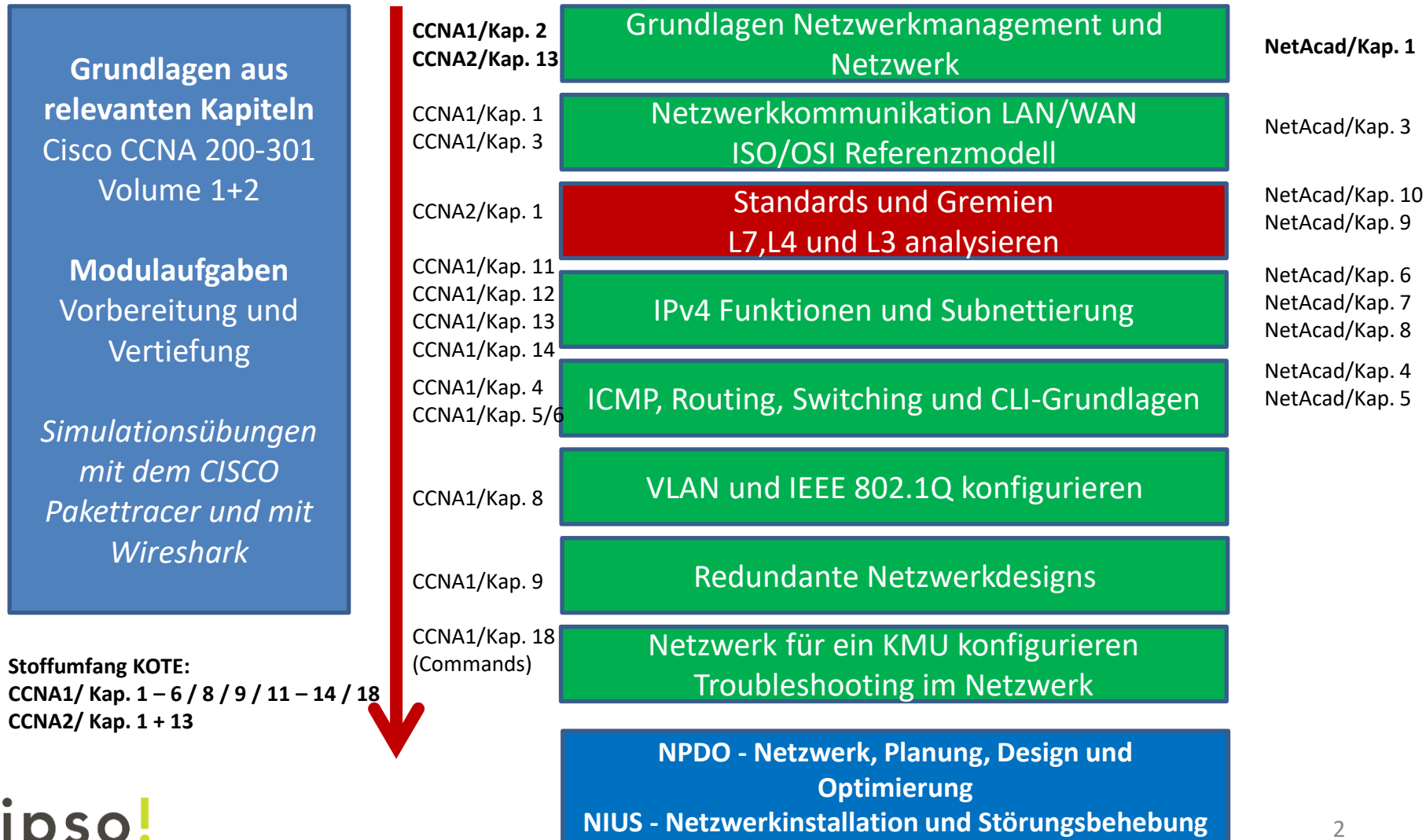




Kommunikationstechnik KOTE / Netzwerkgrundlagen

3. Unit

Übersicht der einzelnen Modulblöcke (roter Faden)



Lernziele des 3. Modulblocks

- **Du kannst...**

1. ...wichtige Standards und Gremien, wie ISOC, IANA, RFC, IEEE usw. erklären.
2. ...die grundlegenden Funktionen der Anwendungsschicht, der Transportschicht und der Vermittlungsschicht anhand von TCP/IP-basierenden Protokollen mittels Wireshark analysieren.
3. ...den Aufbau des Domain Name System (DNS) beschreiben.
4. ...grundlegende technische Funktionen von TCP und UDP einordnen.

Agenda

«Kurztest»

Ablauf Kurztest

- Ergänze nachfolgend in den Folien die Lücken. Du hast jeweils **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!**

1. Aufgabe zu den Grundlagen der technischen Kommunikation

- Ein Multiport Repeater läuft imDuplex Modus. Dagegen läuft eine Multiport Bridge imDuplex Modus. Eine Multiport Bridge wird auch genannt.
- Mit dem Netzwerktool können Netzwerkverbindungen aufgezeichnet werden. Ein solches Programm wird generell als bezeichnet.
- Ein wichtiges Sicherungsschichtprotokoll für WAN-Standleitungen ist

2. Aufgabe zu den Grundlagen der Netzwerktechnik

- Schreiben Sie die 7 Schichten des ISO/OSI-Modells in Deutsch und in der richtigen Reihenfolge auf.
- Welche Schichten gehören dabei zu den transportorientierten und welche zu den anwendungsorientierten (sowohl OSI- als auch TCP/IP-Modell)

1. Aufgabe Musterlösung zu den Grundlagen der technischen Kommunikation

- Ein Multiport Repeater läuft im **Halb Duplex** Modus. Dagegen läuft eine Multiport Bridge im **Voll Duplex** Modus. Eine Multiport Bridge wird auch **Switch** genannt.
- Mit dem Netzwerktool **Wireshark** können Netzwerkverbindungen aufgezeichnet werden. Ein solches Programm wird generell als **Sniffer** bezeichnet.
- Ein wichtiges Sicherungsschichtprotokoll für WAN-Standleitungen ist **HDLC (High-Level Data Link Control)**.

2. Aufgabe Musterlösung

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

Agenda

«Repetition Blöcke 1 und 2»

Gruppenarbeit

Repetition Block 2

Auftrag: Jede Gruppe bereitet eines der folgenden 5 Themen soweit vor, dass sie es den Kollegen im Anschluss erklären können.

Form: keine Vorgabe

Zeit: Vorbereitung ca. 25 Minuten

Themen:

1. Erklärung der Grundlagen des Schichtenmodells TCP/IP (aktualisiert)
2. Erklärung des Kapselungs- und Fragmentierungsprozesses über alle Schichten
3. Erklärung der Vor- und Nachteile der verschiedenen Übertragungsmedien
4. Erklärung der WAN-Anschlusstechnologien

Repetition Block 2

Fragen zur Vertiefung:

- CCNA1 Kapitel 1 «Introduction to TCP/IP Networking»
- CCNA1 Kapitel 2 «Fundamentals of Ethernet LANs»

Praxistransfer: Besprechung in den Gruppen

Zeit: 30 Minuten

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.

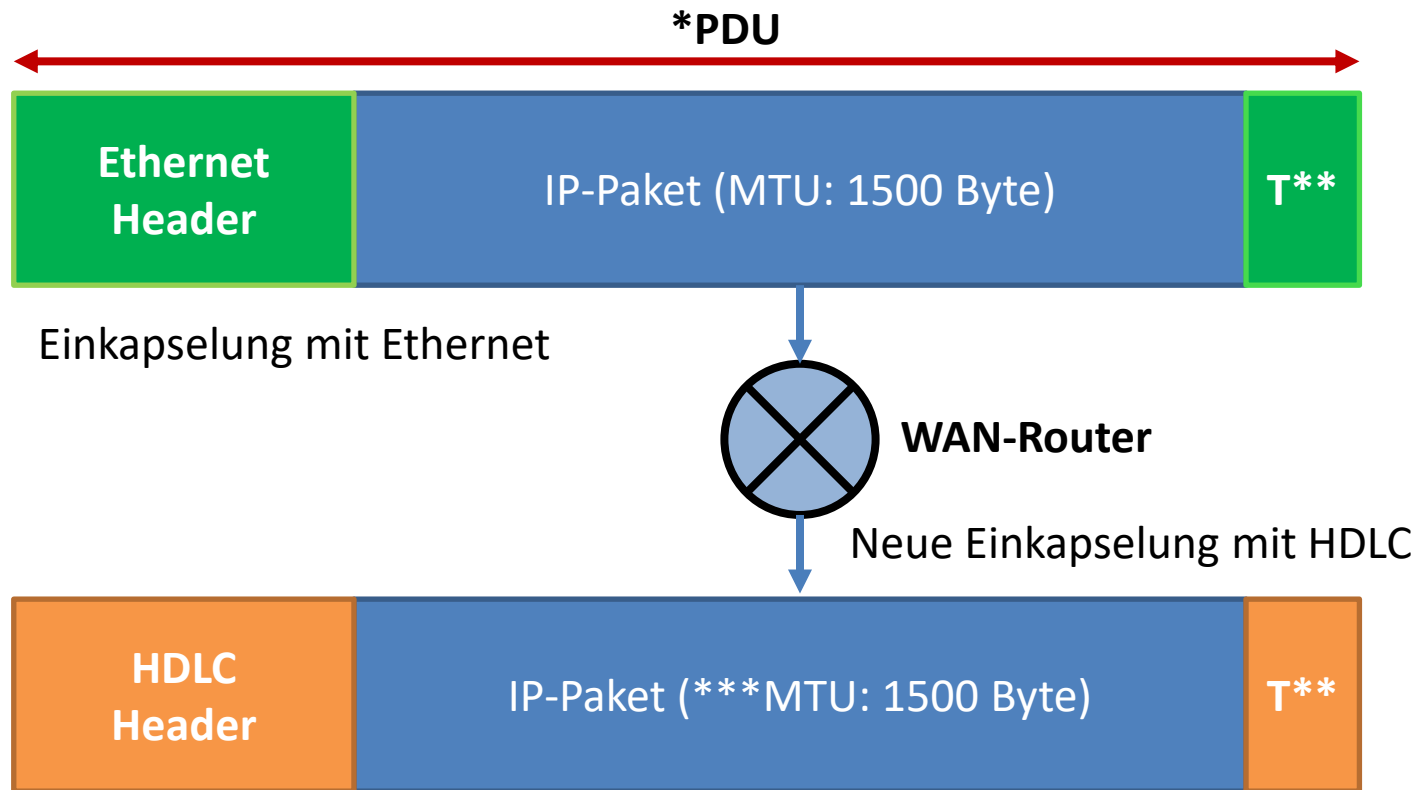
Zeit: 10 Minuten

Musterlösung

WAN-Technologie	Beschreibung
Modem Analog oder ISDN	Noch teilweise für Wartung und Fernüberwachung im Einsatz
DSL (ADSL/VDSL)	Bestehende Telefonverbindung kann genutzt werden. Relativ günstig und schnell aber ohne Servicelevel (DSL-Business) nicht ausfallsicher.
Breitbandkabel (Cable)	Bestehende Fernsehverbindung kann genutzt werden. Relativ günstig und in der Regel schneller als DSL.
Fiber to the Home FTTH	Verbindung über schnelle Glasfaserleitungen. Auch hier ist auf SLAs zu achten.
Standleitung «Dark Fiber o. Dark Copper»	Nur Leitung wird gemietet, Geräte müssen selber beschafft werden (daher Dark).

Repetition

Der Kapselungsprozess (Encapsulation)



