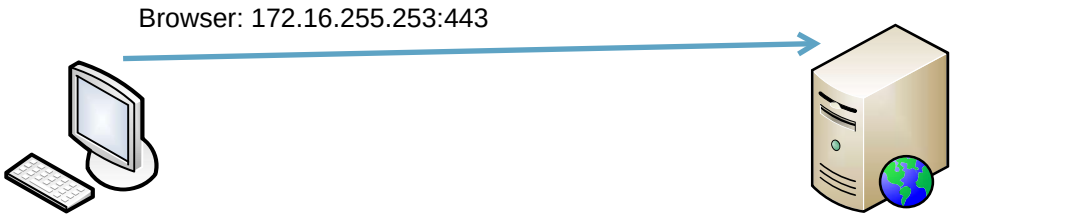
5. TCP/IP intensiv

Betrachten Sie zunächst den folgenden Fall – ein Client möchte im Intranet die Verbindung zu einem Webserver aufbauen, um sich Informationen über den Speiseplan für die nächste Woche abzurufen:



Client
IP: 172.16.0.1
SN: 255.255.0.0
GW: 172.16.255.254

Webserver
IP: 172.16.255.253/16
SN:
GW: 172.16.255.254

a) Welche IP-Adressen vergeben Sie?

b) Welche Anwendung benutzt der Client? Welche Anwendung läuft auf dem Server?

Client: Firefox, Chrome

Server: Apache, NGinx

c) Nehmen wir an, Sie könnten festlegen, welche Informationen im Datenverkehr zwischen Client und Server ausgetauscht werden sollen.

speiseplan.html

Welche Informationen würden Sie außer den Nutzdaten zwischen Client und Server über das Netz austauschen, um die Kommunikation zu ermöglichen?

Q-IP, Z-IP, Ziel-Port, Quell-Port

Größe der zu übertragenden Daten

Sequenznummer

d) Beim Aufbau einer Verbindung zwischen einem Client in unserem Schulnetz (10.0.0.0/8) und dem Webserver de.wikipedia.org (91.198.174.2) wurde folgendes IP-Paket mitgeschnitten:

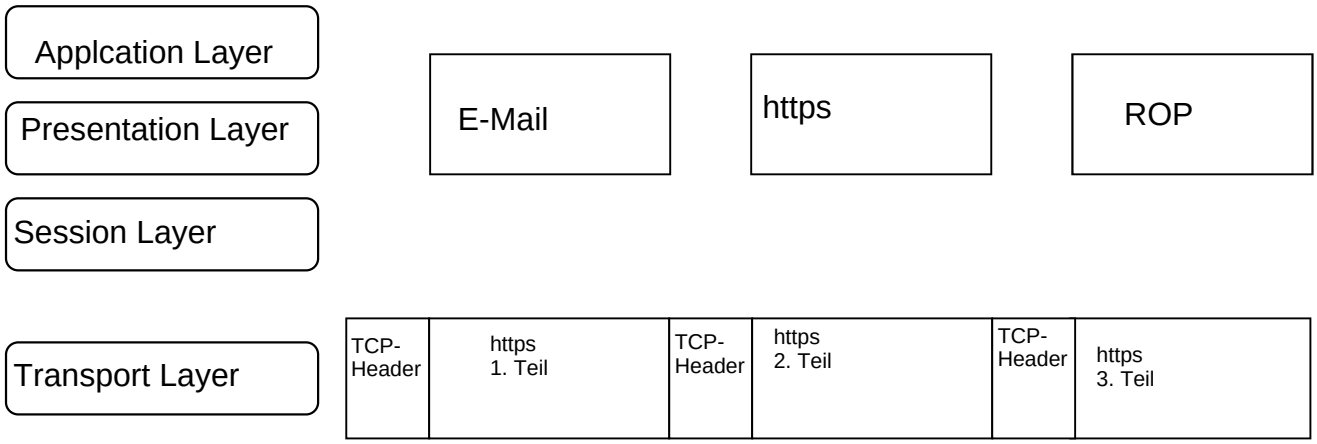
45	00	00	30	IP v4, Header Length: 5* 32 Bit zeilen, importance: 0 Größe: 48 Byte	
2e	8f	40	00	identification: 11.919,	Flags: 2
80	06	00	00	available hops: 128 protocol: TCP,	Prüfsumme: 0
0a	a1	0b	14	source IP: 10.161.11.20	
5b	c6	ae	02	Destination IP: 91.198.174.2	

Welche Informationen sind wohl in diesem Paket enthalten? Versuchen Sie die Zeilen 4 und 5 zu entschlüsseln!

