



Kommunikationstechnik KOTE / Netzwerkgrundlagen
2. Unit

Übersicht der einzelnen Modulblöcke (roter Faden)

**Grundlagen aus
relevanten Kapiteln**
Cisco CCNA 200-301
Volume 1+2

Modulaufgaben
Vorbereitung und
Vertiefung

*Simulationsübungen
mit dem CISCO
Pakettracer und mit
Wireshark*

Stoffumfang KOTE:

CCNA1/ Kap. 1 – 6 / 8 / 9 / 11 – 14 / 18

CCNA2/ Kap. 1 + 13

CCNA1/Kap. 2
CCNA2/Kap. 13

**Grundlagen Netzwerkmanagement und
Netzwerk**

NetAcad/Kap. 1

CCNA1/Kap. 1
CCNA1/Kap. 3

**Netzwerkkommunikation LAN/WAN
ISO/OSI Referenzmodell**

NetAcad/Kap. 3

CCNA2/Kap. 1

**Standards und Gremien
L7,L4 und L3 analysieren**

NetAcad/Kap. 10
NetAcad/Kap. 9

CCNA1/Kap. 11
CCNA1/Kap. 12
CCNA1/Kap. 13
CCNA1/Kap. 14

IPv4 Funktionen und Subnettierung

NetAcad/Kap. 6
NetAcad/Kap. 7
NetAcad/Kap. 8

CCNA1/Kap. 4
CCNA1/Kap. 5/6

ICMP, Routing, Switching und CLI-Grundlagen

NetAcad/Kap. 4
NetAcad/Kap. 5

CCNA1/Kap. 8

VLAN und IEEE 802.1Q konfigurieren

CCNA1/Kap. 9

Redundante Netzwerkdesigns

CCNA1/Kap. 18
(Commands)

**Netzwerk für ein KMU konfigurieren
Troubleshooting im Netzwerk**

**NPDO - Netzwerk, Planung, Design und
Optimierung**

NIUS - Netzwerkinstallation und Störungsbehebung

Lernziele des 2. Modulblocks

- **Du kannst...**

1. ...anhand des ISO/OSI-Referenzmodells den Kommunikationsprozess beschreiben.
2. ...mittels dem Tool Wireshark Protokolle analysieren.
3. ...mittels Wireshark Displayfilter die Anzeige auf das Gesuchte eingrenzen.
4. ...die grundlegenden Elemente betreffend LAN- und WAN Netzwerken beschreiben.

Agenda

«Kurztest»

Ablauf Kurztest

- Löse auf den nachfolgenden Folien die jeweiligen Fragen. Du hast 3 Minuten Zeit pro Folie. Danach kommt die nächste Aufgabe.
- Schreibe die Grundlagen sinnvoll auf ein Blatt, so dass eine Korrektur möglich ist.
- **Es handelt sich hier um eine Einzelarbeit!**
- Wir besprechen am Schluss kurz die Ergebnisse. **Es gibt keine Note!**

Aufgabe zu den Grundlagen der technischen Kommunikation

- Simplex ist eine Verbindungsart, nennen Sie die zwei weiteren mit je einem Beispiel.
- Point to Point oder Punkt zu Punkt Verbindung ist eine Kommunikationsart, nennen Sie die zwei weiteren mit je einem Beispiel.

Aufgabe Musterlösung

- Simplex-Verbindung (Radio, Fernsehen)
 - Halbduplex-Verbindung (Funkgeräte)
 - Duplex-Verbindung (z.B. PC Netzwerke)
-
- Point to Point (Telefon, Leitungsvermittlung)
 - Multicast (Client-Server-Appli, Pay-TV)
 - Broadcast (Radio, Fernsehen)


Repetition Block 1

Praxistransfer: Besprechung in den Gruppen

- Versuche diese Fragen innerhalb Deiner Unternehmung zu klären und nimm die Antworten zur gemeinsamen Besprechung in den Unterricht mit:
 - Wer ist in deinem Unternehmen für das Netzwerk-Management zuständig?
 - Verwendet deine Firma den ISO/OSI-Managementmodell Ansatz? Wenn Nein, welcher andere Standard wird verwendet?
 - Verwendet deine Firma eine 2-Schichten oder 3-Schichten Netzwerkarchitektur?

max. Zeit: 20 Minuten

Agenda



«Grundlagen Schichtenmodelle»

CCNA1 Kapitel 1 «Introduction to TCP/IP Networking»

Grundlagen Schichtenmodelle

- Es gibt verschiedene Darstellungen von Schichtenmodellen
 - http://en.wikipedia.org/wiki/Internet_protocol_suite
- Viele beziehen sich auf **RFC1122** (Requirements for Internet Hosts -- Communication Layers)
 - <http://tools.ietf.org/html/rfc1122>

ICT-Grundlagen

Das ISO/OSI-Modell

- Standard seit 1983
 - Entwicklung begann 1979
- Förderung der Interoperabilität
 - Geräte unterschiedlicher Hersteller müssen miteinander funktionieren
 - Reduzieren der Komplexität
- Ergebnis war das ISO/OSI-Modell
 - **International Standards Organisation / Open Systems Interconnection**

Grundlagen ICT

Übersicht ISO/OSI-Modell

TCP/IP

International Standards Organisation /
Open Systems Interconnection

OSI-Schicht	Einordnung	DoD-Schicht	Protokollbeispiel	Einheiten
7 Anwendungen (Application)	Anwendungs-orientiert	Anwendung	HTTP FTP HTTPS SMTP LDAP NCP	Daten
6 Darstellung (Presentation)				
5 Sitzung (Session)				
4 Transport (Transport)	Transport-orientiert	Transport	TCP UDP SCTP SPX	TCP = Segmente UDP = Datagramme
3 Vermittlung (Network)		Vermittlung	ICMP IGMP IP IPsec IPX	Pakete
2 Sicherungsschicht (Data Link)		Netzzugriff	Ethernet Token Ring FDDI ARCNET	Rahmen (Frames)
1 Bitübertragung (Physical)				Bits

Quelle: wikipedia.org
DoD = Department of Defense

Die sieben OSI Schichten

Layer	OSI-Schichten	Englisch	Merksatz
Layer 7	Anwendung	Application	Alle
Layer 6	Darstellung	Presentation	Priester
Layer 5	Sitzung	Session	saufen
Layer 4	Transport	Transport	Tequila
Layer 3	Vermittlung	Network	nach
Layer 2	Sicherung	Data Link	der
Layer 1	Bitübertragung	Physical	Predigt.

Kurzübersicht Aufgaben der einzelnen OSI-Schichten

Layer	OSI-Schichten	Aufgabe
Layer 7	Anwendung	Anwendungsbezogene Protokolle (z.B. HTTP)
Layer 6	Darstellung	Übersetzung (Dateisyntax) und Verschlüsselung (SSL/TLS)
Layer 5	Sitzung	Kommunikationssteuerung (Sessions)
Layer 4	Transport	Sorgt für zuverlässige Zustellung (Ports und Sockets) und Segmentierung der Pakete
Layer 3	Vermittlung	Logische IP-Adressierung und Weiterleitung (Routing)
Layer 2	Sicherung	Ordnen der Bits in logische Gruppen (Frames) Unterteilung in MAC und LLC Physische Adressierung mit MAC-Adresse
Layer 1	Bitübertragung	Physische Übertragung Bits und Bytes, Eigenschaften Medien und Geräte (z.B. nach IEEE)

