

Zusammenfassung Datennetze 1

Mathis Hermann

December 28, 2022

Diese Zusammenfassung ist anhand der Lernziele aufgebaut. Dementsprechend sind nicht ganz alle Themen der Vorlesung enthalten. It's been a f*cking pain...

1 Übersicht über Datennetze

Client-Server Paradigma – Meiste Kommunikation; Daten auf Server; User können Daten auf Server bearbeiten

Peer-to-Peer Paradigma – Rechner kann Server und Client sein; Einfach aufzusetzen, weniger Komplexität, weniger Kosten; Keine zentralisierte Administration, nicht so sicher, nicht skalierbar

LAN und WAN – Es gibt verschiedene Typen von Netzen:
Kriterien:

- Kanalzugang
 - Multiaccess Netze
 - Punkt-zu-Punkt Netze
- Ausdehnung
 - LAN (sind immer Multiaccess Netze)
 - WAN (traditionell: Punkt-zu-Punkt Netze; neu auch Multiaccess Netze)

Begriffe

Begriff	Erklärung
Client	Wird ein- und ausgeschaltet; wechselt IP; stellt Anfrage an Server
Server	Ein Programm, das immer läuft; fixe IP; meistens DNS- Eintrag; läuft ununterbrochen und wartet auf Anfragen
LAN	Local-Area Network; Enthält Endgeräte; Medium-Access Control; <i>multi-access</i> Netz
WAN	Wide-Area Network; Keine Endgeräte; <i>point-to-point</i> Leitungen
Physikalische Darstellung	Definiert die physikalischen Verbindungen und Konfigurationen; Zeigt welches Gerät sich wo befindet und mit welchem verbunden ist
Logische Darstellung	Darstellung Ebene 3; Netze werden gezeichnet
Switch	Layer 2 Kommunikation; leitet Rahmen innerhalb eines Netzwerkes weiter
Router	Layer 3; Verbindet IP-Netze; leitet Pakete von einem Netz in ein anderes
Konvergierte Netze	Ein Netz für alle Dienste; single point of failure im Netz durch Komplexität; billiger im Unterhalt
Downstream	(Stärke der) Leitung von ISP zu Konsument
Upstream	(Stärke der) Leitung von Konsument zu ISP
QoS	Dienstgüte
Leitungs-vermittlung	Endgerät baut Leitung zu Ziel auf; feste Bandbreite wird reserviert in festem zeitlichen Rahmen; starke QoS; geringer Durchsatz (stark begrenzt in Bandbreite); sicher
Paket-vermittlung	Nachricht wird segmentiert; Pakete werden anhand der Informationen (Absender, Empfänger) verteilt; gute Ausnutzung der Bandbreite; nicht so sicher; viel Overhead bei Paketen - nicht so effizient

Netzwerkelemente und deren Funktion – Netzwerkelemente sind *Endgeräte* (Computer, Laptop, Drucker, Tablet); *Zwischengeschaltete Geräte* (Router, Switch) ; *Anschlussleitung* (Wireless Media, LAN Media, WAN Media)

Dedizierte und Konvergierte Netze – verschiedene Dienste über das Internet

Dedizierte Netze – Spezifische Netze für entsprechende Anwendungen; *Konvergente Netze* – Ein Netz für alle Dienste;

Logische und Physikalische Darstellung von Netzwerken – *Logische Sicht* Beschreibt welche IP-Netze (Benutzergruppen) es gibt; *Physikalische Sicht* Beschreibt wo welches Netzelement befindet

Grundanforderungen des Internets Kriterien für zuverlässige Netze:

- Fehlertoleranz (z.B. bei Leitungunterbruch)
- Skalierbarkeit
- Dienstgüte
- Sicherheit (e.g. Abhören oder Manipulation der Daten)

Anforderung verschiedener Anwendungen an die verschiedenen Parameter der Dienstgüte

Anwendung	Durchsatz	Verzögerung	Jitter	Paketvermittlung
Web	Hoch	Gering	Gering	Hoch
E-Mail	Gering	Gering	Gering	Gering
Sprache	Gering	Hoch	Hoch	Gering (VoIP)
Video	Mittel	Hoch	Hoch	Gering

Unterschied: Leitungsvermittlung und Paketvermittlung *Leitungsvermittlung* – Viele mögliche Pfade; ein Pfad wird gewählt pro Call; Wenn ein Call etabliert ist, geht alle Kommunikation über diesen Pfad; Eine Leitung ist bestimmt für die gesamte Dauer des Calls

Paketvermittlung – Viele verschiedene Pfade können verwendet werden, um individuelle Pakete zum Ziel zu routen; kein fixer Pfad; Pakete werden entsprechend des besten Pades zur Zeit geroutet

2 Konfiguration von Netzen

Zugänge zum Betriebssystem IOS von Cisco – Hauptsächlich über drei HW-Schnittstellen kann ein Router konfiguriert werden: 1) Console Port, blau: Management Port für lokale Konfiguration (Lokale Konsole, Serial), 2) Auxiliary Port, schwarz: Management Port für entfernte Konfiguration (“Remote out-of-band”, wird kaum mehr genutzt), 3) LAN Anschlüsse, gelb: Remote Management (“inband management”) mit SSH, Telnet.

Kommandos IOS – Drei verschiedene Arten von Kommandos in IOS: 1) Betriebskommandos (“ping”; Speichern von Konfiguration etc), 2) Konfigurationskommandos (zur Konfiguration eines Interfaces, Passwort etc.), 3) Statusabfragen.

Kommandostruktur von IOS – Es gibt vier verschiedene Modi im IOS: 1) User Mode, 2) Privileged Mode, 3) Global Config Mode, 4) Config Mode (und Sub-Menus).

```
Router>enable // exec zu privileged mode
Router#configure terminal // in Konfigurationsmodus
Router(config)#interface FastEthernet 0/0
// IF-Konfigurationsmodus – Interfaces konfigurieren

Router(config-if)# // Ebene zurueck
Router(config)# // Ebene zurueck
Router#disable // zurueck in den user mode
Router>

// Hilfe im IOS

Router# cl? // liste von commands, die mit ”cl” starten
clear clock

Router#clock set ? // next possible arguments
hh:mm:ss          Current Time

Router#clock set 19:50:00 ? // mehrere Argumente
<1-31>           Day of the month
MONTH             Month of the year
```

```

Router#clock set 19:50:00 25 June 2022

// Konfiguration auslesen
Router#show running-config
    // laufende Konfiguration aus RAM

Router#show startup-config
    // Abgespeicherte Konfiguration aus NVRAM

Router#show flash // Inhalt von Flashspeicher
Router#show version // Informationen zum aktuellen IOS
Router#show ip interface brief // Zustand aller IFs

```

Grundkonfiguration für Router und Switch Eine Grundkonfiguration beinhaltet:

- Hostname
- Einschränkung des Zugangs zu Netzelementen mit Passwörtern
 - Lokales Einloggen (Console)
 - Entferntes Einloggen (Telnet, SSH)
 - Übergang user mode zu privileged mode
- Rechtlicher Hinweis mit einem Banner

```

Router>enable
Router#configure terminal

// Hostname
Router(config)#hostname NAME
NAME(config)#

// Loeschen eines Konfigurationsbefehls
NAME(config)#no hostname NAME
Router(config)#

// PW fuer lokales Einloggen
Router(config)#line console 0
Router(config-line)#password PASSWORD

```

```

Router(config-line)#login

// PW fuer entfernes Einloggen (telnet)
Router(config)#line vty 0 4 // sesions 0-4
Router(config-line)#password PASSWORD
Router(config-line)#login
Router(config-line)# transport input telnet

// PW fuer privileged mode ohne Verschluesselung
Router(config)#enable password PASSWORD
// PW fuer privileged mode mit Verschluesselung
Router(config)#enable secret PASSWORD

// Verschluesselung aller PW in Konfiguration
Router(config)#service password-encryption

// Rechtlicher Hinweis
Router(config)#banner motd "
-----
Authorized Access Only!
-----
"

// Speichern von Konfiguration in NVRAM
Router#copy running-config startup-config

// Speichern auf TFTP-Server
Router#copy running-config tftp

// Speichern in Datei
Router#show running-config // copy & paste in externe Datei

// Loeschen von lokal gespeicherten Konfigurationen
// Router
Router#erase startup-config
// Switch
S1#erase startup-config
S1#delete flash:vlan.dat

```

```
// Router
    // interface konfigurieren
Router(config)#interface Fastethernet 0/0
Router(config-if)#ip address IF-ADRESSE NETZMASKE
Router(config-f)#no shutdown // IF einschalten

// Switch
S1(config)#interface vlan 1
S1(config-if)#ip address IF-ADRESSE NETZMASKE
S1(config-if)#no shutdown
```

Zustand von Leitungen abfragen und Erreichbarkeit von Netzelementen prüfen Wenn die IP-Adresse bekannt ist, kann mit ping geprüft werden, ob ein Netzelement erreichbar ist.

3 Netzwerkprotokolle und Datenkapselung

Protokoll Bei Rechnernetzen gibt es Regeln, wie Nachrichten auszutauschen sind:

- *Kodierung der Daten* (wie wird ein Zeichen kodiert)
- *Format für die Kapselung der Nachricht* (welche Informationen werden wie ausgetauscht)
- *Maximal erlaubte Grösse*
- *Zeitliche Abfolge* (Wie erfolgt der Zugang zum Übertragungskanal? Wie schnell darf ein Sender senden?)
- *Optionen*, auf die sich beide Seiten einigen können
- *Fehlerbehandlung*

Ein Protokoll ist ein *Satz von Regeln*, der die Form der Kommunikation hinreichend genau bestimmt, so dass Rechner verschiedener Hersteller effizient miteinander Daten austauschen können.

Protokolle im TCP/IP-Modell TCP/IP ist einer der meist angewendeten Protokoll-Stapel. Dieser beinhaltet verschiedene Protokolle und deren Integration.