0	4	8	15	16	24	31
VERSION	HLEN	Service Type		Total Length		
Identification				Flags	Fragment Offset	
Time-To-Live		Protocol		Header Checksum		
Source IP-Address						
Destination IP-Address						
IP Options						Padding
Data						
…						

VERSION	Dieses Feld gibt das Format des IP-Paket-Headers an. Dieses 4-Bit-Feld enthält die Zahl 4, wenn es sich um ein IPv4-Paket handelt, oder 6, wenn es sich um ein IPv6-Paket handelt.
HLEN	Dieses Feld zeigt die Länge des Datagramm-Headers in 32-Bit-Wörtern an.
Service Type	Dieses Feld enthält 8 Bits, welche die Wichtigkeitsstufe angeben, die von dem Protokoll einer bestimmten höheren Schicht zugewiesen wurde.
Total Length	Dieses Feld enthält 16 Bits, welche die Länge des gesamten Pakets in Bytes angeben. Darin sind die Daten und der Header inbegriffen.
Identification	Dieses Feld enthält 16 Bits, welche das aktuelle Datagramm bezeichnen. Dabei handelt es sich um die Sequenznummer.
Flags	Steuerung der Fragmentierung
Fragment Offset	Dieses 13-Bit-Feld dient der Zusammensetzung der Datagramm-Fragmente
Time-To-Live (tatsächlich mit „v“!)	Dieses Feld gibt die Anzahl der Hops an, die ein Paket passieren kann. Diese Zahl wird um eins verringert, wenn das Paket einen Router passiert. Wenn der Zähler null erreicht, wird das Paket verworfen. Dadurch wird verhindert, dass Pakete endlos Schleifen durchlaufen
Protocol	Die 8 Bits in diesem Feld zeigen an, welches höhere Protokoll (wie z. B. TCP oder UDP) ankommende Pakete empfängt, nachdem die IP-Verarbeitung abgeschlossen ist
Header Checksum	Prüfsumme über den ganzen IP-Header
Source IP-Address	Quell-IP-Adresse
Destination IP-Address	Ziel-IP-Adresse
IP Options	Zusatzinformationen für das Paket. Die einzelnen Optionen selbst können unterschiedliche Länge haben, es gibt sowohl Optionen fester Länge als auch Optionen mit variabler Länge.
Padding	In diesem Feld werden zusätzliche Nullen hinzugefügt, um sicherzustellen, dass die Länge des IP-Headers stets ein Vielfaches von 32 Bits beträgt.

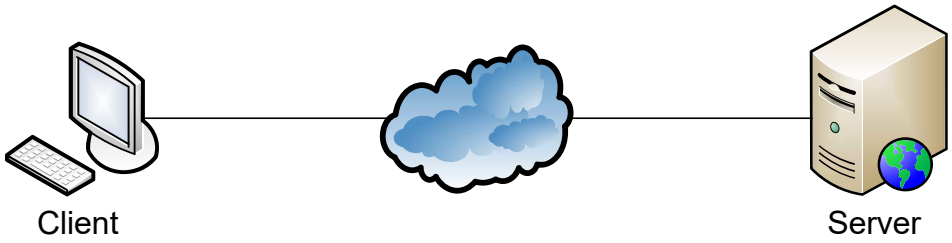
5.1 Layer 4: allgemeine Aufgaben der Transportschicht

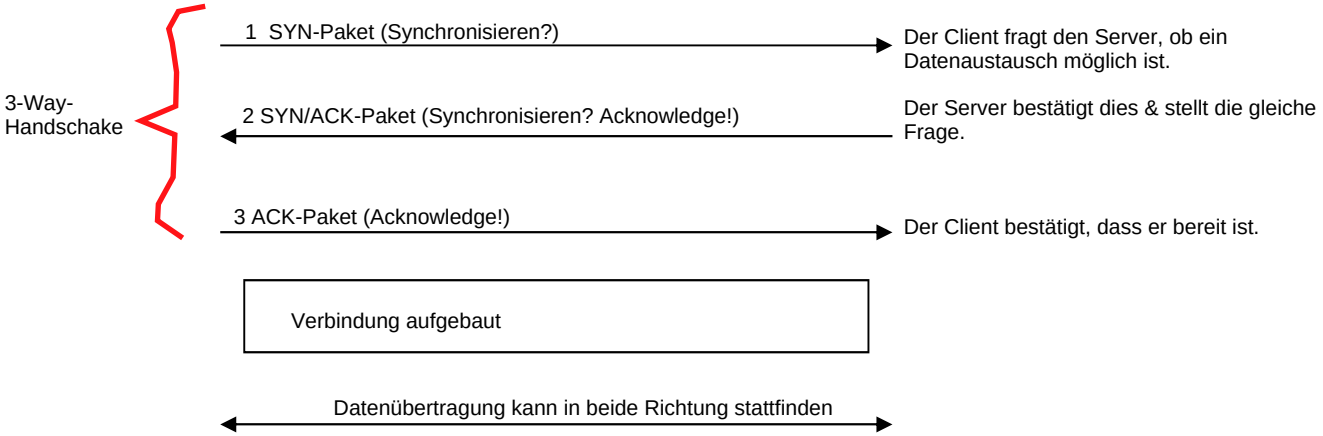


Die Transport-Layer stellt der Anwendung bzw. schicht 5-7 über die Port nummer eine einheitliche Zugriffsmöglichkeit aus dem Netz zur Verfügung. Die Anwendung muss die Eigenschaften des Netzes nicht berücksichtigen.