Vergleich OSI und TCP/IP Modelle

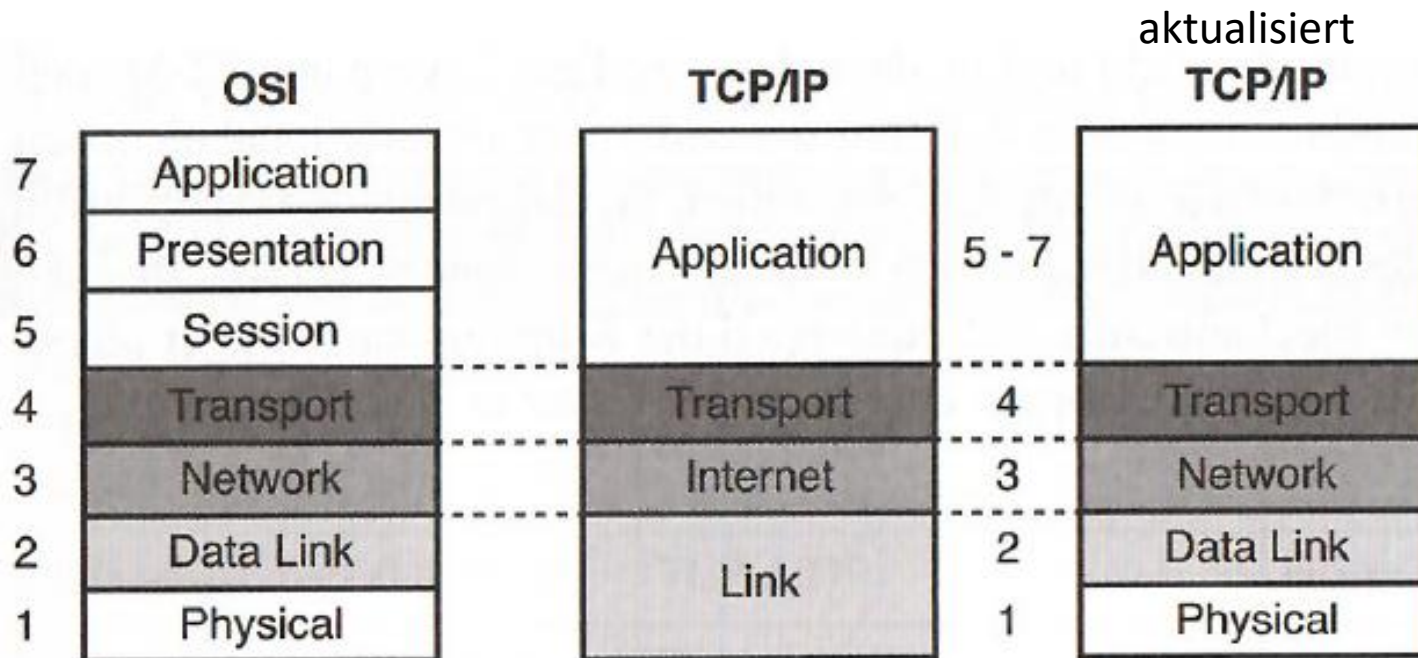
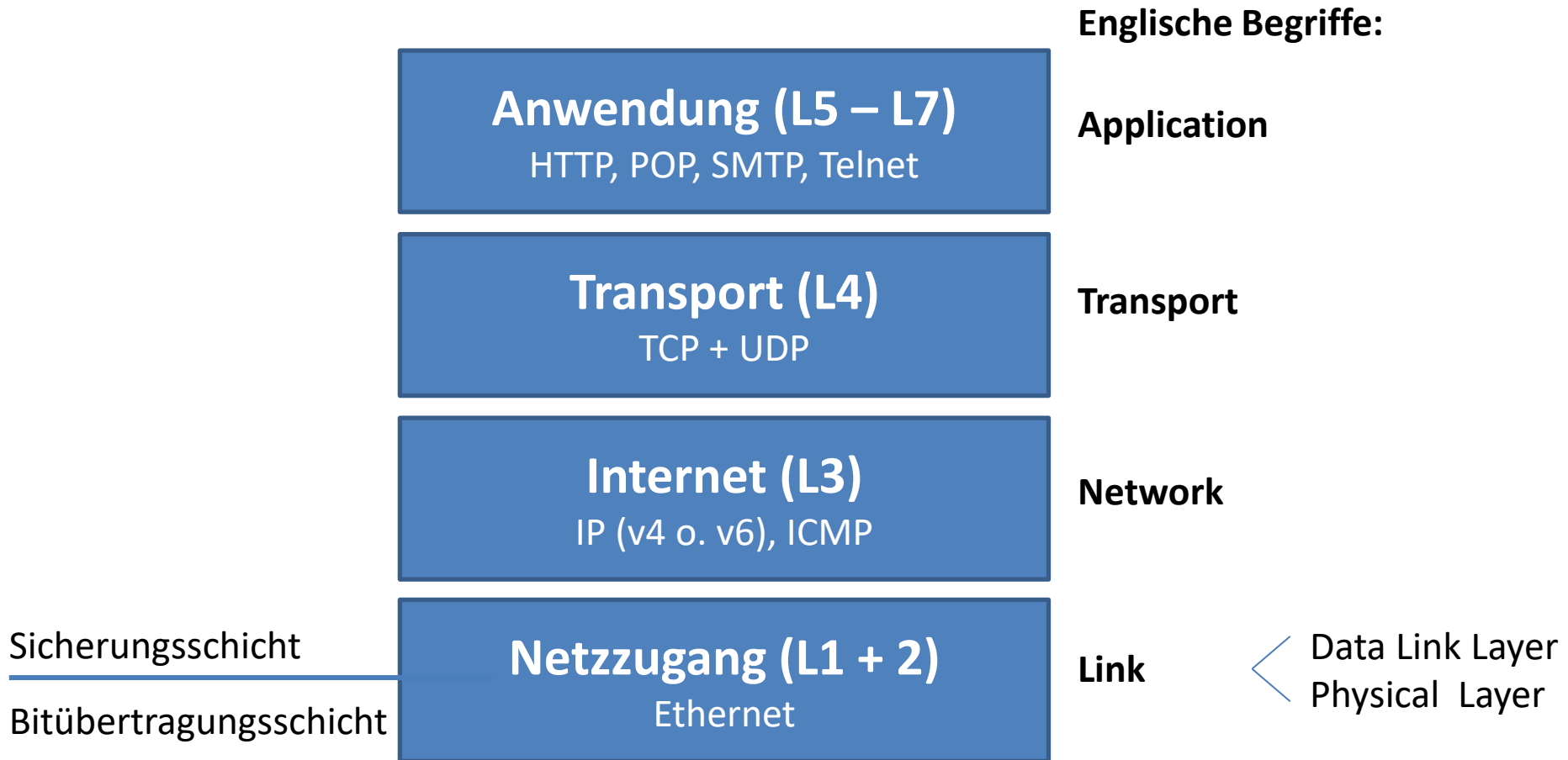
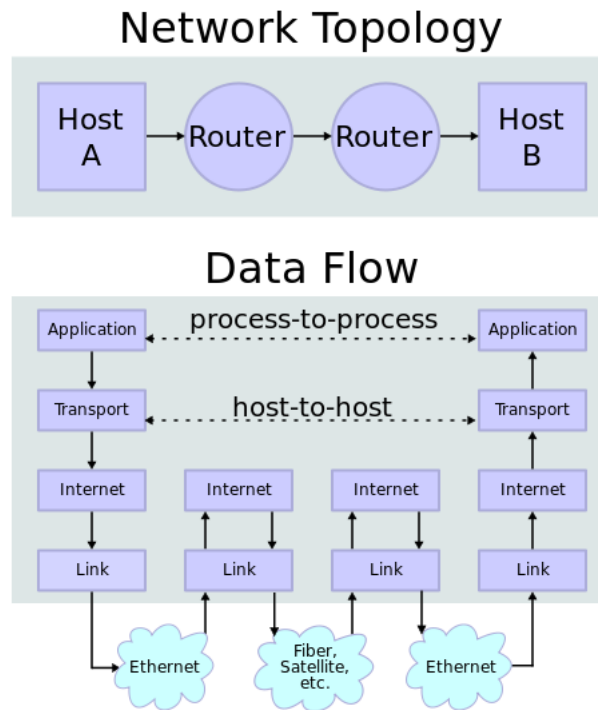


Abbildung 1.15 OSI-Modell und die beiden TCP/IP-Modelle im Vergleich

Aufbau des TCP/IP Modells



Data Flow between 2 Hosts (schematic)



Two Internet hosts connected via two routers and the corresponding layers used at each hop. The application on each host executes read and write operations as if the processes were directly connected to each other by some kind of data pipe. Every other detail of the communication is hidden from each process. The underlying mechanisms that transmit data between the host computers are located in the lower protocol layers.

Agenda

«Grundlagen Kommunikationsprozess»

CCNA1 Kapitel 1 «Introduction to TCP/IP Networking»

Grundlagen Kommunikationsprozess

- **Der Header enthält Steuerinformationen**
- Jede Schicht fügt einen eigenen Header an
- Jede nächste Schicht betrachtet diesen Header als Daten und fügt seinen Header an
- **Dies nennt man Kapseln**
- **Umgekehrte Prozess heisst Fragmentierung**

Grundlagen ICT

OSI-Modell (visuelle Darstellung)

OSI-7-Layer-Model (Open Systems Interconnection Reference Model)

Begriffe: Englisch - Deutsch

- | | |
|----------------------|--|
| 7 Application Layer | - Anwendungsschicht |
| 6 Presentation Layer | - Darstellungsschicht |
| 5 Session Layer | - Sitzungs- bzw. Kommunikationsschicht |
| 4 Transport Layer | - Transportschicht |
| 3 Network Layer | - Netzwerk- bzw. Vermittlungsschicht |
| 2 Data Link Layer | - Sicherungsschicht |
| 1 Physical Layer | - Bitübertragungsschicht |

PC im Netzwerk
A

W <http://www.wikipedia.org>



Der Benutzer empfängt lediglich die Antwort des Servers ("wikipedia.org"-Startseite). Im Allgemeinen bekommt er von der Schachtelung seines Seitenaufrufs durch die Ebenen seines PCs (abwärts) und vom Parsen der Antwort des Servers zurück durch die Ebenen seines PCs (aufwärts) nichts mit!

