Kapitel 5 Kontrollfragen

1. **Nennen Sie vier typische Protokollfunktionen, die in der Transportschicht implementiert sein sollten. (S. 138)**

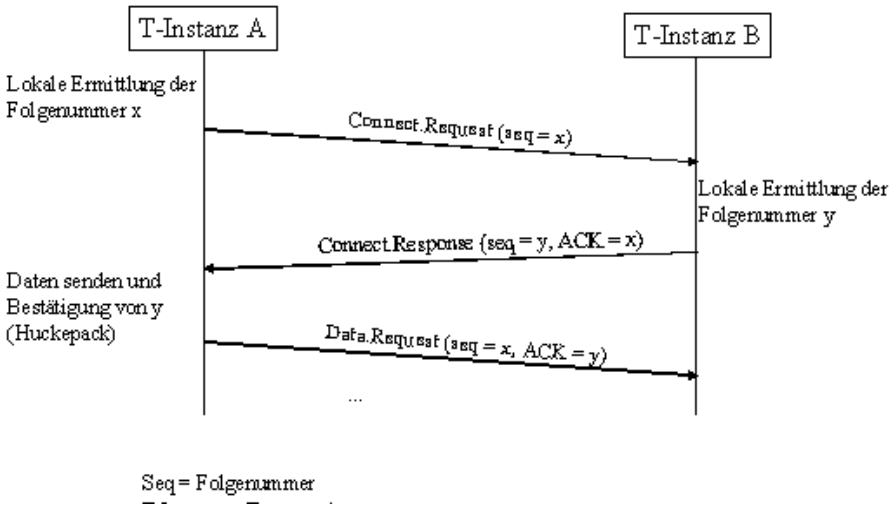
- Verbindungsmanagement und Adressierung
- Zuverlässiger Datentransfer
- Flusskontrolle
- Staukontrolle
- Multiplexing und Demultiplexing
- Fragmentierung und Defragmentierung

2. **Beschreiben Sie einen Drei-Wege-Verbindungsaufbau und erläuter Sie kurz, wie man durch diese Art des Verbindungsaufbaus Duplikate erkennen kann (S.139 f)**

- Host A initiiert den Verbindungsaufbau mit einer Connect-Request-PDU und sendet dabei eine vorher ermittelte Folgenummer (seq=x) mit. Mit der Connect-Request-PDU wird auch die Transportadresse gesendet, um den Empfänger zu identifizieren.
- Host B bestätigt den Verbindungswunsch mit einer ACK-PDU, bestätigt dabei die Folgenummern (Seq) und sendet seine eigene Folgenummer (seq=y) mit der ACK-PDU an Host A
- Host A bestätigt die Folgenummer von Host B mit der ersten Data-PDU im Pickypacking-Verfahren und damit ist die Verbindung aufgebaut.

Normaler Protokollverlauf

- Instanz A und B suchen eigene Folgenummern x und y (seq) aus



Duplikate werden vermieden durch: Duplikate entstehen dadurch, dass Duplikate PDUs alter Verbindungen beim Empfänger ankommen. Das soll durch Folgenummern verhindert werden. Folgenummer dienen als fortlaufender Zähler der abgesendeten Nachricht kombiniert mit einer maximalen Paketlebensdauer.
Erkannt werden Connect-Request-Duplikate von Host A.

3. **Was ist eine Ende-zu-Ende – Verbindung im Sinne der Transportschicht? (S.146)**

Eine Verbindung von Teilnehmer zu Teilnehmer anstatt von Knoten zu Knoten

4. **Nennen Sie je einen Vorteil für verbindungsloses und verbindungsorientiertes Protokoll in der Transportschicht.**
    - Verbindungslos (S.137)
    - Negativ:
        - Der Verlust von Daten ist möglich
        - Die Daten können ggf. verfälscht sein
        - Die Reihenfolge ist nicht garantiert
        - Die Adressierungsinformation muss in allen T-PDUs enthalten sein.
    - Vorteil:
        - Nicht so komplex
        - Ist für z.B. Videoübertragungen gut, da hier eine Verzögerung vertretbar ist
    - Allgemein:
        - Verlust von Datenpaketen wird nicht gemerkt
        - Verfälschung der Nutzdatenteils ist nicht unbedingt nachvollziehbar
        - Reihenfolgezerstörung ist möglich
        - Kein Zusammenhang bei Aufeinander folgenden Dienstaufrufen
        - T-PDUs enthalten die Adressinformation von Sender und Empfänger

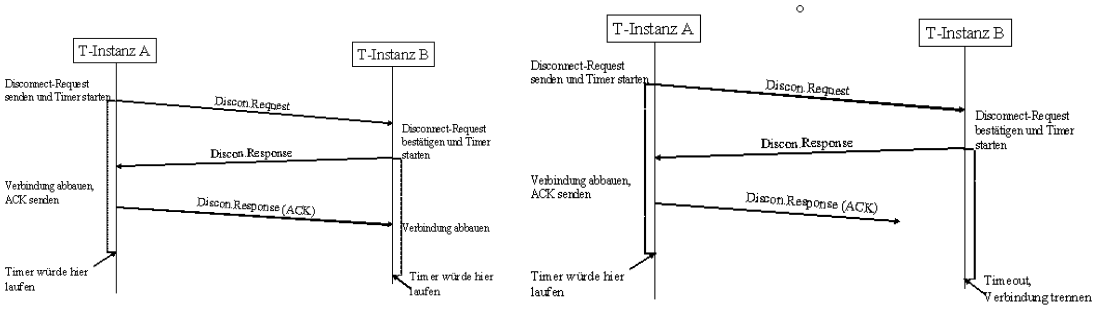
    - Verbindungsorientiert
    - Kennzeichen: Verbindngsaufbau, Datenübertragung, Verbindungsabbau
    - Vorteil: Zuverlässiger
    - Allgemeines:
        - Verbindung wird etabliert
        - Gemeinsamer Kontext wird aufgebaut
        - Geprägt von trad. Kommunikationsdiensten wie Telefonie
        - Hohe Zuverlässigkeit
        - Fehlerfreie und reihenfolgerichtige Auslieferung der Daten beim Empfänger
        - Verbindungsorientierte Protokolle sind komplexer (warum?)
        - Wann braucht man Verbindung
5. **Was will man mit einer Timerüberwachung beim Verbindungsabbau einer Transportverbindung erreichen? Kann das angestrebte Ziel absolut sicher erreicht werden? Begründen Sie ihr Entscheidung**

Bei TCP wird der Timed-Wait-Timer für den Verbindungsabbau eingesetzt. Dieser läuft über die doppelte Paketlebensdauer. Der Timer soll sicherstellen, dass alle Pakete bei einem Verbindungsabbau noch übertragen werden**.**

Evt. noch S. 164

- Kein Protokoll ist absolut zuverlässig
- Eine Seite wird immer unsicher sein
- Bei Verbindungsabbau:
    - Kann immer disconnect-Request oder Bestätigung verloren gehen
- Prakt. Lösung: Timerüberwachung mit begrenzter Anzahl an Nachrichten Wiederholungen

Normal Timer läuft ab



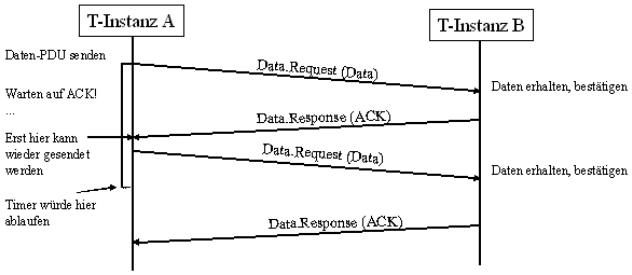
6. **Bei der Fehlerbehandlung nutz man in einer gesicherten Transportschicht u.a. das positiv selektive und das negativ selektive Quittierungsverfahren. Erläutern Sie diese beiden Verfahren.**

   Quittierungsverfahren sind dazu da, um einen zuverlässigen Datentransfer ohne Duplikate zu gewährleisten

- Positiv-selektives Verfahren (z.B. Stop-and-Wait-Protokoll):
  - Der Empfänger sendet pro empfange Nachricht eine Quittung (ACK). Die Folge ist ein hoher zusätzlicher Nachrichtenverkehr

Positiv selektives Quittierungsverfahren

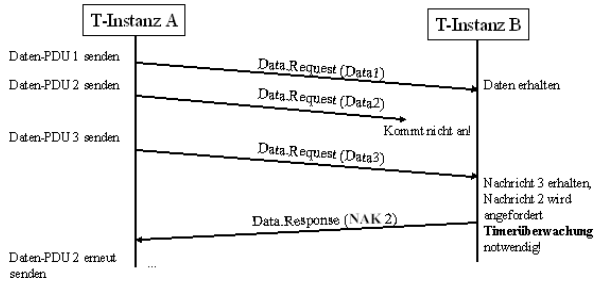
- Stop-and-go: Eine Quittung pro gesendeter Nachricht
- Hoher Zusatzverkehr



- Negativ-Selektives Verfahren
  - Vom Empfänger werden nur selektiv nicht empfangene (verlorene) Nachrichten erneut vom Sender angefordert. Alle anderen gelten als beim Empfänger angekommen. Die Folge ist, die Netzlast wird reduziert, jedoch können die negativen Quittierungen des Empfängers verloren gehen (NAK=NOT-Acknowledge). Dem kann entgegengewirkt werden durch eine Timerüberwachung der Instanz B, damit die NAK-Nachricht erneut gesendet wird.

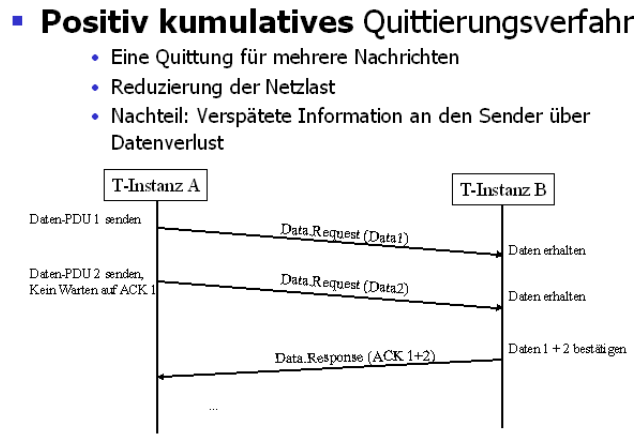
Negativ selektives Quittierungsverfahren

- Weitere Reduzierung der Netzlast
- Problem: Verlust von Quittungen und dessen Behandlung



- Positiv-kumulatives Quittierungsverfahren:

- Eine Quittierung wird für mehrere Nachrichten verwendet. Vorteil: Reduzierung der Netzlast. Nachteil: Informationen über Datenverlust kommen verspätet beim Sender an



7. **Zur Fehlerbehebung nutz man in der Transportschicht das Verfahren der Übertragungswiederholung. Nennen Sie hierzu zwei Verfahren und erläutern sie diese kurz. Was muss der Sender tun, damit eine Übertragungswiederholung möglich ist? (s.145)**
   Übertragungswiederholung: Verlorengegangene Nachrichten müssen erneut übertragen werden.

- Selektives Verfahren
  - Nur Negativ quittierten Nachrichten werden wiederholt
  - Der Empfänger puffert die nachfolgenden Nachrichten so lange, bis die fehlende da ist.
  - Dann werden die Daten im T-SAP weiter nach oben zur Anwendung gereicht
  - Vorteil: Reguläre Übertragung wird während der Wiederholung fortgesetzt
  - Nachteil: Hohe Pufferkapazität beim Empfänger nötig
- Go-Back-N-Verfahren:
  - Es werden alle fehlerhaften Nachrichten sowie alle nachfolgenden Nachrichten erneut gesendet.
  - Vorteil: Empfänger braucht nur geringe Kapazitäten
  - Nachteil: Reguläre Übertragung wird unterbrochen

Sender und Empfänger müssen sich einig über das verwendete Verfahre sein, dass muss vorher in der Protokollspezifikation festgellegt werden. Zusätzlich muss der Sender Nachrichten über einen bestimmten Zeitraum zur Übertragungswiederholung bereitstellen. Das ist beim Stop-and Wait einfacher, da der Sender nur eine Nachricht zur Verfügung halten muss, erhält er den ACK vom Empfänger kann er die Nachricht verwerfen. Beim positiv-kumulativen und negativ-selektiven (vor allem hier, Sender weiß nie wirklich ob de Nachricht angekommen ist) ist das schwieriger.

8. **Was bedeutet in der Transportschicht selektive und was Go-Back-N-Übertragungswiederholung? Nennen sieh einen Nachteil der selektiven und einen Vorteil der Go-Back-N-Übertragungswiederholung.**
   - Siehe Aufgabe7
9. **Was ist bei TCP ein Port und was ist bei TCP ein well-known Port? (S. 155)**
   Adressierung: Die Adressierung erfolgt über eine Tupel von IP-Adresse und TCP-Portnummer
   - Well-Known Port
     - Ein Server stellt einen Dienst zur Verfügung und bietet ich über eine wohlbekannte Portnummer, well-Known-Port, an

- Hat ein Client die IP-Adresse, Portnummer des Dienstes und das zugehörige Protokoll, kann er mit dem server kommunizieren
- Bsp.: Port 23, Telnet: Port 20, 21, ftp (File Transfer Protocol); Port 25, SMTP (Simple Mail Transfer Protocol)

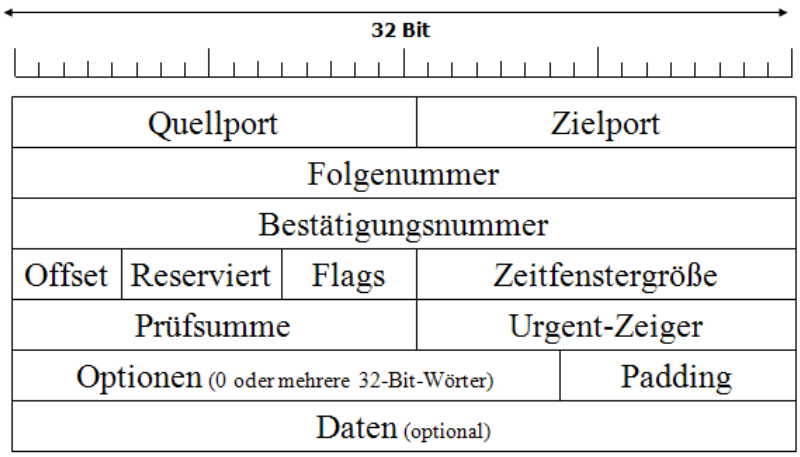
- Port (Portnummer)
  - 16-Bit-lange Integerzahl
  - Sind eigens definierte Portnummern
  - Es können Überlappungen im Netz entstehen, ist ok solange die Domänen disjunkt sind
  - Auf einem Rechner gibt's aber zum Beispiel nur einmal den Port 80

10. TCP ist datenstromorientiert (stream-orientiert). Was bedeutet das?

- TCP überträgt reihenfolgerichtig einen seriellen Bitstrom in der Form von 8-Bit Bytes

11. Was sind TCP-Segmente, wie groß sind diese mindestens und warum? (S.151) (Folien: TCP Teil 1: 13)

- TCP unterteilt den Datenstrom in Octets (Byte) und unterteilt diese für die Übertragung in Segmente.
- Segmente bestehen aus einem mind. 20 Byte langen Header
- Header enthält sämtliche Informationen zur Steuerung, für den Verbindungsaufbau, den zuverlässigen Datentransfer und Verbindungsabbau.
- Wahlweise kommen noch bestimmte Optionen dazu, was dazu führt, dass der Header auch größer als 20 Byte sein kann, sprich eine variable Länge hat.

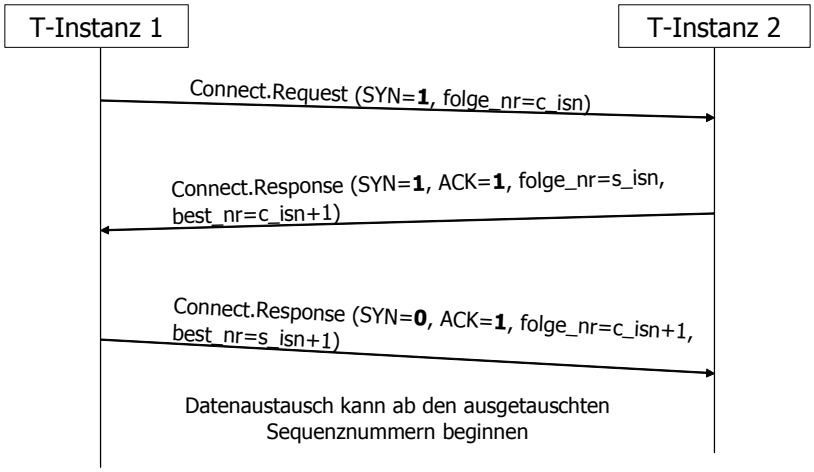


TCP-Protokoll-Header (T-PCI)

- Quell- und Zielport: Portnummer des Anwendungsprogramms des Senders und des Empfängers
- Folgenummer: Nächste Byte innerhalb des TCP-Streams, das der Sender absendet
- Bestätigungsnummer: Gibt das nächste erwartete Byte im TCP-Strom an und bestätigt damit den Empfang der vorhergehenden Bytes.
- Offset: Gibt die Länge des TCP-Headers in 32-Bit Worten an. Das ist notwendig da er auf Grund der Optionen keine Fixe Länge aufweist
- Reserviert: Keine Verwendung
- Flags: Steuerkennzeichen für diverse Aufgaben. Sind Kontroll-Bits mit unterschiedlicher Bedeutung:
  - URG=Urgent-Zeiger ist gefüll
  - ACK=Bestätigung, dh. Die ACK-Nummer hat einen gültigen Wert
  - PSH=Zeigt Push-Daten an. Dh. Der Empfänger darf sie nicht zwischen speichern sonder muss sie gleich an den Empfänger-Prozessweiterleiten
  - RST= Dienst zum
    - Rücksetzen der Verbindung (z.B. Absturtz eines Hostes)

        - Abweisen eines Verbindungswunsches
        - Abweisen eines ungültigen Segments
    - SYN=Genutzt bei Verbindungsaufbau
    - FIN=Genutzt bei Verbindungsabbau
- Zeitfenstergröße: Erlaubt es dem Empfänger, mit der ACK dem Sender den vorhanden Pufferplatz in Byte zum Empfang der Daten mitzuteilen
- Prüfsumme: Verifiziert das Gesamtpaket (Header+Daten) mit Hilfe eines einfachen Algorithmusses
- Urgent-Zeiger: Beschreibt die Position an der dringliche Daten vorgefunden werden. Diese Daten werden vorrangig behandelt, kommt aber selten vor.
- Optionen: Optionale Angaben zum Aushandeln bestimmter Verbindungsparameter z.B.:
    - MSS (Maximun-Segment-Size)
    - SACKOK: Selektive Wiederholung antatt go-back n Verfahren
- Padding: Ausfüllen auf Wortgrenzen, wenn das Optionsfeld kleiner als ein Vielfaches von 4 Byte ist
- Daten: Nutzlast, die auch fehlen kann

12. Skizzieren Sie den Drei-Wege-Handshake für den TCP-Verbindungsaufbau und gehen Sie dabei auf die verwendeten Flags im TCP-Header ein. Skizzieren sie den Ablauf mit einem Sequenzdiagramm. (S. 162,)



c_isn = Initial Sequence Number des Clients (Instanz 1)
s_isn = Initial Sequence Number des Servers (Instanz 2)

- Aufbau ist die Synchronisation von einem aktiven Partner der eine Verbindung wünscht und einem passiven Partner, der auf einen Verbindungswunsch wartet
- Während des Verbindungsaufbaus werden die MSS und die Sequenznummer ausgehandelt
- Aktiver Partner (Instanz 1) beginnt den Verbindungsaufbau mit einem Connect-Aufruf(je nach Socket Programmierung kann das variieren).
- Dabei richtet Instant 1 noch lokal einen Kontext und eine Initiale Folgenummer ein die im Feld Folgenummer im Header steht
- Das SYN-Flag wird auf 1 gesetzt. –Zusätzlich werden noch der Ziel Port und eigene Port angegeben
- Der passive Partnern wartet schon auf einen Aufbau Wunsch indem er bereits einen Listen Aufruf in der Socket-Schnittstelle geleistet hat
- Es wird ebenfalls ein Kontext auf der passiven Seite erstellt und ein Respons geschickt, in der das SYN-Flag und ACK-FLag auf 1 gesetzt ist.
- Desweitern wird die Folgenummer des aktiven Partners dadurch bestätigt, indem die Folgenummer von diesem um eins erhöht wird (wird in Feld Bestätigungsnummer eingetragen)
- Da heißt nächste Byte muss diese Folgenummer enthalten
- Server richtet auch Folgenummer ein und wird in das Feld Folgenummer geschrieben

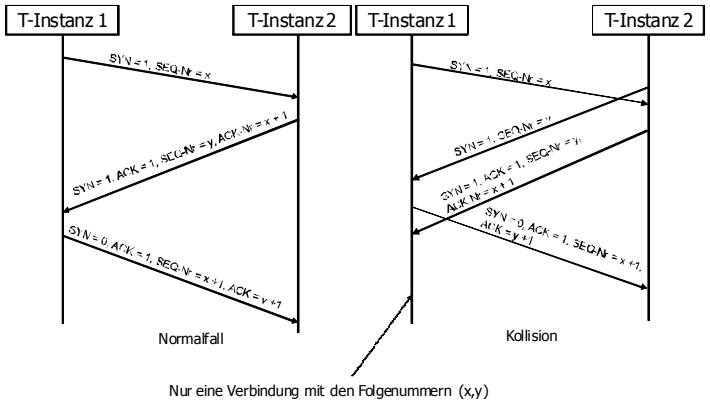
- Erhält der Aktive Partner die ACK-PDU, stellt er eine ACK-PDU zusammen:
  - SYN-FLAG auf 0
  - ACK-FLag auf 1
  - Feld Bestätigungsnummer kommt die um eins erhöhte Folgenummer des passiven Partners
  - Feld Folgenummer ist die Nummer kommt die um 1 erhöhte Folgenummer des aktiven Partners