TCP ist ein verbindungsorientiertes Protokoll → Alle Pakete kommen beim Empfänger an, es gibt keine Dublikate

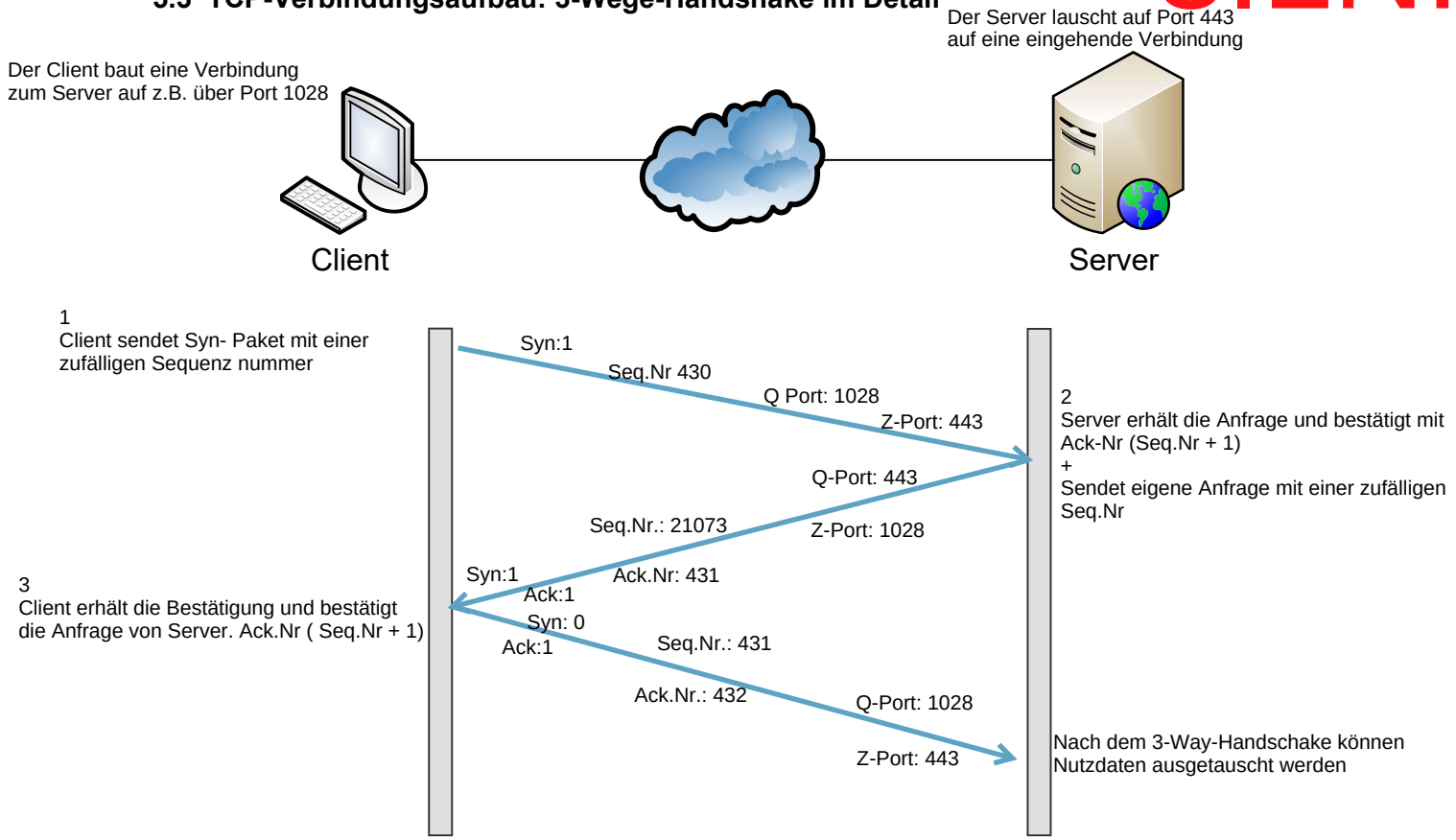
5.2 Layer 4: TCP-Protokoll - Verbindungsaufbau



