Vermittlungsschicht - Kontrollfragen

Skript Seite 132

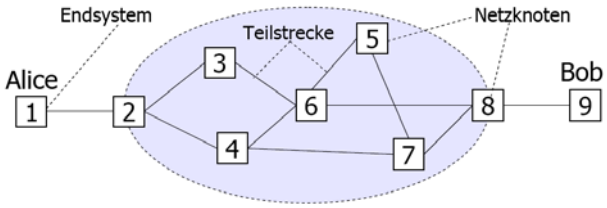
1. Nennen Sie zwei Aufgaben der Vermittlungsschicht und beschreiben Sie diese kurz!

- Wegwahl (Routing) – wesentliche Aufgabe der Vermittlungsschicht, das Ziel ist es durch
- Multiplexen und Demultiplexen (einer Teilstreckenverbindung auf der Schicht 2 wird für mehrere Vermittlungsverbindungen auf der Schicht 3 verwendet)
- Staukontrolle (Congestion Control)
- Segmentierung und Reassemblierung (Fragmentierung / Defragmentierung)

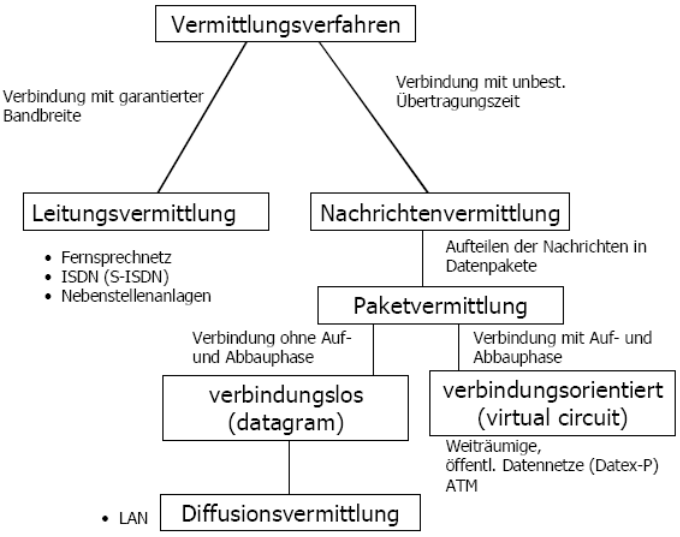
2. Was unterscheidet die Vermittlungsverfahren „Leitungsvermittlung“ und „Nachrichtenvermittlung“ (speziell Paketvermittlung)?

Allgemein

In der Vermittlungsschicht haben wir es vor allem mit Teilsteckennetzen zu tun, also mit über Netzknoten (Router) verbundenen Leitungen, an die auch die Datenendeinrichtungen (DEE) angeschlossen sind.



Die Vorgänge der Verbindungsherstellung, des Haltens und Abbauen einer Verbindung bezeichnet man als Vermittlung (Switching).
Beispiel: von Alice (1) zu Bob (9) über die Netzknoten 2, 3, 6, 8.



Leistungsvermittlung

Alle Ressourcen auf dem Netzwerkpfad (Bandbreite und Puffer in den Netzwerkknoten) werden vorab für die Dauer der Verbindung reserviert. Daher wird oftmals viel Bandbreite unnötig reserviert (Nachrichtenaufkommen ist meist unkonstant) und es ist mit Blockierungen zu rechnen, wenn viele Verbindungen aufgebaut werden möchten und kein Verbindungsweg mehr frei ist.

Als Lösung werden die Verbindungen oftmals mit Frequenzmultiplexen (FDM) oder Zeitmultipplexen (TDM) in mehrere Schaltkreise aufgebaut. So hat beim TDM jede Verbindung einen Zeitschlitz zugeordnet.

Typische Vertreter: ISDN oder das analoge Fernsprechnetz. Hier wird über die gesamte Verbindung ein physikalischer Verbindungsweg geschaltet, daher wird das Verfahren auch Durchschaltevermittlung (Circuit Switching) genannt.

Nachrichtenvermittlung

Hier werden immer komplette Nachrichten zwischen den Netzwerkknoten ausgetauscht und erst weitergeleitet, wenn sie vollständig sind (Store-and-Forward). Dabei wird keine dauerhaft bereitgestellte physische Verbindung genutzt, sondern es werden standardisierte Transporteinheiten (Pakete, Frames) übertragen.

Paketvermittlung

Die Paketvermittlung ist eine effizientere Methode der Nachrichtenvermittlung. Längere Nachrichten werden hier in einzelne Datenpakete unterteilt und als Datagramme (verbindungslos) oder verbindungsorientiert über eine Virtuelle Verbindung (Virtual Circuit) übertragen.

Die Ressourcen werden nicht vorab reserviert, sondern zur Laufzeit dynamisch zugewiesen. Daher kann es sein, dass zwei Kommunikationspartner auf eine Verbindung etwa in einer Warteschlange warten müssen, bis die Ressourcen verfügbar sind. Es wird dabei auch keine Bandbreite reserviert, dafür gibt es kaum Blockierungen.

Typische Vertreter sind das Internet (Internet Protocol) und Breitband-ISDN auf Basis von ATM (verbindungsorientiert).

Bei der **verbindungslosen Paketvermittlung** werden Datagramme ohne vorherigen Verbindungsaufbau gesendet und jedes Datagramm enthält die Quell- und Zieladresse. Die Knoten ermitteln dann für jedes Paket den optimalen Weg.

Beispiel: Diffusionsvermittlung im LAN, hier sendet jeder Knoten die empfangenen Pakete an alle Nachbarknoten weiter (außer an den Sender).

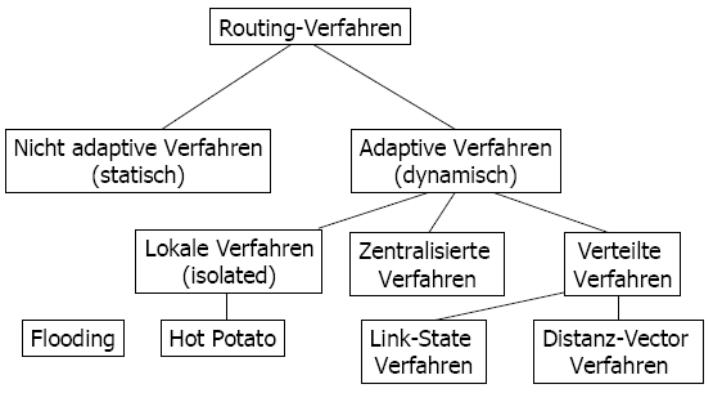
Die **verbindungsorientierte Paketvermittlung** (Virtual Circuit) bauen scheinbare Verbindungen auf, die für die Dauer der Datenübertragung erhalten bleiben. Dies erfolgt nicht physisch wie bei der Leitungsvermittlung, sondern dynamisch anhand Routing-Informationen, die in den Netzwerkknoten gespeichert werden (siehe auch: Aufgabe 3).
Die Verbindungen selbst bestehen aus drei Phasen bzw.Diensten: connect, data und disconnect.

3. Warum werden virtuelle Verbindungen in der Schicht 3 auch scheinbare Verbindungen genannt?

Die Verbindung besteht nur scheinbar, da keine physikalische Verbindung (wie bei der Leitungsvermittlung) durchgeschaltet wird.

Der Verbindungsaufbau erfolgt Schrittweise über die Netzknoten und die beim Verbindungsaufbau ermittelten Routinginformationen werden in den Netzknoten gespeichert, um eine gewisse Kontextverwaltung zu erreichen.
Um eine virtuelle Verbindung zu identifizieren mappen die Router die eingehenden Pakete zu den Ausgangsteilstrecken und speichern Status- und Verbindungstabellen.

4. Erläutern Sie den Unterschied zwischen statischen und dynamischen Routing-Mechanismen! Nennen Sie je ein konkretes Verfahren hierzu!



Statische Verfahren:
Flussbasiertes Routing
Shortest Path Routing
Flooding

Dynamische Verfahren:
Isoliertes Routing – Hot Potatoe
Zentrales Routing (mit Routing Control Center)
Verteiltes Routing (Denzentrales Routing)
- Distance Vector Verfahren (RIP, IGRP)
- Link-State-Verfahren (OSPF)
- Path-Vector-Verfahren (BGP)

Die Wegwahl ist eine wesentliche Aufgabe in paketorientierten Netzen und bedeutet so viel, wie einen optimalen Weg zu geringen Kosten (Pfadlänge, Kosten) zu finden. Zur Unterscheidung der Routing-Verfahren wird beispielsweise nach dem Zustand (statisch, dynamisch) oder nach dem Umfang (global, dezentral) unterschieden.

Statische (nicht adaptive) Verfahren

Das Routing erfolgt unabhängig von aktuellen Verkehrsmessungen, sondern nur anhand von Metriken, die vor der Inbetriebnahme ermittelt worden sind. Hier wird eine statische Routing-Tabelle verwendet, die fest vorgegebene Routen enthält.

Dynamische (adaptive) Verfahren

Diese Verfahren nutzen Verkehrsmessungen zur Routenermittlung und die Routing-Tabellen werden dynamisch über definierte Metriken angepasst. Diese Optimierungskriterien können sich dynamisch ändern und werden im Algorithmus berücksichtigt.

Beispiel Statische Verfahren

- Flussbasiertes Routing
- Shortest-Path-Routing
- Flooding: Jedes ankommende Paket wird an alle oder eine begrenzte Auswahl (selektives Flooding) der Teilstrecken weitergeleitet. Sehr robust, findet immer den optimalen Weg, sehr ineffizient

Beispiel Dynamische Verfahren

- Isoliertes Routing (wie Hot Potatoe)
- Zentrales Routing (via Routing Control Center)
- Verteiltes (dezentrales) Routing
    - Distance-Vector-Verfahren (wie RIP, IGRP)
    - Link-State-Verfahren (wie OSPF)
    - Path-Vector-Verfahren (wie BGB)

Siehe auch: Aufgabe 5

5. Was versteht man unter einem zentralen Routing-Verfahren? Handelt es sich hier um ein statisches oder um ein adaptives Routing-Verfahren?

Adaptive (dynamische) Verfahren werden unterteilt in lokale (isolierte) Verfahren, zentralisierte Verfahren und Verteilte Verfahren (dezentrales Routing).

Isoliertes Routing

Hier trifft jeder Knoten die Routing-Entscheidungen alleine.
Beispiel: Hot-Potato Verfahren – jedes Paket wird so schnell wie möglich zum Ausgang mit der geringsten Auslastung weitergeleitet.Verfahren wird jedoch in reiner Form nicht verwendet.

Zentrales Routing

Hier existiert ein zentraler Knoten (Routing Control Center RCC), der die gesamten Routing-Informationen sammelt. Dieser RCC sendet periodisch alle Veränderungen der Routing-Infos an alle Router. Das Verfahren ist zwar nicht fehlertolerant (Gefahr, dass Routing-Informationen veralten), aber konsistent.

Verteiltes Routing

Hier liegt die Routing-Funktionalität bei jedem einzelnen Knoten, wobei die Routing-Tabellen im Zusammenspiel mehrerer Router ermittelt werden.

Hier werden im Wesentlichen zwei Verfahren unterschieden: Distance-Vector und Link-State.

Einige Routing-Algorithmen:

- Statische Algorithmen:
  - Shortest-Path-Routing
  - Flooding
- Dynamische Algorithmen
  - Distance-Vector-Routing
  - Link-State-Routing
  - Hierarchisches Routing

6. Welche Vorteile bringt ein hierarchisches Routing-Verfahren?

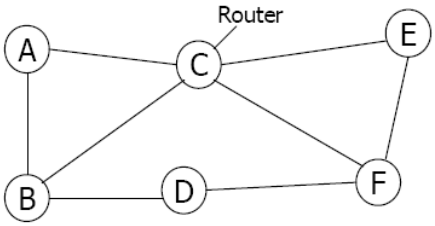
Durch eine hierarchische Organisation der Router mit unterschiedlichen Hierarchiestufen (z.B. Regionen) wird versucht, die Routing-Tabellen zu verkleinern. Insbesondere bei großen Netzen sind die Routingtabellen sehr groß und es treten lange Suchzeiten auf.

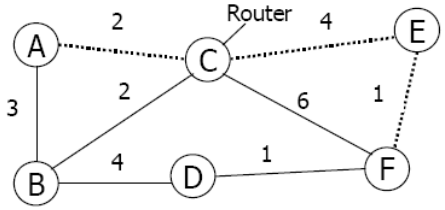
So gibt es z.B. in einzelnen Regionen spezielle Router, die für die Außenkommunikation zuständig sind. Jeder Router muss daher nicht mehr jeden anderen Router kennen, als Nachteil sind jedoch die ansteigenden Pfadlängen zu nennen.

7. Erläutern Sie kurz das Optimierungsprinzip beim Routing!

Optimierungsprinzip - Allgemein

Optimierungsprinzip: „Wenn Router C auf dem optimalen Pfad zwischen A und F liegt, dann fällt der Pfad von C nach F ebenso auf diese Route." Eine Annhame, es existiert eine bessere Route zwischen C und F, führt dabei zu einem Widerspruch. Die Aufgabe ist es, einen Weg zu minimalen Kosten bzw. einen optimalen Weg mit der kürzesten Pfadlänge zu ermitteln.



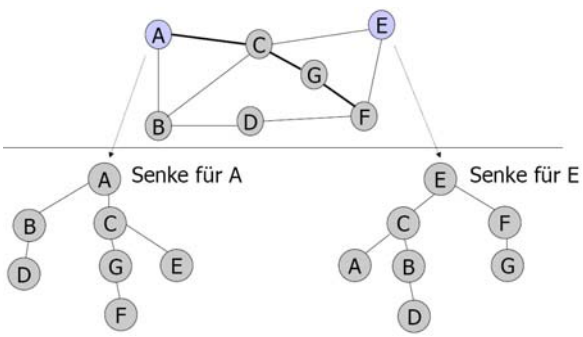


2+4+1 = 7
A-C-E-F = sparsamster Weg, obwohl Route nicht auf dem direkten Weg liegt.

Als kürzester Pfad von A-F ergibt sich im obigen Bild der Pfad A – C – E – F mit einer Pfadlänge von 7. Die Pfadlänge kann eine beliebige (Kombination von) Metrik(en) sein, wie z.B. die Entfernung, Bandbreite, Durchschnittsverkehr, Durchschnittliche Warteschlangenlänge in den Routern oder die Verzögerung.

Optimierungsprinzip – Sink Tree

Wenn das Optimierungsprinzip auf das Routing angewendet wird, bilden die optimalen Routen von allen Quellen zu einem bestimmten Ziel einen Baum, dessen Wurzel das Ziel ist. Dieser Baum enthält keine Schleifen und heißt Sink Tree oder Senke.



Ein Sink-Tree wird zum finden eines optimalen Weges verwendet. Ausgehend von einem Startrouter (Wurzel B des Baumes) in einem Rechnernetz werden die Verbindungen zu allen anderen Routern analysiert und ausgehend von den verschiedenen Zweigen die kürzesten Verbindungen zu allen anderen Routern gezogen. Dadurch erhält man die optimalen Routen. Alle anderen möglichen Verbindungen werden nicht mehr dargestellt und sozusagen verworfen.

