

1. Grundlagen und Netzarchitekturen:

- Heterogenität Hardware, Software (Typen, Hersteller)
- Unabhängigkeit, autonome Handlung
- räumliche Trennung der Rechner

Netz Vertragsarten:

- Persönliches Netz, wenige Meter (Bluetooth, USB)
- Lokales Netz, max. 100m (Ethernet, WLAN, LAN)
- Metro Netz, max. 100km (Metropolian Area Network (MAN), Zugangsnetze, regionale Glasfasernetze)
- Weltweites Netz, weltweite Anbindung (Wide Area Network (WAN), Internet, Satelliten)

Komplexe Netzstruktur Topologien:

- Baum: schleiffrei
- Vollverbindung: nicht schleiffrei
- Teilverbindung: nicht schleiffrei

Übertragungsmethoden:

- Simplex: nur eine Richtung \rightarrow unidirektional (Radio, Leuchtfäden)
- Halfduplex: entweder senden oder empfangen, nicht beides gleichzeitig (alte 10 Mbit/s Ethernet, diverse Funktechniken)
- Fullduplex: gleichzeitig senden u. empfangen \rightarrow bidirektional (Ethernet, aktuelles VoIP)

Kommunikationsstrukturen:

- Unicast: Punkt zu Punkt $○ \rightarrow ○$
- Broadcast: Rundsendung an alle $○ \xrightarrow{?} ○$
- Multicast: zu einer ausgewählten Gruppe $○ \xrightarrow{?} \{ \text{Gruppe} \}$
- Anycast: Anzahl Empfänger aus Gruppe $○ \xrightarrow{?} \{ \text{Gruppe} \}$

Grundlegende Leistungsmetriken:

- Datenrate: Datenrate $r = \frac{\text{Datenmenge } L}{\text{Zeitspanne } t}$

- Bandbreite: maximale Übertragungsrate
- Overhead: Datenrate / Bandbreite (in %)

Prinzip Konzept:

- Vereinbarung, wie Daten übertragung zwischen zwei oder mehr Partnern abläuft
- Definiert als Menge von Regeln
- Abgrenzen von Protokollen:
 - ↳ Normativitätsansatz: Definition überregionaler Datenträger (Binärcodierung, Textformat, etc...)
 - ↳ Nachvollziehbarkeit: Längen mit maximal möglicher Datumsreihe, Regeln für aktuelle, Wechselseitig
 - ↳ Identifizierung: Identifikation des Empfängers Interessen der Abnehmer
 - ↳ Fehlerbehandlung: Erkennung fehlerhafter Daten (z.B. Daten Abbrüche), Regeln für wiederholte Übertragungen von Datenblöcken
 - ↳ Zeitverteilung: Taktierung von Datenrate und anderen Parameter, Nutzen und Risiken von Verbindungen

CRC - Prüfsumme:

Beispielaufgabe

Für eine 3-bit Dateneinheit mit dem binären Wert 101 soll die CRC-5 Prüfsumme berechnet werden. Das Generatorpolynom sei $x^5 + x^2 + 1$. Welche Bits (Daten und Prüfsumme) werden anschließend versendet?

$$D = \underline{101}$$

$$G = x^5 + x^2 + 1 = \underline{100101}$$

$n=5$, da x^5 höchste

$$\underline{10100000} : \underline{100101} = 101 \text{ Rest } 10001$$

$$\begin{array}{r} \oplus 100101 \\ 0011010 \\ \oplus 000000 \\ \hline 0110100 \\ \oplus 100101 \\ \hline 010001 \end{array}$$

Beispielaufgabe 2:

Beispielaufgabe

Eine CRC-4 Prüfsummen verwendet das Generatorpolynom $x^4 + x + 1$. Es wird angenommen, dass ein Sender die CRC-4 Prüfsumme jeweils für eine Dateneinheit der Länge 6 bit berechnet und die CRC-4 Prüfsumme dann an die Nutzdaten anhängt. Ein Empfänger empfängt das Bitmuster 010000101 mit Daten und Prüfsumme. Ist die Prüfsumme in diesem Fall korrekt? Begründen Sie Ihre Antwort.

$$G = x^4 + x + 1 = 10011$$

$$D = 010000$$

$$P = 0101 \quad P = \text{Prüfsumme}$$

\oplus	0 1 0 0 0 0 0	0 1 0 1 · 1 0 0 1 1 = 0 1 0 0 1 1	Reft 0 0 0 0
\rightarrow	1 0 0 0 0 0		<i>Nullvektor genau wie oder 5 Bits lang</i>
\oplus	1 0 0 1 1		
\rightarrow	0 0 0 1 1 0	<i>immer eine reine 0 nach unten ziehen, Verschiebung um 1!</i>	
\oplus	0 0 0 0 0		
\rightarrow	0 0 1 1 0 1		
\oplus	0 0 0 0 0		
<i>Nach</i>	1 1 0 1 0		
<i>Brechstich</i>	1 0 0 1 1		
<i>immer</i>	1 0 0 1 1		
<i>Verschiebung</i>	0 0 0 0 0		<i>um 1 nach rechts</i>

Standardisierungen:

- IEEE : Institute of Electrical and Electronics Engineers (Ethernet, WLAN)
- IETF: Internet Engineering Task Force (Internet - Protokolle)

Hierarchisches Schichtmodell:

5-7: Anwendungsenschicht:

4: Transportschicht: Ende zu Ende Kommunikation

3: Vermittlungsenschicht: Weiterleitung zwischen Knoten

2: Sicherungsschicht: Bitrate Übertragung von Rahmen

1: Bitübertragungsschicht: ungeteilte Übertragung von Bits

Bsp World Wide Web

HTTP: Datenaustausch zw. Anwend. Progr.