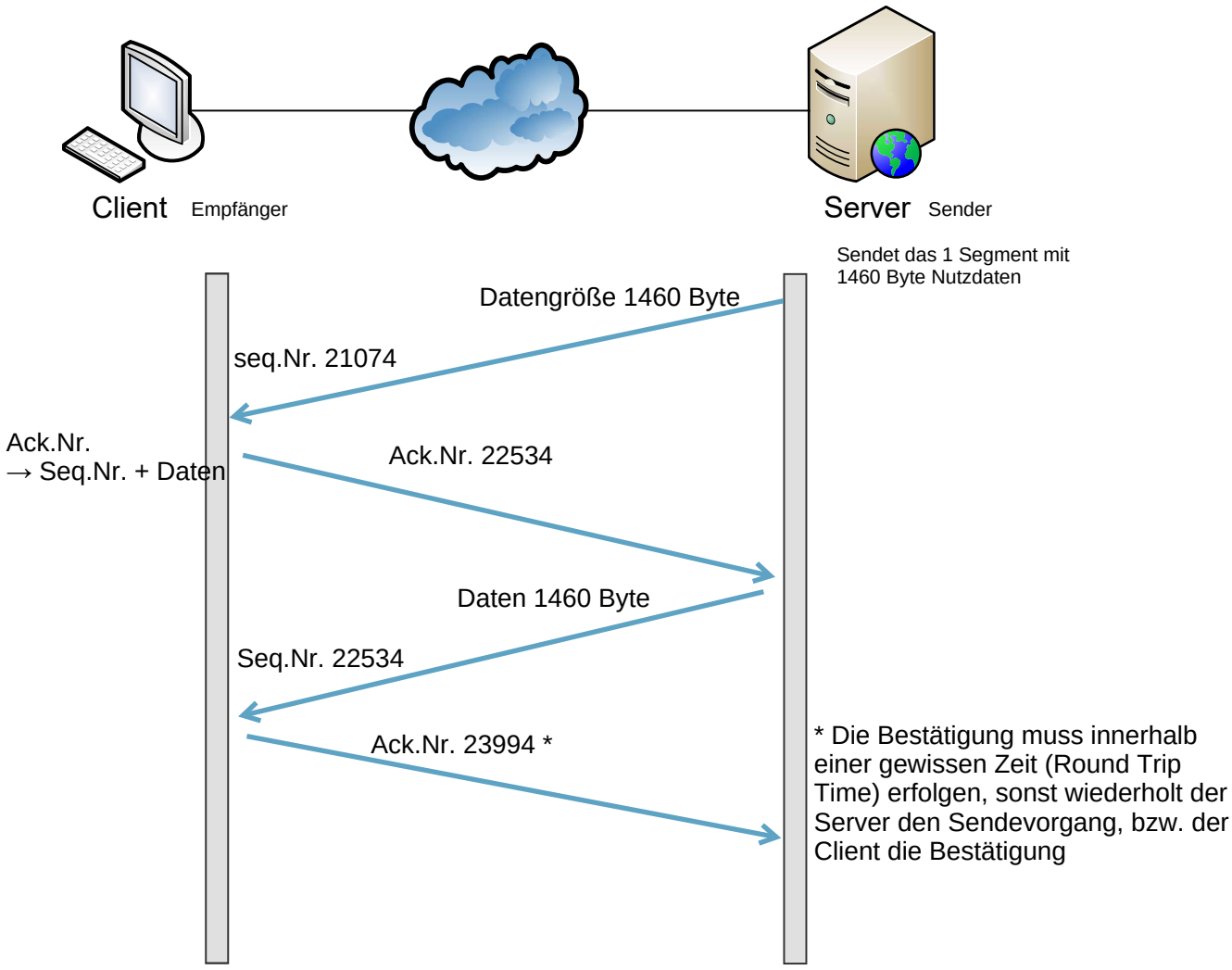


3.LN!

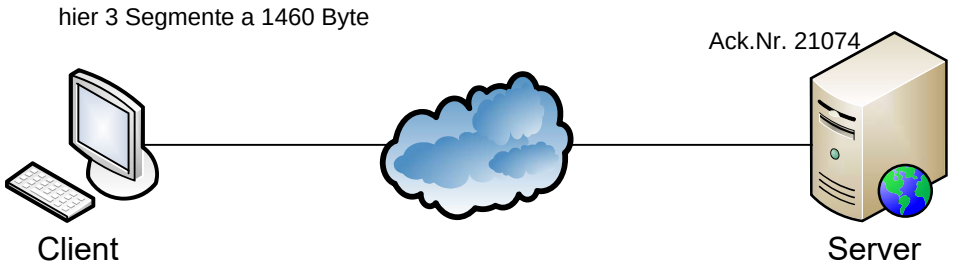
5.3 TCP-Verbindungsaufbau: 3-Wege-Handshake im Detail