Shortest Path Routing

Ein statischer Graph des Teilnetzes wird erstellt:

- Knoten als Router, Kanten als Leitungen
- Kanten werden mit der Pfadlänge beschriftet, also einer beliebigen Metrik
- Die Berechnung des kürzesten Pfad erfolgt über einen Algorithmus, wie Dijkstras Algorithmus
- Bild: siehe oben (Optimierungsprinzip – Allgemein)

Distance-Vector-Routing

- Jede Route führt eine dynamisch aktualisierte Routing-Tabelle mit allen Zielen
- Einträge enthalten auch die bevorzugte Ausgangsleitung zu einem Ziel
- Nur die Nachbarn tauschen Routing-Informationen aus
- Schleifen (Count-to-Infinity) möglich, schlechte Konvergenz

Ziel	Distanz	Nächster Knoten	Hops

Link-State-Routing

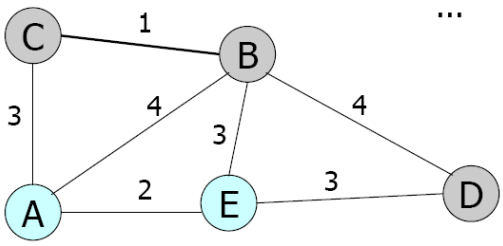
- Jeder Router verwaltet eine Kopie der gesamten Netzwerktopologie und kennt alle Ziele
- Ziel: Jeder Router kennt darüber hinaus alle Kosteninformationen
- Jeder Router verteilt die Routen-Informationen an alle Router (nicht nur an die Nachbarn)
- Jeder Knoten errechnet den absolut kürzesten Pfad selbst
- keine Schleifen möglich und höhere Konvergenzzeit

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

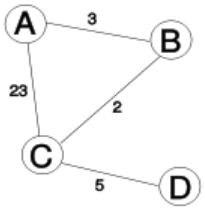


8. Was versteht man im Distance-Vector-Routing-Verfahren unter dem Count-to-Infinity-Problem und wie verhält sich das Verfahren im Hinblick auf Konvergenz? Begründen Sie Ihre Entscheidung!

Beim Distance-Vector-Verfahren führt jeder Router eine dynamisch aktualisierte Routing-Tabelle mit allen Zielen der näheren Umgebung. Dabei speichert ein Router die Entfernung zu jedem Router (Entfernung = Pfadlänge bzw. Kosten) und diese Aufstellungen werden mit anderen Routern ausgetauscht. Die von anderen Routern erhaltenen Informationen werden dann in die eigene Tabelle eingerechnet.

Der Begriff Entferungsvektor kommt daher, dass eine Route zu einem Ziel als Kombination von Entfernung (Metrik) und Richtung (bevorzugte Ausgangsleitung zu nächstem Knoten) gespeichert wird.

Probleme: Count-to-Infinity und Konvergenzzeit



Es sind Schleifen möglich, dadurch können Pakete ewig kreisen (Count-to-Infinity Problem). Beispiel aus Sicht von Router A:

- C sagt, Router D ist nur noch schlecht zu erreichen. Bester Pfad von A nach D nach wie vor über Router B
- B sagt, Router D ist nur noch schlecht zu erreichen, neue Pfadlänge: 13. Nun haben sich auch die Pfadkosten von A nach D geändert.
- Das die Kosten über B nicht weiter angestiegen sind liegt daran, dass B denkt, er könne D noch indirekt über A erreichen (Pfadlänge 10 + 3 = 13). Problem: B weiß nicht, dass er auf dieser indirekten Route über A liegt (Route: B-A-B-C-D).
- So steigen die Pfadkosten langsam, anstatt sprunghaft anzusteigen. Außerdem können sich so Schleifen bilden, da die beiden Router das Paket mehrmals hin und her schicken, da sie denken, der nächste Router hat die bessere Ausgangsroute zu dem nur noch schwer erreichbaren Ziel.

Daraus ergibt sich das Problem der schlechten Konvergenz – Schlechte Nachrichten verbreiten sich nur sehr langsam im Netz. Dies liegt daran, dass kein Knoten über die vollständigen Informationen über eine Route verfügt, da er ja immer nur seinen Nachbarn kennt.

Die Routing-Informationen beim Distance-Vector-Verfahren liegen übrigens beim Netzstart noch nicht vor, erst nach einer gewissen Konvergenzdauer verfügen alle Knoten über die optimalen Routinginformationen. Daher gibt beim Start jeder Router für jeden bekannten Knoten die Entfernung 0, für alle unbekannten Ziele die Entfernung unendlich an. Diese Informationen werden nach und nach mit jeder gesendeten Information iterativ verbessert.

Definition Konvergenzzeit: Die Zeit, die benötigt wird, bis alle Router die aktuelle Vernetzungsstruktur kennengelernt haben.

Konvergenz und Count-to-Infinity: siehe auch Aufgabe 36

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

Das Distance-Vector-Verfahren ist ein adaptives (dynamisches) Verfahren und gehört hier zu den Verteilten Verfahren. Verteiltes Verfahren bedeutet, dass die Routing-Funktionalität dezentral in jedem einzelnen Knoten liegt. Die Routing-Tabellen werden dabei im Zusammenspiel mehrerer Router ermittelt.

Das Verfahren ist in den Routingprotokollen RIP und IGRP implementiert, da die Implementierung sehr einfach ist und nahezu ohne Wartung funktioniert.

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

Siehe Aufgabe 7: Entfernung, Anzahl Teilstrecken (Hops), Bandbreite, Durchschnittsverkehr, Durchschnittliche Warteschlangenlänge der Router oder die Verzögerung. Es ist auch eine Kombination mehrerer Metriken möglich.

11. Wie sieht ein einzelner Router im Link-State-Routing-Verfahren die aktuelle Netzwerktopologie?

Beim Link-State-Verfahren verwaltet ein Router eine Kopie der gesamten Netzwerktopologie ein einer Link-State-Datenbasis (Distance-Vector speichert nur die nähere Umgebung) – jeder Router kennt also die Kosteninformationen des gesamten Netzwerks. Dabei verteilt jeder Router die lokale Informationen per Flooding an alle anderen Router und so kennt jeder Router alle anderen.

Der Name Link-State des Verbindungszustandsverfahren kommt daher, da es die globalen Zustandsinformationen des Netzes mit den Kosten aller Verbindungsleitungen (Links) kennen muss. Zu Anfang sind diese Informationen noch nicht bekannt, werden aber durch den Empfang von Link-State-Broadcasts ermittelt.

Die Berechnung der optimalen Routen erfolgt dezentral, jeder Router errechnet den absolut kürzesten Pfad, z.B. über den Shortest-Path-Algorithmus (Dijkstra).

Der Vorteil ist, dass keine Schleifen möglich sind, allerdings eignet sich das Verfahren nicht für sehr große Netze wie dem Internet. Daher ist es empfehlenswert, eine gewisse Hierarchie im Netz einzuführen und innerhalb der Teilnetze eigene Routing-Verfahren zu nutzen.

12. Sind im Link-State-Routing-Verfahren Schleifen möglich? Begründen Sie Ihre Entscheidung!

Da jeder Router das gesamte Netzwerk kennt und jeder Knoten die gleichen Informationen über die Topologie besitzt, sind keine Schleifen möglich. Ein weiter Vorteil ist so, dass auf Toplologieänderungen schnell reagiert werden kann.

13. Was versteht man unter einem Leaky-Bucket-Verfahren und wozu dient es?

Auch in der Vermittlungsschicht können Überlastsituationen (Cognestions) auftreten, weil z.B. zu viele Pakete unterwegs sind, oder die Netzknoten zu langsam sind oder zu wenig Speicher haben.

Das ganze kann zu einem Teufelskreis führen, wenn die Absender verloren gegangene Pakete erneut versenden und dies die Last weiter erhöht. Als Lösung eignen sich Verfahren zur Staukontrolle, die in den Schichten 2-4 implementiert werden können.

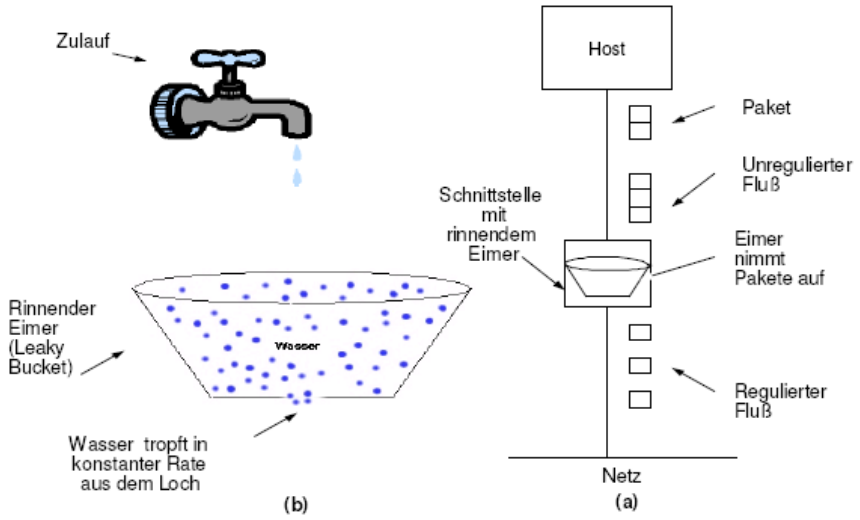
- Lokale Steuerung der Einzelleitungen (Schicht 2)
- Ende-zu-Ende Steuerung der Endsysteme (Schicht 4)
- Globale Steuerung über das gesamte Netz (Schicht 3)

Da Staukontrolle ein Mechanismus mit netglobalen Auswirkungen ist, sollte er auf der Schicht drei implementiert werden. Ursache für Überlastungen sind vor allem Verkehrsspitzen.

Eine wesentliche Ursache für Überlastungen sind Verkehrsspitzen. Im Vorfeld können diese beispielsweise durch Traffic Sharping eingedämmt werden, dass die durchschnittliche Datenübertragungsrate der Endsysteme reguliert. Hierzu ist eine Überwachung der Endsysteme von Seiten des Netzbetreibers notwendig (Traffic Policing).

Beispiel: Leacky-Bucket-Algorithmus:
Die Endsysteme verfügen über eine Netzwerkschnittstelle (in Kernel und Netzwerkkarte) mit einer internen Warteschlange, die als Leacky Bucket (rinnender Eimer) bezeichnet wird. Wenn die Warteschlange voll ist, wird ein Paket schon im Endsystem verworfen und belastet nicht das Netz.

Auf technischer Seite müssen sich Sender, Empfänger und das Netzwerk beim Verbindungsaufbau über die Flussspezifikationen (Paketgröße, Übertragungsrate, ...) einigen, daher eignet sich das Verfahren besonders für virtuelle Verbindungen (VC).

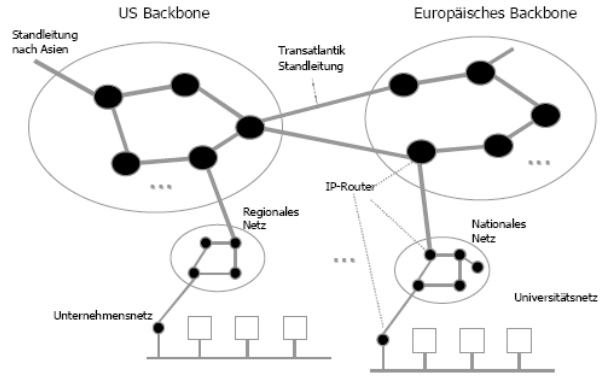


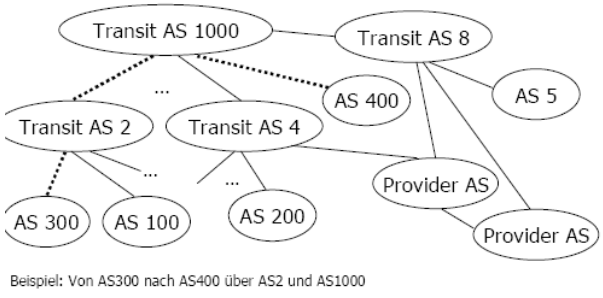
14. Was ist ein autonomes System im Internet und welche Arten von autonomen Systemen kennen Sie?

Das Internet besteht aus einer Sammlung von Autonomen Systemen (AS), also eigenständig verwalteten Teilnetzen. Das Internet ist also eine hierarchische Organisation dieser Teilnetze, die mit großen Backbones mit hoher Leistung über schnelle Router miteinander verbunden sind (das Internet wird dadurch hierarchisch Strukturiert!).
An regionalen Netzen hängen Netzen von Unternehmen, Universitäten und ISPs, die wiederum zu überregionalen Netzen verbunden sind, die wiederum über noch größere Leitungen (z.B. Transatlantik Standleitung) verbunden sind.

Autonome Netze haben sich unterschiedlich entwickelt und verfügen über unterschiedliche Routingstrategien.

Neben normalen AS von Universitäten, Providern und Organisationen gibt es noch Transit-AS, die als Transportnetze arbeiten um von einem Netz in ein anderes zu kommen.





15. Was ist im globalen Internet ein Transit-AS?

Siehe Aufgabe 14

16. Beschreiben Sie kurz den Dienst, den IP für die darüber liegenden Schichten zur Verfügung stellt im Hinblick auf die Übertragungssicherheit!

IP (Internet Protocol) ist ein paketvermitteltes (datagrammorientiertes) und verbindungsloses Protokoll, dass einen ungesicherten verbindungslosen Dienst zur Verfügung stellt. Die Pakete werden also nach dem Best-Effort-Prinzip ausgeliefert, es besteht keine Übertragungsgarantie. Jedes Paket des Datenstroms wird dabei isoliert betrachtet

Die Pakete sind unterschiedlich groß, die Längenrestriktionen kommen von der zugrunde liegenden Schicht 2. In Ehternet-Netzen sind die Pakete bspw. auf 1500 Byte beschränkt. Der Versand erfolgt meist über mehrere Zwischenstationen (Router), bevor ein Paket beim Ziel eintrifft.

Aufgaben: Beförderung der Datagramme, Fragmentierung der Datagramme der darüberliegenden Schicht, Routing-Unterstützung.

17. Welches Vermittlungsverfahren verwendet die Internet-Schicht?

Das Internet verwendet eine datagrammorientierte, verbindungslose Paketvermittlung.

Auf der Schicht 3 stellt IP einen ungesicherten verbindungslosen Dienst zur Verfügung, die Auslieferung erfolgt ohne Garantie nach dem Best-Effort Prinzip.
Erst auf der Schicht 4 werden virtuelle Verbindungen (TCP-Protokoll) ermöglicht.

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?

Mit NAT werden Adressen eines privaten Netzes über Abbildungstabellen öffentlich registrierten IP-Adressen (Internet) zugeordnet. Interne Rechner müssen demnach keine öffentlichen IP-Adressen mehr haben, sondern es reicht eine Verbindung nach draußen.

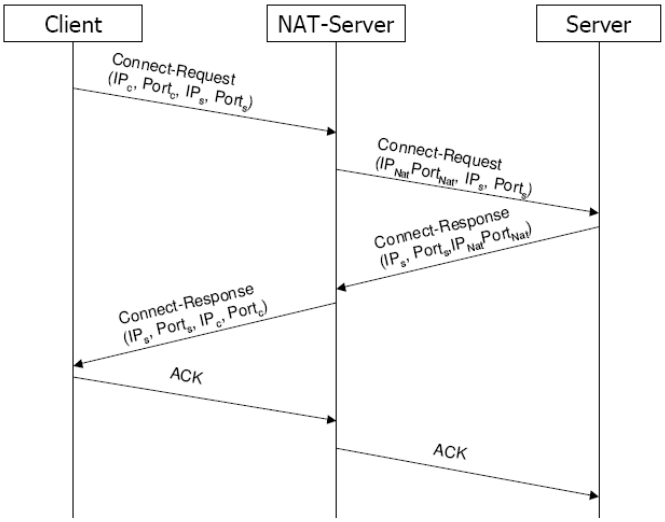
Zuordnungen:

- 1:1 – für jede interne IP-Adresse wird eine externe IP-Adresse zugeordnet
- 1:n – Alle Internen IP-Adressen werden auf eine öffentlich registrierte Adresse abgebildet (PAT – Port and Address Translation bzw. IP-Masquerading). Die Abbildung erfolgt hier über Portnummern.