Server schickt die entsprechenden Daten über die selbe Methode zurück. (s.u.)

Server im Netzwerk
B



Zusammenbau des Pakets:
(Package Assembling/Formatting)

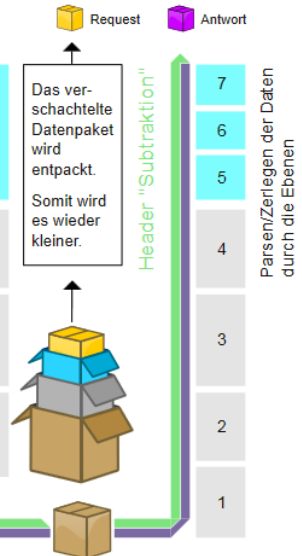


Zusammensetzung der Abkürzungen oben:
Anfangsbuchstabe der Schicht und "H" für Header.
z.B. Application Header = AH

Datenpaket z.B. Serverrequest
OSI-Layers

Header "Addition"
Schichten werden ineinander eingebettet.
Das Datenpaket wird nach unten hin größer.

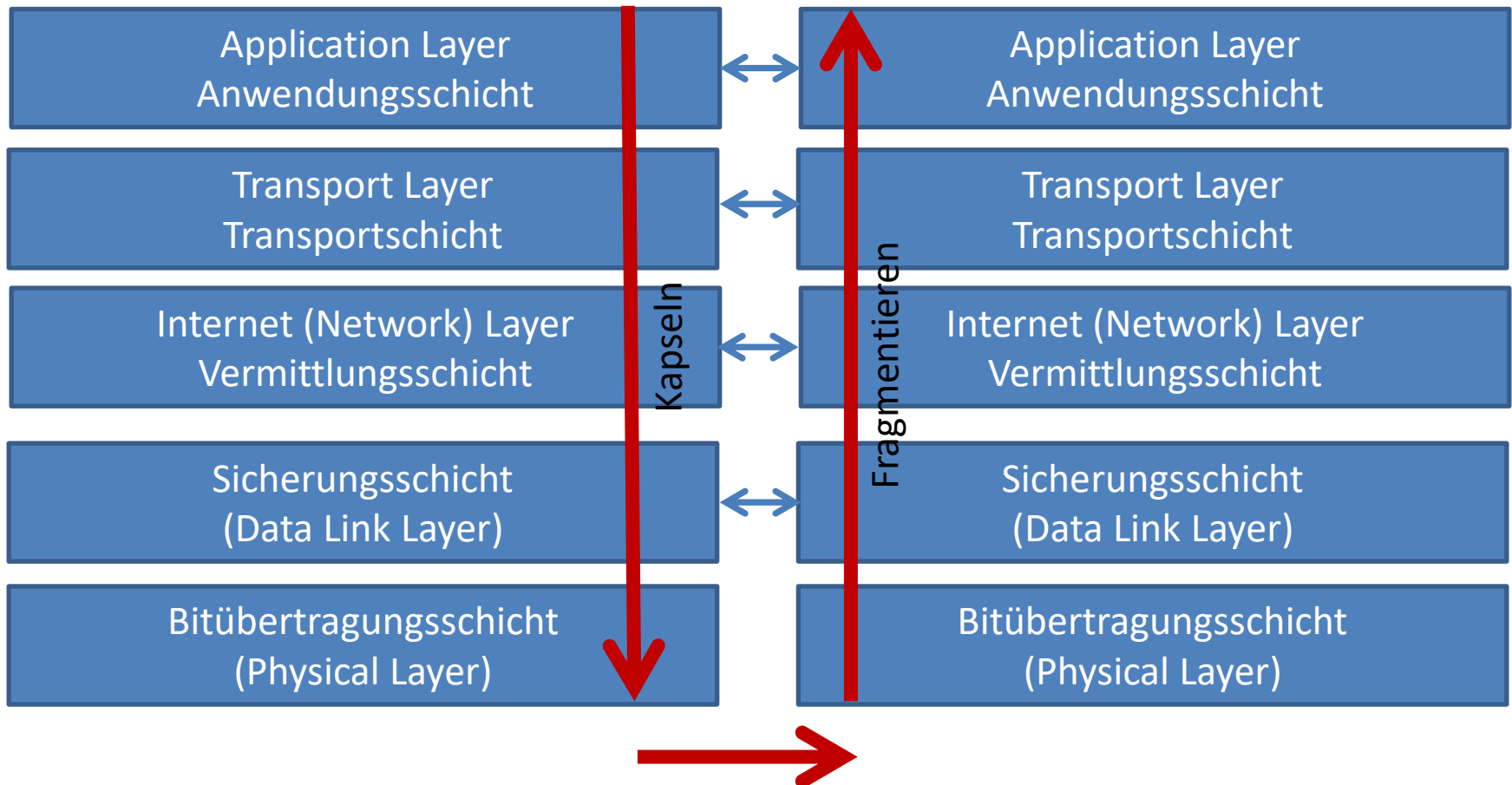
Einordnung der Orientierung	Standard	TCP/IP Schicht	Einordnung der Verbindung	Protokoll
Anwendungsorientiert	FTAM ASN.1 ISO 8326	Anwendung	Ende zu Ende (Multihop)	HTTP FTP HTTPS NCP
Transportorientiert	ISO 8073	Transport		TCP UDP SPX
	CLNP	Internet	Punkt zu Punkt	ICMP IGMP IP IPX
	HDL Token Bus	Netzzugang		Ethernet Token Ring FDDI ARCNET



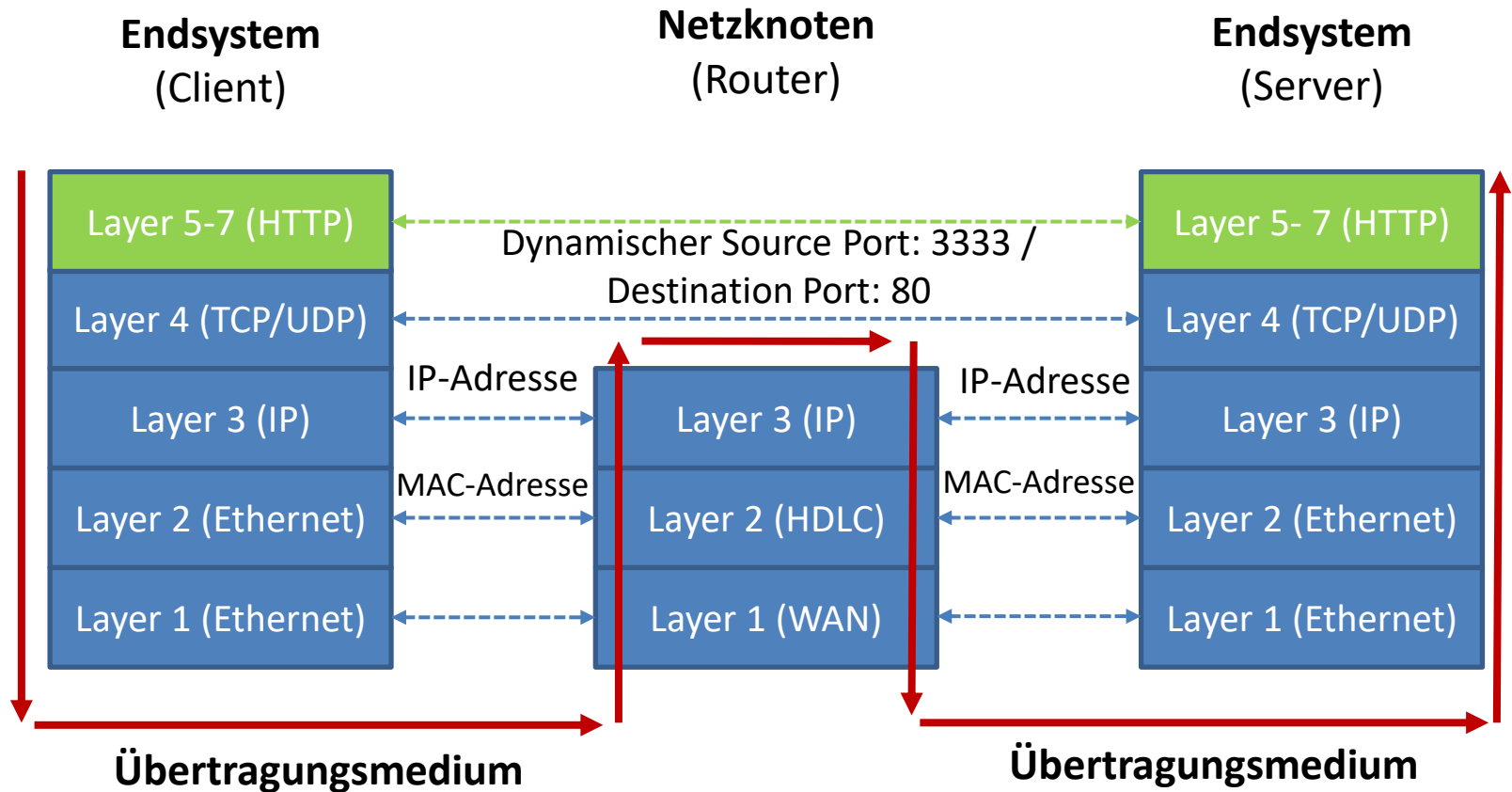
physikalische oder logische Verbindung
Tatsächlicher Datendurchsatz / Übertragungspfad

