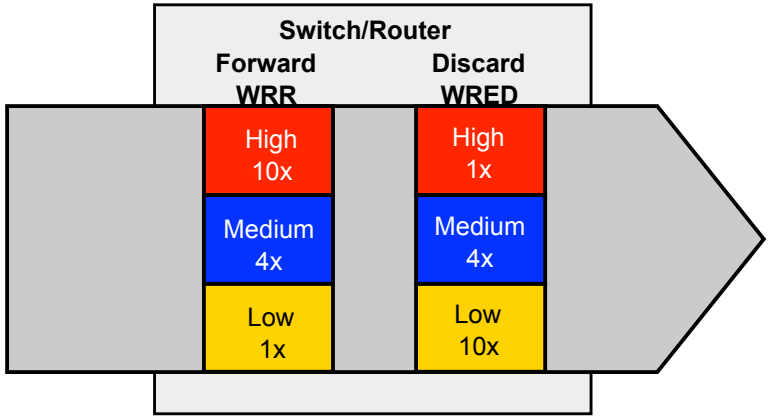
Weighted Random Early Discard

DHBW Stuttgart



Scheduling Methoden: WRR und WED

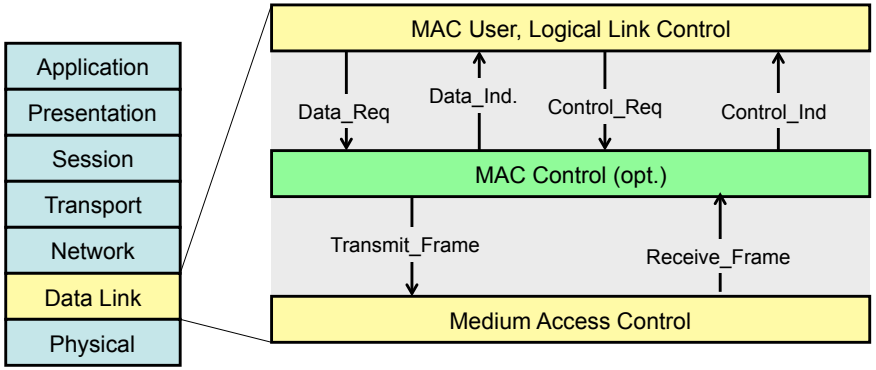
WRR: Weighted Round Robin
WED: Weighted Early Discard



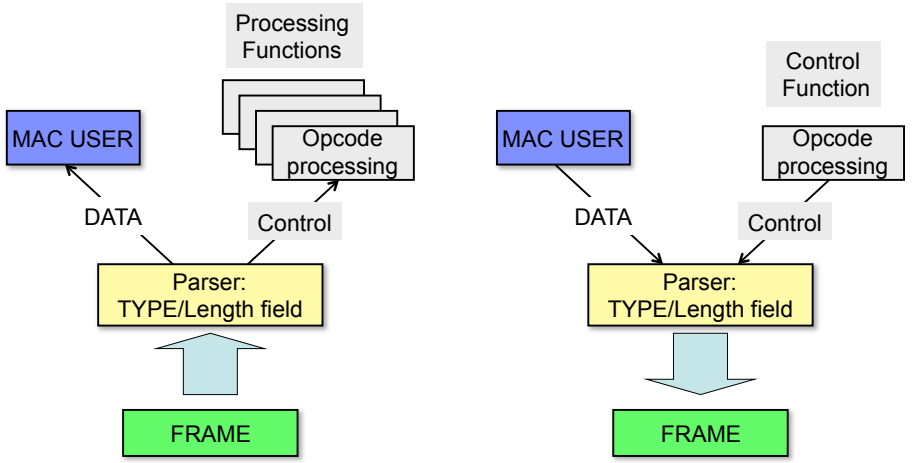
Inhalt

- 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

MAC 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)

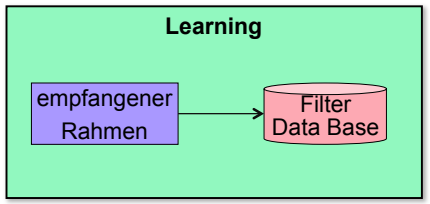
Roundtrip Delay
Beträgt die doppelte Signalverzögerungszeit zweischen Sender und Empfänger.
Regel: Roundtrip Delay < Slot Time

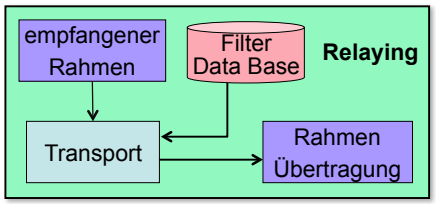
Backoff Time
Wartezeit nach einer Kollisieonserkennung. Backoff time = N * Slot Time. N ist eine Zufallszahl zwischen 1 und 1023. Maximalwert: 52377.6 µs.

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

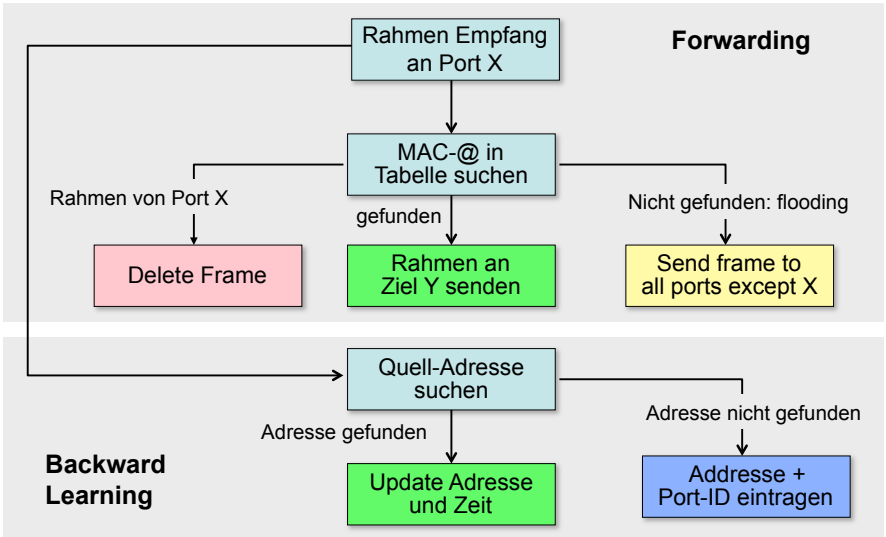
Daten Filter

- 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

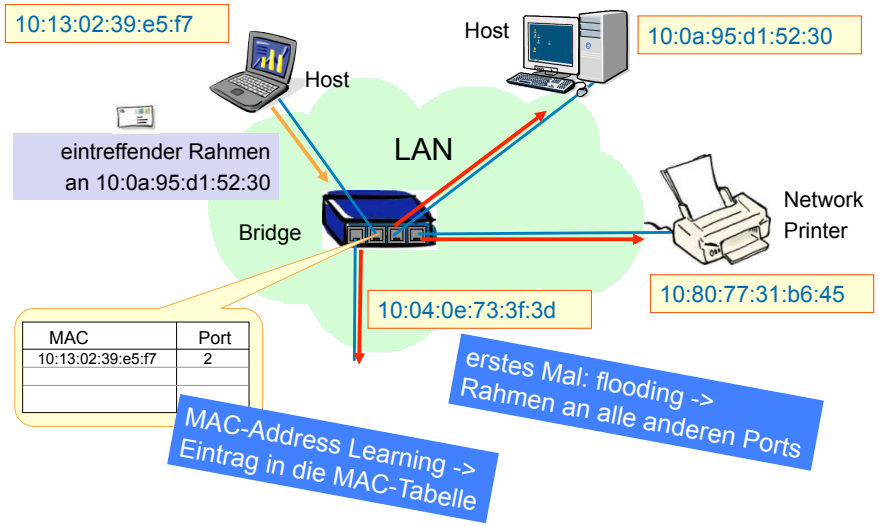




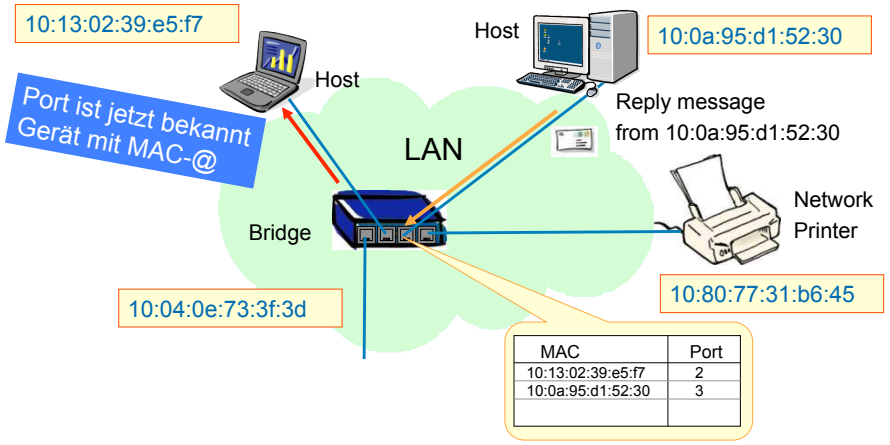
Rahmen Übertragung : Frame Forwarding



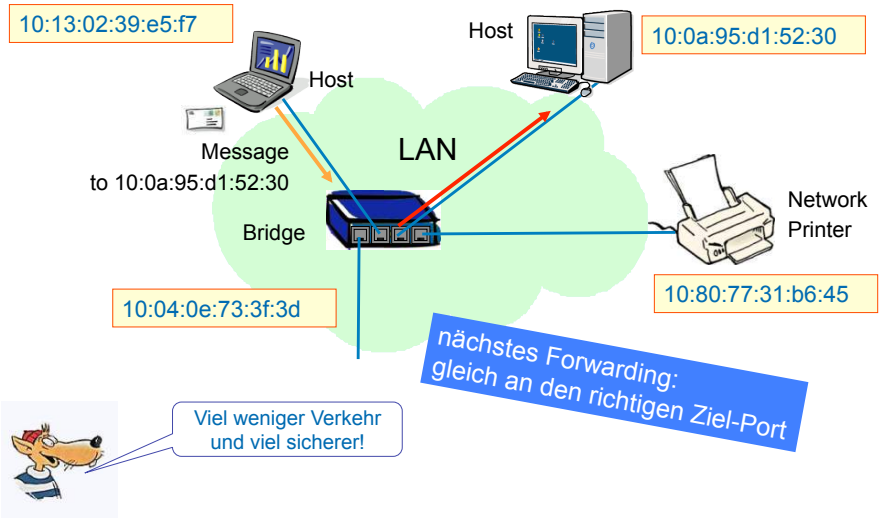
Ablauf : 1. Anfrage



Ablauf : Antwort



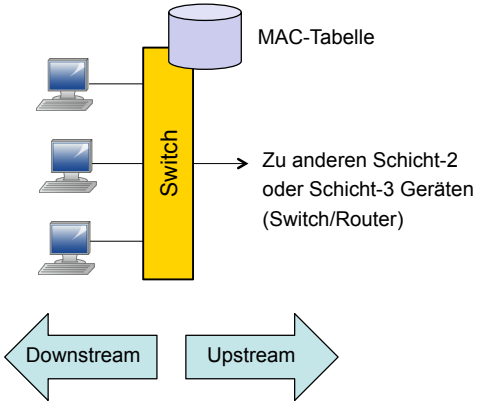
Ablauf : weitere Anfragen



Zusammenfassung

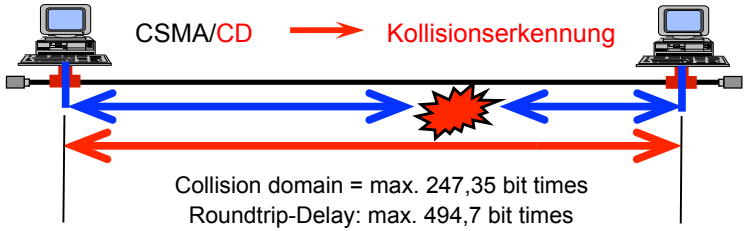
Schicht-2 Netzelement : Switch

- 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.

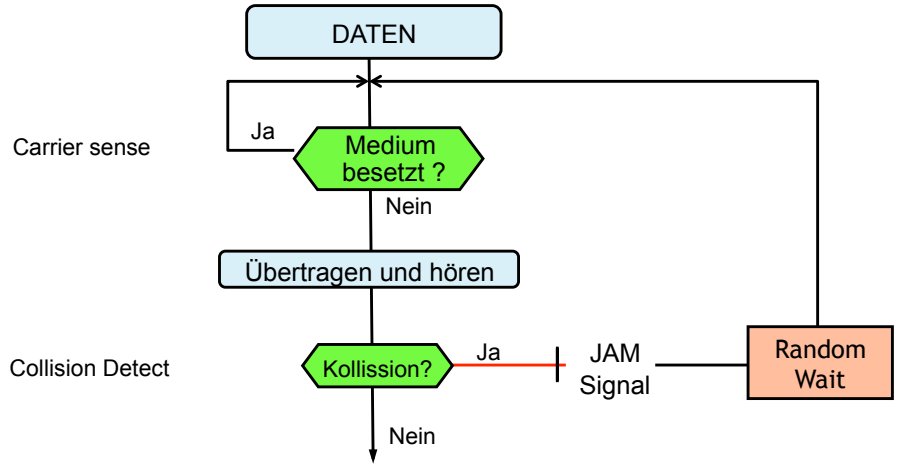


Kollisionen

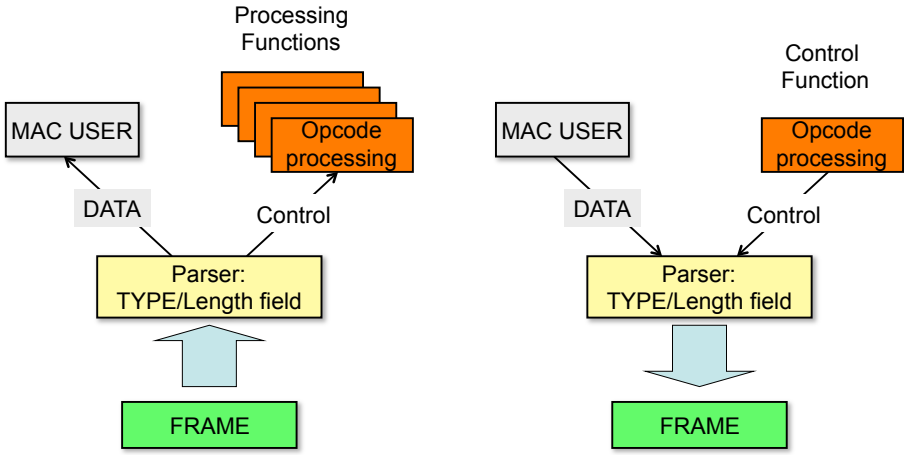
- Moderne Ethernet LANs vermeiden Kollisionen durch Punkt-zu-Punkt Topoligie
- Eine Collision Domain ist ein Netzsegment in dem Datenkollisionen auftreten können, wenn zwei Stationen gleichzeitig den Bus belegen.
- Zur Vermeidung von Kollissionen dient CSMA-Zugangsmethode, bei der der the Medium-Zustand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



CSMA/CD Prozedur



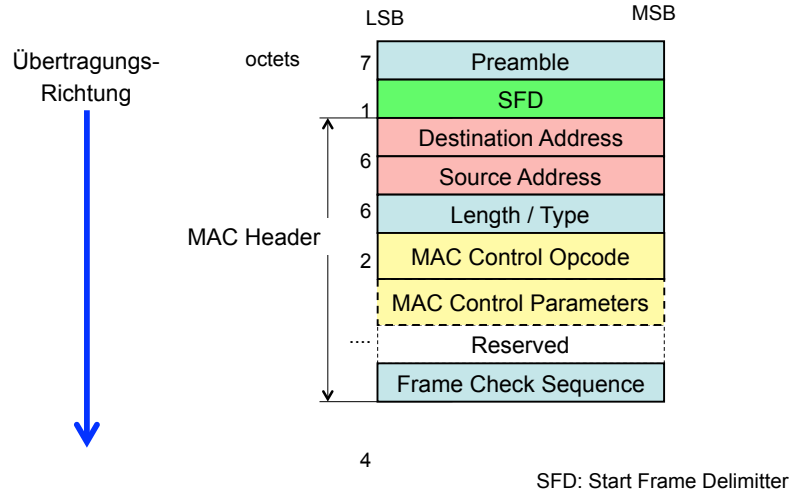
MAC-Schicht : Management Operationen



MAC Control Operations

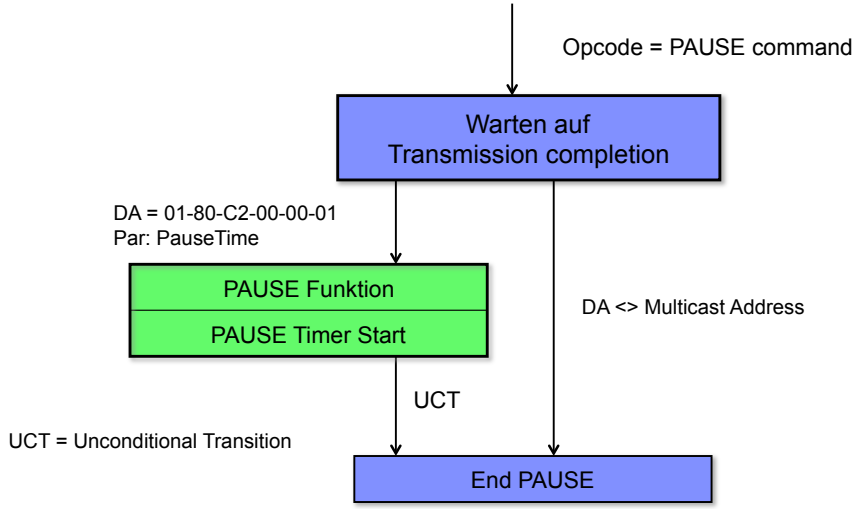
Code	Function Name	Comment
00 00	Reserved	
00 01	PAUSE	Flow Control: stop transmission
00 02	GATE	Flow Control: start transmission
00 03	REPORT	Pending transmission requests
00 04	REGISTER_REQ	Flow Control: registration request
00 05	REGISTER	Flow Control: registration
00 06	REGISTER_ACK	Flow Control: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

MAC Control Frame

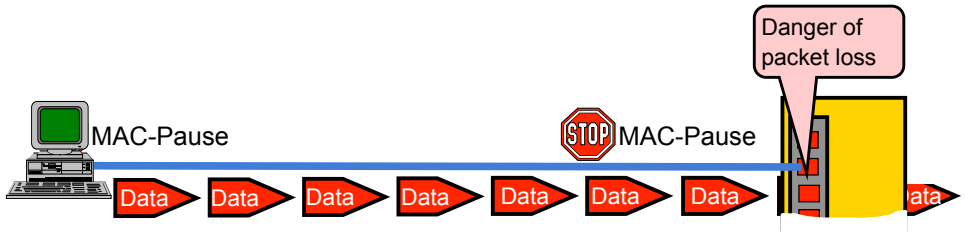


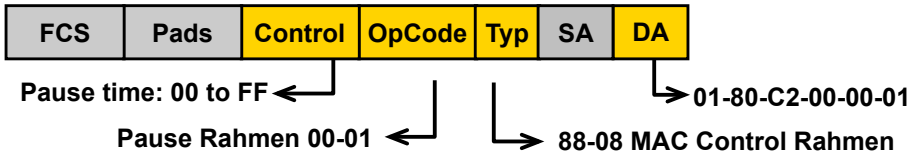
SFD: Start Frame Delimitter

PAUSE Operation



Full Duplex Flusskontrolle

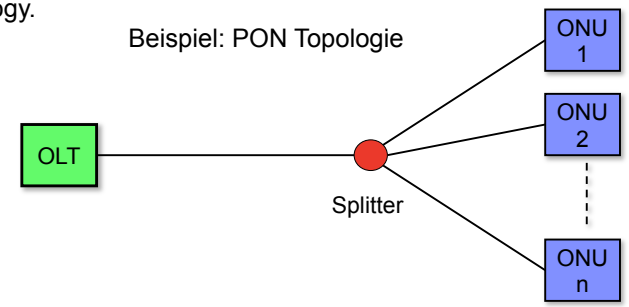




Multipoint MAC Control

- 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



Inhalt

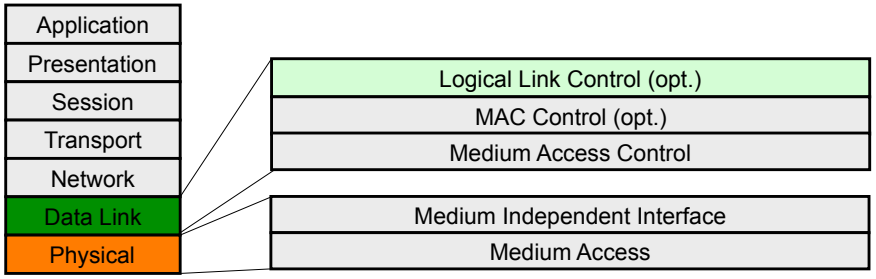
- Ethernet Übersicht und Protokolle
- Ethernet Schicht-1
- Ethernet Link Schicht
- Medium Access Control
- Logical Link Control – LLC
- Ergänzende LAN Protokolle

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)