Der NAT-Server arbeitet nach außen hin als Stellvertreter (Proxy) für alle internen Hosts. Er tauscht bei allen ausgehenden und ankommenden IP-Paketen die IP-Adressen und die Ports der Transportschicht aus. Bei ausgehenden Paketen werden im IP-Header die Felder Quell-IP und im TCP-Header der Quellport durch den NAT-Server ausgetauscht. Bei ankommenden Paketen wird Ziel-

IP ausgetauscht. Diese Mapping-Informationen werden dabei intern in einer Tabelle gespeichert und verwaltet, um auch die PDUs der Gegenseite wieder übersetzen zu können.

Dadruch gibt es keine echten Ende-zu-Ende-Verbindungen bei TCP, die Verbindung wird immer wieder unterbrochen.



Vorteile von NAT / PAT:

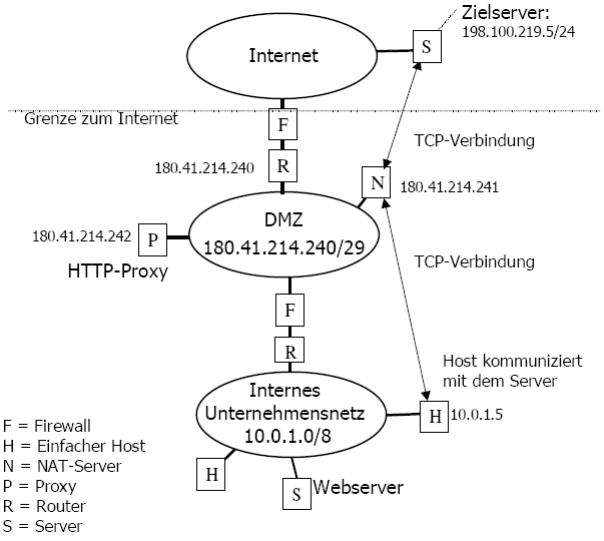
- Die Sicherheit in einem Unternehmen wird erhöht, da potentiellen Angreifern die Netzwerkstruktur verborgen bleibt und kein interner Host direkt adressiert werden kann
- IP-Adressen werden eingespart, da nur noch eine offizielle IP-Adresse für ein Unternehmensnetzwerk benötigt wird.

Beispiel: DMZ (De-Militarized Zone)

NAT wird heute auch in DMZ verwendet, damit die internen Rechner ohne Verletzung der Sicherheit nach außen kommunizieren können.

Eine DMZ ist eine Art Zwischennetz zwischen dem Internet und einem privatem Netz, das speziell an jedem Ende mit Firewalls und Routern gesichert ist.

Möchte ein Host mit dem Internet kommunizieren, geht das nur über die DMZ. In der DMZ selbst stehen die Rechner, die nach außen hin sichtbar sein sollen, wie HTTP- und Webserver. Diese können zur weiteren Erhöhung der Sicherheit auch durch Proxys vertreten werden.



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

- Austausch von Quell-IP (IP-Header) und Quell-Port (TCP-Header) in ausgehenden Paketen.
- Austausch von Ziel-IP (IP-Header) und ggfs. Ziel-Port (TCP-Header) in eingehenden Paketen

Siehe Aufgabe 19

21. Warum muss ein 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?

Die Checksumme im IP-Header wird über die Bestandteile des Headers errechnet. Da der NAT-Server die Quell-IP-Adresse austauscht, ändert sich der Kopfdatenbereich und die Prüfsumme muss demzufolge neu berechnet werden. (Vermutung!)

Wenn der NAT-Server gleichzeitig auch als Router fungiert ändert sich auf alle Fälle der TTL-Wert und die Prüfsumme muss dann so oder so neu berechnet werden (Vermutung!).

22. Nennen Sie den Unterschied zwischen der klassischen Subnetz-Adressierung und dem Classless Interdomain Routing (CIDR)! Welche Vorteile bringt CIDR für die Adressenknappheit im Internet (Begründung)?

Subnetze

Die klassische Subnet-Adressierung ermöglicht die interne Aufteilung des Netzwerkes einer Organisation in mehrere Subnetze. Die Änderungen betreffen nur die interne Struktur, nach außen hin ist das Netzwerk wie gewohnt durch die ursprüngliche Netzwerkadresse adressierbar.

- Die Einteilung der Klassen (Klasse A – E) bleibt nach wie vor bestehen.
- Eine festgelegte Subnetzmaske muss für alle Subnetze gelten, d.h. ein Subnetz kann nicht weiter unterteilt werden.

VLSM

VLSM ist ein erweitertes Subnetting und ermöglicht variable lange Subnetzmasken innerhalb einer Organisation, d.h. die Länge der Subnetzmaske kann innerhalb der verschiedenen Subnetze unterschiedlich sein.

- VLSM ist ähnlich wie Subnetze nur auf das lokale Netz beschränkt.

CIDR

CIDR ist ein Verfahren zur noch effizienteren Nutzung der IP-Adressen. Hier entfällt die feste Zuordnung IP-Adresse zu Netzklasse und das Subnetting. Es gibt nur noch eine Netzmaske, welche die IP-Adresse in einen Host- und Adressteil aufteilt. Deren Länge kann wie bei VLSM variabel sein.

- Die Klassenstruktur (A, B, C) wurden hierzu fallen gelassen
- Unterstützung geographischer Regionen für ein hierarchisches Routing (zur Entlastung der Routing-Tabellen)
- Es gibt keine Subnetze mehr, sondern nur noch eine Unterteilung in Host- und Adressteil. Dadurch ist es möglich, den Adressbereich beliebig auszugestalten, ähnlich wie mit VLSM-Subnetzen mit einer variabel langen Subnetzmaske möglich ist.

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

Die Netzmaske trennt eine IP-Adresse in einen Netzwerkteil (Adressteil) und einen Hostteil. Für die Router ist es daher wichtig zu wissen, in welches Netz ein Paket verschickt werden soll. Durch die Netzmaske können die Router beispielsweise rausfinden:

- Welche Adressen im eigenen Netzwerk liegen und welche nur über einen anderen Router adressiert werden können
- Welche Adressklasse in einem Netz als Ziel adressiert ist

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

Die Darstellung 132.10.1.8 /24 weißt auf folgende Informationen hin:

- Netzwerkadresse: 132.10.1.0
- Subnetzmaske: 255.255.255.0
- Adressteil: 24 Bit
- Hostteil: 8 Bit

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

- Gewöhnlich wird die IP-Adresse oder der Hostname vom Benutzer in der Anwendung angegeben.
- Reverse ARP (falls MAC-Adresse vorhanden ist, siehe Aufgabe 26)
- DNS, falls der Hostname bekannt ist
- …?

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

Beschreibung

Ein Host kennt Initial nur seine eigene MAC-Adresse und nicht die der Partnerhosts in eigenen oder fremden Netzwerken. Er benötigt diese Adresse aber, da diese für die Adressierung in der Bitübertragungsschicht (Schicht 2) notwendig sind. Im OSI-Modell werden MAC-Adressen statisch per Vorabkonfiguration mit IP-Adressen gekoppelt, in internetbasierten Netzen muss eine MAC-Adresse jedoch zur Laufzeit ermittelt werden. Dies ermöglicht das Steuerprotokoll ARP (Address Resolution Protocol), dass zur Hälfte in Schicht 2 und 3 angesiedelt ist. Es wird für das dynamische Mappen von Schicht2-Adressen (MAC-Adressen) auf IP-Adressen (Schicht3) verwendet.

Funktionsweise (eigenes LAN):

- Wenn ein bisher unbekannter oder ein bereits bekannter Zielhost adressiert wird, der längere Zeit nicht mehr adressiert wurde, wird ein ARP-Request mit der Ziel-IP-Adresse in einem begrenzten Broadcast im LAN gesendet. Mit diesem ARP-Request fragt der Host quasi, wer diese Adresse kennt.
- Der Zielhost oder ein anderer Host, der den Zielhost kennt, antwortet mit einem ARP-Reply und übergibt die MAC-Adresse

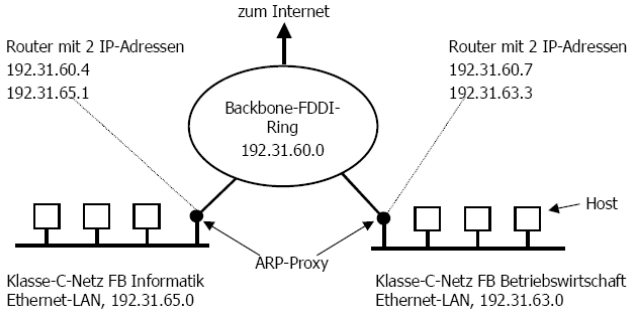
Damit nicht jedes Mal neu angefragt werden muss, führt jeder Host einen ARP-Cache und merkt sich das Mapping der Hosts, mit denen er aktuell zu tun hat. Dieser Cache wird periodisch bereinigt, um Inkonsistenzen zu vermeiden. Hierzu wird ein TTL-Feld geführt und nach Ablauf (z.B. 20 Minuten) der Zeit wird der Eintrag im ARP-Cache automatisch gelöscht.

Funktionsweise (anderes LAN):

Wenn der Zielhost nicht im lokalen Netz ist, kann dieser nicht antworten. In diesem Fall übernimmt der zuständige IP-Router die Rolle eines Stellvertreters (ARP-Proxy) und sendet seine MAC-Adresse an den anfragenden Host. Über die IP-Adresse kann der ARP-Proxy dann aus seiner Routing-Tabelle die gewünschte Route bestimmen.

Reverse ARP

Dieses Protokoll wird benötigt, wenn zu einer MAC-Adresse eine IP-Adresse gesucht wird. Beispiel: Plattenlose Workstation fährt hoch und möchte ihre IP-Adresse erfahren. Durch einen RARP-Request antwortet ihr ein zuständiger RARP-Server und teilt die Adresse mit.



Beispiel für einen ARP-Request über einen ARP-Proxy.

Unterschied DHCP / RARP:
RARP gibt nur die IP-Adresse zurück, keine Konfigurationsdaten wie DHCP.

RARP ist nur auf Subnetze beschränkt, DHCP (bei Verwendung eines DHCP-Relays nicht).

27. Über welches Steuerprotokoll wird eine Ping-Nachricht abgesetzt? Verwendet das besagte Steuerprotokoll TCP, UDP oder direkt IP zur Nachrichtenübertragung?

Das ICMP-Protokoll (Internet Control Message Protocol) dient zum Austausch von Informations- und Fehlermeldungen über IP-Netze. Das Protokoll ist dabei direkt auf der Vermittlungsschicht (OSI) bzw. Netzwerkschicht (non-OSI) angesiedelt. Daher nutzt es für die Datenübertragung direkt das IP-Protokoll und nicht etwa UDP oder TCP.

Der Header eines ICMP-Pakets enthält den Nachrichtentyp und einen Code sowie eine Prüfsumme. Im Nutzdatenteil wird ein Teil des ursprünglichen Pakets übertragen, und zwar der alte IP-Header und ein Teil des Nutzdatenteils (64 Bit).

Es gibt mehrere Typen von ICMP-Nachrichten (Beispiele):

- Destination unreachable, wenn Datagramm nicht ausgeliefert werden kann
- Network unreachable, wenn addressiertes Netzwerk von einem Router nicht erreicht werden kann
- Source quench, wenn der Speicherplatz erschöpft ist
- Echo-Requests und Echo-Replys, um zu Prüfen, ob ein Host / Router erreichbar ist (ping)
- Time-Exceedet, wird z.B. vom Commando traceroute verwendet, um die Route zwischen zwei Rechnern zu ermitteln

28. Erläutern Sie den Unterschied zwischen *limited Broadcast* und *directed Broadcast* in IPNetzen! Wann benötigt man z.B. diese Broadcast-Varianten (Nennen Sie je ein Beispiel)?

Ein Broadcast ist eine Nachricht, die an alle Teilnehmer eines Netzwerkes übertragen werden. Der Unterschied zwischen einem direkten und limitierten Broadcast ist das Zielnetzwerk: der direkte Broadcast richtet sich an ein bestimmtes Netz, der limitierte Broadcast immer nur auf das eigene Netz.

Direkter Broadcast

Ein direkter (gerichteter) Broadcast ermöglicht das Senden eines Broadcastes an ein beliebiges Netzwerk von einem Host aus einem anderen Netzwerk. Die Adresse wird als Kombination aus Zielnetz und dem Setzen aller Hostbits auf 1 angegeben, z.B. x.y.z.255.

Limitierter Broadcast

Ein begrenzter Broadcast bezieht sich auf das lokale Netz und wird von den Routern nicht durchgelassen. Die limited Broadcast-Adresse ist die 255.255.255.255 und Pakete mit dieser Zieladresse werden von allen Hosts entgegengenommen.

Beispiel Direkter Broadcast: DoS-Angriff, DHCP

Beispiel Limitierter Broadcast: RARP

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

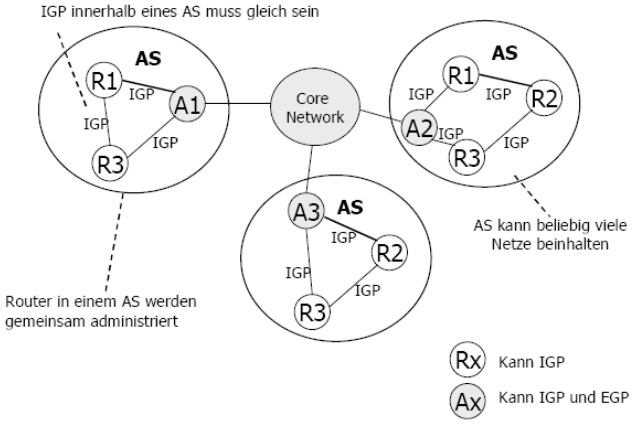
Leacky Bucket Algorithmus – ein Verfahren zum Traffic Shaping (siehe Aufgabe 13)

Choke Pakete – Die überlasteten Stellen schicken zur Überlastvermeidung eine explizite Aufforderung an den Verursacher, die Netzlast zu reduzieren.

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

Verschiedene Autonome Systeme kommunizieren über ein gemeinsames EPG (siehe Aufgabe 37) übereinander. Innerhalb eines Autonomen Systems müssen alle Netzwerkknoten über ein gemeinsames IPG kommunizieren.

Wie die nebenstehende Abbildung zeigt, muss das IGP innerhalb eines Autonomen Systems gleich sein. Dies liegt unter anderem daran, dass die EGPs meistens auf die Infrastruktur aufbauen, die von den IGPs geschaffen werden und die Router in einem IGP gemeinsam administriert werden.