Autor: gob (www.godofbytes.de)
Bildversion 3.0 (14. Okt. 2006)
SVG-Neuaufbau + Korrektur: der_Fahrer
Dateiversion 3.1 (21. Juni 2010)

Einordnung der Übertragung in das aktualisierte fünf Schichten TCP/IP-Modell



Übertragungsprozess



Einordnung der wichtigsten Protokolle und Einheiten

ISO/OSI	Protokoll	PDU*	Genaue Einheit	Adressierung
Layer 1	Ethernet IEEE 802.3	Bit	Signale in Bits	keine
Layer 2	Ethernet IEEE 802.3	Frame	Frames	MAC-Adresse
Layer 3	IPv4 IPv6	Paket	IP-Datagramme	IP-Adresse
Layer 4	TCP	Segment	TCP-Segmente	gehört zu IP-Paket (verbindungsorientiert)
Layer 4	UDP	Segment	UDP-Datagramme	Gehört zu IP-Paket (verbindungslos)
Layer 7	Anwendung (z.B. HTTP)	Daten	Nachricht	Wird an Layer 4 über API weitergereicht

*PDU=Protocol Data Unit. Allgemein kann der Begriff **Datenpaket** für verschiedene Einheiten (Frames, Datagramme, usw.) verwendet werden. Ein Teil davon wird **Fragment** genannt.

Überblick der TCP/IP Suite

Anwendungsschicht

- NTP, BOOTP (DHCP), FTP, DNS, TFTP, SMTP, NNTP, SNMP, HTTP, BGP

Transportschicht

- TCP, UDP

Vermittlungsschicht

- RIP, OSPF, IP, ICMP, IGMP

Sicherungsschicht

- **Ethernet (IEEE 802.3)**, ARP, RARP, SLIP, **PPP**, **HDLC**

Bitübertragungsschicht

- **Ethernet (IEEE 802.3)**, Binäre Daten

Agenda



«Grundlagen Adressierung im Netz»

CCNA1 Kapitel 1 «Introduction to TCP/IP Networking»

Visualisierung IP-Adressierung mit Wireshark

The image shows a Wireshark network traffic capture. The top bar indicates the capture source as 'Microsoft:\Device\NPF_{37FAF8A3-D329-4408-8FE7-FB887A4D8901}' and the version as 'Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The filter bar shows 'ip' as the active filter. The packet list pane displays a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packet details pane shows the selected packet (No. 1) as an Ethernet II frame, followed by an Internet Protocol Version 4 header, and a User Datagram Protocol header. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates 'Packets: 717 Displayed: 709 Marked: 0' and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.77.45	146.228.101.20	DNS	73	Standard query 0xf1b2 A www.google.ch
2	0.01988600	146.228.101.20	192.168.77.45	DNS	121	Standard query response 0xf1b2 A 173.194.44.216 A 173.194.44.215 A 173.194.44.223
3	0.20541700	192.168.77.1	224.0.0.1	IGMPV2	60	Membership query, general
4	0.75281500	192.168.77.45	173.194.44.216	TCP	66	53611 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
5	0.77380000	173.194.44.216	192.168.77.45	TCP	66	http > 53611 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=64
6	0.77384700	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
7	0.85197200	192.168.77.45	146.228.101.20	DNS	73	Standard query 0x4833 A api.mywot.com
8	0.86517700	192.168.77.45	173.194.44.216	HTTP	370	GET / HTTP/1.1
9	0.87191600	146.228.101.20	192.168.77.45	DNS	89	Standard query response 0x4833 A 83.145.197.2
10	0.87339300	192.168.77.45	83.145.197.2	TCP	66	53613 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
11	0.88684700	173.194.44.216	192.168.77.45	TCP	60	http > 53611 [ACK] Seq=1 Ack=317 win=6912 Len=0
12	0.94406500	83.145.197.2	192.168.77.45	TCP	66	http > 53613 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=128
13	0.94411900	192.168.77.45	83.145.197.2	TCP	54	53613 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
14	0.94947900	192.168.77.45	83.145.197.2	HTTP	516	GET /0.4/update?id=e4ac84f4c9f4d90bd90e308d09a92882d17c96af&nonce=74ad37d9ee59d1130b4d2b1332b873d74e0bb5d9&format=4&lang=de-DE&v
15	0.96598700	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]

Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
Ethernet II, Src: IntelCor_6a:7d:d8 (10:0b:a9:6a:7d:d8), Dst: ZyxeCom_fd:7a:80 (00:13:49:fd:7a:80)
Internet Protocol Version 4, Src: 192.168.77.45 (192.168.77.45), Dst: 146.228.101.20 (146.228.101.20)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
Total length: 59
Identification: 0x031c (796)
Flags: 0x00
0... .. = Reserved bit: Not set
.0... .. = Don't fragment: Not set
..0... .. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x31c8 [correct]
Source: 192.168.77.45 (192.168.77.45)
Destination: 146.228.101.20 (146.228.101.20)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 53850 (53850), Dst Port: domain (53)
Domain Name System (query)
0000 00 13 49 fd 7a 80 10 0b a9 6a 7d d8 08 00 45 00 ..I.Z...j...E.
0010 00 3b 03 1c 00 00 80 11 31 c8 c0 a8 4d 2d 92 e41..M..
0020 65 14 d2 5a 00 35 00 27 11 f2 f1 b2 01 00 00 01 e..Z..S'.....
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6cw ww.googl
0040 65 02 63 68 00 00 01 00 01e.ch....

Agenda

**«Kurzeinführung in
Wireshark»**

Übersicht Wireshark

- Wireshark ist ein typischer **Netzwerksniffer**
- Gründer ist Gerald Combs
- Erste Version 1998 hiess Ethereal
- Seit Mitte 2006 heisst das Projekt Wireshark
- Das Projekt steht unter GNU Public License
- Unterstützt verschiedenste Protokolle
- Download: **www.wireshark.org**

Voraussetzungen für Aufzeichnungen mit Wireshark

1. Netzwerkkarte ist im **promiscuous mode**
 - Braucht bei Windows WinPcap
2. Installation von Wireshark auf Client oder Server
3. Switch mit port mirroring oder Benutzung eines TAP

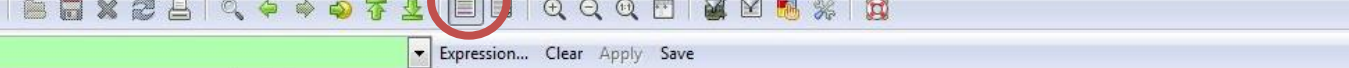
Das Hauptfenster von Wireshark

The screenshot displays the Wireshark interface with the following components:

- Filter:** `ip`
- Packet List:** A table of captured packets. The first packet is a DNS Standard query from 192.168.77.45 to 146.228.101.20.
- Packet Details:** A hierarchical view of the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol.
- Packet Bytes:** A hex dump and ASCII representation of the packet data.