13. Wie wird in TCP eine Verbindung eindeutig identifiziert?

Durch den Header

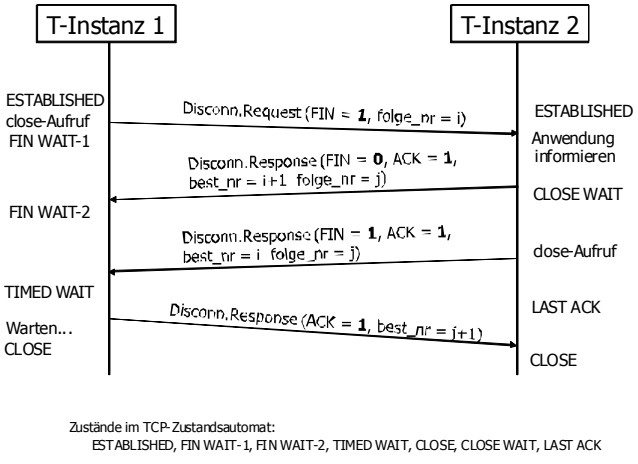
14. Auch beim TCP-Verbindungsaufbau ist es möglich, dass beide Seiten (quasi) gleichzeitig versuchen, eine Verbindung aufzubauen. Wie behandelt TCP diesen Kollisionsfall? Skizzieren Sie das in einem Time-Sequenz-Diagramm.(S. 162, Folie TCP Teil 1: 25-26)

- TCP sorgt dafür, dass nur eine Verbindung mit gleichen Parameter aufgebaut wird



- Problem Crash der Initialen Sequenz Nummer (ISN)
- Wird verhindert durch die Synchronisation der Sequenznummer durch 3-Wege-Handshake

15. Zeigen sie an Hand eines Time-Sequenz-Diagrammes auf, wie der Verbindungsabbau einer TCP-Verbindung prinzipiell Funktioniert. Stellen Sie dabei auf beiden Seiten die Zustandsübergänge im jeweiligen Zustandsautomaten dar! (S.164, Folien TCP Teil 1: 28)



Zustände im TCP-Zustandsautomat:
ESTABLISHED, FIN WAIT-1, FIN WAIT-2, TIMED WAIT, CLOSE, CLOSE WAIT, LAST ACK

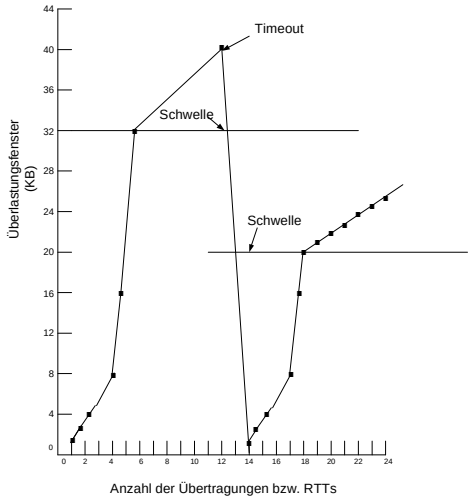
- Jede der beiden Vollduplex-Verbindungen wird abgebaut, d.h. beide Seiten bauen ihre „Senderichtung“ ab
- Wird an der Socket-Schnittstelle mit einem close-Aufruf erreicht
- Ablauf:
  - Aktiv abbauender Partner sendet zunächst ein Segment mit FIN-FLag=1
  - Passiver Partner antwortet zunächst mit einer ACK-Flag=1 und Informirmiert die Anwendung
  - Wenn die Anwendung close aufruft, sendet die Partner Instanz ein weiteres TCP-Segment mit FIN=1

    - Aktiver Partner sendet abschließend ein Segment mit ACK=1
- Besonderheit des Aktiven Partners:
    - Nach allen Bestätigungen des Partners baut er die Verbindung nicht gleich ab, sondern geht erst noch in den Zustand TIMED WAIT.
    - Hier wartet er noch eine bestimmte Zeit auf Pakete die noch im Netz unterwegs sind, damit diese nicht verloren gehen
    - Alle Segmente die die Folgenummer <i oder <j haben müssen noch beim Zielhost ankommen
    - Aktiver Partner wartet eine doppelte Paketlebensdauer (siehe Times-Wait-Timer)
- Laut Zustandsautomat gibt es mehrere Möglichkeiten des Verbindungsabbaus
    - Gehen auch drei wege mit Segment (FIN=1 und ACK=1)
- Es kann etwas dauern bis die Anwendung den close-Aufruf betätigt, manchmal ist dazu die Eingabe eines Benutzer notwendig
- Abnormale Beendigung, wenn der Empfänger das RST-FLAG=1 setzt, Empfänger bricht Verbindung sofort ab
- Erst komplett abgebaut, wenn beide Seiten den Zustand close erreicht haben

16. Wieviele TCP-Segmente werden für die Übertragung von 100 Byte Nutzdaten durchs Netz gesendet? Erläutern Sie dies an Hand eines Time-Sequence-Diagramms

17. Welche Quittierungsvariante wird bei TCP eingesetzt, damit der Empfänger den ordnungsgemäßen Empfang einer Nachricht bestätigen kann? Was macht der Sender eines Pakets, wenn er keine Quittung vom Empfänger erhält? (S. 165, Folien TCP: Teil 2 Folie 8ff)

- Slow-Start-Verfahren (Staukontrolle= Netzprobleme vermeiden vs. Flusskontrolle= Empfangspuffer dürfen nicht überlaufen)
- Läuft in zwei Phasen ab:
    - Slow-Start-Phase:
        - Sender und Empfänger einigen sich auf eine erste sendbare TCP-Segmentlänge
        - Sender sendet Segment dieser Länge
        - Jeweils Verdoppelung der Anzahl an Segmenten bei erfolgreicher Übertragung (ACK kommt rechtzeitig zurück) (expot. Anstieg)
        - Ein Schwellenwert (Threshold) wir ermittelt
        - Bei Erreichen des Schwellenwertes geht es in die Probing-Phase über
    - Probing Phase:
        - Bei jeder empfangenen Quittung wird die Größe des TCP-Segments erhöht, aber langsamer
        - Berechnung des Staukontrollfensters
            - Neues Überlastungsfenster +=1 Segment
            - Gilt Sendekredit= min {Überlastungsfenster, Empfangsfenster}
        - Tritt kein Problem auf
            - Überlastungsfenster stiegt bis zum Empfangsfenster
            - Bei Änderung des Empfangsfensters wird Überlastungsfenster angepasst
- ACk (Quittung) wird nicht empfangen:
    - Man geht davon aus, dass ein weiterer Sender hinzugekommen ist
    - Mit diesem neuen Sender muss man die Pfadkapazität teilen
    - Der Schwellwert wird auf die Hälfte runter gesetzt
    - Segmentlänge wird auf das min. runter gesetzt
- Timerlänge wichtig:
    - Zu kurz: Erhöhte last durch erneutes senden
    - Zu lang: evt. Leistungsverlust
    - AM besten: Dynamische Berechnung an Hand der Umlaufzeit eines Segment



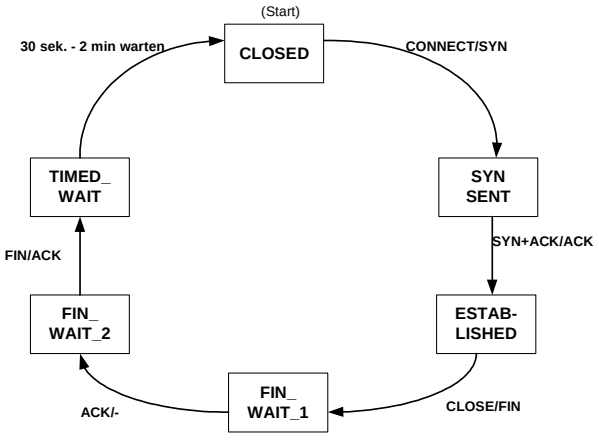
18. Erläutern Sie das Silly-Window-Syndrom bei TCP (s.157)

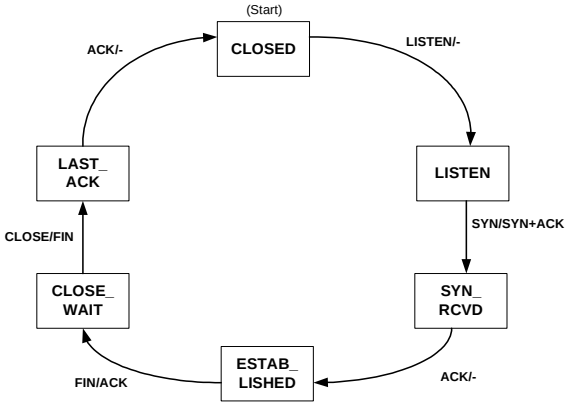
- Bereich Flusskontrolle
- Es tritt auf, wenn ein empfangener Anwendungsprozess die Daten bytweise ausliest, der Sender aber in größeren Nachrichten sendet
- Empfangspuffer wird immer um ein Byte geleert
- TCP-Instanz sendet dann in der ACK-PDU mit dem Hinweis, dass wieder ein Byte übertragen werden kann.
- Lösung ist die von CLARK: Hier wird der Sender zurückgehalten, eine ACK-PDU zu senden, bis man eine vernünftigen Fenstergröße senden kann.

19. Wozu dient das Slow-Start-Verfahren bei TCP? Beschreiben Sie das Verfahren kurz.(s.165)

- Vgl. Aufgabe 17
- Es dient dazu Stauprobleme im Netz zu vermeiden
- Kommt keine Antwort vom Empfänger zurück wird die Datenübertragung vom Sender gedrosselt
- Der Sendekredit ergibt sich aus min{Überlastungsfensters, Empfamgsfensters}D.h. der Sendekredit einer Verbindung darf nich größer sein, als das Min- aus der Größe des Überlastfensters und des Empfangsfensters (Fenstergröße der Flusskontrolle)
- TCP tastet sich an die optimale Datenübertragungsrate ran

20. Wozu dienen die beiden Zustände TIMED_WAIT und CLOSE_WAIT im TCP-Zustandsautomaten? Gehen Sie dabei kurz auf den Verbindungsabbau ein.





CLIENT SERVER

- Jedes Protokoll kann durch Zustandsautomaten dargestellt werden

Zustand	Beschreibung

CLOSED	Keine Verbindung aktiv oder anstehend
LISTEN	Der Server wartet auf eine ankommende Verbindung
SYN RCVD	Ankunft einer Verbindungsanfrage und Warten auf Bestätigung
SYN SENT	Die Anwendung hat begonnen, eine Verbindung zu öffnen
ESTABLISHED	Zustand der normalen Datenübertragung
FIN WAIT 1	Die Anwendung möchte die Übertragung beenden
FIN WAIT 2	Die andere Seite ist einverstanden, die Verbindung abzubauen
TIMED WAIT	Warten, bis keine Pakete mehr kommen
CLOSING	Beide Seiten haben versucht, gleichzeitig zu beenden
CLOSE WAIT	Die Gegenseite hat den Abbau eingeleitet
LAST ACK	Warten, bis keine Pakete mehr kommen

- Befehle die nur beim aktiven Partner genutzt werden
- Befehle die nur beim passiven Partner genutzt werden
- Verbindungsabbau:
    - Aktiver Parter (im Sinne des Abbaus) initiiert Abbau
    - Einleitung durch die close-Funktion
    - AKTIV. Sendet disconnect-Request-PDU (FIN Bit=1) geht in den Zustand FIN-WAIT ; es wird keine weitere Data-PDU mehr gesendet, dürfen aber noch empfangen werden
    - Nach dem erhalten einer antwort mit FIN-Bit=1 und ACK-Bit=1und dem senden einer erneuten ACK-PDU kommt der Zustand TIMED_WAIT. Hier wird dann ein Time-Wait-Timer aufgezogen und zwar au die doppelte Paketlebensdauer (30 sec max 2 min.)
    - Zustand CLOSE Verbindung beendet
    - Der Status wird im sog. TCB(Transmission Control Block) durch die T-Instanz verwaltet wie auch die Variablen: Fenstergröße, Größe des Überlastungsfensters etc.

21. Nennen Sie zwei Timer, die bei TCP verwendet werden und beschreiben –sie kurz deren Aufgabe.

- Retransmission Timer:
  Dieser Timer dient der Überwachung der Übertragung der TCP-Segmente nach dem sog. Karn-Algorithmus und wird für jede einzelne Übertragung verwendet. Wenn ein Timer abläuft, wird er verlängert und das TCP-Segment wird erneut gesendet (Übertragungswiederholung)

- Keepalive Timer
  Hier wird geprüft ob ein Partner, der schon längere Zeit nicht gesendet hat, noch lebt. Läuft der Timer ab, überprüft eine Seite durch das Senden einer Nachricht, ob der Partner noch lebt. Kommt keine Antwort zurück, wird die Verbindung abgebaut.
- Time-Wait-Timer:
  Für Verbindungsabbau. Läuft über doppelte Paketlebensdauer. Dabei soll sicher gestellt werden, dass alle Pakete bei einem Abbau noch übertragen werden

22. Was unternimmt die empfangene UDP-Instanz , wenn eine UDP-PDU ankommt? Gehen Sie hier auf den Sinn des UDP-Pseudoheaders ein

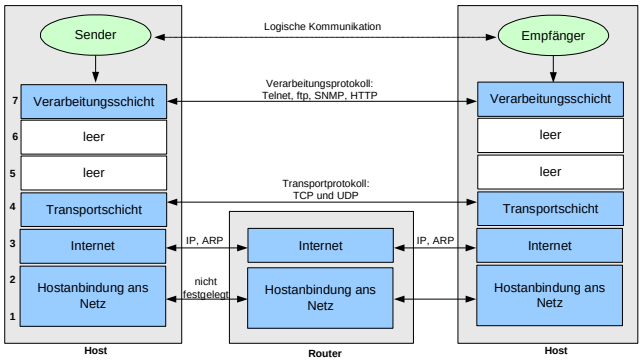
- Der Header:
  - UDP-Quell-Port-Nummer:
    - Nummer des Sendenden Ports
  - UDP-Ziel-Portnummer:
    - Nummer des empfangenden Ports, also der addresierte Partner
  - Länge:
    - Hier wird die Größe des UDP-Paketes inkl. Des Headers in Byte angegeben. Notwending, da UDP-PDUs keine feste Länge haben
  - Prüfsumme(optional):
    - Prüft das Gesamtpaket in Verbindung mit einem Pseudo-Header
  - Daten
    - Nettodaten des Datagramms (Nachrichten)
- Prüfsumme ist die einzige Möglichkeit einigermaßen sicher zustellen, dass der richtige Empfänger das Datagramm erhalten hat
- Pseudo Header:Vor dem berechnen der Prüfsumme wird ein virtueller Header gebildet mit folgenden Feldern:
  - IP-Adresse des Senders
  - IP-Adresse des Empfängers
  - Zero, Protokoll, UDP-Länge(ohne Pseudo Header)
- Der Empfänger muss bei Empfang einer UDP-Nachricht, die eine Prüfsumme enthalten, folgendes unternehmen:
  - Ip-Adresse aus dem ankommenden IP-Paket lesen.
  - Der Pseudo-Header muss zusammengebaut werden
  - Die Prüfsumme muss ebenfalls berechnet werden
  - Die mitgesendete Prüfsumme mit der berechneten vergleichen
- Sind beide Summe identisch, hat man die Gewissheit, dass das Datagramm seinen Zielrechner und auch den richtigen UDP-Port erreicht haben muss.
- Eine Fehlerbehebung findet aber nicht statt. Fehlerhafte Pakete werden nicht an die Anwendung weitergegeben sondern meistens verworfen

23. Nennen Sie 2 Vorteile von UDP im Vergleich zu TCP (S.174)?

- Keine explizite Aufbau- und Abbauphase erforderlich. Protokolle sind einfach zu implementieren. Für jede Verbindung braucht man ein Port
- UDP kann auch Multicasting und Broadcasting. D.h. Eine Nachricht, die einen Produzenten-Prozess erzeugt, mit einer einzigen UDP-PDU an mehrer Partner senden
- Senderarte wird nicht gedrosselt, es können so evt. Nachrichten verloren gehen, aber für Audio- und Video-Ströme kann das günstiger sein.

24. Suchen Sie die Datei etc/services in einem Unix- oder Windows-System und schauen sich den Inhalt an

25. **Suchen sie in den Regeln….**
    - TcpTimedWaitDelay (TIMED_WAIT)=
    - TcpMaxDataRetransmissions (wie oft wird eine Übertragungswiederholung durchgeführt)
    - TcpWindowSize (Fenstergröße)=64512
    - TcpMaxTransmission (Wie oft wird Verbindungsaufbauwunsch wiederholt)=
    - MaxUserPort (Wie hoch ist die höchstmögliche Portnummer im System?)=
26. **Wozu dienen die Stati SYN_RECVD, SYN_SENT, TIMED_WAIT, CLOSE_WAIT des TCP-Zustandsautomaten)** Betrachten Sie mit dem Kommando natstat die Zustände diverser TCP-Verbindungen, die auf ihrem Rechner laufen
27. **Welchen Sinn hat der UDP-Pseudo-Header**
    Siehe aufgabe 23
28. **Übernimmt eine UDP-Instanz die Aufgabe der Segmentierung eines langen Datagramms oder muss diese Aufgabe das Anwendungsprotokoll erledigen?**
    - Die UDP-Instanz wickelt bei Bedarf eine Segmentierung/Desegmentierung ab, übernimmt aber sonst keine weiteren Aufgaben zur Datenübertragung
    - Die Datagramme haben eine Länge von 16 Bit. Ein Länge eines UDP-Paketes ist min. 8 Byte (Header) und max 2^{16}-1=65.535 Byte Lang (Netto: 2^{16}-1-8= 65.527 Byte)
    - Man sollte diese länge nicht überschreiten da sonst eine Fragmentierung statt findet und die Wahrscheinlichkeit steigt, dass Datagramme verloren gehen
29. **Erläutern Sie kurz, was bei einer negativen Quittierung für eine Transport-PDU passiert, wenn in einem Netzwerk mit hoher Pfadkapazität eine fensterbasierte Flusskontrolle mit einem großen Fenster angewendet wird und die Übertragungswiederholung im Go-Back-N-Verfahren erfolgt.**
    Siehe Aufgabe 8
    - Negative QuittierungS.144:
      Der Empfänger sendet nur eine NCK zurück, wenn die Nachricht nicht beim Empfänger angekommen ist. Nachricht wird erneut beim sender angefordert
    - Fensterbasierte Flusskontrollen (Sliding-Window-Verfahren) (S.147):
        - Empfänger vergibt Sendekredite (max. Anzahl an Bytes). Der Kredit verringert sich bei jedem Senden. Der Empfänger kann den Sendekredit durch positive Quittierung erhöhen
        - Für Kommunikation werden vier Folgenummern-Intervalle verwendet

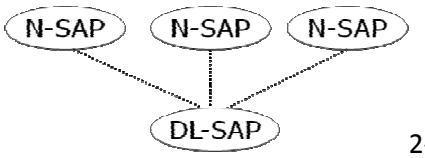


    - Das linke Intervall sind Folgenummern, die gesendet und vom Empfänger bereits bestätigt wurden

- Das zweite Intervall von links stellt alle Folgenummern dar, die gesendet aber vom Empfänger nochnicht bestätigt worden sind. Zeiger base verweist auf den NAfang dieses Intervalls
- Nächste Intervall gibt alle Folgenummer sn, die noch verwendet werden dürfen, ohne eine weiter Bestätigung vom Empfänger eintritt. Zeiger nextseqnum zeigt auf den Anfang des Intervalls
- Vierte Intervall sind Folgenummern die noch nicht verwendet werden dürfen

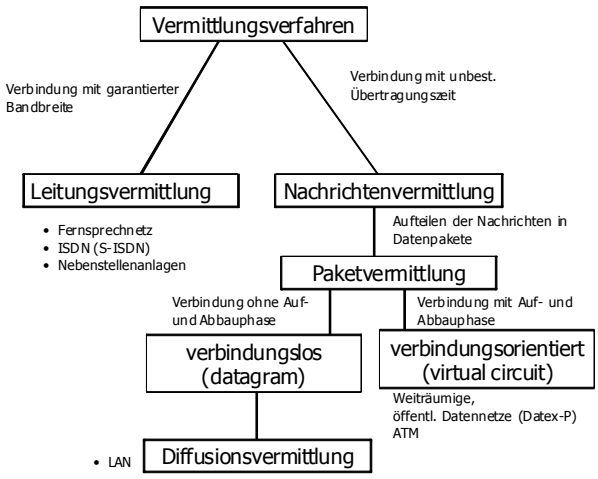
Kontrollfragen Vermittlungsschicht

1. **Nennen Sie 2 Aufgaben der Vermittlungsschicht und beschreiben Sie diese kurz S.66.**
    - Vermittlung (switching): Verbindungsherstellung, Halten und der Abbau einer Verbindung
    - Endsysteme kommunizieren über einen oder mehrere Netzknoten (Knoten, Router)
    - Übertragungswege werden von Knoten zu Knoten bereitgestellt (Teilstrecken)
    - Fehlersicherung findet auf der Teilstrecke statt
    - Schnittstelle zur Vermittlungsschicht, ist auch meist die Netzbetreiberschnittstelle
    - Wegewahl (Routing)
    - Multiplexen und Demultiplexen
    - Multiplexen:
        - Gemeinsame Verwendung einer Teilstrecke, also einer Schicht-2-Verbindung, für mehrere Schicht-3-Verbindungen
        - Erster Schicht-3-Verbindungsaufbau baut auch die Teilstreckenverbindung auf
        - Weitere Schicht-3-Verbindungen können dann bestehende Schicht-2-Verbindung nutzen