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

Im Internet wurden früher viele Adressen uneffizient vergeben. Schuld daran waren insbesondere die starren Adressklassen (Klasse A, B und C Netzwerke).
Wenn eine Organisation beispielsweise 20 Adressen benötigt hat, so musste sie ein Klasse-C Netzwerk erwerben, wobei dann (256 – 2) – 20 Adressen verschenkt worden sind.
Für das Problem wurden bzw. werden folgende Einsparvarianten verwendet:

- Subnetting (Subnetze mit fixer Länge)
- VLSM (Subnetze mit variabler Länge im Intranet)
- CIDR (Wegfallen der Klassenstruktur, Einführung von Netzen mit variablem Adressteil)
- NAT (Network Access Translation)
- zukünftig: das IPv6-Protokoll mit Adresslängen von 128 Bit

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

- Die MAC-Adresse bekommt der Host über das ARP
- Die Veralterung wird vermieden durch den ARP-Cache
- siehe Aufgabe 26

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

Das TTL-Feld im IP-Header steht für Time To Live und soll verhindern, dass unzustellbare Pakete endlos im lange von Router zu Router weitergeleitet werden. Der Wert in diesem Feld gibt einen Hop-Count an, der beim Versenden typischerweise mit 64, 128 oder 255 initialisiert wird. Jeder Router, den ein Paket passiert, verringert den Wert um 1, wenn der Wert 0 erreicht ist wird das Paket verworfen und eine ICMP-Nachricht an den Absender gesandt.
(Früher stand der TTL-Wert für die Anzahl der Sekunden, die das Paket zu leben hat.)

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

Das Feld Protokoll aus dem IP-Header definiert das darüberliegende Protokoll, an das die Daten des Paketes weitergeleitet werden sollen. Es ist wichtig für die Zuordnung ankommender Pakete an die entsprechende Transportinstanz, damit die ankommenden Daten weiterverarbeitet werden können

Beispiel: 6 = TCP, 89 = OSPF, …

35. Beschreiben Sie kurz den Protokollmechanismus der Fragmentierung am Beispiel von IPv4 und gehen Sie dabei auf die genutzten Felder *Identifikation, Fragment Offset* und *Flags* ein!

Fragmentierung allgemein:

Das Internet unterstützt eine Vielzahl von Netzwerkzugängen (Schicht 2), die alle eine unterschiedliche Nutzdatenlänge haben.

Ethernet (LAN) haben bspw. eine Maximaldatenlänge von 1500 Bytes, im WAN können viele Protokolle nicht mehr als 576 Byte übertragen. Diese Größe wird auch als MTU (Maximum Transfer Unit bezeichnet).

Wenn ein IP-Datagramm größer ist als die MTU des Netzwerkzugangs, dann muss ein Router das Paket zerlegen (fragmentieren) und der Zielknoten muss alle Pakete wieder zusammenbauen (reassemblieren / defragmentieren).

Beschreibung der für Fragmentierung wichtigen Felder im IP-Header

Im IP-Header ist ein 3 Bit Feld „**Flags**“ enthalten, dass zur Kontrolle der Fragmentierung dient. Es sind drei Flags enthalten, wovon nur die Flags DF uund MF benutzt werden.

- DF=1 (Disable Fragmentation)
  Wenn dieses Feld gesetzt ist, darf keine Fragmentierung erfolgen. Wenn ein Paket, das nicht fragmentiert werden darf, fragmentiert werden muss, dann wird das Paket verworfen.
- MF=0 / 1 (More Fragments)
  Wenn MF=1 gesetzt ist, dann folgen noch weitere Fragmente. Wenn MF=0 ist, dann handelt es sich um das letzte Paket.

Das Feld **„Fragment Offset (FO)**“ im IP-Header dient der korrekten Herstellung der Ursprungssequenz, wenn ein Paket fragmentiert worden ist. Damit lassen sich maximal 8192 * 8 Bytes darstellen, was mit der maximalen Paketlänge 65536 korrenspondiert, der kleinste Fragment hat die Länge 8 Byte (ohne Header). Korrekte Anwendung: siehe unteres Beispiel.

Vorgehen bei der Fragmentierung:

- Überprüfung DF-Flag, wenn DF=1 wird das komplette Paket verworfen, wenn DF=0 wird das Datenfeld des Ur-Pakets in mehrere Teile zerlegen
- Alle neuen Pakete (außer das Letzte) weißen eine Länge von einem Vielfachen von 8 Byte auf
- Alle Datenteile werden in ein neu erzeugtes IP-Paket eingebettet, der Header ist eine Kopie des Ur-Paketes mit einigen Modifikationen
  - MF wird bei allen (außer dem letzten) Paket(en) auf 1 gesetzt
  - FO enthält relative Angabe (Offset) in Byte
  - Für die Optionen des Ur-Paketes wird abhängig vom Type-Feld entschieden, ob Angabe übernommen wird.
  - Headerlänge und Headerprüfsumme werden für jedes Paket errechnet

Vorgehen bei Defragmentierung:

- Alle ankommenden Fragmente werden zunächst gepuffert. Beim Eintreffen des ersten Fragments wird darüber hinaus ein Timer gestartet.
- Ist der Timer abgelaufen, bevor alle Fragmente eingetroffen sind, werden alle Pakete verworfen
- Im anderen Fall wird die Reassemblierung am Zielhost durchgeführt und das komplette IP-Datagramm am N-SAP zur Transportschicht hochgereicht

Beispiel Fragmentierung

Ein Datagramm mit 4.000 Bytes inkl. IP-Header soll über eine Ethernet-Verbindung mit einer MTU von 1500 Bytes übertragen werden. Daher dürfen die Nutzdaten der IP-Pakete bei einem IP-Header von 20 Bytes nicht größer als 1480 Bytes tragen, um kleinergleich 1500 Bytes der Ethernet-MTU zu sein.

Wichtig: die MTU limitiert die Nutzdaten der darunterliegenden Schicht, also wird der Header der Ethernet-Frames beispielsweise nicht mit einberechnet. In den Ethernet-Nutzdaten sind die Nutzdaten und der Header der darüber liegenden Schicht (IP-Schicht) enthalten, also die IP-Daten und der IP-Header. Ein Ethernet-Frame ist bei einer MTU von 1500 Bytes also 1520 Bytes groß.

Fragment	Byteanzahl im Datenfeld	Identifikation	Fragment-Offset in Byte (im FO-Feld)[163]	Flags
1	1.480	777	0 (0)	MF=1
2	1.480	777	1.480 (185)	MF=1
3	1.020	777	2.960 (370)	MF=0

Tip: Um eine Fragmentierung, die viel Overhead erzeugt, zu verhindern, sollte die Paketgröße bereits auf der Transportschicht eingeschränkt werden.

Beispiel: Eine Ethernet-MTU von 1500 bedeutet für TCP eine Nutzdatenlänge von 1460 Bytes oder eine Gesamtpaketlänge von 1480 Bytes, da 20 Bytes für den TCP-Header und 20 Bytes für den IP-Header dazukommen.

36. Welches Problem im Routing-Protokoll RIP versucht die Split-Horizon-Technik zu lösen und wie funktioniert diese Technik? Zeigen Sie dies anhand eines einfachen Beispiels mit Skizze!

Beschreibung RIP-1

RIP wurde ursprünglich von XEROX entwickelt und ist ein leicht zu implementierendes Distance-Vector-Protokoll auf UDP-Basis. Beim Start eines Routers sendet dieser eine Request-PDU an alle Nachbarn (Broadcast) und fordert Routing-Informationen an, die er in einer Response-PDU als Unicast-Nachricht erhält. Im normalen Betrieb senden die Router unaufgefordert alle 30 Sekunden ihre Routing-Informationen in einer Response-PDU (Broadcast Advertisements) mit maximal 25. Tabelleneinträgen an ihre Nachbarn (jeder Router kennt nur die direkten Nachbarn!).

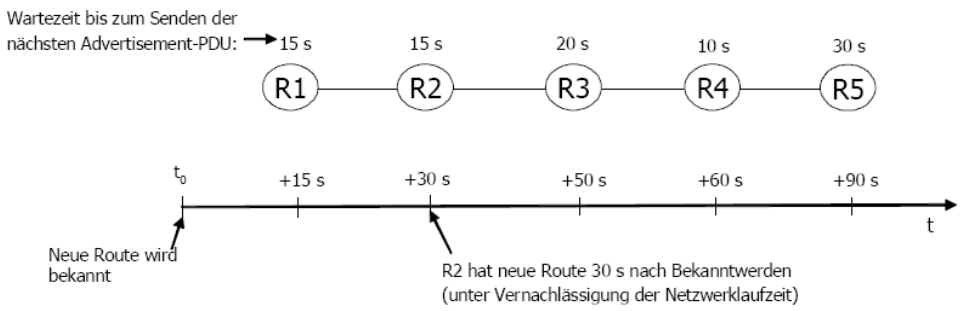
Als Metrik wird in den Routen-Informationen immer die Anzahl der Sprünge (Hops) von Router zu Router (Ermittlung über TTL) verwendet. Der maximale Hop-Count ist 15, alles was darüber liegt wird als unendlich interpretiert.

Wenn ein Router 180s nichts von einem Nachbarn hört, gilt dieser als nicht erreichbar und die Route zu ihm wird mit einem Hop von 16 belegt. Im Anschluss daran wird der Router aus der Routing-Tabelle entfernt.

Probleme bei RIP-1: Count-to-Infinity-Problem und Konvergenzverhalten

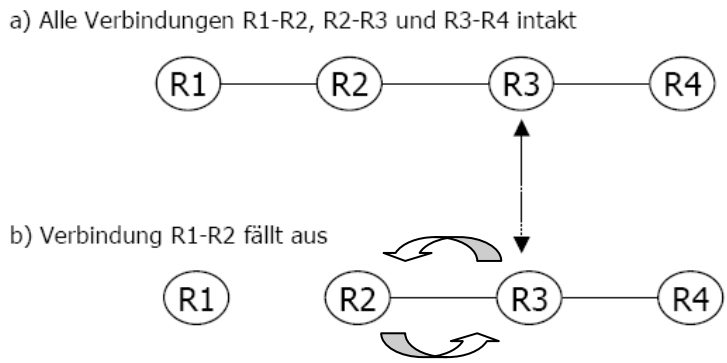
Langsames Konvergenzverhalten

Die Konvergenzzeit, bis eine Änderung des Netzes bei einer maximalen Ausdehnung des Netzes von 15 Hops kann bis zu 7 Minuten betragen, da die Router nur alle 30 Sekunden ihre geänderten Routen-Informationen verteilen.



Beispiel mit zufälligen Zeitintervallen bis ein Router die Informationen weiterleitet (im Mittel 15 Sekunden).

Count-to-Infinity-Problem



Beispiel: Router R1 fällt aus:

- R3 hat die Routing-Information, dass R1 über einen Hop erreichbar ist
- R3 propagiert diese Infos an R2 und R4
- R2 glaubt diese Information und sendet seine Pakete nun über R3 an R1

- Es entsteht ein Ping-Pong Effekt (Schleife), erst wenn HopCount 16 erreicht worden ist, wird bemerkt, dass R1 nicht mehr erreichbar ist

Probleme: siehe auch Aufgabe 8

Lösungen:

Split-Horizon

Ein Router propagiert keine Routen an einen anderen Router, über den er die Route kennengelernt hat. Im oberen Beispiel wüsste R3 woher die Route nach R1 kommt (über R2) und würde die R2 nicht anbieten.

Split-Horizon mit Poison-Reverse

Bei dieser Technik werden alle Routen propagiert, jedoch werden die Route, die von demselben Knoten kennengelernt worden sind, mit einer Metrik von 16 Hops gesendet. Damit ist dieser als nicht erreichbar markiert.

Triggered Update

Routen-Aktualisierungen werden unmittelbar nach dem Eintreffen dieser Ereignisse weitergeleitet. Dies erhöht Netzwerkbelastung, reduziert aber die Konvergenzzeit.

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!

IGP (Interior Gateway Protokolle)

Diese Protokolle werden innerhalb eines Autonomen Systems (AS) verwendet (Intra-AS-Routing).

Beispiel: RIP und OSPF

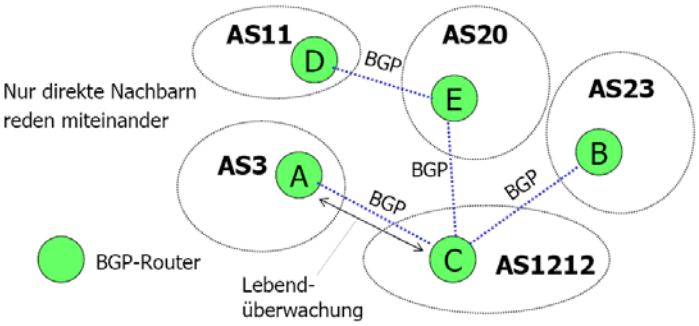
EGP (Exterior Gateway Protokolle)

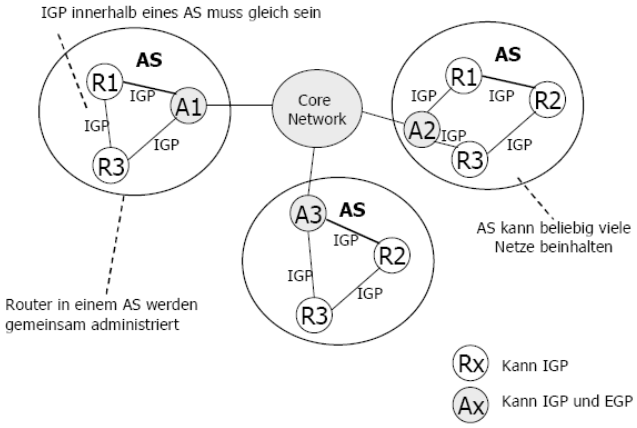
Diese Protokolle werden für die Kommunikation zwischen Autonomen Systemen (AS) (Extra-AS-Routing).verwendet. Dabei werden andere Ziele als bei IGP-Protkollen verfolgt:

- Nicht alle Pakete zwischen den Autonomen Systemen dürfen befördert werden
- Für den Transitverkehr werden Gebühren berechnet
- Wichtige Informationen dürfen nicht durch unsichere AS gesendet werden

Beispiel: BPG (Broader Gateway Protokoll)

Das BGP ist ein Distance-Vector-Protokoll und quasi der De-facto Standard. Hier werden nicht nur die Kosten pro Ziel verwaltet, sondern auch eine Buchführung über die Nutzung der Verbindungen durchgeführt.





Beispiel für ein EGP: BGP (Border Gateway Protocoll, z.B. BGPv4)

BGP ist ein Exterior Gateway Protocoll (EGP) und ein heutzutage im Internet verwendetes Path-Vector-Protocoll (Pfadvektorprotokoll). Es ermöglicht das Routing zwischen verschiedenen Autonomen Systemen (AS) und ähnelt vom Grundprinzip dem Distance-Vector-Verfahren.
#
Es verwendet jedoch keine Kosteninformationen, sondern nur die Pfadinformationen, wobei die Pfade hier auf AS-Ebene und nicht auf Router-Ebene verwaltet werden (z.B. AS1 – AS100 – AS200 – AS888). Da es etwa 26.000 Autonome Systeme (AS) gibt, umfassen heutige Routing-Tabellen ungefähr 200.000 Einträge für die Routen zu allen erreichbaren Systemen.

Mittels Update-PDUs tauschen die Router Informationen über neue Router (Announcements) oder weggefallenen Routen (Withdrawls) aus. Anhand den eigenen Routing-Policies entscheidet ein Router, was mit der Information zu machen ist. Diese Policies können unterschiedliche Regelwerke, wie Sicherheitsaspekte, Kostenaspekte oder variable Sperren für bestimmte Absender oder Emfpfänger sein, die vom Administrator eines Routers verwaltet werden. Wenn eine Route eine Regel verletzt, kann sie bspw. auf „unendlich“ gesetzt werden.