«Verschiedene Headerinformationen»

Verschiedene Farben für Protokolle schaffen Übersicht in Wireshark



The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons. A red circle highlights the icon representing the packet list pane. Below the toolbar is a filter bar with the text 'Filter: ip' and buttons for 'Expression...', 'Clear', 'Apply', and 'Save'. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are numbered 1 through 14, showing a sequence of DNS queries and responses, and TCP connections to www.google.ch and api.mywot.com.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.77.45	146.228.101.20	DNS	73	Standard query 0xf1b2 A www.google.ch
2	0.01988600	146.228.101.20	192.168.77.45	DNS	121	Standard query response 0xf1b2 A 173.194.44.216 A 173.194.44.215 A 173.194.44.223
3	0.20541700	192.168.77.1	224.0.0.1	IGMPv2	60	Membership Query, general
4	0.75281500	192.168.77.45	173.194.44.216	TCP	66	53611 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
5	0.77380000	173.194.44.216	192.168.77.45	TCP	66	http > 53611 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=64
6	0.77384700	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
7	0.85197200	192.168.77.45	146.228.101.20	DNS	73	Standard query 0x4833 A api.mywot.com
8	0.86517700	192.168.77.45	173.194.44.216	HTTP	370	GET / HTTP/1.1
9	0.87191600	146.228.101.20	192.168.77.45	DNS	89	Standard query response 0x4833 A 83.145.197.2
10	0.87339300	192.168.77.45	83.145.197.2	TCP	66	53613 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
11	0.88684700	173.194.44.216	192.168.77.45	TCP	60	http > 53611 [ACK] Seq=1 Ack=317 win=6912 Len=0
12	0.94406500	83.145.197.2	192.168.77.45	TCP	66	http > 53613 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=128
13	0.94411900	192.168.77.45	83.145.197.2	TCP	54	53613 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
14	0.94433800	192.168.77.45	83.145.197.2	HTTP	516	200 / HTTP/1.1 (text/css) 516 bytes

Durch Einfärbung der Pakete wird die Übersicht verbessert. Farben können individuell angepasst werden.

Nützliche Einstellungen in Wireshark

«Preferences»

1. Name Resolution einstellen

- Enable transport name resolution deaktivieren (echte Portnummern werden angezeigt)


2. Nützliche zusätzliche Columns

- Hinzufügen Cumulative Bytes
- Hinzufügen Delta time displayed
 - Mit Delta Times kann sortiert werden und du siehst wo eine Antwort lange gedauert hat.

Nützliche Profiles in Wireshark

- Nützliche Profile erstellen für Aufgaben (Shift + Ctrl + A)
 - Default
 - Nicht relative Sequenze Nummern & genaue Zeit
 - Preferences – TCP
 - AbsDandT

Anzeige eines Frames in Wireshark



```

+ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
+ Ethernet II, Src: IntelCor_6a:7d:d8 (10:0b:a9:6a:7d:d8), Dst: ZyxelCom_fd:7a:80 (00:13:49:fd:7a:80)
- Internet Protocol Version 4, Src: 192.168.77.45 (192.168.77.45), Dst: 146.228.101.20 (146.228.101.20)
  Version: 4
  Header length: 20 bytes
  + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 59
  Identification: 0x031c (796)
  - Flags: 0x00
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  + Header checksum: 0x31c8 [correct]
  Source: 192.168.77.45 (192.168.77.45)
  Destination: 146.228.101.20 (146.228.101.20)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  + User Datagram Protocol, Src Port: 53850 (53850), Dst Port: domain (53)
  + Domain Name System (query)

```

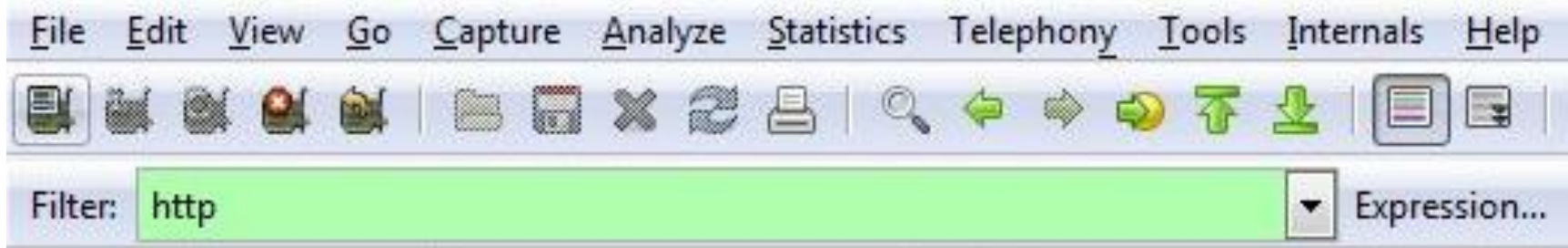
Packet Details

ISO/OSI	Protokoll	PDU*	Genaue Einheit	Adressierung
Layer 1	Ethernet IEEE 802.3	Bit	Signale in Bits	keine
Layer 2	Ethernet IEEE 802.3	Frame	Frames	MAC-Adresse
Layer 3	IPv4 IPv6	Paket	IP-Datagramme	IP-Adresse
Layer 4	TCP	Segment	TCP-Segmente	gehört zu IP-Paket (verbindungsorientiert)
Layer 4	UDP	Segment	UDP-Datagramme	Gehört zu IP-Paket (verbindungslos)
Layer 7	Anwendung (z.B. HTTP)	Daten	Nachricht	Wird an Layer 4 über API weitergereicht

Wichtig:

Ein Paket beginnt mit dem Metadaten Teil Frame (Layer 2).
Der effektive Frame beginnt allerdings erst bei Ethernet II.

Nützliche Anzeigefilter in Wireshark



- Mit Filtern kann die Auswahl der Pakete einfach auf die Gesuchten reduziert werden.
- Einige nützliche Filter:
 - http, dns, ip, ipv6, arp, bootp, icmp, tcp
- Mit «Clear» werden Filter aufgehoben

Weitere Anzeigefilter einfach verwenden in Wireshark

- Rechte Maustaste auf Feld (z.B. IP)
- Klicke auf «**Apply as Filter**»
- Klicke auf «**Selected**»

Nützliche Filter um unnützen Traffic auszuschliessen

Filter	Bemerkung
ip.addr == 192.168.1.2 host 192.168.1.2 host hostname ether host 00-02-a3-bb-00-01 dst host 192.168.1.2 src host 192.168.1.2 dst port 80	Nach einer spezifischen Host oder Port filtern
port 80	Nur Traffic auf Port 80
!port 80	Jeder Traffic ausser auf Port 80
!ip6	Jeder Traffic ausser IPv6
!arp	Jeder Traffic ausser ARP
not(tcp.port==80) and not (tcp.port==8080) and not(udp.srcport==53 and udp.dstport==53)	Ausschlussverfahren für guten Netzwerkverkehr

Follow TCP-Stream

Mit der nützlichen Funktion «Follow TCP-Stream» kann ein ganzer Stream einfach angezeigt werden.

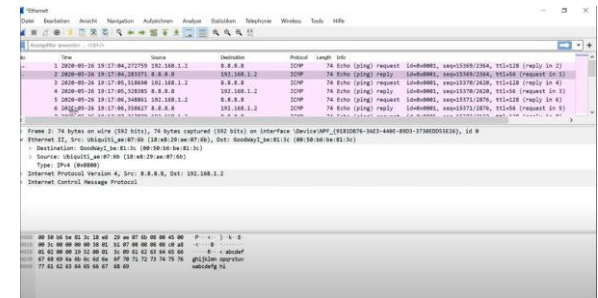
- Rechte Maustaste auf gewünschtes Paket
- Klicke «**Follow TCP-Stream**»

Nützliche Wireshark WIKI Informationen

- Das WIKI findet ihr unter
 - wiki.wireshark.org
 - Schnellsuche z.B. wiki.wireshark.org/ARP
- Direkt aus Wireshark
 - Rechte Maustaste auf Protokoll
 - Klicken **«Wiki Protocol Page»**

Nützliche Lernvideos und Beispiel Aufzeichnungsdateien auf www.wireshark.org

- Auf **www.wireshark.org** findest du nützliche Lernvideos und Beispiel Aufzeichnungsdateien.
- Schau dir das Lernvideo «**Introduction to Wireshark**» an <https://www.wireshark.org/#learnWS>
- <https://www.youtube.com/watch?v=yn3yzFDub1E> (deutsches Video)




Wireshark Einfärbungsregeln

Im Menü "View" auf "Coloring Rules...".

Im neuen Fenster ändern Sie entweder die bestehenden Farbregeeln durch einen Doppelklick ab oder Sie löschen sie komplett und legen neue an.