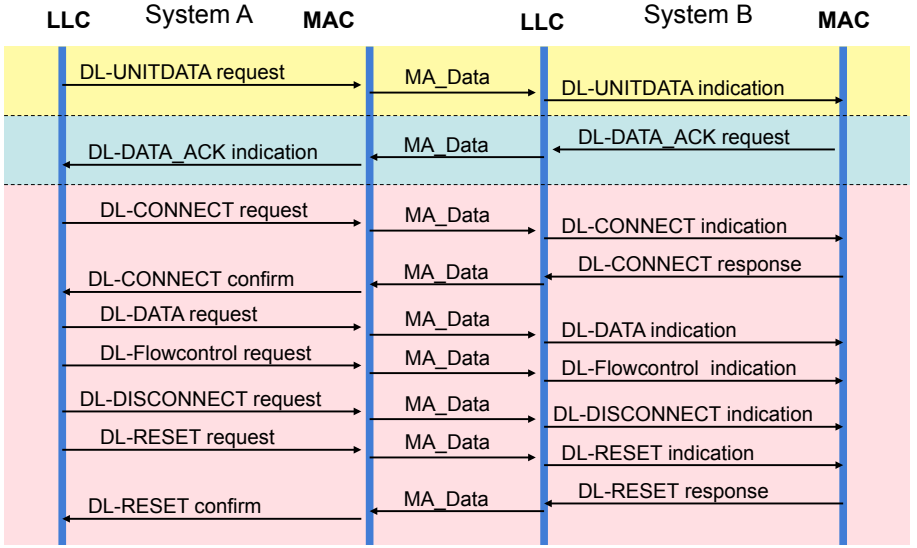
LLC Dienste

- 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 Primitives



LLC Nachrichten

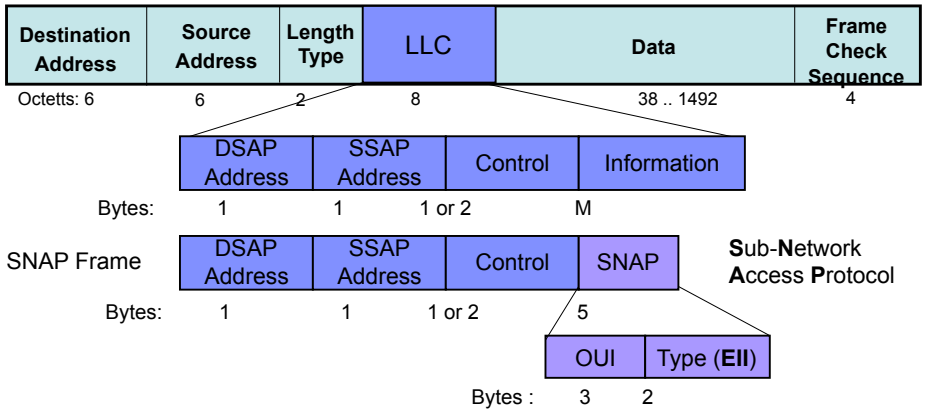
Symbol	Name	C/R
I	Information	C/R
RR	Receive Ready	C/R
RNR	Receive not Ready	C/R
REJ	Reject	C/R
FRMR	Frame Reject	R
UI	Unnumbered Information	C
UA	Unnumbered Ack	R
DISC	Disconnect	C
DM	Disconnect Mode	R
SABME	Set Asynchronous Balaced Mode extended	C

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

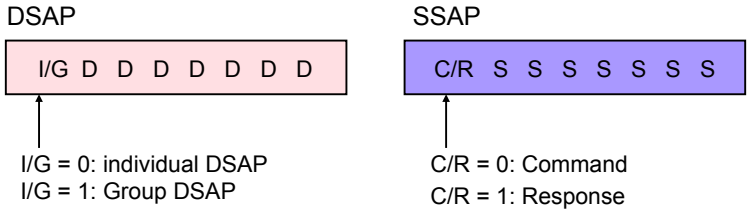
non-HDLC Messages

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

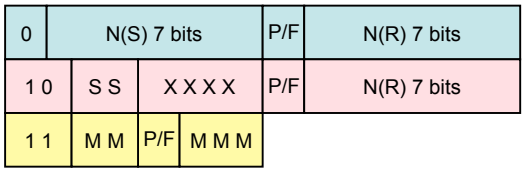


I/G = 0: individual DSAP
I/G = 1: Group DSAP

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:



Inhalt

- 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

DHBW Stuttgart

- 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

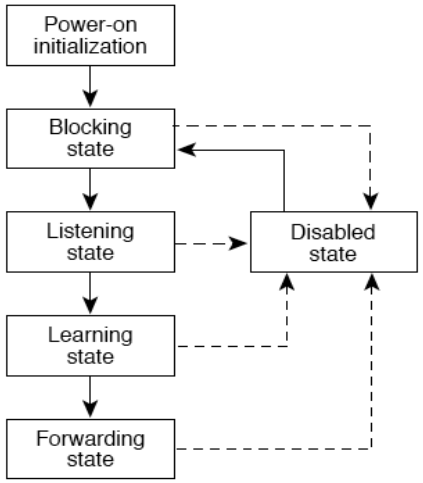
DHBW Stuttgart

- 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 States

DHBW Stuttgart

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



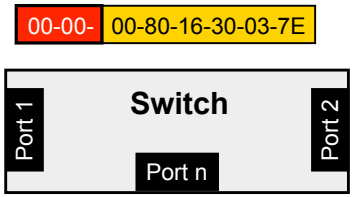
Spanning Tree Adressen

DHBW Stuttgart

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

Spanning Tree Prozedur

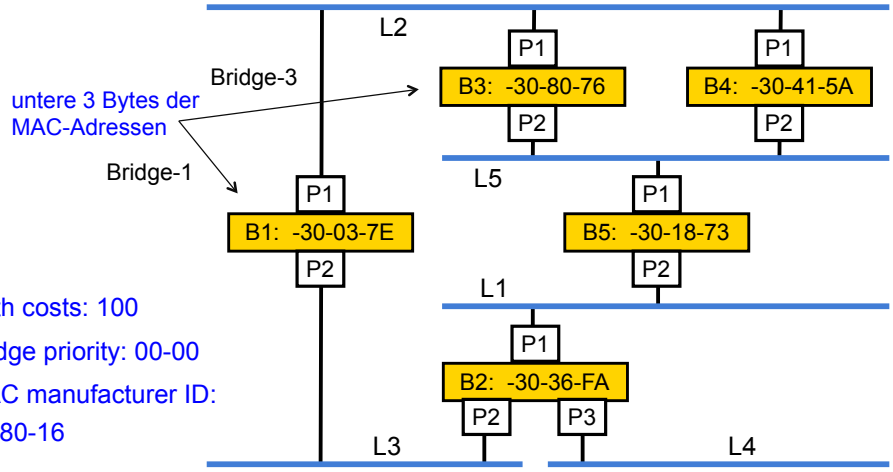
1. Jeder Switch erhält eine relative Prioritätszahl. Die **BID = Prioritätszahl + MAC-Adresse** definieren die Bridge-Priorität
2. Die Bridge mit der niedrigsten BID wird die **Root Bridge**
3. Jede Bridge bestimmt einen **Root Port = niedrigste Path Cost + geringste Entfernung** zur Root Bridge.
  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

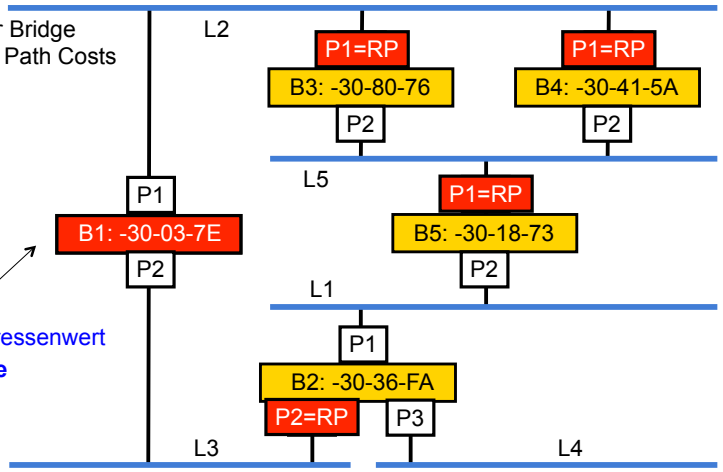
MAC manufacturer ID: 00-80-16

Root Bridge und Root Port Festlegung

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

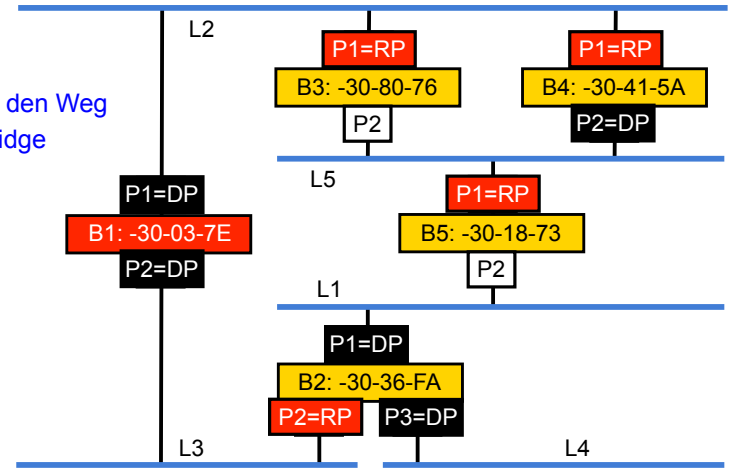
Falls es mehrere Ports mit den selben Path Costs zur Root Bridge gibt entscheidet die Port-Id.

Niedrigster Adressenwert
-> **Root Bridge**



Designated Bridge Port Festlegung

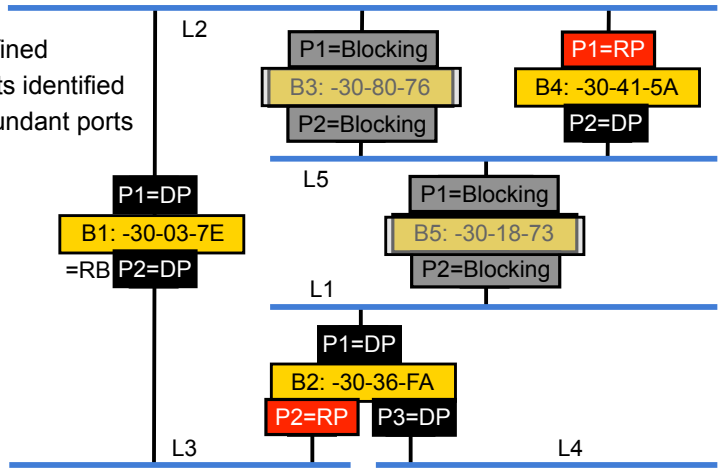
DP markiert den Weg zur Root bridge



Ergebnis der Spanning Tree Prozedur

DHBW Stuttgart

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



Bridge Protocol Data Unit (BPDU)

DHBW Stuttgart

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

DHBW Stuttgart

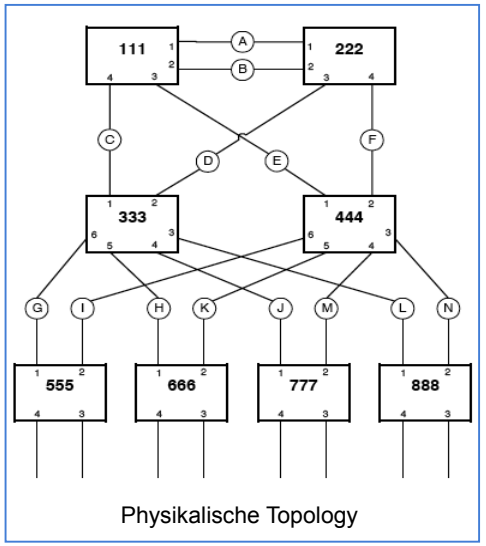
- Rapid Spanning Tree Protocol (RSTP) Bridges tauschen Informationen (BPDUs) aus zur Ermittlung der **Root Bridge** und der **kürzesten Entfernung** (shortest path) von jedem LAN und allen anderen Bridges.
- Diese Information heißt: *Spanning Tree Priority Vector*.

Priority Vector Komponenten

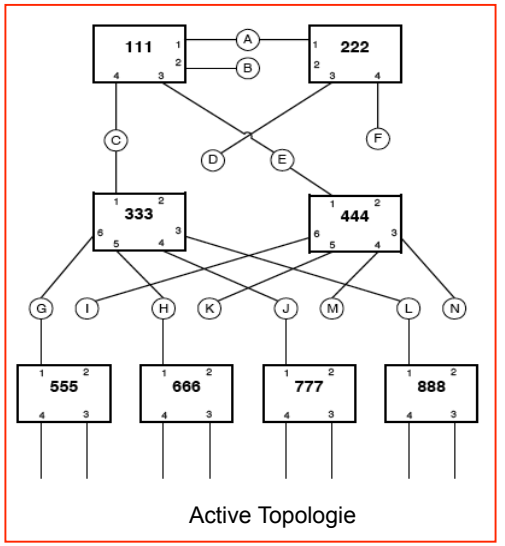
Root Bridge Identifier, Root Path Cost zur Root Bridge von der sendenden Bridge	Netz
Bridge Identifier der sendenden Bridge Port Identifier von dem Port über den die Nachricht übertragen wurde	Lokal
Port Identifier von dem Port über den die Nachricht empfangen wurde	internal

Bridge Configuration Example

DHBW Stuttgart



Physikalische Topology



Active Topologie

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 die 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))

Inhalt

Link Aggregation - LACP

Definition

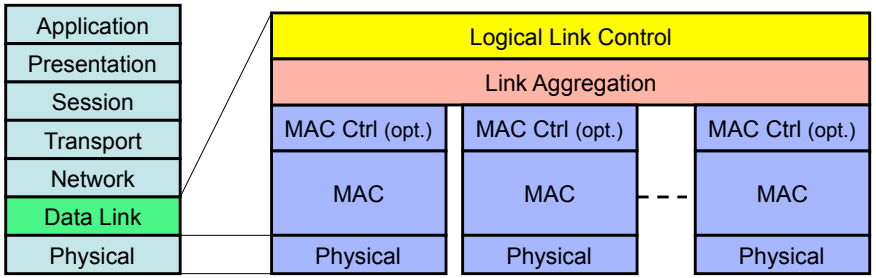
- Das Link Aggregation Control Protocol LACP unterstützt die Gruppierung von physikalischen Links zu einer logischen Einheit. Diese Link-Gruppe wird wie ein physikalischer Link behandelt

Eigenschaften:

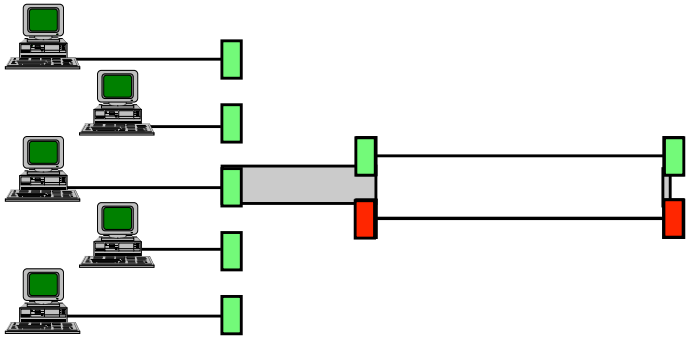
- **Erhöhung der** Datenrate:
  Die Kapazität mehrerer Ports addiert sich zu einem logischen Link
- **Load sharing**:
  Schicht-2 Verkehr wird über mehrere Links verteilt
- Keine Änderung im IEEE 802.3 Rahmenaufbau
- **Netzmanagement**:
  Link Aggregation Objecte sind im Standard Netzmanagement definiert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

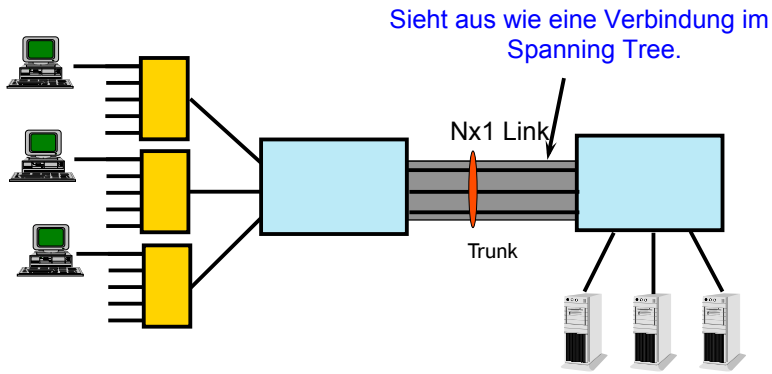


Spanning Tree Nachteile



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

Link Aggregation (IEEE 802.3-Clause 43)



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

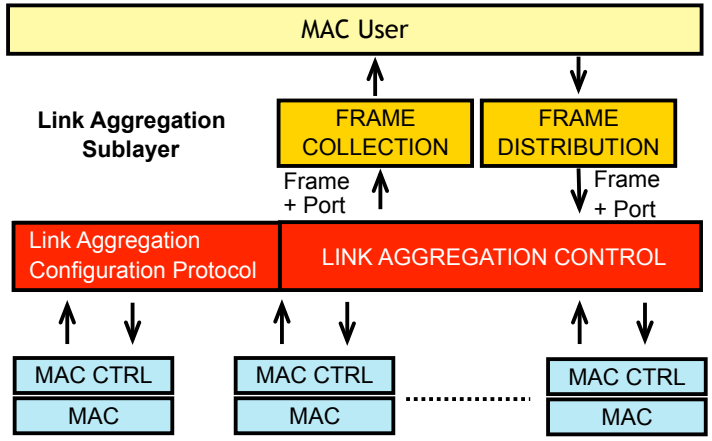
System:

- 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 Functions

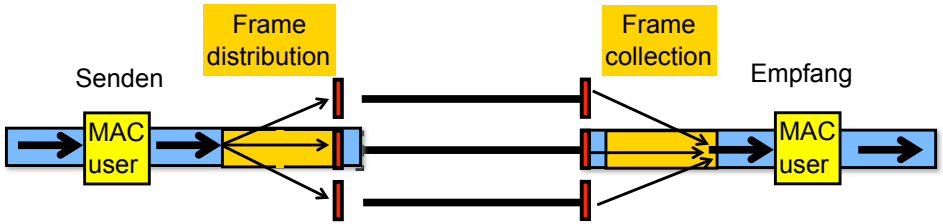
DHBW Stuttgart

Frame distribution

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

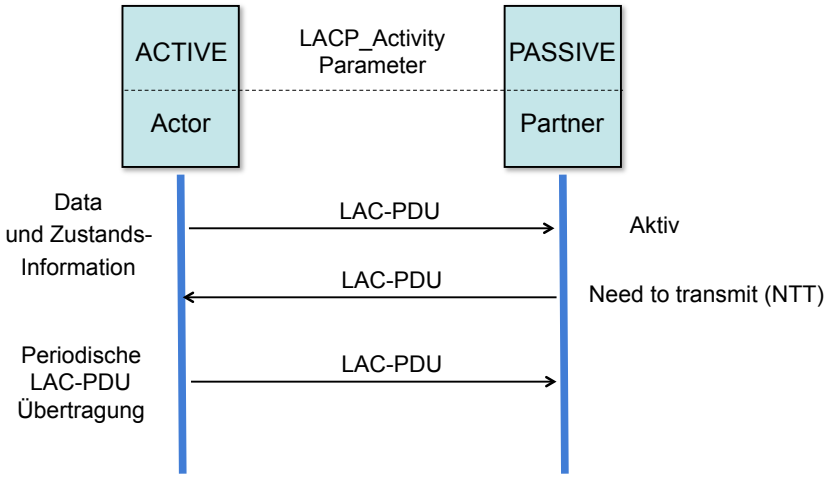
Frame collection

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



Link Aggregation Control Protocol Konzept

DHBW Stuttgart



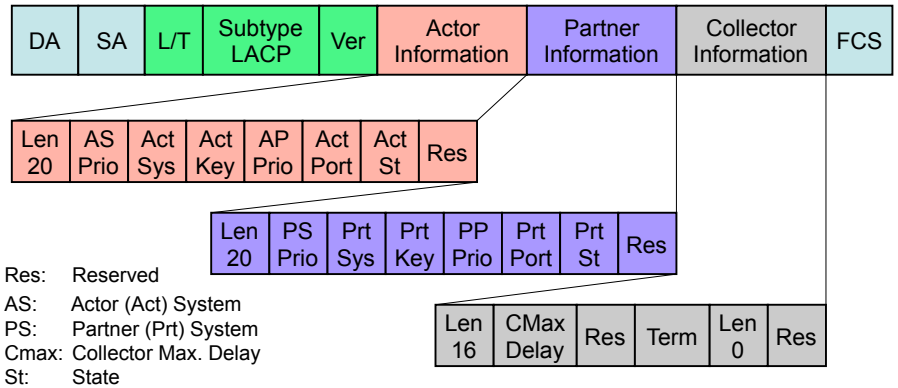
Im LACP gibt es keinen Frame Loss Detection und Retry Mechanismus

LACP Nachrichten

DHBW Stuttgart

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

LACP Protocol Data Unit Format:

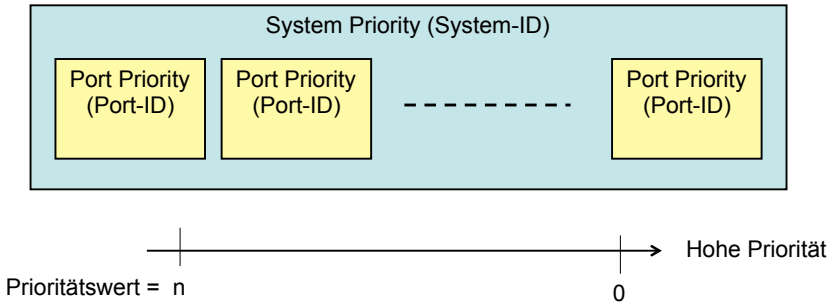


Res: Reserved
AS: Actor (Act) System
PS: Partner (Prt) System
Cmax: Collector Max. Delay
St: State

Link Priority

DHBW Stuttgart

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



Rechnerkommunikation und Vernetzung
Teil 2: Internet Protokoll

Dr. Leonhard Stiegler
Nachrichtentechnik

www.dhbw-stuttgart.de

Kursgliederung

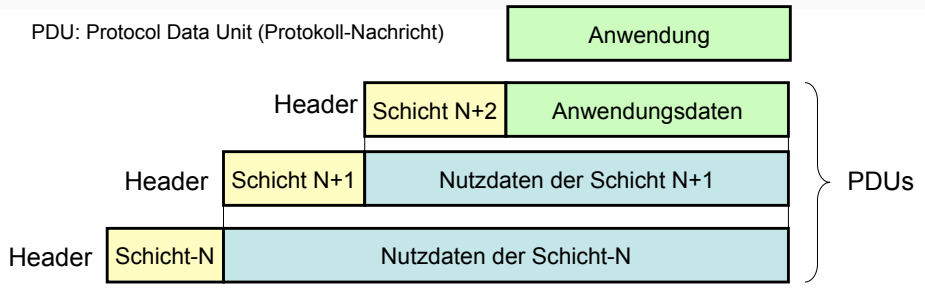
Definition: Kommunikationsprotokoll

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.