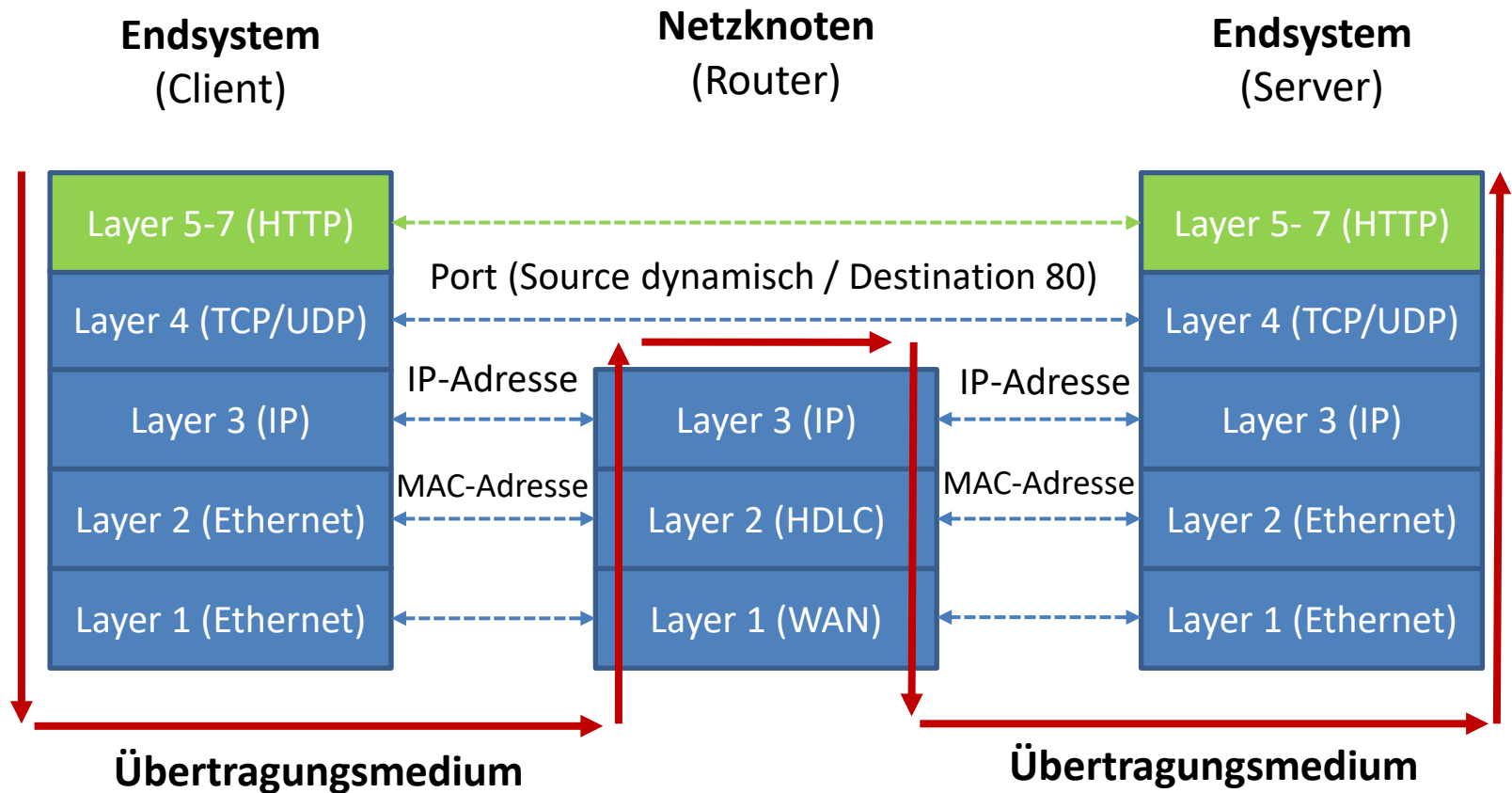
*Protocol Data Unit

**Trailer / CRC-Prüfsumme

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

Repetition

Der Übertragungsprozess



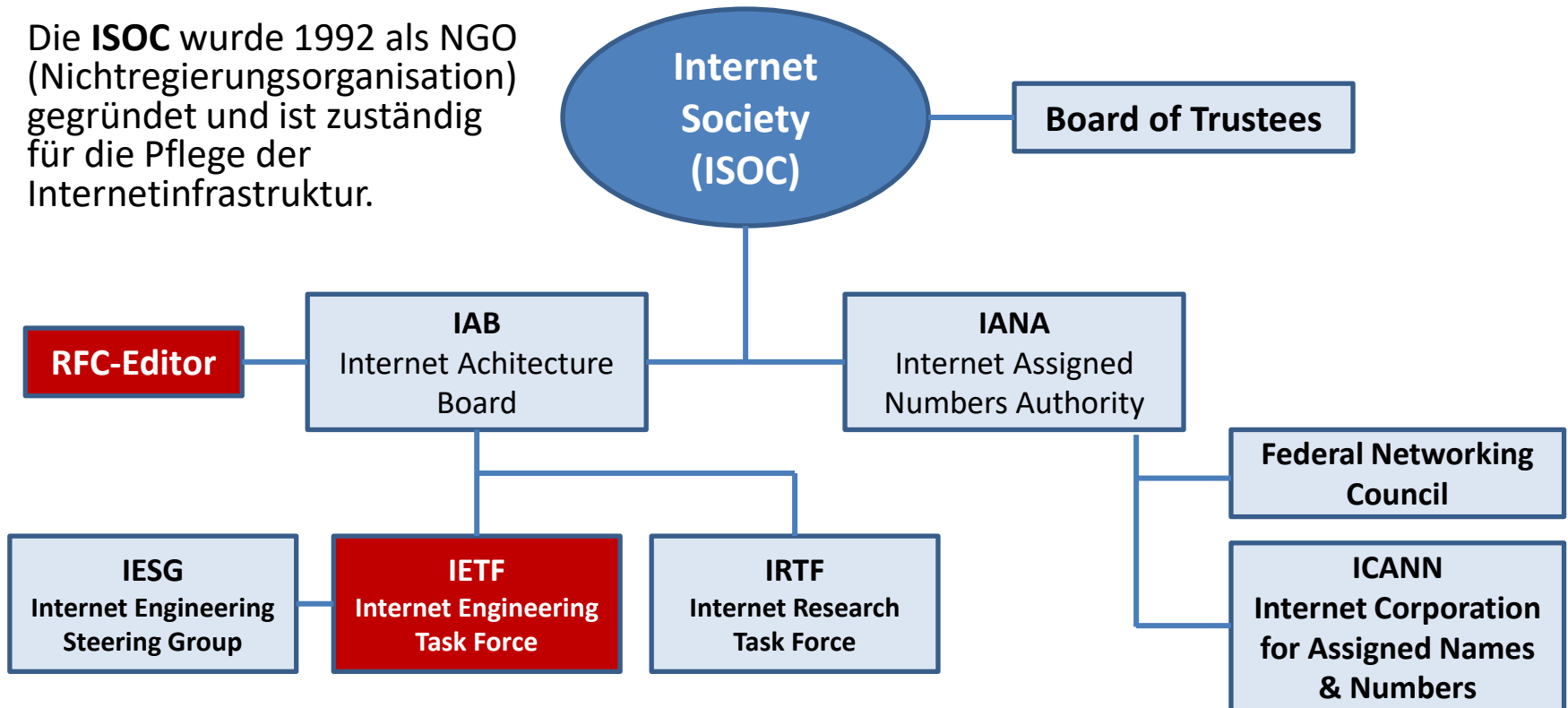
Agenda



«Grundlagen TCP/IP Standards»

Wichtige Organisationen (ISOC)

Die **ISOC** wurde 1992 als NGO (Nichtregierungsorganisation) gegründet und ist zuständig für die Pflege der Internetinfrastruktur.



In Anlehnung an Darstellung auf Wikipedia - <http://de.wikipedia.org/wiki/ISOC>

RFC (Request for Comments)

RFC Status (RFC 2026)	Beschreibung
Proposed Standard	Ein Vorschlag für einen Standard
Draft Standard	Entwurf zur Begutachtung nach erfolgreichen Implementierungen
Internet Standard	Implementierter offizieller Standard
Informational	Hinweis oder Idee
Experimental	Zum Ausprobieren, Potentieller neuer Standard im Anfangsstadium
Historic	Wird nicht mehr benutzt oder ist abgelöst

Die Weiterentwicklung von Internetstandards mit neuen RFCs ist dynamisch. Mehr dazu auf www.rfc-editor.org

Weitere wichtige technische Standards

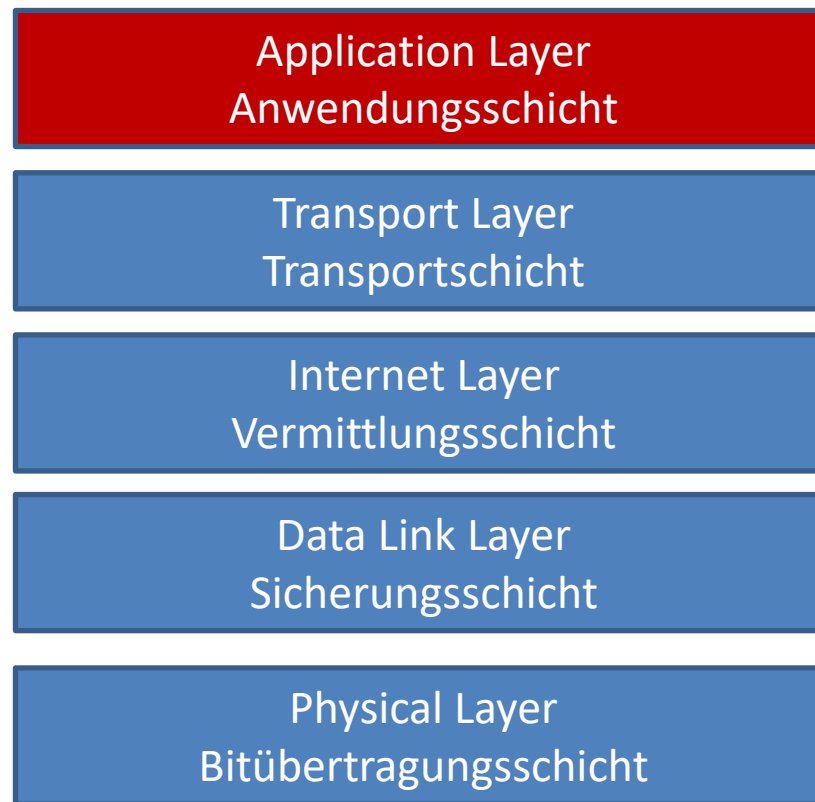
Standardgremien	Beschreibung
ITU – International Telecommunication Union www.itu.int	Sonderorganisation der UNO . Beschäftigt sich mit technischen Aspekten (Standards) der weltweiten Telekommunikation.
IEEE – Institute of Electrical and Electronics Engineers www.ieee.org	Ein weltweiter Berufsverband von Elektrotechnik und Informationstechnik Ingenieuren. Hier werden unter anderem die IEEE-Standards festgelegt.
W3C – World Wide Web Consortium www.w3.org	Gremium zur Festlegung der World Wide Web «Standards». Gibt Empfehlungen (Recommendations) heraus (z.B. HTML, XHTML, CSS, RSS, XML,..). Gründer und Vorsitzender ist niemand geringerer als Tim Berners-Lee, Erfinder des WWW.

Agenda

«Anwendungsschicht»

CCNA2 Kapitel 1 «Introduction to TCP/IP Transport and Applications»

Einordnung der Anwendungsschicht



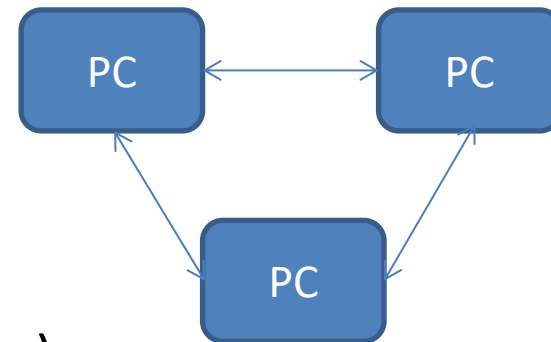
TCP/IP				
OSI-Schicht	Einordnung	DoD-Schicht	Protokollbeispiel	Einheiten
7 Anwendungen (Application)	Anwendungs- orientiert	Anwendung	HTTP FTP HTTPS SMTP LDAP NCP	Daten
6 Darstellung (Presentation)				
5 Sitzung (Session)				
4 Transport (Transport)	Transport- orientiert	Transport	TCP UDP SCTP SPX	TCP = 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

ICT-Grundlagen

Netzwerkstrukturen (Aufbau)

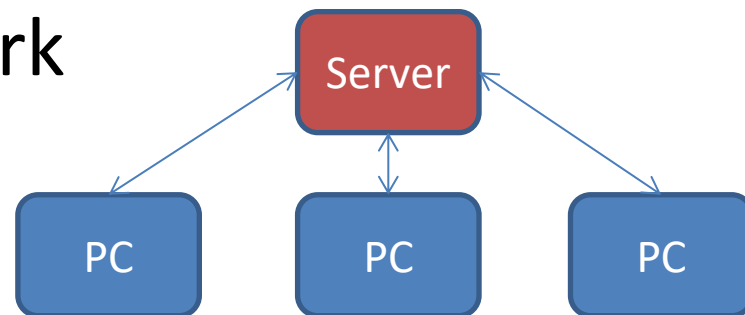
- Peer-to-Peer Netzwerk

- File-Distribution (BitTorrent)
- Internettelefonie (Skype)
- File-Sharing (eMule, LimeWire)



- Client-Server-Netzwerk

- Internethandel (Amazon)
- Webmail (Hotmail)
- Suchmaschine (Google)



ICT-Grundlagen

Three Tier Architecture

Präsentation
(Front End)

Geschäftslogik
(Funktion, Middle
Tier)

Datenhaltung
(Datenbank)

ICT-Grundlagen

Beispiele für verteilte Systeme

Thin-Client Remote Presentation

Präsentation
(Front End)

Geschäftslogik
(Funktion)

Datenhaltung
(Datenbank)

Client

Server

Daten-Server Remote Datamanagement

Präsentation
(Front End)

Geschäftslogik
(Funktion)

Datenhaltung
(Datenbank)

Fat-Client Distributed Database

Präsentation
(Front End)

Geschäftslogik
(Funktion)

Datenhaltung
(Datenbank)

Datenhaltung

Die Anwendungsschicht im Überblick

- Hier sind die **Anwendungsschichtprotokolle** beheimatet:
 - HTTP (Anzeigen von Webseiten)
 - DNS (Auflösen von Hostnamen in IP-Adressen)
 - FTP (Einfacher Datentransfer)
 - SMTP (Übermittlung von E-Mails)
 - POP3 (Abholen von E-Mails beim Hoster/ISP)
 - DHCP (Verteilen von Netzwerkkonfigurationen wie IPs)
- Die Informationspakete heissen **Nachricht**

Agenda

**«Beispiel HTTP
Anwendungsprotokoll»**

HTTP GET (Anfordern von Webseiten)

HTTP-Aufzeichnung mit Wireshark

The screenshot displays the Wireshark network protocol analyzer interface. The top 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 at the top shows 'Filter: http' and 'Expression... Clear Apply Save'. The packet list pane on the left shows a list of captured packets, with packet 8 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data of the selected packet.