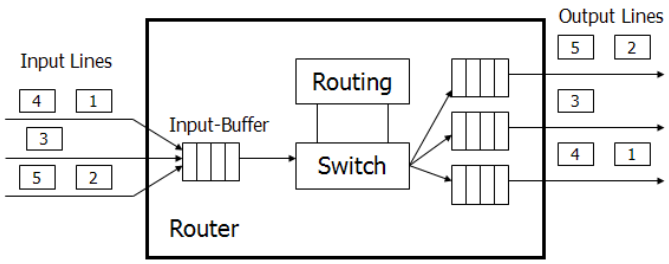


2-schicht

    - Staukontrolle (Congestion Control)
    - Segmentierung und Reassemblierung (Fragmentierung und Defragmentierung)
2. **Was unterscheidet die Vermittlungsverfahren „Leitungsvermittlung“ und „Nachrichtenvermittlung“ (speziell Paketvermittlung) (s.67)?**



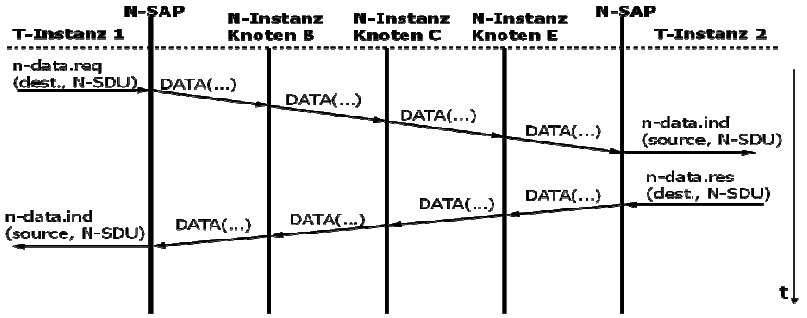
- Leitungsvermittlung
  - Alle auf dem Netzpfad benötigen Ressourcen wie z.b. Bandbreite und Pufferspeicher in den Netzknoten werden für die Dauer der Verbindung vorab reserviert.
  - Typische Bsp. Für Leitungsvermittlung sind ISDN, Telefon: dabei werden physikalische Verbindungswege durch das Netzwerk geschaltet
  - Eine feste Bandbreite wird garantiert und zwar unabhängig von dem, was tatsächlich übertragen wird.
  - Sehr wahrscheinlich, dass Bandbreite verschwendet wird (Telefonhörer daneben legen)
  - Teuren Leitungen zwischen den Netzknoten werden in heutigen Netzen mit Hilfe von Multiplexverfahren in mehreren Schaltkreisen aufgeteilt.
  - Verfahren:
    - Frequenzmultiplexing(FDM)
    - Timemultiplexing(TDM): Bei jeder Ende zu ende Verbindung zw. 2 Knotenrechnern wird ein Zeitschlitz zugeordnet in dem dann eine bestimmte Bitrate möglich ist
- Nachrichtenvermittlung
  - Werden immer komplette Nachrichten übermittelt zw. Den Netzwerkknoten
  - Nachrichten werden erst weitergesendet wenn sie vollständig sind→Store-and-Forward-Verfahren
  - Paketvermittlung:
    - Hier werden längere Nachrichten in einzelne Datenpakete unterteilt und als Datagramme oder über eine vorher aufgebaute sog. Virtuelle Verbindung übermittelt
    - Keine Ressourcen werden vorab reserviert, sondern dynamisch zur Laufzeit ermittelt; Folge: Kann passieren, dass 2 Kommunikationspartner auf eine Verbindung etwa in einer Warteschlange warten müssen, bis erforderliche Ressource frei wird
    - Netz überträgt Daten immer mit Zieladresse evt. über mehrere Knoten mit Zwischenspeicherung und zerlegt sie ggf. in einzelne Pakete (N-PDUs).
    - Paketvermittlung effizienter als Leistungsvermittlung
    - Bsp.: Internet, Breitband ISDN
    - Bsp. Wie Knoterechner (Router)arbeiten.
      - Über eine oder mehrere Eingangsleitungen werden ankommende Pakete entgegen genommen und über eine Switching- oder Routing-Logik an die passende Ausgangsleitung weitergeleitet



- Einfache Form der Datagramm-Vermittlung ist die **Diffusionsvermittlung**

- Hier sendet jeder Knoten die empfangenen Pakete an alle Nachbarknoten weiter
    - mit Ausnahme des sendenden Knotens!
- Sinnvoll bei Netzen mit geringer Knotenanzahl
- Klassische Vermittlungsform **in LANs**
    - Siehe z.B. Ethernet-LAN

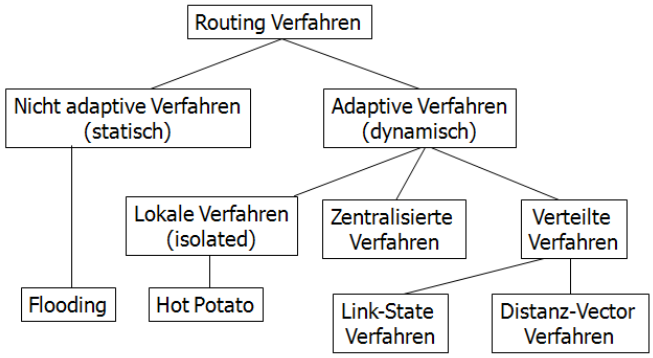
- Verbindungslos:
    - Datagramme (N-PDUS) werden ohne vorherigen Verbindungsaufbau gesendet
    - Jedes Datagramm erhält Quell-und Zieladresse und der optimale Routing-Weg wird berechnet
    - Nur einfacher Data Dienst zum Senden von Datagrammen ist erforderlich



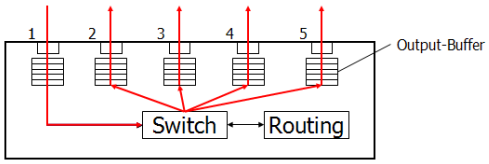
- Verbindungsorientierten Dienst:
    - VC (Virtual Circuits=scheinbare Verbindungen): Verbindung bleibt hier für die Dauer der Übertragung erhalten. Bei VC, werden keine physikalischen Durchschaltungen genommen, sondern die beim Verbindungsaufbau ermittelte Routing-Information in den Knoten verwendet.
        - 3 Phasen: Verbindungsaufbau (connect-Dienst), Datenübertragung (data-Dienst) und Verbindungsabbau (disconnect-Dienst)
        - Verbindung über 2 endsysteme wird schrittweise über Teilstrecken aufgebaut.
        - Knoten müssen in der Verbindungsaufbauphase Info über das Mapping von eingehenden Paketen zu Ausgangsteilstrecke speichern, also eine gewisse Kontextverwaltung (Status und Verbindungstabelle) durchführen

3. **Warum werden virtuelle Verbindungen in der Schicht 3 auch scheinbare Verbindungen genannt S. 70?**
    - Virtual Circuits werden auch **„scheinbare Verbindungen“** genannt
    - Verbindung bleibt für die Dauer der Datenübertragung erhalten
    - (siehe Aufgabe 2)
4. **Erläutern Sie den Unterschied zwischen statischen und dynamischen Routing S.70?**
    - Notwendig bei paketorietirtenNetzen, wenn in einem Netzwerk alternative Wege zwischen den Endsystemen vorhanden sind

- Verschiedene Routing-Kriterien und -Algorithmen sind möglich:
  - Netzlast
  - Suche der geringsten Entfernung
  - Möglichst geringe Anzahl von Hops (Anzahl der zu durchlaufenden Knoten)



- **Statische** Algorithmen:
  - Keine Messungen, vorher ermittelte Metriken
  - Statische Routing-Tabellen (enthält fest vorgegebene Routen), die bei der Knotenkonfigurierung eingerichtet werden (vor Beginn des Betriebs)
  - Bsp: Flooding, Shortest Path
  - Flooding:



    - Eingehende Pakete werden über alle Teilstrecken weiter versendet
    - Pakete werden nicht über die eingehende Leitung und nur einmal weiter versendet
    - Statischer und sehr einfacher Routing-Algorithmus
    - Viele doppelte Pakete und somit ineffizient
- **Dynamische** (adaptive) Algorithmen:
  - Verkehrsmessungen
  - Routing-Tabellen werden dynamisch angepasst (Metriken)
  - Optimierungskriterien können sich dynamisch verändern und werden im Algorithmus berücksichtigt
  - Möglichkeiten:
    - **Isoliertes Routing**: Knoten trifft Entscheidungen alleine (Hot Potato)
    - **Zentrales** Routing über einen zentralen Knoten (Routing-Kontroll- Zentrum), Zentrale ermittelt und überträgt alle Routing-Tabellen
    - **Dezentrales** Routing mit Routing-Funktionalität in jedem Knoten . Routing-Tabelle wird im Zusammenspiel ermittelt
  - Beispiele (heute üblich):
    - Distance-Vector-Routing

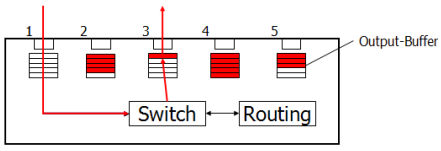
    ursprünglicher Algorithmus im ARPANET, RIP

- Link-State-Routing

löste Distance-Vector-Routing Ende der 70er im ARPANET ab

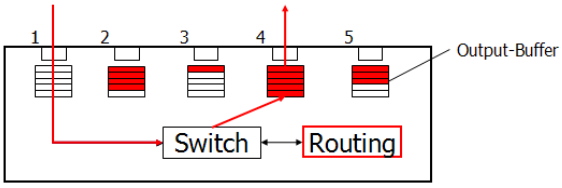
- Hierarchisches Routing

Beispiel :**Hot Potato** (dynamisch/loakes Verfahren (isolated)):



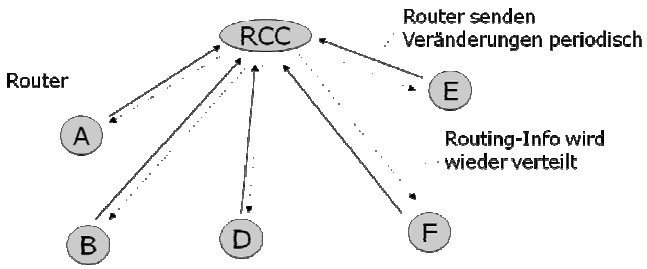
- Eingehende Pakete werden so schnell wie möglich zum nächsten Netzknoten gesendet
- Es wird der Ausgang mit dem am geringsten belegten Output-Buffer gewählt
- Dynamischer und sehr einfacher Routing-Algorithmus
- Wird in seiner reinen Form nicht verwendet

Beispiel: **Link-State Verfahren** (dynamisch/Verteilt)

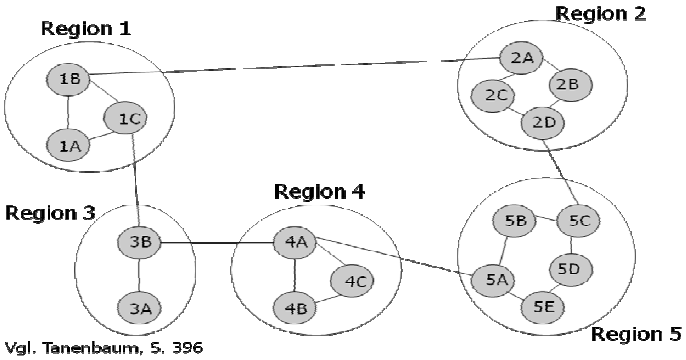


- Jeder Router verwaltet eine Kopie der Netzwerktopologie und berechnet selbst die optimale Route für ein Paket
- Verschiedene Optimierungskriterien sind möglich
- Dynamischer und verteilter Routing-Algorithmus
- Router muss komplexe Aufgaben erledigen

5. **Was versteht man unter einem zentralen Routing-Verfahren? Handelt es sich hier um eine statisches oder adaptives Verfahren (s.70)?**
   - Adaptives Verfahren
   - Es gibt ein Routing Control Center (RCC): hier werde sämtliche Routing-Infos gesammelt
   - Verfahren ist nicht fehlertolerant (Engpass) aber konsistent, jedoch Gefahr der veralteten Informationen



6. **Welche Vorteile bringt ein hierarchisches Routing?**
   - Große Netze erfordern (zu) große Routing-Tabellen mit langen Suchzeiten
   - VORTEIL: Verringerung der Routing-Tabellen: Netze hierarchisch organisieren
     - Z.B mit folgenden Hierarchiestufen: Regionen – Cluster – ...



Vgl. Tanenbaum, S. 396

Routing-Tabelle für 1A (vorher)

	Leitung	Teilstr.
1A	--	--
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Ziel

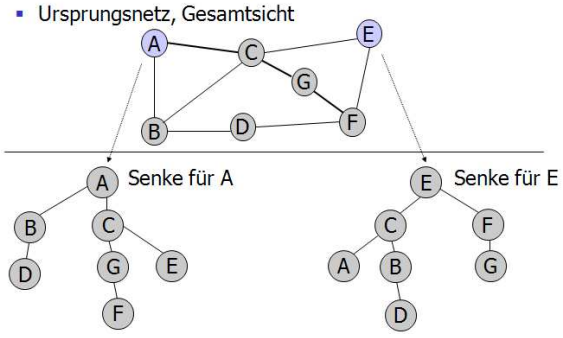
Routing-Tabelle für 1A (nachher)

Ziel	Leitung	Teilstr.
1A	--	--
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

- Reduktion von 17 auf 7 Einträge!
- Nachteil: Ansteigende Pfadlängen
- Es gibt bestimmte Knoten die nach außen hin bekannt sind und Datagramme weiterleiten

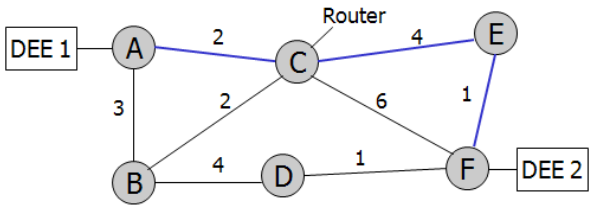
7. Erläutern Sie kurz das Optimierungsprinziep beim Routing (S. 72)

- Wenn Router C auf dem optimalen Pfad zwischen A und F liegt, dann fällt der Pfad von C nach F ebenso auf diese Route. (Wenn ACF optimal, ist auch AC bzw. CF optimal)
- Die Annahme, es existiert eine bessere Route zwischen C und F, führt zu einem Widerspruch
- Optimierungsprinzip angewendet auf das Routing:
  - Die optimalen Routen von allen Quellen zu einem bestimmten Ziel bilden einen **Baum**, dessen Wurzel das Ziel ist
  - Dieser Baum enthält keine Schleifen und heißt **Sink Tree** oder **Senke**
- Ziel von Routing-Algorithmen
  - Senken für alle Router ermitteln
  - Senken für das Routing nutzen



- Beim Shortest-Path-Verfahren wird ein Graph des Teilnetzes statisch erstellt

- Jeder Knoten entspricht einem Router, Kanten sind Leitungen
- Kanten werden beschriftet(„Pfadlänge“)
- Metrik kann aus verschiedenen Kriterien berechnet werden:
    - Entfernung
    - Bandbreite, Durchschnittsverkehr etc.
- Berechnung des kürzesten Pfads z.B. über Dijkstras Algorithmus
    - Beispiel: Der kürzeste Pfad zwischen DEE 1 und DEE 2 geht von A nach F über A C E F
    - Summierte Pfadlänge = 7



8. Was versteht man im Distance-Vektor-Verfahren unter dem Count-to-Infinity-Problem und wie verhält sich das Verfahren im Hinblick auf Konvergenz? Begründen Sie Ihre Antwort (s.72).

- Jeder Router führt eine **dynamisch aktualisierte Routing-Tabelle** mit allen Zielen
    - Einträge enthalten bevorzugte Ausgangsleitung zu einem Ziel

Ziel	Distanz	Nächster Knoten	Hops

- Distance-Vector kommt daher, dass eine Route zu einem Ziel aus einer Kombination aus Entfernung und Richtung (Vektor) angegeben wird.
- Voraussetzung: Ein Router kennt die Entfernung zu allen Zielen, wobei die Berechnung mit Hilfe der Nachbarknoten durchgeführt wird.
- **Metrik** kann z.B. sein:
    - Verzögerung in ms
    - Anzahl der Teilstrecken (**Hops**) zum Ziel
- Verteilt – iterativ – asynchron (unabhängig voneinander)
- Benachbarte Router tauschen Routing-Information aus
- **Schleifen** möglich „**Count-to-Infinity-Problem**“
    - Bei Ausfall eines Links evtl. keine Terminierung mehr sichergestellt
- **Gute Nachrichten** verbreiten sich schnell
- **Schlechte Konvergenz**
    - Schlechte Nachrichten z.B. über nicht mehr verfügbare Routen, verbreiten sich sehr langsam in Netz
- Nach einiger Zeit, nach dem Netzstart (Konvergenzdauer) verfügen alle Router über optimale Routing-Tabellen
- Durch Zyklisches versenden der bekannten Entpfernungsvektoren, breitet sich die Info im Netz aus.
- Eigenschaften zusammengefasst:

- Verfahren ist verteilt. Nachbarn tauschen Info über die nächsten Umgebungen aus, die Router berechnen die besten Pfade aus ihrer Sicht und tauschen erneut Info aus
- Verfahren ist iterativ, und wird zyklisch wiederholt
- Einzelne Knotenarbeiten selbstständig
- Gute Nachrichten verbreiten sich schnell und schlechte eher langsam
- Bei Ausfall eines Links ist evtl. keine Terminierung mehr sichergestellt

Knoten A

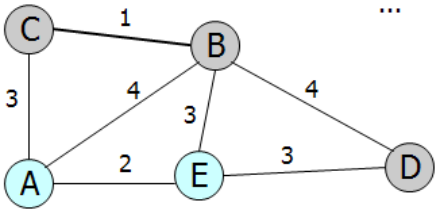
Ziel	Distanz	Nächster Knoten	Hops
B	4	B	1
C	3	C	1
E	2	E	1
D	5	E	2

Knoten E

Ziel	Distanz	Nächster Knoten	Hops
A	2	A	1
B	3	B	1
C	4	B	2
D	3	D	1

...

Nach einiger Zeit (Konvergenzdauer) verfügen alle Router über optimale Routing-Tabellen



- In der Routing-Tabelle von A: A lernt hier z.B. von den benachbarten Knoten, dass der optimale Weg zu D über E in 5 Hops (in dem Fall die Kosten) ist

9. Welche Art von Routing-Verfahren ist das Distance-Vector-Verfahren und wann wird es in IP-Netzen auch heute noch eingesetzt?

- Dynamisches verteiltes verfahren
- Wann wird es in IP-Netzen heute noch eingesetzt? im Internet z. B. als RIP und IGRP implementiert.

10. Nennen Sie drei mögliche Metriken, die ein Routing Verfahren zur Ermittlung der optimalen Routen nutzen kann!

- Eine **Routing-Metrik** ist ein Wert, mit dessen Hilfe ein Routing-Algorithmus feststellen kann, ob eine Route im Vergleich zu einer anderen besser ist
- Beispiel:
  - Bandbreite
  - Bandbreite,
  - Verzögerung,
  - Hop Count,
  - Pfadkosten, etc.

11. Wie sieht ein einzelner Router im Link-State-Routing-Verfahren die aktuelle Netzwerktopologie (s.73/74)?

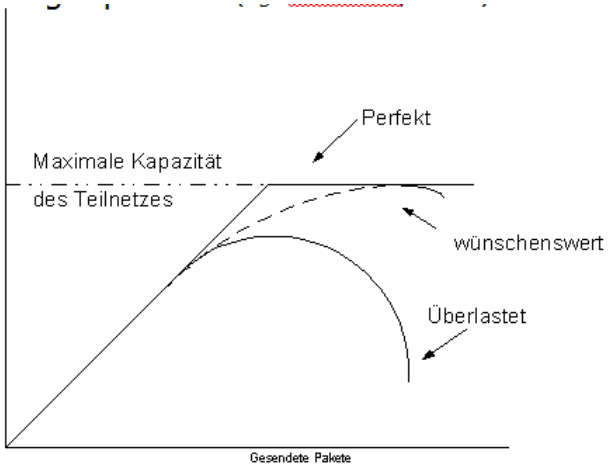
- Jeder Router verwaltet eine **Kopie der Netzwerktopologie** (in Link-State-Datenbank)
- **Zielsetzung**: Jeder Knoten muss alle Kosteninformationen kennen
- Jeder Router verteilt die lokale Information per Flooding an alle anderen Router im Netz

- Die Berechnung der Routen erfolgt **dezentral**
- Jeder Knoten errechnet den **absolut kürzesten Pfad**
- **Berechnung der kürzesten Pfade** z.B. über Shortest-Path-Algorithmus (z.B. Dijkstras Algorithmus)
- **Keine Schleifen** möglich, da jeder Knoten die gleiche Information über die Topologie besitzt
- Schnelle Reaktion auf Topologieänderungen möglich
- Heißt deshalb Link-State-Verfahren, da es die globale Zustandsinformation des Netzes mit den Kosten aller Verbindungsleitungen (Links) kennen muss. Knoten kennen zwar am Anfang nicht alle anderen Knoten, aber durch den Empfang von sog. Link-State-Broadcasts (Flooding) wird die Information unter den Knoten ausgetauscht.