IETF Dokumente

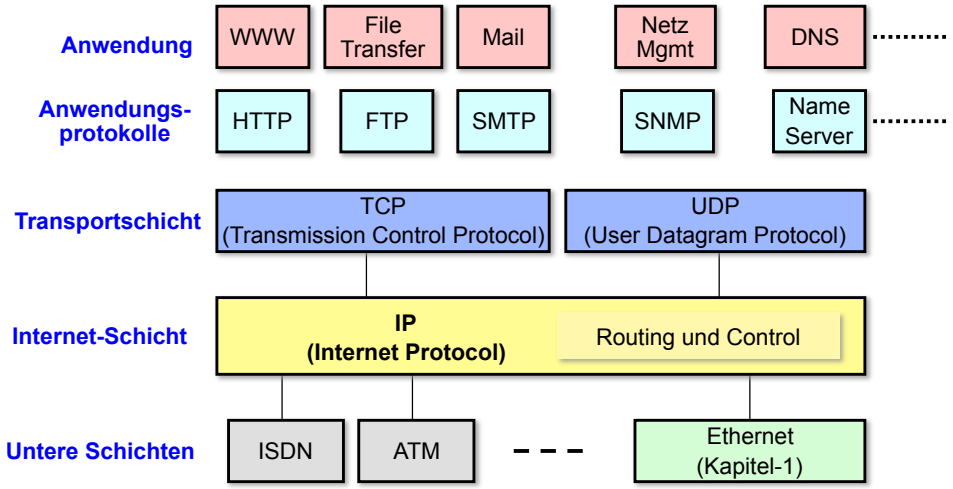
Request for Comments RFC: offizielle IETF Dokumente

- 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

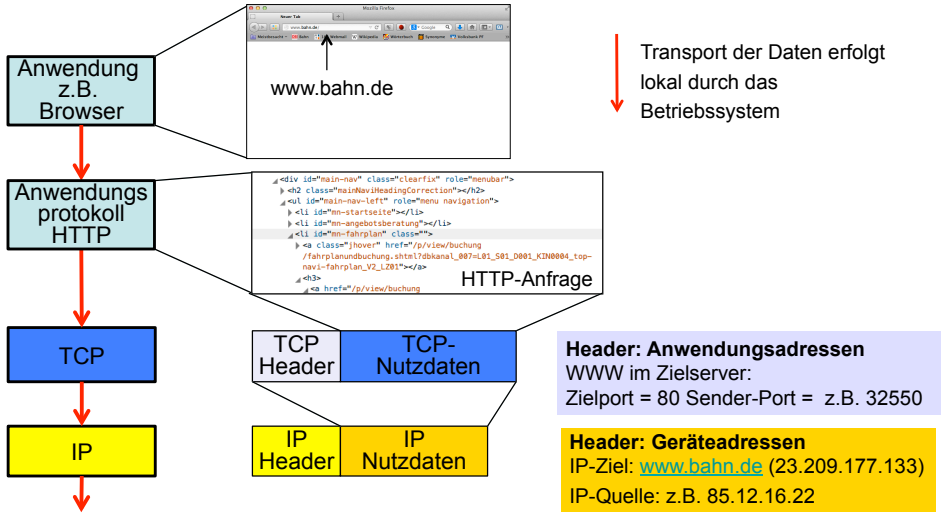
Kursgliederung

- 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

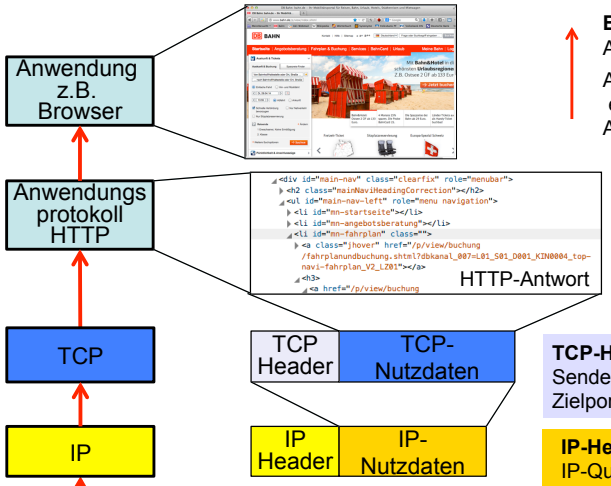
Internet-Protokollfamilie



Verarbeitung von IP-Paketen : Sender



Verarbeitung von IP-Paketen : Empfänger



Betriebssystem ermittelt die richtige Anwendung (Port-Nr)

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

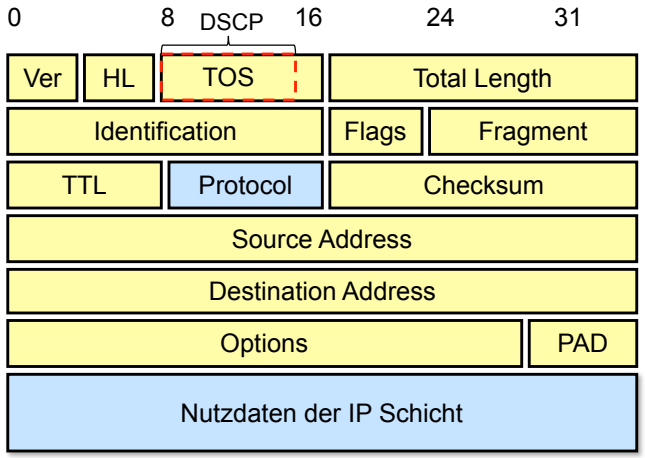
TCP-Header: Anwendungsadressen
Sender-Port = 80
Zielport = 32550

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

Kursgliederung

- 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

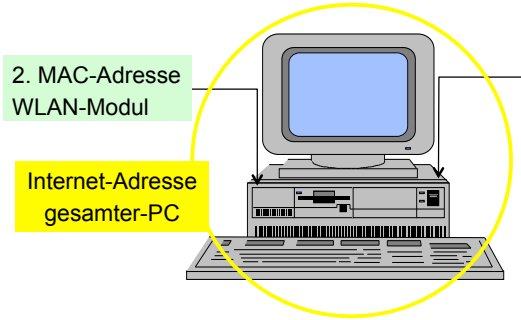
IP-Header Parameter (2)

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

Kursgliederung

MAC-Adressen und IP-Adressen

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



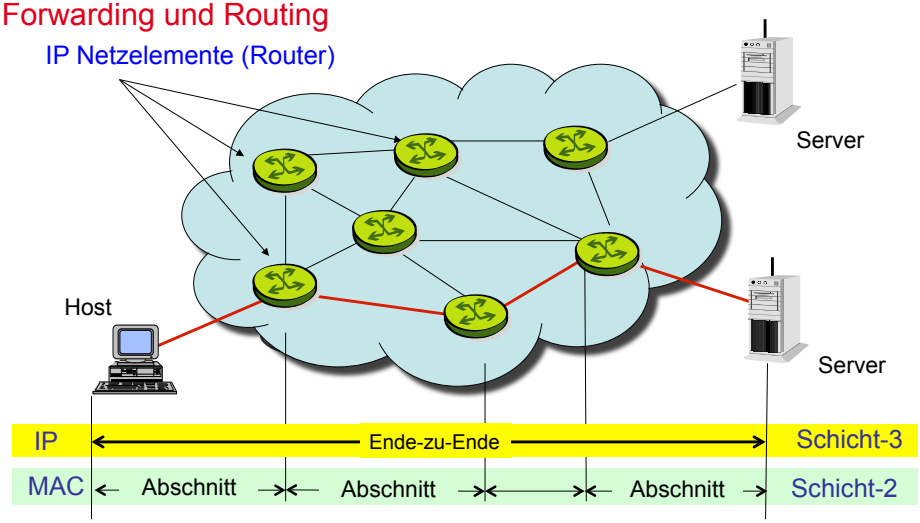
Lokal von PC zu PC, von PC zum Drucker, etc. werden IP-Pakete in **Ethernet-Rahmen** transportiert

Internet Adressen werden **zugeteilt**

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

MAC-Adressen und IP-Adressen : Forwarding und Routing

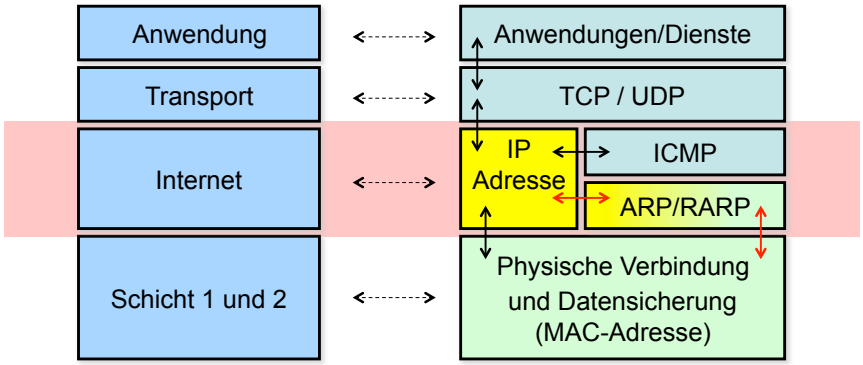
IP Netzelemente (Router)



IP - MAC Adressenzuordnung

DHBW Stuttgart

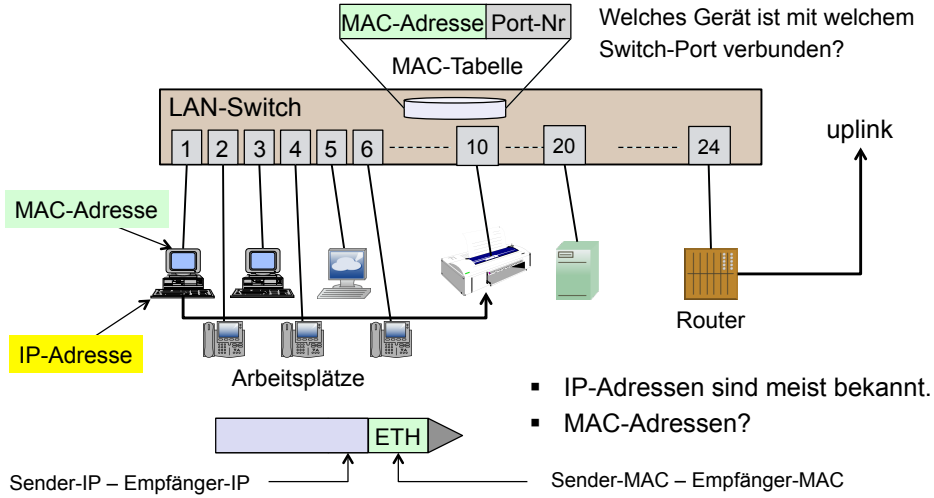
Die Kooperation zwischen Schicht-2 und Schicht-3 spielt
für die Kommunikation im Anschlussbereich eine entscheidende Rolle.



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

Adressierung im LAN

DHBW Stuttgart

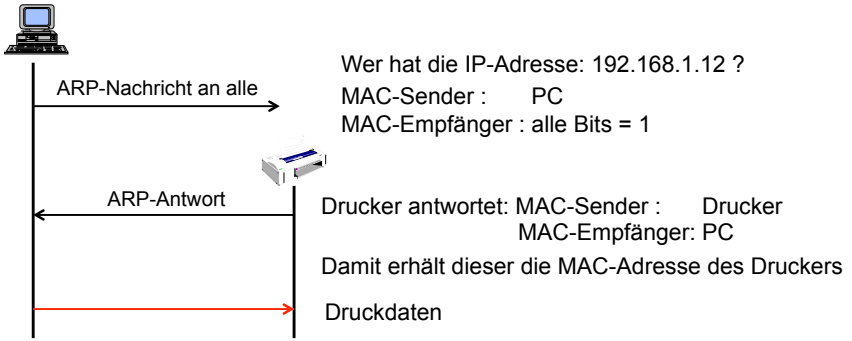


- IP-Adressen sind meist bekannt.
- MAC-Adressen?

Address Resolution Protocol – ARP Beispiel

DHBW Stuttgart

- 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



Aufgabe

DHBW Stuttgart

- 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?

Kursgliederung

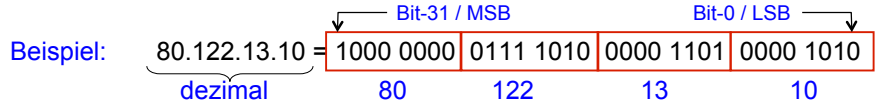
DHBW Stuttgart

- 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

DHBW Stuttgart

- 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

DHBW Stuttgart

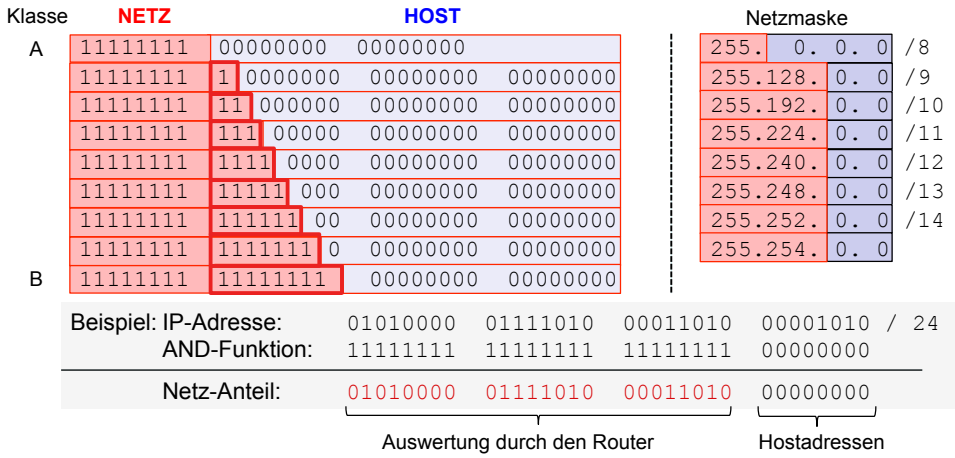
IPv4 Adressen werden in Klassen und Spezialfunktionen eingeteilt.
Die Klasseneinteilung geschieht je nach Größe der Netz- bzw. Host-Anteile.

- **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

DHBW Stuttgart

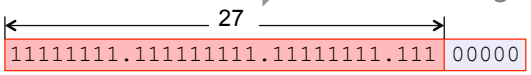
- Subadressierung durch Maskierung = Trennung von Netz- und Host-Adressen



Subnetz-Berechnung

DHBW Stuttgart

- 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		

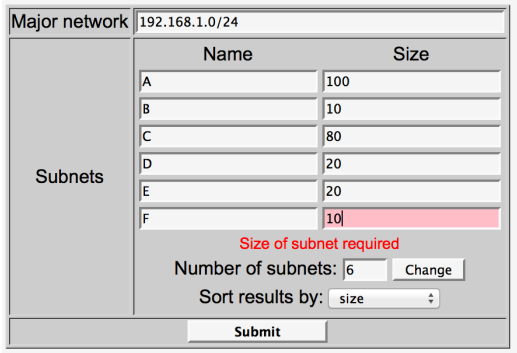
- **Beispiel: 192.168.10.40 /27 :**

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

DHBW Stuttgart

- **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

DHBW Stuttgart

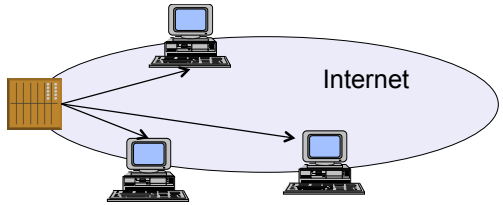
- Nicht-öffentliche Adressenbereiche
  - sind nicht eindeutige, mehrfach verwendbare Adressen
  - werden verwendet für effektive Verwendung des begrenzten Adressraumes
  - sind durch spezielle IETF-Standards definiert
- Als **nicht-öffentliche Adressbereiche** sind reserviert:
  - 10. 0. 0. 0 – 10.255.255.255 (/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

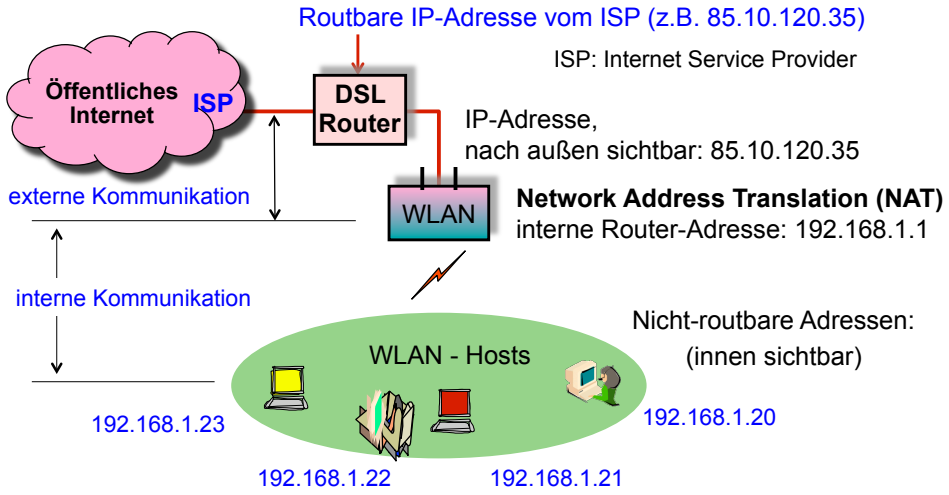
DHBW Stuttgart

- 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



Kursgliederung

- 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

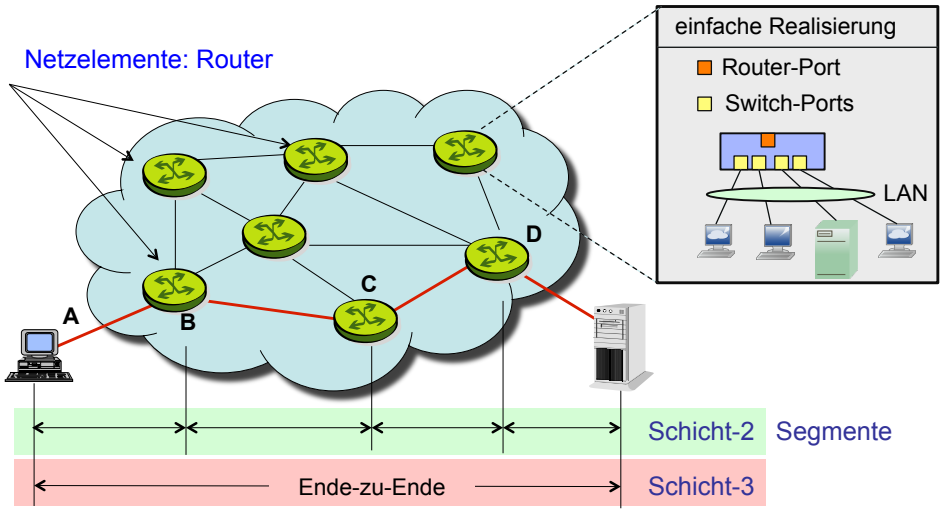
Grundlegender Prozess in allen Telekommunikations- Netzen