Schicht	Protokolle
Application Layer	DNS (Name System), DHCP (Host Config), SMTP (Email), FTP (File Transfer), HTTP (Web)
Transport Layer	UDP, TCP
Internet Layer	IP, ICMP (IP Support), OSFP (Routing Protocols)
Network Access Layer	ARP, PPP, Ethernet

Standardisierungsbehörden

- The Internet Architecture Board (IAB)
- The Internet Engineering Task Force (IETF) – Standardisiert viele Protokolle
- Internet Assigned Numbers Authority (IANA) – vergibt IP Adressen
- The Institute of Electrical and Electronics Engineers (IEEE) – kontrolliert Protokolle in der unteren Schicht
- The International Standardization Organization (ISO)

Aufgaben der Schichten im OSI-Modell

#	Schicht	Aufgabenbereich
7	Anwendung	Stellt die Dienste und Funktionalitäten für den Anwender bereit
6	Darstellung	Verwaltet die Darstellungsinformation des Dateninhalts (Komprimierung, Verschlüsselung)
5	Sitzung	Verwaltet die verschiedenen Sitzungen zwischen den Endpunkten
4	Transport	Stellt der Anwendung zwei Dienste für die Übertragung der Daten von der Quelle zum Ziel bereit (Endgerät zu Endgerät)
3	Netzwerk	Wegleitung vom Netz der Quelle zum Zielnetz
2	Sicherung	Legt fest, wie die Daten innerhalb eines Netzes ausgetauscht werden
1	Physik	Legt die elektrischen Signalformen für die Übertragung innerhalb eines Netzes fest

Mechanismen beim Versenden von Daten Grosse Datenblöcke verschiedener Teilnehmer werden beim Sender segmentiert und "gemultiplext" über eine Leitung übertragen. Jede Leitung legt eine maximale Grösse eines einzelnen Rahmens (MTU = maximal transmission unit) fest. Datenkapselung: Protocol Data Unit (PDU) = [Header, Payload]

Kapselung verschiedener Protokolle beim Sender – Die Sendeseite fügt einen Header hinzu und übergibt die PDU der darunter liegenden Schicht.

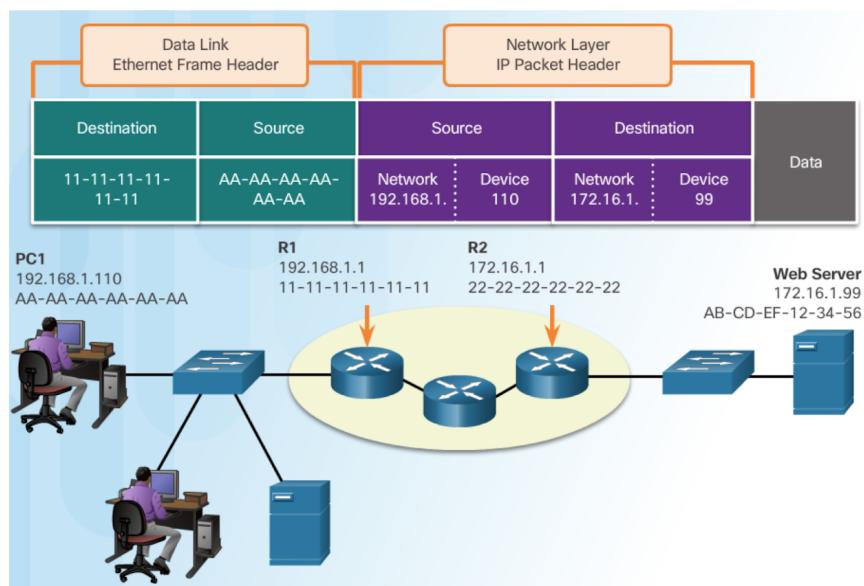
Entkapselung beim Empfänger – Die Empfangsseite wertet den Header aus, entfernt ihn wieder und übergibt die Payload der darüberliegenden Schicht.

Adressen in den verschiedenen Schichten

Abläufe beim Senden einer Dateneinheit Ziel im gleichen Netz – Schicht 2 MAC-Adressen (Destination, Source), Schicht 3 IP (Source, Destination), Data; Header bleiben gleich

Ziel in anderem Netz – Schicht 2 MAC-Adressen (Destination, Source), Schicht 3 IP (Source, Destination), Data; Schicht 3 Header bleibt gleich, Schicht 2 Header wird ausgetauscht.

- Die Schicht 3 geht von Ende zu Ende
- Die Schicht 2 wird beim Übergang von einem Netz in ein anderes neu gebildet



4 Schichten 1 und 2: Network Access

Aufgaben Schicht 1 Die physikalische Schicht (Layer 1) bietet der Sicherungsschicht (Layer 2) den Dienst an, Bits über einen Link zu übertragen. Ethernet umfasst Layer 1 und Layer 2.

Wichtigste Physikalische Schnittstellen an Netzelementen Folgende physikalische Komponenten werden standardisiert:

- Netzwerkanschlüsse (Network Interface Card – NIC)
- Übertragungsmedien (Leitungen)
- Steckverbinder
- Elektrische Signale
- Kodierung

Drei wichtigste Übertragungsmethoden und deren Eigenschaften

- *Synchrone Übertragung* – Das Taktsignal wird mit dem Datensignal mitübertragen
- *Asynchrone Übertragung* – Nur das Datensignal wird übertragen. Der Empfänger benötigt eine *Taktrückgewinnung*

Im Allgemeinen wird asynchron übertragen. Der Empfänger muss das Taktsignal aus dem Empfangssignal zurückgewinnen. Das Ziel ist es, 1) so viele Daten pro Zeiteinheit wie möglich und 2) so weit wie möglich zu übertragen. Die Dämpfung elektrischer Signale in einem Leiter nimmt i.A. mit der Frequenz zu.

Das Empfangssignal ist ein analoges Signal. Der Empfänger entscheidet um welches Symbol es sich handelt. Dabei können Fehler auftreten.

Wichtigste Kabel und wie sie eingesteckt werden

- *Unshielded Twisted-Pair Cable* – Verschiedene Kabel mit verdrillten Kupferadern
- *Shielded Twisted-Pair Cable* – Verschiedene Kabel mit verdrillten Kupferadern; abgeschirmt
- *Coaxial cable*

Medium	Eigenschaften	Vorteile	Nachteile
Kupfer	Twisted / Untwisted	Billiges Material	Dämpfung hoch bei hohen Frequenzen
Glas	Multimode (mehrere Pfade für das Licht), Singlemode (Pfad in eine Richtung)	Störungs-unabhängig, dämpfungs-arm	Teure Hardware
Luft	Signal wird auf Träger moduliert	Mobilität	Hohe Dämpfung bei hohen Frequenzen, alle können Signale empfangen und mithören, Interferenzen mit anderen Sendern, beschränkte Bandbreite wird geteilt

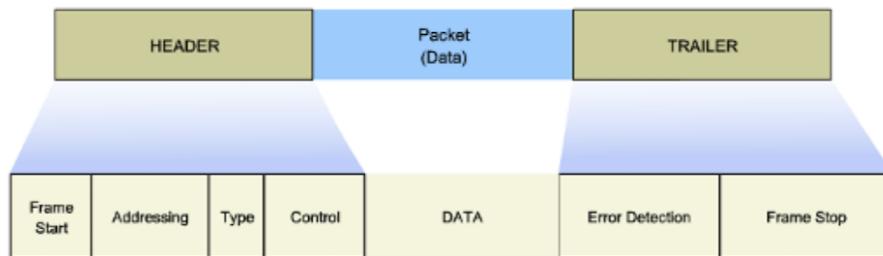
Leitungscode Der Sender wandelt das binäre Signal zuerst in einen dem Kanal angepassten Leitungscode um. Der Leitungscode legt fest, wie das Signal übertragen wird. Dabei ist es wichtig, das Signal dem Übertragungsmedium entsprechend anzupassen, um eine optimale Übertragung zu erreichen.

Aufgaben der Sicherungsschicht (data link layer)

- Rahmenbildung um Pakete zu begrenzen
- Regelung des Zugriffs auf den Übertragungskanal
- Fehlererkennung
- Optional (von Ethernet nicht unterstützt)
 - Aufbau, Halten und Auflösen einer Verbindung
 - Fehlerkorrektur durch Übertragungswiederholung
 - Flusssteuerung

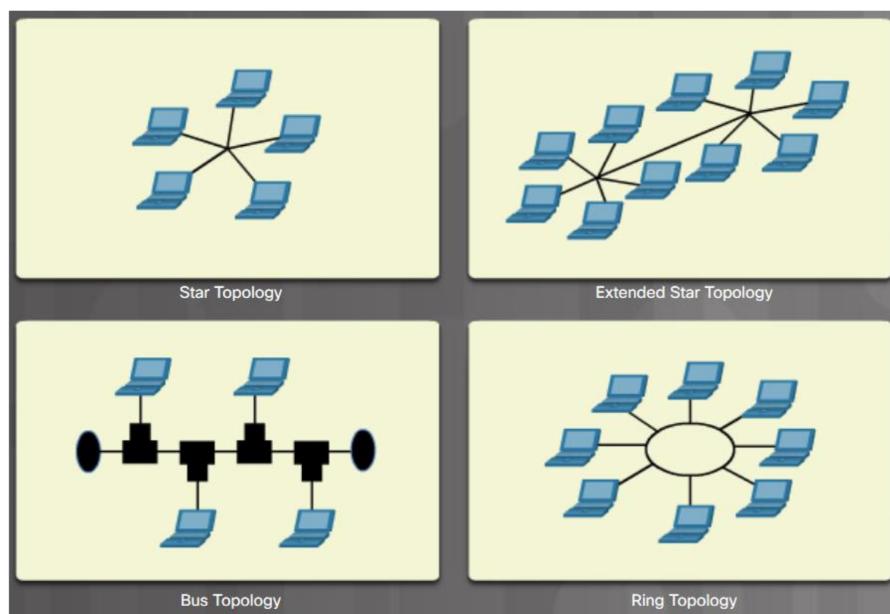
Dafür werden Protokolle der Sicherungsschicht verwendet: *LAN* – Ethernet2, Ethernet IEE 802.3, TokenBus IEEE 802.4, Token Ring IEEE 802.5, WLAN IEEE 802.11; *WAN* – HDLC (High-Level Data Link Control), PPP, FrameRelay

Allgemeine Struktur eines Schicht-2-Rahmens Die Schicht 2 legt die Felder des Rahmens und die maximale Länge der Daten (Maximum Transmission Unit, MTU) in einem Rahmen fest.