12. Sind im Link-State-Routing-Verfahren Schleifen möglich? Begründen Sie ihre Entscheidung!
    - **Keine Schleifen** möglich, da jeder Knoten die gleiche Information über die Topologie besitzt
    - Siehe Aufgabe 11

13. Was versteht man unter einem Leaky-Bucket-Verfahren S. 75/76

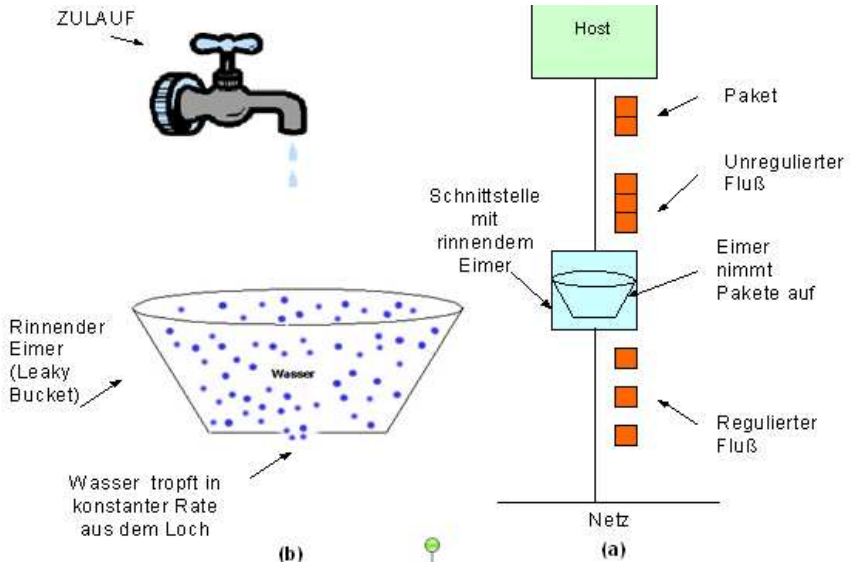
- **Staukontrolle du Überlastung:**
- Zu viele Pakete (mehr als die Übertragungskapazität) in einem Netz führen **zum Abfall der Leistung** → Überlastung (Congestion), Verstopfung
- Ursachen:
    - Viele Pakete zu einer Zeit → Lange Warteschlangen
    - Langsame Prozessoren in den Netzknoten
    - Zu wenig Speicher in den Netzknoten
- Eine Überlastung kann zu einem **Teufelskreis** führen
    - Pakete gehen verloren
    - Pakete werden evtl. in Netzknoten verworfen
    - Sendungswiederholungen erhöhen die Last
- Bei übermäßiger Verkehrsbelastung des Netzes sinkt die Leistung rapide ab“



- Durch Staukontrolle sollen Verstopfungen bzw. Überlastungen im Netz vermieden werden
- Möglichkeiten der Staukontrolle: (vgl. Kerner, S.165ff)

- Lokale Steuerung (gehört zur Schicht 2), da sie sich auf Einzelleitungen bezieht
- Ende-zu-Ende-Steuerung zwischen Endsystemen (Schicht 4)
- Globale Steuerung über das gesamte Netz (Schicht 3)

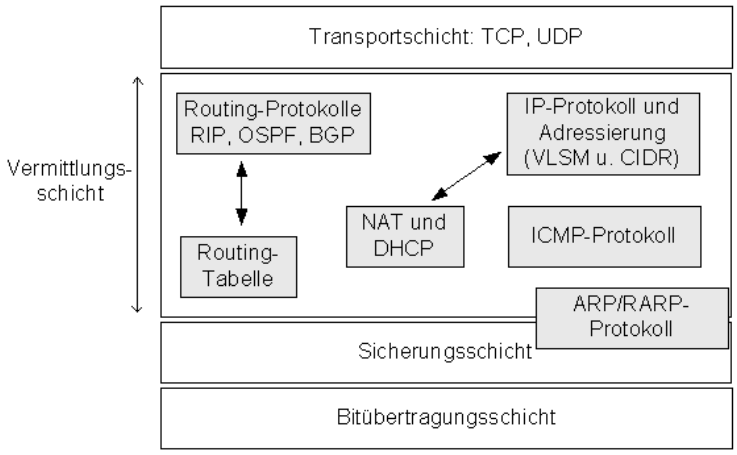
- Die Schichten 2-4 können Maßnahmen ergreifen
- Im Gegensatz zur Flusssteuerung ist die Staukontrolle ein Mechanismus mit **netzglobalen Auswirkungen**
- Maßnahmen der Vermittlungsschicht:
  - Virtuelle Verbindungen statt Datagrammen in Teilnetzen
  - Warteschlangen verwalten
  - Routing-Algorithmus
  - Verwaltung der Lebensdauer von Paketen
- **Traffic Shaping**
  - Eine wesentliche Ursache für Überlastungen sind **„Verkehrsspitzen“**
  - **Traffic Shaping** ist eine Maßnahme zur Regulierung der durchschnittlichen Datenübertragungsrate von Endsystemen
  - Überwachung der Endsysteme (**Traffic Policing**) durch den Netzbetreiber
  - Besser realisierbar für virtuelle Verbindungen (virtual circuits) als für Datagramm-orientierte Netze
  - Nutzung des **Leaky-Bucket**-Algorithmus
    - **Endsysteme (Hosts) verfügen über Netzwerkschnitt-stellen (Kernel, Netzwerkkarte) mit einer internen Warteschlange → rinnender Eimer**
    - **Wenn die Warteschlange voll ist, wird ein neues Paket schon im Endsystem verworfen**
    - **Sender, Empfänger und Netzwerk müssen sich einig sein**
    - **Flussspezifikation für virtuelle Verbindungen bei Verbindungsaufbau**
    - **Man einigt sich über die max. Paketgröße, die max. Übertragungsrate,...**



14. Was ist ein autonomes System im Internet und welche Arten von autonomen Systemen kennen Sie S. 77?

ALLGEMEIN INTERNETÜBERBLICK:

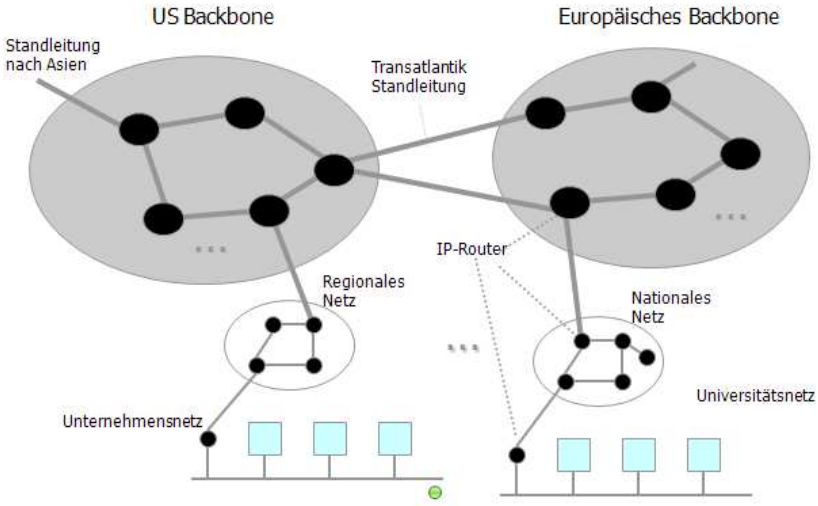
- **Internet paketorientiertes Netzwerk**
- **Wichtigste Aufgabe der Vermittlungsschicht hier: Routing (gibt ver. Routing Protokolle)**



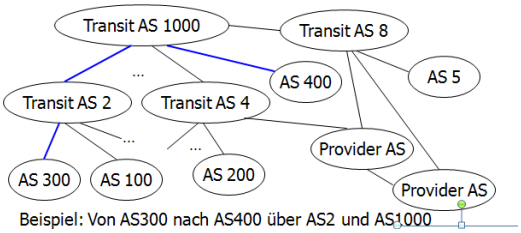
- **ICMP: Steuerprotokoll von Übertragung von Fehlermeldungen**
- **IP (Internet Protokoll): paketvermittelndes, verbindungsloses Protokoll. Befördert Datagramme von einer Quelle zu einem Ziel. Datagramme werden zerlegt und zum Schluss wieder zusammengeführt. Datenübertragung mit Best-Effort-Prinzip**
- **Hat spezielle Protokolle für Adressierung und Adresskonfiguration wie DHCP (Dynamic Host Configuration Protocol) und NAT (Network Address Translation)**
- **ARP (Adress Resolution Protocol) und RARP (Reverse Address Resolution Protocol): Mapping der MAC-Adressen auf die IP-Adressen**

AUTONOME SYSTEME:

- **Autonome Systeme (AS) sind eigenständig verwaltete Teilnetze**
- Das Internet ist eine **hierarchische Organisation** des Netzwerks
- **Große Backbones** sind über Leitungen mit hoher Bandbreite und schnellen Routern verbunden
- An den Backbones (Netzwerkrückrad) hängen **regionale Netze**
- An den regionalen Netzen hängen die **Netze von Unternehmen, Universitäten, Internet Service Providern** (ISP),...
- Der Zugriff über das Internet von Deutschland aus auf einen Server in den USA wird über mehrere IP-Router geroutet



- Autonome Systeme haben sich unterschiedlich entwickelt → z.B. verschiedene Routing-Strategien
- Es gibt derzeit mehrere Tausend autonome Systeme weltweit
- Jedes AS hat eine **eindeutige Nummer**
  - 11, Harward-University
  - 1248, Nokia
  - 2022, Siemens
  - 3680, Novell
  - 4183, Compuserve
  - 6142, Sun
- Typische AS sind:
  - Institutionen (Universitäten,...)
  - Regionale Internet-Provider
  - Transit AS: Internet-Backbone, hohe Bandbreite



Beispiel: Von AS300 nach AS400 über AS2 und AS1000

15. Was ist im globalen Internet ein TRANSIT-AS (S.77)?

- Transit AS: Internet-Backbone, hohe Bandbreite
- *Transit-AS* sind an andere Transit-AS angebunden und stellen die Serviceprovider für die vorgenannten drei Typen in der Form von Internet-Backbone-Netzwerken dar (Zwischenknoten). Ein Transit-AS ist also immer ein Provider für mindestens ein anderes AS.

16. Beschreiben sie kurz den Dienst, den IP für die darüber liegenden Schichten zur Verfügung stellt im Hinblick auf die Übertragungssicherheit (s.77)?

- **Routing**

17. Welches Vermittlungsverfahren verwendet die Internet Schicht (s.78)?

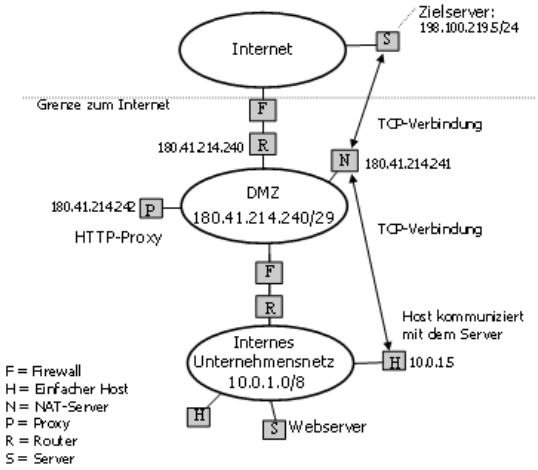
- Paketvermitteltes (datagramm-orientiertes) und verbindungsloses Protokoll der Vermittlungsschicht

18. Was versteht man unter einem Sink Tree im Sinne der Wegewahl ?

- **Siehe Aufgabe 7**

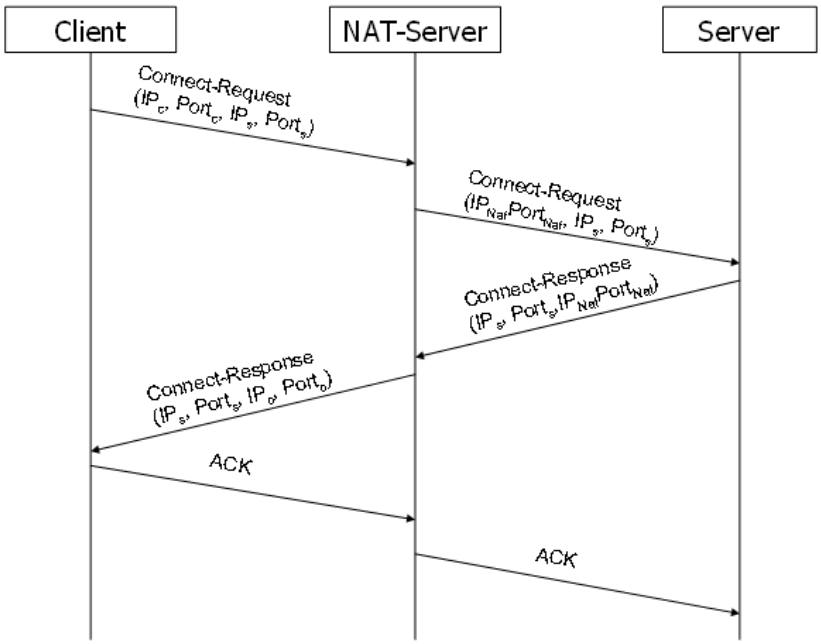
19. Was versteht man unter NAT (Network Address Translation) und welche Vorteile bietet das Verfahren (S.111)?

- Adressen eines privaten Netzes werden über Abbildungstabellen öffentlich registrieren IP-Adressen zugeordnet
- Interne IP-Adressen müssen keine öffentliche IP-Adresse haben
- Zuordnung kann 1:1 ergolgen (eine interne IP-Adr. Bekommt eine öffentliche IP-Adre.) oder aber mit IP Masquerading oder PAT(Port and Address Translation) werden alle internen IP-Adr. Auf genau eine öffentliche registrierte IP-Adresse abgebildet. Dafür werden Portnummern benutzt.
- Bei NAT handelt sich vorwiegend um eine Möglichkeit, die Sicherheit im Unternehmensnetz (oder Uni-Netzen) zu erhöhen. NAT/PAT werden heute in DMZ (De-Militarized Zone) eingesetzt, damit interne Rechner mit der Außenwelt ohne Verletzung der Sicherheit kommunizieren können.
- NAT dient auch dazu, Netzwerkadressen einzusparen
- Für ein Netz (Unternehmensnetz) benötigt man nur noch eine offizielle IP-Adresse
- Intern kann dann eine beliebige, nach außen nicht sichtbare, Netzwerknummer verwendet werden



- DMZ ist in einem Unternehmens oder Uni Netzwerk, dass an das Internet angeschlossen ist, angeschlossen. Schützt vor Angriffen auf Interne Hosts.
- DMZ eine Art Zwischen Netz
- Möchte Host aus Internen Netzwerk mit einem Host aus dem Internet kommunizieren, so geht das nur über das DMZ.
- In DMZ stehen die Rechner die nach außen hin sichtbar sein sollen.
- IP-Router oder NAT-Server arbeiten nach außen als Stellvertreter (Proxies) für alle internen Hosts.
- IP-Router bzw. NAT-Server „mappen“ bei NAT ankommende Pakete auf interne Hostadressen und umgekehrt.

- Dabei werden bei ausgehender Kommunikation wird das Feld Quell-IP-Adresse im IP-Header die IP-Adresse und im TCP-Paket der Quellport durch den NAT-Server eingetragen.
- Bei eingehender Kommunikation, wird Das Feld IP-Adresse ausgetauscht.
- Somit sieht man nur NAT-Server



- Bei Verbindungsaufbauwünschen von außen , die an einen internen Server gerichtet sind, wird bei TCP die Verbindung immer unterbrochen.--> Es gibt keine echte Ende-zu-Ende-Beziehung mehr
- Werden 2 TCP-Verbindungen aufgebaut: Eine von Client zu NAT und NAT zu internen Server. Weiß aber nur NAT-Server
- IP-Pakete werden bereits bei Aufbau verändert: NAT-Server ändert die Connect –Request PDU, indem er in das Feld Quell-IP-Adresse seine eigene Adresse schreibt.
- NAT verwaltet in Mapping-Tabelle welches Mapping er durchgeführt hat um auhc PDUs von der Gegenseite zuordnen zu können.
- Connect-Respons-PDU wird genauso maskiert, wobei hier die Adresse des Quellhosts eingetragen wird
-

20. Welche Aufgaben verrichtet ein NAT-Router im Rahmen der Adressierung für ankommende und abgehende IP-Pakete?

- Tauscht bei eingehender Kommunikation den Ziel-Adresse aus
- Bei ausgehender den Quell-Adresse, und Quell-Port (siehe Aufgabe 19)

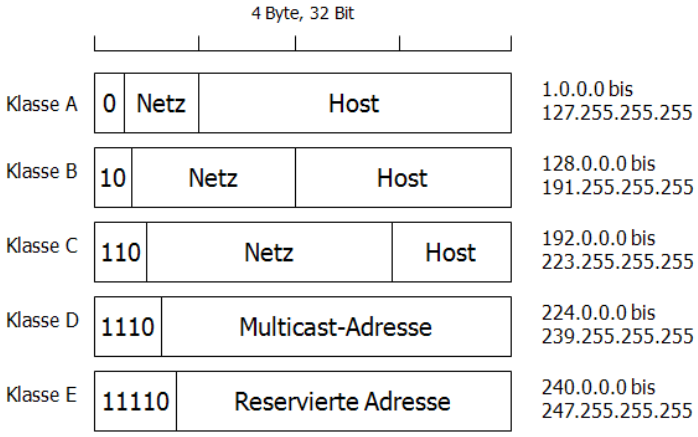
21. Warum muss in NAT-Router vor dem Weiterleiten eines vom globalen Internet ankommenden oder vom Intranet abgehenden IP-Paketes die Checksumme im IP-Header jedes Mal neu berechnen?

- Weil sich der TLL ändert

22. Nenne Sie den Unterschied zischen der klassischen Subnetz-Adressierung und dem Classless Interdomain Routing (CIDR (S. 85)). Welche Vorteile bringt CIDR für die Adressenknappheit im Internet?

EINSCHUB: ADRESSIERUNG in Internet-basierten Netzen:

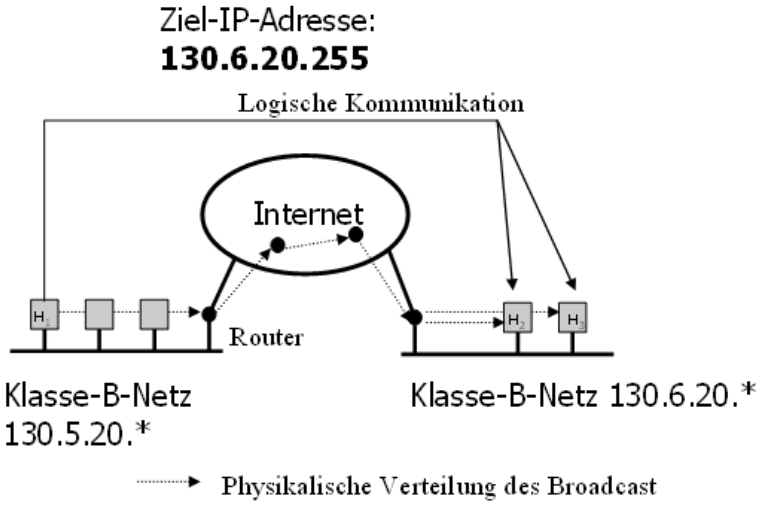
- **Rechnersystem im Internet heißt Host**
- **IP-Adresse ist nicht an den Host, sondern an den Netzzugang gebunden (z.B ist ein Host an Ethernet-Adapter angeschlossen, so ist diesem Adapter eine IP-Adresse zugeornet)**
- **Hosts können also mehrere IP-Adressen haben**
- **IP-Adressen sind in der IP-Version 4(IPv4) mit 32 Bit langen Adressen verfügbar. Also gibt es 2^{32}=4.294.967.296 IP-Adressen**
- **Adresse besteht aus einem Tupel: Hostnummer und Netzwerknummer**
- **IP-Adresse von Quelle und Ziel werden in allen IP-Paketen mit übertragen**
- **Es gibt verschiedene Adressformate**
  - **man unterscheidet die Klassen A, B, C, D und E**
- **Schreibweise für IP-Adressen in gepunkteten Dezimalzahlen, jeweils ein Byte als Dezimalzahl zwischen 0 und 255**
- **Beispiel:**
  - **Hexformat: 0xC0290614**
  - **Dezimalzahl: 192.41.6.20**



Alle Adressen der Form 127.xx.yy.zz sind Loopback-Adressen!