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

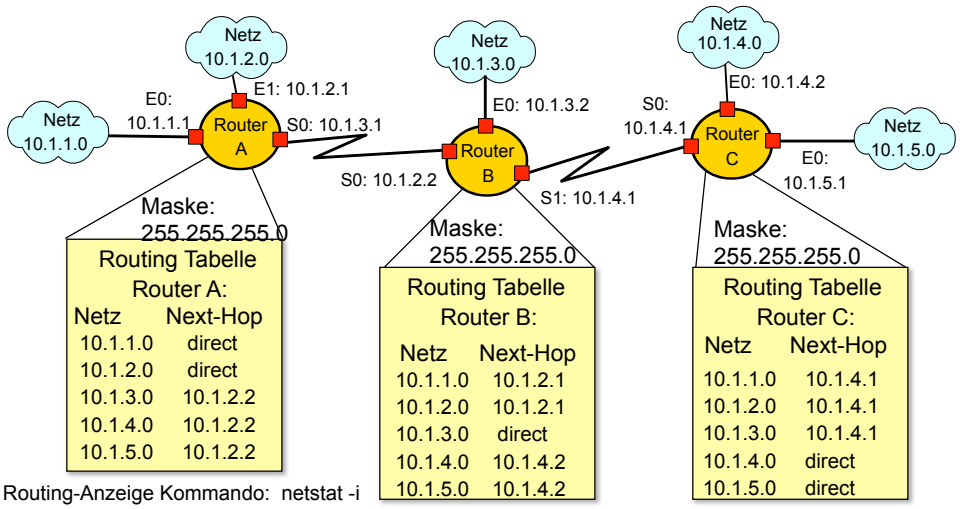
DHBW Stuttgart

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

DHBW Stuttgart



Routing-Anzeige Kommando: netstat -i

Routing Protokolle

DHBW Stuttgart

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

DHBW Stuttgart

- 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

DHBW Stuttgart

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

DHBW Stuttgart

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

DHBW Stuttgart

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

Kursgliederung

DHBW Stuttgart

- 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

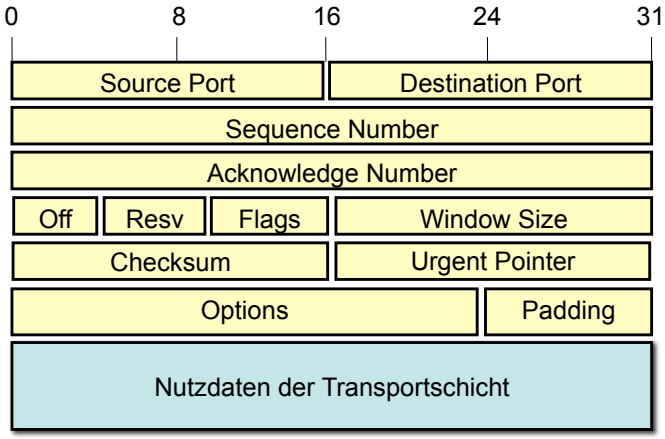
DHBW Stuttgart

- 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

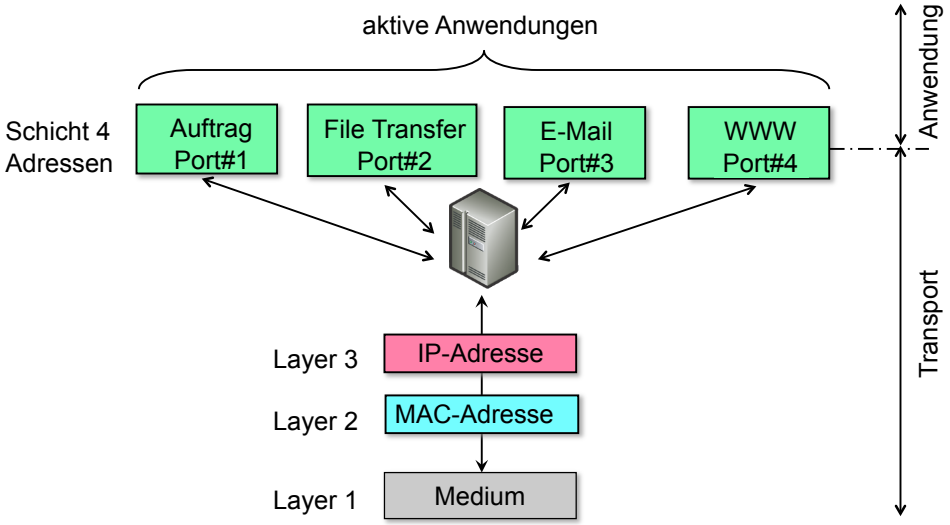
DHBW Stuttgart

RFC 793



Transport-Adresse (Port)

DHBW Stuttgart



Standard Anwendungen

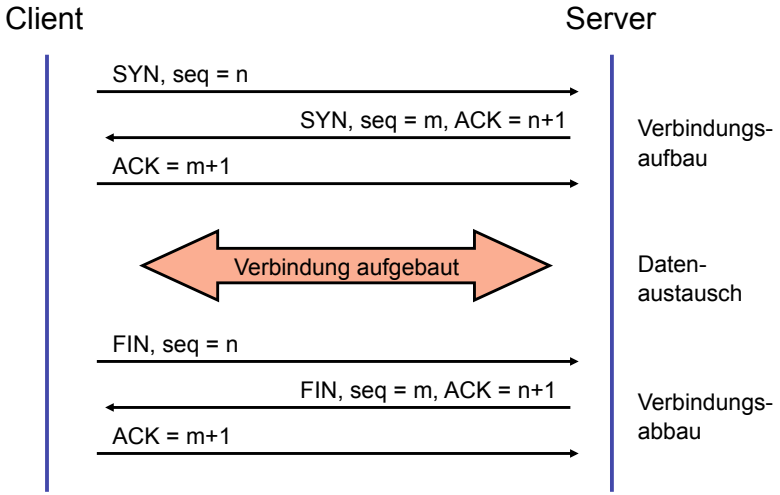
DHBW Stuttgart

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

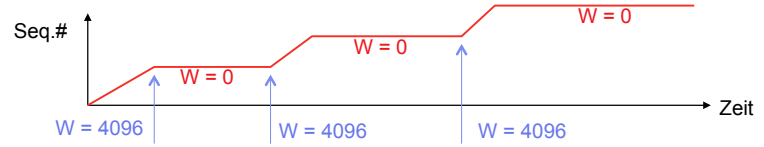
.....

TCP Signalisierung

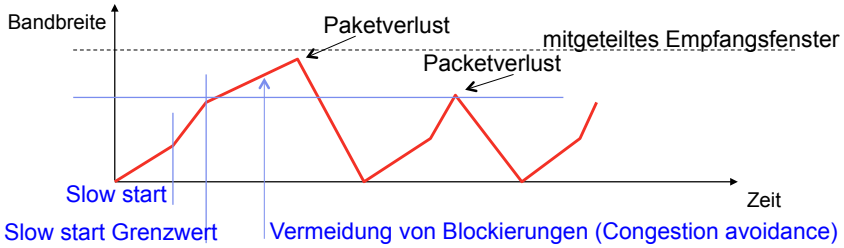


Flusskontrolle / Blockierungs-Kontrolle

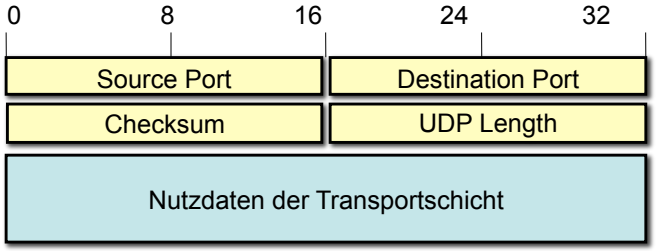
1. Der Empfänger bestimmt die Quittungs-Fenstergröße des Senders



2. Paketverlust:



User Datagram Protocol UDP



RFC 768

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

Kursgliederung

- 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

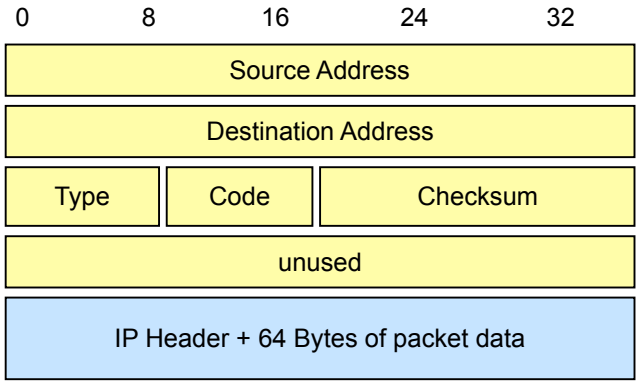
- ICMP ist ein integraler Bestandteil des Internet Protokolls, und muss in jedem IP-Modul implementiert sein. ICMP Protocol-Id = 1
- ICMP Nachrichten zeigen Protokollfehler bei der Verarbeitung von IP-Paketen an.
- ICMP Nachrichten werden in verschiedenen Umständen generiert:
  - wenn ein Paket sein 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):



Rechnerkommunikation und Vernetzung Teil 3: Voice over IP

Dr. Leonhard Stiegler
Nachrichtentechnik

www.dhbw-stuttgart.de

Kursgliederung

DHBW Stuttgart

- Raspberry PI
- Netzwerkdiagnose
  - Kommandos
  - Analyse-Software Wireshark
  - Arbeiten mit Wireshark
- Asterisk – VoIP Einführung
- Asterisk Software
- Asterisk Programmierung

Laboraufbau : Raspberry PI

DHBW Stuttgart

Raspberry PI

- Einplatinen-Rechner mit Kommunikations- und Funktions-Schnittstellen
- ARM Prozessor
- OS: Debian Linux Derivat auf 8GB Typ10 SD-Speicherkarte
- Kommunikationsschnittstellen
  - RJ45 Ethernet, USB, HDMI, Video-Out
  - WLAN via USB-Stecker
- Funktionsschnittstellen
  - General-Purpose I/O (GPIO) mit I^2C, SPI, ...
- Anwendung: Netzwerkdiagnose (Wireshark)
- Anwendung: VoIP Telefonserver (Asterisk)

Kursgliederung

DHBW Stuttgart

- Raspberry PI
- Netzwerkdiagnose
  - Kommandos
  - Analyse-Software Wireshark
  - Arbeiten mit Wireshark
- Asterisk – VoIP Einführung
- Asterisk Software
- Asterisk Programmierung

Test und Diagnose Tools: ipconfig / ifconfig

DHBW Stuttgart

- IP Verbindungsanalyse (Connectivity)
  Zeigt die eigene IP- und MAC-Adresse an
  Windows: ipconfig (im DOS-Fenster) Linux/Mac: ifconfig
- Beispiel:

```
Ethernetadapter LAN-Verbindung 3:
        Verbindungspezifisches DNS-Suffix: Speedport_W_700V
         Beschreibung. . . . . . . . . . . : Ethernetadapter der AMD-PCNET-Familie #2
        Physikalische Adresse . . . . . . : 08-00-27-35-47-D6
        DHCP aktiviert. . . . . . . . . . : Ja
        Autokonfiguration aktiviert . . . : Ja
        IP-Adresse. . . . . . . . . . . . : 192.168.2.102
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 192.168.2.1
        DHCP-Server . . . . . . . . . . . : 192.168.2.1
        DNS-Server. . . . . . . . . . . . : 192.168.2.1
        Lease erhalten. . . . . . . . . . : Freitag, 6. September 2013 16:16:04
        Lease läuft ab. . . . . . . . . . : Dienstag, 10. September 2013 16:16:04
```

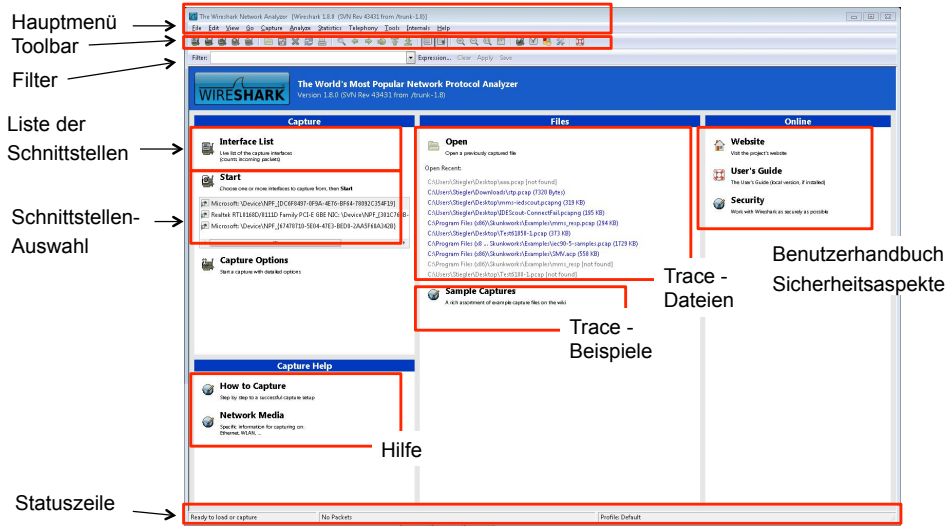
Test und Diagnose Tools: Netstat

- IP Verbindungsanalyse (Connectivity)
  - Zeigt die aktiven Verbindungen (Windows: im CMD-Fenster: netstat)
- Beispiel

Aktive Verbindungen

Proto	Lokale Adresse	Remoteadresse	Status
TCP	vm-win:1201	localhost:44080	HERGESTELLT
TCP	vm-win:1203	localhost:44080	HERGESTELLT
TCP	vm-win:1205	localhost:44080	SCHLIESSEN_WARTEN
TCP	vm-win:1214	localhost:44080	HERGESTELLT
TCP	vm-win:44080	localhost:1201	HERGESTELLT
TCP	vm-win:44080	localhost:1203	HERGESTELLT
TCP	vm-win:44080	localhost:1205	FIN_WARTEN_2
TCP	vm-win:44080	localhost:1214	HERGESTELLT
TCP	vm-win:1202	95.100.97.67:http	HERGESTELLT
TCP	vm-win:1204	62.159.74.11:http	HERGESTELLT
TCP	vm-win:1215	62.156.238.46:http	HERGESTELLT

Protokollanalyse mit Wireshark : Startmenü



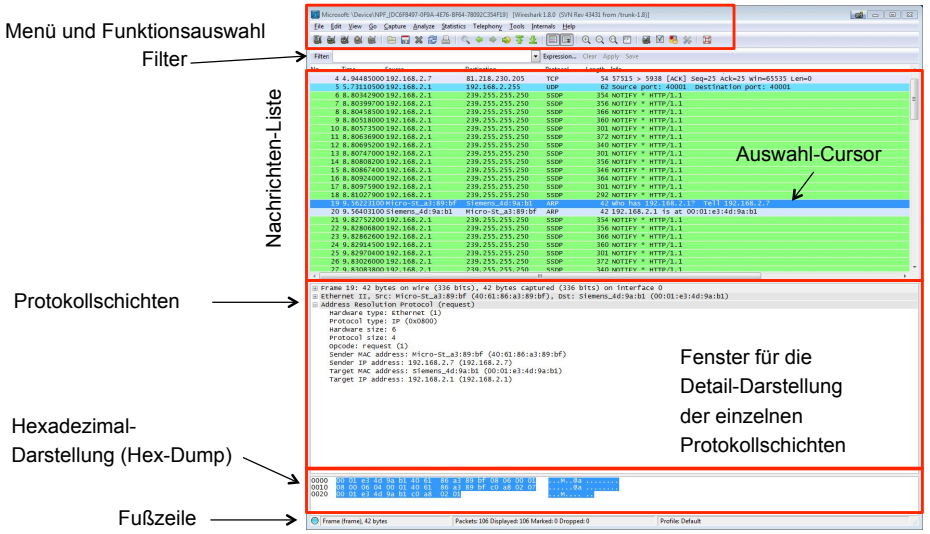
Wireshark :Toolbar

- Interface Auswahl
- Optionen Auswahl
- START Trace
- STOP Trace
- STOP+Restart Trace
- Datei öffnen
- Datei speichern
- Datei schließen
- Aktuelle Trace Datei noch einmal öffnen
- Drucken Dialog
- Suchen Dialog
- Capture Filter Dialog
- Display Filter Dialog
- Einstellungen Dialog
- Farb-Einstellungen
- Hilfe

Cursor bewegen:

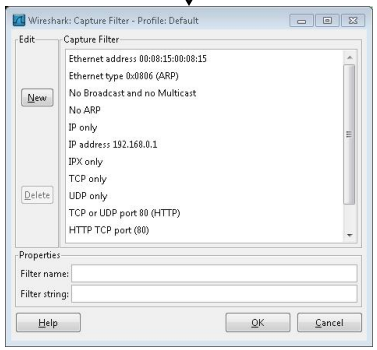
- Rückwärts
- Vorwärts
- Springen zu
- Zum 1. Paket
- Zum letzten Paket
- Ausgabe vergrößern
- Ausgabe verkleinern
- Originalgröße

Wireshark Bildschirmbereiche



Filter-Arten

- **Capture Filter**:
  - Hauptmenü – Capture – Capture Filters …
  - Aufnahme-Filter
    Datenmenge wird bei der **Aufnahme** gefiltert
- **Display Filter**:
  - Hauptmenü – Analyze – Display Filters …
  - Anzeige-Filter
    Datenmenge wird bei der **Wiedergabe** gefiltert



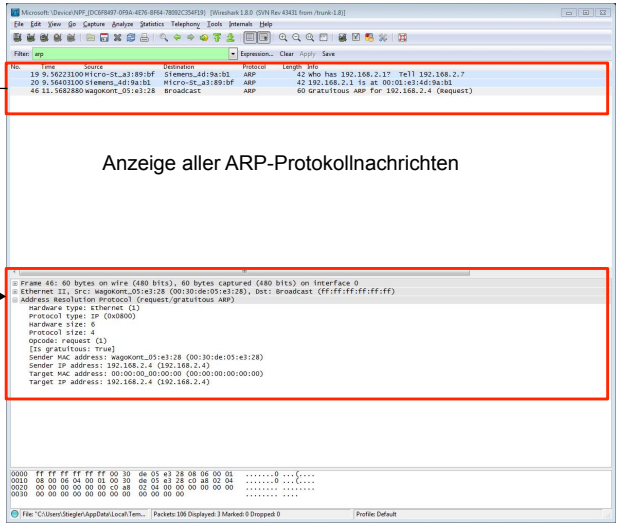
Protokoll-Filter Direkteingabe

Filter = **arp**
Nur ARP-Nachrichten werden angezeigt

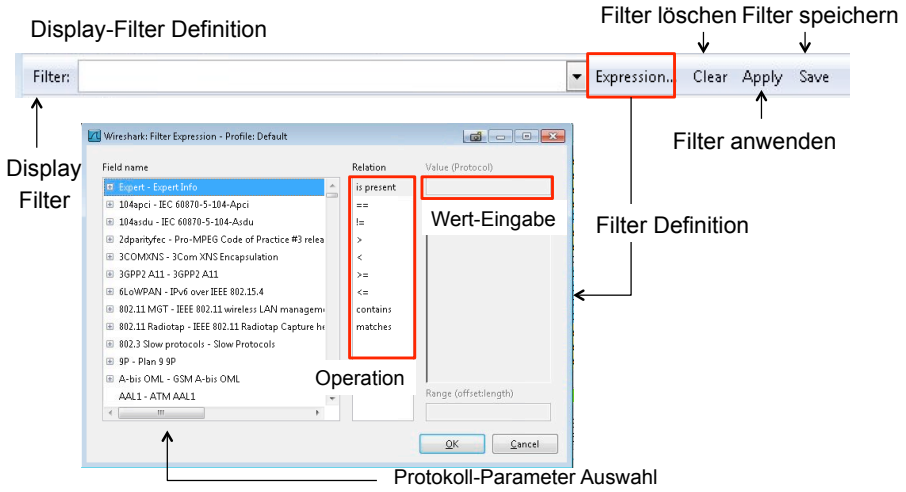
Anzeige aller ARP-Protokollnachrichten

Dekodierung der ausgewählten Nachricht

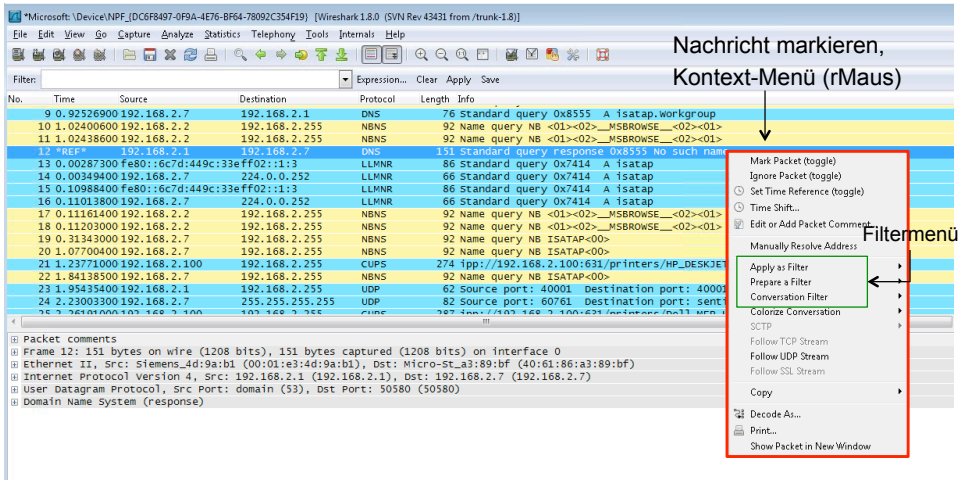
ARP: Address Resolution Protocol



Manuelle Protokoll-Filter Definition



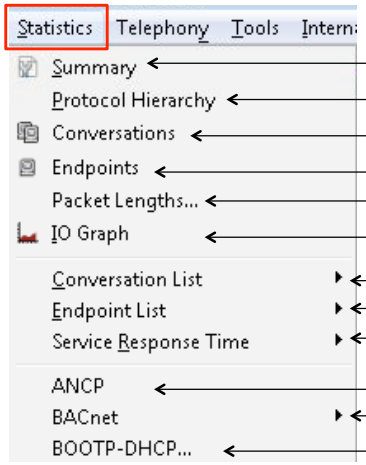
Automatische Protokoll-Filter Definition



Statistik-Menü (1)