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
8	0.86517700	192.168.77.45	173.194.44.216	HTTP	370	GET / HTTP/1.1
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
45	1.01328400	173.194.44.216	192.168.77.45	HTTP	428	HTTP/1.1 200 OK (text/html)
51	1.03679300	83.145.197.2	192.168.77.45	HTTP/XM	1323	HTTP/1.1 200 OK
65	1.17333900	192.168.77.45	83.145.197.2	HTTP	572	GET /0.4/query?id=e4ac84f4c9f4d90bd90e308d09a92882d17c96af&nonce=1f6112cc855a450656b66d834bc8e8965c5636df&target=SeoowEGAyfa2&la
72	1.24973000	83.145.197.2	192.168.77.45	HTTP/XM	877	HTTP/1.1 200 OK
76	1.26751300	192.168.77.45	173.194.44.216	HTTP	629	GET /images/icons/product/chrome-48.png HTTP/1.1
82	1.29694900	173.194.44.216	192.168.77.45	HTTP	757	HTTP/1.1 200 OK (PNG)
89	1.30280800	192.168.77.45	173.194.44.216	HTTP	617	GET /images/srpr/logo3w.png HTTP/1.1
90	1.30620400	192.168.77.45	173.194.44.216	HTTP	757	GET /xjs/_/js/s/c/sb,cr,vm,cdos,jjsa,sf,tbpr,tbui,rsn,ob,mb,lc,hv,k1c,kat,esp,erh,bihu,amcl,kp,lu,m,shb,sfa,hsm,j,p,pcc,csi/rt=j/
100	1.34561000	173.194.44.216	192.168.77.45	HTTP	122	HTTP/1.1 200 OK (PNG)
127	1.37964700	192.168.77.45	83.145.197.2	HTTP	658	GET /0.4/link?id=e4ac84f4c9f4d90bd90e308d09a92882d17c96af&nonce=7c7f8652e13738b743a3da48dec469ba466f0b94&hosts=vRTn1s5%2BSqSOMNV
182	1.46355600	83.145.197.2	192.168.77.45	HTTP/XM	612	HTTP/1.1 200 OK
281	1.60610000	192.168.77.45	188.121.36.239	OCSP	541	Request
292	1.62321700	173.194.44.216	192.168.77.45	HTTP	376	HTTP/1.1 200 OK (text/javascript)

Frame 8: 370 bytes on wire (2960 bits), 370 bytes captured (2960 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: 173.194.44.216 (173.194.44.216)

Transmission Control Protocol, Src Port: 53611 (53611), Dst Port: http (80), Seq: 1, Ack: 1, Len: 316

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]

Request Method: GET

Request URI: /

Request Version: HTTP/1.1

Host: www.google.ch\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:17.0) Gecko/20100101 Firefox/17.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

DNT: 1\r\n

Connection: keep-alive\r\n

\r\n

[Full] request URI: http://www.google.ch/

0000 00 13 49 fd 7a 80 10 0b a9 6a 7d d8 08 00 45 00 ...I.Z... .}}...E.

0010 01 64 03 20 40 00 80 06 0e 04 c0 a8 4d 2d ad c2 ...d. Q... ..M...

0020 2c d8 d1 6b 00 50 d8 ac 74 6f a0 9a 3d 6f 30 18 ...k.P... to...oP.

0030 11 04 b8 e7 00 00 47 45 54 20 2f 20 48 54 54 50 ...GE T / HTTP

0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e .../1.1..Ho st: www.

0050 67 6f 6f 67 6c 65 2e 63 68 0d 0a 55 73 65 72 2d ...google.c h..User-

Frame (frame), 370 bytes

Packets: 1673 Displayed: 150 Marked: 0

Profile: Default

HTTP 200 OK (Daten vom Server zum Client und OK-Meldung)

HTTP-Aufzeichnung mit Wireshark

Capturing from Microsoft\Device\NPF_{37FAF8A3-D329-440B-8FE7-FBB87A4D8901} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
8	0.86517700	192.168.77.45	173.194.44.216	HTTP	370	GET / HTTP/1.1
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
45	1.01328400	173.194.44.216	192.168.77.45	HTTP	428	HTTP/1.1 200 OK (text/html)
51	1.03679300	83.145.197.2	192.168.77.45	HTTP/XM	1323	HTTP/1.1 200 OK
65	1.17333900	192.168.77.45	83.145.197.2	HTTP	572	GET /0.4/query?id=e4ac84f4c9f4d90bd90e308d09a92882d17c96af&nonce=1f6112cc855a450656b66d834bc8e8965c5636df&target=5e0owEGayfa2&la
72	1.24973000	83.145.197.2	192.168.77.45	HTTP/XM	877	HTTP/1.1 200 OK
76	1.26751300	192.168.77.45	173.194.44.216	HTTP	629	GET /images/icons/product/chrome-48.png HTTP/1.1
82	1.29694900	173.194.44.216	192.168.77.45	HTTP	757	HTTP/1.1 200 OK (PNG)
89	1.30280800	192.168.77.45	173.194.44.216	HTTP	617	GET /images/srpr/logo3w.png HTTP/1.1
90	1.30620400	192.168.77.45	173.194.44.216	HTTP	757	GET /xjs/_/js/s/c, sb, cr, vm, cdos, jsa, sf, tbpr, tbui, rsn, ob, mb, lc, hv, klc, kat, esp, erh, bihu, amcl, kp, lu, m, shb, sfa, hsm, j, p, pcc, csi/rt=j/
100	1.34561000	173.194.44.216	192.168.77.45	HTTP	122	HTTP/1.1 200 OK (PNG)
127	1.37964700	192.168.77.45	83.145.197.2	HTTP	658	GET /0.4/link?id=e4ac84f4c9f4d90bd90e308d09a92882d17c96af&nonce=7c7f8652e13738b743a3da48dec469ba466f0b94&hosts=vRTn1s5s2B5QsOMNV
182	1.46355600	83.145.197.2	192.168.77.45	HTTP/XM	612	HTTP/1.1 200 OK
281	1.60610000	192.168.77.45	188.121.36.239	OCSP	541	Request
292	1.62321700	173.194.44.216	192.168.77.45	HTTP	376	HTTP/1.1 200 OK (text/javascript)

Internet Protocol Version 4, Src: 173.194.44.216 (173.194.44.216), Dst: 192.168.77.45 (192.168.77.45)

Transmission Control Protocol, Src Port: http (80), Dst Port: 53611 (53611), Seq: 28137, Ack: 317, Len: 374

[21 Reassembled TCP Segments (28510 bytes): #15(1452), #16(1452), #18(1068), #19(1452), #21(1452), #22(1192), #24(1452), #25(1452), #27(1192), #28(1452), #30(1452), #31(1452), #33(1452), #34(1452)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: wed, 02 Jan 2013 14:14:11 GMT\r\n

Expires: -1\r\n

Cache-Control: private, max-age=0\r\n

Content-Type: text/html; charset=UTF-8\r\n

Set-Cookie: PREF=ID=ee92050a3f049faa:FF=0;TM=1357136051:LM=1357136051:S=awEKRUvLk805cjG3; expires=Fri, 02-Jan-2015 14:14:11 GMT; path=/; domain=.google.ch\r\n

Set-Cookie: NID=67=DBktPbNog2_80jubTz9V5jPwU9L_XY2CK6f4dsxSCUR50ye8BqkLYITVpZB8u73IUVIotmt98gz459lCs0kQixxqNEUvyrQ8-lSudocNayIM8v78AxPj2Pq7o0cmv; expires=Thu, 04-Jul-2013 14:14:11 GMT; path=/P3P: CP="This is not a P3P policy! See http://www.google.com/support/accounts/bin/answer.py?hl=en&answer=151657 for more info.""\r\n

Content-Encoding: gzip\r\n

Transfer-Encoding: chunked\r\n

Server: gws\r\n

X-XSS-Protection: 1; mode=block\r\n

X-Frame-Options: SAMEORIGIN\r\n

\r\n

HTTP chunked response

Content-encoded entity body (gzip): 27709 bytes -> 95543 bytes

Line-based text data: text/html

Frame (428 bytes) | Reassembled TCP (28510 bytes) | De-chunked entity body (27709 bytes) | Uncompressed entity body (95543 bytes)

Frame (frame), 428 bytes

Packets: 2404 Displayed: 255 Marked: 0

Profile: Default

Agenda

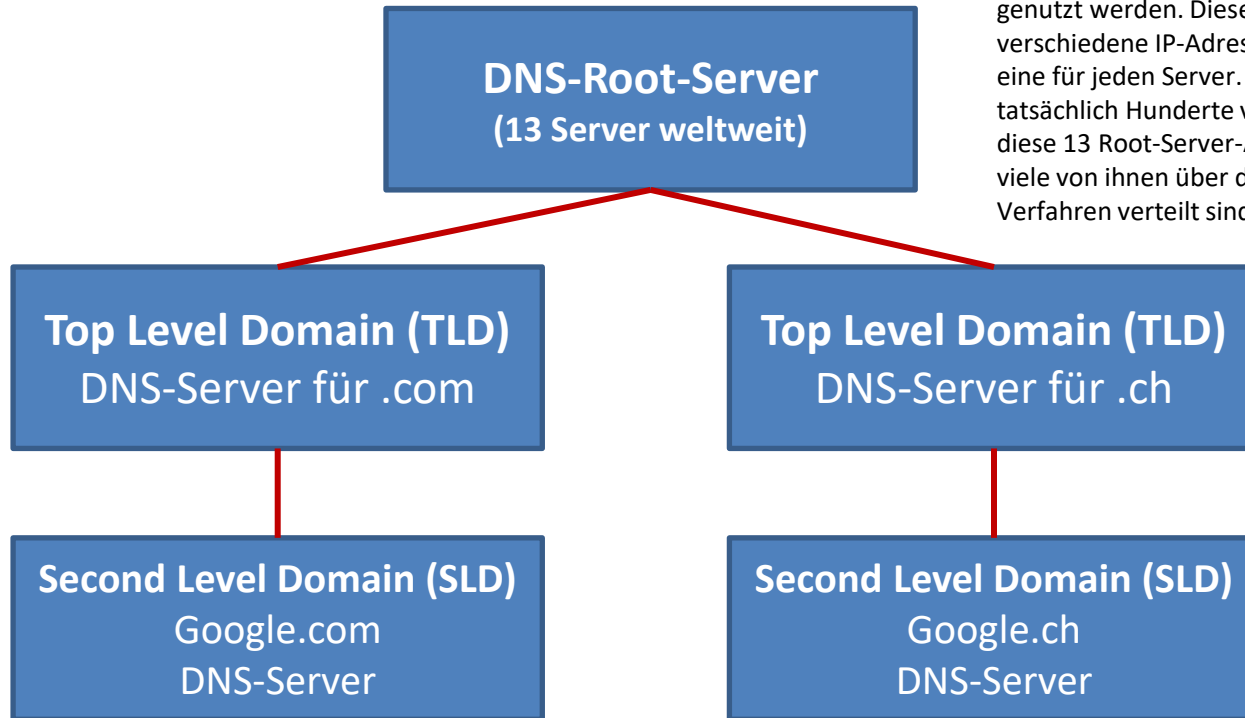
«Domain Name System»

CCNA2 Kapitel 1 «Introduction to TCP/IP Transport and Applications»

Namensauflösungsmöglichkeiten

Namensauflösung	Kurzbeschreibung
Hosts-Datei Obwohl die Hosts-Datei sehr nützlich sein kann, ist sie nicht für groß angelegte oder dynamische Netzwerkanwendungen geeignet. Sie muss manuell gepflegt werden, was in großen Netzwerken oder bei häufigen Änderungen unpraktisch ist. Moderne DNS-Dienste bieten dynamische, skalierbare und automatisch verwaltete Lösungen, die für die heutigen Internet- und Netzwerkanforderungen besser geeignet sind.	<ul style="list-style-type: none">• Einfache Textdatei zur Zuordnung von IP-Adressen zu Hostnamen• Zum Beispiel: 127.0.0.1 localhost• Achtung vor Hackermanipulation
WINS (Windows Internet Naming Service) NetBIOS wurde ursprünglich in den 1980er Jahren entwickelt und war eine Schlüsselkomponente in den LAN-Manager- und späteren Windows-Netzwerken. Mit der Zeit wurde es jedoch durch modernere Technologien wie das Domain Name System (DNS) verdrängt, das dynamischere und skalierbare Netzwerklösungen bietet, insbesondere im Internet.	<ul style="list-style-type: none">• Wurde von Microsoft entwickelt• Auflösungen von NetBIOS-Namen• Wird im Gegensatz zu DNS nur im internen Netzwerk verwendet• WINS sollte nicht mehr eingesetzt werden
DNS (Domain Name System)	<ul style="list-style-type: none">• Wird in IP-basierenden Netzwerken im LAN und Internet zur Namensauflösung verwendet. (RFC 1034 und RFC 1035)• Auflösung URL in IP-Adresse

DNS-Hierarchie in der Übersicht (Auflösung URL in IP-Adresse)



Es gibt 13 DNS-Root-Server, die im Internet genutzt werden. Diese Server sind durch 13 verschiedene IP-Adressen repräsentiert, jeweils eine für jeden Server. Allerdings gibt es tatsächlich Hunderte von physischen Servern, die diese 13 Root-Server-Adressen verwenden, da viele von ihnen über das Anycast-Routing-Verfahren verteilt sind

Verantwortung trägt die **ICANN*** für die DNS-Root-Server und Top Level Domains (TLD)

*Internet Corporation for Assigned Names and Numbers

DNS-Root-Server in der Übersicht

<http://www.internic.net/domain/named.root>

13 DNS-Root-Server

- A. Verisign, Dulles (USA)
- B. USC-ISI Marina del Rey (USA)
- C. Cogent, Herndon und Los Angeles (USA)
- D. U Maryland College Park (USA)
- E. NASA, Mt. View (USA)
- F. Internet Software C., Palo Alto und 36 weitere Standorte (USA)
- G. US DoD Vienna (USA)
- H. ARL Aberdeen (USA)
- I. Autonomica, Stockholm und 28 andere Standorte (EU)
- J. Verisign und 21 Standorte (USA)
- K. RIPE, London und 16 weitere Standorte (EU)
- L. ICANN, Los Angeles (USA)
- M. WIDE Tokyo und Seoul, Paris, San Francisco