- **Die Klasse einer Adresse erkannt man an den ersten Bits**
  - **Klasse A beginnt mit einer binären Null**
  - **Router nutzen Info um eine Zieladresse zu interpretieren**
- **Klassen haben unterschiedliche Längen für Netz und Host**
  - **Klasse A: 1 Byte für Netz und 3 Byte für Host**
- **Spricht von /8 für Klasse A, /16 Klasse B, /24 Klasse c. Nach dem / stehen Bits für Netz→ Präfix-Schreibweise**
  - **Es gibt insgesamt 2^7-2 Netzwerkadressen der Klasse A, Sieben für Netzwerknummer reserviert sind. Es werden die Netzwerkadressen 0.0.0.0 (Standard-Router) und 127.0.0.0. (Loopback-Adresse) abgezogen. Hostadressen gibt es 2^{24}-2 ,abgezogen werden die Adressen mit lauter einsen und nullen.**
  - **Klasse B-Netze haben 2 Bit zur identifikation „10“ 2^{14} 16.384. Hostst 2^{16}-2 Hosts.**
  - **Klasse C hat 3 identifikation Bits also 2^{21} Netzadressen 2.097.152 und 245 Host (2^8-2)**
  - **Insgesamt 85, 5% belegt**

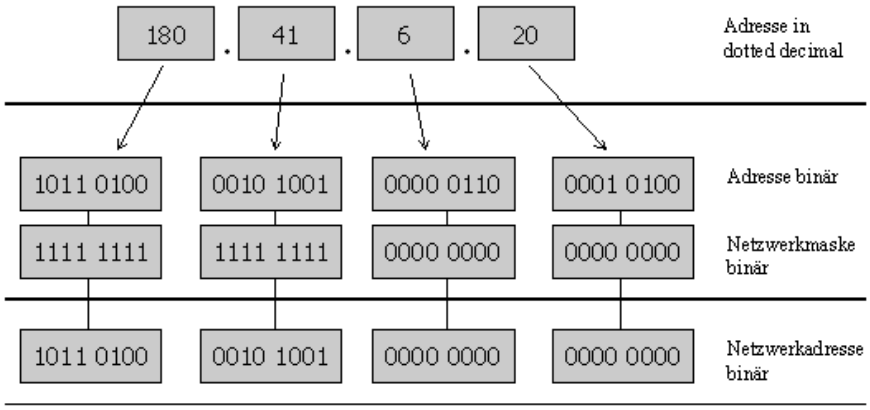
- **Klasse D ist für Multicast Adressen reserviert und Klasse E wird momentan nicht genutz.**
- **Besondere IP-Adressen sind:**
    - **Die niedrigste IP-Adresse 0.0.0.0. Ist ein „bestimmtes Netz oder bestimmter Host". Braucht man evtl. beim Booten (Hochfahren des BS) eines Hosts**
    - **Adresse mit Netzwerknummer aus lauter binären einsen und einem beliebigen Hostanteil, ermöglicht es Hosts, auf das eigene Netzwerk zu verweisen, ohne die Netzwerknummer zu kennen**
    - **Höchste Ip-Adresse 255.255.255.255 wir als Broadcast Adresse verwende. Beim Broadcast werden alle Hosts eines Netzwerkes mit einem Datagramm angesprochen. Alle Hosts nehmen also Pakete mit der Zieladresse 255.255.255.255 vom Netz und leiten sie an die Anwendungsprozesse weiter, die darauf warten.**
    - **Alle Adressen die mit 127. Beginnen sind Loopback-Adressen und für die interne Hostkommunikation reserviert. Pakete mit Zieladressen in diesem Bereich werden nicht auf das Netz gelegt.**



- **Broadcast:**
    - **Direktes:**
        - **Senden einer Broadcast-Nachricht an ein beliebiges Netzwerk im Internet und zwar direkt von einem Host eines anderen Netzwerks aus.**
        - **Router sendet das Paket über den entsprechenden Pfad zum Zielrouter, der dann den Broadcast in seinem lokalen Netzwerk sendet.**
        - **Adresse für den direkten Broadcast enthält die Netzwerknummer und im Host teil lauter binäre Einsen**
    - **Begrenztes (limited):**
        - **Bezieht sich auf das lokale Netzwerk und wird von den Routern nicht durchgelassen. Adresse für alle Netze gleich 255.255.255.255.**
- **Private Adressen:**
    - **1.0.0.0 mit einem Netzwerkanteil von 8 Bit (Netzwerkmaske 255.0.0.0./8)**
    - **172.16.0.0. mit einem Netzwerkanteil von 12 Bit (Netzwerkmaske 255.0.0.0./12)**
    - **Etc.**
    - **Werden von Routern besonders behandelt. Pakete mit der Ziel-Adresse werde vom Router nicht weitergeleitet und verlassen so nie das interne Netz. Wird gerne fürs Intranet genutzt.**

- **Netzwerkmasken und Routing:**
  - **Router müssen wissen welche Adressklasse in einem IP-Paket als Ziel Adresse ist.**
  - **Steht aber nicht im IP-Header, d.h. Router muss das auf andere weise ermitteln. In Routing-Tabellen gibt es noch die Info : Netzwerkmaske**
  - **32 bit breites Feld, hier ist für jedes Adressbit genau ein Bit zugeordnet ist. Steht ein Bit auf Binär 1 so ist das Bit in der IP-Adresse der Netzwerknummer zugeordnet. Bei ABC können das natürlich nur alle Bits der Netzwerknummer sein**
  - **Wenn Router Paket empfängt wird , legt er Netzwerkmaske über die IP-Adresse und ermittelt so die Netzwerkadresse und Hostadresse**

▪ Hier handelt es sich um eine Klasse B-Adresse, warum?

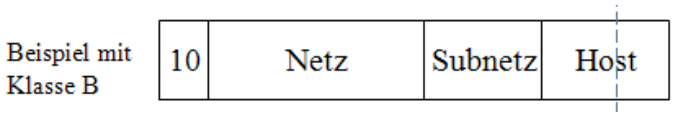


Logische Und-Verknüpfung der IP-Adresse mit der Netzmaske
Die Netzwerkadresse ist demnach: 180.41.0.0
Netzwerkmaske in dotted decimal: 255.255.0.0

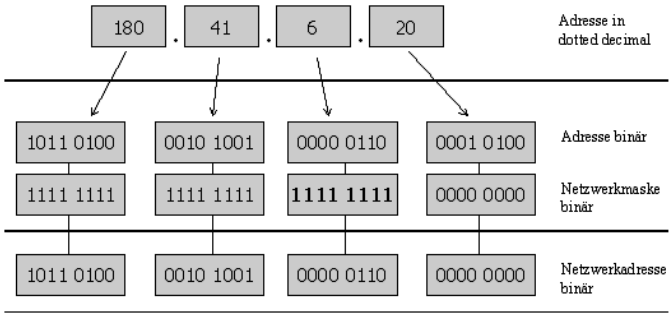
Subnetze:

- Durch Klasseneinteilung ergab sich Verschwendung von Adressen
- Zwei Stufige Adressierung (Netzwerknummer und Hostnummer) führte zudem zu dem Problem, wenn eine Organisation sein internes Netzwerk strukturieren wollte. Aufgliederungen waren nur mit neuer zusätzlichen Netznummer möglich

  ➔ Lösung Subnetze→ so konnten interne Netze besser gegliedert werden
- Die Hostadresse kann zu besseren organisatorischen Gliederung noch mal zur Subnetz-Bildung in zwei Teile zerlegt werden:
  - Teilnetznummer
  - Hostnummer



- Außerhalb des Teilnetzes ist die Aufgliederung nicht sichtbar
- Interne IP-Router in einem Teilnetz berücksichtigen die Subnetzadresse
- Netzwerkmaske wird als Bitmaske verwendet, um die Bits der Subnetzwerknummer zu identifizieren



Subnetz mit zwei Byte für Netzwerknummer und ein Byte für Subnetzwerknummer
Die Netzmaske ist hier: 255.255.255.0

- Der lokale Administrator besitzt alle Freiheiten zur Bildung von Subnetzen, ohne die Komplexität auf den Internet-Router zu übertragen
- Bei einer Klasse B-Adresse wäre folgende Struktur denkbar:
    - 1.+2. Byte sind die Netzwerknummern
    - 3. Byte gibt die Organisationseinheit im Unternehmen an (Subnetz-Adresse)
    - 4. Byte erlaubt die Nummerierung der Geräte: (Stationsadresse)
        - Netzkomponenten (Switch, Hub, etc.): 1 - 9
        - Arbeitsplätze: 10 - 249
        - Server: 250 - 254

CIDR (Classless Inter Domain Routing)/VLSM (Variable Length Subnet Mask):

- **Problem:**
    - **Vergeudung von vielen IP-Adressen durch die Aufteilung des Adressraums in Klassen (siehe Klasse-B-Adressen). Organisationen die gar nicht soviele Adressen brauchten bekamen eine Klasse C-Netz**
    - **Mehr Bit für den Hostanteil der Klasse-C-Adresse könnten das Problem scheinbar lösen, aber**
        - **Routing-Tabellen der Router explodieren → nicht akzeptabel**
- **Netzwerknummern sind nicht starr sondern flexibel einstellbar**
- **IP-Adressen werden in Netzwerkpräfixes beschrieben**
- **Restliche Klasse-C-Netze (ca. 2 Millionen) werden in Blöcken variabler Länge vergeben → Vergabe und Verwaltung durch ISP (Internet Service Provider)**

  Beispiel: Braucht ein Standort 2000 Adressen erhält er acht aufeinanderfolgende Klasse-C-Netze zugewiesen (2032 echte Adressen), kann also auf eine B-Adresse verzichten
- **Weitere Verbesserung für das Routing durch Zuordnung der Klasse-C-Adressenbereiche zu Zonen, z.B.**
    - **Europa: 194.0.0.0 bis 195.255.255.255**
    - **Nordamerika: 198.0.0.0 bis 199.255.255.255**
- **Europäischer Router erkennt anhand der Zieladresse, ob ein Paket in Europa bleibt oder z.B. zu einem amerikanischen Router weitergeleitet werden soll**
- **Beispiel:**
    - **Netzwerkpräfix-Notation (NP-Notation) ermöglicht die Angabe der Netz-Id-Bits in der IP-Adresse**
    - **Notationsbeispiel: 194.24.19.25/20**

- IP-Adresse binär:
  - 11000010.00011000.00010011.00011001 -> Klasse C
- Die Präfixlänge (hier 20) gibt die Anzahl der fortlaufenden Einsen in der Netzwerkmaske an:
- Netzwerkmaske der IP-Adresse:
  - 11111111. 11111111.11110000. 00000000 = 255.255.240.000
- Klasse A = /8
- Klasse B = /16
- Klasse C = /24

o Cambridge University benötigt 2048 (2^{11}) öffentliche IP-Adressen
- Klasse-C Netz mit max. 256 (2^8) Adressen reicht nicht aus.
- Alternative ist ein Klasse-B Netz mit 65536 (2^{16}) Adressen.
  - -> 63488 öffentliche IP-Adressen werden nicht benötigt und somit verschwendet! (über 95% der bereitgestellten Adressen!!!)
- Besser: Nutzung mehrerer zusammenhängender Klasse-C Netze
- Für den Hostteil der Adresse werden zusätzlich 3 Bit benötigt (2^{11} / 2^8)
- Cambridge University wird folgender Adressbereich zugewiesen.
- 194.24.0.0/21 -> 194.24.0.0 bis 194.24.7.255 (255.255.248.0)
- oder
- 11000010.00011000.00000000.00000000 bis
- 11000010.00011000.00000111.11111111 mit
- 11111111.11111111.11111000.00000000 als Netzwerkmaske

o Nach dem gleichen Verfahren werden auch den Universitäten Oxford und Edinburgh mehrere Klasse-C Netze zugewiesen.

o Oxford benötigt 4096 (2^{12}) öffentliche IP-Adressen.

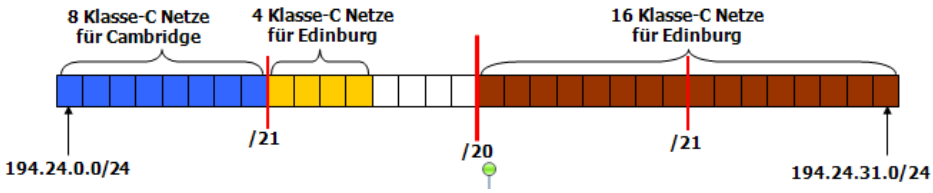
o Edinburgh benötigt 1024 (2^{10}) öffentliche IP-Adressen.

o Folgende Adressbereiche werden zugewiesen.

o Cambridge: 194.24.0.0/21 194.24.0.0 bis 194.24.7.255

o Oxford: 194.24.16.0/20 194.24.16.0 bis 194.24.31.255

o Edinburgh: 194.24.8/22 194.24.8.0 bis 194.24.11.255



- Ein Standard IP-Router kann die mittels VLSM zusammengefassten Klasse-C Netz nicht erkennen. Routing muss um CIDR erweitert werden.

Routingtabelle ohne CIDR

194.42.0.0	-> Cambridge
194.42.1.0	-> Cambridge
...	
194.42.7.0	-> Cambridge
194.42.8.0	-> Edinburgh
...	
194.42.11.0	-> Edinburgh
194.42.16.0	-> Oxford
...	
194.42.31.0	-> Oxford

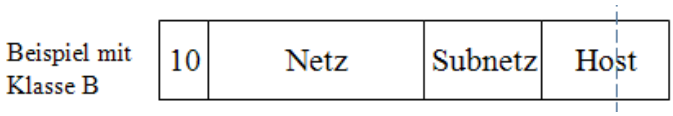
Routingtabelle mit CIDR

194.42.0.0/21	-> Cambridge
194.42.8.0/22	-> Edinburgh
194.42.16.0/20	-> Oxford

Nur 3 statt 28 Einträge!!!

23. Wozu wird in IPv4 im Router das Wissen über eine Netzwerkmaske für jedes angeschlossene Netz benötigt?

- Die Hostadresse kann zu besseren organisatorischen Gliederung noch mal zur Subnetz-Bildung in zwei Teile zerlegt werden:
  - Teilnetznummer
  - Hostnummer



- Außerhalb des Teilnetzes ist die Aufgliederung nicht sichtbar
- Interne IP-Router in einem Teilnetz berücksichtigen die Subnetzadresse
- Netzwerkmaske wird als Bitmaske verwendet, um die Bits der Subnetzwerknummer zu identifizieren
- Der lokale Administrator besitzt alle Freiheiten zur Bildung von Subnetzen, ohne die Komplexität auf den Internet-Router zu übertragen
- Bei einer Klasse B-Adresse wäre folgende Struktur denkbar:
  - 1.+2. Byte sind die Netzwerknummern
  - 3. Byte gibt die Organisationseinheit im Unternehmen an (Subnetz-Adresse)
  - 4. Byte erlaubt die Nummerierung der Geräte: (Stationsadresse)
    - Netzkomponenten (Switch, Hub, etc.): 1 - 9
    - Arbeitsplätze: 10 - 249
    - Server: 250 - 254

(siehe Aufgabe 22)

24. Was bedeutet in CIDR die Darstellung 132.10.1.8/24?

- Netzwerkpräfix-Notation (NP-Notation) ermöglicht die Angabe der Netz-Id-Bits in der IP-Adresse
- Hier werden 24 Netz ID-Bits benötigt
- Klasse B-Netz, Adresse binär 1000 0100.0000 1010. 0000 0001.0000 1000.
- Netzwerkmaske: 1111 1111.1111 1111. 1111 0000.0000 0000 (255.255.240.0)

- Von 132.10.1.8. bis 132.10.15.255?

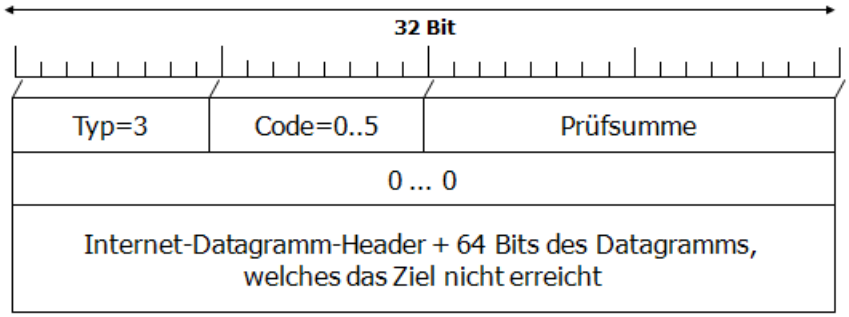
25. Wie findet ein Host innerhalb eines LAN (IPv4) die IP-Adresse eines Partner-Hosts, wenn er das erste Mal ein IP-Paket an diesen senden will?

26. Wie findet ein Host die MAC Adresse eines Partner-Hostes, der nicht im eigenen LAN, sondern irgendwo in einem entfernen LAN, das aber über einen Router erreichbar ist, liegt?

Siehe Aufgabe 32

27. Über welches Steuerprotokoll wird eine Ping-Nachricht abgesetzt? Verwendet das besagte Steuerprotokoll TCP, UDP oder direkt IP zur Nachrichtenübermittlung (S.108)?

- **ICMP** (Internet Control Message Protocol, RFC 792)
- Dient der Übertragung von unerwarteten Ereignissen und für Testzwecke
  - Beispiel 1: Ein Netzwerk ist nicht erreichbar: Ein IP-Router sendet in diesem Fall die ICMP-PDU „Network Unreachable“
  - Beispiel 2: Das ping-Kommando verwendet z.B. ICMP-PDUs (Echo Request, Echo Reply)
- ICMP-Nachrichten werden in IP-Datagrammen versendet
- ICMP gehört in die Internet Vermittlungsschicht und nutzt IP-Protokoll
- Werden in TCP/UDP Paketen als IP-Nutzdaten übertragen
- ICMP-Beispiel: **Destination unreachable** → Ein Router kann ein Datagramm nicht ausliefern (Typ=3, Code=1)



- Router sendet ICMP-Nachricht an den Absender
- Code: 0 = Netzwerk nicht erreichbar, 1 = Rechner nicht erreichbar,...

28. Erläutern Sie den Unterschied zwischen limited Broadcast und directed Broadcast in IP-Netzen. Wann benötigt man z.B. diese Broadcast-Varianten (Nennen Sie ein Bsp.)

- Direktes:
  - Senden einer Broadcast-Nachricht an ein beliebiges Netzwerk im Internet und zwar direkt von einem Host eines anderen Netzwerks aus.
  - Router sendet das Paket über den entsprechenden Pfad zum Zielrouter, der dann den Broadcast in seinem lokalen Netzwerk sendet.
  - Adresse für den direkten Broadcast enthält die Netzwerknummer und im Host teil lauter binäre Einsen
- Begrenztes (limited):
  - Bezieht sich auf das lokale Netzwerk und wird von den Routern nicht durchgelassen. Adresse für alle Netze gleich 255.255.255.255.

- Bsp.: PING?

29. Was kann die Vermittlungsschicht zu Vermeidung bzw. Abbau von Stausituationen im Netz beitragen? Nennen Sie zwei Möglichkeiten.

30. Kann man innerhalb eines autonomen Systems im globalen Internet unterschiedliche Routing-Verfahren verwenden? Begründen Sie ihre Entscheidung.

- Man muss unterscheiden zwischen der Wegewahl innerhalb autonomer Systeme (Intra-AS-Routing) und der Wegewahl im globalen Internet, also zwischen autonomen Systemen (Inter-AS-Routing)

ALLGEMEIN ROUTING IM INTERNET:

- Jeder IP-Router und Host verwaltet eine Routing-Tabelle

Netzwerk-ziel	Netzwerk-maske	Nächster Router	Ausgangsport	Metrik
...	...	...	...	...