DHBW Stuttgart

Hauptmenü



BAC: Building Automation and Control

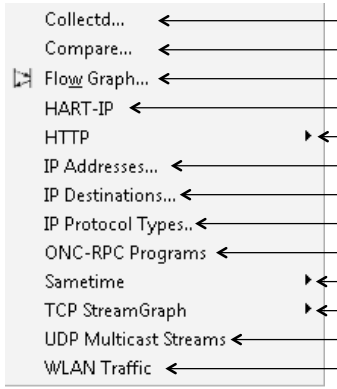
- Zusammenfassung der Trace-Daten
- Trace-Daten: Protokollstatistik
- Kommunikations-Statistik
- Adressen-Statistik
- Statistik: Paket-Länge
- Statistik: Zeitverteilung
- Liste der Verbindungen
- Liste der Adressen-Endpunkte
- Liste der Antwortzeiten
- Access Node Control Protocol Statistik
- BAC-Network Statistik
- Bootstrap-Protocol und DHCP Statistik

Statistik-Menü (2)

DHBW Stuttgart

Fortsetzung:

HART-IP: Highway Addressable Remote Transducer over IP
ONC-RPC: RFC 1831 Network File System (NFS) - Protokoll

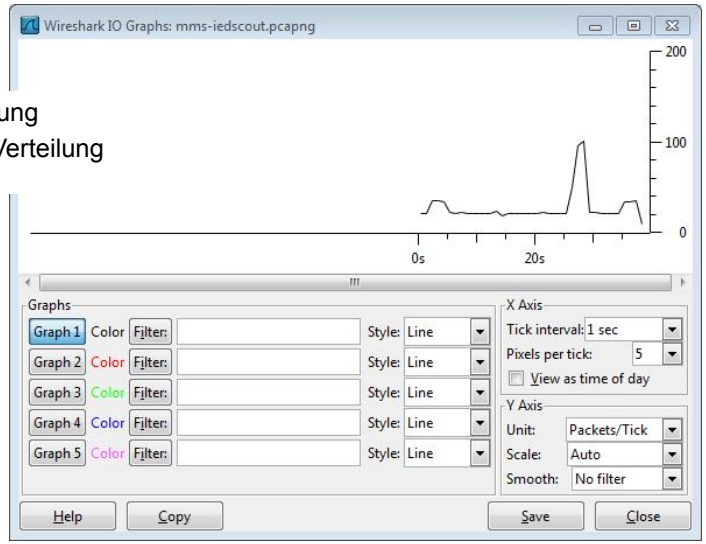


- Paketzähler und Filter
- Vergleich von Capture-Dateien
- Flussdiagramm erzeugen
- HART-IP Statistik
- Statistik: Paket-Zähler, Requests, Lastverteiluung
- Statistik: IP-Adressenverteilung
- IP-Adressen, Transportschicht und Portnummer
- Liste der Transportverbindungen
- Liste der ONC-RPC Applikationen
- Anzahl Nachrichten mit gleichem Zeitstempel
- TCP-Nachrichtentransport Statistik
- Liste der UDP-Multicast Streams
- WLAN - Verkehrsdaten

Statistik-Beispiel: Lastverteilung

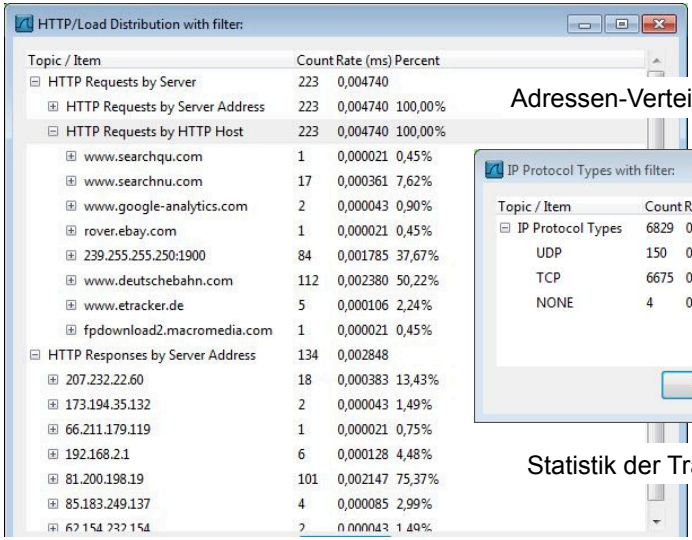
DHBW Stuttgart

Diese Darstellung
zeigt die Zeit-Verteilung
der Pakete

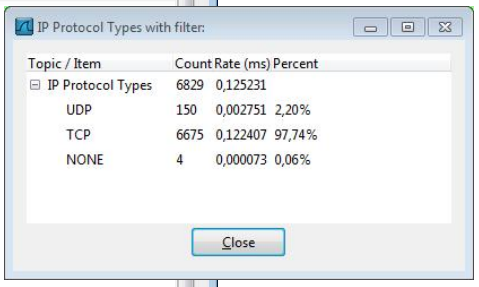


Statistik-Beispiel: Adressen- und Protokolle

DHBW Stuttgart



Adressen-Verteilung der Pakete

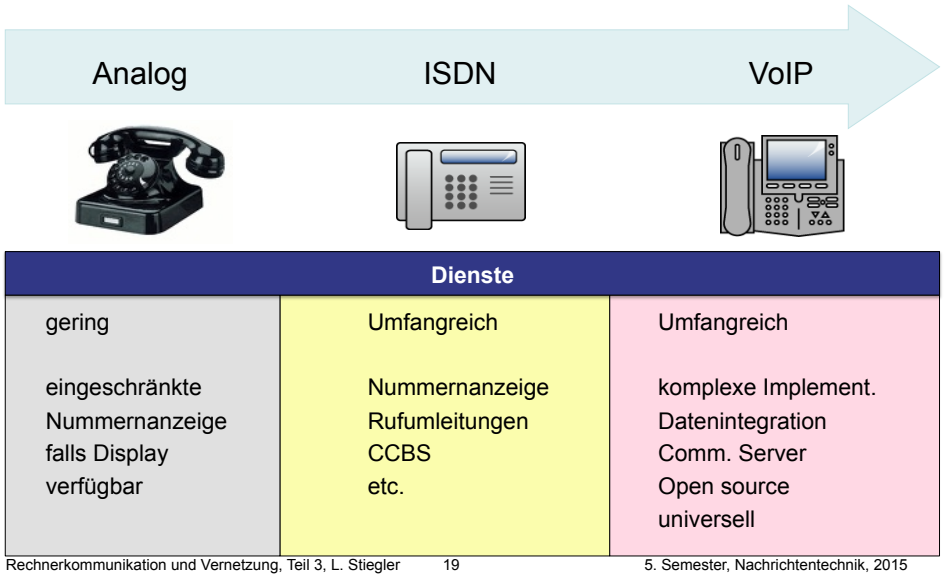


Statistik der Transportprotokolle

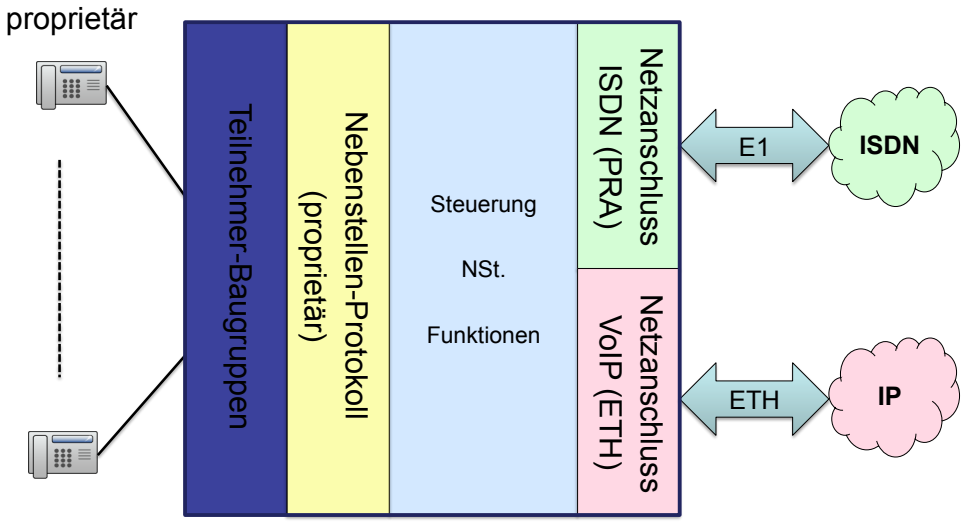
Kursgliederung

- Raspberry PI
- Netzwerkdiagnose
  - Kommandos
  - Analyse-Software Wireshark
  - Arbeiten mit Wireshark
- Asterisk – VoIP Einführung
- Asterisk Software
- Asterisk Programmierung

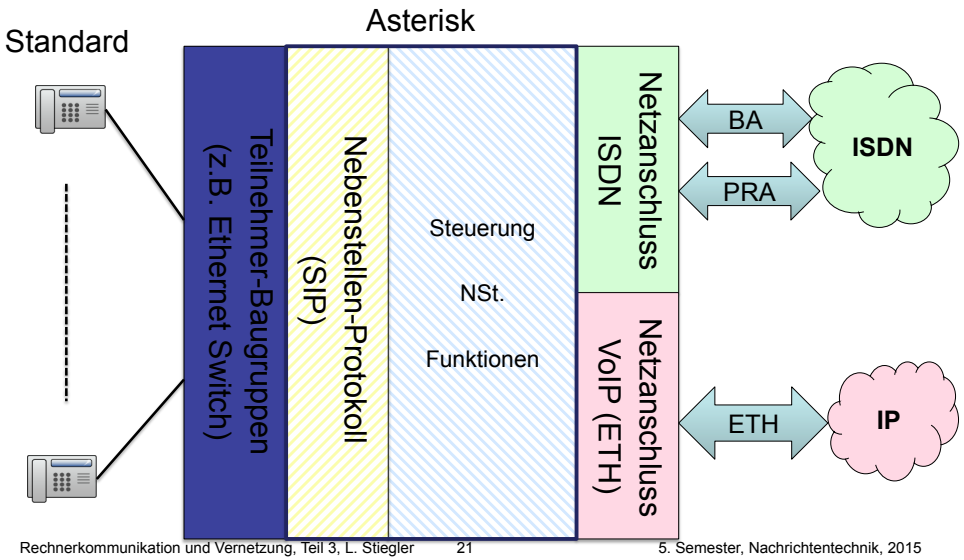
Evolution der Telefon-Dienste



Nebenstellentechnik (Hardware)



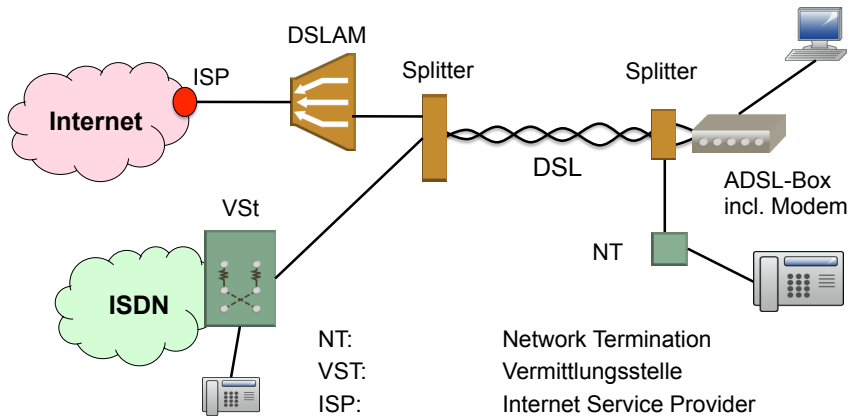
Nebenstellentechnik (Software)



VoIP und DSL: ADSL

DHBW Stuttgart

ADSL: Trennung von Sprache und Daten

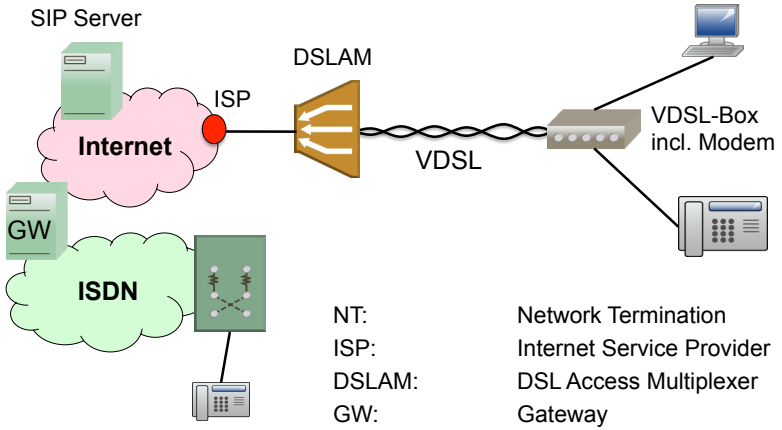


NT:	Network Termination
VST:	Vermittlungsstelle
ISP:	Internet Service Provider
DSLAM:	DSL Access Multiplexer

VoIP und DSL: VDSL

DHBW Stuttgart

VDSL: Sprache und Daten kombiniert

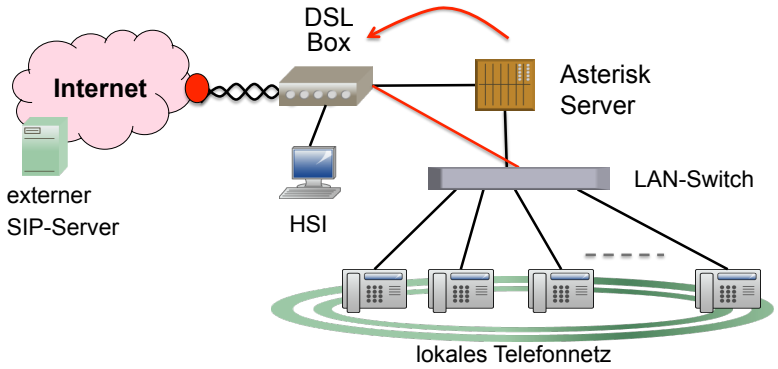


NT:	Network Termination
ISP:	Internet Service Provider
DSLAM:	DSL Access Multiplexer
GW:	Gateway

Asterisk Netzeinbindung

DHBW Stuttgart

Asterisk als lokale VoIP Vermittlungsstelle



HSI: High-Speed Internet

SIP Konzept

DHBW Stuttgart

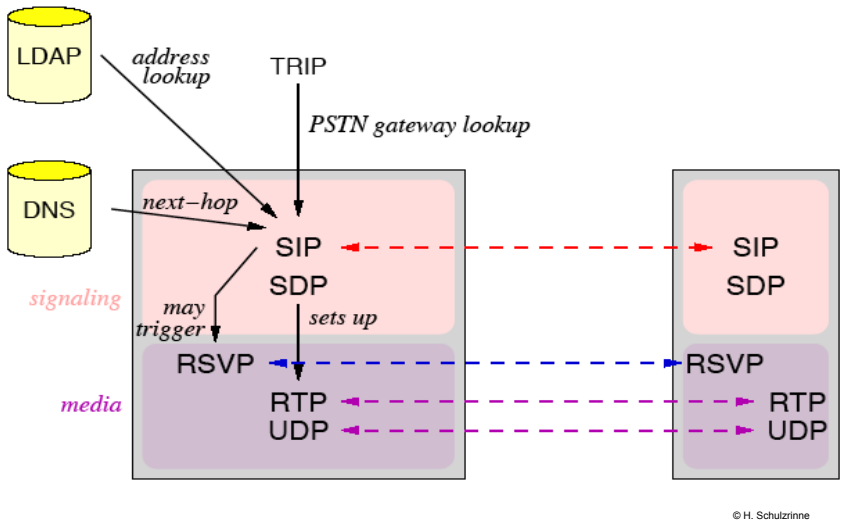
Die Protokollfamilie des Session Initiation Protocol (SIP) bildet eine Multimedia Architektur.

Andere dazu gehörende Protokolle sind :

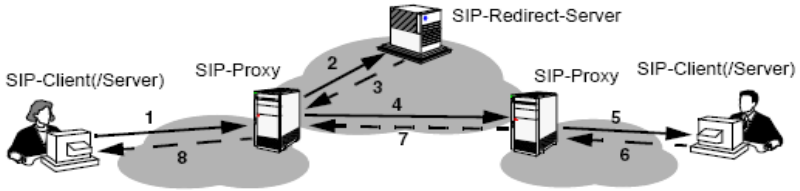
- Real Time Transport Protocol (RTP)
- Real Time Control Protocol (RTCP)
- Session Description Protocol (SDP)
- Real Time Streaming Protocol (RTSP)
- Gateway Control Protocol (MEGACO) etc.

Die grundlegenden SIP Funktionen werden durch diese Protokolle ergänzt damit vollständige Multimediadienste angeboten werden können.

SIP Protokollfamilie



SIP Netzelemente

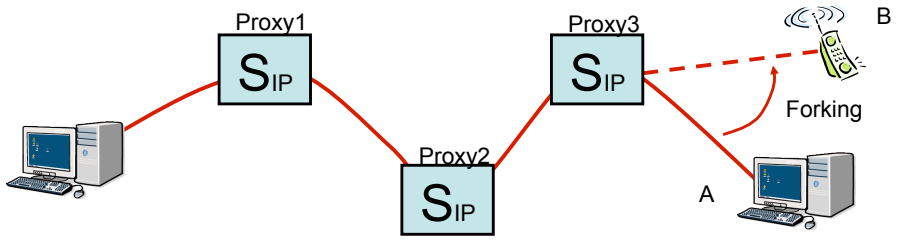


Nachrichtenfolge:

1. User Verbindungsaufbau (INVITE message) zu einem SIP-Proxy
2. Zieladresse wird vom redirection server ermittelt
3. Antwort: Zieladresse (z.B. Rufumleitung)
4. INVITE Nachricht zum Ziel-Proxy
5. INVITE zum SIP-Zielendgerät

6. – 8 Antworten vom SIP-Zielendgerät über den Signalisierungspfad

SIP Message Routing



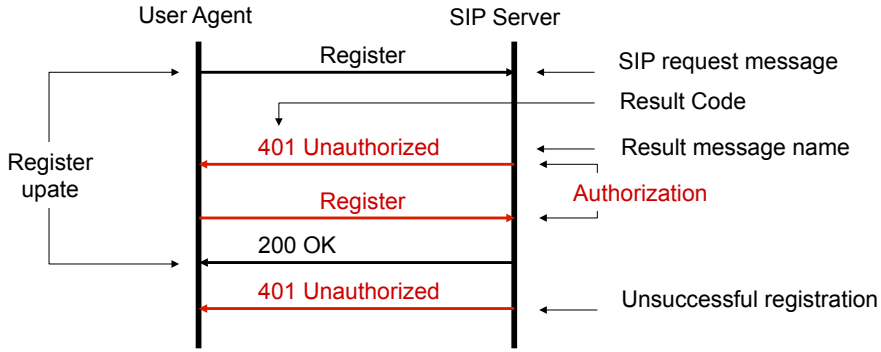
Pfad: SIP Proxy-1 - SIP Proxy-2 - SIP Proxy-3

Route: wird verwendet, um ein SIP-Request über Proxyrechner zum Ziel und zurück zu leiten Diese “Route list” + “Contact” - Parameter heissen “Route Set”.