Quelle: James F. Kurose, Keith W. Ross, Pearson Deutschland GmbH, Computernetzwerke, Der Top-Down-Ansatz, S.165

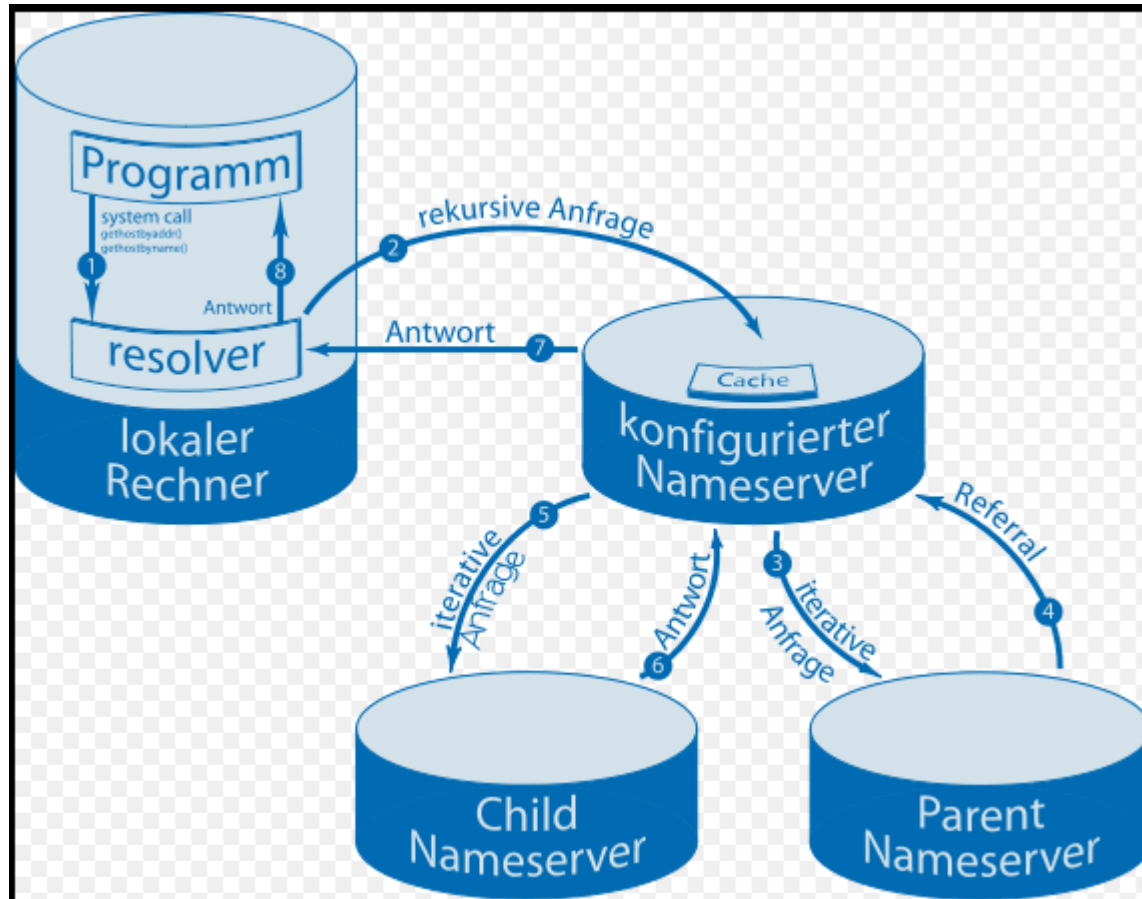
Vergabe Second-Level-Domains (SLD)

- Die Vergabe von SLD übernehmen Registrierungsfirmen
- Zum Beispiel wird .ch und .li in der Schweiz durch die Registrare vergeben (nic.ch)
 - Dort werden dann auch die DNS-Server für die eigene Domäne eingetragen (mind. 2)

Wichtiges zu DNS

Bezeichnung	Kurzbeschreibung
FQDN – Fully Qualified Domain Name z.B. www.google.ch	<ul style="list-style-type: none">• Absolute eindeutige Adresse
Resolver (Programm auf lokalem Gerät, zur Anfrage an DNS Server)	<ul style="list-style-type: none">• Es braucht dazu mindestens einen DNS-Server-Eintrag• Iterativ (immer weitergeleitet von Server zu Server, z.B. DNS-Server)• Rekursiv direkte Antwort der IP-Adresse oder Name nächster DNS Server
Ressource Records (RR) DNS-Objekte (Beinhalten die Antwort vom DNS Server) (siehe auch nächstes Slide)	<ul style="list-style-type: none">• Z.B. mit einem Resource Record «A» wird einem DNS-Namen eine IPv4-Adresse zugeordnet• Diese werden in einer Zonendatei gespeichert (z.B. Hosts)

Funktion DNS-Abfrage



<https://www.youtube.com/watch?v=t6aMwtbyEoo>

Die DNS-Datenbank (Zonendatei)

Resource Records Typen	Kurzbeschreibung
SOA	<ul style="list-style-type: none">• Startpunkt der Zone
NS	<ul style="list-style-type: none">• Verknüpfungen der Nameserver der Domain
A	<ul style="list-style-type: none">• Host-Adresse mit IPv4
AAAA	<ul style="list-style-type: none">• Host-Adresse mit IPV6
CNAME	<ul style="list-style-type: none">• Verweis auf einen anderen Namen (Aliase)
MX	<ul style="list-style-type: none">• Mailserver (SMTP)
PTR	<ul style="list-style-type: none">• Reverse Lookup (IP in Hostnamen)• IN-ADDR.ARPA. IPv4, IP6.ARPA. IPv6

Gruppenarbeit

DNS-Abfrage aufzeichnen

- Gruppenarbeit zu zweit:
 - Zeichnet zusammen eine DNS-Abfrage mit Wireshark auf.
 - Wie läuft eine Abfrage ab?
- **Zeit: 10 Minuten**

DNS-Query

DNS-Aufzeichnung mit Wireshark

Filter: **udp** Expression... Clear Apply Save

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
7	0.85197200	192.168.77.45	146.228.101.20	DNS	73	Standard query 0x4833 A api.mywot.com
9	0.87191600	146.228.101.20	192.168.77.45	DNS	89	Standard query response 0x4833 A 83.145.197.2
53	1.04538900	192.168.77.45	146.228.101.20	DNS	83	Standard query 0x5ef6 A secure.informaction.com
56	1.06599500	146.228.101.20	192.168.77.45	DNS	147	Standard query response 0x5ef6 A 82.103.140.42 A 69.195.141.179 A 69.195.141.178 A 82.103.140.40
216	1.51335100	192.168.77.45	146.228.101.20	DNS	76	Standard query 0x0396 A ocsp.godaddy.com
237	1.54406100	146.228.101.20	192.168.77.45	DNS	133	Standard query response 0x0396 CNAME ocsp.godaddy.com.akadns.net A 188.121.36.239
302	1.74905500	192.168.77.45	146.228.101.20	DNS	74	Standard query 0xc07c A www.google.com
304	1.77317700	146.228.101.20	192.168.77.45	DNS	154	Standard query response 0xc07c A 173.194.44.208 A 173.194.44.209 A 173.194.44.210 A 173.194.44.211 A 173.194.44.212
364	1.95225500	192.168.77.45	146.228.101.20	DNS	75	Standard query 0x7150 A plus.google.com
365	1.95258400	192.168.77.45	146.228.101.20	DNS	74	Standard query 0x91e6 A maps.google.ch
366	1.95267300	192.168.77.45	146.228.101.20	DNS	75	Standard query 0x084f A play.google.com
370	1.97353600	146.228.101.20	192.168.77.45	DNS	251	Standard query response 0x7150 A 173.194.35.34 A 173.194.35.32 A 173.194.35.38 A 173.194.35.35 A 173.194.35.36 A 173.194.35.46
371	1.97462300	192.168.77.45	146.228.101.20	DNS	75	Standard query 0xbfe4 A ssl.gstatic.com

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)
- User Datagram Protocol, Src Port: 53850 (53850), Dst Port: domain (53)
- Domain Name System (query)
 - Response in: 21
 - Transaction ID: 0xf1b2
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.google.ch: type A, class IN
 - Name: www.google.ch
 - Type: A (Host address)
 - Class: IN (0x0001)

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 e4 ;.....1...M..
0020 65 14 d2 5a 00 35 00 27 11 f2 f1 b2 01 00 00 01 e..Z.5.....
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6cw ww.goog
0040 65 02 63 68 00 00 01 00 01 ..e.ch....

Frame (frame), 73 bytes Packets: 1652 Displayed: 263 Marked: 0 Profile: Default

DNS-Response

DNS-Aufzeichnung mit Wireshark

The image shows a Wireshark capture of a DNS response packet. The top pane displays a list of network packets, with the selected packet (No. 1) highlighted. The middle pane shows the packet details, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

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
7	0.85197200	192.168.77.45	146.228.101.20	DNS	73	Standard query 0x4833 A api.mywot.com
9	0.87191600	146.228.101.20	192.168.77.45	DNS	89	Standard query response 0x4833 A 83.145.197.2
53	1.04538900	192.168.77.45	146.228.101.20	DNS	83	Standard query 0x5ef6 A secure.information.com
56	1.06599500	146.228.101.20	192.168.77.45	DNS	147	Standard query response 0x5ef6 A 82.103.140.42 A 69.195.141.179 A 69.195.141.178 A 82.103.140.40
216	1.51335100	192.168.77.45	146.228.101.20	DNS	76	Standard query 0x0396 A obsp.godaddy.com
237	1.54406100	146.228.101.20	192.168.77.45	DNS	133	Standard query response 0x0396 CNAME obsp.godaddy.com.akadns.net A 188.121.36.239
302	1.74905500	192.168.77.45	146.228.101.20	DNS	74	Standard query 0xc07c A www.google.com
304	1.77317700	146.228.101.20	192.168.77.45	DNS	154	Standard query response 0xc07c A 173.194.44.208 A 173.194.44.209 A 173.194.44.210 A 173.194.44.211 A 173.194.44.212
364	1.95225500	192.168.77.45	146.228.101.20	DNS	75	Standard query 0x7150 A plus.google.com
365	1.95258400	192.168.77.45	146.228.101.20	DNS	74	Standard query 0x91e6 A maps.google.ch
366	1.95267300	192.168.77.45	146.228.101.20	DNS	75	Standard query 0x084f A play.google.com
370	1.97353600	146.228.101.20	192.168.77.45	DNS	251	Standard query response 0x7150 A 173.194.35.34 A 173.194.35.32 A 173.194.35.38 A 173.194.35.35 A 173.194.35.36 A 173.194.35.46
371	1.97462300	192.168.77.45	146.228.101.20	DNS	75	Standard query 0xbfe4 A ssl.gstatic.com

Packet Details:

- User Datagram Protocol, Src Port: domain (53), Dst Port: 53850 (53850)
- Domain Name System (response)
 - [Request in: 1]
 - [Time: 0.019886000 seconds]
 - Transaction ID: 0xf1b2
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 0
 - Additional RRs: 0
- Queries
 - www.google.ch: type A, class IN
- Answers
 - www.google.ch: type A, class IN, addr 173.194.44.216
 - Name: www.google.ch
 - Type: A (Host address)
 - Class: IN (0x0001)
 - Time to live: 2 minutes, 55 seconds
 - Data length: 4
 - Addr: 173.194.44.216 (173.194.44.216)
 - www.google.ch: type A, class IN, addr 173.194.44.215
 - www.google.ch: type A, class IN, addr 173.194.44.223

Raw Data:

```
0000 10 0b a9 6a 7d d8 00 13 49 fd 7a 80 08 00 45 00  ...]}... I.Z...E...
0010 00 6b 37 2e 00 00 3d 11 40 86 92 e4 65 14 c0 a8  ...k7... @...e...
0020 4d 2d 00 35 d2 5a 00 57 75 3c f1 b2 81 80 00 01  M-.5.Z.W u<.....
0030 00 03 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c  ....w ww.googl
0040 65 02 63 68 00 00 01 00 01 c0 0c 00 01 00 01 00  e.ch...
0050 00 00 af 00 04 ad c2 2c d8 0c 0c 00 01 00 01 00  .....