TCP (Transmission Control Protocol): zuverlässige Übertragung

IP: Erreichbarkeit im Internet

Ethernet: verschiedene Techniken und Medien

Ethernet 100Base-T

TCP/IP Funktionsweise:

- Knoten: (Node), Gerät das IP implementiert
- Routier: Knoten, der IP Pakete weiterleitet
- Host: Knoten, der IP Pakete nicht weiterleitet (Endsystem)
- Link: Verbindung zwischen zwei Knoten (z.B. zwischen Host und Router)
- Hop: Verbindung über einen Knoten, insbesondere zum Zählen freigesetzter Router
- Pfad: Folge der Routen (Hops) vom Sender zum Empfänger

⑥ Technologien im lokalen Netz:

Vergleich Switch / Router:

Switch:

- Schicht 2 mit MAC-Adressen
 - ↳ Rahmen über Ethernet, eine Tendenz
 - ↳ einfache Vermittlung aufgrund Switch Tabelle
- Steuer Protokolle
 - ↳ (Rapid) Spanning Tree Protocol und weitere
- Management nicht zwingend
 - ↳ Grundfunktionen selbsttunend (z.B. Learning Bridge Algorithmus)
 - ↳ Unmanaged Ethernet Switches ohne externe Konfigurationsmöglichkeit
- Wartungsstand transparent auf Pfad
- Layer 3 Switch Abschlussschicht für Ethernet LANs

Router:

- Schicht 3 mit IP-Adressen
 - ↳ Pakete über beliebige Sicherungsprotokolle
 - ↳ Nötigste Vermittlung anhand Routing-Tabelle (RIB)
- Steuer Protokolle
 - ↳ Routing Protokolle (z.B. RIB, OSPF, BGP, ICMP, IGMP, ARP)
- Management erforderlich
 - ↳ Konfiguration notwendig (IP-Adr. Netzwerkstellen, Protokoll-Parameter)
 - ↳ min. eine Schnittstelle für Config. (z.B. Commandline, Website)
- Nicht transparent auf Pfad
 - ↳ Robustes Routing im Nachbarnetzen (Next-Hop)
 - ↳ Pfahlerweiterung (insbesondere TTL Wert)
 - ↳ Sichtbare Routing- und Steuernprotokolle

gewagte und ungern gesehene Switches:

- gewagter Switch:
 - ↳ ports configuration
 - ↳ besitzt min. 1 MAC Adresse und idr. auch IP-Adr.
 - ↳ Layer 2 Switch für Ethernet
 - ↳ Layer 3 Switch für
 - Schichter Ethernet Switch plus einfaches Routing
 - Konstruktion wie DHCP-Server auch möglich
 - nur kleine Routing Tabelle, nur einzelne dynamische Routing-Protokolle
 - konfigurierbar, d.h. immer gewagtes Gerät
 - ↳ infestigung logischer IP-Netzwerkstellen

- Nehschichtstelle mit IP-Adr. ohne physikalischen Netzadapter
- Virtuelle logische Routing-Schichtstelle zur Identifizierung des Geräts

umgekehrter Switch:

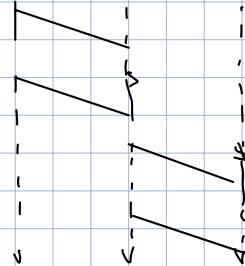
↳ "normaler Switch"

↳ hat nicht MAC noch IP Adr.

Forwarding Verfahren:

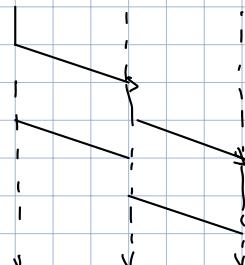
Store-and-Forward Forwarding:

- kontinuierliche Empfangung des Rahmens vor der Weiterleitung
- Zwischenprüfung ermöglicht Versetzung des Rahmens
- Latenz pro Switch abhängig von Länge
- Integritätsprüfung von Protokollen am Ende des Rahmens möglich



Cut Through Forwarding (fast Forwarding):

- Rahmen wird weitergeleitet sobald Schichtkopf empfangen wurde
- Rückfall auf Store-and-forward Forwarding ggf. notwendig
 - Asynchronie: Datumszeit des Ursprungspunkt weiter als die des Zielungspunkt
 - Weitwurf: Zielungspunkt durch andere Übertragung bedient
- Sehr geringe Latenz im Switch ($< 10 \mu s$)
- keine Integritätsprüfung und ggf. Weiterleitung fehlerhafter Rahmen



Forwarding Schichtbarkeit:

- Durchsatz mehrfach nicht begrenzt durch Datumszeit r sondern Paketraten $R = r / L$ (packets per sec)

Nehmenpunkt:

- Planung, Verwaltung, Betrieb und Überwachung von Rechnernetzen bzw. Kommunikationsnetzen mittlere Technischer Systeme wie z.B. Network Management System

Begriffserklärung:

Hostadresse:

- ↳ spezifische Adressen innerhalb eines Subnetz, die Geräten zugeordnet werden
- ↳ Bsp im Subnetz 10.1.0.0/16 können Hostadressen von 10.1.0.1 bis 10.1.255.254 reichen
 - ↳ wichtig! Die Adresse 10.1.0.0 ist das Netzwerkteil und 10.1.255.255 ist die Broadcast Adresse

Broadcast Adresse:

- ↳ ist die Adresse die verwendet wird, wenn man Daten an alle Hosts in einem Subnetz zu senden
- ↳ ist die größtmögliche IP-Adresse
- ↳ z.B. Subnetz 10.1.0.0 /16 ist Broadcast Adresse 10.1.255.255 da alle Bits der Hostadresse auf 1 gesetzt sind
- ↳ Broadcast MAC Adresse FF - FF - FF - FF - FF - FF

Netzwerkkomponenten:

- ↳ ist immer die erste Adresse im Subnetz, also immer die lokale Adresse
- ↳ definiert das Subnetz selbst, kann nicht Host (Computer, Router) zugewiesen werden

Verfahren CSMA/CD:

- ↳ Protokoll zur Steuerung des Zugriffs auf ein gemeinsames Netzwerkkomponenten und zur Fehlerfreiheit Datenübertragungen
- Carrier Sense: überprüfen ob Medium frei
- Multiple Access: mehrere Geräte teilen gleiches Medium
- Collision Detection: erkennen und beenden von Konflikten

↳ nicht mehr unbedingt in modernen Ethernet Netzwerken -> Gigabit Ethernet unterstützt CSMA/CD nicht!