Verschiedene logische Topologien in LAN

- Stern
- Erweiterte Stern
- Bus
- Ring



LAN Ursprünglich Shared Medium. Viele Stationen benützen denselben Kommunikationskanal. Weiterentwicklung: *switched networks*

Half-Duplex – Ein Endgerät kann zu einem Zeitpunkt entweder senden oder empfangen (Ethernet mit einem Hub; Wireless Access Point)

Half-Duplex – Beide Enden können gleichzeitig senden und empfangen (Ethernet mit Switches).

Maximum Transmission Unit

- Jedes L2-Protokolldefiniert eine MTU
- Ein Rahmen darf nicht grösser sein als die MTU; ggf. muss das Schicht 3 Protokoll einen Rahmen fragmentieren, wenn er für einen Link zu gross ist
- Typische MTU: 1500 Bytes
- Grund: Ein Benutzer darf einen Kanal nicht zu lange belegen damit andere auch senden / empfangen können

Verschiedene logische Topologien in WAN

- Punkt-zu-Punkt – dedizierte Leitungen
- Point-to-Multipoint – Hub and Spoke, partial mesh; Hub Standort mit mehreren Standorten verbunden
- Full Mesh – Alle Geräte können miteinander kommunizieren
- Ring – Weniger anfällig auf Fehler wegen Verbindung im Kreis; kein single-point-of-failure
- Stern – nur zentraler Hub kann single-point-of-failure werden

Kategorien des Kanalzugriffsverfahren *Controlled Access* – Jede Station hat eine Zeit, die für sie zum Senden reserviert ist. In dieser Zeit darf nur sie senden (Token Ring, FDDI).

Contention-based Access – Als Wettbewerb: Der schnellere darf senden. Es ist ein Verfahren definiert, wie vorzugehen ist, wenn zwei Stationen gleichzeitig senden.

5 Ethernet

OSI-Schichten von Ethernet abgedeckt – Ethernet deckt die Schichten 1 (Physikalisch) und 2 (Data Link, Sicherung) ab.

Aufgaben der MAC-Schicht

- Kapselung der Daten
 - Markierung des Beginns eines Rahmens
 - Adressierung
 - Fehler Detektion
- Kontrolle des Kanalzugangs
 - Platzierung der Rahmen auf den Kanal
 - Fehlerbehandlung bei Kollisionen

Physikalische Unterlagen von Ethernet

- Coax N-Style – 500m
- Coax BNC – 185m
- UTP RJ45 – 100m
- STP mini-DB-9 – 25m
- MM Fiber SC – 220-550m
- MM Fiber SC – 550-5000m

Topologie vom ursprünglichen Ethernet

- Offen
- Einfachheit, einfacher Unterhalt, Zuverlässigkeit
- Neue Technologien integrieren, ohne Alte ersetzen zu müssen.
- Günstig in Installation und Aufrüstung

Mit Koaxkabel ("Bus") wurde das Ethernet ursprünglich entwickelt.

Kollisionsdomänen – Kollisionsdomänen werden unterteilt nach Geräten, die gleichzeitig senden / empfangen können. Wenn zwei Rechner in der gleichen Kollisionsdomäne sind, kann je nur einer der beiden gleichzeitig senden / empfangen.

Kollisionsdomänen können mit Hub erweitert (mehr Geräte einschliessen) und mit Switch oder Bridge in mehrere aufgetrennt werden.

Ethernet-Adressen – Allgemein werden entsprechend dem Adressaten drei Arten von Paketen unterschieden

- *Unicast* – Ziel ist ein Rechner
 - Unicast-Adressen – LSB des ersten Byte ist Null
- *Multicast* – Ziel ist eine Gruppe von Rechnern oder NIC
 - Die IP-Adressen von 224.0.0.0 - 231.255.255.255 repräsentieren Multicast-Gruppen
 - Wenn sich eine Anwendung an einer Multicast-Gruppe anmeldet, wird dem Rechner eine IP-Adresse vom Multicast-Bereich zugeordnet
 - Zuordnung geschieht auf Schicht 3. Schicht 2 wird nachgezogen (Für IP-MC muss auch MAC-Adresse gebildet werden)
- *Broadcast* – Ziel sind alle NIC in einem Netz
 - Ziel-Adresse lautet FF:FF:FF:FF:FF:FF

Aufbau MAC-Adresse – MAC-Adressen bestehen aus zwei Teilen (je 3x 2 Oktet). Somit werden die ersten 6 Oktet der dem Hersteller (Organizationally Unique Identifier, OUI) vergeben. Der zweite Teil kann der Hersteller frei vergeben (Vendor Assigned; NIC, Interfaces)

Es gibt 2^{48} mögliche MAC-Adressen. Eine Organisation kann also 2^{24} verschiedene MAC-Adressen generieren.

Normen für Ethernet Als Standards werden hauptsächlich *IEEE 802.3* und *Ethernet2* verwendet.



Die Definition eines Ethernet-Rahmens impliziert, dass sie eine MTU (1500 Bytes) und eine Minimum Transmission-Unit (46 Bytes).

Anhand Byte 13 und 14 kann unterschieden werden nach welchem Standard, der Rahmen aufgebaut ist:

- Inhalt > 0x0600: Ethernet2
- Inhalt < 0x0600: IEEE 802.3

Das Netzwerk-Interface prüft bei jedem Rahmen, wie er interpretiert werden muss. Bei IEEE-Rahmen folgt auf das Feld Length/Type das Feld LLC (3 Byte). LLC enthält den Protokollcode für das innere Protokoll der Payload. Alle IEEE 802.n-Normen haben das gleiche LLC-Feld.

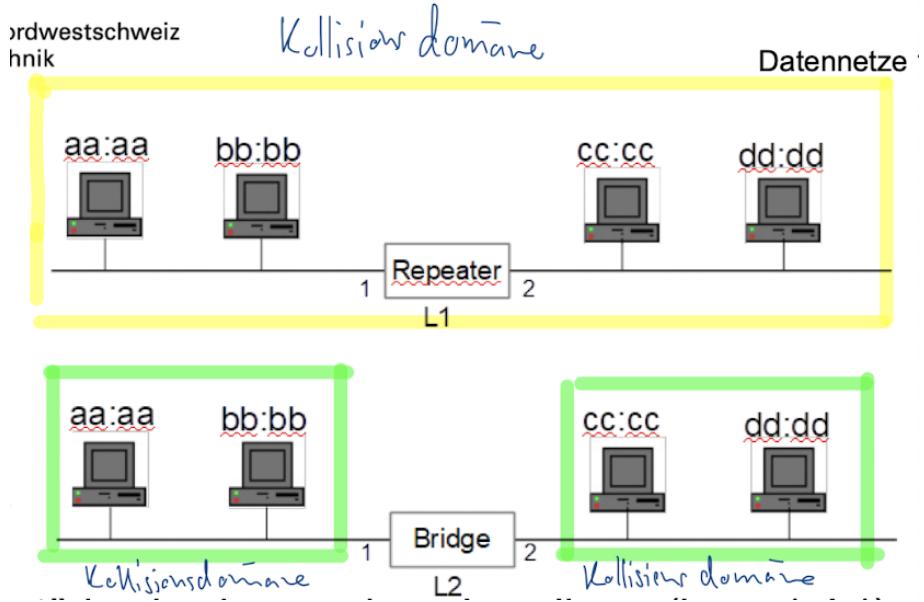
Kanalzugriffsverfahren für Ethernet Carrier Sense Multiple Access / Collision Detection: Eine Station, die senden möchte, hört zuerst, ob der Kanal frei ist. Wenn Kanal frei ist, darf gesendet werden. Dabei kann es zur Kollision kommen.

Eine Kollision muss sicher von jeder Station detektiert werden. Bei einer Kollision: 1) Senden des Jam-Signals; 2) Rückzug vom Kanal; 3) Station generiert Zufällige n und wartet $n * t_s$ wobei t_s die Slotzeit ist. Dafür muss jeder Ethernet-Rahmen eine minimale Länge haben.

Repeater und Bridge Ein *Repeater* ist ein elektrischer Verstärker in einem "shared medium". Segment 1 und 2 bleiben Verbunden und bilden somit eine Kollisionsdomäne.

Eine *Bridge* macht Zwischenspeicherung von Rahmen in Layer 2. Somit wird in zwei Kollisionsdomänen aufgetrennt.

Multipoint Bridge – Switch: Aufteilung in verschiedene Kollisionsdomänen.



MAC-Tabelle – Lernen der MAC-Adressen: Switch merkt sich für jeden ankommenden Rahmen den *Eingangsport* und die *Absenderadresse*. Die Absenderadresse wird in die entsprechende Zeile eingefüllt. Nicht mehr auftretende MAC-Adressen werden wieder gelöscht.

Anhand der Tabelle werden ankommende Rahmen weitergeleitet.

Hub und Switch – Weiterleitung von Ethernet-Rahmen

Auf Hub muss geprüft werden, ob Bus frei, dann kann gesendet werden. Wenn ein Switch verwendet wird, können alle senden und empfangen – Switch handelt den Verkehr.

Ein Switch hat vier Operationen: 1) Learning (MAC-Tabelle), 2) Aging (nach ca. 2 Min ohne Auftreten wird ein Eintrag gelöscht), 3) Flooding, 4) Selective Forwarding

Flooding – Wenn Zieladresse von ankommendem Rahmen nicht in MAC-Tabelle: Rahmen wird an alle Ports (ausser Eingangsport) weitergeleitet.

Selective Forwarding – Zieladresse ist in MAC-Tabelle: Rahmen wird nur an den entsprechenden Port weitergeleitet.

Ablauf ARP Wenn der Quellrechner die Ziel-Adresse, aber nicht die Ziel-MAC-Adresse kennt wird die Zuordnung der MAC-Adresse zu einer IP-Adresse mittels *Address Resolution Protocol* gemacht. Rechner und Router speichern die MAC-Adresse con Ziel-IP-Adressen lokal in der ARP Tabelle. Nach entsprechender Zeit werden die Einträge in der Tabelle entfernt (gealbert).