Default-Regeln:

 Wireshark · Einfärbungsregeln Default

Name	Filter
<input checked="" type="checkbox"/> Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
<input checked="" type="checkbox"/> HSRP State Change	hsrp.state != 8 && hsrp.state != 16
<input checked="" type="checkbox"/> Spanning Tree Topology Change	stp.type == 0x80
<input checked="" type="checkbox"/> OSPF State Change	ospf.msg != 1
<input checked="" type="checkbox"/> ICMP errors	icmp.type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.type eq 1 icmpv6.type eq 2 icmpv6.type eq 3
<input checked="" type="checkbox"/> ARP	arp
<input checked="" type="checkbox"/> ICMP	icmp icmpv6
<input checked="" type="checkbox"/> TCP RST	tcp.flags.reset eq 1
<input checked="" type="checkbox"/> SCTP ABORT	sctp.chunk_type eq ABORT
<input checked="" type="checkbox"/> TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && ip.protocol != 112)
<input checked="" type="checkbox"/> Checksum Errors	eth.fcs.status=="Bad" ip.checksum.status=="Bad" tcp.checksum.status=="Bad" udp.checksum.status=="Bad" sctp.checksum.status=="Bad"
<input checked="" type="checkbox"/> SMB	smb nbss nbns netbios
<input checked="" type="checkbox"/> HTTP	http tcp.port == 80 http2
<input checked="" type="checkbox"/> DCERPC	dcerpc
<input checked="" type="checkbox"/> Routing	hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp
<input checked="" type="checkbox"/> TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1
<input checked="" type="checkbox"/> TCP	tcp
<input checked="" type="checkbox"/> UDP	udp
<input checked="" type="checkbox"/> Broadcast	eth[0] & 1
<input checked="" type="checkbox"/> System Event	systemd_journal sysdig

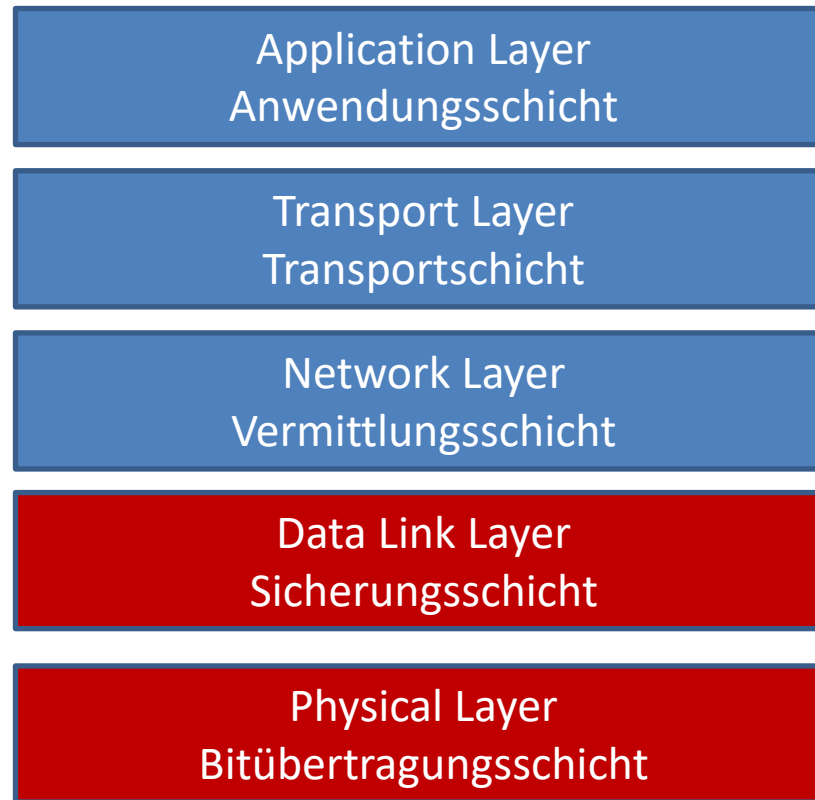
Agenda



«Grundlagen Local Area Networks»

CCNA1 Kapitel 1 «Introduction to TCP/IP Networking»

Einordnung LAN/WAN



TCP/IP					
OSI-Schicht	Einordnung	DoD-Schicht	Protokollbeispiel	Einheiten	
7	Anwendungen (Application)	Anwendungsorientiert	HTTP	Daten	
6	Darstellung (Presentation)		FTP		
5	Sitzung (Session)		HTTPS		
4	Transport (Transport)	Transportorientiert	TCP	TCP = Segmente UDP = Datagramme	
3	Vermittlung (Network)		UDP		
2	Vermittlungsschicht (Data Link)		SCTP		
1	Bitübertragung (Physical)	Netzzugriff	SPX	Pakete	
			ICMP		
			IGMP		
		Netzzugriff	IPsec	Rahmen (Frames)	
			IPX		
			Ethernet		
		Netzzugriff	Token Ring	Bits	
			FDDI		
			ARCNET		

Typische Bandbreitenverwendung im LAN

Basisbandübertragung

- Gesamte Bandbreite steht zur Verfügung
- **LAN Bereich** (z.B. Ethernet)



Breitbandübertragung

- Nur ein Teil (einzelner Kanal) der gesamten Bandbreite wird genutzt
- WAN Bereich (z.B. Fernsehen)








Repetition

Überblick der Übertragungsmedien

Medium	Medien-Typen	Wichtige Details
Kupferkabel (Twisted Pair, verdreht)	UTP = Unshielded Twisted Pair STP = Shielded Twisted Pair Elektronische Signale	RJ45-Stecker 4 verdrehte Aderpaare
Lichtwellenleiter (Glasfaserkabel)	Multimode (bis ca. 500m) Monomode/Singlemode (bis zu 50 KM mit 1Gbit/s) Optische Datenübertragung	SC-Stecker ST-Stecker LC-Stecker LWL-BNC-Stecker
Funk (Wireless LAN)	Access Point IEEE 802.11g – 54Mbit/s (2.4GHz) IEEE 802.11a – 54Mbit/s (5GHz) IEEE 802.11n – 600Mbit/s (2.4GHz und 5GHz) IEEE 802.11ac – 6.77Gbit/s	WEP (unsicher), WPA und WPA2 Verschlüsselung (sicher) WiFi (Wireless Fidelity) www.wi-fi.org

Die verschiedenen Twisted-Pair Kabel

Shielded-Twisted-Pair		Genaue Abschirmung
FTP		Foiled-Twisted-Pair, Folienabschirmung um alle Adernpaare
STP		Shielded-Twisted-Pair, Jedes Adernpaar ist ummantelt (Aluminiumfolie)
F/STP		Foiled/Shielded-Twisted-Pair, Kombination von Folienabschirmung und Ummantelung
S/STP		Screened-Foiled-Twisted-Pair, Jedes Adernpaar ist ummantelt und das ganze Kabel wird mit einem Metallgeflecht geschirmt.
SF/STP		Screended-Foiled/Shielded-Twisted-Pair, Kombination von Geflecht und Folie und Abschirmung einzelner Adernpaare

STP Kabel werden verwendet um elektromagnetischen Einflüssen (EMI) zu verringern!

Twisted-Pair Verdrahtung

Twisted-Pair Verdrahtung	Beschreibung
Straight-Through-Kabel	<p>Die Leiterpaare sind an den Steckern (RJ-45) gleich belegt, also gerade (z.B. 100BASE-T, Kontakte 1+2 und Kontakte 3+6).</p> <p>Diese Verkabelung wird zwischen PC und Switch verwendet.</p>
Crossover-Kabel	<p>Die Leiterpaare sind an den Steckern (RJ-45) gekreuzt (z.B. 100BASE-T, Kontakte 1 mit 3, 2 mit 6)</p> <p>Diese Verkabelung wird zwischen Switch und Switch oder PC und PC verwendet.</p>

Wichtig:

Heutige Switch-Geräte (Cisco: auto-mdix) erkennen die Kontaktbelegung automatisch und berichtigen diese ebenfalls automatisch.

Gruppenarbeit Vor- und Nachteile der verschiedenen Übertragungsmedien im LAN

Medium	Vorteile	Nachteile
Kupferkabel TP		
Lichtwellenleiter		
Funk (Wireless LAN)		

Zeit: 10 Minuten in Gruppen

Gruppenarbeit Vor- und Nachteile der verschiedenen Übertragungsmedien (Musterlösung)

Medium	Vorteile	Nachteile
Kupferkabel TP	Relativ günstig (Kabel und Komponenten) Einfach zu montieren Hohe Übertragungsgeschwindigkeit PoE	Störanfälligkeit (Dämpfung, Übersprechen) Abhören einfach möglich
Lichtwellenleiter	Relativ abhörsicher Nicht anfällig für elektro-magnetische Störungen und Überspannung (Blitz) Sehr weite Distanzen möglich Hohe Übertragungsgeschwindigkeit	Relativ teuer Kabel anfällig gegen knicken Viele Stecker Typen Komplexe Kabelverbindung
Funk (WLAN)	Relativ günstig (keine teure Verkabelung) Höchste Mobilität möglich	Beschränkte Reichweite Anfällig gegenüber Störeinflüssen Niedrige Übertragungsgeschwindigkeit