Klar in frühen Ethernet Netzwerken wichtig gewesen um sicherzustellen, dass Daten effizient und ohne Verzögerungen übertragen werden.

Default Route:

- ↳ 0.0.0.0 /0 ist die Standard Route
- ↳ verwendet, wenn keine spezifische Route für Zielpunkt in Routing-Tabelle vorhanden ist
- ↳ zeigt auf nächstes Gateway oder Router

MSS:

- ↳ Maximum Segment Size: maximale Größe der TCP-Nutzlast, die in einem TCP-Segment übertragen werden kann
- ↳ $MSS = MTU \text{ (1500 Byte)} - \text{IP-Header (20 Byte)} - \text{TCP-Header (20 Byte)} = 1460 \text{ Byte}$

Datumsverzerrung:

- ↳ Ziel Dataverlust im Empfänger zu verhindern → Empfänger limitiert Gesamte Maximale Menge zu sendenden Daten
- ↳ Receive Window: im TCP Header, gibt Menge an Daten an die Empfänger bereit ist zu empfangen

Überlastung:

- ↳ Ziel Steuereinfluss / Überlastung im Netz zu verhindern → Sender kann Ergebnisse abtunnen
- ↳ Congestion Window: nicht im Header, regelt Menge an Daten, die Sender in Wohnung senden kann, bevor Bestätigung empfangen wird um Wettbewerbung zu verhindern

Sendefenster in TCP:

- ↳ Sendefenster = $\min(CWND, RWNND) = \min(1634 \text{ bytes}, 3334 \text{ bytes}) = 3334 \text{ bytes}$
- ↳ Stellt sicher, dass Sender nicht mehr Daten sendet, als Empfänger verarbeiten kann

1000 base-T:

- ↳ 1000 mbps → 1Gbit → 1000 000 000 bit

Ethernet:

Hop:

↳ überqueren einzelner Netze oder Gateways

↳ Bsp. Punkt zu Punkt von einem Computer über 3 Router an Zielcomputer dann hat es 3 Hops durchlaufen

TTL:

V

- wird immer reduziert bei einem Hop bzw. wenn es Router durchquert

lokales Netzsegment für Ethernet:

- logischer Verbund Netzwerkgeräte

- Es verbindet Stationen in einem lokalen Netzwerk (LAN)

- In einem lokalen Netzsegment erreicht ein Broadcast alle Stationen

Traceroute:

↳ Sendet IP-Packet TTL-Wert von 1 und erhält davon Schrittwise um jeden Hop auf Weg zum Ziel zu ermitteln

↳ Das Paket wird gesendet und erster Router auf dem Weg reduziert Wert auf 0

↳ Da TTL Wert 0 ist, verzögert Router das Paket und sendet ICMP-Zeitüberschreitungsnachricht (Time-Exceeded) zurück zum Absender

↳ Traceroute kann IP-Adresse daraus ermitteln -> es wird als Antwort IP-Adresse zurückgespielt

↳ Prozess wird fortgesetzt, solange TTL-Wert schrittweise erhöht wird bis Punkt Ziel erreicht oder maximale TTL Wert erreicht wird

Lokal mit Ethernet:

ping:

Die Studierenden versuchen nun mit dem Programm „ping“ auf Rechner A, durch Ausprobieren aller möglichen IPv4 Adressen in 192.168.3.224/27 die richtige IPv4 Adresse von Rechner C zu ermitteln.

- q) Ist es möglich, Rechner C von Rechner A aus erfolgreich anzupingen, d.h. von Rechner A aus auch eine ping-Antwort von Rechner C zu bekommen, wenn die Studierenden die richtige IPv4 Adresse von Rechner C erraten? Begründen Sie Ihre Antwort sorgfältig. [2P]

- Zu unter den genannten Annahmen können Rechner A und C bidirektional kommunizieren
- C hat Adresse im Subnetz 192.168.3.224/27, die innerhalb von 192.168.2.0/23 liegt
- Sie liegt aus Sicht des Routers im mittigen Sub-Netw 192.168.2.0/23, so dass dieser die ICMP Echo Request Anfrage zustellen wird

↳ Hinweis: für ICMP Echo Reply Antwort von Rechner C ist Default-Gate zum Next-Hop relevant, die aber laut Aufgabenstellung zur richtigen Adresse 192.168.3.224 des Rechners vorliegt und auch in 192.168.3.224 liegt.

Protokolle:

ARP: (lokal)

- ARP genetisches Protokoll zur Ermittlung der Hardware-Adresse zu einer Netzwerkadresse.
- Es wird verwendet um MAC Adresse zu einer gegebenen IPv4 Adresse zu suchen
(ARP nur für IPv4 nicht für IPv6 verwendet)

ICMP: (lokal / Internet)

- Übertragung von Fehler und Kontrollnachrichten → ping, traceroute (testet ob Erreichbarkeit Gerät zu prüfen)



PDUs:

↪ allgemeiner Überbegriff → Daten die von einer Protokollsicht zur nächsten übertragen werden

↪ jeder Protokoll das Daten versendet sendet PDUs

↪ spezifische Einheit von Daten die zwischen Schichten eines Netzwerkprotokolls angepasst wird

und notwendige Steuerinformationen enthält, die von der jeweiligen Protokollsicht benötigt werden

Verschleißprinzip:

- Protocol-Dateneinheiten eines höheren Schicht werden durch Einwappeln zur Nutzlast (Payload)

der darunterliegenden Schicht

- Sie werden außerdem um Steuerinformationen im Header und/oder Anhang (Trailer) ergänzt

↪ übersicht aller Protokolle, zusammen mit OSI und auch (lokal, Ethernet, IP, Internet)