Probleme – Zu viel Broadcastverkehr; ARP-Spoofing (Attacker gibt sich als Default Gateway aus und kann so allen Verkehr mitlesen)

6 Netzwerkschicht

Von einem Netz ins andere und Protokolle IPv4, IPv6, AppleTalk, ICMP, OSPF und andere werden angewendet. Daten von Schicht 2 werden in Schicht 3 gekapselt.

Aufgaben Schicht 3

- Adressierung
- Kapselung in Senderichtung
- Wegleitung – Routing durch viele Netze
- Entkapselung beim Empfang
- Fehlerbehandlung

Eigenschaften IP Das Protokoll *IP* ist:

- *verbindungslos* – Es werden IP-Pakete bei der Quelle los geschickt ohne, dass das Ziel davon weiss
- *best effort* – Das Netz leitet soviele Pakete weiter, wie gerade möglich; Pakete werden weggeworfen bei Überlauf
- *Media independent* – Läuft über allen möglichen Schicht 2 Protokollen (Ethernet, TokenRing, PPP, ATM) und Schicht 1 Medien

Header: IPv4 – Der Header wird mit Zeilen à vier Byte dargestellt.

- *Version* – IP Version 4
- *IP Header Length* – Header hat nicht immer Länge von 20 Bytes; wird in Anzahl Zeilen, $n * 4$ Bytes angegeben
- *Differentiated Services* – ursprünglich vorgesehen, Verkehr zu priorisieren – wird nicht angewendet; kann in lokalen Services für QoS für e.g. Sprachanwendungen verwendet werden
- *Total Length* – Länge des gesamten Paketes
- *Identification, Flag, Fragment Offset* – werden (selten) verwendet, wenn Paket grösser als zulässige länge für Schicht 2 Protokoll (e.g. 1500 Bytes für Ethernet); Oft machen Implementationen der Transport Schicht (Layer 4) Segmente mit einer maximalen Länge von 1460 Bytes;

- *Time-to-live* – Zahl dekrementiert bei jedem Hop; wenn TTL=0 wird das Paket verworfen und über ICMP Meldung an Absender; wird benötigt, damit Pakete nicht unendlich lange kreisen
- *Protocol* – gibt an, welchem Protokoll ein angekommenes IP-Paket übergeben werden soll
- *Header Checksum* – Paket wird verworfen, wenn Checksum nicht korrekt
- *Source IP Address* – Adresslänge 4 Bytes
- *Destination IP Address* – Adresslänge 4 Bytes
- *Options* – wird oft nicht verwendet;
- *Padding*

Header: IPv6

- *Version* – Inhalt ist 6
- *Traffic Class (4 bit)* – ursprünglich vorgesehen, Verkehr zu priorisieren – wird nicht angewendet; kann in lokalen Services für QoS für e.g. Sprachanwendungen verwendet werden
- *Flow Label (20 bit)* – Spezial-Dienst für Echtzeitanwendungen; Information an die Router, den selben Pfad für den Strom beizubehalten; Pakete müssen an Ziel nicht geordnet werden
- *Payload Length (16 bit)* – Länge des ganzen IP-Paketes; exklusive Header und Extension Header
- *Next Header (8 bit)* – Gibt das Protokoll an, das auf den IPv6-Header folgt
- *Hop Limit (8 bit)* – Wird bei jedem Router dekrementiert. Erreicht es 0 wird das Paket verworfen und es wird eine ICMPv6 Meldung an Quelle gesendet (Paket nicht an Ziel angekommen)
- *Source IP Address (128 bit)*
- *Destination IP Address (128 bit)*

Was macht ein Router mit einem eingehenden Paket? – Paket wird anhand der Routing-Tabelle weitergeleitet

Funktion von Default Gateway – Ein Default Gateway muss an jedem Rechner (der nach aussen kommunizieren soll), auf jedem Switch (der aus anderen Netzen angesprochen werden soll) und auf jedem Router konfiguriert werden.

Das Default Gateway wird beim Rechner entweder manuell oder per DHCP-Server definiert.

Auf Switch: S1(config)#ip default-gateway 192.168.10.1

Funktion von Routing-Tabelle – Es kann zwischen Routing-Tabelle auf Rechner und Router unterschieden werden.

In der Routing-Tabelle auf dem Rechner wird das Loopback Interface (127.0.0.1), das lokale Netz und eine Default-Route eingetragen. Für die Default-Route muss das Default Gateway konfiguriert sein. Wird entweder durch DHCP Server oder manuell gesetzt.

In der Routing-Tabelle auf einem Router werden direkt angeschlossene Netze, entfernte Netze (statische Einträge; dynamische Routingprotokolle) und die Default Route eingetragen

Aufbau Router; Prozess während Aufstarten Ein Router hat:

- CPU – Weiterleitung Pakete; rechnet Routing-Algorithmus
- RAM – IOS wird nach Aufstarten in RAM geladen; enthält running-config; enthält Routing-Tabelle; enthält ARP-cache
- ROM – Diagnostic Software für Tests bei Aufstarten (POST: Power On Self Test); Speichert bootstrap BefehleM
- Flash – Permanente Speicherung IOS
- NVRAM – nichtflüchtiger Speicher für startup-config
- mindestens 2 Netzwerk-Interfaces – Anschlüsse

Beim Aufstarten wird 1) POST durchgeführt, 2) die bootstrap Befehle geladen, 3) das IOS lokalisiert und geladen, 4) und das configuration file lokalisiert und geladen.

Die Konfiguration wird entweder aus dem NVRAM oder von einem TFTP-Server geladen.

```
Router#show ip interface brief // IF Zustand  
Router#show ip route // Routing-Tabelle
```

7 IP-Addressierung

IPv4: Adresse und Subnetzmaske

- *Netzadresse* – Hat lauter Nullen im Hostteil (erste Adresse des Netzes)
- *Broadcastadresse* – Hat lauter Einsen im Hostteil (letzte Adresse)
- *Hostadressen* – alles zwischen Netz- und Broadcastadressen

Rechner- und Router-IFs erhalten *immer* eine Hostadresse.

IPv4: Unicast, Multicast und Broadcast – Es gibt drei verschiedene Arten von Ziel-Adressen:

- *Unicast* – Ein IP-Paket geht an genau ein IF. In einem /24-er Netz sind dies die Adressen 1 bis 254
 - Werden auf Rechner entweder über DHCP-Server oder manuell eingerichtet
- *Broadcast* – Ein Rechner stellt eine Anfrage mit lauter Einsen im Hostteil (255)
- *Multicast* – Pakete an eine Gruppe von Rechnern senden; 224.0.0.0 - 239.255.255.255; 224.0.0.0 - 224.0.0.255 nur link-lokal und werden nicht geroutet; 224.0.1.0 - 239.255.255.255 sind globale Multicast Adressen
 - Hilft bei Verteilung eines Datenstroms; Sender sendet Pakete nur einmal und Switch/Router leiten Pakete an jeweilige Ports weiter

Unterscheiden: Öffentliche und Private Adressen – Es sind drei Adressräume für private Verwendung vorgesehen: 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16

Private Adressen werden im öffentlichen Internet nicht weitergeleitet.

Spezielle Adressen

- 127.0.0.1 – Loopback (127.0.0.1/8 ist reserviert)
- 169.254.0.0/16 – Link-lokale Adressen; können automatisch dem "Local Host" zugewiesen werden
- 192.0.2.0/24 – Unterricht und Dokumentation
- 240.0.0.0/4 – ist reserviert und darf nicht gebraucht werden

Klassenbezogene und Klassenlose Adressierung – Ursprünglich wurde der IPv4 Adressbereich in fünf Klassen unterteilt (A-E). Mit der Netzklasse wird nicht die tatsächliche Grösse eines Netzes angegeben, sondern wie viele Adressen es umfassen kann.

- A – 0.0.0.0 - 127.255.255.255; 0 + 7 bit Netz, 24 bit Host; 128 Netze; 16'777'214 Hosts pro Netz
- B – 128.0.0.0 - 191.255.255.255; 10 + 14 bit Netz, 16 bit Host; 16'384 Netze; 65'534 hosts
- C – 192.0.0.0 - 223.255.255.255; 110 + 21 bit Netz, 8 bit Host; 2'097'150 Netze; 254 Hosts pro Netz
- D – 224.0.0.0 - 239.255.255.255 (Multicast Gruppe); 1110 + 28 bit Multicast-Gruppen-ID
- E – 240.0.0.0 - 255.255.255.255 (reserviert; wird nicht genutzt); 1111 + 28 bit

Mittlerweile ist diese Technologie veraltet und es wird mit Subnetzmasken definiert, welchen Adressbereich ein Netz abdeckt. Dies nennt man klassenlos oder Classless Inter-Domain Routing (CIDR).

IPv6: Adressierung, Struktur mit Präfix, Subnet-ID und Interface-ID Mit der Einführung von IPv6 wird 1) ein grösserer Adressraum eingeführt 2) hierarchische Vergabe der Adressen unterstützt 3) eine feste Headerlänge definiert 4) das ICMP verbessert und 5) Network Address Translation (NAT) abgeschafft.

IPv6-Adressen bestehen aus einem Prefix und einer Interface ID. Diese sind definiert durch ”/n” nach der Adresse, wobei es n-bit des Prefixes definiert. 2001:0DB8:000A::/64 entspricht also 2001:0DB8:000A:0000 (prefix) :0000:0000:0000:0000 (Interface ID)

Übergang IPv4 zu IPv6 – Mit tunneling von IPv6-Inseln über ein IPv4-Netz können IPv6-Netze miteinander sprechen.

Dual-Stack ist, wenn IPv4 und IPv6 koexistieren. Dabei laufen beide Protokolle parallel. Wenn beide Enden IPv6 unterstützen, läuft Kommunikation über IPv6, ansonsten über IPv4.