- Ausgangsport = die dem Interface zugeordnete IP-Adresse
- Metrik = Anzahl der Hops zum Ziel (enthält „Kosten“)
- Netzwerkziel: Netzwerkadresse des Ziels, kann auch Hostadresse stehen (Hostroute mit Maske 255.255.255.255)
- Netzwerkmaske oder evt.Länge der Subnetzmaske
- Nächster Router: Nächste Router in der Reihenfolge (Gateway)
- IP-Paket kommt am Router an. Was passiert?
    - Zieladresse des Pakets wird mit Einträgen in den Routing-Tabellen verglichen
        - Bitweise Und-Verknüpfung zwischen Zieladresse aus IP-Paket und Netzwerkmaske aus Routeneintrag (für alle Einträge)
        - Vergleich des Ergebnisses mit Netzwerkziel aus Routeneintrag
        - Übereinstimmung → potentielle Route gefunden!
    - Die Route mit der größten Übereinstimmung wird ausgewählt
    - Bei gleichwertigen Einträgen: Beste Metrik entscheidet!
    - Keine Übereinstimmung → Standardroute

Beispiel:

Aktive Routen:

Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle	Anzahl
0.0.0.0	0.0.0.0	10.28.1.253	10.28.16.21	20
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
10.28.16.21	255.255.255.255	127.0.0.1	127.0.0.1	20
224.0.0.0	240.0.0.0	10.28.16.21	10.28.16.21	20
255.255.255.255	255.255.255.255	10.28.16.21	10.28.16.21	1

Standardgateway: 10.28.1.253

- **Annahmen:**
- Eigene IP-Adresse: 10.28.16.21
- Nur eine Ethernet-Karte im Rechner
  Standard-Gateway: 10.28.1.253

- Schnittstelle entspricht Ausgangsport

Zeile 1:

- Dies ist die **Standardroute**: Immer Netzwerkziel 0.0.0.0 und Netzwerkmaske 0.0.0.0 (/0)
- Jede IPv4-Zieladresse, für die eine bitweise logische UND-Operation mit 0.0.0.0 ausgeführt wird, führt zu dem Ergebnis 0.0.0.0
- Die Standardroute führt daher zu einer Übereinstimmung mit jeder IPv4-Zieladresse
- Wenn die Standardroute die längste übereinstimmende Route ist, lautet die Adresse des nächsten Knotens 10.28.1.253 (Standard-Gateway) und die Schnittstelle für den nächsten Knoten ist der Netzwerkadapter mit der IPv4-Adresse 10.28.16.21 (einziger LAN-Adapter)

Zeile 2:

- **Loopback-Route:** Netzwerkziel 127.0.0.0 und der Netzwerkmaske 255.0.0.0 (/8)
- Für alle Pakete, die an Adressen in der Form 127.*x.y.z* gesendet werden, wird die Adresse des nächsten Knotens auf 127.0.0.1 (die Loopback-Adresse) gesetzt
- Die Schnittstelle für den nächsten Knoten ist die Schnittstelle mit der Adresse 127.0.0.1 (die TCP-Loopback-Schnittstelle)
- Das Paket wird nicht in das Netzwerk gesendet

Zeile 3:

- **Loopback-Route:** Netzwerkziel 127.0.0.0 und der Netzwerkmaske 255.0.0.0 (/8)
- Für alle Pakete, die an Adressen in der Form 127.*x.y.z* gesendet werden, wird die Adresse des nächsten Knotens auf 127.0.0.1 (die Loopback-Adresse) gesetzt
- Die Schnittstelle für den nächsten Knoten ist die Schnittstelle mit der Adresse 127.0.0.1 (die TCP-Loopback-Schnittstelle)
- Das Paket wird nicht in das Netzwerk gesendet

Zeile 4:

- **Loopback-Route:** Netzwerkziel 127.0.0.0 und der Netzwerkmaske 255.0.0.0 (/8)
- Für alle Pakete, die an Adressen in der Form 127.*x.y.z* gesendet werden, wird die Adresse des nächsten Knotens auf 127.0.0.1 (die Loopback-Adresse) gesetzt
- Die Schnittstelle für den nächsten Knoten ist die Schnittstelle mit der Adresse 127.0.0.1 (die TCP-Loopback-Schnittstelle)
- Das Paket wird nicht in das Netzwerk gesendet sondern es wird gleich mit dem Kernel Kommuniziert

Zeile 5+6:

- Der Eintrag mit dem Netzwerkziel 224.0.0.0 und der Netzwerkmaske 240.0.0.0 (/4) ist eine Route für **Multicast-Verkehr**, der von diesem Host gesendet wird
- Für alle Multicast-Pakete wird die Adresse des nächsten Knotens auf die Zieladresse gesetzt und für die Schnittstelle des nächsten Knotens wird der LAN-Adapter festgelegt
- Der Eintrag mit dem Netzwerkziel 255.255.255.255 und der Netzwerkmaske 255.255.255.255 (/32) ist eine Hostroute, die der **limited Broadcast-Adresse** entspricht
- Für alle an 255.255.255.255 gesendeten IPv4-Pakete wird die Adresse des nächsten Knotens auf 255.255.255.255 gesetzt und die Schnittstelle des nächsten Knotens ist der LAN-Adapter

31. Warum werden in IPv4 IP-Adressen „verschenkt“ und wie werden im derzeitigen globalen Internet IP-Adressen eingespart? Nennen Sie zwei Einsparungen

- Einsparung durch CIDR und Subnetz (siehe Aufgabe 22)

- CIDR: **Problem:**
- **Vergeudung von vielen IP-Adressen durch die Aufteilung des Adressraums in Klassen (siehe Klasse-B-Adressen). Organisationen die gar nicht soviele Adressen brauchten bekamen eine Klasse C-Netz**
- **Mehr Bit für den Hostanteil der Klasse-C-Adresse könnten das Problem scheinbar lösen, aber**
  - **Routing-Tabellen der Router explodieren → nicht akzeptabel**
- **Netzwerknummern sind nicht starr sondern flexibel einstellbar**

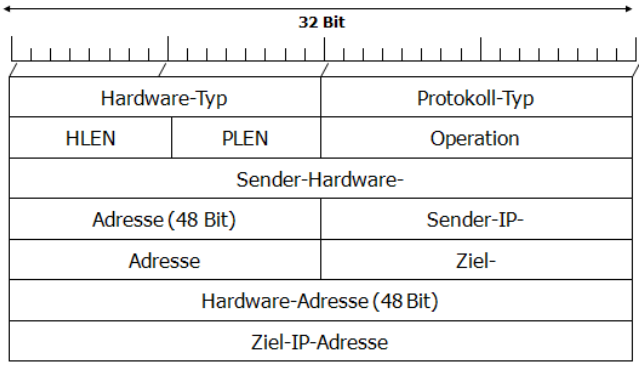
- Durch Klasseneinteilung ergab sich Verschwendung von Adressen
- Zwei Stufige Adressierung (Netzwerknummer und Hostnummer) führte zudem zu dem Problem, wenn eine Organisation sein internes Netzwerk strukturieren wollte. Aufgliederungen waren nur mit neuer zusätzlichen Netznummer möglich
  - Lösung Subnetze→ so konnten interne Netze besser gegliedert werden

32. Wie bekommt ein IPv4-basierter Host die MAC-Adressen seiner Partnerrechner und wie vermeidet er, dass eine MAC-Adresse eines Partnerrechners veraltet?

ARP und RARP (Address Resolution Protocol)

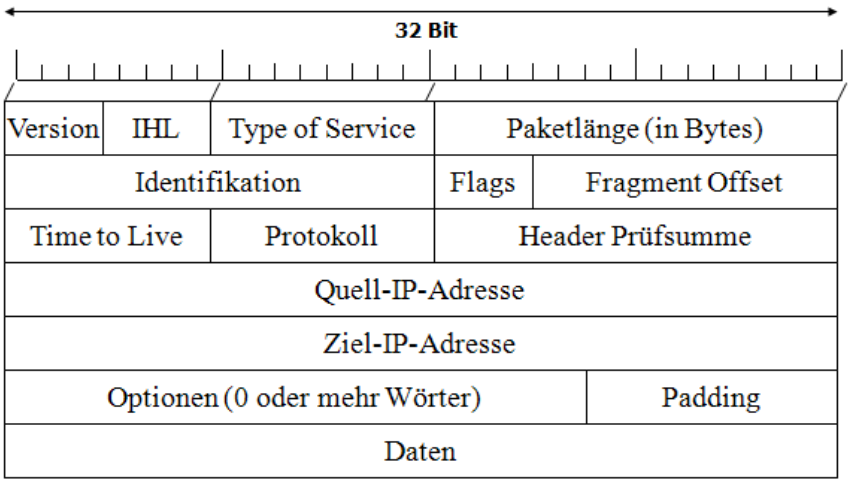
- ARP (Address Resolution Protocol), RFC 826
  - ARP dient dem **dynamischen Mapping** von IP-Adressen auf Schicht-2-Adressen (MAC-Adressen)
  - Funktioniert so:
    - Wenn Zielhost adressiert wird, der bisher noch nicht oder schon länger nicht mehr addressiert wurde, wird ein ARP-Request in einem begrenzten Broadcast im LAN versendet. Request enthält IP-Zieladresse. Fragt so alle Rechner an, wer denn diese Adresse kennt.
    - Zielhost oder ein anderer antwortet mit einem ARP-Reply und übergibt dabei seine MAC-Adresse
  - Jeder Host kennt seine eigene Schicht-2-Adresse, nicht aber die Adressen der anderen Hosts
  - Jeder Host führt einen **ARP-Cache** und merkt sich darin Schicht-2-Adressen (so muss nicht ständig neu angefragt werden), die über ARP im **IP-Broadcasting** erfragt werden können → **Periodisches Löschen vermeidet Inkonsistenz! (Jeder Eintrag hat TTL –Time to live, der Einträge löscht wenn Sie eine längere Zeit z.B. 20 min nicht genutzt werden)**
  - Ist Zielhost nicht gespeichert, wird ein **ARP-Broadcast** mit der IP-Zieladresse als Parameter versendet
  - Der Zielrechner antwortet mit einem **ARP-Reply** (MAC-Adresse)
  - IP-Router übernehmen Rolle des **ARP-Proxy**

- Nachrichtenformat eines ARP/RARP-Pakets



- **Hardware-Typ:**
  - Hardware-Typ, 1 = Ethernet
- **Protokoll-Typ:**
  - Typ des High-Level-Protokolls, X`0800` = IP
- **HLEN:**
  - Hardware-Adressenlänge =MAC-Adresse
- **PLEN:**
  - IP-Adressenlänge
- **Operation**:
  - 1 = ARP-Request
  - 2 = ARP-Response
  - 3 = RARP-Request
  - 4 = RARP-Response
- Wird z.B. MAC-Adresse gesucht ist IP-Adresse ausgefüllt
- RARP (Reverse Address Resolution Protocol): Wenn zu MAC-Adresse eine IP-Adresse gesucht wird

33. Welche Bedeutung hat das Feld TTL im IP-Header und wie wird es in einem Router im Rahmen der Bearbeitung eines ankommenden IP-Paketes bearbeitet?



- 32 Bit also 8 Byte für jede Zeile
- **Version**: Spezifiziert die genutzte IP-Version; z.Zt. Wechsel von IPv4 auf IP Next Generation (IPv6)

- **IHL (Headerlänge)**: Gibt die Länge des Paket-Headers an, gemessen in 32-Bit-Worten; ist aufgrund der variablen Länge des Optionsfeldes nötig (mind. 5 → keine Option, max. 15 Worte → 60 Byte)
- **Type of Service** : Dieses 8-Bit-Feld ist wiederum aufgeteilt in:
    - Priorität (3 Bit): 000=Standard, 001=Priorität, ..., 101=kritisch, ...
    - ToS-Spezifikation (3 Bit): Flags zur Angabe von Servicetypen (hoher Durchsatz, niedrige Verzögerung, ...)
    - 2 unbenutzte Bit, IPv4 nutzt Type of Service nicht
- **Paketlänge**: Gesamtlänge des Datenpaketes inkl. Header; gemessen in 8-Bit-Wortenmax. 65.535 Byte
- **Identifikation**: Alle Fragmente eines Datagramms erhalten hier den gleichen Wert
- **Flags**: (3 Bit) Dient der Kontrolle der Fragmentierung
    - Geben an, ob das Feld geteilt werden muss und weitere Pakete folgen oder ob das aktuelle Paket das letzte ist
    - Drei Flags, erstes unbenutzt: 0|DF|MF
    - DF=1 → Fragmentierung ist nicht erlaubt
    - More Fragments=0 → letztes Fragment; MF=1 weitere folgen
- **Fragment Offset**: Dient der korrekten Herstellung der Ursprungssequenz, da Pakete das Ziel in unterschiedlicher Reihenfolge erreichen, gemessen in 8-Byte-Worten
    - Dient der Ermittlung der relativen Lage des Fragments im Datagram
    - 13 Bit lang
- **Time to live (TTL):** Gibt an, wie lange ein Datagramm im Internet verbleiben darf
    - Es dient dazu, zu alte Pakete vom Netz zu nehmen, bei 0 wird Paket verworfen und eine ICMP-Nachricht zum Quellhost gesendet
    - War gedacht als Zeit in Sekunden (max. 255 s)
    - Wird aber als Hop-Count genutzt, jeder Router subtrahiert 1 von dem Feld
- **Protokoll**: Definiert das darüber liegende Protokoll, an das IP die Daten des Pakets weiterreicht (6=TCP, 89=OSPF,...)
- **Header-Prüfsumme**: Dient der Erhaltung der Header Einträge
    - Prüft also **nur** den Header, Daten in höheren Protokollen prüfen!
    - Wird für jede Teilstrecke neu berechnet werden, warum? –Weil sich der TTL-Wert immer verändert
- **Quell-IP-Adresse und Ziel-IP-Adresse**:
    - Jeweils 32 Bits
    - Identifikation der einzelnen Endsysteme (Hosts)
    - Hier stehen die IP-Adressen von Sender- und Empfängerhost
- **Optionen**: Zusätzliche, optionale Angaben:
    - Loose Source Routing → Möglichkeit, den Weg eines Paketes durch das Internet aufzuzeichnen;
    - Strict Source Routing-> die Pakete müssen die Pfadvorgabe einhalten
    - ...
    - Wird selten verwendet!!

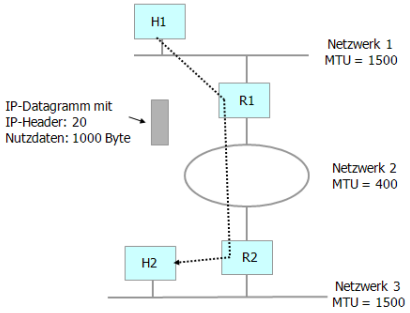
- **Padding**: Wenn eine Option genutzt wird, ist das Datagramm bis zur nächsten 32-Bit-Grenze mit Nullen aufzufüllen
- **Daten**: Die Nutzdaten der höheren Schicht

34. Wozu benötigt eine IP-Instanz das Feld Protokoll aus dem IP Header?

(siehe Aufgabe 33)

35. Beschreiben Sie kurz den Protokollmechanismus der Fragmentierung am Beispiel von IPv4 und gehen Sie dabei auf die genutzten Felder Identifikation, Fragment Offsets und Flags ein (S.91-92)!

- Wenn ein IP-Paket von einem Netzknoten zum anderen weitergeleitet wird, muss es
  - evtl. verschiedene physikalische Netze durchqueren, die unterschiedliche maximale Transfereinheiten haben (MTU)
  - in unterschiedlich zulässige Paketgrößen aufgeteilt werden
- Daher besteht die Notwendigkeit, IP-Datagramme zu zerlegen und am Ziel wieder zusammenzusetzen
  - Fragmentierung und Defragmentierung
  - Alle Router müssen Fragmente der Größe **576 Byte** oder kleiner akzeptieren
- Sobald eine Fragmentierung einsetzt, laufen in einem Knoten mehrere Schritte ab
- Das **DF**-Flag wird überprüft, um festzustellen, ob eine Fragmentierung erlaubt ist. Ist das Bit auf „1“ gesetzt, wird das Paket verworfen
- Ansonsten wird entspr. der zulässigen Paketgröße das Datenfeld des Ur-Paketes in mehrere Teil zerlegt
- Alle neu entstandenen Pakete weisen - mit Ausnahme des letzten Paketes - eine Länge mit einem **Vielfachen von 8 Byte** auf
- Alle Datenteile werden in neu erzeugte IP-Pakete eingebettet. Die Header dieser Pakete sind Kopien des Ursprungskopfes mit einigen Modifikationen
- Header-Modifikation bei der Fragmentierung:
  - Das **MF**-Flag wird in allen Fragmenten mit Ausnahme des letzten auf „1“ gesetzt
  - Das **Fragment-Offset**-Feld enthält Angaben darüber, wo das Datenfeld in Relation zum Beginn des nicht fragmentierten Ur-Paketes platziert ist
  - Enthält das Ur-Paket Optionen, wird abhängig vom Type-Byte entschieden, ob die Option in jedes Paketfragment aufgenommen wird (z.B. Protokollierung der Route)
  - Die **Headerlänge** (IHL) und die Paketlänge sind jeweils **neu** zu bestimmen
  - Die **Headerprüfsumme** wird neu berechnet
- Ablauf der Defragmentierung:
  - Die Zielstation setzt die Fragmente eines Datagramms wieder zusammen
  - Die **Zusammengehörigkeit** entnimmt sie dem **Identifikationsfeld**
  - Die ankommenden Fragmente werden zunächst gepuffert
  - Bei Eintreffen des ersten Fragments wird ein **Timer** gestartet
  - Ist der **Timer** abgelaufen bevor alle Fragmente eingetroffen sind, wird alles **verworfen**
  - Im anderen Fall wird das Datagramm am N-SAP **zur Transportschicht hochgereicht**



- Wollen 1000 Byte verschicken
- Netzwerk 2 schafft aber nur 400 Byte (380+20 Header)

Fragment 1

Rest des Headers		
Identifikation=120	Flags:**MF = 1**	**FO = 0**
Datenbyte 0 ... 375		

Fragment 2 — 376 / 8 = 47

Rest des Headers		
Identifikation=120	Flags:**MF = 1**	**FO = 47**
Datenbyte 376 ... 751		

Fragment 3 — 752 / 8 = 94

Rest des Headers		
Identifikation=120	Flags:**MF = 0**	**FO = 94**
Datenbyte 752 ... 999		

  - 375 wird auf 376 erhöht, da durch 8 teilbar

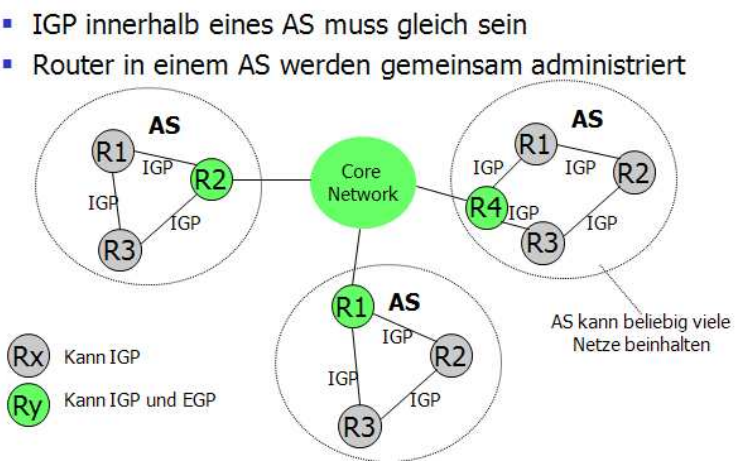
36. Welches Problem im Routing-Protokoll RIP versucht die Split-Horizone-Technik zu lösen und wie funktioniert diese Technik? Zeigen Sie dies anhand eines einfachen Beispiels mit Skizze (S.97-98).

IGP und EGP:

- Jedes autonome System kann intern eigene Routing-Algorithmen verwenden
- Routing-Protokolle für autonome Systeme werden als Interior Gateway Protokolle (**IGP**) bezeichnet
- IGP: RIP, OSPF
- EGP: Border Gateway Protokoll (BGP)
- Älteres Verfahren für kleinere Netze: **RIP**
  - Distance-Vector-Protokoll, aber: Count-to-Infinity-Problem
- Nachfolger von RIP seit 1990 ist **OSPF** (Open Shortest Path First), RFC 1247
  - Wird von der Internet-Gemeinde empfohlen
  - Netz wird als gerichteter Graph abstrahiert
  - Kanten zwischen den Knoten werden mit Kosten gewichtet (Entfernung, Verzögerung,...)
  - Entscheidung über das Routing anhand der Kosten
- Zwischen AS werden andere Routing-Protokolle benötigt (Exterior Gateway Protocol, **EGP**)
  - Andere Ziele werden verfolgt, Beispiele:

- Nicht alle Pakete sollen befördert werden
- Für Transitverkehr muss bezahlt werden
- Wichtige Informationen nicht durch unsichere autonome Systeme senden

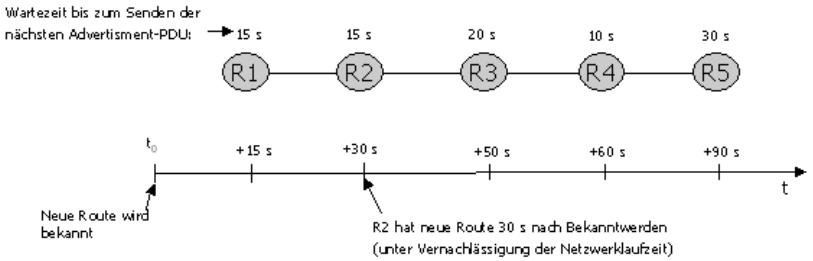
- Routing-Regeln sind erforderlich, die vom Routing-Protokoll unterstützt werden müssen
- Im Internet wird das Border Gateway Protokoll (**BGP**) empfohlen
  - Pfadvektorprotokoll



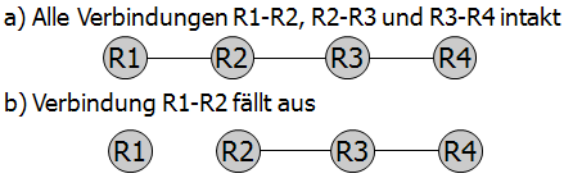
RIP:

- RIP (Routing Information Protocol) wurde ursprünglich von XEROX entwickelt
- Beim Start eines Routers sendet dieser zunächst an alle Nacher-Router eine Request –PDU und fordert damit die Routing Informationen an
- Antwort erfolgt zielgerichtet (Respons-PDU) (also nicht über Broadcast sondern Unicast-Nachrichten)
- Nutzt UDP
- Wird in kleinen Autonomen Systemen (AS) immer noch stark verwendet
- Einfach und leicht zu implementierendes Distance-Vector-Protocol
- Als Metrik wird ein **Hop-Count** verwendet
- Im globalen Internet heute schon mehr erforderlich
- Implementierung unter Unix durch **routed**-Prozess
- RIP versendet die Routing-Einträge alle 30 s in sog. Advertisement-PDUs
  - RIPv1 über MAC-Broadcast
  - RIPv2 über Multicast auf Subnetzebene
- Nicht geeignet für WAN-Routing, eher im LAN wegen Broadcast/Multicast
- Max. 25 Routeneinträge pro RIP-Nachricht
- Hört Router 180 sec nichts vom Nachbarn , gilt dieser als nicht erreichbar.
  - Routing-Tabelle wird aktualisiert: Metrik wird auf 16 gesetzt, an Nachbarn weiter gegeben , Routing Tabellen angepasst und Überwachung der Nachbarn auf 120 sec runter gesetzt (Garbage-Collection)
- Problem: langsame Konvergenz und Schleifen (Count-to-Infinity-Problem)
- **Konvergenzzeit**: Zeit, die erforderlich ist, bis alle Router die aktuelle Struktur eines Netzes kennen gelernt haben