UDP

Internet:

CIDR:

- gibt IP-Adressen und Präfixlänge (Netzmaske) ($/24$)
 - Notation: $182.168.1.0/24$ → ersten 24 Bits der IP-Adresse stellen das Netzprefix dar
 - erlaubt IP-Adressen effizienter zu nutzen und kleinere oder größere Subnetze zu erstellen bzw. aufzuteilen
- ↳ Klassisches Internet Domäne Routing zur Unterteilung des Adressraums des Internet Protocols
- ↳ In einem IP-Sub-Netz ist seit dessen Einführung die Netzmaske / Präfixlänge flexibel nutzbar
- ↳ Netzmaske / Präfixlänge kann für Sub-Netze immer angegeben werden

Routing-Tabelle:

- Destination: wo Datenpaket hingeendet werden soll
- Next-Hop: IP-Adresse des nächsten Routers an den Datenpaket weitergeleitet wird
- Interface / Netzschmittstelle: Das Netzwerkinterface des Routers über das das Datenpaket weitergeleitet wird
 - ↳ repräsentiert den Zugangspunkt des Routers zu diesem Subnetz und besitzt eine IP-Adresse in diesem Subnetz die einzigartig ist
 - ↳ diese sind sogenannte physischen LAN-Buchsen Anschlüsse am Router wo man LAN-Kabel anschließt (zum Verständnis)
- ↳ Reihenfolge Routing Tabelle spielt keine Rolle
- ↳ zutreffende Einträge werden durch longest Prefix Matching Algorithmus ermittelt, der unabhängig von der Reihenfolge des passenden Eintrags ermittelt

↳ SS 22 1q) als Beispiel zum Verständnis:

Die drei Router haben unter anderem die folgenden Netzschmittstellen:

- Router S: 10.1.0.1/16, 10.0.12.1/30, 10.0.13.1/30
- Router H: 10.2.0.1/16, 10.0.12.2/30, 10.0.23.1/30
- Router T: 10.3.0.1/16, 10.0.13.2/30, 10.0.23.2/30

↳ beide befinden sich im Subnetz
} 10.0.12.0/30 deshalb steht es diese

Router H habe für IPv4 die folgende Routing-Tabelle, in der Metrik-Einträge vernachlässigt wurden und alle zunächst relevanten Sub-Netze enthalten sind:

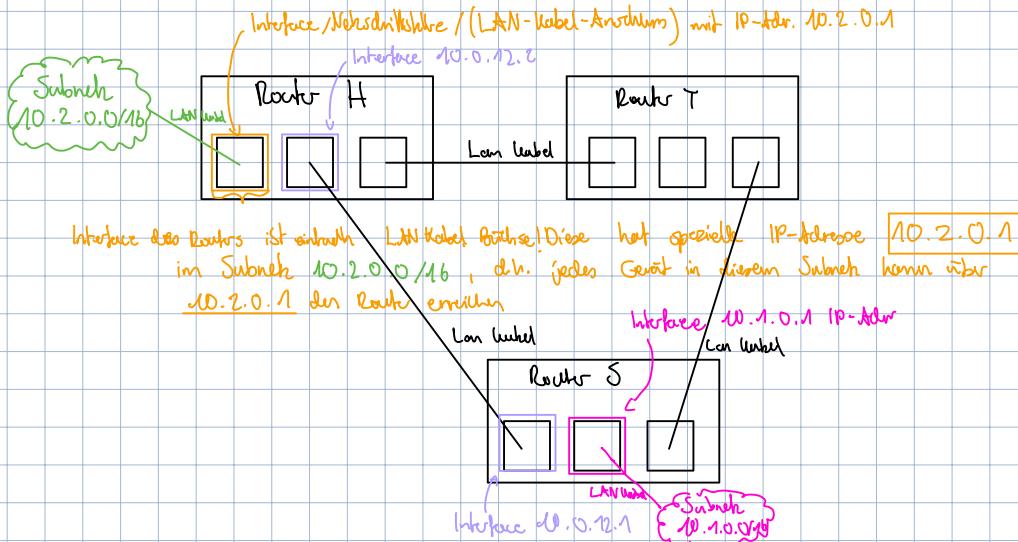
Nr.	Destination	Next Hop	Interface
1	10.1.0.0/16	10.0.12.1	10.0.12.2
2	10.2.0.0/16	-	10.2.0.1
3	10.3.0.0/16	10.0.23.2	10.0.23.1
4	10.0.12.0/30	-	10.0.12.2
5	10.0.13.0/30	10.0.23.2	10.0.23.1
6	10.0.23.0/30	-	10.0.23.1
7	0.0.0.0/0	10.0.12.1	10.0.12.2

Welche IPv4 Adresse hat Router S auf dem Link, der Router S direkt mit Router H verbindet? [1P]

↳ Die IP-Adresse von Router S auf dem Link kann man ganz einfach aus Aufgabenstellung über (rot markiert ablesen)

↳ beide Router müssen sich nämlich im selben Subnetz befinden

Beispiel zum Verständnis was genau Interface / Netzschmittstelle ist zum Verständnis:



Eine Reihe von Geräten mit IP Adressen zwischen 10.3.0.24 und 10.3.0.63 (jeweils einschließlich) soll vom Standort Talstadt an den Standort Stallhofen umziehen. Die IP Adressen der Geräte sollen sich dabei jedoch nicht ändern. Beispielsweise soll Client T30 mit der IP Adresse 10.3.0.30 in diesem Adressbereich nach dem Umzug mit Router S direkt per LAN-Technik verbunden sein. Der Client T70 ist aber nicht von dem Umzug betroffen.

Nach dem Umzug soll die Routing-Tabelle des Routers H daher so geändert werden, dass Pakete an alle IP Adressen zwischen 10.3.0.24 und 10.3.0.63 an Router S weitervermittelt werden. Für alle anderen IP Adressen soll sich das Routing in Router H jedoch nicht ändern.