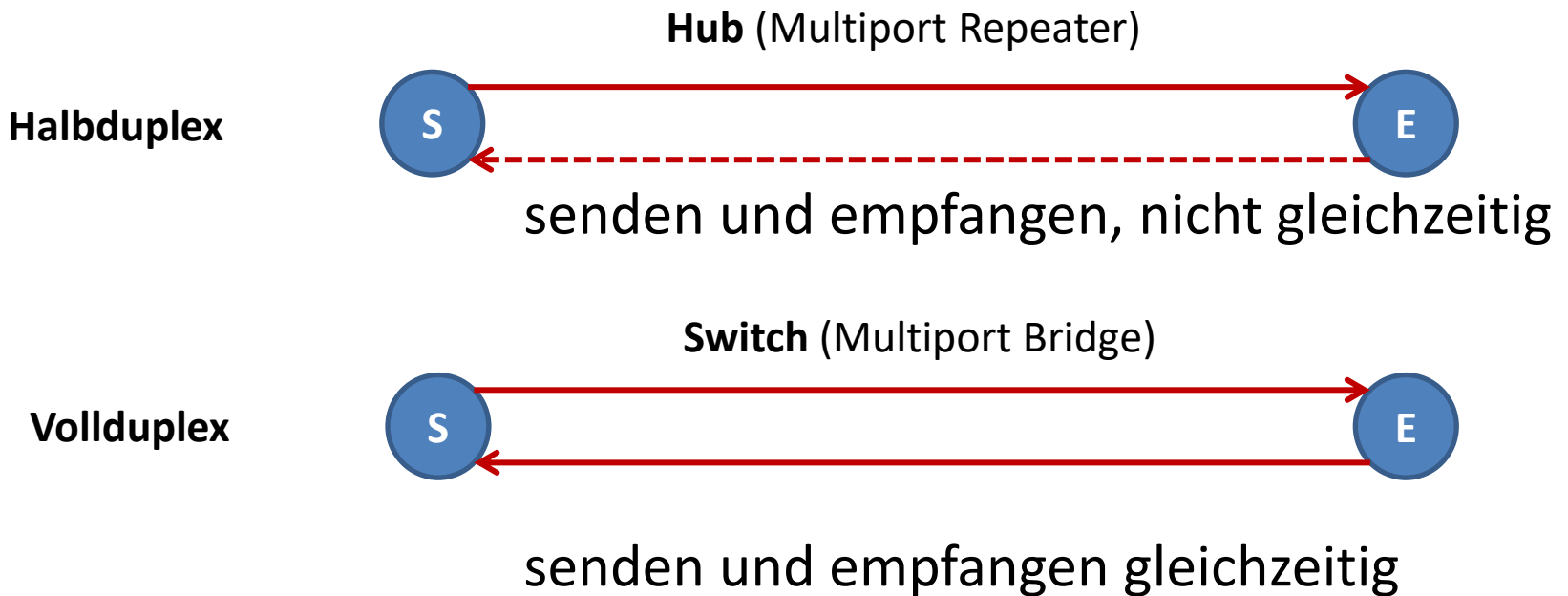
Einzelarbeit

Verschiedene Ethernet Typen

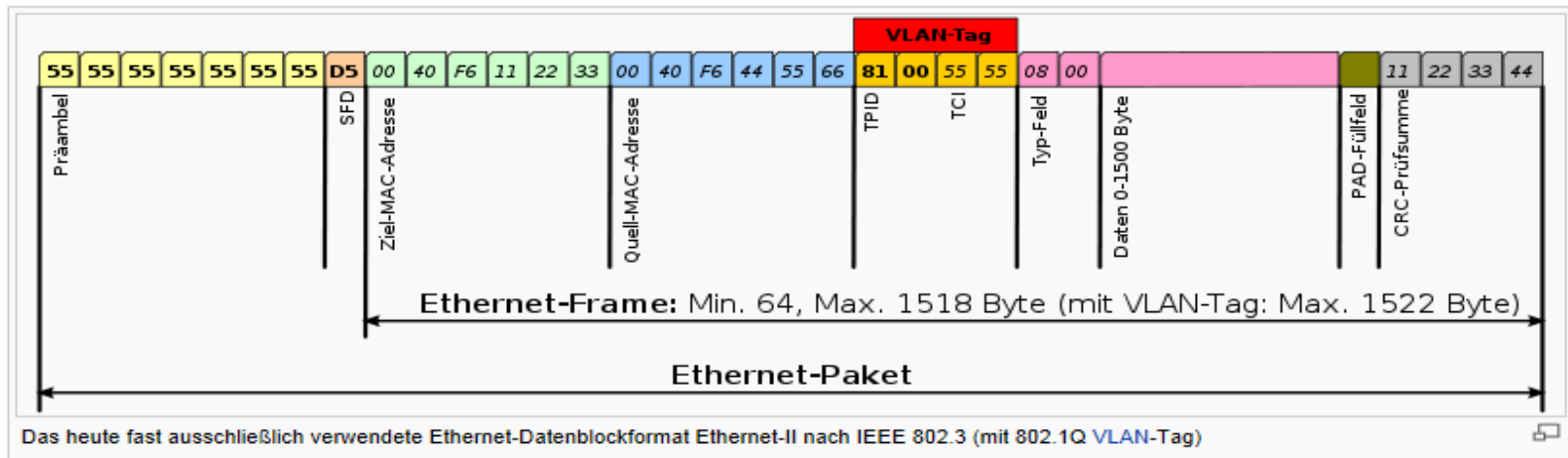
- Schaue einzeln die Tabelle Ethernet-Typen auf der Seite 37 und 48 im Buch an.
- Zeit: ca. 5 Minuten

Duplex-Modi in Ethernet-LANs mit CSMA/CD

In **Ethernet** basierenden Netzwerken nach **IEEE 802.3** wird als Medienzugriffsverfahren **CSMA/CD** (Carrier Sense Multiple Access/Collision Detection) verwendet. Dadurch kann ein Ethernet-Netzwerk mit Hub (Multiport Repeater) nur im Halbduplex Modus ausgeführt werden.



Aufbau eines IEEE 802.3 - Ethernet Frames (Gruppenarbeit)



Frames gemäss Ethernet **IEEE (Institute of Electrical and Electronics Engineers) 802.3:**

- Präambel zur Synchronisierung/ Start Frame Delimiter gibt an wann das erste Bit mit MAC beginnt
- VLAN-Tag für die Definition von VLANs
- Type Feld für die Definition des folgenden Protokolls auf höherer Schicht
- PAD Feld dient der Definition der Mindestgrösse von 64 Byte
- FCS (Frame Check Sequence)/Ethernet-Trailer enthält die CRC Prüfsumme des Frames. Stimmt dieser Wert nicht mit dem Frame überein wird das Frame verworfen. Für die Wiedertzustellung sind höhere Schichten, typischerweise TCP verantwortlich!

Quelle Grafik: Wikipedia.org

Die MAC-Adresse

Wert	Beschreibung
MAC-Adresse	Genannt auch: <ul style="list-style-type: none">- Ethernet Adresse, Physische Adresse, NIC-Adresse, LAN-Adresse- Burned-In-Adresse, weil fest vom Hersteller zugewiesen
Syntax	Beispiel: 00:60:2f:84:61:0a <ul style="list-style-type: none">- Erste 24 Bit (00:60:2f) sind OUI (Organizationally Unique Identifier) und bezeichnen den Hersteller (hier Cisco)- Letzten 24 Bit (84:61:0a) werden einmalig vom Hersteller vergeben
Darstellung	Darstellung mit - oder . also 00-60-2f-84-61-0a oder 00:60:2f:84:61:0a Unicast-Adresse: 00:60:2f:84:61:0a Broadcast-Adresse: ff:ff:ff:ff:ff:ff Multicast-Adressen: 01:00:5e:00:00:00 bis 01:00:5e:7f:ff:ff und 00:00:5e:00:01:ID für VRRP (Virtual Router Redundancy Protocol)

Aufgaben aus CCNA-Büchern

- Lösen der Aufgaben CCNA1, Kapitel 2
«Fundamentals of Ethernet LANs» S. 33
- Lösen der Aufgaben CCNA2, Kapitel 13
«LAN Architecture» S. 289

max. Zeit: 20 Minuten

Agenda



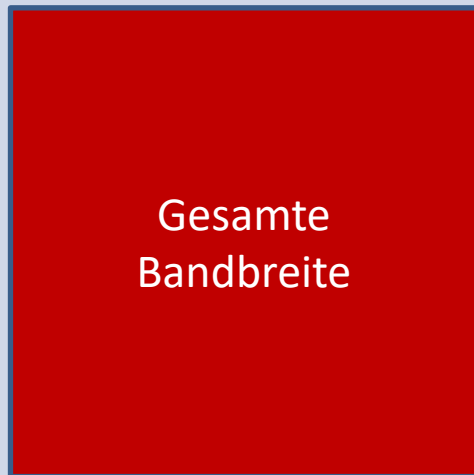
«Grundlagen Wide Area Networks»

CCNA1 Kapitel 3 «Fundamentals of WANs and IP Routing»