IPv6 Adressen

- *Unicast* – Ein Empfänger
 - Global – 2000::/3; weltweit eindeutig; Im Internet geroutet
 - Link-Local – werden nur lokal verwendet; FE80::/10
 - Loopback – Logisches IF zum eigenen IPv6 Stack; ::1/128
 - Unspecified – kann verwendet werden, wenn Quelle irrelevant ist
 - Unique/Site Local – Nicht verwenden für Kommunikation ins Internet; Für Kommunikation in Firmennetzen
 - Embedded – IPv4 kompatible Adressen für IPv4-IPv6 Translation
- *Multicast* – eine Gruppe von Empfängern
- *Anycast* – Eine unicast Adresse, die Gruppen von Network IFs zugewiesen wird; Das Paket wird an das nächste IF weitergeleitet

IPv6 Unicast Adressen

- *Global Routing Prefix* – Regional Internet Registry vergibt Adressen aus dem Adressraum 2000::/3; ISP erhält /32er-Adressbereiche; ISP geben Kunden /48er oder kleinere Netze;
- *Subnet ID* – Adress-Teil vom 49. bis zum 64. bit
- *Interface ID* – 64 letzte bit; entsprechen Host-Teil von IPv4; Rechner kann mehrere IPv6-Adressen auf einem physikalischen IF haben

Auf Cisco Router muss IPv6-Routing eingeschaltet werden:

```
// IPv6 Routing einschalten
R1(config)#ipv6 unicast-routing

// Interface fa0/0 mit IPv6 Adresse konfigurieren
R1(config)#interface fa0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown

// Kontrolle
R1#show ipv6 interface brief
R1#show ipv6 route // Routing Tabelle
    // Spezifische Adresse pingen (Verbindung testen)
R1#ping 2001:db8:acad:10::5
```

ICMPv4/v6 – Mit dem Internet Control Message Protocol kann überprüft werden, ob in einem Netzwerk das Routing soweit stimmt, dass Rechner A den Rechner B in einem anderen Netz erreichen kann.

Die wichtigsten ICMP Meldungen sind:

- Host confirmation mit echo request und echo response – feststellen ob ein Host erreichbar ist (ping, traceroute)
- Destination or Service Unreachable – Router sendet Nachricht an Absender, wenn er ein Paket nicht weiterleiten kann, weil er keinen passenden Eintrag in der Routingtabelle findet.
- Time exceeded – TTL auf null; Fehlermeldung zurück an Absender
- Route redirection – Router kann einem direkt angeschlossenen Rechner sagen, dass es einen schnelleren Weg gibt als über diesen Router

Protokoll-Stack von ICMPv4 ist [L2-Header | IP | ICMP] – L2 Header ist meistens ein Ethernet Header; ICMP ist Schicht-3-Protokoll (benutzt Dienste von Schicht 3 aber nicht höhere).

Bei ICMPv6 wird zudem 1) Router Solicitation Meldungen (RS), 2) Router Advertisments (RA) 3) Neighbour Solicitation (NS) und 4) Neighbour Advertisement (NA) durchgeführt. RS und RA werden für die Autokonfiguration bei IPv6 verwendet. NS und NA werden für Address resolution (IPv4 ARP) und Duplicate Address Detection verwendet.

Neighbour Solicitation für Adress Resolution – Station sendet eine ICMPv6 NS Meldung zu einer IPv6 Adresse, um zugehörige MAC-Adresse zu finden.

8 Unterteilen und Zusammenfassen von IP-Netzen

Da der IPv4-Adressraum rasch knapp wurde, hat man begonnen Adressraum wo möglich zu sparen. Netze wurde nur so gross gemacht, wie nötig – man hat begonnen IPv4-Netze zu unterteilen.

Zudem ist es sinnvoll, nicht zu grosse Netze zu haben. Jede Station verursacht Broadcast-Anfragen. Viele Hosts in einem Netz machen viel Broadcast-Verkehr.

Mit der Unterteilung von IPv4-Netzen kann dem entgegengewirkt werden.

IPv4-Netz in gleich grosse Subnetze unterteilen – Netze können halbiert werden, um in gleich grosse Subnetze unterteilen. Beispiel: 192.68.1.0/24 in zwei Netze

- 192.68.1.0/25
- 192.68.1.127/25

Somit wurde das ursprüngliche Netz in zwei gleich grosse Subnetze unterteilt. Anzahl Subnetze pro Netz ist jeweils eine 2er-Potenz.

Anzahl nutzbare Host-Adressen ist $2^{32-n} - 2$ – also 2er-Potenz minus Netzadresse und Broadcast-Adresse

IPv4-Netz in verschiedenen grosse Subnetze unterteilen – Für WAN-Netze werden /30er Netze verwendet! Diese werden oft ans Ende des Adressraumes gesetzt.

Berechnungen mit Subnetzmasken variabler Länge Geeignete Subnetzmasken bei variabler Grösse:

- Bis 126 Hosts – 255.255.255.128
- Bis 62 Hosts – 255.255.255.192
- Bis 30 Hosts – 255.255.255.224
- Bis 14 Hosts – 255.255.255.240
- Bis 6 Hosts – 255.255.255.248
- Bis 2 Hosts – 255.255.255.252 (kann für WAN verwendet werden)

Beispiel:

Netzname	#	Subnetzmaske	Netzadresse	Broadcast-Adresse
Sales Office	40	255.255.255.192	172.16.0.0	172.16.0.63
Technical Support	35	255.255.255.192	172.16.0.64	172.16.0.127
Engineering	30	255.255.255.192	172.16.0.128	172.16.0.191
HR	23	255.255.255.224	172.16.0.192	172.16.0.223
Executive Mgmt	10	255.255.255.240	172.16.0.224	172.16.0.239
WAN1	-	255.255.255.252	172.16.0.240	172.16.0.243
WAN2	-	255.255.255.252	172.16.0.244	172.16.0.247
WAN3	-	255.255.255.252	172.16.0.248	172.16.0.251
WAN4	-	255.255.255.252	172.16.0.252	172.16.0.255

Daraus resultieren die Netze:

- 172.16.0.0/26
- 172.16.0.64/26
- 172.16.0.128/26
- 172.16.0.192/27
- 172.16.0.224/28
- 172.16.0.240/30
- 172.16.0.244/30
- 172.16.0.248/30
- 172.16.0.252/30

Netze in IP-Adressräumen zusammenfassen Die Zusammenfassung muss den gleichen Adressraum bedecken, wie die einzelnen Netze.

Adressraum sinnvoll einteilen und planen Zudem wird empfohlen bei der Belegung eines Adressraumes nach einem ähnlichen Muster zu folgen. Beispiel:

Engeät	Von	Bis
Router / Switch	.1	.15
Andere Netzwerkgeräte	16	.23
Server	.24	.31
Clients	.32	.240
Reserve	.241	.255

Entwurfsleitlinien für IPv6 – IPv6-Netze immer gleich gross wählen:
/64

9 Transportschicht

Schicht 4 sorgt dafür, dass der Sender, so langsam sendet, wie die langsamste Leitung senden kann.

Aufgaben der Transportschicht (Schicht 4)

- Multiplexierung
- Falls grosse Datenblöcke erwartet werden:
 - Segmentierung und Wiederzusammensetzen von grossen Datenblöcken
 - Sicherung der Übertragung (fehlerfreie Übertragung)
 - Flusssteuerung

Multiplexierung – Die Datenströme werden beim Empfänger entsprechend der Anwendung zugeordnet. Gewisse Anwendungen (e.g. für Filetransfer) senden / empfangen grosse Datenblöcke.

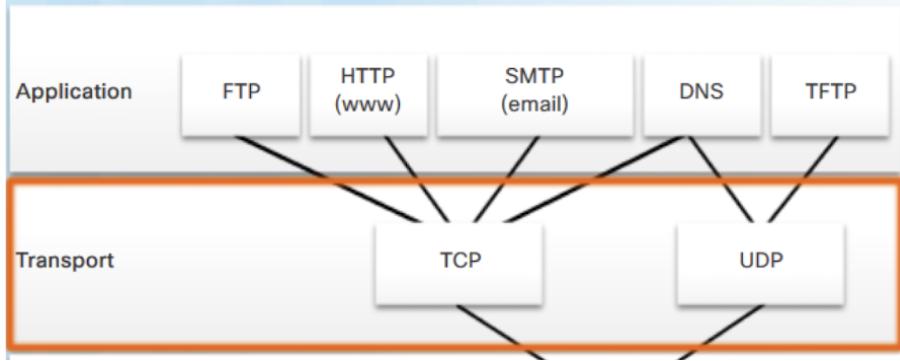
Segmentierung – Wenn ein Datenblock grösser als die MSS (Maximum Segment Size) ist, segmentiert das Transport-Protokoll die Daten und verpackt jedes Segment einzeln in ein IP-Paket. Segmente werden beim Zielrechner wieder zusammengesetzt.

Anforderungen von Anwendungen an die Kommunikation Es gibt Anwendungen, welche grosse und andere die kleinen Datenblöcke senden. Dafür werden zwei Protokolle unterschieden:

Protokolle in Schicht 4 Am verbreitetsten für Schicht 4 sind die Protokolle TCP und UDP.

TCP – Verbindungsorientierte, fehlerfreie Übertragung; viel Overhead – kann also langsam werden; Anwendungen benötigen einen zuverlässigen Dienst

UDP – Anwendungen mit Nachrichten kürzer als die MSS; verbindungslos – schnell; Jedes Datagramm wird am Ziel einzeln und sofort der Anwendung abgeliefert;



9.1 TCP

TCP baut eine bidirektionale (verbindungsorientierte) Verbindung zwischen Client und Server auf. Dabei werden zwei Datenströme ($A \leftarrow B$ und $A \rightarrow B$) vorbereitet und kontrolliert.

TCP segmentiert grosse Blöcke, nummeriert sie, bestätigt empfangene Segmente, wiederholt nicht bestätigte Segmente, ordnet die Reihenfolge empfangener Segmente und regelt die Geschwindigkeit der Übertragung.

Wenn TCP verwendet wird, wird – gesteuert durch das Feld *Control* – eine bidirektionale Verbindung aufgebaut. Dabei werden 1) die Maximum Segment Site (MSS), 2) Selective Acknowledgement (Ja/Nein) und 3) die Skalierung der Window-Size vereinbart.