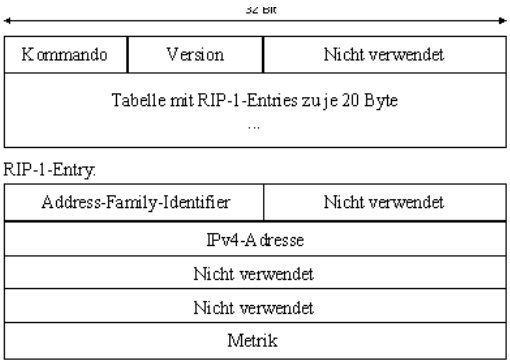
- **Split Horizon** ist eine Methode, um die Konvergenzzeit kurz zu halten
- Anm: **Max. 15 Hops wurden gewählt, um die Konvergenzzeit zu beschränken**
- Verbreitung von Routing-Tabellen-Einträgen in mehreren Takten a‘ 30 s bestimmt die Konvergenzzeit
- Bis zum nächsten Senden einer Advertisement-PDU dauert es im Mittel 15 s, zufallsabhängig



  - Es kann also 90 sec dauern bis Router 5 die Info von R1 bekommen hat
  - **Schleifen** („Count-to-Infinity-Problem“) möglich
    - Lösung: **Split-Horizon-Technik** (mit oder ohne **Poison-Reverse** (vergifteter Rückweg), Routing-Tabellen enthalten **zusätzlich** die Info, woher die Routing-Info kommt
  - Beispiel:

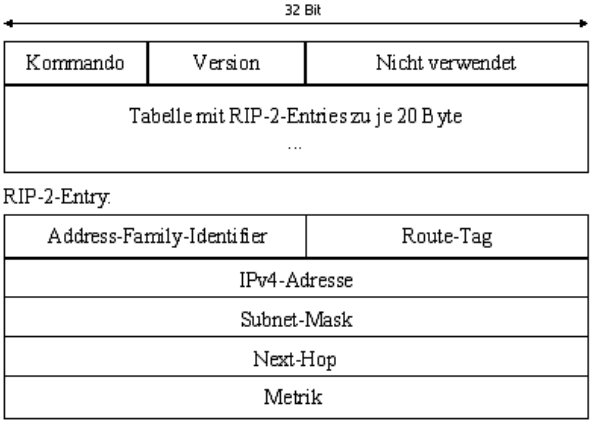


    - Was passiert mit und ohne Split-Horizon?
  - **Ohne Split Horizon:**
    - R3 hat noch die Routing-Info, dass R1 über einen Hop erreichbar ist
    - R3 propagiert diese Info an R2, also an den Router, über den R1 erreicht wurde
    - R2 glaubt dies und sendet Pakete zu R1 nun über R3
    - Ping-Pong-Effekt, Routing-Schleife bis Hop-Count = 16, dann erst wird R1 als nicht erreichbar markiert
  - **Mit Split Horizon:**
    - **R3 weiß, woher die Routing-Info für R1 kommt (von R2)**
    - Route mit höheren Kosten wird nicht zurückpropagiert
    - Keine Routing-Schleife
  - Metrik = 16 → Netzwerkziel nicht erreichbar
  - AFI = Adressierungsart, bei IP-Adressen immer 0x02



- Genutzte felder:
    - Kommando: Wird angegeben ob es sich um ein RIP- Request (0x01) oder RIP-Response (0x02)handelt.
    - Version: RIP1 oder RIP2
    - AFI (Address-Family-Identifier: Gibt Adressierungsart an und enthält für IP-Adressen immer den Wert 0x02
    - IPv4-Adresse: IP-Adresse der Router also Netzwerkziel
    - Metrik: Anzahl Hops

RIP2:



- Next-Hop: Direkte Angabe eines Zielhosts möglich
- RIPv1 **unterstützt** CIDR/VLSM **nicht**
- Subnetzmaske wird in RIPv1 **nicht** übermittelt
- RIPv2 kann **Split-Horizon**, und Split-Horizon mit Poisson-Reverse
- RIPv2 kann selbst ausgelöste Router-Aktualisierungen (**Triggered Updates**) bei Ankunft einer Advertisement-PDU
- höhere Konvergenz
- RIPv2 ist zu RIPv1 **abwärtskompatibel**
- RIPv2 **unterstützt** CIDR/VLSM
- RIPv1 kommuniziert über **Broadcast**, RIPv2 über **Multicast (Klasse D-Adressen)**

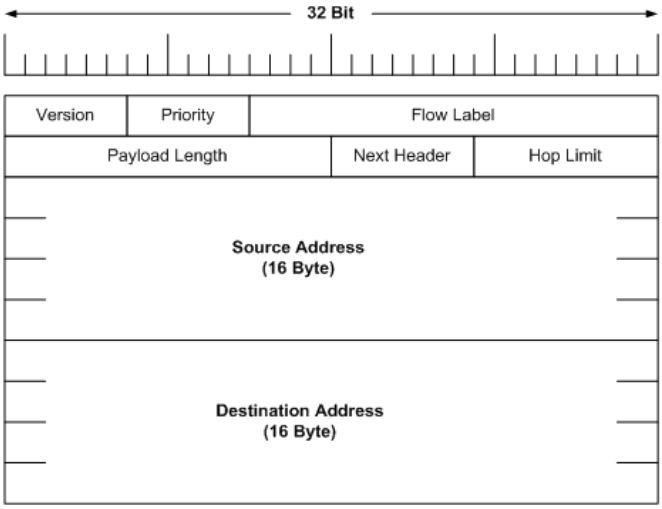
37. Im globalen Internet setzt man prinzipiell zwei verschiedene Routing-Verfahren ein (EGP und IGP). Erläutern Sie den Unterschied zwischen EGP und IGP und stellen Sie dar, wo beide Verwendung finden? Nennen Sie je ein konkretes Routing-Protokoll für die beiden Verfahren.

(siehe Aufgabe 36)

38. Nennen Sie drei Ziele der IPv6 Entwicklung.

- CIDR reicht nicht für alle Zeit, daher wurde eine neue Version von IP konzipiert (seit 1990)
- Zukunftsszenarien:
  - **Jeder Fernseher ist möglicheweise bald ein Internet-Knoten** (Video-on-Demand)
  - **Millionen von drahtlosen** Systemen im Internet
- Hauptziel von IPv6 (IPnG) ist es, die **Adress-problematik** umfassend und langfristig zu lösen
- Koexistenz mit IPv4 erforderlich und angestrebt
- **Vereinfachung** des Protokolls zur schnelleren Bearbeitung von Paketen in Routern
- Umfang der **Routing-Tabellen reduzieren**
- **Anwendungstypen** wie Multimedia-Anwendungen (Echtzeitanwendungen) unterstützen
  → Unterstützung von **Flussmarken**
- Höhere **Sicherheit** (Datenschutz, Authentifikation)
- **Multicasting** besser unterstützen
- **Mobile IP-Adressen**: Möglichkeit schaffen, dass Hosts Ihr Heimatnetz verlassen können
- Möglichkeiten der **Weiterentwicklung** schaffen

39. Welchen Sinn haben im IPv6-Protokoll die sog. Erweiterungsheader? Nennen Sie zwei Erweiterungsheader und beschreiben Sie kurz deren Aufbau.



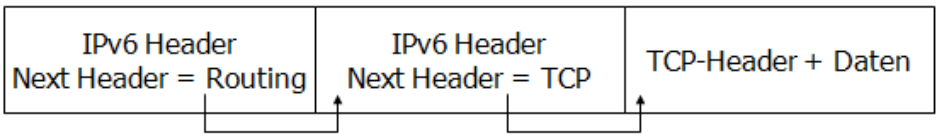
- **Version** Versionsnummer des Internet-Protokolls (6)
- **Priorität**: auch **Traffic Class** / **DS** = Differenciated Service Field (neu) mit neuen Werten (RFC 2474, 2478)
  - Information für Router, interessant bei Überlastsituationen
    - 4 stoßartiger Verkehr (ftp, NFS) → hoher Durchsatz
    - 6 interaktiver Verkehr (telnet) → geringe Verzögerung
    - 8-15 Verkehrsarten ohne Staukontrolle (z.B. für Videoanwendungen)
- **Flussmarke**: Identifikation des Flusses, falls ungleich 0
  - Zweck: Zusammengehörige Datenflüsse (Video/Audio) auf Netzebene speziell behandeln

- Quelladresse+Zieladresse+Flussmarke kennzeichnen einen Fluss
- Flussmarken werden im Quellknoten in die IPv6-PDU eingetragen

- **Payload Length:** Nutzdatenlänge **ohne** die 40 Bytes des IPv6-Headers
- **Next Header**: Verweis auf ersten Erweiterungs-Header
  - Letzter Header verweist auf Protokolltyp der nächst höheren Schicht (siehe IPv4-Feld **Protokoll**)
- **Hop Limit**: Verbleibende Lebenszeit des Pakets in Hops
  - Jeder Router zählt Hop Limit um 1 herunter
  - Entspricht dem TTL-Feld in IPv4
  - Name entspricht jetzt der eigentlichen Nutzung im Internet
- **Source und Destination Adresse**: IPv6-Adressen der Quelle und des Ziels
- Kodierung im Next-Header-Feld
  - EGP = 0x08
  - Routing = 0x2B
  - Fragment = 0x44
  - TCP = 0x06 …

Erweiterungs-Header	Beschreibung
Optionen für Teilstrecken (Hop-by-Hop)	Verschiedene Informationen für Router
Routing	Definition einer vollen oder teilweisen Route
Fragmentierung	Verwaltung von Datengrammfragmenten
Authentifikation	Echtheitsüberprüfung des Senders
Verschlüsselte Sicherheitsdaten	Informationen über den verschlüsselten Inhalt
Optionen für Ziele	Zusätzliche Informationen für das Ziel

- Header und Erweiterungs-Header sind miteinander **verkettet,** jeder Typ **max. einmal**
- Die Erweiterungen werden **nicht** in den Routern bearbeitet, nur in den Endsystemen
- Eine **Ausnahme**: Routing-Erweiterungs-Header
- Reihenfolge der Header ist festgelegt (siehe Zitterbart, Band 2, S. 72)
- Beispiel eines IPv6-Headers mit einem Erweiterungs-Header und einer anschließenden TCP-PDU



Routing-Header:

- Der **Routing-Header** dient der Quelle zur Festlegung des Weges bis zum Ziel

Next Header	Header Ext. Länge	Routing Typ	Verbl. Segmente
1-24 Adressen			

- **Next Header**: siehe vorne
- **Header Ext. Länge:** Länge des Routing-Headers
- **Routing Typ:** Gibt den Typ der Routing-Headers an

- **Verbleibende Segmente:** Anzahl der folgenden Adressen, die besucht werden müssen

Fragmentierungs-Header:

- Der **Fragmentierungs-Header** wird verwendet, um größere Dateneinheiten zu senden, als zugelassen
  - PDU-Länge > MTU des Pfades (MTU = Maximum Transmission Unit)
  - Minimum auch in IPv6 576 Bytes
- Segmentierung erfolgt bei IPv6 nur im Quellknoten, Router segmentieren nicht → geringe Routerbelastung

Next Header	reserviert	Fragment Offset	00M
Identifikation			

- **Fragment Offset:** Position der Nutzdaten relativ zum Beginn der PDU (Ursprungs-Dateneinheit) → 13 Bit (wie IPv4)
- **Identifikation:** Id der PDU (wie IPv4)
- **M:** More-Flag, M=1 → weitere Segmente kommen (wie IPv4)

Sicherheitspakete:

- Im Gegensatz zu IPv4 sind in IPv6 schon Sicherheitsmechanismen im Protokoll spezifiziert (siehe IPv4+IPsec)
  - Authentifizierung
  - Verschlüsselung
- **MD5-Algorithmus** (Message Digest) kann zur Authentifizierung der Partner verwendet werden
- Verschlüsselung des Nutzdatenteils wird mit einer Variante des **DES-Verschlüsselungsalgorithmus** unterstützt
  - DES = Data Encryption Standard
  - Symmetrisches Verschlüsselungsverfahren

40. Wozu sollen im IPv6-Protokoll Flussmarken dienen?

Flussmarken:

- Ziel: Aufbau von **Pseudoverbindungen** zwischen Quelle und Ziel mit QS-Merkmalen wie Verzögerung und Bandbreite
  - Ressourcenreservierung
  - Datenströme für Echtzeitanwendungen
- Flexibilität von Datagramm-Netzen kombiniert mit virtuellen Verbindungen
- Ein „Fluss“ wird durch Quell- und Zieladresse sowie einer Flussnummer identifiziert
- Router führen eine Sonderbehandlung durch
- Noch in der Experimentierphase!

Neighbor Discovery:

Router-Discovery:

- Wenn ein Endsystem seinen nächsten Router sucht, sendet es eine ***Router-Solicitation*-Nachricht** über Multicast an die Adresse **FF02::2**
- Router antworten mit einer ***Router-Advertisement*-Nachricht**

- Damit unterstützt das ND-Protokoll das Auffinden des verantwortlichen Routers zur Laufzeit → DHCP kann auch wegfallen
- Mehrere Router können aktiv sein

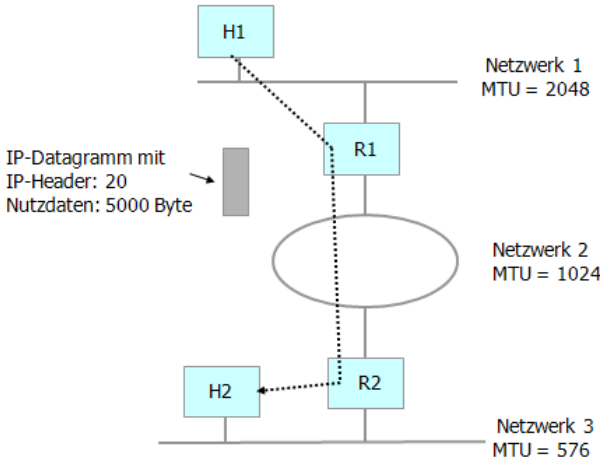
Das ND-Protokoll nutzt zur Abwicklung seiner Aufgaben einige ICMPv6-Nachrichten

Parameter-Discovery:

- Netzwerkparameter werden vom Host zum Startzeitpunkt auch über ***Router-Solicitation*-Nachricht** besorgt (DHCP-Aufgaben)
- Nachricht geht an Multicast-Adresse **FF02::2**
- Ein Router antwortet mit einer ***Router-Advertisement*-Nachricht** an die Link-Adresse des Endsystems
- Folgende Parameter kann eine *Router-Advertisement*-Nachricht u.a. übertragen:
  - *Max-Hop-Limit*: Dies ist der Wert „Hop-Limit“ der in die IPv6-PDUs eingetragen wird
  - *Retransmission-Timer*: Zeit in Millisekunden, die seit dem Absenden der *Solicitation*-Nachricht ablaufen darf, bevor wiederholt wird
  - …
  - Über ein *Optionsfeld* wird z.B. vom Router auch die *MTU-Size* übermittelt

41.Host A sendet in einem IPv4-Netzwerk seinem Partnerhost B ein IP-Paket der Länge 5000 Byte. 20 Byte davon enthält der IP-Header des Paketes. Es gelten folgende Bedingungen…

Netz	ID	MF	FO	Rest des Headers	Daten
1 (2048 Byte)		1	0		0…2047
		1	(2048/8=256)		2048…4095
		0	**512**		**4096…4979**
2 (1024 Byte)		1	0		0…1023
		1	128		1024…2047
		1	256		2048…3071
		1	384		3072…4095
		0	**512**		**4096…4979**
3 (576 Byte)		1	0		0…575
		1	72		576…1151
		1	144		1152…1727
		1	216		1728…2303
		1	288		2304…2879
		1	360		2880…3455
		1	432		3456…4031
		1	504		4032…4607
		0	**576**		**4608…4979**



- Wie viele Fragmente verlassen R1 ?
  - 5
- Wie viele Fragmente verlassen R2?
  - 9
- Im welchen System(Host oder Netz) werden Pakete Zusammen gfügt?
  - Netz
- Wie erkennt System, welches IP Fragmet zum ursprünglichen IP-Paket gehört?
  - ID?

42. Eine Organisation hat von seinem IP die IPv4-Adressblock : 131.42.0.0./16 zugewiesen bekommen . Die Organisation möchte gern ihr Netzwerk intern wie folgt aufteilen:
    - 1 Subnetz mit bis zu 32.000 Rechnern
    - 15 Subnetze mit bis zu 2.000 Rechnern
    - 8 Subnetze mit bis zu 250 Rechner
    - Adressen werden zunächst in die Blöcke 131.42.0.0./17 und 131.42.128.0/17 aufgeteilt

43. Was passiert, wenn ein IPv4-Pakets, in einem Netzwerk landet, dessen MTU, kleiner ist als die Länge des Fragments?

- Sie müssen zerteilt werden und einzeln geschickt werden (Siehe Aufgabe 35)

44. Wo (auf welchen Rechner) werden IPv4-Fragmente wieder zum ursprünglich abgesendet IPv4-Datagramm reassembliert?

- Am Zielrechner

45. Was versteht man im Sinne der IP-Adressvergabe unter einem multihomed Host?

Ein multihomed host ist ein Rechner, der über mehrere IP-Adressen erreichbar ist. Dadurch kann der Rechner gleichzeitig in mehreren Subnetzen sein und ist ohne Routing aus verschiedenen Subnetzen erreichbar. Allerdings ist ein solcher multihomed host von nicht mehr eideutig über genau einen Namen adressierbar, sodern muß über eine der IP-Adressen bzw. den zugehörigen IP-Namen angesprochen werden. Ohne entsprechendes Routing ist ein solcher Rechner nur über die richtige zum Subnetz passende IP-Adresse erreichbar.

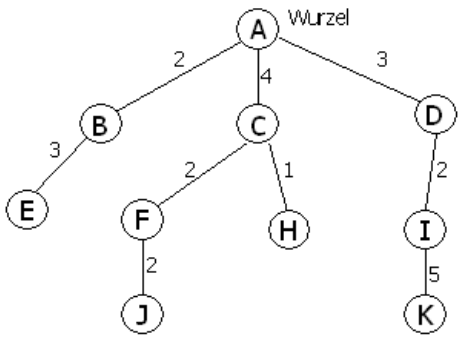
46. Wie lauten die entsprechende Netzwerkmasken für CIDR-Präfixnotationen /16, /20, und /24

- /16: 1111 1111.1111 1111.0000 0000.0000 0000=255.255.0.0.
- /20: 1111 1111.1111 1111.1111 0000.0000 0000=255.255.240.0

- /24: 1111 1111.1111 1111.1111 1111.0000 0000=255.255.255.0.