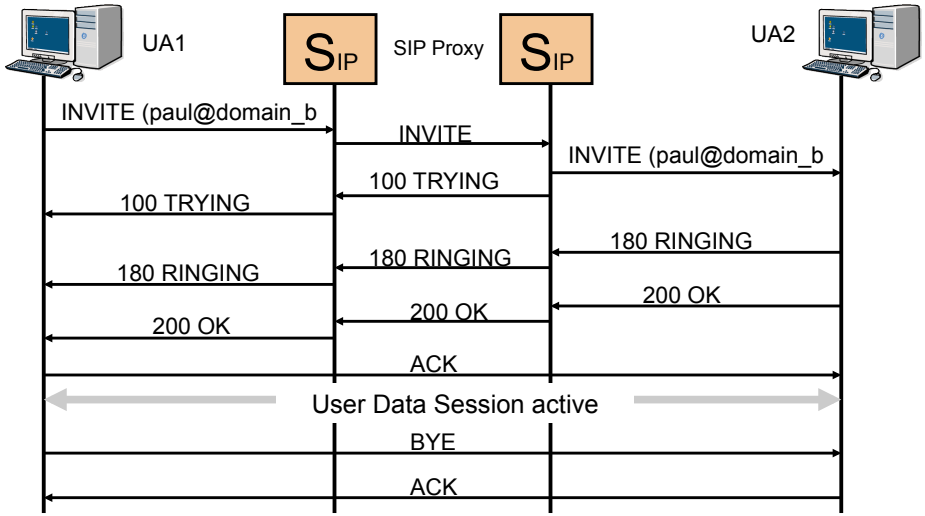
Register Prozedur

Die Registrierung verbindet eine Geräteadresse mit einem SIP user Address of Record (AOR)

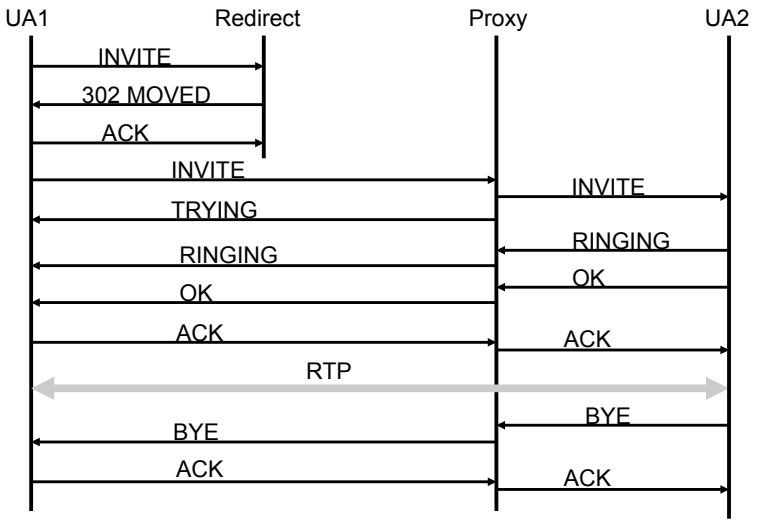
Die Registrierung läuft nach einer gewissen Zeit aus und muss periodisch erneuert werden



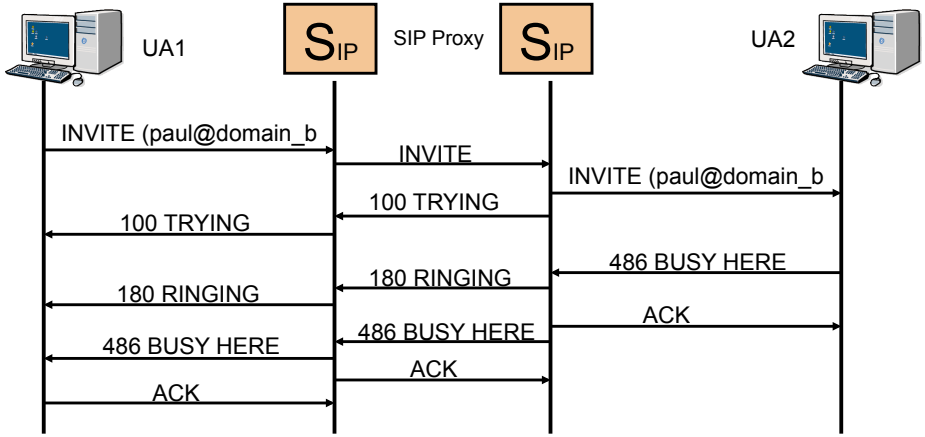
Verbindungsaufbau



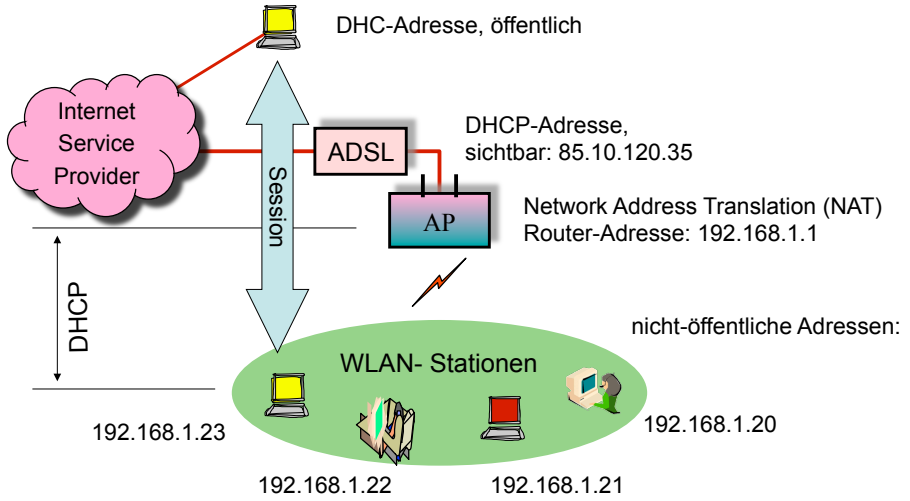
Redirect Server



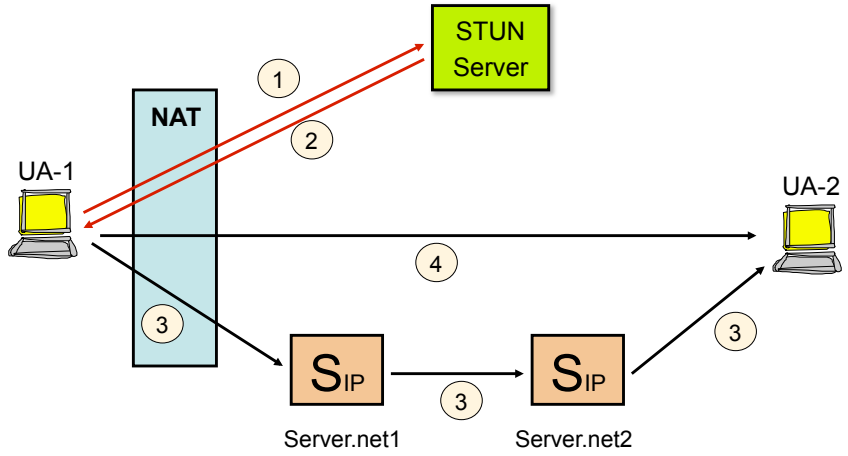
Teilnehmer Besetzt (User Busy)



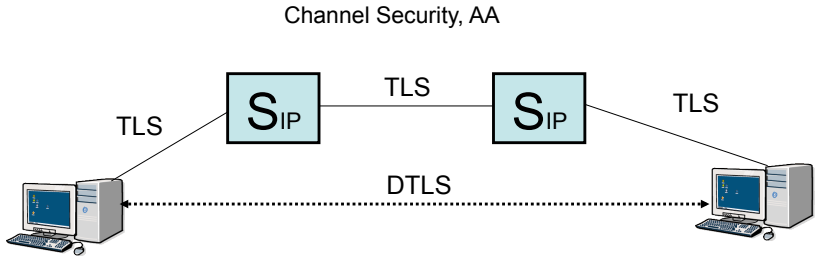
NAT Traversal: Beispielkonfiguration



NAT Traversal



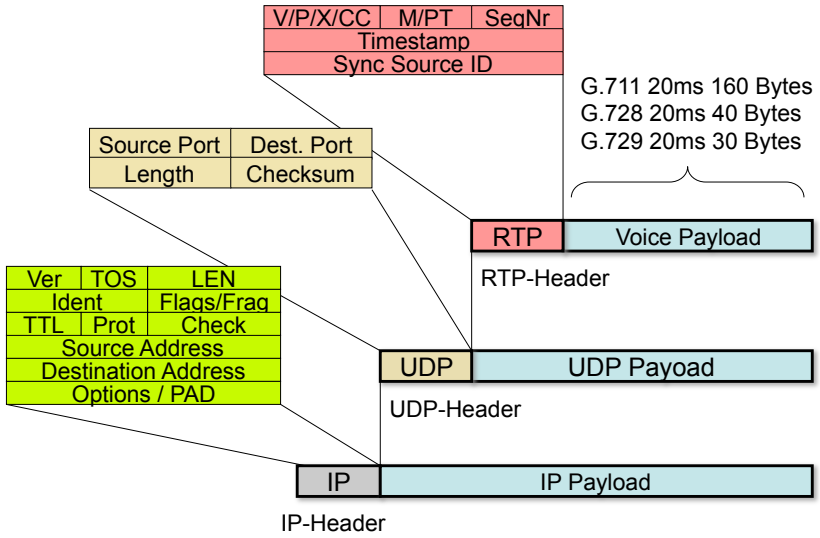
SIP Sicherheit



Verwendet Transport Layer Security (TLS)
Datagram TLS (DTLS) für UDP
Authentisierung : Proxy überprüft user
Proxy überprüfen einander
UA verifiziert proxy
UA(S) verifiziert UA(C) mittels S/MIME

AA: Authentication & Authorization

RTP Protokollschichten



RTP Payload Types

Payload Art	Kodierung	Audio/Video	Abtasttakt	Kanäle
0	PCMU	A	8000	1
2	G.721	A	8000	1
3	GSM (FR)	A	8000	1
9	G.722	A	8000	1
15	G.728	A	8000	1
26	JPEG	V	90,000	n.a.
31	H.261	V	90,000	n.a.
96 - 127	dynamic	dynamic	dynamic	dynamic

Session Description Protocol (SDP)

SDP definiert in der RFC 2327.

SDP beschreibt Multimedia Sessions:

Parameter Gruppen:

- session description (e.g. Name, owner/creator ..)
- time description (Aktive Zeit, Wiederholungszeit)
- media description (Titek, Bandbreiteninfo, Verschlüsselung, ..)

SDP ermöglicht die Teilnahme an einer Multimedia Session

SDP enthält kein Transportprotokoll

SDP Protokoll-Information wird im SIP-Body transportiert

Sprachqualität

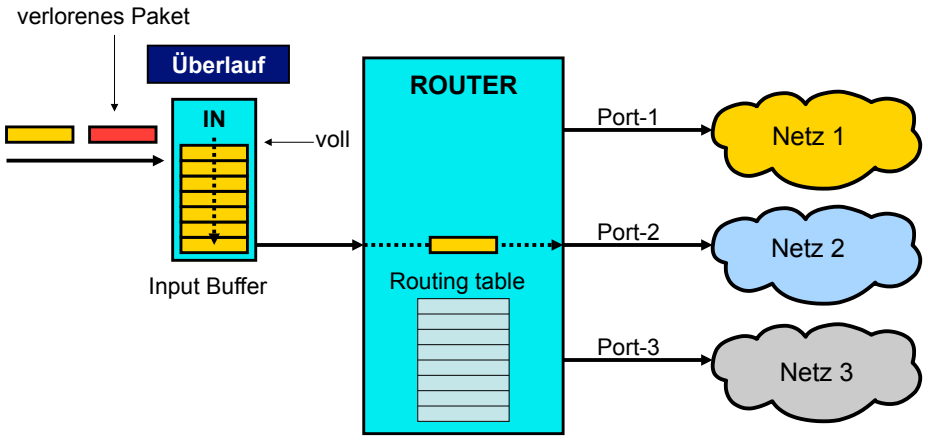
Objektive Sprachqualitätsmessungen verwenden VQA (Voice Quality Analysis) Technik.

Sbjektive Sprachqualitätsmessungen verwendet MOS (Mean Opinion Score) Skala bestehend aus 5 Stufen (excellent – bad) gemäß ITU-T P. 800.

Die Sprachqualität hängt von folgenden Faktoren ab:

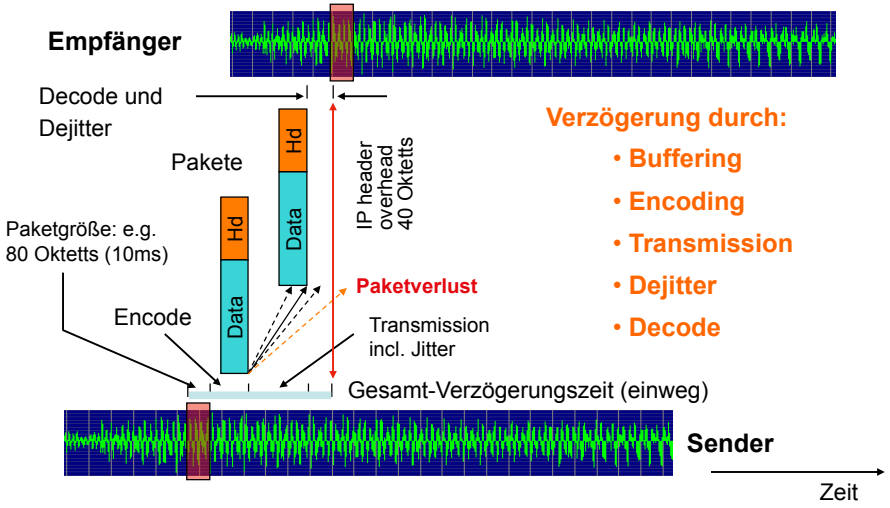
Packet Loss Rate	packets received / packets sent
End-to-end delay	packet received time - packet sent time
Delay jitter	Inter-packet delay time variation

Paketverlust

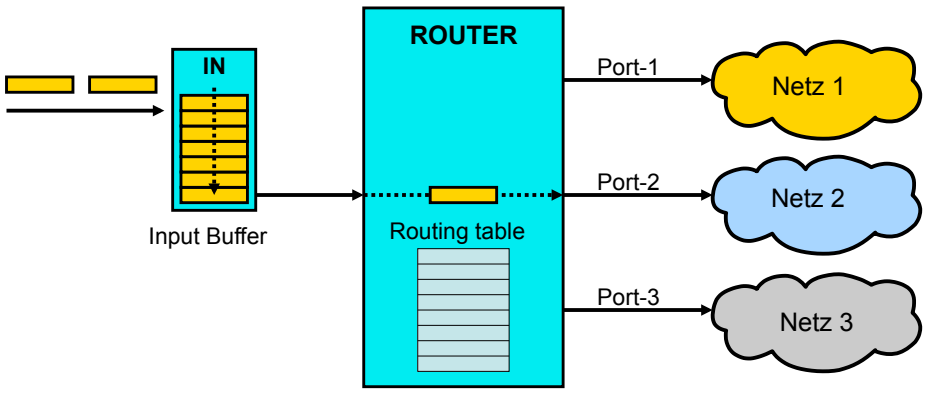


Ursache für Paketverlust:
Buffergröße nicht ausrechend

Paketverzögerung (1)

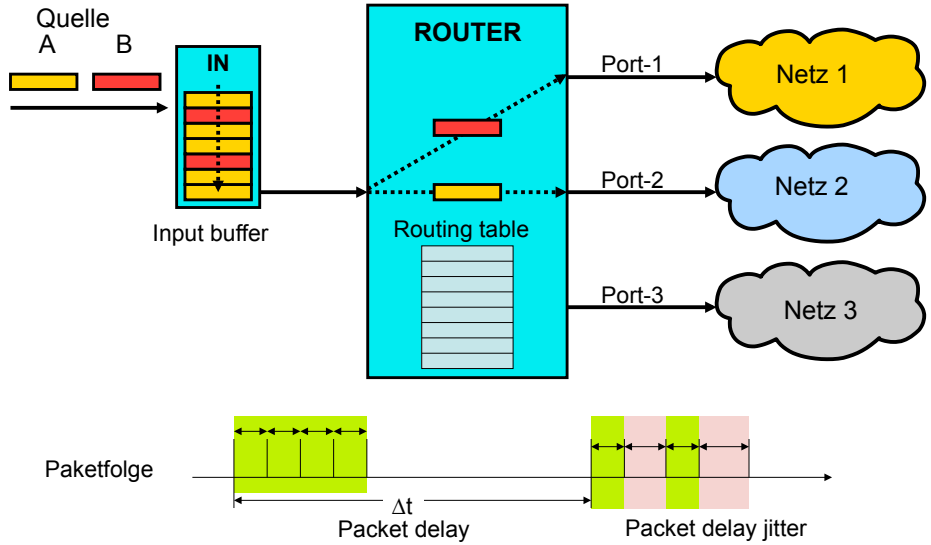


Paketverzögerung (2)



Ursache der Paketverzögerung im Router:
I/O Operations, Prozessorzeit

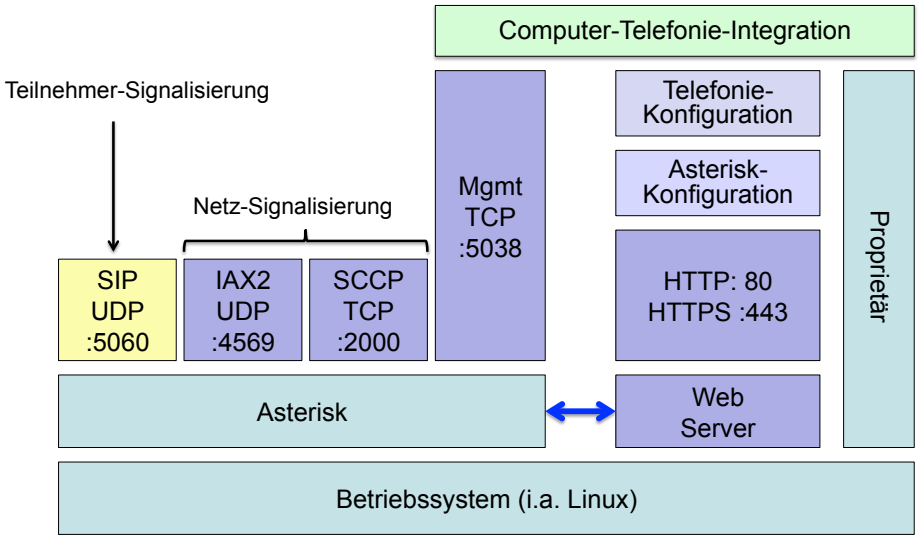
Paket Jitter



Kursgliederung

- Raspberry PI
- Netzwerkdiagnose
  - Kommandos
  - Analyse-Software Wireshark
  - Arbeiten mit Wireshark
- Asterisk – VoIP Einführung
- Asterisk Software
- Asterisk Programmierung

Asterisk Server Aufbau



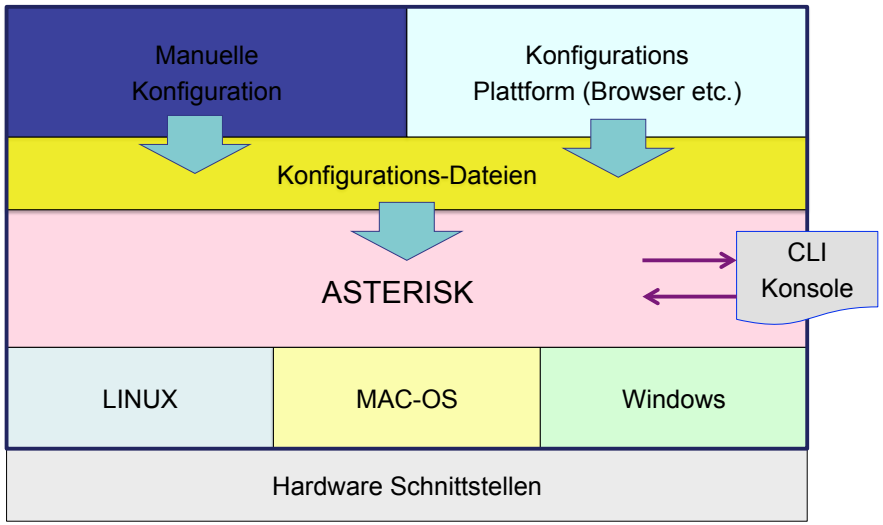
Asterisk Installation: Software Pakete

- **Software-Pakete unter Linux:**
  - DEBIAN und UBUNTU : Asterisk mit **APT** installieren
    Benutzerschnittstelle für die Verwaltung von Software-Paketen
  - Red Hat und CentOS : Asterisk mit **YUM** installieren
    Software-Paketmanagement System
  - Software-Komponenten: Basispaket: Asterisk
    DAHDI : Hardware Treiber
- **Windows :**
  - Asterisk Win32 mit PBX-Manager Softwareplattform
  - 3CX Asterisk-basierte Softwarelösungen
  - AsteriskNOW von DIGIUM

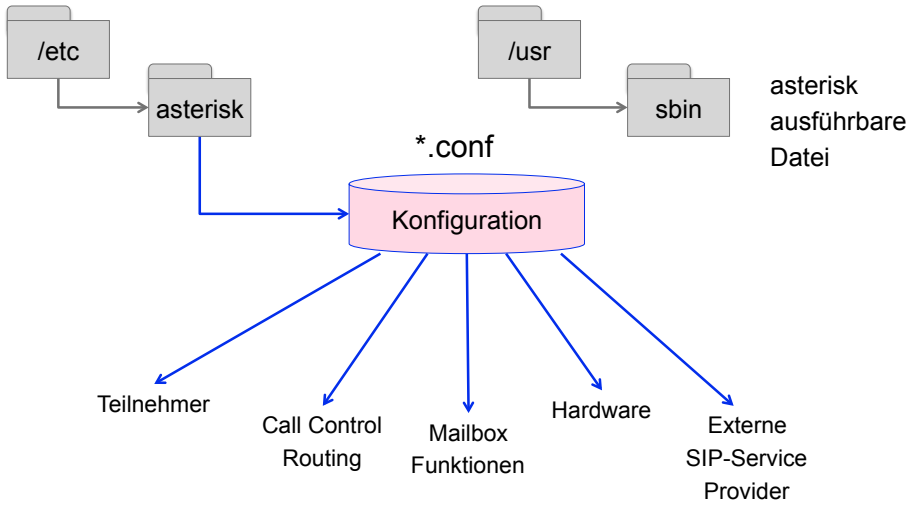
Asterisk Installation: Hardware

- Hardware Dimensionierung
  - Anzahl gleichzeitiger Telefongespräche
  - Anzahl und Art abgehender Telefonleitungen (analog, ISDN (BRA, PRA), Ethernet)
  - Art der Telefongeräte (Analog/ISDN, SIP, H.323,…)
  - Art der Sprachkodierer (G.711, …)
  - Erforderliche Features (Echokompensator, Sprach-Mailbox, Konferenz-Funktionen,…)
  - Anforderungen bezüglich Verfügbarkeit, Erweiterungsfähigkeit
  - IP-Netzanforderungen: Echtzeitfähigkeit, Dienstgüte (QoS)