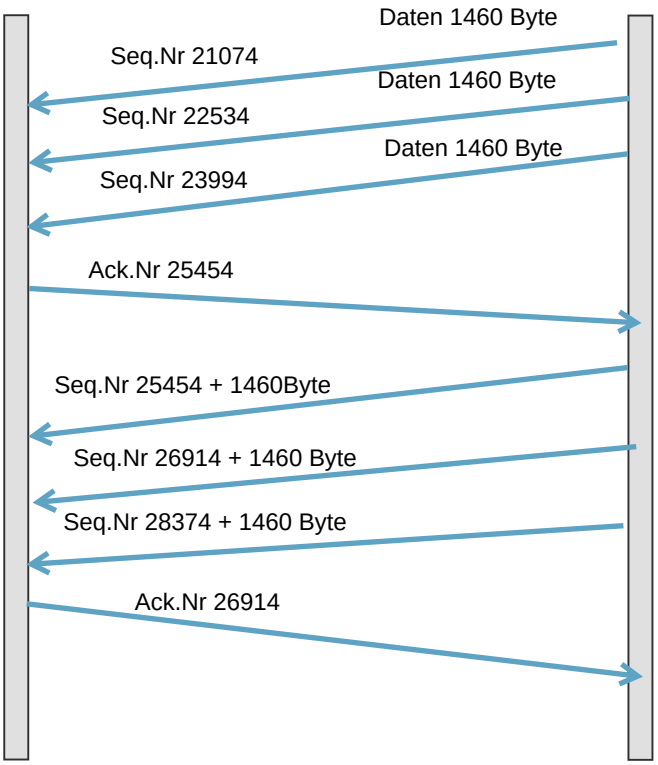


5.4 Einfacher Datenaustausch mit TCP



5.5 Datenaustausch mit Sliding Windows und Windowsize





Windowsize = max Anzahl an Bytes, die gesendet werden können, bevor eine Bestätigung erfolgen muss.

Auf beiden Seiten wird ein Sende-/bzw Empfangsbuffer verwendet, indem die Daten vorgehalten werden.

Die Flusskontrolle übernimmt der Sliding-Window Algorithmus.

Vorteil: WEniger Overload, da bei Überlast die Fenstergröße verkleinert wird.

5.6 Der TCP-Header

0	4	8	15	16	24	31
Source Port				Destination Port		
Sequence Number						
Acknowledgement Number						
H. Length	Reserved		Code Bits	Windowsize		
Checksum				Urgent Pointer		
Options						
Data						

Source Port	Nummer unter dem ein Dienst auf einem Rechner ansprechbar ist
Destination Port	
Sequence Number	Nummerierung in Senderichtung, erhöht sich um die Zahl der gegebenen bytes
Acknowledgement Number	Quittungsnummer in Empfangsrichtung Welches Byte wird als nächstes erwartet?
Header Length	Wert * 32 Bit
Reserved	6 Bits für künftige Ideen
Code Bits	Flags für spezielle Segmente
Windowsize	Wie viele Bytes können unbestätigt gesendet werden
Checksum	Prüfsumme
Urgent	
Options	
Data	z.B. Speiseplan.html

Die Codebits haben die folgende Bedeutung:

0	URG	UrgentPointer	Kennzeichnet Vorrang-Daten für bestimmte Anwendungen
1	**ACK**	**Acknowledgement**	Mit dem Wert 1 wird der Empfang von Daten bestätigt
0	PSH	Push	Kennzeichnet die sofortige Weiterleitung an die Anwendung (nicht erst in den Puffer), z. B. bei Telnet-Sitzungen
0	RST	Reset	Beendet die Verbindung aufgrund einer nicht näher bestimmbaren Fehlersituation
1	**SYN**	**Synchronization**	Sender signalisiert, dass eine Verbindung aufgebaut werden soll
0	FIN	Final	Leitet das ordentliche, endgültige Verbindungsende ein.

5.7 Layer 4: Das UDP-Protokoll

!