```

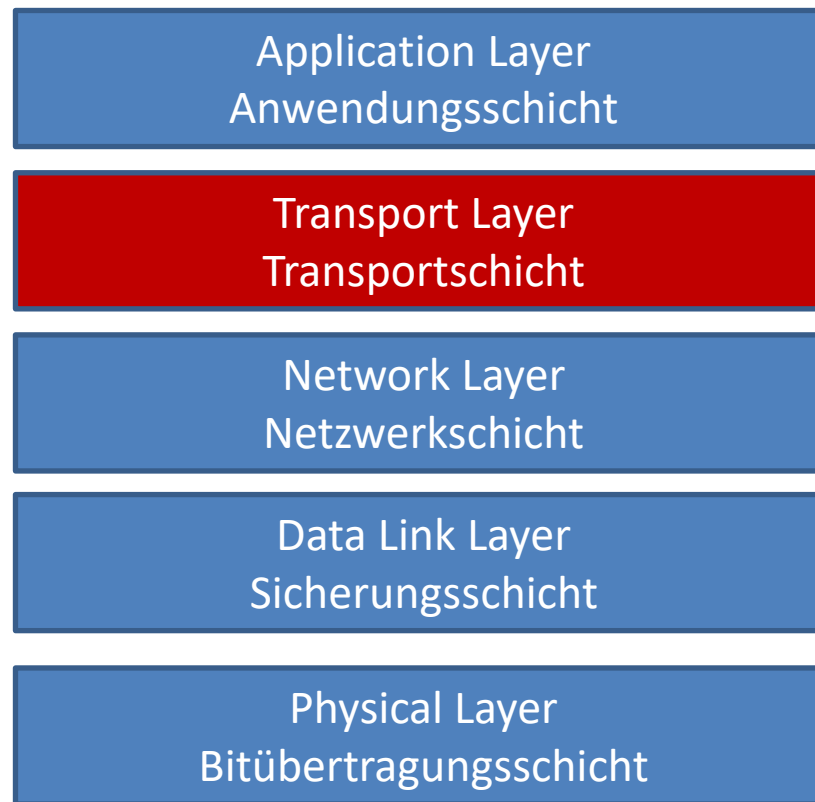

Agenda



«Transportschicht»

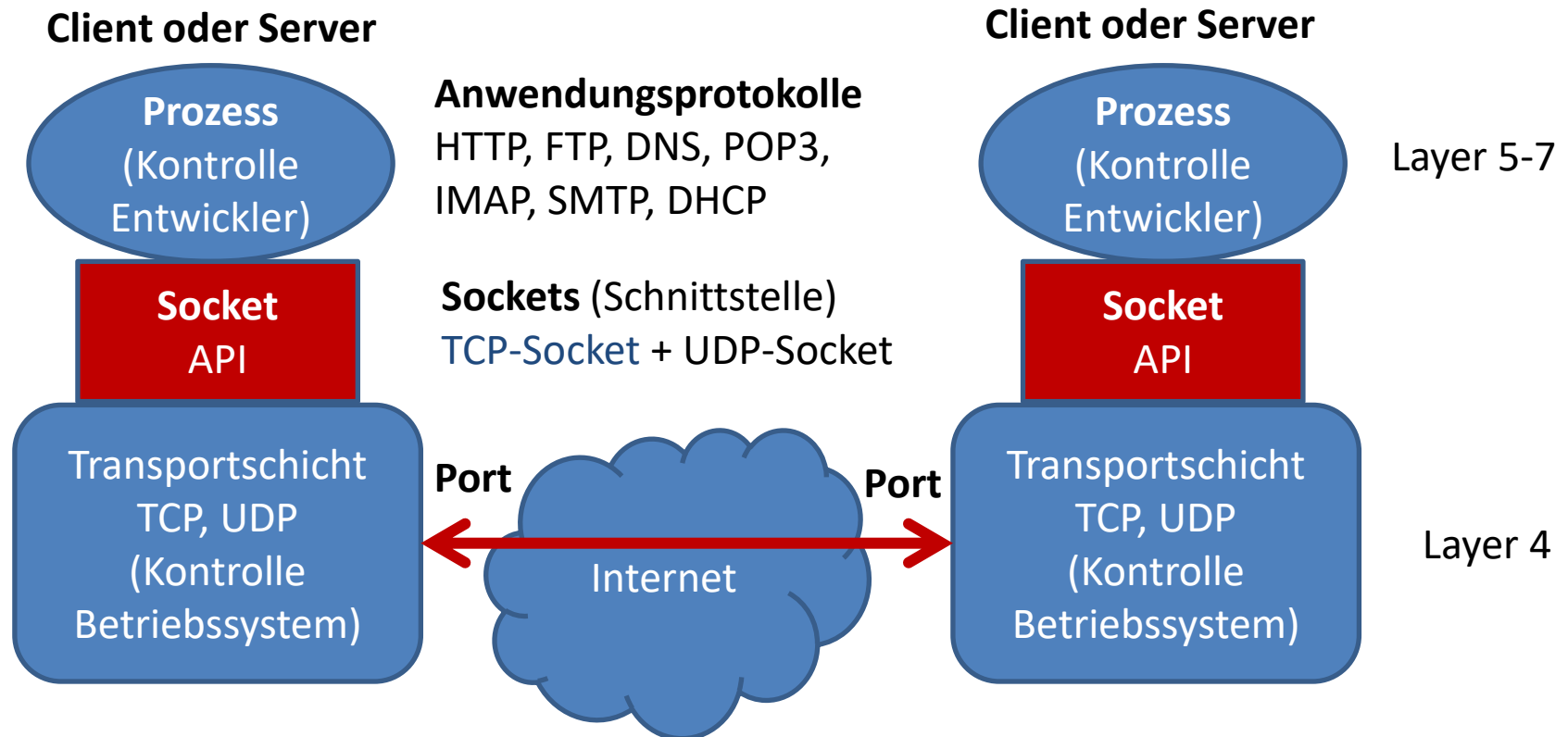
CCNA2 Kapitel 1 «Introduction to TCP/IP Transport and Applications»

Einordnung der Transportschicht



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

Verbindung Anwendung mit Transportschicht (OSI-Layer 4)



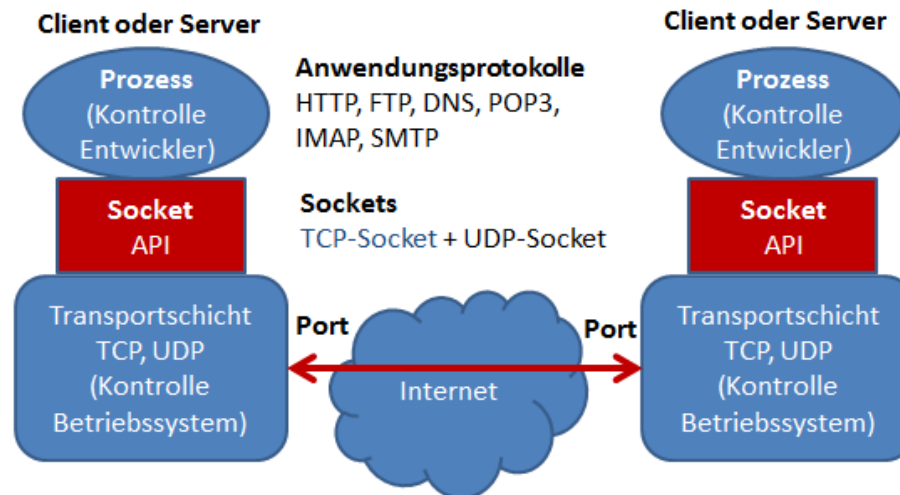
Socket = Port-Nummer + IP-Adresse für eindeutige Zuordnung zu einem Prozess

In Anlehnung an Quelle:

Kurose J. F., Keith W. R., S.193, Computernetzwerke. 5. akt. Auflage. Pearson Deutschland GmbH

Die Transportschicht im Überblick

- Überträgt die Nachrichten der Anwendungsschicht mit TCP oder UDP **zwischen den Endpunkten** der Anwendung
 - Es entsteht eine logische Kommunikation



Unterschiede TCP und UDP

TCP - Transmission Control Protocol	UDP - User Datagram Protocol
Verbindungsorientiert	Verbindungslos
Garantiert Übermittlung	Garantiert Übermittlung nicht
TCP stellt garantierte Übermittlung der Anwendungsschicht bereit	Anwendungen sind für Übermittlung selber verantwortlich
Nur Punkt-zu-Punkt	Punkt-zu-Punkt wie auch Punkt-zu-Multipunkt
Verwendet Ports für die Kommunikation	Verwendet Ports für die Kommunikation
Anwendungsprotokolle über TCP: <ul style="list-style-type: none">- FTP (20 und 21)- HTTP (80)- SMTP (25)- POP3 (110)	Anwendungsprotokolle über UDP: <ul style="list-style-type: none">- DNS (53)- DHCP (67, 68)

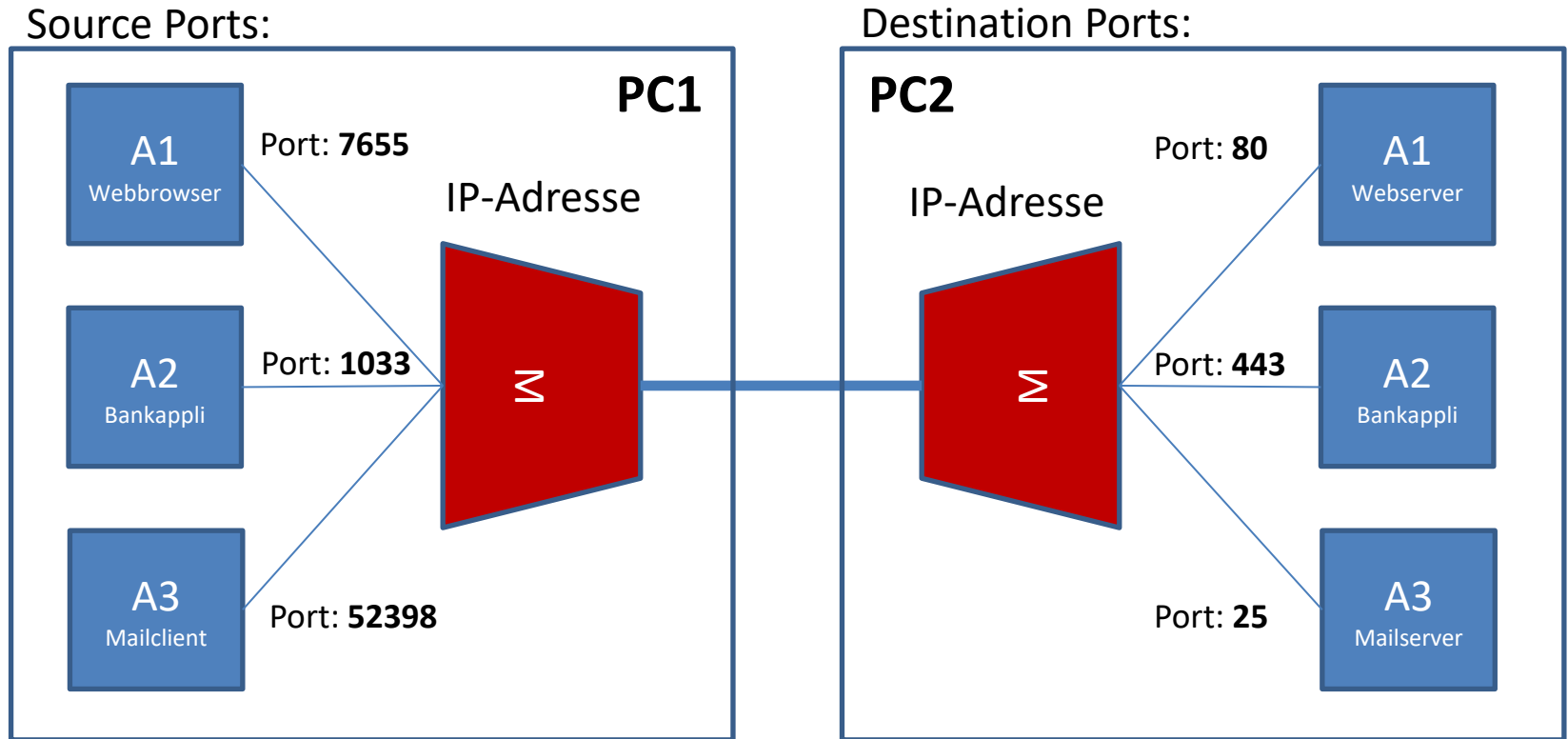
Port-Nummern

Ein Port wird benötigt um den Datenstrom einem Prozess/Programm zuzuordnen

Port-Arten	Port-Nummern
Well-Known-Ports (Sind für Dienste und Anwendungen reserviert)	0 - 1023
Registrierte Ports (Werden Benutzerprozessen oder Benutzeranwendungen zugeordnet)	1024 - 49151
Dynamische oder private Ports (Werden dynamisch Clientanwendungen zugewiesen)	49152 - 65535

Socket = Port-Nummer + IP-Adresse für eindeutige Zuordnung zu einem Prozess

Multiplexing mit Portnummern



Client: In der Regel registrierte oder dynamische-Port Nummern

Server: In der Regel «Well-Known-Port» Nummern

Anmerkung:

Verbindungen können mit dem Befehl **netstat** angezeigt werden (inkl. Port).

*The netstat command is a Command Prompt command used to display very detailed information about how your computer is communicating with other computers or network devices.

Die wichtigsten Anwendungen und deren Ports

1. Teil

Dienstbezeichnung	Protokoll	Ports
Dateifreigabe (Serverdienste)	SMB 2.1 (Win 7 / Win Server 2008 R2) SMB 3.0 (Win 8 / Win Server 2012) SMB 3.1.1 (Win 10 / Win Server 2016)	TCP 445
WWW-Webdienste	HTTP HTTPS (SSL/TLS)	TCP 80 TCP 443
E-Mail-Dienste	SMTP (Mailversand) SMTPS (SSL/TLS) POP3 (Mailempfang) POP3S (SSL/TLS) IMAP (Mailempfang) IMAPS (SSL/TLS)	TCP 25 TCP 465 TCP 110 TCP 995 TCP 143 TCP 993
Namensauflösung	DNS (Domain-Namen in IP-Adressen)	UDP 53
Automatische IP-Vergabe	DHCP (Server oder Relay-Agent) DHCP (Client Anfragen)	UDP 67 UDP 68

Die wichtigsten Anwendungen und deren Ports

2. Teil

Dienstbezeichnung	Protokoll	Ports
Datenübermittlung	FTP (Datenübertragung) FTP (Kontrollport)	TCP 21 TCP 20
Zeitsynchronisierung	NTP (Network Time Protocol)	UDP 123
Verzeichnisdienste	LDAP LDAPS (SSL/TLS)	TCP/UDP 389 TCP/UDP 636
IP-Telefonie VoIP	SIP SIP (SSL/TLS)	UDP 5060 (TCP) TCP 5061
Netzwerkverwaltung	SNMPv3 SNMPv3 (Trap)	UDP 161 UDP 162
VPN Site-to-Site	IPSEC, IKE	UDP 500
Konsolenverbindung (Fernwartung)	SSH (Secure Shell)	TCP 22

User Datagram Protocol

UDP-Header

32 Bit

0-15	16-31
Source Port	Destination Port
Packet Länge	Checksumme

- Unzuverlässig (keine Kontrolle)
- Weniger Overhead als TCP
- UDP überwacht keine Sequenznummern
 - Setzt deshalb Datagramme nicht in der richtigen Reihenfolge zusammen. Anwendung muss dies tun.