TCP (Header und Bedeutung der Felder)

- Source Port (16 Bit) – Bezeichnung der Anwendung auf der Quellrechner
- Destination Port (16 Bit) – Bezeichnung der Anwendung auf der Empfangsrechner
- Sequence Number (32 Bit) – Zählen der Bytes, welche gesendet werden
- Acknowledge Number (32 Bit) – Zählen der Bytes, die empfangen werden und Bestätigung bei ACK
- Header Length (4 Bit) – Länge des Headers
- Reserved (6 Bit) –
- Control Bits (6 Bit) – 6 Bits für 6 verschiedene Flags: Urgent (URG), Acknowledgement (ACK), Push (PSH), Reset (RST), Synchronize Sequence Numbers (SYN), Finish (FIN)

- Window (16 Bit) – gibt an, wie viele Bytes eine Station senden darf, bevor von der Gegenseite der Empfang der Daten bestätigt wurde; Wird gegenseitig zugesprochen
- Checksum (16 Bit) –
- Urgent (16 Bit) –
- Options (0 or 32 Bit) –

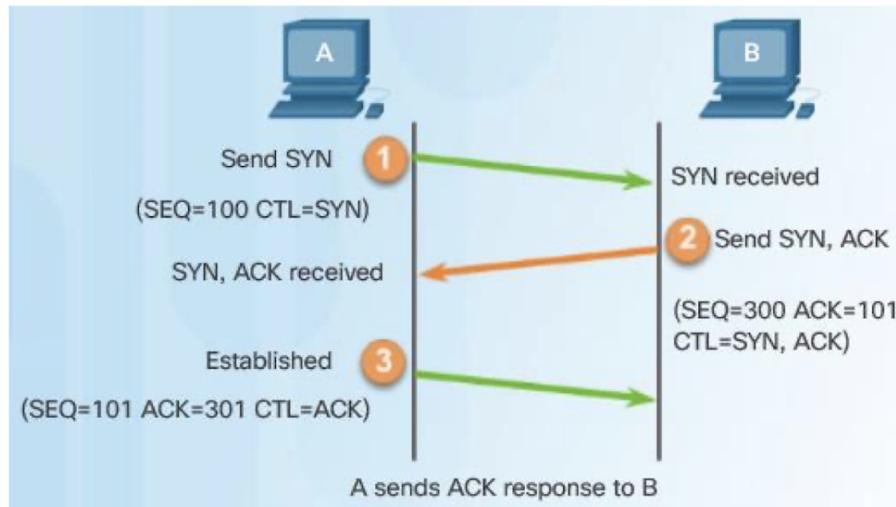
TCP Header Flags im Feld Control

- *URG* – Urgent (wird nicht mehr benutzt)
- *ACK* – Acknowledgement: Ist dann gesetzt, wenn die Verbindung geöffnet ist.
- *PSH* – Push: Zeigt das letzte Segment eines Datenblocks an. Wenn ein Empfänger ein Segment mit gesetztem PSH erhält, so setzt er die Segmente zusammen und übergibt den Datenblock der Anwendung.
- *RST* – Reset
- *SYN* – Synchronize Sequence Numbers (siehe unten)
- *FIN* – No more data from sender

Verbindungsauftbau TCP Für den Verbindungsauftbau wird ein Drei-Wege-Handshake ohne Payload angewendet (send nach received):

1. Send SYN (Sender → Empfänger)
2. Send SYN, ACK (Sender ← Empfänger)
3. Send ACK (Sender → Empfänger)

Danach ist eine Verbindung etabliert.



Verbindungsabbau TCP Für den Verbindungsabbau werden vier Schritte benötigt (send nach received):

1. Send FIN (Sender → Empfänger)
2. Send ACK (Sender ← Empfänger)
3. Send FIN (Sender ← Empfänger)
4. Send ACK (Sender → Empfänger)

Die etablierte Verbindung wird entweder so abgebaut oder es findet ein Time-Out statt.

Schwachstellen TCP Wenn der Client (Sender) den dritten Schritt nicht sendet, bleiben beim Server (Empfänger) ggf. RAM-Ressourcen reserviert. Wenn viele Clients dies machen, dann kann der Server langsam werden.

9.2 UDP

macht keine Flusskontrolle

UDP (Header und Bedeutung der Felder)

Fehlerkorrektur Wenn ein Segment nicht ankommt sendet der Empfänger 3-mal eine ACK. Somit wird dem Sender gezeigt, dass dieses Segment erneut gesendet werden soll. Der Empfänger fordert jedes Segment an, welches nicht in der erwarteten Reihenfolge ankommt – *Fast Retransmission*.

Flusssteuerung / Flusskontrolle Die Window-Size wird jedesmal halbiert, wenn ein Segment nicht angekommen ist. Somit wird der Fluss gesteuert, damit die Netze nicht überlastet werden. Wenn Segmente wieder durchkommen, wird die Window-Size wieder vergrößert.

Flusskontrolle wird in UDP nicht gemacht.

Vorteile und Gefahren UDP Da der Header von UDP sehr klein ist, entsteht wenig Overhead. Somit können kurze Nachrichten effizient und schnell ausgeführt werden.

Beim UDP-Empfänger wird jedes empfangene Datagramm sofort an die Anwendung geliefert.

Damit e.g. VoIP funktioniert, wird für die Sprache das Real-Time-Protocol (RTP) verwendet. Damit werden die Datagramme nummeriert.

Abschluss UDP ist gefährlich und TCP ist gutmütig dafür langsam.

10 Anwendungsschicht

Anwendungen übernehmen die Aufgaben der theoretischen Schichten *Darstellung* und *Sitzung*.

10.1 Position der Anwendung innerhalb des Protokollstacks

Die Anwendung

- ist die oberste Schicht im Protokollstack und stösst den Datenaustausch an – ist der Beginn der Kommunikation
- hat ganz eigene Regeln, wie zwei Endsysteme Daten miteinander austauschen (e.g. HTTP – geht immer über TCP)
- greift über einen "Socket" auf die Transportschicht zu. Socket: Über das Vier-Tupel [Quell-IP-Adresse, Quell-Port-Nr., Ziel-IP-Adresse, Ziel-Port-Nr.] (ist der Socket) kann eine Verbindung eindeutig bestimmt werden.

10.2 Standards der Internetanwendungsprotokolle

HTTP geht über TCP und Port 80; Möglicher Protokollstack: [HTTP; TCP; IP; Ethernet]; Ablauf, wenn alle Speicher leer sind:

- Ermittlung der MAC-Adresse des Default Gateway: ARP-Anfrage für IPv4 oder Neighbour Discovery mit ICMPv6
- Auflösung des Domainnames in eine IP-Adresse mit der Anwendung DNS
- Verbindungsauftbau mit dem TCP-3-Weg-Handshake von Endgerät zu Endgerät
- Datenaustausch
- Beim Schliessen des Browsers: Abbau der TCP-Verbindung

eMail Möglicher Protokollstack: [SMTP/POP3; TCP; IP; Ethernet]

- SMTP – Simple Mail Transfer Protocol (port 25)
- POP3 – Post Office Protocol (port 110)
- IMAP – Internet Message Access Protocol (port 143)

Wenn die Mail-Server in der Cloud sind erfolgt der Nachrichtenaustausch über https.

DHCP Dynamic Host Configuration Protocol; DHCP Server port 67; DHCP Client port 68; Möglicher Protokollstack: [DHCP; UDP; IP; Ethernet] (UDP, da keine IP-Adresse bekannt);

FTP

10.3 Ansätze DNS

Wird benötigt für die Zuordnung von Servernamen zu IP-Adressen und umgekehrt. Die DNS löst einen Full Qualified Domain Name (FQDN) in eine IP-Adresse auf.

- ist dezentral und hierarchisch (delegiert nach unten) – Root-Level Domain (Server); Top-Level Domain (Server); Second Level Domain (Server)
- beruht auf Delegation
- Die IP-Adresse des Servers, bestimmt dessen Betreibers

Verschiedene Resource records eines DNS Servers:

- A – IPv4 Adresse
- AAAA – IPv6 Adresse
- NS – Angabe des authorativen Name Servers
- MX – Mail exchange record
- CNAME – Alias
- SOA – Start Of zone Authority
- PTR – Domain Name Pointer (inverse Operation)
- TXT – TeXT string (gefährlich; Datenexfiltration)

Angriffspunkte Die Antworten werden nicht auf Authentizität geprüft und könnten gefälscht werden; Mit DNSSEC und DNS over HTTPS gibt es aber neue, sicherere Varianten von DNS.

Ablauf DNS

1.

11 Routing-Konzepte

11.1 Aufgaben eines Routers

Der Router hat zwei Aufgaben: 1) Finden des besten Weges zu den Zielnetzen und 2) Weiterleitung der Pakete.

Bestimmung des besten Weges In vermeshnten Netzen wird meist ein dynamisches Routing Protokoll ausgeführt.

- Ein Routing Protokoll benötigt eine *Metrik*, um den Weg der Pakete zu bestimmen
- Metriken:
 - Anzahl Hops (RIP)
 - Summe der Kosten der einzelnen Links (konstante / Datenrate) OSPF; Die Kosten eines Links sind proportional zur Bandbreite des Links

11.2 Longest Prefix Matching

Die Einträge in der Routing Tabelle sind IP-Netze. Es wird der Eintrag mit der längsten Subnetzmaske gewählt; der spezifischste Eintrag. Dies bedeutet, dass immer die gesamte Routing Tabelle abgesucht werden muss.

Destination IPv4 Address		Address in Binary
172.16.0.10		10101100.00010000.00000000.00001010
Route Entry	Prefix/Prefix Length	Address in Binary
1	172.16.0.0/12	10101100.00010000.00000000.00001010
2	172.16.0.0/18	10101100.00010000.00000000.00001010
3	172.16.0.0/26	10101100.00010000.00000000.00001010

11.3 Paketweiterleitung

11.4 Routing-Tabellen

Schritte der Paketweiterleitung:

1. Entfernung des L2-Rahmens beim eingehenden Paket
2. Finden der Zieladresse im IP-Header
3. Absuchen der Routing Tabelle und Bestimmung des Ausgangs-Interfaces
4. Entweder Weiterleitung an Zielgerät (Bildung eines neuen Ethernet Headers) – oder Weiterleitung an den Next-Hop
5. Paket wird verworfen, falls kein zutreffender Eintrag in der Routing Tabelle

Prinzip

- Jeder Router trifft seine Entscheidungen für die Weiterleitung selbstständig aufgrund seiner Routing Tabelle. R1 weiß nicht was bei R2 in der Tabelle steht
- Die Einträge in der Routing Tabelle von R1 sind nicht notwendigerweise konsistent mit R2
- Information über den kürzesten Weg beinhaltet nicht, dass alle Router auf dem Weg den Rückweg kennen

Der Weg zu den entfernten Netzen muss entweder durch statische Routen oder durch ein dynamisches Routing Protokoll eingetragen werden.