BGP-Router speichern die beste Route zu einem anderen AS als vollständigen Pfad, wobei genau diese Informationen auch zwischen den Routern (Kommunikation erfolgt immer nur mit den direkten Nachbarn) ausgetauscht werden. Wenn ein Router innerhalb eines Pfads von einem anderen Router ist, wird diese Route nicht akzeptiert, um so das Count-to-Infinity Problem zu umgehen.

Ausfälle werden dahingehend erkannt, dass sich die Router über ein Hearbeat-Protokoll gegenseitig überwachen um Ausfälle schnell zu erkennen (Lebendüberwachung). Die Kommunikation erfolgt immer nur über die direkten Nachbarn. Zur Erhöhung der Sicherheit muss jedes AS mindestens einen Stellvertreter-BGP-Router haben Zur Einordnung des Protokolls: BGP wird als Protokoll zwischen AS-Grenzroutern (ASBR, siehe OSPF) verwendet.

BGP-PDUs

- Open-PDU nach dem Verbindungsaufbau zur Identifikation, Authentifizierung und dem Parameteraustausch (z.B. Timer für Zeitüberwachungen). BGP nutzt TCP als Transportprotokoll für den Nachrichtenaustausch (verbindungsorientiert).
- Update-PDU werden zum Advertisement der Routen-Informationen an die Nachbarn verwendet
- Keepalive-PDU werden zur Lebendüberwachung und der Bestätigung von Open-PDUs verwendet
- Notification-PDU werden für Fehlermeldungen oder zur Information verwendet, dass der sendende Router die Verbindung schließen möchte.

38. Nennen Sie drei Ziele der IPv6-Entwicklung!

Das Hauptziel war es, die Adressproblematik langfristig zu lösen (Zukunftsszenario: bald hat jeder Fernsehr einen Internet-Anschluss und es gibt viele mobile Internetgeräte).

Weitere Ziele waren:

- Vereinfachung des Protokolls zur schnelleren Bearbeitung in Routern
- Verringerung der Routing-Tabellen
- Spezielle Unterstützung für Anwendungstypen wie Echtzeitanwendungen
- Höhere Sicherheit (Verschlüsselung, Authentifikation)
- Flussmarken sollen unterstützt werden
- Multicasts sollen besser unterstützt werden
- Mobile Hosts mit spezieller Unterstützung sollen ihr Heimantnetz verlassen können
- Weiterentwicklung des Protokolls soll vereinfacht werden

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

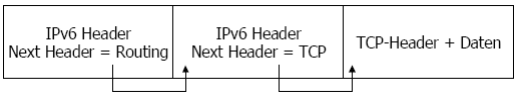
Der IPv6-Header besteht aus folgenden Feldern:

- Version: Versionsnummer des Internet-Protokolls
- Priorität: Information für Router, der Interessant bei Überlastsituationen ist
- Flussmarke: Identifikation des Flusses, wird vom Quellknoten eingetragen. Ein Fluss wird mit Zieladresse + Flussmarke identifiziert und dient dem Aufbau von Pseudoverbindungen mit definierten QS-Merkmalen (wie Verzögerung und Bandbreite). Ziel: Kombination von virtuellen Verbindungen mit der Flexibilität von Datagramm-Netzen
- Payload-Length: Nutzdatenlänge ohne die 40 Byte des IPv6-Header
- Next-Header: Verweis auf einen Erweiterungsheader – der letzte Erweiterungsheader muss auf die den Protokolltyp der höherliegenden Schicht verweisen (wie beim Feld Protocol des IPv4-Headers, verweist z.B. auf den Protokolltyp FTP)
- Hop-Limit: Lebenszeit des Paketes (gemessen in TTL)
- Source- und Destination Adresse

Der Erweiterungsheader dient der Übermittlung von weiteren Informationen an das Endsystem und sie werden von den Routern nicht bearbeitet. Eine Ausnahme hierzu ist der Routing-Erweiterungsheader, der auch von den Routern bearbeitet wird. Jeder Erweiterungsheader darf nur ein Mal vorkommen und die Reihenfolge in einem IP-Paket ist genau festgelegt:

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 verschlüsselten Inhalt
Optionen für Ziele	Zusätzliche Informationen für das Ziel

Beispiel für die Kette eines Erweiterungsheader



Beispiel: Routing-Erweiterungsheader
Dient dem Quellhost zur Festlegung des Weges als Vorabdefinition bis zum Ziel. Es kann strikt, als auch lose sein, d.h. es kann ein voller Pfad definiert werden oder nur ausgewählte Router zugelassen werden

- Next-Header: Verweis auf den nächsten Erweiterungsheader
- Anzahl Adressen: Anzahl der folgenden IP-Adressen die besucht werden müssen
- Next Address: Index innerhalb der folgenden IP-Adressliste auf die nächste zu besuchende Adresse
- Bitmuster: Bitmap, in der für jede IP-Adresse ein Bit vorhanden ist. Bei einer Bitfolge mit Werten für 1 müssen die korrenspondierenden Adressen unmittelbar aufeinander besucht werden, ansonsten können andere Router dazwischen sein
- Addresslsiste: Bis zu 24 IP-Adressen, die durchlaufen werden müssen

Beispiel: Fragmentierungs-Erweiterungsheader
Wird verwendet, um Dateneinheiten zu senden, die größer als die MTU des Pfades ist. Das MTU-Minimum ist wie bei IPv4 ebenfalls 576 Bytes. Die Maximalgrenze ist noch nicht definiert.

- Next Header: Verweis auf nächsten Erweiterungsheader
- Fragment Offset: Position der Nutzdaten relativ zum Beginn der Ursprungs-Dateneinheit
- Identifikation: Identifikation der PDU
- M (More-Flag): M=1 bedeutet, dass weitere Pakete folgen

40. Wozu sollen im IPv6-Protokoll Flussmarken dienen?

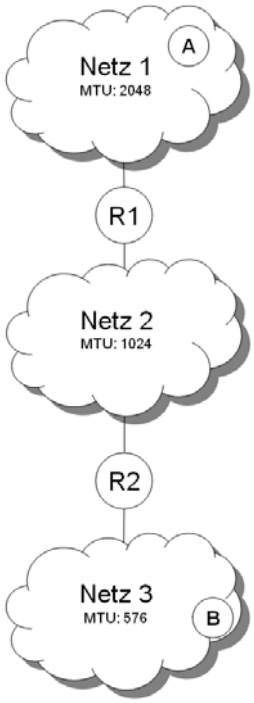
Siehe Aufgabe 39.

Sie dienen der Identifikation des Flusses im IPv6-Header und werden vom Quellknoten eingetragen. Ein Fluss wird mit Zieladresse + Flussmarke identifiziert und dient dem Aufbau von Pseudoverbindungen mit definierten QS-Merkmalen (wie Verzögerung und Bandbreite).
Ziel: Kombination von virtuellen Verbindungen mit der Flexibilität von Datagramm-Netzen

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 Pakets (minimaler IP-Header ohne Optionen). Es gelten folgende Bedingungen:

a. **Das IP-Paket muss von A nach B drei IP-Netze durchlaufen, Host A liegt im Netz 1, Netz 2 ist ein Transitnetz und Host B liegt in Netz 3**
b. **Netz 1 und Netz 2 werden durch Router R1 verbunden**
c. **Netz 2 und Netz 3 werden durch Router R2 verbunden**
d. **Netz 1 hat eine MTU von 2048 Byte**
e. **Netz 2 hat eine MTU von 1024 Byte**
f. **Netz 3 hat eine MTU von 576 Byte**

Skizze:



Skizzieren Sie die gesamte Netzwerktopologie!

Datagram	Netz 1	Netz 2	Netz 3
5000	2048	1024	576
			468
		1024	576
			468
		40	40
	2048	1024	576
			468
		1024	576
			468
		40	40
	944	944	576
			388

Wie viele IP-Fragmente verlassen R1 für das besagte IP-Paket in Richtung Netzwerk mit der Nummer 2?

Wie viele IP-Fragmente verlassen R2 für das besagte IP-Paket in Richtung Netzwerk mit der Nummer 3?

- Innerhalb von Netz 1 werden 3 Pakete übertragen.
- Netz 1 sendet an Netz 2 7 Pakete
- Netz 2 sendet an Netz 3 12 Pakete.

In welchem System (Host oder Router) werden die IP-Fragmente wieder zusammengebaut?

Die Fragmente werden erst wieder auf der Zielstation zu einem Datagramm zusammengesetzt. Hierzu werden alle Pakete gepuffert und wenn alle angekommen sind, zusammengesetzt und an die Transportschicht weitergeleitet.

Alle anderen (Zwischen-)Stationen leiten die eingehenden Fragmente nur weiter ohne sich über den Gesamtzusammenhang Gedanken zu machen.

Wie wird in diesem System erkannt, welche IP-Fragmente zum ursprünglichen IP-Paket gehören?

Im IP-Header gibt es ein Feld „Identifikation“. Alle IP-Fragmente eines Datagramms erhalten hier den gleichen Wert, der in allen Fragmenten enthalten ist.

Generell: Siehe Aufgabe 35

42. Eine Organisation hat von seinem ISP den IPv4-Adressblock 131.42.0.0/16 (classless) zugewiesen bekommen. Die Organisation möchte gerne ihr Netzwerk intern wie folgt aufteilen:

- **a. 1 Subnetz mit bis zu 32.000 Rechnern**
- **b. 15 Subnetz mit bis zu 2.000 Rechnern**
- **c. 8 Subnetze mit bis zu 250 Rechnern**

Der Adressblock wird zunächst mal in die zwei Adressblöcke 131.42.0.0./17 und 131.42.128.0/17 aufgeteilt.

Zeigen Sie auf, wie die Organisation intern die Adressen weiter aufteilen könnte, um obiges Ziel zu erreichen.

Hinweis: Alle beteiligten Router beherrschen CIDR.

Adressbereich		Binäre Netzwerkadresse	von Adresse	bis Adresse	Adressen
131.42.0.0	/17	**11111111.11111111.1**0000000.00000000	131.42.0.0	131.42.127.255	32768
~~131.42.128.0~~	~~/17~~	~~**11111111.11111111.1**0000000.00000000~~	~~131.42.128.0~~	~~131.42.255.255~~	~~32768~~
131.42.128.0	/21	**11111111.11111111.11111**000.00000000	131.42.128.0	131.42.135.255	2048
131.42.136.0	/21	**11111111.11111111.11111**000.00000000	131.42.136.0	131.42.143.255	2048
131.42.144.0	/21	**11111111.11111111.11111**000.00000000	131.42.144.0	…	2048
131.42.152.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.160.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.168.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.176.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.184.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.192.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.200.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.208.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.216.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.224.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.232.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
131.42.240.0	/21	**11111111.11111111.11111**000.00000000	…	…	2048
~~131.42.248.0~~	~~/21~~	~~**11111111.11111111.11111**000.00000000~~	~~131.42.248.0~~	~~131.42.255.255~~	~~2048~~
131.42.248.0	/24	**11111111.11111111.11111111.**00000000	131.42.248.0	131.42.248.255	256
131.42.249.0	/24	**11111111.11111111.11111111.**00000000	131.42.249.0	131.42.249.255	256
131.42.250.0	/24	**11111111.11111111.11111111.**00000000	…	…	256
131.42.251.0	/24	**11111111.11111111.11111111.**00000000	…	…	256
131.42.252.0	/24	**11111111.11111111.11111111.**00000000	…	…	256
131.42.253.0	/24	**11111111.11111111.11111111.**00000000	…	…	256
131.42.254.0	/24	**11111111.11111111.11111111.**00000000	…	…	256
131.42.255.0	/24	**11111111.11111111.11111111.**00000000	…	…	256

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

Der Router initiiert eine Fragmentierung und zerlegt das Fragment in kleinere Fragmente, sofern dies anhand dem Flag DF im IP-Header erlaubt ist. Wenn das Flag DF auf 1 steht, ist eine Fragmentierung nicht erlaubt. Falls die Fragmentierung jedoch erlaubt ist, läuft ein Prozess ab, der in Aufgabe 35 beschrieben ist.

Siehe auch: Aufgabe 35

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

Die Fragmente werden erst wieder auf der Zielstation zu einem Datagramm zusammengesetzt. Hierzu werden alle Pakete gepuffert und wenn alle angekommen sind, zusammengesetzt und an die Transportschicht weitergeleitet.
Alle anderen (Zwischen-)Stationen leiten die eingehenden Fragmente nur weiter ohne sich über den Gesamtzusammenhang Gedanken zu machen.

Siehe auch: Aufgabe 35

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

Damit ist ein Host gemeint, der mehr als eine Verbindung zu einem Netzwerk hat. Der Host kann auf allen Verbindungen Daten senden und empfangen, routet aber keine Daten für andere Rechner.

Multihoming-Varianten: siehe http://en.wikipedia.org/wiki/Multihoming

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

/16	11111111.11111111.00000000.00000000	255.255.0.0
/20	11111111.11111111.11110000.00000000	255.255.240.0
/24	11111111.11111111.11111111.00000000	255.255.255.0

47. Aus dem Adressbereich 11.1.253/24 eines VLSM-Teilnetzes sollen /27-Teilnetze herausgeschnitten werden. Wie lauten die Teilnetzwerkadressen? Wie viele Adressen bleiben pro /27-Teilnetz?

Netzadresse: 11.1.253.0 /27
Subnetzmaske (dezimal): 255.255.255.224
Subnetzmaske (binär): 11111111.11111111.11111111.**111**00000

Anzahl Subnetze (fixe Länge): $2^3 = 8$
Anzahl Hosts: $2^5 = 32$
Anzahl Hosts (nutzbar): $2^5 - 2 = 30$

Netzadresse	Subnetzmaske
11.1.253.0	11111111.11111111.11111111.**000**00000
11.1.253.32	11111111.11111111.11111111.**001**00000
11.1.253.64	11111111.11111111.11111111.**010**00000
11.1.253.96	11111111.11111111.11111111.**011**00000
11.1.253.128	11111111.11111111.11111111.**100**00000
11.1.253.160	11111111.11111111.11111111.**101**00000
11.1.253.192	11111111.11111111.11111111.**110**00000
11.1.253.224	11111111.11111111.11111111.**111**00000

48. Suchen Sie in der Registry eines Windows-Systems die möglichen einstellbaren TCP/IPParameter unter dem entsprechenden Registry-Path. Suchen Sie z.B. nach einem Eintrag mit dem Namen \System\CurrentControlSet\Services\Tcpip\Parameters unter HKEY-LOCAL_MACHINE. Führen Sie folgende Recherchen durch:

a. Wie hoch ist der TTL-Wert (Time To Live) eingestellt (siehe Parameter TTL) und was besagt er?

Wert: nicht gesetzt
Bedeutung: Siehe Aufgabe 33

b. Wie lange ist die maximale Lebensdauer eines Cache-Eintrags im ARP-Cache (Parameter ArpCacheLife) für benutzte und unbenutzte Einträge?

Wert: nicht gesetzt

49. Erläutern Sie, wie ein neu in ein Netzwerk hinzukommender OSPF-Router seine Routing-Information aufbaut und verwaltet. Gehen Sie dabei auf den Begriff des Spanning-Tree und auf die nachbarschaftliche Beziehung der OSPF-Router ein.

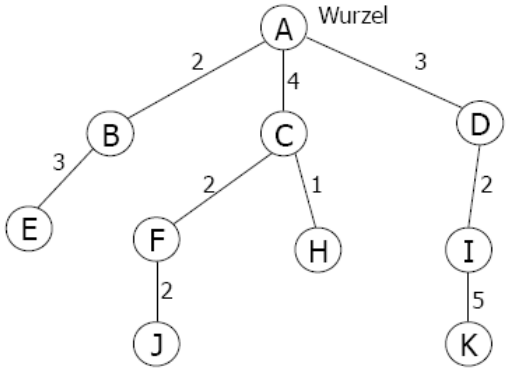
OSPF Einführung

RIP eignet sich aus obenstehenden Gründen eher für kleinere Netze, OSPF hingegen ist für größere Netze gedacht. OSPF ist ein offener Standard (Open SPF) für ein Link-State-Protokoll, dass zustandsorientiert ist. Der Link-State ist ein Zustand einer Verbindung zwischen zwei IP-Routern.