UDP-Header

UDP/DNS-Aufzeichnung mit Wireshark

Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)

Filter: ip

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 173.194.44.215 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 > 53613 [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&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)

User Datagram Protocol, Src Port: 53850 (53850), Dst Port: domain (53)

Source port: 53850 (53850)

Destination port: domain (53)

Length: 39

Checksum: 0x11f2 [validation disabled]

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 e4 ;.....1...M...
0020 65 14 d2 5a 00 35 00 27 11 f2 f1 b2 01 00 00 01 e..Z.5.....
0030 00 00 00 00 00 00 03 77 77 06 67 6f 6f 67 6dw ww. googl
0040 65 02 63 68 00 00 01 00 01e.ch.....

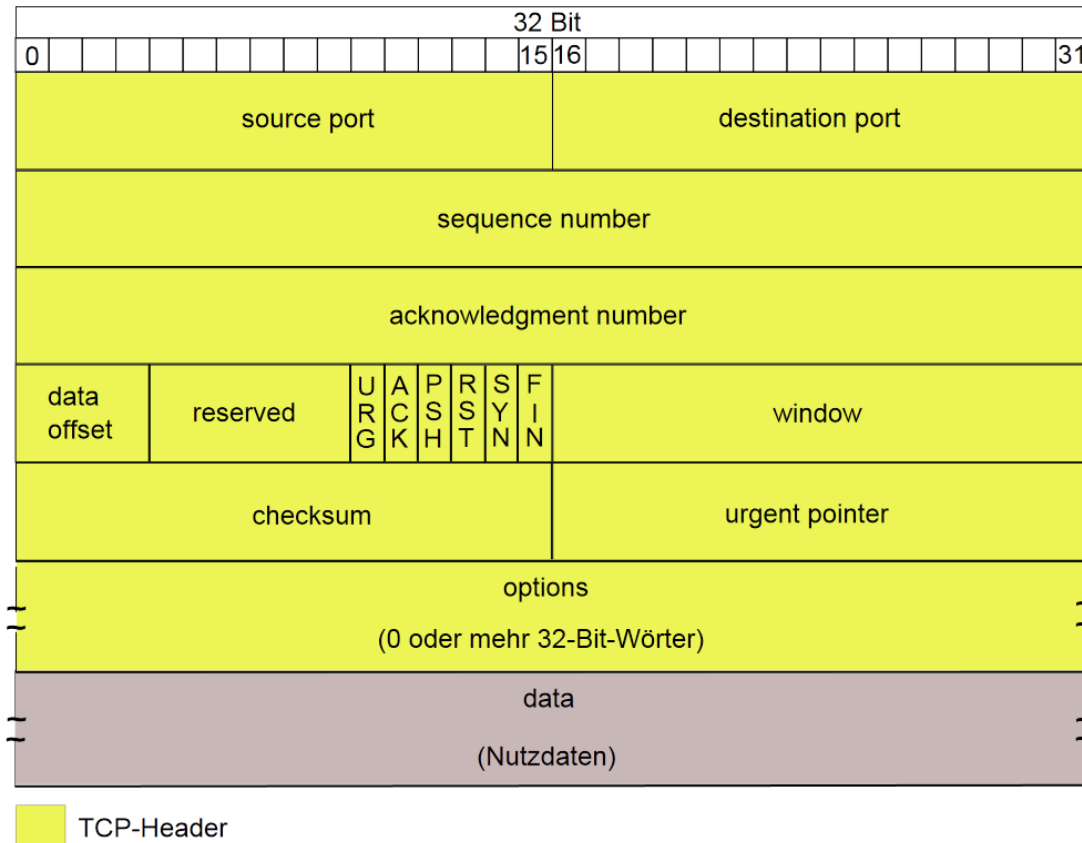
Frame (frame), 73 bytes

Packets: 1491 Displayed: 1457 Marked: 0

Profile: Default

Transmission Control Protocol

TCP-Header



Quelle: Wikipedia.org, Appaloosa, 23:04, 6. Jul. 2007 (CEST)

http://de.wikipedia.org/w/index.php?title=Datei:TCP_Header.svg&filetimestamp=20070706210301

TCP Verbindung aufbauen und gewährleisten (three-way-handshake)

1.

Sende SYN

(SEQ=100, CTL=SYN)

2.

Empfange SYN

Sende SYN-ACK

(SEQ=300, ACK=101,
CTL=SYN, ACK)

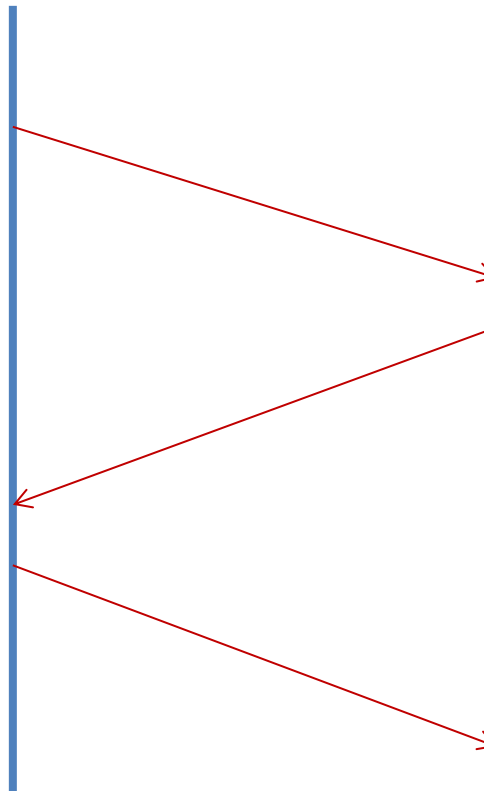
3.

SYN wurde empfangen

Verbindung aufgebaut

Sende ACK

(SEQ=101, ACK=301,
CTL=ACK)



[http://de.wikipedia.org/
wiki/Drei-Wege-
Handschlag](http://de.wikipedia.org/wiki/Drei-Wege-Handschlag)

1. Three-Way-Handshake SYN-Aufzeichnung mit Wireshark

Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8) - Capturing from Microsoft:\Device\NPF\{37FAF8A3-D329-4408-8FE7-FB887A4D8901}

Filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
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
8	0.86517700	192.168.77.45	173.194.44.216	HTTP	370	GET / HTTP/1.1
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-D
15	0.96598700	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
16	0.96827400	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
17	0.96829700	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=317 Ack=2905 win=17424 Len=0
18	0.97023300	173.194.44.216	192.168.77.45	TCP	1122	[TCP segment of a reassembled PDU]
19	0.97269200	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
20	0.97272400	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=317 Ack=5425 win=17424 Len=0

Internet Protocol Version 4, Src: 192.168.77.45 (192.168.77.45), Dst: 173.194.44.216 (173.194.44.216)

Transmission Control Protocol, Src Port: 53611 (53611), Dst Port: http (80), Seq: 0, Len: 0

Source port: 53611 (53611)
Destination port: http (80)
[Stream index: 0]
Sequence number: 0 (relative sequence number)
Header length: 32 bytes

Flags: 0x002 (SYN)

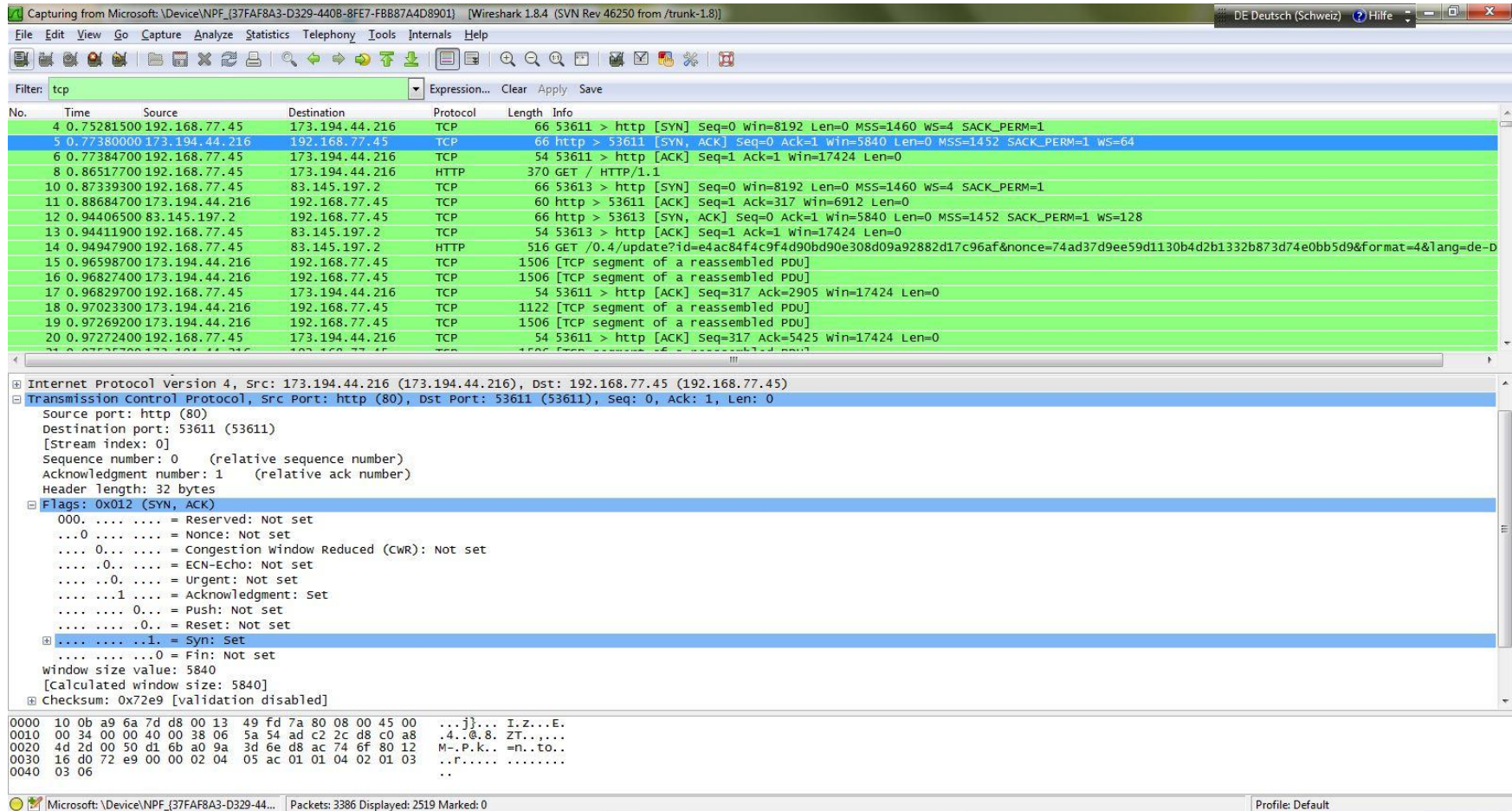
- 000. = Reserved: Not set
- ...0 = Nonce: Not set
- ...0 = Congestion window reduced (CWR): Not set
- ...0 = ECN-Echo: Not set
- ...0 = Urgent: Not set
- ...0 = Acknowledgment: Not set
- ...0 = Push: Not set
- ...0 = Reset: Not set
- ...1 = Syn: Set
- ...0 = Fin: Not set

window size value: 8192
[calculated window size: 8192]
Checksum: 0x47cf [validation disabled]
Options: (12 bytes), Maximum segment size, No-operation (NOP), window scale, No-operation (NOP), No-operation (NOP), SACK permitted

0000 00 13 49 fd 7a 80 10 0b a9 6a 7d d8 08 00 45 00 ...I.Z... }...E.
0010 00 34 03 1d 40 00 00 06 0f 37 c0 a8 4d 2d ad c2 ...4..@... 7..M..
0020 2c d8 d1 6b 00 50 d8 ac 74 6e 00 00 00 00 80 02 ...K.P.. tn.....
0030 20 00 47 cf 00 00 02 04 05 b4 01 03 03 02 01 01 ...G.....
0040 04 02

Frame (frame), 66 bytes
Packets: 3379 Displayed: 2519 Marked: 0
Profile: Default

2. Three-Way-Handshake SYN-Aufzeichnung mit Wireshark



3. Three-Way-Handshake ACK-Aufzeichnung mit Wireshark

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (No. 54), which is an ACK packet from 192.168.77.45 to 173.194.44.216. The third pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
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
8	0.86517700	192.168.77.45	173.194.44.216	HTTP	370	GET / HTTP/1.1
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-D
15	0.96598700	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
16	0.96827400	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
17	0.96829700	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=317 Ack=2905 Win=17424 Len=0
18	0.97023300	173.194.44.216	192.168.77.45	TCP	1122	[TCP segment of a reassembled PDU]
19	0.97269200	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
20	0.97272400	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=317 Ack=5425 Win=17424 Len=0

Internet Protocol Version 4, Src: 192.168.77.45 (192.168.77.45), Dst: 173.194.44.216 (173.194.44.216)

Transmission Control Protocol, Src Port: 53611 (53611), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

Source port: 53611 (53611)
Destination port: http (80)
[Stream index: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header length: 20 bytes

Flags: 0x010 (ACK)