- s) Geben Sie zweizusätzliche statische Routing-Tabelleneinträge für Router H an, die sicherstellen, dass im Router H alle IP Pakete an die IP Adressen 10.3.0.24 bis 10.3.0.63 direkt an Router S weitergeleitet werden. Die richtige Antwort besteht aus nur zwei weiteren Routing-Tabelleneinträgen. Begründen Sie kurz Ihre Antwort. [4P]

Nr.	Destination	Next Hop	Interface
1	10.1.0.0/16	10.0.12.1	10.0.12.2
2	10.2.0.0/16	-	10.2.0.1
3	10.3.0.0/16	10.0.23.2	10.0.23.1
4	10.0.12.0/30	-	10.0.12.2
5	10.0.13.0/30	10.0.23.2	10.0.23.1
6	10.0.23.0/30	-	10.0.23.1
7	0.0.0.0/0	10.0.12.1	10.0.12.2

Router S: 10.1.0.1/16, 10.0.12.1/30, 10.0.13.1/30 → an Router S weitergeleitet

Router H: 10.2.0.1/16, 10.0.12.2/30, 10.0.23.1/30 → von Router H soll weitergeleitet werden

Router T: 10.3.0.1/16, 10.0.13.2/30, 10.0.23.2/30

↳ Schwellstelle die beide Netze miteinander verbindet

↳ IP-Adressen die umzuordnen: 10.3.0.24 -> 10.3.0.63

NR	Destination	Next Hop	Interface
8	10.3.0.24/29	10.0.12.1	10.0.12.2
9	10.3.0.32/27	10.0.12.1	10.0.12.2

↳ Startet von Router H aus mit Schwellstelle 10.0.12.2

Soll an Router S weiterleiten aber hat IP-Adr. 10.0.12.1

Es werden nur die spezifischen IP-Adr. angewählt /29 = 8 IP-Adr. möglich + /27 = 32 IP-Adr möglich = 40 IP-Adr.

↳ von 10.3.0.24 bis 10.3.0.63 sind es insgesamt 40 IP-Adr. die eine geänderte Route brauchen

↳ Begründung:

- Der Adressbereich 10.3.0.24 bis 10.3.0.24 bedient an zwei Subnetzen, für die jeweils Routing-Tabelleneinträge erforderlich sind
- Die IP Adressen 10.3.0.24 bis 10.3.0.31 sind im Subnetz 10.3.0.24/29 enthalten
- Die IP Adressen 10.3.0.32 bis 10.3.0.63 sind im Subnetz 10.3.0.32/27 enthalten
- Für beide neuen Routing-Tabelleneinträge ist der NextHop 10.0.12.1 und entsprechende Schwellstelle ist 10.0.12.2

Formeln:

Bandbreite - Verzögerungsprodukt:

$$\text{BDP} = B \cdot \text{RTT} = 6 \text{ Mbit/s} \cdot 100 \text{ ms} \cdot 8 \text{ byte} = 300000 \text{ byte} \quad (\text{als Beispiel})$$

Datenrate:

$$\text{Datenrate } r = \frac{\text{Datenumenge } L}{\text{Zeit } t}$$

↳ Menge an Daten die pro Schende über Netzwerk gesendet wird

Pakethalte:

$$\text{Pakethalte } R = \frac{\text{Datenrate } r}{\text{Datenumenge } L}$$

↳ beschreibt Pakethalte, wie viel Pakete pro Schende über Netzwerk gesendet werden

Serialisierungszzeit:

↳ gibt an, wie lange es dauert, Datapunkt vollständig auf Netzwerkmedium zu übertragen

$$\hookrightarrow t_s = \frac{\text{Anzahlpakete } L}{\text{Datenrate } r} = \frac{12000 \text{ Bits}}{100.000 \text{ Bit/s}} = 120 \text{ ms als Beispiel}$$

Propagationszeit:

↳ Zeit die Datapunkt benötigt um durch Übertragungsmedium von der Quelle zum Ziel zu reisen

$$\hookrightarrow t_p = \frac{\text{Distanz}}{\text{Ausbreitungsgeschwindigkeit}} = \frac{d}{c} = \frac{36000 \text{ km}}{300 \text{ km/ms}} \rightarrow \begin{array}{l} \text{Lichtgeschwindigkeit } 300 \text{ km/s} \\ \text{Ausbreitung in Glasfaser } 200 \text{ km/ms} \end{array}$$

RTT

↳ handl Trip time also hin und zurück

$$\hookrightarrow \text{RTT} \approx t_s + 2 \cdot t_p = L/r + 2 \cdot d/c$$

Aufgaben zu Kunden:

SSZ2 1m):

- m) Auf der Glasfaser zwischen Router T und Router S können während einer 50 ms dauernden Unterbrechung keine Daten übertragen werden. Berechnen Sie, wie viele Bytes während dieser Zeittyp nicht von Router T an Router S gesendet werden können. Die Struktur von Rahmen und Protokollmechanismen können hierbei vernachlässigt werden. [5P]

↳ zwischen Router T und Router S ist ein 10GBase-ER Glasfaser habe (nun nun aus Netztopologie rauslesen)

$$\hookrightarrow \text{Datenrate } r = 10 \text{ Gbit/s}, \text{ Formel } r = L/t \rightarrow L = r \cdot t$$

↳ gewehlt ist die Datenumenge $L = r \cdot t = 10 \text{ Gbit/s} \cdot 50 \text{ ms}$

$$= 10000000 \text{ bit/s} \cdot 0.05 \text{ s} = 500 \text{ bit}$$

↳ 500 bit umwandeln in Byte: $500 \text{ bit} : 8 = 62.5 \text{ Byte}$

)

SSZ2 1m):

Studierende Delta spielt regelmäßig zusammen mit anderen Personen interaktive Computer-Spiele über das Internet. Der Client des Spiels auf Rechner D greift dazu auf einen Spiele-Server im Internet zu. Für einen flüssigen Spielverlauf ist eine niedrige Verzögerungszeit zum Spiele-Server erforderlich.