User Datagram Protocol: ein verbindungsloses
"nicht zuverlässiges" Netzwerkprotokoll

→ Keine Empfangsgarantie und keine garantierte Empfangsreihenfolge

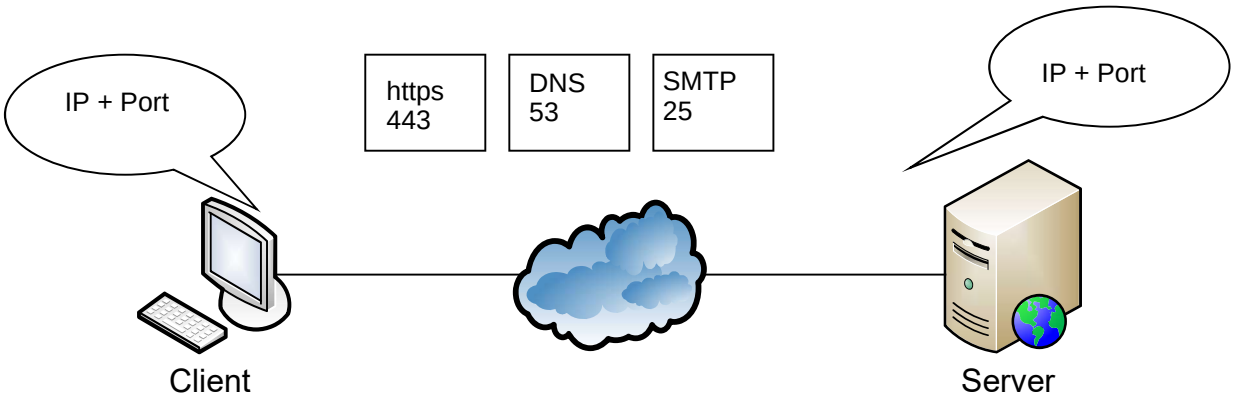
0	4	8	15	16	24	31
Source Port				Destination Port		
Length				Checksum		
Data						

sehr kompakt 96 Bit vs 160 Bit TCP

Source Port	siehe TCP
Destination Port	" "
Length	" "
Checksum	" "
Data	" "

Kombination aus ip + Port = Socket

5.8 Layer 4: Ports in der Datenkommunikation



Q-Port >1023	Z-Port 443	Daten

5.9 Wellknown und Registered Ports

0-1023	Well-Known Ports von der IANA fest für eine Anwendung vergeben!
1024 - 49151	Registered Ports Anwendungshersteller kann bei Bedarf einen Port bei der Iana registrieren
49152 - 64738	Dynamic Ports oder private Ports

5.10 Die wichtigsten Ports

Protokoll	Port	Beschreibung
FTP	20&21	20 Daten File Transfer Protocol 21 Verbindungsaufbau
SSH	22	Secure Shell verschlüsselte Kommandozeile
Telnet	23	remote Konnandozeile unverschlüsselt
SMTP	25 287	simple mail transfer Protocol → verschlüsselt
DNS	53 853	Domain Name System → verschlüsselt
http	80	Hypertext transfer Protocol is used to load webpages
HTTPs	443	Hypertext transfer Protocol secure is an extension to http to load webpages secure
TFTP	69	Trivial file transfer protocol is for exchanging files between two TCP/IP machines.
POP3	110 995	Post Office Protocol, version 3 (POP3) abrufen von mails → verschlüsselt
IMAP4	143 993	verwaltung, Synchronisierung von mails → verschlüsselt
RDP	3389	Remote desktop Protocol
SIP	5060 5061	Session Initiation Protocol → Verschlüsselt

5.11 Aus IHK-Prüfungen...

6. Handlungsschritt (20 Punkte)

Im Intranet der Spare Parts GmbH ist auf einem Internet Information Server ein browserfähiger User-Help-Desk eingerichtet, der für alle Clients im LAN erreichbar ist.

Während eines Netzwerkmonitorings wurde bei einem TCP-Verbindungsaufbau folgendes IP-Datagramm (Version 4) im Hex-Code aufgezeichnet.

ADDR	Hex-Code															
0000	45	00	00	28	D1	00	00	00	80	06	06	FD	C0	A8	02	10
0010	C0	A8	02	FE	04	0D	00	50	00	16	C1	52	00	00	00	00
0020	50	02	20	00	8F	CD	00	00								

aa) Ordnen Sie den o.g. Hex-Code in das Format des IP-Datagramms (Version 4) ein.

Hinweise:

- Das Optionsfeld bleibt leer
- IHL = IP-Header Length
- TTL = TimeTo Live

IP-Datagramm (Header + Nutzlast im 32 Bit-Raster)

<table>
<tr><td colspan="4">0 7 15 23 31</td></tr>
<tr><td>Version: 4</td><td>IHL: 5</td><td>Type of Service: 00</td><td>Gesamtlänge (Header + Nutzlast): 28</td></tr>
<tr><td colspan="3">Identifikation: D1 00</td><td>Fragmentflags / Fragmentoffset: 0000</td></tr>
<tr><td colspan="2">TTL: 80</td><td>Nutzlastprotokoll: 06</td><td>Kopfprüfsumme: 06 FD</td></tr>
<tr><td colspan="4">IP-Adresse des Absenders: C0 A8 02 20</td></tr>
<tr><td colspan="4">IP-Adresse des Empfängers: C0 A8 02 FE</td></tr>
<tr><td colspan="4">Eventuelle Optionen:</td></tr>
<tr><td colspan="4">IP-Nutzlast: 04 0D 00 50
00 16 61 52</td></tr>
</table>