Beiträge in der Routing Tabelle:

- *Direkt angeschlossene Netzt* – Alle an einen Router angeschlossenen Netze, deren Router-IF eine gültige IP Adresse konfiguriert haben und bei denen das Schicht-1/2 Protokoll läuft werden automatisch als *directly connected routes* in die Routing Tabelle eingetragen
- *IP Adresse des lokalen IF* – IP Adresse des lokalen Router IFs (/32 oder /128)
- *Statische Routen* – Werden durch den Administratoren manuell in die Routing Tabelle eingetragen
- *Statische Routen*

11.5 Administrative Distanz

Gibt es für ein Zielnetz mehrere Quellen für die Routinginformation, wird die Quelle mit der niedrigeren administrativen Distanz in Routing Tabelle eingetragen.

Quelle der Route	Administrative Distanz
Direkt angeschlossen	0
Statische Route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Beispiele IPv4 und IPv6 Routing Tabellen

```
R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PFR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0

S*  0.0.0.0/0 [1/0] via 209.165.200.226
    10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O     10.0.1.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
O     10.0.2.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
C     10.0.3.0/24 is directly connected, Serial0/1/0
L     10.0.3.2/32 is directly connected, Serial0/1/0
C     10.0.4.0/24 is directly connected, GigabitEthernet0/0/0
L     10.0.4.1/32 is directly connected, GigabitEthernet0/0/0
C     10.0.5.0/24 is directly connected, GigabitEthernet0/0/1
L     10.0.5.1/32 is directly connected, GigabitEthernet0/0/1
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C     209.165.200.224/30 is directly connected, Serial0/1/1
L     209.165.200.225/32 is directly connected, Serial0/1/1
R2#
```

```
R1# show ipv6 route
(output omitted for brevity)
OE2 ::/0 [110/1], tag 2
    via FE80::2:C, Serial0/0/1
C  2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L  2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0/0, receive
C  2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/0/1, directly connected
L  2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/0/1, receive
C  2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/1/1, directly connected
L  2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/1/1, receive
O  2001:DB8:ACAD:4::/64 [110/50]
    via FE80::2:C, Serial0/1/1
O  2001:DB8:ACAD:5::/64 [110/50]
    via FE80::2:C, Serial0/1/1
L  FF00::/8 [0/0]
    via Null0, receive
R1#
```

12 Statisches Routing

12.1 Informationen zum Weiterleiten von Paketen

Ziel-Adresse, Quell-Adresse

12.2 Vor- und Nachteile und Einsatzgebiete von statischem Routing

Vorteile

- Benötigen wenig Ressourcen

- Routing ist stabil, sobald Routen definiert sind
 - Einfache Konfiguration in kleinen Netzwerken
 - Kein Routing Protokoll verwendet – Weniger Angriffspunkte

Statisches Routing soll mit soviel Einträgen wie nötig, aber mit sogenannten Einträgen wie möglich realisiert werden.

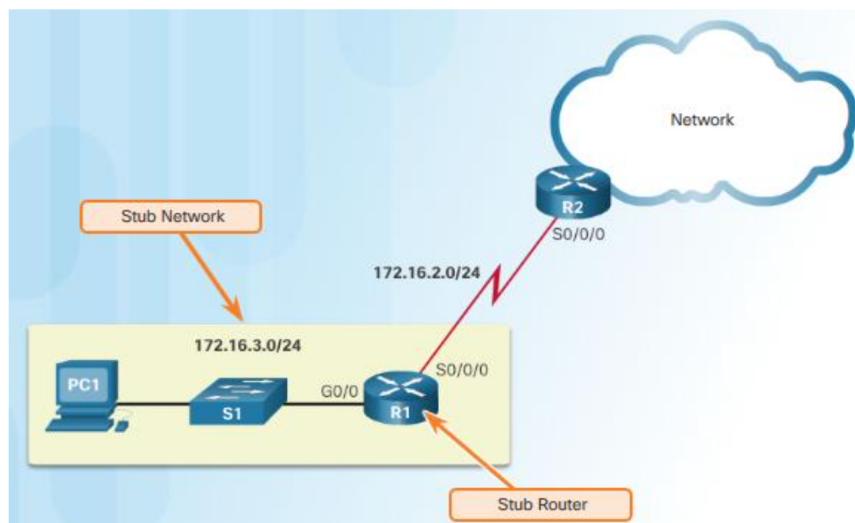
Nachteile

- Aufwand für Unterhalt nicht zu unterschätzen
 - Durch falsche Konfiguration von Routen können Routing Loops entstehen
 - Änderungen an Topologie im Netzwerk müssen manuell auf jedem Router nachgepflegt werden

Einsatzgebiete Firmennetze werden oft als Hub-and-Spoke Netze entworfen. Der Hub bekommt eine statische Route zu jedem Stub-Netz; Stub-Router erhält eine Default-Route.

12.3 Stub-Netzwerk und Stub-Router

Ein Netz, das nur einen Router und nur Weg zu einem Internetwork hat – Wie Blatt am Baum; *Stub-Router R1 erhält Default Route auf das WAN-Netz;* Router R2 erhält statische Route zum Stub-Netz.



12.4 Typen von statischen Routen

- Standard statische Routen – Bekanntgabe des Weges zu einzelnen Netzen
- Default Routen – Aller Verkehr zu unbekannten Zielen nimmt einen bestimmten Weg (IPv4: 0.0.0.0/0; IPv6: ::/0)
- Floating Routen – Angaben eines Backup Weges für den Fall, dass das Routing Protokoll ausfällt
- Summary Routen – Der Weg zu einer Reihe von Netzen wird zusammengefasst mit einer einzigen Wegangabe

12.5 Next-Hop und IF-Routen

Next-Hop Es werden Ziel-Netz (Netzadresse und Subnetzmaske) und IP-Adresse des next-hop angegeben. Spezifische Angabe von Empfänger, kann also in multi-access Netzen verwendet werden.

```
R2(config)# ip route 172.16.3.0 255.255.255.0 172.16.2.1
```

IF-Routen Es werden Ziel-Netz (Netzadresse und Subnetzmaske) und der IF-Ausgang des next-hop angegeben. Da kein spezifischer Empfänger angegeben ist, wird ggf. ein Broadcast gesendet (also nur für P2P empfohlen, sonst können alle mitlesen).

```
R2(config)# ip route 172.16.3.0 255.255.255.0 ser0/0/0
```

Wann welche anwenden Bei Multiaccess: Next-Hop; Bei P2P: IF-Routen.

12.6 statische Routen für IPv4 und IPv6 in allen Varianten konfigurieren

- *Default Route*
 - *IPv4* – R1(config)# ip route 0.0.0.0 0.0.0.0 ser0/0/0
 - *IPv6* – R1(config)# ipv6 route ::/0 s0/0/0
- *Summary Route*
 - *IPv4* – Rx(config)#ip route 172.16.0.0 255.255.252.0 s0/0/0
 - *IPv6* – Rx(config)#ipv6 route 2001:db8:acad::/62 s0/0/0

- *Floating Static Route*
 - *IPv4 – R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 5*
(Administrative Distanz = 5)
 - *IPv6 – R1(config)#ipv6 route ::/0 2001:db8:acad:4::2 111*

13 Dynamisches Routing

Die Aufgaben sind 1) das Auflisten von entfernten Netzen, 2) die Laufende Aktualisierung der Routing-Information, 3) die Wahl des besten Weges zum Ziel, 4) das Finden eines neuen Weges zu einem Ziel im Falles eines Leitungsunterbruchs.

Datenstrukturen, Nachrichtenformate und Algorithmen werden definiert.

13.1 Vor- und Nachteile von statischem Routing

Vorteile

- Skalieren besser
- Automatisches Re-Routing bei Leitungsunterbuchen

Nachteile

- i.A weniger sicher, weil Informationen in Band übers Netz ausgetauscht werden
- Höhere Belastung von CPU, RAM und Leitungen
- Wege können ändern
- Eher komplexe Implementation

13.2 Wann lohnt es sich dynamisches Routing einzusetzen

Wenn sich die Netz-Struktur dynamisch ändert und regelmässig die Vorteile von dynamischem Routing relevant sind (e.g. Skalierbarkeit, Leitungsunterbrüche etc.)

13.3 Autonomes System

Ein *autonomes System* (AS) ist eine Menge von Routern, die unter einer einheitlichen Verwaltung stehen. Typischerweise haben mittlere und grössere ISPs ein eigenes AS. Im allgemeinen Sprachgebrauch denkt man oft an eine Gruppe von Routern, die das gleiche Routing Protokoll benützen. Interior Gateway Protokolle (IGPs) sind Routing Protokolle, die innerhalb eines AS ausgeführt werden. Wesentlich komplexer sind Exterior Gateway Protokolle (EGPs), die zwischen AS Routen austauschen.

13.4 Distanz-Vektor Protokolle

Ein Router hat die Information, wie weit weg sich das Ziel in gegebener Richtung befindet. Dafür wird die Distanz-Vektor Technologie verwendet:

- DV Router sendet periodische Updates mit dem Inhalt seiner Routingtabelle
- Updates werden per Broadcast oder Multicast gesendet; alle hören Broadcast aber nur TN, welche das Routing-Protokoll ausführen können etwas damit anfangen
- DV Router kennt die Topologie des Netzes nicht; weiss nicht definitiv, wieviele Router im Netz mitmachen
- Routing-Prozess wird dezentral durchgeführt; Berechnung Routing-Tabelle ist eine verteilte Anwendung

Algorithmus Der Algorithmus umfasst jeweils einen Mechanismus für 1) das Senden und Empfangen von Routing-Informationen, 2) die Berechnung des besten Weges zum Ziel und das Eintragen in die Routing-Tabelle und 3) das Entdecken von Änderungen in der Netz-Topologie und Massnahmen, um das Routing aktuell zu halten.