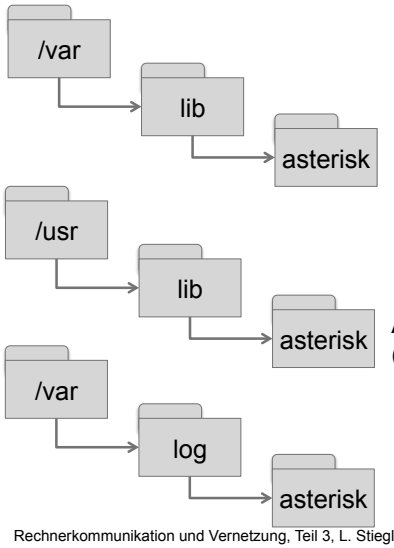
Asterisk Software Struktur



Asterisk Konfigurationsverzeichnis



Weitere Asterisk Verzeichnisse



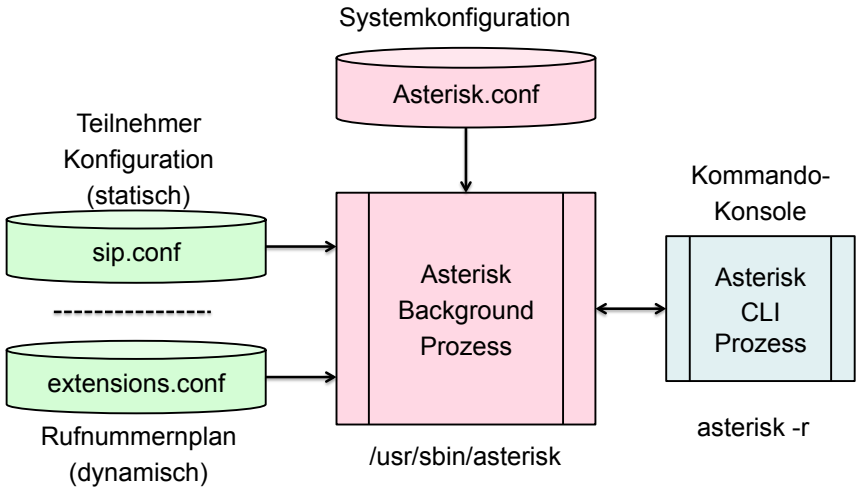
Unterverzeichnisse:

- agi-bin: Script-Dateien
- firmware: Hardware Gerätedateien
- keys: öffentliche Schlüssel
- mohmp3: Haltemusk-Dateien
- sounds: Sprache-Ansagedateien

Asterisk Module
(Anwendungen, Codecs, Formate, Channels

Asterisk Log-Information

Asterisk Prozesse



Asterisk Kommando Konsole - CLI

- CLI-Start mit dem Kommando: “asterisk -r”
- CLI-Kommandogruppen
- CLI-Liste der Kommandos: help <gruppenname>

core	DAHDI	dialplan	IAX2
System Kommandos	Hardware Kommandos	Routing Kommandos	Inter-Asterisk Exchange Kommandos
manager	sip	voicemail	rtp/rtcp
Asterisk Management	SIP Parameter	Voicemail Kommandos	rtp/rtcp Monitor

Wichtige Core-Kommandos

Asterisk CLI-Kommandos sind Versions-abhängig
Übersicht über die verfügbaren Kommandos mit: “help”

- Core – CLI-Kommandos
  - **core show sysinfo:**
    Anzeige der Prozesse und Speichervolumen
  - **core show settings:**
    System-Auslastung, Verzeichnisse, Subsysteme , Zeitgeber
  - **core show codecs:**
    Anzeige der unterstützten Codecs (Sprache, Bild, Video)
  - **core show setting :**
    Anzeige der SIP-Einstellungen
  - **core restart/stop (now):**
    Asterisk restart/stop

Wichtige CLI SIP-Kommandos

DHBW Stuttgart

- SIP – CLI-Kommandos
  - **sip show peers :**
    Anzeige der SIP-Telefone
  - **sip show registry :**
    Statusanzeige der registrierten Telefone
  - **sip set debug on :**
    Anzeige der SIP – Signalisierung
  - **sip show setting :**
    Anzeige der SIP-Einstellungen
  - **sip show users :**
    Liste der SIP-User

Wichtige CLI Dialplan-Kommandos

DHBW Stuttgart

- Dialplan – CLI-Kommandos
  - **dialplan show :**
    Anzeige des Dialplans
  - **dialplan add/remove extension :**
    Telefon hinzufügen / entfernen
  - **dialplan reload :**
    Dialplan laden – nach einer Veränderung
  - **dialplan show globals:**
    Anzeige der globalen Dialplan-Parameter
  - **dialplan show ?:**
    Liste der Dialplan Anzeigemöglichkeiten

Konfiguration: sip.conf

DHBW Stuttgart

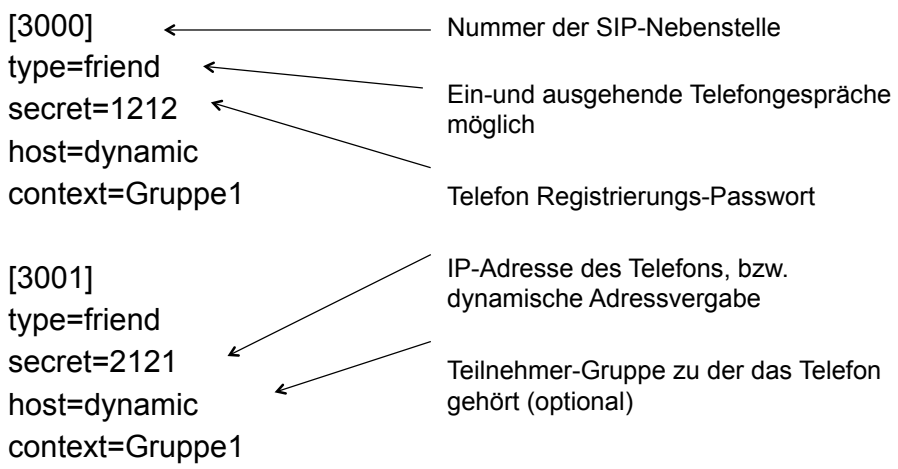
- Definition der einzelnen SIP-Telefone
- Registrierung und Konfiguration der VoIP-Parameter

Allgemeiner Teil: [general]
- IP-Adresse und Port-Nummer des Asterisk Servers

Spezieller Teil: [<nr>]
- Beschreibung der SIP-Telefone
  - SIP-Id
  - Caller-Id-Name + Caller-Id-Nummer
  - Dynamische IP-Adresse
  - User, secret: Identifikationsdaten <nr>,
  - Server-Adresse (Domain-Name)
  - NAT-Router vorhanden ?
  - Typ: friend = ein- und ausgehende Verbindungen erlaubt
  - Mailbox-nummer

Beispiel-Konfiguration: sip.conf

DHBW Stuttgart



SIP Provider Definition

Beispiel-Definition für einen Provider: “provider1” in sip.conf:

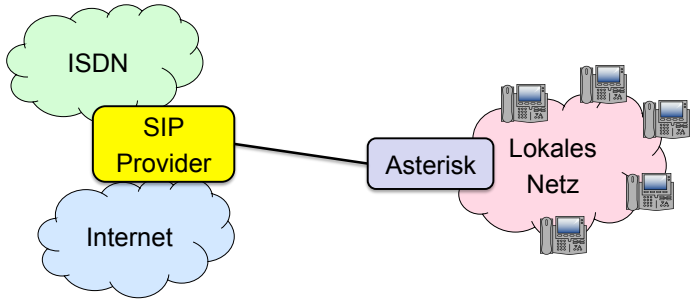
register => 123456:passwort@sip-provider1.de/123456

User	Passwort	Provider	User

```
[provider1]
type=friend
host=sip.provider1.de
fromdomain=sip.provider1.de
username=123456
fromuser=123456
secret=passwort
callbackextension=3000
transport=udp,tcp
nat=yes
```


Externe Registrierung

- Asterisk muss sich bei einem externen SIP-Server registrieren.
- Die Registrierung wird periodisch durchgeführt
- Das entsprechende Kommando lautet:
  - register => *user*[:*passwort*[:*authuser*]]@*host*[:*port*][/*extension*



Konfiguration: Extensions.conf

- Enthält den Rufnummern-Plan (Dialplan)
- Dialplan Aufgaben
  - logische Abarbeitung einer Telefon-Transaktion
  - logische Verbindungssteuerung
  - enthält Aktionen und Funktionen
  - ist in unterschiedliche Bereiche untergliedert
  - verwendet eine Script-Sprache: Asterisk Extension Language
  - allgemeines Script-Format:
    exten => extension,priority,command(parameters)

Dialplan Syntax

exten => extension,priority,command(parameters)

- extension: Rufnummer der Nebenstelle oder Name
- priority: Reihenfolge der Aktionen, beginnt mit 1
  keine Numerierungs-Lücken,
  ab nr. 2 kann Platzhalter “n” verwendet werden
- command: Steuerungs-Befehle (Dialplan Applications
- parameters: Befehl-Parameter

Dialplan Beispiele

Beispiele:

```
exten => 123,1, Answer( )
exten => 123,n,Playback(Ansage1)
exten => 123,n,Hangup( )

exten => 3000,1,Dial(SIP/3000)

exten => 3000,1,Dial(SIP/${EXTEN},60)
exten => 3000,2,Hangup()

exten => 123456,1,Dial(SIP/3000)
```

externe SIP-UserId

Falls ein Telefon die Nr. 123 wählt wird, so geschieht folgendes:

1. Ruf wird angenommen
2. Ansage1 wird abgespielt
3. Ruf wird beendet (auflegen)

1. Verbinden mit Nummer 3000

1. Verbinden mit Nummer (EXTEN = 3000), Timer: 60 sek.
2. Falls nicht erfolgreich: Auflegen

Eintreffendes Gespräch von 123456 erreicht die Extension 3000 "123456" muss in sip.conf definiert sein.

Mailbox Funktionen

- Konfiguration in Datei: voicemail.conf
- Syntax: MailboxNr => Paßwort, Name, E-Mail, Pager, Optionen
  Mailbox-Nummer = Extension
- Beispiele (in voicemail.conf):
  - 3000 => 000,Mailbox3000
    3001 => 111,Mailbox3001
    3002 => 222,Mailbox3002
- Verwendung (in extensions.conf):
  - exten => 3001,1,Dial(SIP/${EXTEN},60)
    exten => 3001,2,VoiceMail(${EXTEN},u)
  - exten => 999,1,VoiceMailMain (${CALLERID(num)},s)

Mailbox der Extension 3000: Paßwort=000, Name: Mailbox3000

Mailbox der Extension 3001: Paßwort=111, Name: Mailbox3001

Mailbox der Extension 3002: Paßwort=222, Name: Mailbox3002

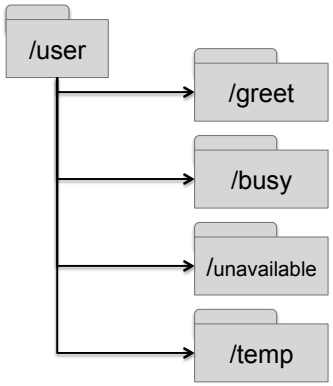
Aufruf der Mailbox 3001:

Abfrage der Mailbox mit der Nummer: 999

Asterisk Mini-VoiceMail (MiniVM)

- MiniVM steht ab Release 1.6 zur Verfügung
- Verzeichnis-Struktur:

/var/spool/asterisk/voicemail/domain



Eigene Benutzeransagen

Ansage: Begrüßung

Ansage: Besetzt, im Gespräch

Ansage: Nicht erreichbar

Ansage: Temporäre Ansage

Dialplan Sonderzeichen

Spezielle Zeichen:

_	Beginn einer Zeichenfolge mit Platzhaltern
X	jede Ziffer von 0 – 9
Z	jede Ziffer von 1 – 9
N	jede Ziffer von 2 – 9
[15-7]	Ziffernfolgen: 1 und 5 – 7 = 1, 5, 6, 7
.	Ersatz für einen oder mehrere Buchstaben
!	Ersatz für null oder mehrere Buchstaben

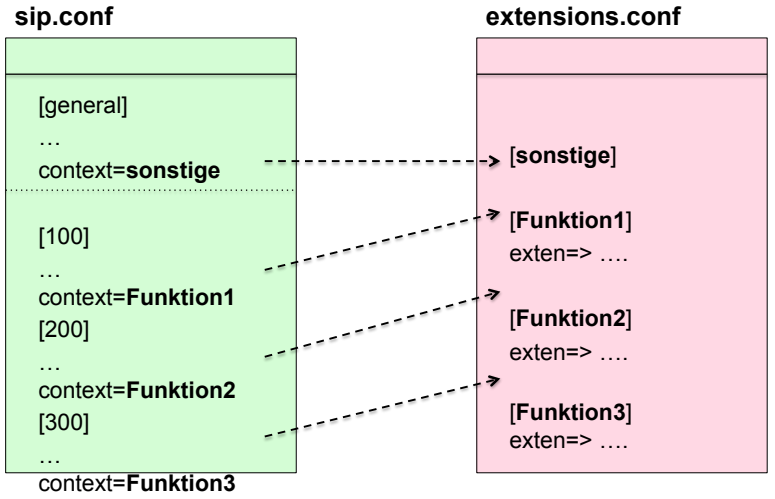
```
[gruppe12]
exten => _12X,1,Answer()
exten => _12X,2,Playback(Ansage1)
exten => _12X,3,Hangup()
```

Die Abfolge von Abheben, Einspielen einer Ansage und Auflegen wird hier für die Nebenstellen "120" bis "129" festgelegt.

Dialplan Struktur: Context

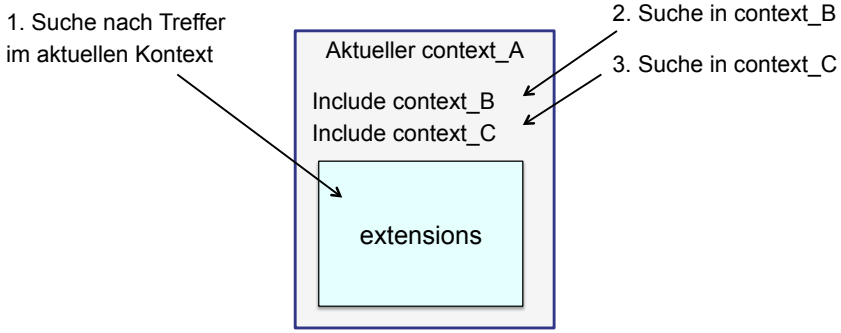
- Kontexte gliedern den Rufnummernplan
  - Syntax: [Kontextname]
  - Vordefinierter Kontext:
    [globals] für die Definition globaler Variablen
    [general] für allgemeine Konfigurationen
- Die Gültigkeit eines Kontextes endet am folgenden Kontext
- SIP-Kontextnamen werden Extensions zugeordnet
- Mittels Kontexten kann die Sicherheit eines Asterisk-Systems erhöht werden.

Context - Verwendung



Dialplan Struktur: Includes

Verwendung: include => ContextName



Bei erfolgreicher Suche wird der Treffer benutzt und der Dialplan weiter abgearbeitet.

Dialplan Effizienz

```
[general]

[intern]
exten => 101,1,Answer()
exten => 101,2,Playback(Text)
exten => 101,3,Hangup()

exten => 102,1,Answer()
exten => 102,2,Playback(Text)
exten => 102,3,Hangup()

exten => 103,1,Answer()
exten => 103,2,Playback(Text)
exten => 103,3,Hangup()
  …….
exten => 109,1,Answer()
exten => 109,2,Playback(Text)
exten => 109,3,Hangup()
```

Durch die Verwendung von “Wildcard” – Zeichen wird der Dialplan im rechten Beispiel wesentlich vereinfacht.

```
[general]

[intern]
exten => _10X,1,Answer()
exten => _10X,2,Playback(Text)
exten => _10X,3,Hangup()
```

Dialplan Variablen

- Globale Variablen: [globals]
  - gelten für all Extensions in allen Kontexten
  - Definition zu Beginn der extensions.conf Datei
- Channel Variablen:
  - gelten nur für den aktuellen Call und für den dadurch aktivierten Kanal.
- ${EXTEN} enthält die Wahlziffern
- ${EXTEN:x}
  - Entfernung der ersten x Zeichen
- ${EXTEN:-x}
  - Entfernung der letzten x Zeichen

Wichtige Dialplan Applikationen (1)

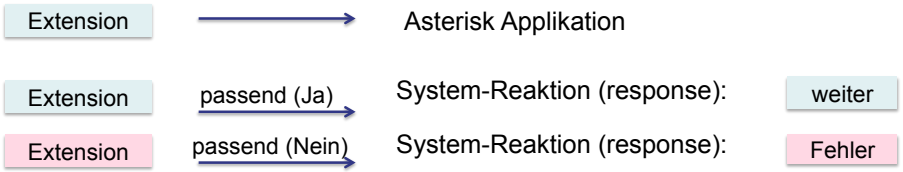
- Answer( )
  - Akzeptiert einen Verbindungsversuch (Hörer abnehmen)
- Hangup( )
  - Verbindung wird getrennt (Hörer auflegen)
- Playback(Soundfile)
  - Abspielen einer Datei aus dem Verzeichnis: /var/lib/asterisk/sounds
- Wait(SekundenDauer)
  - Pause mit SekundenDauer
- VoiceMail(BoxNummer,Option)
  - Sprachnachricht auf BoxNummer, Option

Wichtige Dialplan Applikationen (2)

- VoiceMailMain(MailboxNummer, Optionen)
  - Zugang zum Voicemail System
- Dial( )
  - Verbindet Kanäle
- Background()
  - Im Hintergrund eine Sounddatei abspielen
- BackgroundDetect()
  - Background() mit Spracherkennung
- DateTime()
  - Datum/Uhrzeit ansagen

Asterisk Extension Language – AEL

- AEL ist die Beschreibungssprache für den Rufnummernplan
- Extensions können zu Kontexten (Context) gruppiert werden
- Kontexte können geschachtelt sein
- Vordefinierte Extensions (Asterisk Rel. 1.8):
  - s: Start-Extension; Beginn der Kontext-Aktivierung
  - t: Timeout
  - i: ungültige Antwort (invalid response)
- Priorität: Reihenfolge der Abarbeitung

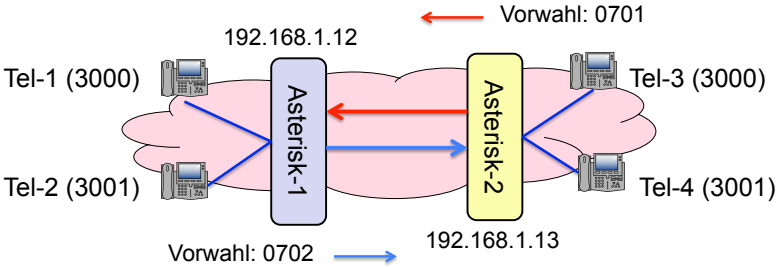


Asterisk – Asterisk Kommunikation : IAX

DHBW Stuttgart

- IAX (Inter Asterisk Exchange) Protokoll ist das Asterisk-eigene VoIP-Protokoll.
- IAX wird optimal verwendet für die Kommunikation zwischen Asterisk Systemen

Beispiel: Workshop-Konfiguration



Asterisk-1 Programmierung

DHBW Stuttgart

iax.conf

```
[ast2]          <-- Asterisk-2 Definition
type = friend   <-- Kommunikation in beide Richtungen
host = 192.168.1.12   <-- IP-@ von Asterisk-1
secret = 1234   <-- Passwort
context = test-telefone   <-- Standard-Kontex für den Dialplan
permit = 0.0.0.0/0.0.0.0   <-- Alle Verbindungen sind zugelassen
```

dialplan.conf

```
[via-asterisk2]
exten => 07023000,1,Dial(IAX2/ast2/3000)
exten => 07023001,1,Dial(IAX2/ast2/3001)
```

externe Vorwahl externe Verbindung

Asterisk-2 Programmierung

DHBW Stuttgart

iax.conf

```
[ast1]          <-- Asterisk-1 Definition
type = friend   <-- Kommunikation in beide Richtungen
host = 192.168.1.11   <-- IP-@ von Asterisk-2
secret = 1234   <-- Passwort
context = test-telefone   <-- Standard-Kontex für den Dialplan
permit = 0.0.0.0/0.0.0.0   <-- Alle Verbindungen sind zugelassen
```

dialplan.conf

```
[via-asterisk1]
exten => 07013000,1,Dial(IAX2/ast1/3000)
exten => 07013001,1,Dial(IAX2/ast1/3001)
```

externe Vorwahl externe Verbindung

Asterisk – zu – Asterisk Verbindung

DHBW Stuttgart

extensions.conf

```
exten => 3000,1,Dial(IAX2/Ast1-user:
Passwort@asterisk2.example.com/
${EXTEN}@IAX_incoming)
exten => 300,2,Hangup
```

Ast1-user :
Kontext, in dem Tln. 3000 definiert ist
asterisk2.example.com :
ist die IP-Adresse von Ast2
IAX_incoming :
verweist auf den Ast2-Kontext, für die Rufnummer 3000

iax.conf

```
[Ast1-user]
type=user
secret=Passwort
context=IAX_incoming
```

extensions.conf

```
[IAX_incoming]
exten => 3000,1,Dial(SIP/3000,30,Ttm)
exten => 3000,n,Hangup()
```

Dialplan-Beispiel: Rufumleitung

DHBW Stuttgart

- Aktivierung der Rufumleitung durch die Vorwahl: 99 + Zielnummer

```
exten => _99X.,1,Answer()
exten => _99X.,n,Set(DB(CF/${CALLERID(num)})=${EXTEN:2})
exten => _99X.,n,SayDigits(${EXTEN:2})
exten => _99X.,n,NoOp(Weiterleitung fuer ${CALLERID(num)} auf ${EXTEN:2}
aktiviert.)
exten => _99X.,n,Hangup()
```

➢ Deaktivierung der Rufumleitung durch Wahlziffern: 99

```
exten => 99,1,Answer()
exten => 99,n,DBdel(CF/${CALLERID(num)})
exten => 99,n,Playback(auth-thankyou)
exten => 99,n,NoOp(Weiterleitung fuer ${CALLERID(num)} deaktiviert.)
exten => 99,n,Hangup(
```