(4 Punkte)

ab) Nennen Sie die Information aus dem IP-Header, die anzeigt, dass das Optionsfeld leer bleibt. (2 Punkte) JHL 26 Wert

ac) Nennen Sie die Information aus dem IP-Header, die anzeigt, dass es sich bei der Nutzlast um ein TCP-Protokoll handelt und nennen Sie den entsprechenden Steuercode. (2 Punkte)

ICMP = 1
UDP = 17

ad) Nennen Sie zwei weitere IP-Nutzlastprotokolle. (2 Punkte)

ae) Übersetzen Sie die IP-Adressen in das dezimale Format.

IP-Adresse des Absenders:	192.250.2.16
IP-Adresse des Empfängers:	192.250.2.254

(4 Punkte)

ba) Ordnen Sie die oben genannte IP-Nutzlast in das Format des TCP-Segments ein.

TCP-Segment (im 32 Bit-Raster)

0 7 15 23 31

TCP - Quellport:	TCP - Zielport:
Sequenznummer:	
Bestätigungsnummer:	
Kopflänge (4Bit) Reserviert (6 Bit) Flags (6Bit)	Fenstergröße:
TCP-Prüfsumme:	Zeiger auf Vorrangdaten:
Optionen (falls vorhanden):	
Daten:	

(4 Punkte)

bb) Nennen Sie den TCP-Zielport (dezimal) und den Dienst, der darüber erreichbar ist. (2 Punkte)

Zusatzfragen:

a) Bestimmen Sie die Fenstergröße!

b) Welcher Flag ist gesetzt?

c) Was können Sie aus dieser Angabe schließen?

Aus der IHK-Prüfung Winter 2006/07

1. Handlungsschritt (20 Punkte)

Im Intranet der BBE AG wurde eine Serverfarm eingerichtet, die für alle Clients im LAN erreichbar ist. Sie testen die neuen Verbindungen. Während eines Netzwerkmonitorings wurden die ersten beiden Datagramme eines TCP-Verbindungsaufbaus (IPv4) von einem Client zu einem Server aufgezeichnet (siehe Frame 1 und Frame 2 in der Anlage 1).

a) Bei Frame 1 handelt es sich um die Verbindungsanfrage eines Clients an einen Server.

aa) Ordnen Sie die Werte aus Frame 1 den entsprechenden Feldern des folgenden TCP-Protokollkopfs zu. (4 Punkte)

TCP-Quellport:	TCP-Zielport:
Sequenznummer:	
Bestätigungsnummer:	
Ack-Flag:	Syn-Flag:

ab) Welchen Server versucht der Client mit dieser Verbindungsanfrage zu erreichen? (2 Punkte)

ac) Welchen Port benutzt der Client? (2 Punkte)

b) Bei Frame 2 handelt es sich um die Antwort des Servers auf die Verbindungsanfrage des Clients.

ba) Ordnen Sie die Werte aus Frame 2 den entsprechenden Feldern des folgenden TCP-Protokollkopfs zu. (4 Punkte)

TCP-Quellport:	TCP-Zielport:
Sequenznummer:	
Bestätigungsnummer:	
Ack-Flag:	Syn-Flag:

bb) Wie hat der Server seine Bestätigungsnummer erzeugt? (2 Punkte)

bc) Wie hat der Server seine Sequenznummer erzeugt? (2 Punkte)

c) Im Three-Way-Handshake-Verfahren wird jetzt die Verbindung von dem Client bestätigt. Wie müsste jetzt der dazugehörige TCP-Protokollkopf aussehen? (4 Punkte)

TCP-Quellport:	TCP-Zielport:
Sequenznummer:	
Bestätigungsnummer:	
Ack-Flag:	Syn-Flag:

— Frame 1 ——

```
TCP: ——— TCP header ———
TCP:
TCP: Source port                    = 1037
TCP: Destination port               = 21
TCP: Initial sequence number        = 1491282
TCP: Acknowledgment number          = 0
TCP: Data offset                    = 24 Bytes
TCP: Flags                          = 02
TCP:              ...0......        = Urgent pointer
TCP:              ....0......       = Ack
TCP:              .....0.....       = Push
TCP:              ......0....       = Reset
TCP:              ...... 1...       = Syn
TCP:              ........0..       = Fin
TCP: Window                         = 8192
TCP: Checksum                       = 8FCD (correct)
TCP:
TCP: Options follow
TCP: Maximum segment size           = 1460
TCP:
```