Grundsätzlich beinhaltet eine Link-State-Datenbank (Verbindungszustandsdatenbank) alle Routing-Informationen des Netzes, die Kommunikation für den Austausch von Routing-Informationen erfolgt jedoch nur mit den unmittelbaren Nachbarn (kleinere Netze) oder zwischen herkömmlichen Routern und designierten Nachbarn (bei größeren Netzen, siehe unten).

Jeder Router erzeigt aus seiner Sicht einen SPF-Baum (Shortest-Path-First), der auch als Spanning-Tree (überspannender Baum) genannt wird. Der eigene Router stellt hier die Wurzel dar und es werden in den Verzweigungen die günstigsten Routen zu allen bekannten Subnetzen und anderen Routern dargestellt.

Hierfür wird auf den Kanten (die gewissermaßen einen Subnetzübergang bzw. einen Link darstellen) eine Kosteninformation verwaltet, wie z.B. die Übertragungsrate oder Verzöerung.



Verwaltung der Routing-Informationen

Die Router teilen untereinander die Routing-Informationen aus, indem jeder Router mit seinen Nachbarn kommuniziert und alle Änderungen an die anderen Router verteilt werden. Der Austausch wird dabei über IP-Multicastadressen (jeder Router hört die Adresse ab) oder Punkt-zu-Punkt-Verbindungen ausgetauscht, und das funktioniert wie folgt:

Beim Start eines Routers sendet dieser seinen Nachbarn Hello-PDUs zu und bekommt auch wieder Hello-PDUs zurück. Anhand der Antworten wird entschieden, welcher Router ein Nachbar (Adjacent) wird, wobei die Nachbarn fortan Routing-Informationen in Form von Database-Description-PDUs austauschen.

Der eigene Router sendet seine eigenen Informationen in Form von Link-State-Adwertisements (LSA) an die Nachbarn (TTL = 1), die diese Informationen wieder jeweils an Ihre Nachbarn weiterleiten (usw..). Dieser Austausch erfolgt normal zyklisch etwa alle 30 Minuten.

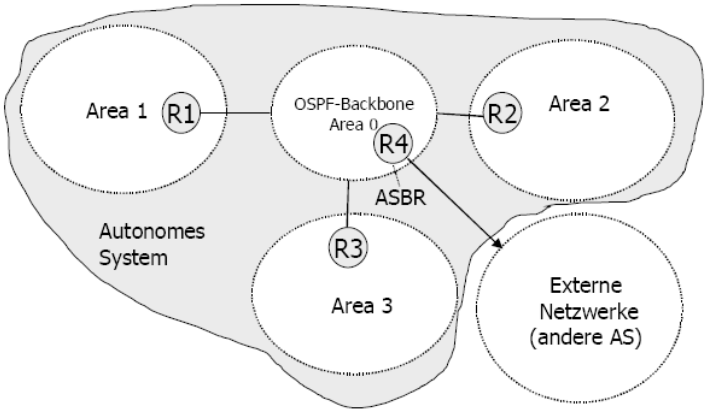
Ebenfalls wird eine Lebendüberwachung durchgeführt, da jeder Router seinen Nachbarn alle 40 Sekunden eine Hello-PDU sendet und diesen mitteilt, dass er noch aktiv ist. Wenn keine Hello-PDU kommt gilt der Router als ausgefallen und der Router, der das bemerkt hat, seindet eine Link-State-Update-PDU an alle anderen Nachbarn (unmittelbar nach bekannt werden, da das Protokoll eine recht hohe Konvergenz hat) und erhält dafür eine Link-State-ACK-PDU.

Unterstützung großer Netze (durch verschiedene Router-Klassen)

Damit die Berechnung der optimalen Routen nicht zu aufwändig wird, können (größere) Netze in mehrere autarke OSPF-Bereiche (Areas) eingeteilt werden. Areas haben eine eigene Area-ID, die ähnlich wie eine IP-Adresse in dottet decimal notiert wird (z.B. 0.0.3.1). Alle Areas müssen über ein OSPF-Backbone-Area miteinander verbunden sein, das die ID 0.0.0.0 besitzt (Area 0). Darüber hinaus hat jeder Router zur Identifikation seine eigene Router-ID.

Um dies zu ermöglichen wird zwischen vier Router-Klassen unterschieden:

- Interne Router sind innerhalb einer Area angesiedelt und führen nur Routing innerhalb einer Area (Bereich) durch. Alle Router in einer Area haben die gleiche Link-State-Datenbank und kennen nur Router aus ihrer Area.
- Area-Grenz-Router sind Router an den Bereichs(Area)-Grenzen, die zwei oder mehrere Areas miteinander verbinden.
- Backbone-Router befinden sich im Backbone und führen das Routing innerhalb der Backbones durch, sind selbst aber keine AS-Grenz-Router (in Grafik nicht eingezeichnet).
- AS-Grenz-Router (ASBR – Area Boundary Router) vermitteln zwischen mehreren Autonomen Systemen (AS), also kommunizieren mit externen Netzen und tauschen mit diesen Routing-Informationen aus. Daher kennen diee Router die LSA_Datenbanken der externen Areas, an denen er angebunden ist.



R1, R2, R3: Area Grenz Router

R4: ASBR

Backbone-Router und Interne Router: nicht dargestellt, sind in dem Backbone Area oder in den einzelnen Areas angesiedelt.

Eine solche Einteilung hat den Vorteil, dass die Größer der LSA-Datenbanken reduziert und die Routing-Tabellen verkleinert werden.

Designierte Router

Die Netzwerkbelastung in einem Netzwerk mit vielen Routern ist sehr groß, da n(n-1)-2 Nachbarschaften aufgebaut werden müssen. In Boradcast-Netzwerken (LAN) können daher ein Designierter Router und ein designierter Backup-Router zur Synchronisation der Routing-Informationen bestimmt werden.

Dieser ist für die Verteilung der Routing-Informationen zuständig und wird mit einer Priorität, die höher als bei herkömmlichen Routern ist, gekennzeichnet. Über diese Information kann dieser Router identifiziert werden und eine direkte kommunikation mit den anderen Routern ist daher nicht mehr erforderlich, da nur noch mit dem designierten Router oder seinem Stellvertreter kommuniziert wird.

Die Netzwerkbelastung wird dabei reduziert, da keine Broadcasts mehr verwendet werden und die Nachbarschaften auf n-1 reduziert werden.

OSPF-PDU-Typen

- Hello-PDU zur Feststellung von Nachbarn
- Database-Description-PDU zur Bekanntgabe der neusten Link-State-Datenbanken
- Link-State-Request-PDU zum Anfordern von aktuellen Routing-Informationen (gezielt(e) Updates)
- Link-State-Update-PDU zum Verteilen von Routing-Informationen (Updates)
- Link-State-ACK-PDU zum Bestätigen eines Updates

Sonstiges zu OSPF

OSPF müsste eigentlich zur Schicht 4 zugeordnet werden, da die PDUs im Gegensatz zu RIP direkt über IP gesendet werden. Die PDUs verfügen über einen Header und Nutzdaten. RIP nutzt zum Versenden der PDUs UDP, ist also der Anwendungsschicht zuzuordnen.

OSPF unterstützt Load-Balancing bei Pfaden mit gleichen Kosten, um die Pakete gleichmäßig zu verteilen. Für die Kommunikation werden Multicast-Adressen (über UDP) enutzt und es wird eine Authentifizierung unterstützt, um die Sicherheit vor Angriffen zu erhöhen.

Die Wegwahl erfolgt über einen Spanning-Tree für das gesamte Netzwerk, wobei die Wurzel der eigene Router ist und die Verzweigungen die günstigste Route darstellen.

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

In beiden Protokollen sind keine Schleifen (Count-to-Infinity-Problem) möglich, außerdem treffen beide Routingprotokolle Maßnahmen zur Verbesserung der Konvergenz.

RIP-2:

- Split-Horizon – es werden keine Routen an einen anderen Router propagiert, die er über diesen Router kennengelernt hat
- Split-Horizon mit Poison-Reverse – Routen, die ein Router über einen anderen Router kennengelernt hat, werden an diesen zwar propagiert, allerdings mit einer Metrik von 16 Hops (= unendlich). Damit ist dieser als nicht erreichbar markiert.
- Triggered Update – Routen-Aktualisierungen werden sofort weitergeleitet
- RIP-2 kommuniziert über Multicast (RIP-1 über Broadcast)
- RIP-1 unterstützt kein CIDR/VLSM, RIP-2 schon und ist vollständig abwärtskombatibel

OSPF:

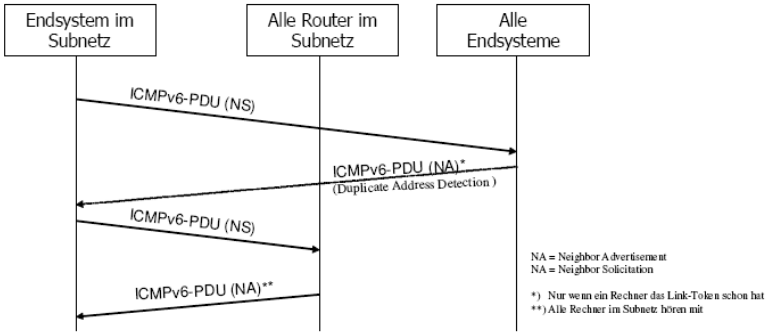
- Link-State-Verfahren – da ein Router alle Router im Netz kennt (allerdings nur mit den Nachbarn kommuniziert) fällt das Count-to-Infinity-Problem weg – jeder Router kennt die optimale Route zu allen anderen Routern
- Die Verteilung von Änderungen im Netz geschieht – nachdem sie erkannt worden ist, relativ schnell. Das Netz hat also eine relativ hohe Konvergenz.

51. Wie funktioniert bei IPv6 prinzipiell die automatische Adresskonfiguration?

Die Automatische Adresskonfiguration kann prinzipiell über zwei Varianten erfolgen: stateless und stateful autoconfiguration.

Stateless Autoconfiguration:

Bei dieser Variante suchen sich die Endsysteme automatisch ohne Unterstützung eines dedizierten DHCP-Servers ihre IP-Adressen. Es funktioniert nur innerhalb von einem IPv6-Subnetz. Als Protokoll wird ICMPv6 verwendet, die wiederum in IPv6-Pakete eingebettet sind. Da als Hop-Limit der Wert 255 (TTL) gesetzt ist, werden die Pakete von Routern nicht weitergeleitet.



Ablauf (Exkurs):

1) *Endystem sendet seine eigene Link-Adresse (MAC-Adresse) in einer ICMPv6-Navchricht über die Solicited-Multicast-Adresse FF02::1 (Neighbor-Solicitation). Damit werden alle Endsysteme und Router des Subnetzes angesprochen. (to solicit sth. – etwas erbitten)*
2) *Wenn ein Rechner im Subnetz die gesendete Subnetzadresse ebenfalls verwendet, sendet dieser eine Neighbor-Advertisement-Nachricht zurück und das Endsystem weiß, dass diese Adresse bereits verwendet wird. In diesem Fall müsste eine manuelle Konfliktauflösung erfolgen.*
3) *Wenn sich kein Rechner beschwert, wird in einem zweiten Schritt eine weitere Neighbor-Solicitation-Nachricht an die All-Routers-Multicast-Adresse versendet.*
4) *Mindestens ein Router antwortet nun an die Solicited-Multicast-Adresse mit einer Neighbor-Advertisement-Nachricht, in der das Präfix der IPv6-Adresse gesendet wird. Da diese Nachricht alle Rechner im Netz mithören, ist diese Adresse somit im Subnetz bekannt.*

Durch dieses Verfahren ist ein einfaches Renumbering der Adressen möglich, wenn die Vergabe der IP-Adressen zeitlich über eine Lease-Zeit begrenzt wird. Dennoch ist dieses Verfahren etwas risikoreicher als das Stateful-Verfahren, da ein Router auch ausfallen kann und dann kein Endsystem mehr in der Lage ist, im Subnetz zu kommunizieren (wenn es nur einen Router im Subnetz gibt).

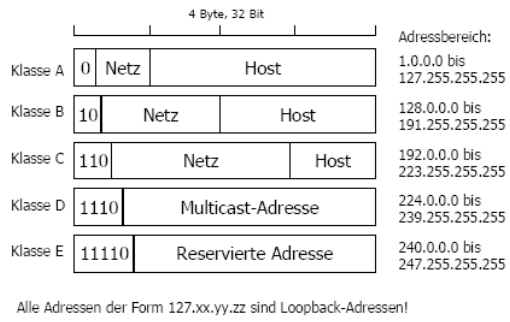
Stateful Autoconfiguration:

Diese zustandsbehaftete Autoconfiguration erfolgt über DHCPv6. Hierfür ist ein DHCP-Server erforderlich, der die Adressen und sonstigen Konfigurationsparameter verwaltet.

Wenn ein DHCP-Server nicht im selben Subnetz wie ein DHCP-Client ist, kann ein Router als DHCP-Relay (DHCP-Agent) fungieren. Dadurch wird es den Clients ermöglicht, indirekt mit einem DHCP-Server außerhalb des eigenen Subnetzes zu kommunizieren.

Ausführliche Beschreibung: Addressierung

Eine IP-Adresse (IPv4) besteht aus einem Tupel aus Netzwerknummer und Hostnummer, die 32 Bit lang sind. Damit gibt es 2^{32} mögliche Adressen.



Um unterschiedlich große Organisationen zu unterstützen gibt es mehrere Netzwerkklassen im Adressraum.

Die Klasse erkennt man den ersten Bits, wie in nebenstehender Abbildung dargestellt. Die Unterscheidung zwischen den Klassen liegt einfach nur an der unterschiedlichen Länge des Netzwerk- und Hostanteils.

Klasse	Anzahl Netze	Anzahl Hosts	Privater Bereich	Sonstig gesperrt
A (/8)	2^7 -2	2^{24} -2	10.x.x.x	0.0.0.0 (Standard Route) 127.0.0.0 (Loopback)
B (/16)	2^{14}	2^{16} -2	172.16.x.x	
C (/24)	2^{21}	2^8 -2	192.168.x.x	
D	reserviert für Multicast-Anwendungen			
E	derzeit noch nicht genutzt			

Gesperrte Hosts

In jedem Netz steht der erste Host (x.x.x.0) und der letzte (x.x.x.255) nicht zur Verfügung. Der erste ist die Netzwerkadresse, die zweite ist die Broadcastadresse eines jeden Netzes.

Private Adressen

Private Adressen werden von Routern gesondert behandelt, da diese Pakete nicht weitergeleitet werden und daher nie das lokale Netzwerk verlassen. Adressen in diesem Adressbereich können von jedem Netzwerk für interne Zwecke verwendet werden.

Klasse	Privater Bereich	Subnetz	
A (/8)	10.x.x.x	255.0.0.0 /8	/8
B (/16)	172.16.x.x	255.240.0.0 /12	/12
C (/24)	192.168.x.x	255.255.0.0 /16	/16

Verweis auf das eigene Netzwerk

Eine Adresse mit einem Netzwerkanteil aus lauter (binären) Einsen und einem beliebigen Hostanteil ermöglicht es Hosts, auf das eigene Netzwerk zu verweisen, ohne die Netzwerknummer zu kennen. Beispiel 255.255.255.x in einem Klasse C Netzwerk.