Typische Bandbreitenverwendung im WAN

Basisbandübertragung

- Gesamte Bandbreite steht zur Verfügung
- LAN Bereich (z.B. Ethernet)



Breitbandübertragung

- Nur ein Teil (einzelner Kanal) der gesamten Bandbreite wird genutzt
- **WAN Bereich** (z.B. Fernsehen)



Wichtige WAN Begriffe

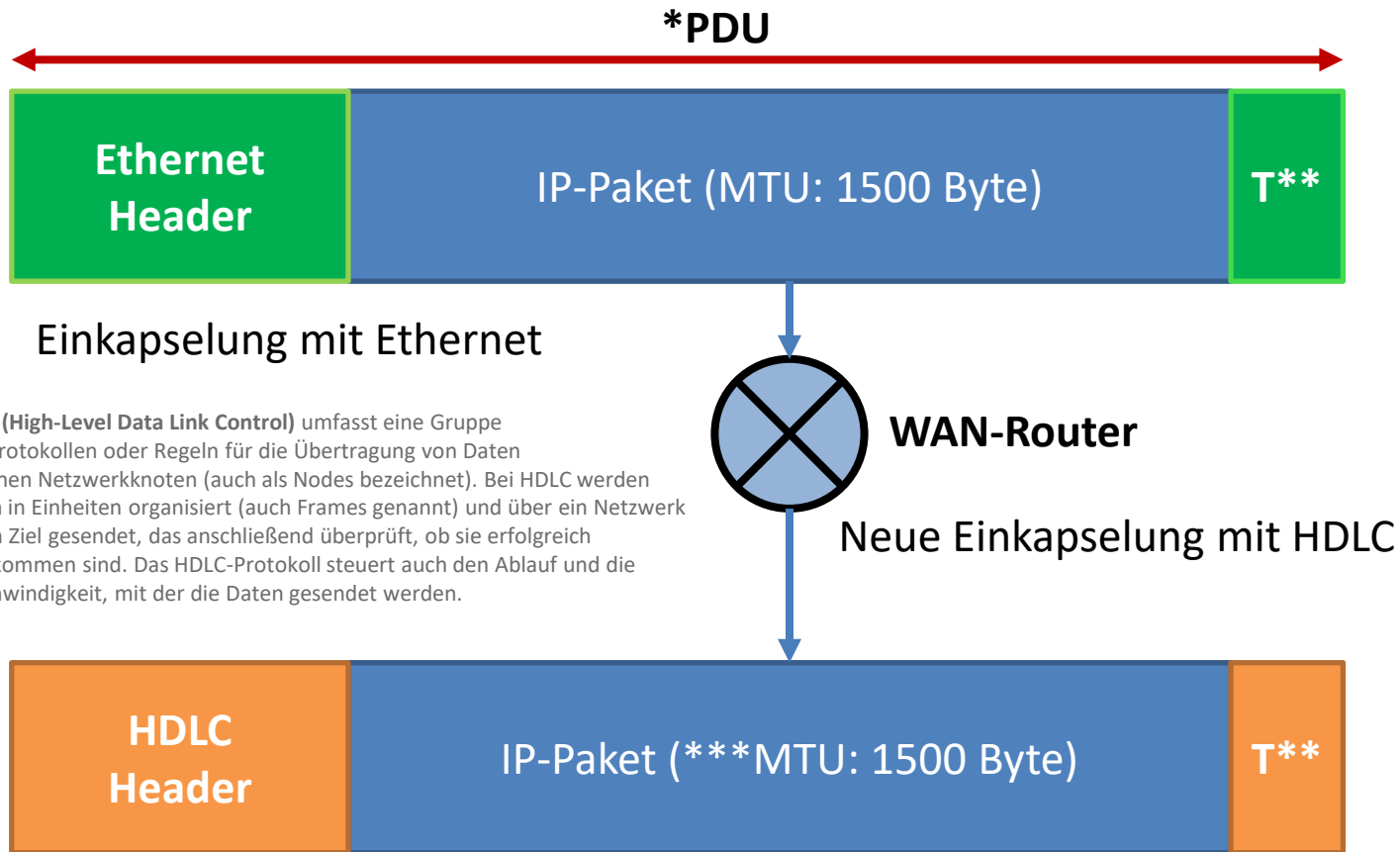
WAN-Begriffe	Beschreibung
CPE	Customer Premises Equipment (Kundenstandorteinrichtung) Dazu gehört der Router und die serielle Interfacekarte (CSU/DSU)
CSU/DSU	Channel Service Unit / Data Service Unit für die physische WAN Leitung (extern oder im Router integriert)
Point-to-Point Standleitung	Punkt zu Punkt Verbindung zwischen zwei Standorten
DTE- und DCE-Kabel	Data Terminal Equipment und Data Communication Equipment Kabel für serielle Schnittstelle
HDLC	High-Level Data Link Control Für Point-to-Point Verbindung (Standleitung zwischen Routern)
PPP	Point-to-Point Protocol Ebenfalls für Point-to-Point Verbindungen

MPLS - Protokoll

(NGN - Next Generation Network)

Technologie	Kurzbeschreibung
MPLS (Multiprotocol Label Switching)	<ul style="list-style-type: none">• Ist eine erste technische Umsetzung von NGN• Technologie wird auch IP over ATM (Asynchronous Transfer Mode) genannt• OSPF als Standard-Routingprotokoll (Open Shortest Path First)• Kleiner Bearbeitungsaufwand und Beschleunigung bei Routern (Label Switched Routers) <div><div>MPLS im TCP/IP Modell</div><div>Anwendung (z.B. HTTP)</div><div>Transport (TCP und UCP)</div><div>Internet (IP)</div><div>MPLS</div><div>Netzzugang (ATM, FR, Ethernet)</div></div>

Der Kapselungsprozess (Encapsulation)



*Protocol Data Unit

**Trailer / CRC-Prüfsumme / FSC

***Maximum Transmission Unit (Bezieht sich hier auf max. Nutzdatenteil bei Ethernet.)

Gruppenarbeit WAN-Anschlusstechnologien

WAN-Technologie	Kurzbeschreibung und Einsatzzweck
DSL (ADSL/VDSL)	
Breitbandkabel (Cable)	
Fiber to the Home FTTH	
Standleitung «Dark Fiber o. Dark Copper»	

Aufgabe in Zweiergruppen:

Nennt die gängigen Datentechniken für WAN-Verbindungen und wann diese für ein Projekt zu priorisieren sind? Nützliche Quellen sind eure Unterlagen und das Internet.

Zeit: 15 Minuten

Ende Block 2

«Ende»

Lernziele des 2. Modulblocks

- **Du kannst...**

1. ...anhand des ISO/OSI-Referenzmodells den Kommunikationsprozess beschreiben.
2. ...mittels dem Tool Wireshark Protokolle analysieren.
3. ...mittels Wireshark Displayfilter die Anzeige auf das Gesuchte eingrenzen.
4. ...die grundlegenden Elemente betreffend LAN- und WAN Netzwerken beschreiben.

Selbststudium

2. Modul:

- Repetition der Folieninhalte des Modulblocks:
Ergänzen deiner individuellen Zusammenfassung.
- **Lernstoff Vertiefung:**
 - CCNA1 Kapitel 1 «Introduction to TCP/IP Networking»
 - CCNA1 Kapitel 3 «Fundamentals of WANs and IP Routing»
 - optional CCNA2 Kapitel 14 «WAN Architecture»
 - Network Academy: <https://www.netacad.com/portal> Cisco NetAcademy Kapitel 3
- **Lernvideos «Youtube»:**
Suche ein gutes Lernvideo über Wireshark und nimm deinen Vorschlag in den Unterricht für den gemeinsamen Austausch mit.
- **Praxistransfer:**
Analysiere die Webseite deiner Firma mit Wireshark. Nutze dazu Linux. Bringe die Ergebnisse der Aufzeichnungen zur Besprechung in den Unterricht mit. Versuche folgendes zu filtern:
 - Welche DNS-Querys werden beim Öffnen der Webseite gemacht?
 - Welches TLS-Protokoll wird für die Webseite genutzt.
 - Im TLS-Handshake befindet sich das SNI-Feld. Filtere alle SNI Informationen, welche beim Öffnen der Webseite angezeigt werden.
 - Wozu wird SNI «Server Name Indication» bei TLS genutzt?Auf «<https://github.com/OCSAF/freesvcheck>» findest du ein BASH-Skript, welchen du für deine Zwecke für die Analyse mittels tshark anpassen kannst. Vorbereitung auf das nächste Modul:
Lese dich mittels der HELP und der Manpage in die DNS-Tools dig und nslookup ein.
- **Vorbereitung auf das nächste Modul:**
Lese dich mittels der HELP und der Manpage in die DNS-Tools dig und nslookup ein.