Vorteile

- Sehr einfache Handhabung (Wenig Ausbildung nötig)
- Benötigt wenig Rechnerleistung

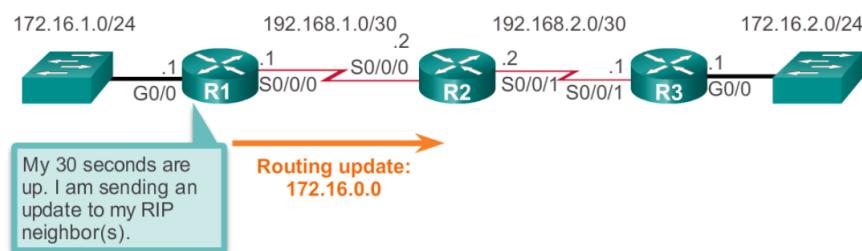
Nachteile

- Konvergiert nur langsam
- Skaliert nicht
- Neigt zu Routingschleifen

klassenbezogenes – klassenloses Routing Wird in einem AS mit klassenbezogenen Netzen gearbeitet oder haben alle beteiligten Netze den gleichen Netzteil, so können klassenbezogene Routingprotokolle eingesetzt werden. Bei klassenbezogenen Routingprotokollen werden in den Updates die Netzadressen ohne Subnetzmasken ausgetauscht. Subnetze werden immer auf klassenbezogene Netze aufgerundet. So gibt der Router R1 in Abb. 13.6 dem Nachbarn R2 anstatt dem Subnetz 172.16.1.0/24 das zugehörige klassenbezogene Netz 172.16.0.0/16 bekannt.

RIPv1 und IGRP waren klassenbezogene Routing Protokolle. Nachfolgende Abbildung veranschaulicht die Problematik klassenbezogener Protokolle. Der Router R3 wird dem Router R2 ebenfalls das klassenbezogene Netz 172.16.0.0 bekannt geben.

Werden Netze unterteilt in Subnetze verschiedener Länge, so muss bei den Updates notwendigerweise zu jedem Netz die Netzmaske mitgegeben werden. Man spricht von klassenlosen Routingprotokollen. RIPv2 und EIGRP sind die klassenlosen Varianten obiger klassenbezogener Protokolle.

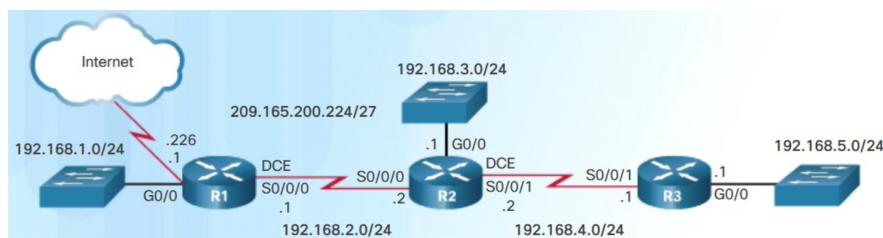


13.5 RIP v2 für Firmennetz

RIPv2 ist klassenlos. Als Metrik wird die Anzahl Hops verwendet (normalerweise begrenzt auf 15). Ist ein Netz weiter entfernt als die definierten Anzahl Hops, gilt es als nicht erreichbar.

Schritte zur Konfiguration:

1. Optional (sofern am lokalen Router angeschlossen – R1): Statische Defaultrouten setzen
2. Routing Submenu wählen
3. RIP version 2 wählen und automatische Summarisierung ausschalten (`no auto-summary`)
4. Bekanntgabe der Netze, die sich am Routing beteiligen sollen
5. Die Netze zu den Clients sollen passiviert werden; Es werden über die IF, an welchen clients angeschlossen sind keine Routing Updates gesendet
6. Optional (Router R1): Defaultroute an die anderen Router weiterverbreiten



Konfiguration für Router 1:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
```

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#passive-interface g0/0
R1(config-router)#default-information originate
R1(config-router)#exit
```

Statusabfragen:

```
R1#show ip route
R1#show ip protocols
R1#debug ip rip
```

14 OSPF

14.1 Ziele von OSPF

- Klassenlos: Adressräume mit variabel landen Subnetzmasken
- Routing-Prozess muss robust sein
- Routing-Prozess soll rasch konvergieren und rasch auf Änderungen reagieren
- Protokoll soll skalieren
- Bandbreite der Links soll berücksichtigt werden

14.2 Vor- und Nachteile von LS Protokollen

Vorteile

- Jeder Router hat seine eigene Sicht des ganzen Netzes
- Rasche Konvergenz
- Updates nur bei Netzänderungen
- Überwachung der Links mit Hello Paketen

Nachteile

- Benötigt erheblich Memory für die LS-DB
- Hohe Last auf der CPU, wenn der Dijkstra-Algorithmus gerechnet werden muss

14.3 Konzepte von OSPF

- OSPF als Schicht-3 Protokoll
- Verschiedene Paket-Typen
- Das Hello-Protokoll und den Aufbau von Nachbarschaften
- Die endliche Zustandsmaschine beim Aufbau einer Nachbarschaft
- Das Versenden von Link State Updates
- Die Bestimmung der Router ID
- Die Besonderheiten auf Multiaccess Netzen: Designated Router

14.4 Funktionsweise

14.5 Metrik von OSPF und Parameter Bandwidth

OSPF rechnet mit Kosten eines Links – umgekehrt proportional der Datenrate des Links: `cost = reference-bandwidth / IF bandwidth`

Standardmäßig wird die Referenz-Datenrate auf 100Mbps gesetzt. Die Referenz-Bandbreite kann konfiguriert werden (in Mbps – Beispiel setzt auf 1 Gbps): `R1(config router)#auto-cost reference-bandwidth 1000`
Die Einheit der Referenz-Datenrate ist Mbps.

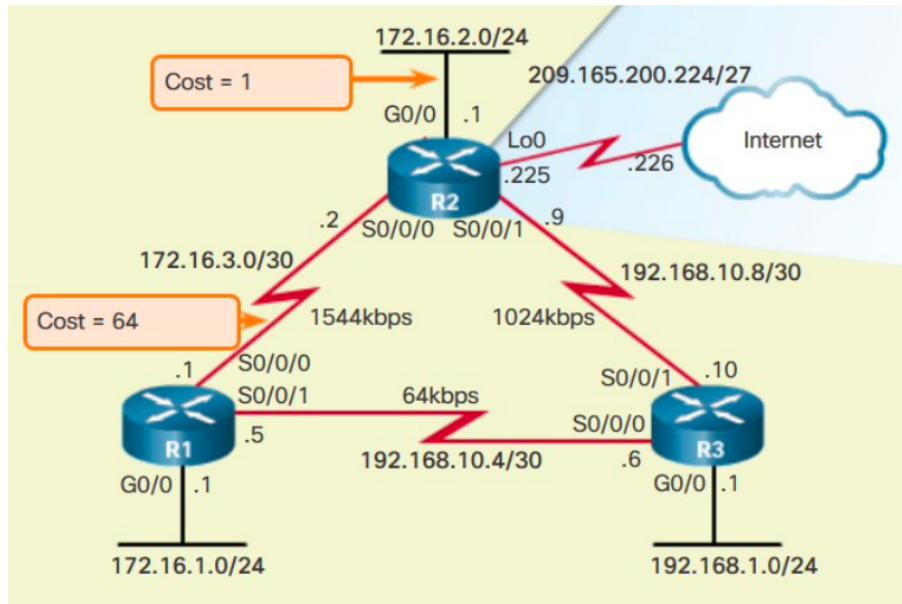
Kosten von Serial Links Bei Ethernet-IF ist einem Router die Datenrate bekannt. Bei WAN-Links müssen (DTE-Ende) die Bandbreite (*bandwidth*) konfiguriert werden – *Standardwert ist 1.544 Mbps*. Wenn der Link dem Standardwert entspricht, muss nicht angepasst werden.

Damit kein asymmetrisches Routing entsteht, müssen bei allen IF am gleichen Netz die gleiche Bandbreite eingestellt werden (vgl. Bild):

```
// Router 1
R1(config)#interface serial0/0/1
R1(config-if)#bandwidth 64

// Router 2
R2(config)#interface serial0/0/1
R2(config-if)#bandwidth 1024

// Router 3
R3(config)#interface serial0/0/0
R3(config-if)#bandwidth 64
R3(config)#interface serial0/0/1
R3(config-if)#bandwidth 1024
```



14.6 Dijkstra-Algorithmus

Berechnet über einer vermaschten Topologie einen Spannbaum als logische Topologie. Spannbaum gibt kürzesten Weg von einem Knoten aus zu allen anderen Knoten. Wenn diese Berechnung bekannt ist, kann der Weg zu den zugehörigen Netzen in der Routing-Tabelle eingetragen werden. Wird nur innerhalb einer Area berechnet.

LS-Algorithmus fuer den Knoten u (Quelle):

- 1 Initialisierung :
- 2 $N = \{u\}$
- 3 fuer alle Knoten v, die noch nicht in N enthalten sind :
- 4 wenn v ein Nachbar von u ist
- 5 dann $D(v) = c(u, v)$
- 6 sonst $D(v) = \text{inf}$
- 7 Wiederhole :
- 8 finde einen Knoten w, der noch nicht in N ist , so dass $D(w)$ minimal ist und fuege w zu N
- 9 Berechne $D(v)$ neu fuer jeden Nachbarn v von w, der nicht in N ist
- 10 $D(v) = \min(D(v), D(w) + c(w, v))$
- 11 /* Die neuen Kosten zu v sind entweder die alten Kosten zu v oder die bekannten Kosten des kuerzesten Pfades zu w, zuzueglich der Kosten von w zu v */
- 12 bis alle Knoten in N sind

14.7 OSPFv2 und OSPF v3

Wildcard Maske

14.8 OSPF konfigurieren

(Router-ID, Default Route, Passivierung von Clientnetzen, Bandbreite von P-zu-P-Netzen)

Statusabfragen zum Fehlersuchen

15 Multiarea OSPF

15.1 —

Wann ist es sinnvoll multi-area OSPF anzuwenden?

15.2 Router in Multi-Area Topologien aufteilen

15.3 LSA Typen

Rechenaufwand auf eine Area beschränken

15.4 MA OSPF für IPv4 und IPv6

- konfigurieren - Statusabfragen

15.5 Routen zusammenfassen (für Bekanntgabe in andere Area)