Direkter Broadcast

siehe Aufgabe 28

Ein direkter (gerichteter) Broadcast ermöglicht das Senden eines Broadcastes an ein beliebiges Netzwerk von einem Host as einem anderen Netzwerk. Dazu muss wie gewohnt die Netzwerknummer angegeben werden, wobei der Hostteil lauter Binäre einsen hat, also z.B. x.y.z.255.

Limitierter Broadcast

siehe Aufgabe 28

Ein begrenzter Broadcast bezieht sich auf das lokale Netz und wird von den Routern nicht durchgelassen. Die limited Broadcast Adresse ist die 255.255.255.255

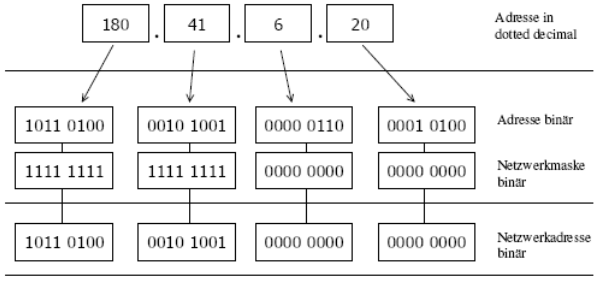
Die IP-Adresse 255.255.255.255 wird als Broadcast-Adresse verwendet. Bei einem Broadcast werden alle Hosts in einem Netzwerk angesprochen, d.h. alle Hosts nehmen Pakete mit der Zieladresse 255.255.255.255 entgegen.

Netzwerkmaske (Subnetmask)

siehe Aufgabe 23

Für die Router im Netz ist es wichtig zu wissen, wie die Netzwerkadresse des lokalen Netzes ist, damit er weiß, welche Geräte im eigenen Netzwerk und welche außerhalb zu finden sind. Dieser Zusammenhang ist besonders interessant, wenn Subnetze gebildet werden und nicht bekannt ist, wieviele Hosts oder Adressen ein Netz beinhaltet und wie die Netzadresse ist.

Als Lösung wird in den Routing-Tabellen eine weitere Information gespeichert, die Netzwerkmaske. Die Netzwerkadresse wird ermittelt, indem die Netzwerkmaske über die IP-Adresse gelegt wird und mit AND Verknüpft wird.



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

[1] gesetztes Bit: Netzwerkteil
[0] freies Bit: Hostteil

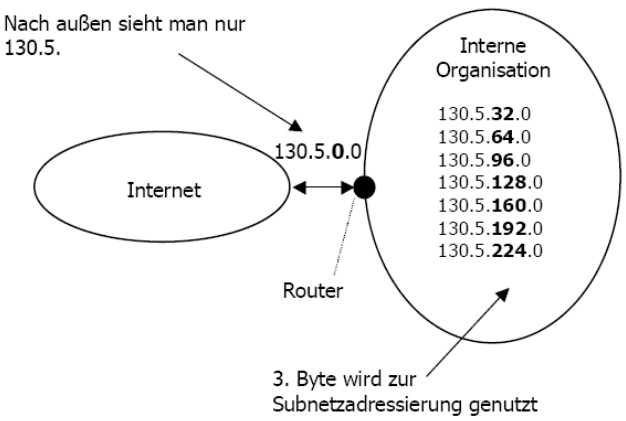
Klasse	Binäre Darstellung	Subnetz-Adresse	CIDR Notation
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Subnetze - Bestehende Probleme

Durch die Klasseneinteilung (insbesondere Klasse A-C) war die Adressaufteilung oftmals nicht optimal. Eine Organisation konnte nur einen Adressraum in festgelegter Höhe kaufen und das führte zu einer Verschwendung, wenn nicht alle Adressen davon benötigt worden sind.

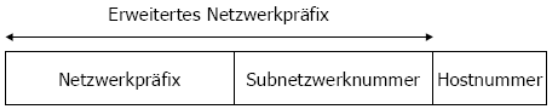
Wenn ein solches Netzwerk aufgeteilt werden sollte, so ging dies nur über die Beantragung einer zusätzlichen Netzwerknummer, die in den Routingtabellen der zentralen Backbones eingetragen werden mussten. Diese wurden daher immer größer.

Ein drittes Problem war die fehlende Möglichkeit der internen Strukturierung eines Netzwerkes innerhalb einer Organisation, die ein Netzwerk angemietet hat.



Subnetze (Fixed Length Subnet Mask)

Bei der Subnetzbildung wird der Hostanteil der bestehenden IP-Adresse (aus dem Netzwerkteil und dem Hostanteil) in zwei Teile aufgeteilt: der Subnetzwerknummer und der Hostnummer.



Die IP-Adresse wird nun mit einem (Netzwerknummer, Subnetzwerknummer, Hostnummer) dargestellt.

Die dadurch bildbaren Subnetze sind nur innerhalb einer Organisation sichtbar, außerhalb ist die Aufteilung nicht zu sehen und es gibt nur einen Routeneintrag für das Netzwerk.
Erst die internen Router berücksichtigen die Netzwerkmaske, um die Bits der Subnetzmaske zu identifizieren.

Im Gegensatz zu VLSM kann eine in einem Netzwerk eingestellte Adresse nicht mehr weiter unterteilt werden, d.h. jedes Netzwerk hat die gleiche Länge der vorher eingestellten Subnetzmaske.

Rechenbeispiel:
In einem Klasse C Netzwerk (192.168.7.0) sollen 4 Subnetze gebildet werden.

Wieviel Bit braucht die SNM?
$2^1 = 2$ <- zu wenig
$2^2 = 4$ <- 2 zusätzliche BIT

SNM: 11111111 11111111 11111111 **11**000000 = 255.255.255.192 = /26

Hostadressen pro Subnetz: $2^6 - 2 = 64 - 2 = 62$

Logisches Netz	Binäre Darstellung	Subnetz-Adresse
0	11000000 10101000 00000111 **00** | 000000	192.168.7.0
1	11000000 10101000 00000111 **01** | 000000	192.168.7.64
2	11000000 10101000 00000111 **10** | 000000	192.168.7.128
3	11000000 10101000 00000111 **11** | 000000	192.168.7.192

Variable Length Subnet Mask (VLSM) und Classless InterDomain Routing (CIDR)

Trotz der Einführung der Subnetze gab es weitere Probleme

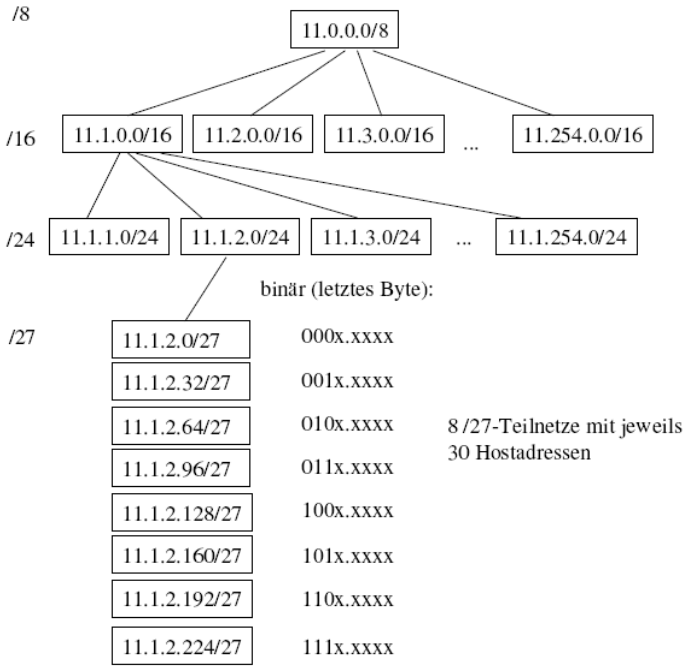
- Das Internet wuchs ständig weiter und verdoppelte sich mehrmals innerhalb kürzester Zeiträume.
- Die Netzwerknummern wurden in der Vergangenheit nicht sehr effizient verteilt und es zeichnete sich langsam eine gewisse Adressknappheit aus
- Aufgrund der Klasseneinteilung kann er gesamte Adressbereich kann nicht immer sinnvoll ausgenutzt werden

Als Lösung dieser Probleme zeichneten sich folgende Lösungsvorschläge ab siehe Aufgabe 31

- Mit VLSM konnten innerhalb einer Organisation Subnetze mit variabler Länge gebildet werden, d.h. bestehende Subnetze können weiter aufgeteilt werden
- Mit CIDR wurde das Konzept der Klasseneinteilung auch im Internet fallen gelassen (innerhalb einer Organisation wurde dies bereits durch Subnetting und VLSM umgangen). Damit wird die bedarfsgerechte Aufteilung des Adressraums im globalen Internet vereinfacht.
- NAT (Network Access Translation) schafft auch eine gewisse Erleichterung
- Das zukünftige IP-Protokoll (IPv6) unterstützt 128 Bit lange Adressen

Variable Length Subnet Mask (VLSM)

VLSM besagt, dass einem IP-Netzwerk mehr als eine Netzwerkmaske bzw. eine variable lange Teilnetzmaske zugewiesen werden kann. Dadurch können Organisationen den Adressraum noch effektiver nutzen.



Siehe Aufgaben 24, 46, 47

Netzwerkadresse und Netzmaske		**Dezimal**		**Beschreibung**
IP SNM	00001011 00000000 00000000 00000000 **11111111** 00000000 00000000 00000000	11.x.x.x	/8	Basisnetz

1) Klasse A Netzwerk **11.**x.x.x /8 wird unterteilt – **11.x.**x.x /16
   -> 254 Subnetze

Netzwerkadresse und Netzmaske		**Dezimal**		**Beschreibung**
IP SNM	00001011 00000001 00000000 00000000 **11111111 11111111** 00000000 00000000	11.1.x.x	/16	Netzwerkadresse #1
IP SNM	00001011 00000010 00000000 00000000 **11111111 11111111** 00000000 00000000	11.2.xx	/16	Netzwerkadresse #2
…	…	…	…	…

2) Subnetz **11.1.**x.x aus 1) wird weiter unterteilt -> **11.x.x.**x /24

-> 254 Subnetze für das Subnetz aus 1) bzw. alle möglichen Subnetze

Netzwerkadresse und Netzmaske		**Dezimal**		**Beschreibung**
IP SNM	00001011 00000001 00000001 00000000 **11111111 11111111 11111111** 00000000	11.1.1.x	/24	Netzwerkadresse #1
IP SNM	00001011 00000001 00000001 00000000 **11111111 11111111 11111111** 00000000	11.1.2.x	/24	Netzwerkadresse #2
…	…	…	…	…

3) Subnetze **11.1.2.**x /24 aus 2) wird weiter unterteilt -> **11.1.2.x** /27
   8 Subnetze für jedes Subnetz aus 2 möglich.
   Pro Subnetz können 32 Hosts adressiert werden, wobei nur 30 praktisch nutzbar sind

Netzwerkadresse und Netzmaske		**Dezimal**		**Beschreibung**
IP SNM	00001011 00000001 00000010 00000000 **11111111 11111111 11111111 000**00000	11.1.2.0	/27	Netzwerkadresse #1
IP SNM	00001011 00000001 00000010 00000000 **11111111 11111111 11111111 001**00000	11.1.2.32	/27	Netzwerkadresse #2
IP SNM	00001011 00000001 00000010 00000000 **11111111 11111111 11111111 010**00000	11.1.2.64	/27	Netzwerkadresse #3
…	…	…	…	…

Routing bei VLSM

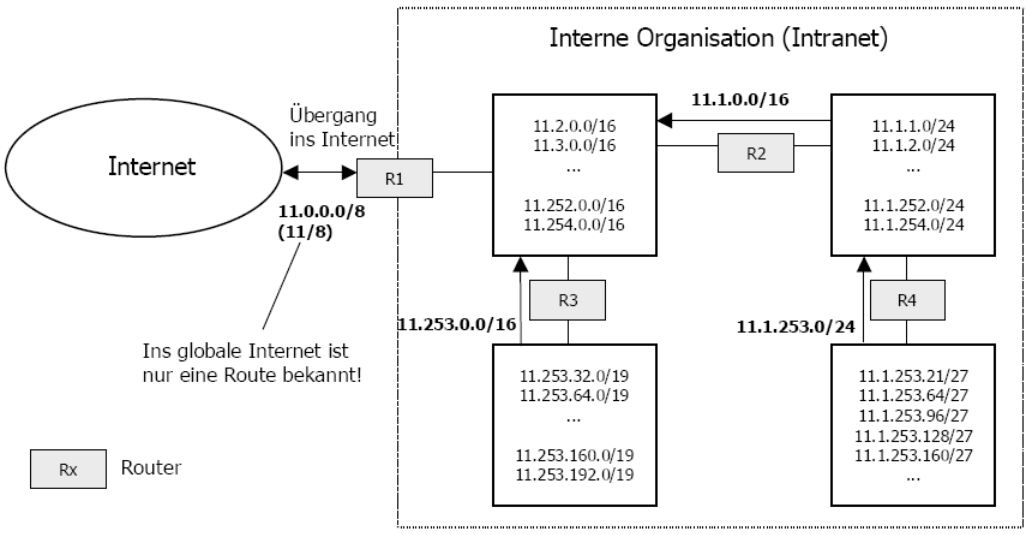
Um VLSM zu ermöglichen müssen die internen Router diese Funktion unterstützen. Hierzu muss ein geeignetes Protokoll verwendet werden, dass die Netzwerkmaske überträgt.

RIP-1 Protokoll

- eines der bekanntesten Protokolle
- unterstützt kein VLSM, da die Netzwerkmaske anhand der Klassenzugehörigkeit ermittelt werden

RIP-2 Protokoll und OSPF-Protokoll

- unterstützt VLSM



Obenstehende Abbildung zeigt, wie das Routing in oder aus dem Internet funktioniert.
Router R1 gibt nach außen nur die der Organisation zugewiesene Nummer 11.0.0.0/8 bekannt.
Intern fassen die verschiedenen Router verschiedene Teilnetze zusammen, d.h. wenn Pakete intern weitergeleitet werden, werden diese über mehrere Router weitergeleitet, die dann die genaue Aufteilung der Subnetze kennen. Die jeweils außenstehenden Router müssen die Subnetze nicht kennen.

Classless InterDomain Routing (CIDR)

CIDR funktioniert ähnlich wie CLSM, da die Netzwerknummern nicht nach Klassen sortiert sind, sondern flexibel bitweise einstellbar sind. Bei CIDR wird genauso wie bei VLSM die Präfix-Notation verwendet und unterstützt zudem noch die Routen-Aggregation, da die zu vergebenden Adressen geographisch sortiert sind und somit RoutingTabellen entlastet werden können.

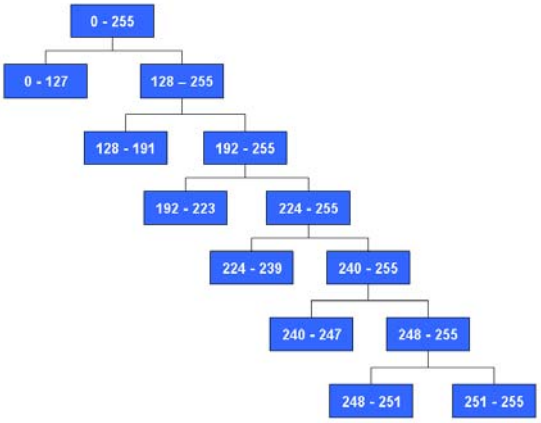
Die Serviceprovider können an ihre Kunden Adressbereiche mit variabler Länge vergeben und dadurch spart man Adressen ein bzw. es werden keine Adressen verschwendet.