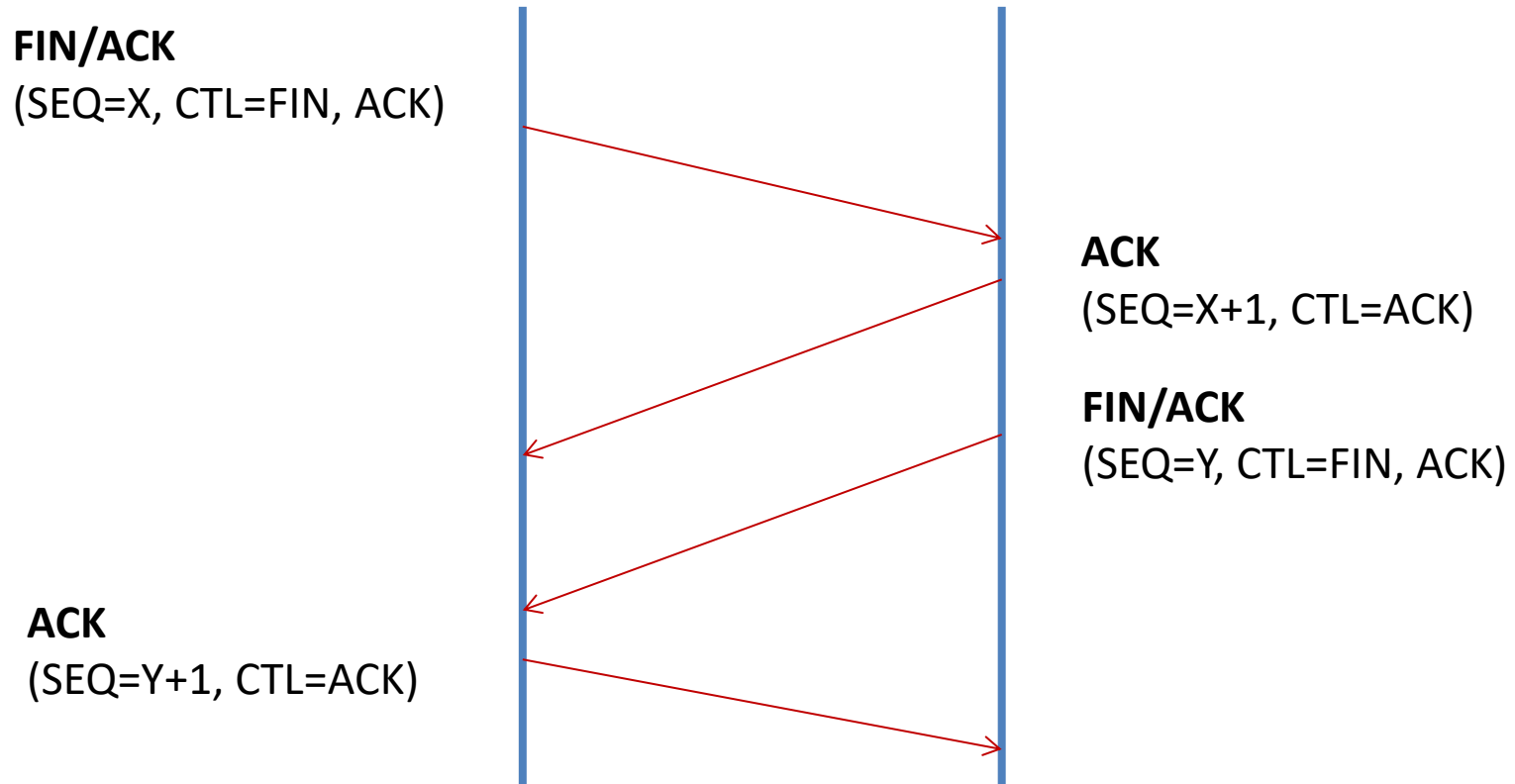
- 000. = Reserved: Not set
- ...0 = Nonce: Not set
- 0... = Congestion Window Reduced (CWR): Not set
- 0... = ECN-Echo: Not set
- 0... = Urgent: Not set
- 1... = Acknowledgment: Set
- 0... = Push: Not set
- 0... = Reset: Not set
- 0... = Syn: Not set
- 0... = Fin: Not set

Window size value: 4356
[calculated window size: 17424]
[window size scaling factor: 4]

0000 00 13 49 fd 7a 80 10 0b a9 6a 7d d8 08 00 45 00 ..I.Z...j}...E.
0010 00 28 03 1e 40 00 80 06 0f 42 c0 a8 4d 2d ad c2 .(.@...B.M-..
0020 2c d8 d1 6b 00 50 d8 ac 74 6f a0 9a 3d 6f 50 10 ...k.P..to..=OP.
0030 11 04 b9 7e 00 00

TCP Verbindung abbauen

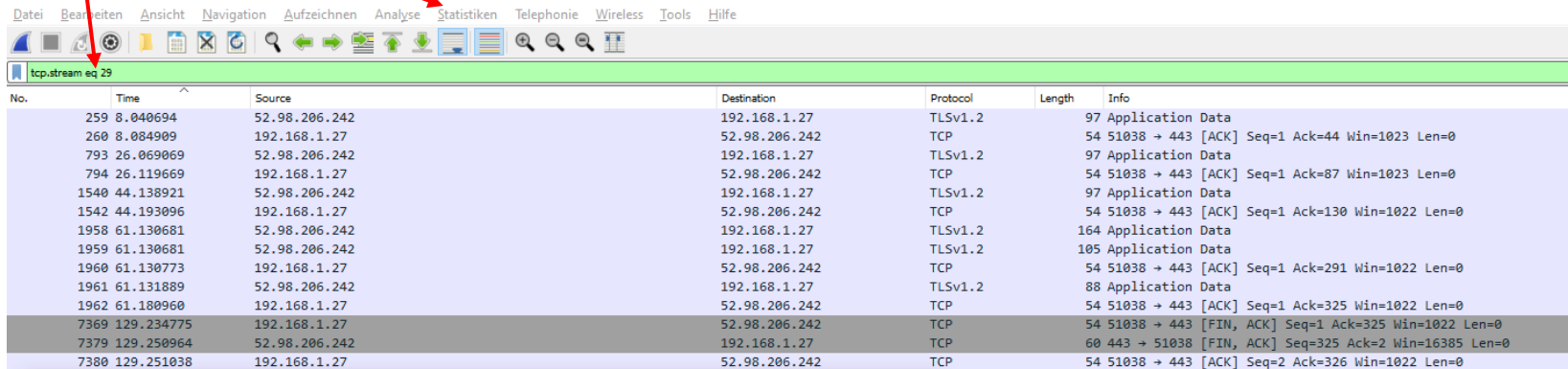
TCP teardown process (ordentlich)



Filter setzen oder
rechte Maustaste
auf TCP-Paket und
Folgen - TCP Stream

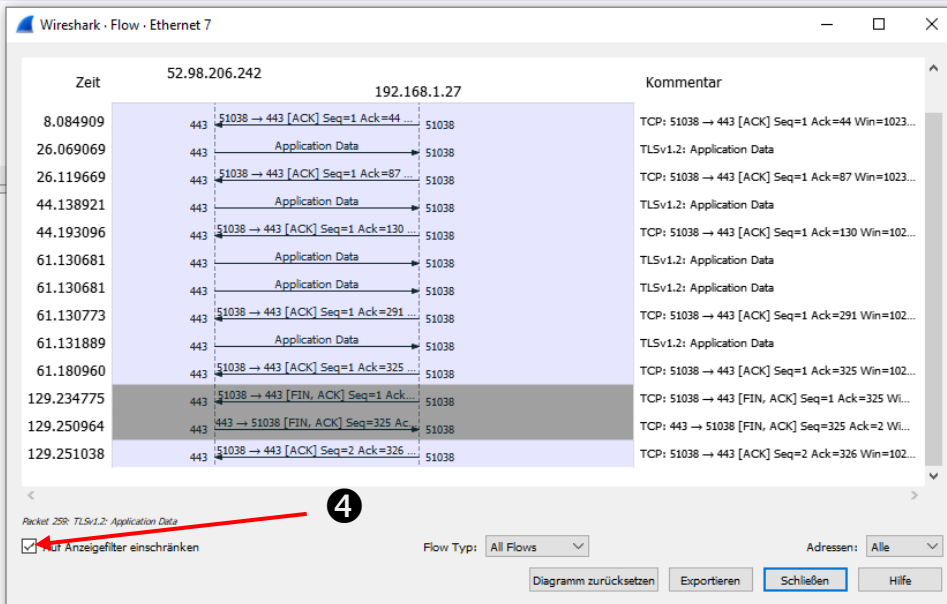
TCP teardown process (ordentlich)

Aufzeichnung mit Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
259	8.040694	52.98.206.242	192.168.1.27	TLSv1.2	97	Application Data
260	8.084909	192.168.1.27	52.98.206.242	TCP	54	51038 → 443 [ACK] Seq=1 Ack=44 Win=1023 Len=0
793	26.069069	52.98.206.242	192.168.1.27	TLSv1.2	97	Application Data
794	26.119669	192.168.1.27	52.98.206.242	TCP	54	51038 → 443 [ACK] Seq=1 Ack=87 Win=1023 Len=0
1540	44.138921	52.98.206.242	192.168.1.27	TLSv1.2	97	Application Data
1542	44.193096	192.168.1.27	52.98.206.242	TCP	54	51038 → 443 [ACK] Seq=1 Ack=130 Win=1022 Len=0
1958	61.130681	52.98.206.242	192.168.1.27	TLSv1.2	164	Application Data
1959	61.130681	52.98.206.242	192.168.1.27	TLSv1.2	105	Application Data
1960	61.130773	192.168.1.27	52.98.206.242	TCP	54	51038 → 443 [ACK] Seq=1 Ack=291 Win=1022 Len=0
1961	61.131889	52.98.206.242	192.168.1.27	TLSv1.2	88	Application Data
1962	61.180960	192.168.1.27	52.98.206.242	TCP	54	51038 → 443 [ACK] Seq=1 Ack=325 Win=1022 Len=0
7369	129.234775	192.168.1.27	52.98.206.242	TCP	54	51038 → 443 [FIN, ACK] Seq=1 Ack=325 Win=1022 Len=0
7379	129.250964	52.98.206.242	192.168.1.27	TCP	60	443 → 51038 [FIN, ACK] Seq=325 Ack=2 Win=16385 Len=0
7380	129.251038	192.168.1.27	52.98.206.242	TCP	54	51038 → 443 [ACK] Seq=2 Ack=326 Win=1022 Len=0

③ Flow Graph auswählen



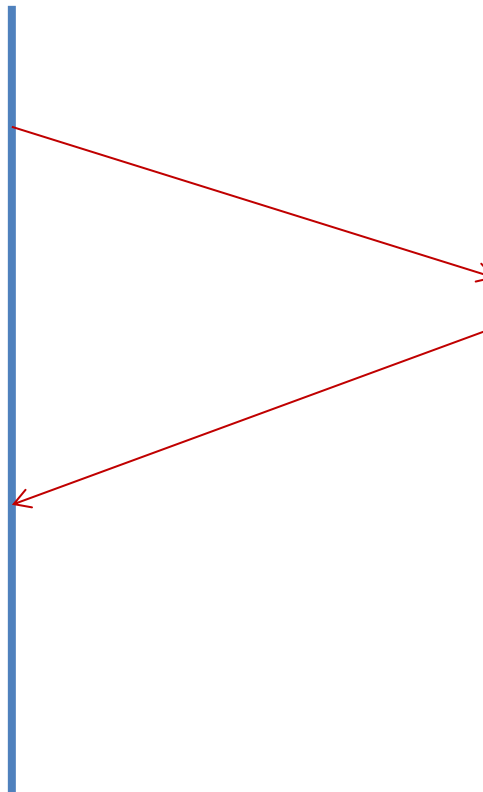
TCP Verbindung abbrechen

Reset / RST-Flag

SYN
(SEQ=X, CTL=SYN)

RST/ACK
(SEQ=X+1, CTL=RST, ACK)

Verbindung ist beendet



CTL Werte (Flags)

CTL-Wert	Beschreibung
URG	Urgent, dringend (selten gebraucht)
ACK	Acknowledgement (Bestätigung des TCP-Segment Empfangs)
PSH	Push (kleinere Segemente werden gesandt, vorher und nachher gepuffert)
RST	Reset (Abbruch der Verbindung, Probleme oder Abweisung)
SYN	Synchronize (Synchronisation von Sequenznummern)
FIN	Finish (Schlussflag, keine Daten kommen mehr)

Nützliches zu TCP ist auf Wikipedia.org zu finden.

http://de.wikipedia.org/wiki/Transmission_Control_Protocol

TCP-Header

TCP/HTTP-Aufzeichnung mit Wireshark

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (Frame 8), and the bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
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
8	0.86517700	192.168.77.45	173.194.44.216	HTTP	370	GET / HTTP/1.1
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-D
15	0.96598700	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
16	0.96827400	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
17	0.96829700	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=317 Ack=2905 win=17424 Len=0
18	0.97023300	173.194.44.216	192.168.77.45	TCP	1122	[TCP segment of a reassembled PDU]
19	0.97269200	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
20	0.97272400	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=317 Ack=5425 win=17424 Len=0

Packet Details (Frame 8):

- Frame 8: 370 bytes on wire (2960 bits), 370 bytes captured (2960 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: 173.194.44.216 (173.194.44.216)
- Transmission Control Protocol, Src Port: 53611 (53611), Dst Port: http (80), Seq: 1, Ack: 1, Len: 316
 - Source port: 53611 (53611)
 - Destination port: http (80)
 - [Stream index: 0]
 - Sequence number: 1 (relative sequence number)
 - [Next sequence number: 317 (relative sequence number)]
 - Acknowledgment number: 1 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x018 (PSH, ACK)
 - Window size value: 4356
 - [Calculated window size: 17424]
 - [Window size scaling factor: 4]
 - checksum: 0xb8e7 [validation disabled]
 - [SEQ/ACK analysis]
 - [Bytes in flight: 316]
- Hypertext Transfer Protocol