- r) Der Client des Spiels misst als Umlaufzeit zum Spiele-Server den Wert RTT = 10 ms. Wie viele Kilometer entfernt kann der Spiele-Server maximal vom Rechner D entfernt sein? [4P]

$$\hookrightarrow \text{RTT} \approx t_s + 2 \cdot t_p \rightarrow t_p \text{ vernachlässigbar}$$

\hookrightarrow ges: $RTT = 10ms$

$$c = 200 \text{ km/ms}$$

\hookrightarrow Anlernungsgeschwindigkeit in Glasfaser

\hookrightarrow ges: d

$$RTT = 2 \cdot \frac{d}{c} \quad | \cdot c \quad | : 2$$

$$d = \frac{RTT}{2} \cdot c = \frac{10ms}{2} \cdot 200 \text{ km/s} = 1000 \text{ km}$$

WS 23/24 1S:

Die Anwendung des Spiels versendet laut einer Messung vom Spiele-Server zum Client im Durchschnitt 1000 byte große Pakete mit einer mittleren Datenrate von 512 kbit/s.

- s) Wie viele Pakete pro Sekunde versendet der Spiele-Server, d.h. wie groß ist die Paketrate in der Einheit pps? [5P]

\hookrightarrow ges: Datumsge L = 1000 byte = 8000 , Datumsge L = 512 kbit/s = 512 000 bit/s

$$\hookrightarrow \text{Paketrate } R = \frac{\text{Datenrate } r}{\text{Datumsge } L} = \frac{512 \text{ kbit/s}}{8000 \text{ byte}} = \frac{512 000 \text{ bit/s}}{8000 \text{ bit}} = \frac{512}{8} \text{ pps} = 64 \text{ pps}$$

|P:

DHCP:

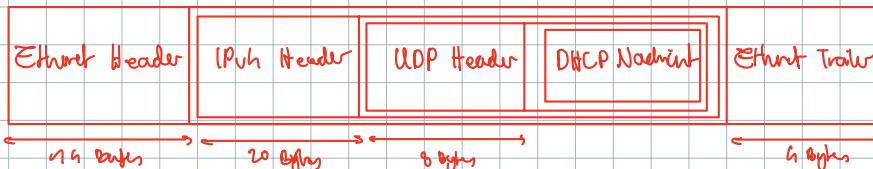
↳ DHCP Workflow:

- Discover: Client sendet Broadcast-Nachricht, um nach DHCP-Server zu suchen
 - ↳ **DHCP-DISCOVER**: Nachricht wird von DHCP Client an DHCP-Server als播送 gesendet um zu finden
 - ↳ wird an Broadcast MAC Adresse generiert **FF-FF-FF-FF-FF-FF**
- Offer: DHCP-Server antwortet mit Angebot, bietet Konfigurationsinformation und IP-Adresse an → **DHCP-OFFER**
- Request: Client wählt Angebot und fordert die darin enthaltene IP-Adresse, Konfigurationsinformation an → **DHCP-REQUEST**
- Acknowledge: DHCP Server bestätigt die Zuweisung der IP-Adresse und übermittelt die endgültigen Konfigurationsparameter → **DHCP-ACK**
 - ↳ falls abgelehnt sendet DHCP-Server → **DHCP-NACK**
 - ↳ falls IP-Adresse bereits in Verwendung sendet DHCP-Client → **DHCP-DECLINE**

↳ DHCP Nutzbarkeit:

- DHCP vereinfacht die Netzwerkkonfiguration und stellt sicher, dass IP-Adressen effizient, konfliktfrei verwaltet werden
- ↳ **Nehparameter die DHCP konfiguriert**: → dazu: Name von 3. Nehparametern die mit DHCP konfiguriert werden können
 - Prefix-Länge bzw. Netzmaske: definiert Größe Subnetz, hilft Gerät zu bestimmen welche IP-Adr. im gleichen Subnetz
 - Default Route bzw. Gateway: IP-Adresse Router mit dem Gerät auf andere Netzwerke zugreifen kann
 - DNS-Server: IP-Adressen Server, die DNS Anfragen auflösen und Domänennamen in IP-Adr. übersetzen
 - weitere: Domain-Name, Lease-Time, WINS-Server, NTP-Server, IPv6-Adresse

↳ Struktur 1200Octet-T Rahmen mit DHCP Nachricht:



DNS:

↳ (Domain Name System) übersetzt Domain Namen in IP-Adressen und umgekehrt

↳ Forward DNS-Lookup: (Suche nach IP-Adresse zu gegebenen Hostnamen)

- z.B. Domain google.com wird zu 178.1.0.24 IP-Adr.

↳ Reverse DNS-Lookup: (Suche nach Hostnamen zu gegebener IP-Adresse)

- z.B. IP-Adresse 178.1.0.24 wird zu google.com Domain

↳ In Wireshark: mögliche Abfragen! (SS22 K2 a-e)

No.	Source	Destination	Info
1	172.20.0.1	172.21.0.1	Standard query 0xda34 A server2.rnlab.test
2	172.20.0.1	172.21.0.1	Standard query 0x9433 AAAA server2.rnlab.test
3	172.21.0.1	172.20.0.1	Standard query response 0xda34 A server2.rnlab.test A 172.21.1.1
4	172.21.0.1	172.20.0.1	Standard query response 0x9433 AAAA server2.rnlab.test SOA ns.rnlab.test

↳ DNS verwendet immer Standard Query und Standard Query Response → somit kann nur so Werte ablesen!

↳ An welche Ziel-Portnummer wurde das erste Paket versendet, wenn die standardisierte Portnummer verwendet wird? [1P]

- Das 1. Paket wurde an Portnummer 53 gesendet → DNS verwendet diese Portnummer standardisiert!

↳ Erläutern Sie kurz, wonach der Client im zweiten aufgezeichneten Paket sucht. [2P]

- Es sieht für IPv4 und AAAA für IPv6!