— Frame 2 ——

```
TCP: ——— TCP header ———
TCP:
TCP: Source port                    = 21
TCP: Destination port               = 1037
TCP: Initial sequence number        = 80735
TCP: Acknowledgment number          = 1491283
TCP: Data offset                    = 24 Bytes
TCP: Flags                          = 12
TCP:              ...0......        = Urgent pointer
TCP:              ....1......       = Ack
TCP:              .....0.....       = Push
TCP:              ......0....       = Reset
TCP:              ...... 1...       = Syn
TCP:              ........0..       = Fin
TCP: Window                         = 8760
TCP: Checksum                       = 5224 (correct)
TCP:
TCP: Options follow
TCP: Maximum segment size           = 1460
TCP:
```

5.12 Weitere Übungen:

Aufgabe 1:

Was versteht man bei TCP/IP unter einem sogenannten „Socket“?

Kombination aus IP-Adresse und Port

Aufgabe 2:

Welche Aufgabe hat das TTL-Feld im IP-Header?

Time To Live: gibt die Anzahl der Hops an. Wenn der Wert "0"

erreicht, wird das Paket verlaufen. Max 255 Hops

→ Auf layer 2 gibt es keine TTL

Aufgabe 3:

Ergänzen Sie die folgende Tabelle zu Ports, den damit verbundenen Anwendungen und ihrer Aufgabe!

Port	Anwendung	Aufgabe
22	SSH	
25	SMTP	
53	DNS	IP <--> Domain
80	HTTP	
110	POP3	
443	HTTPS	
3389	RDP	
5060	SIP	

Aufgabe 4:

Warum eignet sich gerade UDP für die Übertragung von VoIP-Daten? Begründen Sie Ihre Aussage!

Fehlerkorrektur macht keinen Sinn. Das Gespräch ist auch so meist verständlich.

Aufgabe 5:

Beim Verbindungsaufbau zwischen zwei Hosts wurde folgender Datenverkehr mitgeschnitten. Erklären Sie die einzelnen Pakete, indem Sie den HEX-Code decodieren!

Paket 1:

```
45 00 00 30 2e 8f 40 00 80 06 00 00 0a a1 0b 14 5b c6
ae 02 c7 63 00 50 f8 a6 43 10 00 00 00 00 70 02 20 00
1f a0 00 00 02 04 05 b4 01 01 04 02
```

Paket 2

```
45 00 00 10 00 30 40 00 37 06 24 4b 5b c6 ae 02 0a a1
0b 14 00 50 c7 63 6e c4 18 f3 f8 a6 43 11 70 12 16 d0
c1 9e 00 00 02 04 05 b4 01 01 04 02
```

Paket 3

```
45 00 00 28 2e 91 40 00 80 06 00 00 0a a1 0b 14 5b c6
ae 02 c7 63 00 50 f8 a6 43 11 6e c4 18 f4 50 10 fa f0
1f 98 00 00
```

Aufgabe 6:

In einem Netzwerk wird die Internetnutzung nur über einen Proxy erlaubt.

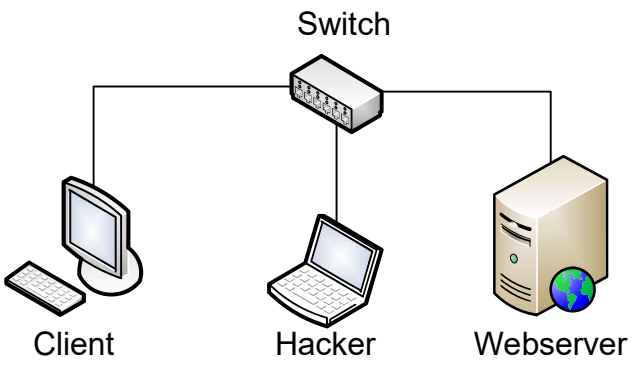
a) Nennen Sie die Aufgaben, die der Proxy im Netzwerk übernimmt.

- Caching; Filtern; stellvertretend Anfragen stellen
- Logging

b) Warum muss im Browser neben der Adresse auch der Proxy-Port eingetragen werden?

Un einen Kommunikationskanal zum Proxy server aufbauen zu können.
→ normalen HTTP-Datenverkehr über den Port auf den Proxy hört z.b. 8080 oder 3128

Aufgabe 7:



Welches Problem ergibt sich, wenn Daten mitgeschnitten werden sollen?

Der switch stellt eine 1:1 - Verbindung her.

→ Hacker bekommt keine anderen Pakete

Lösung: switch durch Hub ersetzen

ARP-Spoofing
MAC-Flooding

Mirror-Port