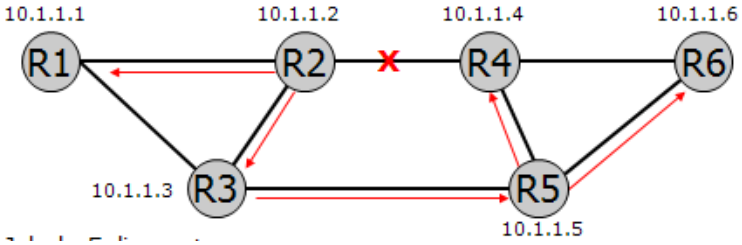
49. Erläutern Sie, wie ein neu in ein Netzwerk hinzugekommener OSPF-Router seine Routing-Informationen aufbaut und verwaltet. Gehen Sie dabei auf den Begriff des Spanning –Tree und auf die nachbarschaftliche Beziehung der OSPG-Router ein. (S.101)

- Gehört zu IGP
- OSPF (Open shortest Path first) ist **für große Unternehmensnetze** gedacht, für kleine wird noch RIP bzw. statische Routing-Tabellen verwendet
- **Offener** Standard (Open SPF), RFC 1247
- OSPF ist ein **Link-State-Protocol**
    - „Link State“ ist der Zustand einer Verbindung zweier Router → zustandsorientiert statt entfernungsorientiert (RIP)
- Kommunikation mit unmittelbaren, **designierten Nachbarn** zum Austausch der Routing-Information
- Jeder Router führt **eigene Datenbasis** (Link-State-Datenbank) mit allen Routing-Einträgen des Netzes
- Jeder IP-Router erzeugt aus seiner Sicht einen Spanning Tree (SPF-Baum) (oder auch Shortest-Path-First genannt) für das ganze Netzwerk
- Wurzel ist der Router selbst
- Verzweigung = günstigste Route
- Kante entspricht Subnetzübergang. Sind Link mit Kosten (z.B. Belastung übertragungsarte oder Verzögerung)

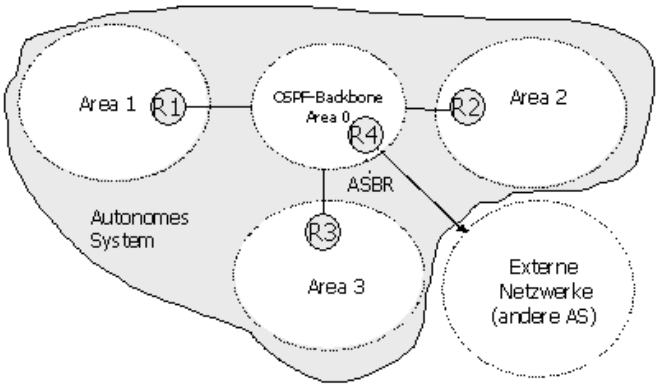


- Damit alle Router Topologie kennen, müssen sie synchronisiert werden. Bei OSPF jeder Router kommuniziert mit seinen Nachban. Jede Veränderung die er erfährt, wird an die Nachbarn weitergegeben
- **Load Balancing** bei Pfaden mit gleichen Kosten
    - gleichmäßige Verteilung, besser als bei RIP
- Nutzung spezieller **Multicast-Adressen (Broadcast)** zur Kommunikation
- Unterstützung der Router-**Authentifizierung** zur Vermeidung von Angriffen (mehr Sicherheit)
- Alle Router suchen beim Start ihre Nachbarn mit **Hello-PDUs**, aber nicht alle angrenzenden Router werden auch zu Nachbarn (sog. **adjacents**)
- An hand der antwort, die auch eine form von Hello-PDU ist, wird entschieden ob nachbar oder nicht. Nachbar swchicjt seine Info mit Database-Description-PDUs
- Bei neuen Router ähnlich:

- **Router sendet seine eigenen Infos mit Zyklischer Abgleich** der Link-State-Advertisements (LSA)
- Erhält ein Router die LSA werden sie an die Nachbarn weiter gegeben
- **Lebendüberwachung** periodisch unter den Nachbarn
- **Link State Updates** (Konsistente Datenhaltung in allen Routern) periodisch und bei Topologie-änderungen
- **Refreshing** spätestens alle 30 Minuten
- Kommt nach 40 sec keine hello-PDU zurück, so gilt dieser als ausgefallen
- Verteilung einer Veränderung im Netz geht schnell (hohe Konvergenz)
- Beispiel für Routen-Austausch:
    - Verbindung zwischen 10.1.1.2 und 10.1.1.4 fällt aus
    - Link-State Updates werden über das ganze Netz verteilt
    - Nachdem DB synchronisiert ist, gibt es nur noch eine kürzeste Route

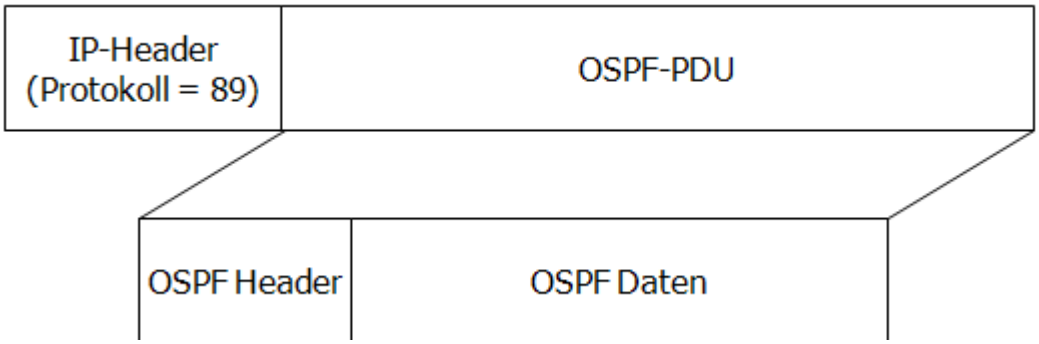


- Unterstützung großer Netze:
    - Netzwerke können in mehrere autarke OSPF-Bereiche aufgeteilt werden
    - Netzbereiche=**Areas** (Hierarchisierung des Systems)mir Areas ID (in dotted dezimal Schreibweise). Areas werden über Backbones miteinander verbunden
    - In einer Area verwenden alle Router den gleichen Shortest-Path-Algo.
    - Jeder Router in einer Area hat gleiche Link-State-Datenbank
    - Router kennen nur Router aus ihrer Area
    - Ein Router der Area muss an OSP-Backbone hängen (über Grenz- oder Area-Router)
- Bei OSPF gibt es **vier Router-Klassen**
    - Interne Router der Area (Führen nur Intra-AS-Routing durch, nach außen nicht sichtbar)
    - Router an Bereichsgrenzen (Area-Grenzen)
        - Verbinden zwei oder mehrere Areas
    - Backbone-Router
        - Befinden sich im Backbone
    - AS-Grenz-Router (ASBR=Area Boundary Router))
        - Vermitteln zwischen autonomen Systemen
        - Kent alle LSD-DB aller Areas
- Bei Einsatz in Broadcast-orientierten LANs: Verwendung von sog. designierten Routern
    - Alle Router bauen eine Nachbarschaft (Adjacencies) zu diesem Router auf → Reduzierung der Kommunikation



- R1, R2, R3 = Router an Bereichsgrenzen
- R4 = AS-Grenz-Router (ASBR), vermittelt zwischen autonomen Systemen

- Die Aufteilung hat den Vorteil, dass die Größe der Linke-State-Datenbanken verringert wird und damit die Routing-Tabelle.
- Designierter Router:
  - Verteilung der Routing-Info verantwortlich
  - Ist mit Prio gekennzeichnet, die höher ist als bei herkömmlichen OSPF-Routern
- Es gibt fünf OSPF-PDU-Typen:
  - **Hello**: Feststellung der Nachbarn, Aufbau von Nachbarschaften
  - **Database Description**: Bekanntgabe der neuesten Daten
  - **Link State Request**: Informationen vom Partner anfordern
  - **Link State Update**: Informationen an Nachbarn verteilen
  - **Link State Acknowledgement**: Bestätigung eines Updates



- Vereinfachter Header
- PDUs werden direkt über IP gesendet, (siehe IP-Header, Protokoll = 89)
- Direkte Übertragung an Nachbarn oder über spezielle Multicast-Adressen
- OSPF-PDUs werden nur zwischen Nachbarn ausgetauscht
- Kein Weiterrouten außerhalb des eigenen Netzes (IP-Header, TTL=1)

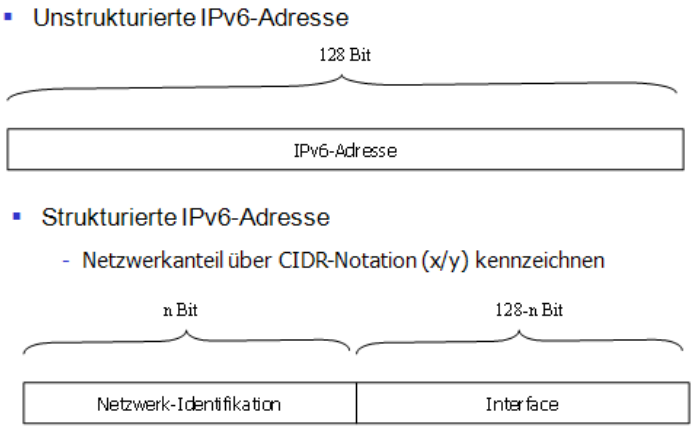
50. Ein Problem bei Routing-Protokollen ist das Konvergenzverhalten bzw. die Konvergenzdauer bei Änderungen der Netzwerktopolgie oder bei Änderungen von Routen. Wie ist das Konvergenzverhalten bei Routing-Protokollen RIP2 und OSPFv2? Welche Mechanismen nutzt RIP-2 zur Verbesserung der Konvergenzen? Sind in beiden Routing-Protokollen Endlosschleifen (Count-to-Infinity-Problem) möglich?

- Konvergenzverhalten RIP2:

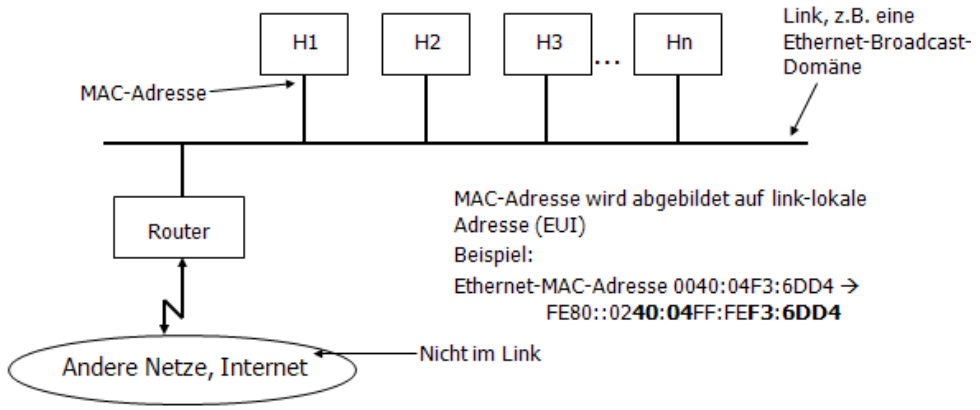
- RIPv2 kann selbst ausgelöste Router-Aktualisierungen (**Triggered Updates= Routen werden unmittelbar nach dem Eintreffen dieser Ereignisse. Kein Timer der erst 30 sec abläuft**) bei Ankunft einer Advertisement-PDU
- Konvergenzverhalten OSPFv2:
- Verteilung einer Veränderung im Netz geht schnell (hohe Konvergenz)
- Snyhronisierung (Siehe Aufgabe 49)
- RIP2 nein
- OSPF nein

51. Wie funktioniert bei IPv6 prinzipiell die automatische Adresskonfiguration?

- **16-Byte-Adressen** (128 Bits) mit neuer Notation
- Verschiedene Klassen von Adressen
    - **Unicast**-Adressen
        - Der traditionelle Adresstyp
        - Adressieren einen Netzanschluss eines Hosts oder Routers
    - **Anycast**-Adressen
        - Adressierung einer Gruppe von Interfaces
        - Aber nur ein Mitglied der Gruppe bekommt das Paket
        - Auswahl übernimmt der zuständige Router
        - Nutzung innerhalb von Teilnetzen, kein Routing außerhalb
    - **Multicast**-Adressen
        - Adressierung einer Gruppe von Interfaces
        - **Keine** Broadcast-Adresse mehr in IPv6!!
- Aufteilung des IPv6-Adressraums in **RFC 4291** geregelt



- MAC-Adresse wird als Interface-Identifikation übernommen
- Abbildung IEEE-803.3-Adresse auf IEEE EUI-64-Adresse wird dabei vorgenommen (siehe Folien)
- Interface=MAC Adresse
- Link-Lokal bezieht sich auf das lokale Netz
- Ausbreitung nur in einem Teilnetz
- Präfix der Adressen: 1111 1110 10 → FE80::/10



- Adressen-Notation mit 8 Gruppen zu je vier Hex-Zahlen abgetrennt durch Doppelpunkte, CIDR-Notation (x/y) auch zulässig

  Beispiel:

  8000:0000:0000:0000:**0**123:5555:89AB:CDEF

- Führende Nullen können in jeder Gruppe weggelassen werden und Gruppen mit lauter Nullen können durch einen Doppelpunkt ersetzt werden, aber „::“ nur an einer Stelle möglich:

  8000::123:5555:89AB:CDEF

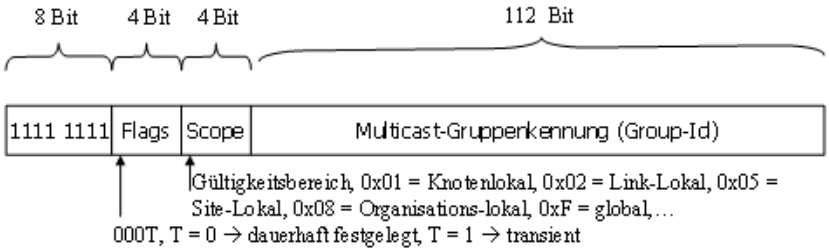
- IPv4-Adressen können mit speziellen Unicast-Adressen (Präfix ::FFFF/96) abgebildet werden. (Mapping-Adressen)

Beispiel: 192.168.0.1 ➔ ::FFFF:C0A8:1

- ::0 entspricht 0.0.0.0 in IPv4 (undefinierte Adresse)
  - Synonym: 0:0:0:0:0:0:0:0 oder ::/128
- ::1 entspricht der Loopback-Adresse 127.0.0.1 in IPv4
  - Synonym: 0:0:0:0:0:0:0:1 oder ::1/128
- FF00::/8 weist auf eine Mulitcast-Adresse hin
- FF80::/10 weist auf eine Link-Lokal-Adresse hin
- Ersten 64 Bit dienen üblicherweise der Netzadressierung und die letzten 64 zur Host-Adressierung

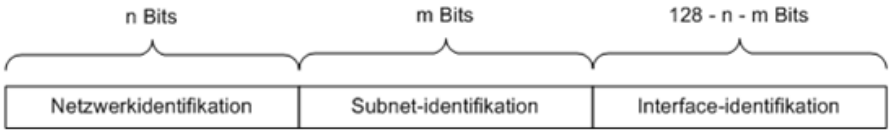
Multicast-Adressen:

- Genutzt für Neighbor Discovery, DHCP und für das Routing. Darf nicht als Absendeadresse genutzt werden
- Beginnen mit 0xFF (0b11111111)
- Flag:letztes Bit gibt an, ob temporär vergebene oder eine well known (ständig vergebene) Multicast-Adresse ist
- SCope: Legt fest wie weit sich ein Paket ausbreiten darf (bei 0xE (1110) ist entspricht der Broadcast Adresse in IPv4)
- Knotenlokale Adresse FF01:0:0:0:0:0:0:1 → Alle Knoten-Mulitcastadresse dieses Knotens (Nachricht verlässt Knoten nicht)
- Knotenlokale Adresse FF01:0:0:0:0:0:0:2 → Alle IP-Router dieses Knotens
- Für das gleiche Link-Segment FF02:…



Global-Unicast:

- Dienen dazu, einen Host (Knoten) im Internet **global** eindeutig zu identifizieren → **öffentliche** Adressen (wie Klasse A, B, C aus IPv4)!
- Hierarchiebildung möglich → Provider-/Netzbetreiberzuordnung
- Eine Unicast-Adresse hat z.B. folgenden Aufbau:

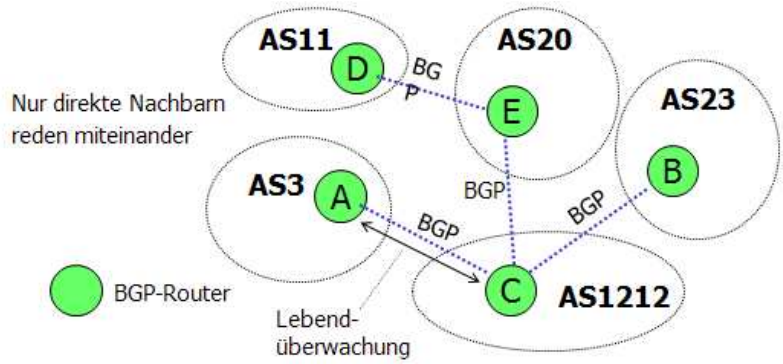


Automatische Adressierung:

- **Selbstkonfiguration:** Host konfiguriert seine eigene Adresse dynamisch (kein ARP mehr notwendig):
  - Die **dynamische Adress-Auflösung** für Layer-2-Adressen wie es heute im **ARP-Protokoll** abgewickelt wird
- **Router Discovery:** Das Auffinden von Routern im gleichen Link (Subnetz)
- **Parameter Discovery:** Die dynamische Zuordnung von Konfigurationsparametern wie der maximalen MTU und dem Hop-Limit an IPv6-Endsysteme
- Die automatische **IP-Adress-Konfiguration** für Interfaces zur Laufzeit
- Die Suche nach dem optimalen MTU zwischen Sender und Empfänger (Path MTU Discovery)

Routingprotokoll BGP(BGP-4) (Border Gateway Protocol):

- Ist ein EGP
- Pfadvektorprotokoll (Path-Vector-Protocol)
- Ermöglicht Routing zwischen verschiedenen Autonomen Systemen (AS)

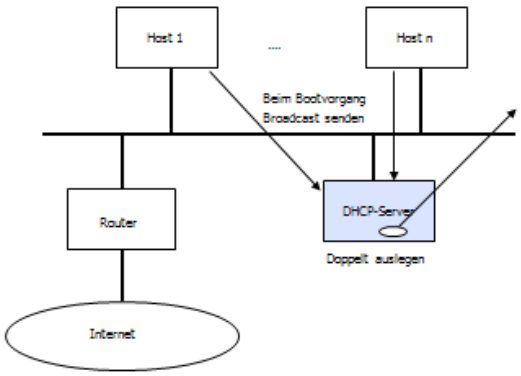


- Lehnt sich ans Distanc-Vector verfahren an, nutzt jedoch keine Kosteninformationen (wie Anzahl der Hops) sondern Pfadinformationen
- BGP-Router kennen die besten Route zu anderen AS als **vollständigen** Pfad (**auf AS-Ebene nicht auf Router-Ebene**)

- Jeder BGP-Router führt eine **Datenbank** mit Routen zu allen erreichbaren autonomen Systemen.
- Routing-Tabellengröße:
    - ~ 200.000 Einträge
    - ~ 26.000 Autonome Systeme
- Routing-Tabelle von D enthält folgende Routen:
    - AS11 – AS20
    - AS11 – AS20 – AS1212
    - AS11 – AS20 – AS1212 – AS23
    - AS11 – AS20 – AS1212 – AS3
- Unmittelbare Nachbaren heißen Peers
- Ein BGP-Router informiert **periodisch** alle **Nachbar**-BGP-Router **genau** über die zu nutzenden Routen
    - UPDATE-PDUs werden versendet, sog. Advertisements
- Jeder BGP-Router kennt also die optimale Route zu einem anderen AS vollständig
- Zyklen in Routen werden bei Übernahme der Information geprüft
    - eigene AS-Nummer darf nicht in Route sei, falls sie dabei steht, wird die Route nicht akzeptiert
    - Count-to-Infinity-Problem tritt so nicht auf
- BGP-Router überwachen sich gegenseitig (Heartbeat-Protokoll → KEEPALIVE-PDU) um ausfälle schnell zu erkennen
- BGP-Router verwendet zur Auswahl der besten Routen eine **Routing-Policy**
- Routing-Policy (Regeln), Beispiele:
    - Kein Verkehr über einen bestimmten Knoten
    - Sicherheitsaspekte
    - Kostenaspekte
- Eine Route, die die Regeln verletzt, wird auf „unendlich“ gesetzt
- BGP nutzt TCP (Port 179) als Transportprotokoll für seine Nachrichten (verbindungsorientiert!)

DHCP:

- Manuelle Netzwerkkonfiguration ist schon bei kleinen Netzen ein Problem
- Dynamic Host Configuration Protocol schafft Abhilfe
    - Hosts müssen Adressen nicht mehr kennen, sie werden dynamisch beim Booten besorgt
- Dynamische Vergabe von IP-Adressen und weiteren Netzwerk-Parametern über einen DHCP-Server:
    - Subnetzmaske
    - DNS-Server-Adresse
    - IP-Router-Adresse
- Meist beziehen nur Arbeitsplatzrechner Ihre IP-Adresse vom DHCP-Server



Konfigurationsdatei z.B.: /etc/dhcpd.conf

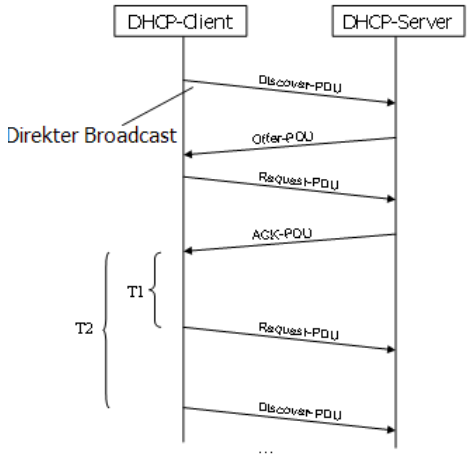
```
default-lease-time 600; # 10 Minuten
max-lease-time 7200; # 2 Stunden

option domain-name "dept101.com";
option domain-name-servers 192.168.1.1 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
{
    range 192.168.1.10 192.168.1.20;
    range 192.168.1.100 192.168.1.200;
}

host mandl
    hardware ethernet 00:00:45:12:EE:E4;
    fixed-address 192.168.1.21;
```

- Vorgang:
  - DHCP-Client (Host) sendet beim Booten eine Discover-PDU über direkten Broadcast ins Netz
  - Der zuständige DHCP-Server, der doppelt ausgelegt sein muss (er sollte kein Single Point of Failure sein (wenn der Server ausfällt, fällt das gesamte System aus)), bietet dem Client eine Netzwerkkonfiguration in einer Offer-PDU an
  - Nimmt der Client an, sendet er direkt eine Request-PDU an den Server
  - DHCP-Server bestätigt das nochmal mit einer ACK-PDU



- Die Lease-Zeit, Zeit in der der Client die Netzwerkkonfig. Nutzen darf, ist mit zwei Parametern beschränkt. T1(gibt 50% der Leas-Zeit an) und T2 (87,5%)
- DHCP-Client sendet nach Ablauf von T1 erneut eine Request PDU an den DHCP Server, dann möchte er die Netzwerkkonfig. Weiter nutzen.
- Kommt eine ACK-PDU vom Server zurück wird die Lease-Zeit erneut gestartet.
- Falls keine kommt sendet der Client nach T2 erneut ein Discovery über einen Broadcast
- IP-Ranges (Adressbereiche) oder direkte Zuordnung von IP-Adressen zu Hosts möglich
  → Zuordnung über MAC-Adresse
- Beim Booten sendet Server die Offer-PDU an den Client über MAC-Adresse
- Diagnose- und Konfigurationskommandos im TCP/IP-Umfeld, die man öfter mal braucht:
  - ping
  - hostname

- netstat
- nslookup (kommt später bei DNS)
- arp
- traceroute (Windows: tracert)
- ifconfig
- route
- ipconfig (Windows)
- nbtstat (Windows)