↳ Das zweite Paket sucht mit dem AAAA Record die IPv6 Adresse zu einem Hostnamen

↳ Der Client fragt nach der IPv6 Adresse zum Hostnamen „server2.rnlab.test“

↳ Das dritte aufgezeichnete Paket enthält eine erfolgreiche Antwort des DNS Servers. Welche IP Adresse hat der antwortende DNS Server? Begründen Sie kurz Ihre Antwort. [2P]

- Der DNS Server hat die IP-Adresse 172.21.0.1 ist als Quelladresse (Source) erkennbar

↳ es ist nicht 172.21.1.1! Das ist die IPv4 Adresse für den Hostnamen server2.rnlab.test

↳ Wäre es denkbar, mit Wireshark auch DNS Nachrichten aufzuzeichnen, die in Transmission Control Protocol (TCP) Segmenten transportiert werden? Begründen Sie Ihre Antwort. [3P]

- Ja, das ist möglich

- DNS verwendet neben UDP auch TCP

- TCP wird verwendet, wenn Längere Abfragen / Antworten, Zonentransfers zwischen Primary und Secondary Name Server

↳ z.B. längere Abfragen / Antworten, Zonentransfers zwischen Primary und Secondary Name Server

TCP:

↳ Aufgabe: zweistufige, verbindungsorientierte Datübertragung mit Fehlerkorrektur, Rahmenfolgestellung und Flusskontrolle

↳ Three-Way Handshake:

- SYN: Client sendet SYN-Paket an Server um Verbindung zu initiieren ("Synchronization")
- SYN-ACK: Server antwortet mit SYN-ACK Paket um Verbindungsaufnahme zu bestätigen
- ACK: ("Acknowledgment") Client sendet ACK-Paket um Verbindung zu bestätigen / bestätigt auch Empfang von Daten

↳ weitere Flags:

- FIN: beendet Verbindung ("Finish")
- RST: schüttelt Verbindung zurück, meist bei Fehlern ("Reset")
- PSH: ("Push") fordert sofortige Übergabe der Daten an die Anwendung
- URG: ("Urgent") markiert dringende Daten

↳ Sequenznummer und Bestätigungsnummer:

- Sequenznummer: gibt Position der ersten Byte-Daten im Segment an z.B. (Seq=100)
- Bestätigungsnummer: gibt an welche Bytes als nächsten erwartet wird z.B. (ACK=101)

↳ Verbindungsorientiert: baut stabile zweistufige Verbindung auf, bevor Daten übertragen werden

↳ SS22 mögliche Aufgaben Wirschen:

```
5 172.20.0.1 172.21.1.1 52444 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
6 172.21.1.1 172.20.0.1 22 → 52444 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=64
7 172.20.0.1 172.21.1.1 52444 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8 172.20.0.1 172.21.1.1 52444 → 22 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=332
9 172.21.1.1 172.20.0.1 22 → 52444 [ACK] Seq=1 Ack=333 Win=64128 Len=0
10 172.21.1.1 172.20.0.1 22 → 52444 [PSH, ACK] Seq=1 Ack=333 Win=64128 Len=32
```

↳ Welche TCP Optionen sind laut dem Ausdruck im Segment in Rahmen Nr. 6 enthalten? [2P]

- MSS: gibt maximale Segmentgröße an die Sender akzeptieren kann (maximale Nutzlast TCP 1460 Bytes)
- SACK Permidi: ermöglicht selektive Bestätigungen, nur effiziente Fehlerkorrektur eingeführt
- WS: (Window Scale) Erweitert Shifting Fenster für Hochleistungsumgebung

↳ len(length), win (window size) sind keine Optionen! Sie sind Standardfelder des TCP-Headers

↳ In welchem Zustand befindet sich die TCP Verbindung im Client nach Versenden des Segments in Rahmen Nr. 7? [1P]

- Verbindungszustand: aufgebaut Verbindung

↳ Woher weiß der Empfänger bzw. die Software Wireshark, dass im Segment in Rahmen Nr. 7 keine Anwendungsdaten enthalten sind? Begründen Sie kurz Ihre Antwort. [2P]

- Es gibt kein spezielles Feld im TCP-Header, das direkt die Länge der TCP-Nutzlast (Anwendungsdaten) angibt
- Wireshark kann es ermitteln aus der Länge dieses IP-Pakets abzüglich IP und TCP-Header

- Len = 0: Länge TCP Anwendungsdaten in der TCP Nutzlast ($\text{len} = 0$) ist nicht im Pakethaupt codiert

(c) Welcher Wert steht in dem 16 bit langen Feld „Window“ im Paketkopf des Segments im Rahmen Nr. 8, d.h. welcher Wert wird tatsächlich zwischen Sender und Empfänger als binärcodierte Zahl übertragen? Begründen Sie Ihre Antwort. [3P]

Hinweise:

- $64256 / 32 = 2008$
- $64256 / 64 = 1004$
- $64256 / 128 = 502$
- $64256 / 256 = 251$

- Window Scale (WS) zum Verständnis:

- Wert win (Window) gibt die Fenstergöße des Senders an, die der Empfänger nutzen soll
- Option WS = 128 (Window Scale) gibt an wie hoch der Shiftratefaktor ist

↳ hier ist der Shiftratefaktor vom Client (172.20.0.1) zu Server (172.21.1.1) laut Segment Nr. 5 Wert 1

5 172.20.0.1 172.21.1.1 52444 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
8 172.20.0.1 172.21.1.1 52444 → 22 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=332

- In Zeile 8 steht $\text{win} = 64256$ also das heißt shiftrate Window

↳ der shiftrate Wert im TCP Pakethaupt ist also $64256 / 128 = 502$

wichtige Tabellen:

Sub-N	Nehmweise	Anzahl IP-Adr.
1/8	255.0.0.0	$2^4 = 16.777.216$
1/9	255.128.0.0	$2^{13} = 8.388.608$
1/10	255.192.0.0	$2^{12} = 4.194.304$
1/11	255.224.0.0	$2^{11} = 2097.152$
1/12	255.240.0.0	$2^{10} = 1.048.576$
1/13	255.248.0.0	$2^9 = 524.288$
1/14	255.252.0.0	$2^8 = 262.144$
1/15	255.254.0.0	$2^7 = 131.072$
1/16	255.255.0.0	$2^6 = 65.536$
1/17	255.255.128.0	$2^5 = 32.768$
1/18	255.255.192.0	$2^4 = 16.384$
1/19	255.255.224.0	$2^{13} = 8.192$
1/20	255.255.240.0	$2^{12} = 4.096$
1/21	255.255.248.0	$2^{11} = 2.048$
1/22	255.255.252.0	$2^{10} = 1.024$
1/23	255.255.254.0	$2^9 = 512$
1/24	255.255.255.0	$2^8 = 256$
1/25	255.255.255.128	$2^7 = 128$
1/26	255.255.255.192	$2^6 = 64$
1/27	255.255.255.224	$2^5 = 32$
1/28	255.255.255.240	$2^4 = 16$
1/29	255.255.255.248	$2^3 = 8$
1/30	255.255.255.252	$2^2 = 4$
1/31	255.255.255.254	$2^1 = 2$
1/32	255.255.255.255	$2^0 = 1$

wichtige Portnummern:

NR	Zweck
80	HTTP (Hypertext Transfer Protocol)
443	HTTPS
20	FTP (Dateübertragung) (File Transfer Protocol)
21	TCP (Kontrollverbindung) (Protocol)
22	SSH (Secure Shell)
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (TCP und UDP)
110	POP3 (Post Office Protocol vor 3)
143	IMAP (Internet Message Access Protocol)
3389	RDP (Remote Desktop Protocol)
8306	MySQL

↳ Aufgabenbeispiel: Subnetz: 10.1.0.0/16

Wie Broadcast? 10.1.1.255 → in /16 müssen ersten beiden Bytes mit Nehmweise übereinstimmen mit 10.1.0.0, letzte beiden Bytes müssen vorstehender Wert eben Bytes haben, d.h. 255

- 10.1.1.100 → liegt in Subnetz, da erste beiden Bytes übereinstimmen
- 10.2.2.200 → liegt nicht in 10.1.0.0/16, da zweite Byte nicht übereinstimmt
- 10.3.3.300 → keine gültige IPv4 Dot-Decimal Notation liegt in keinem Subnetz

Zeit (s)	ms	Micro (μs)	Nano (ns)
1	1.000	1.000.000	1.000.000.000
0,1	100	100.000	100.000.000
0,01	10	10.000	10.000.000
0,001	1	1.000	1.000.000

Problemaufgaben:

SS22 1d)

Der Switch habe insgesamt 8 Anschlüsse mit 1000BASE-T. Wie viele MAC Adressen benötigt der Switch in diesem Fall? Begründen Sie kurz Ihre Antwort. [2P]

- ein ungenutzter Switch benötigt keine MAC Adresse.
- Einige ungenutzte Switches können ohne MAC Adresse aus, da an den Geräten selbst keine Rahmen gesendet werden müssen

SS22 1n):

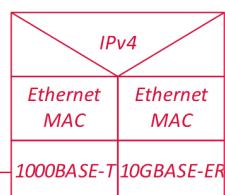
Um Kommunikationsprobleme zu analysieren, soll auf dem Rechner Client T30 analysiert werden, welchen Weg IP Pakete zum Server S10 nehmen. Mit welcher Anwendung kann auf einem Client ermittelt werden, welche Router auf dem Pfad zu einem Server liegen? Beschreiben Sie ausführlich die prinzipielle Funktionsweise dieses Werkzeuges. [5P]

- Pfad kann durch **traceroute** ermittelt werden
- Trace route versendet IP Pakete mit aufsteigendem TTL Wert von = 1, 2, 3 ...
- Pakete entlang des Pfades erhalten ggf. TTL=0 und werden verworfen; in der Regel wird dabei eine ICMP Fehlermeldung (Time Exceeded) zurückgesendet
- Traceroute kann dann den Router aus der ICMP Fehlermeldung identifizieren
- Verfahren bricht ab, wenn angegebenes Ziel erreicht wird. Pro Hop (d.h. TTL Wert) werden in der Regel mehrere (typisch 3) Messungen durchgeführt, die auch die Laufzeit ermitteln.

Es gibt verschiedene Möglichkeiten, welche IP Paket traceroute versendet, neben ICMP Nachrichten auch UDP Datagramme

SS22 1r):

Router H vermittelt ein von Client H20 gesendetes IP Paket zum Server S10. Skizzieren Sie den dafür verwendeten Protokollstapel im Router H. Es reicht eine Darstellung der Protocolschichten auf Router H. Transport- und Anwendungsprotokolle und Adressen müssen nicht angegeben werden. [3P]



- 3 Vermittlungsschicht IPv4 verbindet netz zwischen zwei gebundenen Siedensgeschaltern vermittelt
- 3 Router verbindet zwischen Ethernet MAC in der Sicherungsschicht (Ethernet-Sicherungsschicht)
- 3 Bitübertragungsschichten 1000Base-T und 10GBase-ER also LAN-Knotsch

SS22 1r):

m) Kann auf Rechner A mit einem Netzwerk-Analysetool wie Wireshark die unbekannte MAC Adresse von Rechner C ermittelt werden? Falls ja, wie? Begründen Sie kurz Ihre Antwort. [2P]

- Nur MAC Adresse von Rechner C kann über einen Router hinweg nicht einfach mit Wireshark ermittelt werden
- Rechner C befindet sich in einem anderen lokalen Netzsegment und es ist daher überhaupt keine direkte Ethernet-Kommunikation möglich

Für die in SS22 aufkennen:

→ Tabellen zu 1/16 drc. anstreben

↳ 2 Tabellen können in Frage

→ Serialisierungszeit + Zeit der Warte Formel noch abstimmen

~ NTT Formel