Raw Data:

```
0000 00 13 49 fd 7a 80 10 0b a9 6a 7d d8 08 00 45 00 ..I.Z... .j}...E.
0010 01 64 03 20 40 00 80 06 0e 04 c0 a8 4d 2d ad c2 .d.@... ....M-..
0020 2c d8 d1 6b 00 50 d8 ac 74 6f a0 9a 3d 6f 50 18 ...k.P... to...=OP.
0030 11 04 b8 e7 00 00 74 54 20 2f 20 48 94 54 50 ....GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www.
0050 67 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f 6f google.c h..user-
```

Datenflusssteuerung

TCP Receive Window-Size (Empfangsfenster)

- Mit der Window-Size ist TCP in der Lage mehrere Pakete zu senden ohne bei jedem versandten Paket die Bestätigung ACK abwarten zu müssen.
- Dazu wird eine Window-Size, also ein Empfangsfenster bestimmt.
- Dies ist dann auch das Maximum, welches ohne Empfangsbestätigung ACK gesandt werden kann.
- So ist sichergestellt, dass der Empfangsspeicher (Puffer) nicht überläuft.

netstat in Linux

LAB>_

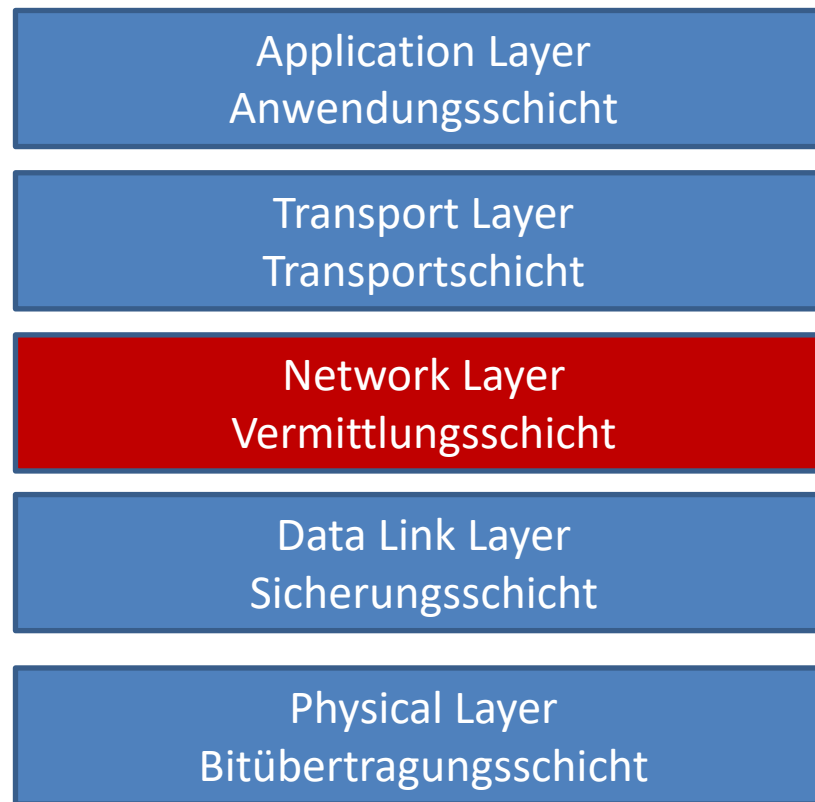
Mit NESTAT laufende Sessions anzeigen:

```
# netstat -an (Zeigt alle Sockets an)
# netstat -tan (Zeigt aktive Verbindungen an)
# netstat -anep (Alles mit Benutzern und Prozess-IDs)
# netstat -an | grep ":80" (Nur Sessions auf Port 80)
# netstat -r (Zeigt die Routingtable an)
# netstat -i (Zeigt Paketstatistik der Interfaces an)
# netstat -s (Zeigt Statistik an)
# netstat -at (Nur alle TCP)
# netstat -au (Nur alle UDP)
```

Agenda

«Vermittlungsschicht»

Einordnung der Vermittlungsschicht



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

Aufgaben der Netzwerkschicht

OSI-Vermittlungsschicht

- Übernimmt Segmente der Transportschicht
- Fügt IP-Header der PDU zu (Die zu transportierenden Nachrichten werden Transport **P**rotocol **D**ata **U**nits genannt)
- Stellt Host zu Host Verbindung her
 - Source- und Destination-Adresse
- Leitet die Pakete ins Ziernetzwerk weiter (Routing → Layer 3)
- Die Netzwerkschicht (IP → Layer 3) ist verbindungslos und ungesichert, dies übernimmt die Transport-schicht (TCP) → Layer 4

Grundlagen IPv4

- IPv4 Paket Header

32 Bit

0–3	4–7	8–13	14–15	16–18	19–23	24–27	28–31
Version	IHL	DSCP	ECN	Gesamtlänge			
Identifikation				Flags	Fragment Offset		
TTL		Protokoll		Header-Prüfsumme			
Quell-IP-Adresse							
Ziel-IP-Adresse							
evtl. Optionen ...							

Version = V4/V6 IHL= IP Header Length DSCP/ECN = Priorisierung (vorher TOS)
Paketlänge = gesamtes Paket inkl. Kopfdaten Kennung = Fragmente erkennen
Flags = 0,1,2 Fragmentierung Kontroll-Schalter Fragmentoffset = Aufteilung
TTL = Lebensdauer des Pakets (Anzahl Hops, Max. 255) **Protokoll = Folgeprotokoll (TCP/UDP)**
Header Checksumme = sichert Header Optionen/Füllbits = Zusatzinfos

<https://de.wikipedia.org/wiki/IPv4>

Selber aufzeichnen / IPv4-Header IPv4-Aufzeichnung mit Wireshark

Capturing from Microsoft:\Device\NPF_{37FAF8A3-D329-440B-8FE7-FB887A4D8901} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip Expression... Clear Apply Save

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: 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)

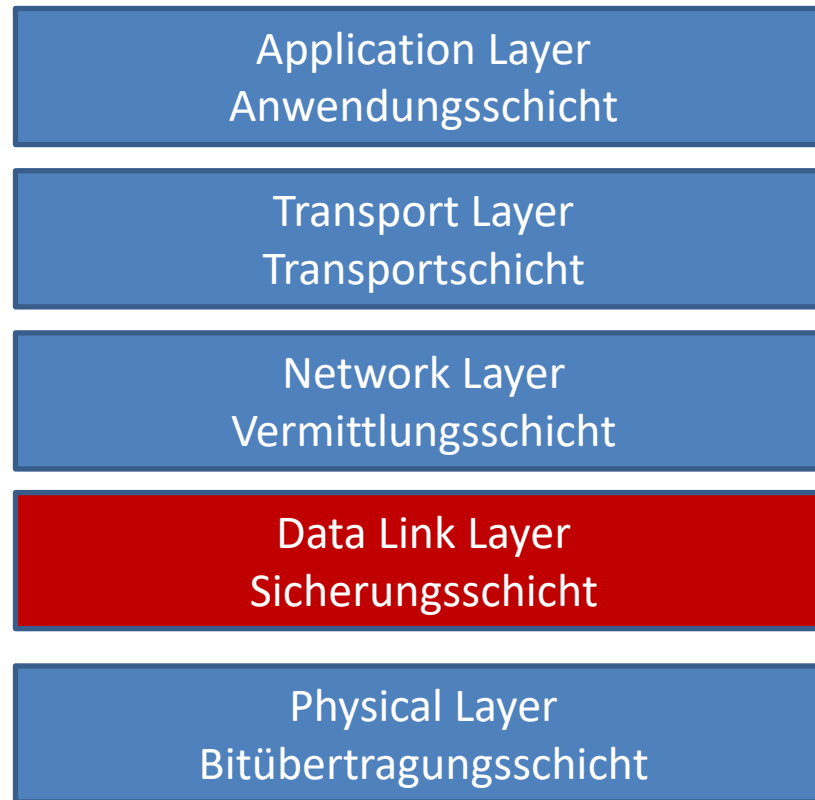
0000	00 13 49 fd 7a 80 10 0b	a9 6a 7d d8 08 00 45 00	..I.Z...j}...E.
0010	00 3b 03 1c 00 00 80 11	31 c8 c0 a8 4d 2d 92 e4	.;.....1..M...
0020	65 14 d2 5a 00 35 00 27	11 f2 f1 b2 01 00 00 01	e..Z.5.'
0030	00 00 00 00 00 00 03 77	77 77 06 67 6f 6f 67 6cw ww.googl
0040	65 02 63 68 00 00 01 00	01	e.ch....

Microsoft:\Device\NPF_{37FAF8A3-D329-44... Packets: 717 Displayed: 709 Marked: 0 Profile: Default

Agenda

«Sicherungsschicht»

Einordnung der Sicherungsschicht

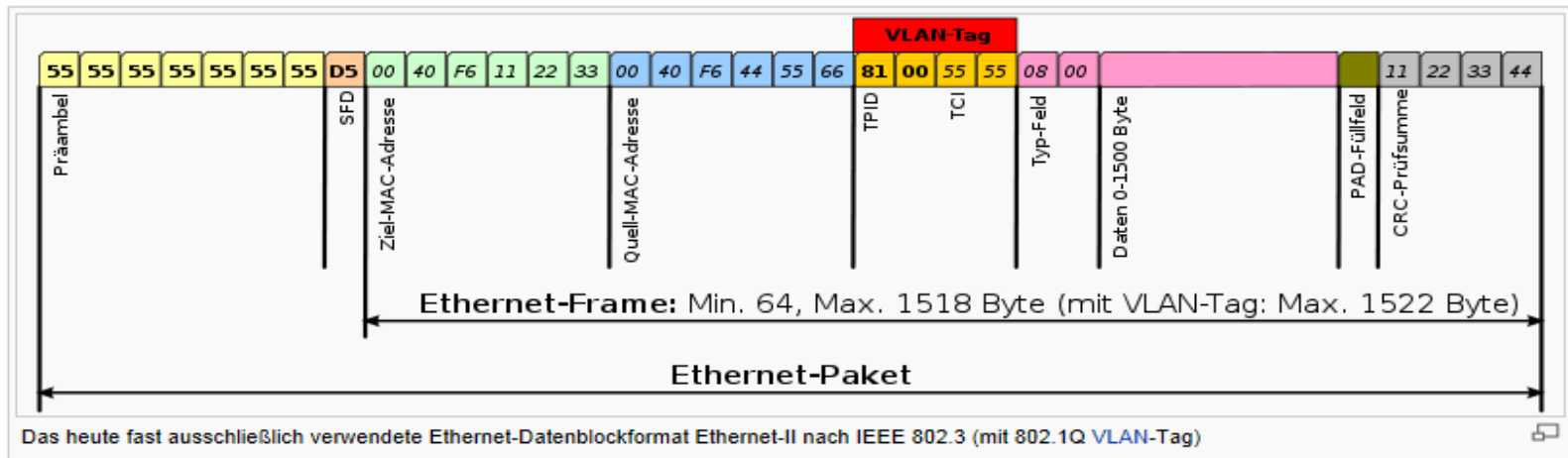


TCP/IP					
OSI-Schicht	Einordnung	DoD-Schicht	Protokollbeispiel	Einheiten	
7	Anwendungen (Application)	Anwendungsorientiert	Anwendung	HTTP FTP HTTPS SMTP LDAP NCP	Daten
6	Darstellung (Presentation)				
5	Sitzung (Session)				
4	Transport (Transport)	Transportorientiert	Transport	TCP UDP SCTP SPX	TCP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

Grundlagen ICT

Beispiel Ethernet Frame

- Frames (Ethernet **IEEE 802.3**) Header-Länge = 18 Bytes



- Präambel / Start Frame Delimiter (aus Kompatibilitätsgründen, diene der Synchronisation)
- 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
- CRC Prüfsumme

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)

Deine Hausaufgaben

Stoff Nachbearbeitung 3. Modul:

- Repetition der Folieninhalte des Modulblocks: Ergänzen deiner individuellen Zusammenfassung.
- Lernstoff Vertiefung:
 - CCNA2 Kapitel 1 «Introduction to TCP/IP Transport and Applications»
 - «https://de.wikipedia.org/wiki/Transmission_Control_Protocol»
 - «https://de.wikipedia.org/wiki/User_Datagram_Protocol»
 - «https://de.wikipedia.org/wiki/Domain_Name_System»
 - Network Academy: <https://www.netacad.com/portal> Cisco NetAcademy Kapitel 9 und 10
- Analysiere die DNS-Zone der Domain deiner Firma mittels dig und beantworte die nachfolgenden Fragen. Bringe die Ergebnisse und die genutzten Befehlszeilen deiner Analyse zur Besprechung in den Unterricht mit:
 - Wie lautet der A-Record Eintrag?
 - Wie lautet der AAAA-Record Eintrag für IPv6?
 - Mit welchen dig Optionen kannst du direkt nur die IP-Adresse des A-Record als Ausgabe anzeigen?
 - Hat es für den A-Record einen «in-addr.arpa» Eintrag?
 - Wie lauten die MX-Einträge?
 - Welche IP-Adressen sind im MX enthalten?
 - Ist ein SPF-Eintrag gesetzt?
 - Welche TXT-Einträge sind in der Zone enthalten?
 - Ist ein DMARC-Eintrag gesetzt?
 - Wird DNSSEC verwendet?
- Vorbereitung auf das nächste Modul:
 - CCNA1 Buch Kapitel 11 «Perspectives on IPv4 Subnetting»