Rufumleitung im Dialplan

DHBW Stuttgart

```
exten => _X.,1,NoOp(Anruf von ${CALLERID(num)} fuer ${EXTEN})
; Ausgabenachricht: CALLERID(num) = Nummer des Anrufers
: ${EXTEN} = Ziel-Rufnummer
exten => _X.,n,GotoIf($[foo${DB(CF/${EXTEN})} != foo]?normal:forward)
; Abfrage : DB(CF/${EXTEN}) CF-Eintrag in der Datenbank ?
; Eintrag vorhanden : 0 -> Sprungziel = normal ; 1 -> Sprungziel=forward
exten => _X.,n(normal),Dial(SIP/${EXTEN})
; Wahlvorgang : normale Verbindung
exten => _X.,n(forward),NoOp(Anruf fuer ${EXTEN} wird verbunden zu
${DB(CF/${EXTEN})})
; Wahlvorgang
exten => _X.,n,Dial(local/${DB(CF/${EXTEN})})
```


Kursgliederung

DHBW Stuttgart

- Raspberry PI
- Netzwerkdiagnose
  - Kommandos
  - Analyse-Software Wireshark
  - Arbeiten mit Wireshark
- Asterisk – VoIP Einführung
- Asterisk Software
- Asterisk Programmierung

AEL2 Einführung

DHBW Stuttgart

- AEL2 Aktivierung durch Modul “pbx_ael.so”
- AEL2:
  - Programmiersprache zur Dialplan-Programmierung
  - AEL2 Syntaxdefinition im BNF-Format
  - Datei-Erweiterung von AEL2-Dialplan: .ael2
  - Datei-Erweiterung von Standard-Dialplan: .conf
- Standard-Dialplan Programmierung: .conf
- AELPARSE als Übersetzer von .ael2 -> .conf
  - AELPARSE als Testprogramm für AEL2-Dateien

AEL2 Syntax (1)

Kommentar: // Text bis zum Zeilenende

Kontext:

```
Context default {  // Kontextname in der selben Zeile wie „context“
.....              // Klammer „{„ in der selben Zeile wie Block-Name
}
```

Extensions:

```
context default {
07231 => Playback(audio-1);  // Wiedergabe-Funktion
 8000 => {                   // Liste abarbeiten
NoOp(Text1);                 // NoOp = CLI-Ausgabe: „Text1“
NoOp(Text2);                 //                     „Text2“
NoOp(Text3);                 //                     „Text3“
};                           // Ende der Liste
 _5XXX => NoOp(Ziffernmuster);    //                 „Ziffernmuster“
  };
```


AEL2 Dialplan-Beispiele

```
123 => {
        Answer()
        Playback(Ansage)
        Dial(SIP/${EXTEN},20)
        Voicemail(${EXTEN},u)
}
```

Ist gleichbedeutend (in conf-Schreibweise) mit:

```
exten => 123,1,Answer()
same => n,Playback(Ansage)
same => n,Dial(SIP/${EXTEN},20)
same => n,Voicemail(${EXTEN},u)
```

kopierfähig für jede Nummer

AEL2 Syntax (2)

AEL2 Variablen-Definition

```
globals {                          // Globale Variablen in einem Block
CONSOLE=Console/dsp;               // Wertzweisung: CONSOLE
TRUNK=Zap/g2;                      // Wertzweisung: TRUNK
};
context default{                   // Variablendefinition in der extension
555 => {                           // entspricht dem Set – Befehl
x=5;                               // Variable x: Wert = 5
y=nix;                             // Variable y: Wert = “nix”
div=10/2;                          // Variable div = 5
NoOp(x is ${x} und y is ${y} !);   // CLI-Ausgabe: “x=5 und y=nix
};
};
```


AEL2 Syntax (3)

Bedingungen: if … else

```
context conditional {                  // Kontext = “conditional”
_8XXX => {                             // 1. Ziffer = 8
Dial(SIP/${EXTEN});                    // Wähle: Rufnummer
if ("${DIALSTATUS}" = "BUSY") {        // Falls besetzt:
Voicemail(${EXTEN}|b);                 // Ansage: besetzt
} else {                               // else-Zweig in Klammern
Voicemail(${EXTEN}|n);                 // Ansage: nicht anwesend
 }
};
```

Schleifensteuerung : Break, Continue

```
context loops {
1 => {                                  // Extension = 1
for (x=0; ${x} < 3; x=${x} + 1) {       // Schleifenbedingung
Verbose(x is ${x} !);
if( ${x} == 2 && ${y} == 17) break;     // Abbruchbedingung (if)
if(${x} == 2 && ${y} == 16) continue } }  // weiter
2 => {                                  // Extension = 2
z=10
y=10; while (${y} >= 0) {               // Schleifenbedingung
Verbose(y is ${y} !);
z=${z} + 1                  // Increment Abbruchbedingung
if (${z}>20) break;         // Abbruchbedingung (if)
y=${y}-1; }                 // Abbruchbedingung (while)
}
}
```


Anwendungsbeispiel : Gesprächszähler

```
[globals]
; Zählerdefinition
ZAEHLEN=1
; sollen die Extensions der laufenden Server-Instanz gezählt werden? (ja = 1)
ANZAHL=NULL     ; Startwert
GESPRAECHE=0 ; Startwert
; zaehlen und weiter sind Sprungmarken
exten => _300[0-3],1,GotoIf($[${ZAEHLEN} = 1}]?zaehlen:weiter)
exten => _300[0-3],n(zaehlen),Set(GLOBAL(GESPRAECHE)=$[${GESPRAECHE}+1])
exten => _300[0-3],n(weiter),Dial(SIP/${EXTEN},10,tT)
; 10 Sek. timer. tT aktiviert Vermitteln & Parken fuer beide Seiten
exten => _300[0-3],n,VoiceMail(${EXTEN},u)
; Mailbox falls Verbindung nicht zustande kommt
```


Macro (1)

- Macro ist ein “Funktionsaufruf”, die von Extensions verwendet werden
- Macro Einsatz:
  - für wiederholt auftretende Ereignisse
  - für zentralisierte Änderung am Dialplan
- Syntax: Makro-Definition: im Kontext: [**Macro-**Macroname]
  extensions ….
- Syntax: Macro-Aufruf: Macroname(Par1,.., Par-n)
- Vorgegebene Variablen:
  - ${MACRO_CONTEXT}, ${MACRO_EXTEN}, ${MACRO_PRIORITY}, $ARG1}, …, $ARGn},

Macro (2)

AEL2 Macro definition

```
Macro norm-exten( ext , dev ) {  // 2 Parameter: extension, device
Dial(${dev}/${ext},20);          // z.B. SIP/123
switch(${DIALSTATUS}) {          // Abfrage von DIALSTATUS
case BUSY:                       // falls besetzt:
Voicemail(${ext},b);             // BUSY-Ansagetext
break;                           // Switch verlassen
default:                         // Switch-Ausgang: sonst
Voicemail(${ext},u);             //  Nicht-Anwesend-Ansagetext
}
}
```

Asterisk Variablen

Einige Built-in Variablen:

- ${CALLERID(num)} Anrufernummer
- ${CONTEXT} aktueller Kontext
- ${EXTEN} Rufnummer
- ${CHANNEL} Channelname
- ${PRIORITY} aktuelle Dialplan-Priorität
- ${HANGUPCAUSE} Auslösegrund

Eigene Variablen definieren:

- same => n,Set(Variable1=10)
  same => n,Set(Variable2=5)
  same => n,Set(Variable3="Ergebnis = ")

Verwenden:

- same => n,NoOp(${Variable3}${Variable1}/${Variable2})

Spezielle Extensions

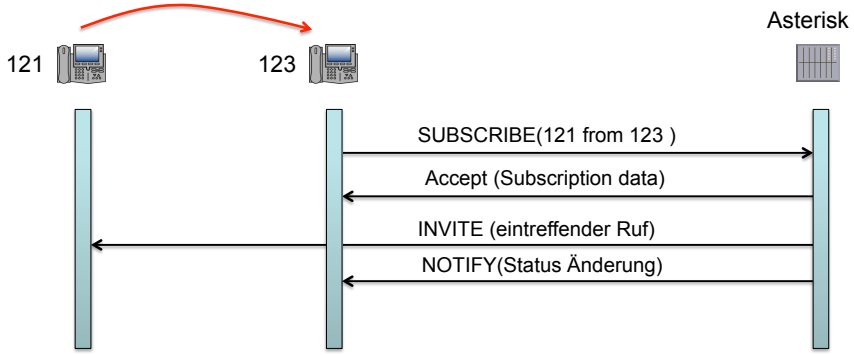
- s-Extension: wird verwendet, wenn das Ziel nicht bekannt ist. s-Extensions werden z.B. in Macros verwendet
- i-Extension: wird für eine ungültiges (invalid) Ziel verwendet
- t-Extension: wird für ein Timeout verwendet
- h-Extension: markiert die Beendigung eines Gesprächs
- o-Extension: Operator Extension durch Eingabe von Null (0) im Voicemailmenü
- a-Extension: Abbruch durch "*" – Eingabe im Voicemailbox Menü

Leistungsmerkmal: Call Pick-Up

- **Vorbereitung**:
  - Programmierung des Telefons-B zur Übernahme der Gespräche des Telefons-A
  - Meldung an das Telefon-A (SUBSCRIBE)
  - Aktivierung des Leistungsmerkmals
- **Durchführung des Leistungsmerkmals**:
  - Eintreffender Ruf am Telefon-A: Telefon-A klingelt
  - Information an Telefon-B (NOTIFY) und Anzeige am Telefon-B
  - Übernahme durch Telefon-B (Funktionstaste oder Zeichenfolge)

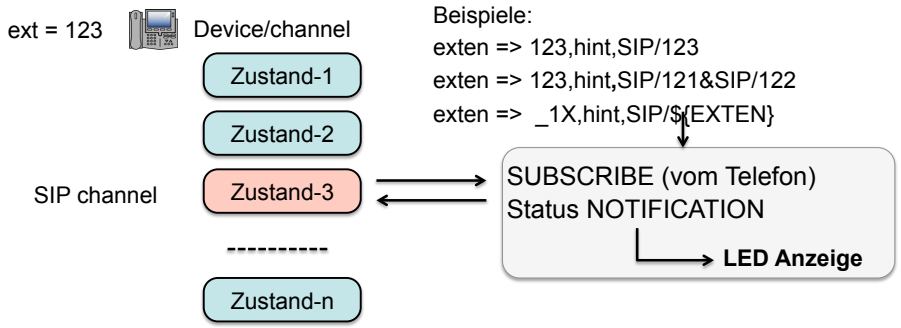
SIP-Prozedur: Call Pick-Up

SIP Beispiel : Call Pick-Up Nr. 121 durch Nr. 123



Telefon-Ansteuerung - BLF

- **BLF** : Besetzt-Anzeige (Busy Lamp Field) durch die Telefonanlage
- **Hint** – Priorität verknüpft:
  - Extension = Folge von Funktionen/Anwendungen mit dem Channel (Gerät, Technologie) und dessen Zustand



Umsetzung in sip.conf

Anzeigesteuerung Telefon-123:

```
[general]
allowsubscribe = yes        /* SUBSCRIBE Prozedur erlauben */
notifyringing = yes         /* NOTIFY bei eintreffendem Ruf */
notifyhold = yes
limitonpeers = yes
```

Context – Ergänzungen:

```
[123]
.....
Subscribecontext=interne-verbindungen  /* Teilnehmer-Kontext */
call-limit=10                          /* Gesprächszähler */
callgroup=2                            /* Rechteverwaltung */
pickupgroup=2                          /* Pickup-Gruppe */
.....
```


Dialplan Programmierung

[interne-verbindungen]

```
exten => _2X,hint,SIP/${EXTEN}
exten => _2X,1,Dial(SIP/${EXTEN},30)
exten => _2X,n,VoiceMail(${EXTEN},u)
```

```
; Gesprächsübernahme mit *8+Nr
; z.B. mit *8121 wird 121 herangeholt
exten => _*8X.,1,Set(nst=${EXTEN:2})
exten => _*8X.,1,Pickup(${nst}@interne-verbindungen)
```

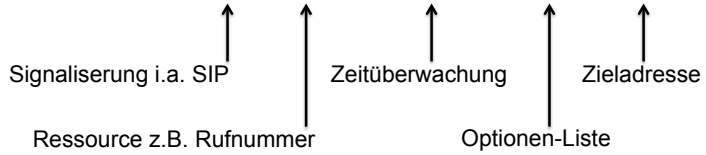
```
context interne-verbindungen {
   hint(SIP/${EXTEN})  _2X => {
    Dial(SIP/${EXTEN},30);
   VoiceMail(${EXTEN},u);
 }
}
// Gesprächsübernahme mit *8+Nr //
_*8X. => {
Set(nst=${EXTEN:2});
Pickup(${nst}@interne-benutzer);
}
}
```


Ergebnis

- Meldung eines Statuswechsel des überwachten Telefons an das überwachende Telefon
- LED-Steuerung (Telefon-Funktion):
  - Keine Aktivität: LED aus
  - Blinkende-LED bei eintreffenden Ruf
  - Rufannahme mit *8 + Nummer des überwachten Telefons
  - Dauer-LED, falls das überwachte Telefon ein aktives Gespräch führt
- Konsolen-Meldungen bei Status-Wechsel

Dial-Funktion und Call Transfer

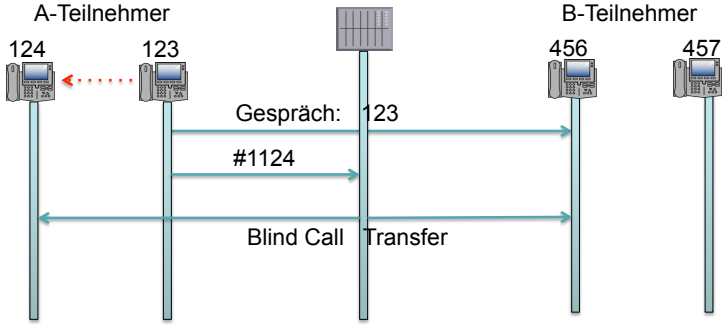
Dial Syntax: **Dial(*Tech*/*Resource*,*Timeout*,*Optionen*,*URL*)**



Wichtige Dial – Optionen:

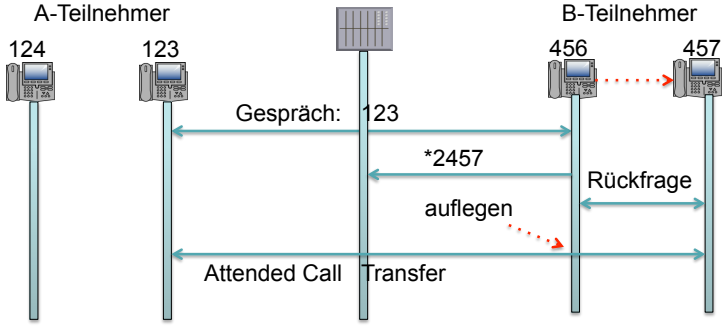
- **t/T:** Transfer durch den angerufenen/rufenden Teilnehmer durch drücken der #-Taste ermöglicht
- w/W: Aufnahme des Gesprächs durch den angerufenen/rufenden Teilnehmer
- M(x[arg]): Ausführen des Makros x[arg] bei der Rufannahme
- L(x): Begrenzt die Gesprächsdauer

Blind Transfer – ohne Rückfrage



- exten => same,1,Dial(SIP/${EXTEN},tT)
  Call Transfer für rufenden/gerufenen Teilnehmer erlaubt
- Standard-Transfer-Kommando: #1 + Zielrufnummer

Blind Transfer – mit Rückfrage



- exten => same,1,Dial(SIP/${EXTEN},tT)
  Call Transfer für rufenden/gerufenen Teilnehmer erlaubt
- Standard-Transfer-Kommando: #1 + Zielrufnummer

Dialplan : Labels und Sprünge

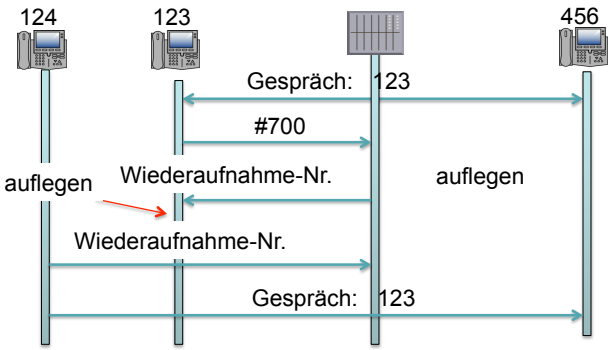
```
; Definition von Sprungzielen (Label):
exten => 123,1,Answer()
         same =>
         same => n(Anfang),Playback(Ansage)
         same => n,Dial(SIP/${EXTEN},20)
         same => n,Voicemail(${EXTEN},u)

; Unbedingter Sprung (Goto):
exten => 124,1,Answer()
exten => 124,n, Goto(123,Anfang)
```

Park-Funktion

Park-Prozedur:

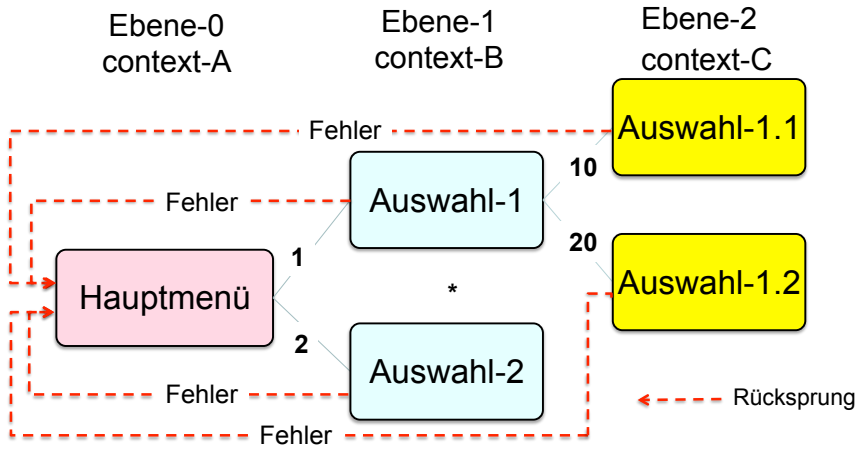
- Ein Telefongespräch soll über ein anderes Telefon fortgesetzt werden.
- Park-Kommando: #700



Interactive Voice Response - IVR

- Mittels IVR erhält der Anrufer ein akkustisches Auswahlmenü und antwortet darauf durch Spracheingabe oder durch Telefon-Tastatureingabe
- Asterisk verwendet die Telefon-Tastatureingabe
- Funktionen zur Abspielen der Menünachricht :
  - Background(Audio-Datei)
  - Playback(Audio-Datei)
- Die Tastatureingabe wird als Extension behandelt.
- Fehlerhafte Eingaben können durch die „i-Extension“ abgefangen werden.
- Mehrstellige Eingaben werden mittels Tastatur-Timeout überwacht.

Mehrstufige IVR Menüs



Jede Ebene besitzt ihren eigenen Kontext, dadurch können Extensions (Tastatureingaben) mehrfach verwendet werden.

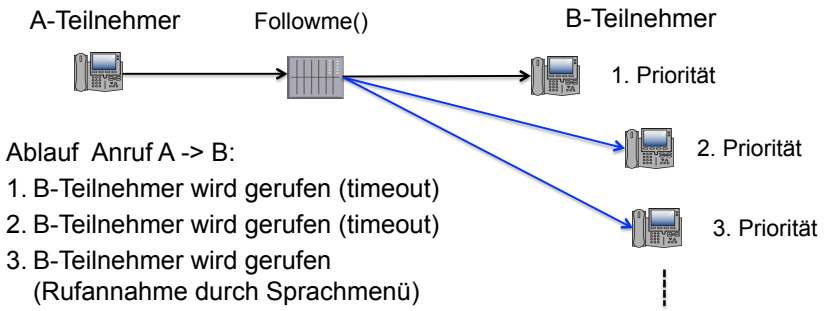
Zählerfunktionen

```
[CounterIncrement]
exten => start,1,Verbose(2,Increment the counter variable)
same => n,Set(CounterVariable=1) /* Zählervariable setzen */
same => n,Verbose(2,Zählerstand: ${CounterVariable})
same => n,Set(CounterVariable=${INC(CounterVariable)})
same => n,Verbose(2,Neuer Zählerstand: ${CounterVariable})
same => n,Hangup()
```

```
[CounterDecrement]
exten => start,1,Verbose(2,Increment the counter variable)
same => n,Set(CounterVariable=3) /* Zählervariable setzen */
same => n,Verbose(2,Zählerstand: ${CounterVariable})
same => n,Set(CounterVariable=${DEC(CounterVariable)})
same => n,Verbose(2,Neuer Zählerstand: ${CounterVariable})
same => n,Hangup()
```

Follow-Me Funktion

- Follow-me:
  - Nachbildung der ISDN-Festnetz Funktion
  - Erreichbarkeit mehrerer Ziele (Liste)
  - Sprachsteuerung z.B. Rufannahme-Menü



Ablauf Anruf A -> B:
1. B-Teilnehmer wird gerufen (timeout)
2. B-Teilnehmer wird gerufen (timeout)
3. B-Teilnehmer wird gerufen
   (Rufannahme durch Sprachmenü)

Dialplan Diagnose

Diagnosemöglichkeiten:

- Textausgaben aus dem Dialplan:
  exten => same,n,Verbose(2, Die Extension ist: ${EXTEN})
  exten => same,n,NoOp("Die Extension ist: " ${EXTEN})
- Ausgabe an der CLI-Konsole
- Verbose() ermöglicht die Ausgabe in Abhängigkeit vom eingestellten verbosity-Level: Diagnose-Switch
- NoOP erzeugt eine CLI-Ausgabe ab Level-2
- CLI Kommandos : dialplan show, etc.

Kursgliederung

- Raspberry PI
- Netzwerkdiagnose
  - Kommandos
  - Analyse-Software Wireshark
  - Arbeiten mit Wireshark
- Asterisk – VoIP Einführung
- Asterisk Software
- Asterisk Programmierung