Die Router müssen einen Weiterleitungsalgorithmus implementieren, der auf der längst möglichen Übereinstummung der Netzwerkmaske basiert.

Beispiel: Aufteilung des Netzes 180.41.214.0 / 24

siehe Aufgabe 42

Adressbereich		Binäre Netzwerkadresse	von Adresse	bis Adresse	Adressen
180.41.214.0	/25	**11000000.00101001.11100000.0**0000000	180.41.214.0	180.41.214.127	128
180.41.214.128	/26	**11000000.00101001.11100000.10**000000	180.41.214.128	180.41.214.191	64
180.41.214.192	/27	**11000000.00101001.11100000.110**00000	180.41.214.192	180.41.214.223	32
180.41.214.224	/28	**11000000.00101001.11100000.1110**0000	180.41.214.224	180.41.214.239	16
180.41.214.240	/29	**11000000.00101001.11100000.11110**000	180.41.214.240	180.41.214.247	8
180.41.214.248	/30	**11000000.00101001.11100000.11111**00	180.41.214.248	180.41.214.251	4
180.41.214.252	/30	**11000000.00101001.11100000. 11111**00	180.41.214.252	180.41.214.255	4



Zuerst wird das Netzwerk in zwei Subnetze mit je 128 Adressen (/25) aufgeteilt, wobei der erste Teil so gelassen wird und der zweite weiter untergliedert wird. Nun werden schrittweise immer mehr Bits zum Netzwerkpräfix hinzugefügt, so dass weitere Subnetze entstehen.

Aufteilung des Adressbereichs: siehe nebenstehende Abbildung.

Geographische Zonen

CIDR verbessert das globale Internet-Routing durch die Einführung von 8 gleich großen Adressblöcken (Areas) mit jeweils 131.072 Adressen. Anhand der Zoeöadresse erkennt ein Router, wo die Zieladresse liegt und dadurch wird die Wegwahl optimiert.

Europa	194.0.0.0	195.255.255.255
Nordamerika	198.0.0.0	199.255.255.255
Zentral- und Südamerika	200.0.0.0	201.255.255.255
Pazifik	202.0.0.0	203.255.255.255

31-Bit-Präfixes

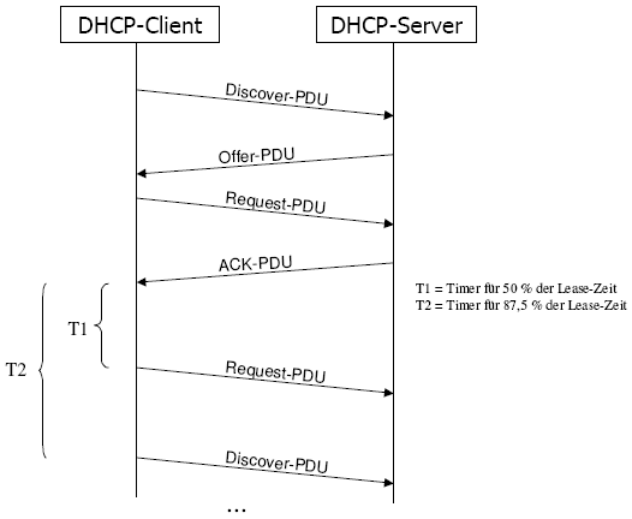
Bei VLSM/CIDR werden durch die Nichtausnutzung von /31 Subnetzen IP-Adressen verschenkt, da man bei einem Klasse-C-Netzwerk gegenüber der klassenweisen Adressvergabe IP-Adressen verschenkt.

Ursprünglich war die Nutzung eines /31 Subnetzes nicht zulässig, da hier nur zwei Hostadressen gebildet werden können. Diese konnten nicht verwendet werden, da sie alle aus binären einsen oder nullen bestehen und mit den Spezialadressen (wie Broadcast) in Konflikt stehen. Diese Einschränkung wurde nun aber beseitigt, als mögliche Anwendung sei bspw. die Verbindung zweier Router genannt.

Ausführliche Beschreibung: DHCP

Eine manuelle IP-Adressvergabe und Netzwerkkonfiguration ist bereits in kleinen Netzwerken problematisch, bei größeren Netzwerken geht dies nur noch durch Automatismen. Zu diesem Zweck wurde das Dynamic Host Configuration Protocoll (DHCP) entwickelt, das es ermöglicht, Hosts dynamisch eine IP-Adresse (und weitere Parameter) zu zuweisen.

Neben der IP-Adresse können Subnetzmaske, DNS-Server, Router und weitere Parameter (wie Web- und Mailserver) konfiguriert werden.

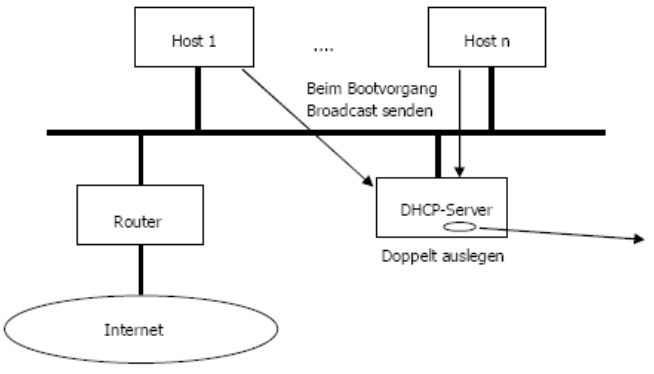


Ablauf:

- DHCP-Client sendet beim Bootvorgang eine Discover-PDU über einen Broadcast ins Netz
- DHCP-Server bietet dem Client eine Netzwerkkonfiguration per Offer-PDU an
- DHCP-Client kann annehmen und sendet hierfür eine Request-PDU an den nun bekannten DHCP-Server
- DHCP-Server bestätigt dies nochmals mittels einer ACK-PDU

Eine IP-Adresse kann entweder dauerhaft vollautomatisch auf unbestimmte Zeit vergeben oder der Client muss nach Ablauf einer vorgegebenen Zeit (Lease-Zeit) erneut nachfragen. In diesem Fall bekommt der Client für eine begrenzte Zeit eine dynamische Zuweisung einer Adresse aus einem Adresspool. Falls der Client die Adresse länger behalten möchte, so fragt er zum Zeitpunkt T1 zum ersten mal nach, ob er die Konfiguration noch länger behalten darf. Falls keine ACK-PDU kommt, fragt er zum Zeitpunkt T2 erneut an. Falls eine Antwort kommt, läuft die Lease-Zeit erneut an, ansonsten endet sie normal zum Ende der ersten Lease-Zeit.

Das Betriebssystem muss für diesen Mechanismus einige Vorkehrungen treffen um die Unterstützung zu gewährleisten und die Adressierung ist trickreich. Der DHCP-Server hat bei der ersten Antwort noch keine IP-Adresse und muss die Offer-PDU daher direkt an die MAC-Adresse senden. Später erfolgt die Kommunikation über UDP.



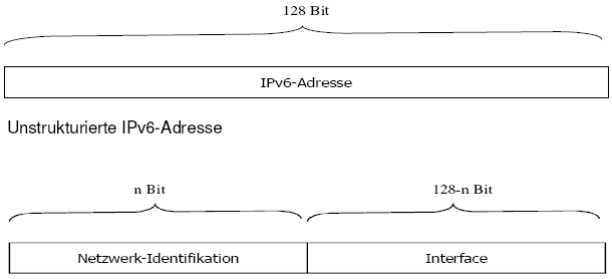
Konfigurationsdatei z.B.: /etc/dhcpd.conf

```
default-lease-time 600; # 10 Minuten                                   1
max-lease-time 7200; # 2 Stunden

option domain-name "dept101.com";
option domain-name-servers 192.168.1.1 192.168.1.2;                    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;                                  3
     range 192.168.1.100 192.168.1.200;
}

host mandl
     hardware ethernet 00:00:45:12:EE:E4;                              4
     fixed-address 192.168.1.21;
```

1) Konfiguration der Lease-Zeiten
2) Optionsangaben, die neben der Adresse an den DHCP-Client übertragen werden
3) IP-Adressbereiche, die von dem DHCP-Server verwaltet werden
4) Konfiguration eines statischen Hosts

Ausführliche Beschreibung: IPv6-Adressierung

In IPv6 kennzeichnet eine Adresse (wie in IPv4) nicht einen Host, sondern ein Interface, also den Netzwerkanschluss des Hosts. Für jedes Interface wird dabei eine IP-Adresse vergeben (Dual Homing).



IPv6 unterstützt 128 Bit Adressen (16 Byte) mit einer neuen Notation. Grob strukturiert lässt sich eine IPv6-Adresse in einen Netzwerk- und Interface-Teil aufteilen. In die Interface-ID wird oder kann dabei die MAC-Adresse der Netzwerkkarte (48 Bit) eingebaut werden.

Adresstypen:

Unicast-Adressen:
Traditioneller Adresstyp zum Adressieren eines Hosts oder Routers.

Multicast-Adressen:
Kennzeichnen eine Reihe von Endsystemen, also eine Gruppe von Interfaces, z.B. für die Gruppenkommunikation. Der Sender benötigt beim Multicast nur die gleiche Bandbreite wie beim Senden eines Paketes, die Vervielfältigung erfolgt am Router oder Switch. Der Unterschied zu einem Broadcast ist, dass Multicasts an eine definierte Empfängergruppe gehen, Broadcasts an alle Empfänger eines Subnetzes.

Anycast-Adressen:
Dient zur Zustellung eines Datagramms an einen bestimmten Host aus einer Gruppe von Netzwerkanschlüssen. Diese gehören zu verschiedenen Routern und Hosts. Welcher Host aus der Gruppe angesprochen wird, ist nicht bestimmt, meist antwortet jedoch der mit der kürzesten Route. Damit kann bspw. die Erreichbarkeit eines Dienstes erhöht werden.

Darstellung der Adressen:

Die 16 Byte werden in acht Gruppen zu je vier Hex-Zahlen (16 Bit), abgetrennt durch Doppelpunkte aufgeteilt (ein Hex-Buchstabe entspricht 4 Bit, da $2^4 = 16$).
Beispiel 1: Beliebige Adresse
8000:0000:0000:0000:0123:5555:89AB:CDEF

Beispiel 2: Führende Nullen können in jeder der 8 Gruppen weggelassen werden, außerdem darf ein mal in der gesamten Adresse Gruppen mit lauter 0en durch einen : ersetzt werden.
8A00:0000:0123:0005:89AB:CDEF:0000:0000 wird zu 8A00:0:123:5:89AB:CDEF::
„::65:78C1:9A:6008“ entspricht „0000:0000:0000:0000:0065:78C1:009A:6008

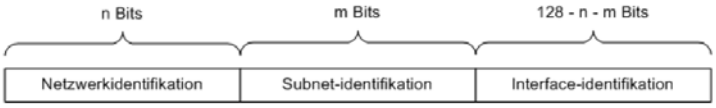
Beispiel 3: IPv4-Adressen können auf die neue Schreibweise abgebildet werden, wobei nur die letzten beiden Gruppen belegt sind und die ersten 6 Gruppen leer sind. Die Darstellung kann entweder dezimal oder hexadezimal erfolgen (dann werden zwei 10er Gruppen gemerged).
„::192.168.0.1 entspricht ::C0A8:1“

Beispiel 4: Darstellung einer IPv6-Adresse mit CIDR-Notation. Meist werden 64 Bit für die Netzidentifikation verwendet. Eine klassenweise Aufteilung gibt es nicht mehr.
„2001::0123:5555:89AB:CDEF/64“

Beispiel 5: Darstellung einer IPv6-Adresse als URL
„http://[2001::0123:5555:89AB:CDEF/64]:8080“

Adresssonderformen:

- IPv4-Adresse: ::FFFF /96 sind Mapping-Adressen von IPv4 auf IPv6
- ::0 /128 entspricht IPv4-Adresse 0.0.0.0 (undefinierte Adresse, bspw. beim Booten)
- ::1 / 128 entspricht der Loopback-Adresse 127.0.0.1 in IPv4 (z.B. ::FFFF:192.168.0.1)
- FF00::/8 weist auf eine Multicast-Adresse hin
- FF80::/10 weißt auf eine Link-Lokale Adresse hin



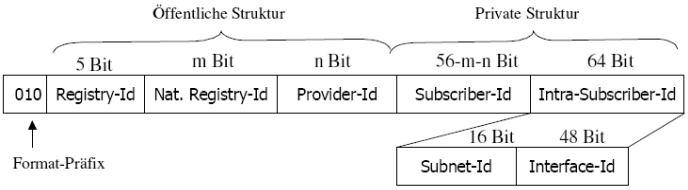
Spezielle Unicast-Adressen:

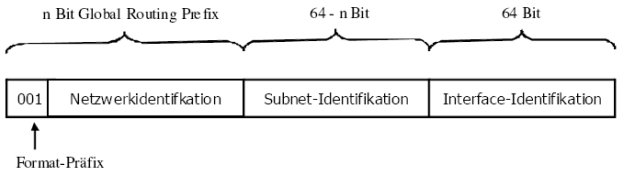
Globale Unicast-Adresse

Diese öffentlichen Adressen dienen zur Identifizierung eines global eindeutigen Hosts im Internet und haben den nebenstehenden Aufbau. Durch eine Provider-/Netbetreiberzuordnung ist eine Hierarchiebildung vorgesehen (weltweit hierarchisches Routing durch die öffentl. Adressbestandteile).

Exkurs: Untergliederung einer globalen Unicast-Adresse

Das Global Routing Prefix kann dazu verwendet werden, den Adressbereich einer Organisation (ISP, Unternehmen) zu identifizieren. Da die Netzwerkidentifikation und Subnetzidentifikation hierarchisch gegliedert werden kann, werden diese Informationen vom Router zur Routenoptimierung verwendet.





- *Registry-ID: internationale RegistrierungsID, wie ICANN, RIPE oder so*
- *Nat.Registriy-ID: identifikation einer nationalen Registrierungsorganisation (DENIC)*
- *Provider ID identifiziert den Anbieter eines Internet-Dienstes, wie ein ISP oder ein Unternehmen. Große Unternehmen erhalten eine kleine ID, damit mehr Bits für die anderen Bestandteile zur Verfügung stehen*
- *Subscriber-ID kennzeichnet einen privaten Netzbetreiber und kann mit der Netzwerk-Id in IPv4 verglichen werden*
- *Intra-Subscriber-ID dient der privaten Nutzung und kann nochmals zur Strukturierung eines privaten Netzes (in mehrere Subnetze) verwendet werden*

Exkurs: weitere Unicast-Adresstypen:

Link-lokale Adressen *(Subnetz lokal)*

Jede Link-Lokale Adresse besteht aus dem Präfix FE80::64/64 und dem 64 Bit langem Interface Identifier. Link-lokakle Adressen werden von jedem Host beim Systemstart erzeugt und auf das lokale Subnetz beschränkt. Sie werden für das Neighbor-Discovery benutzt und darf nicht weiter geroutet werden.

Site-lokale Adressen *(Präfix: FEBF) (Vgl. private IPv4-Adresse)*

Site-lokale Adressen ähneln den privaten IPv4-Adressen. Diese Adressen haben keine globale Gültigkeit und dürfen nicht in das globale Internet weitergeroutet werden. Im Gegensatz zu den Link-Lokalen Adressen werden diese Adressen aber innerhalb des internen Netzwerkes geroutet.

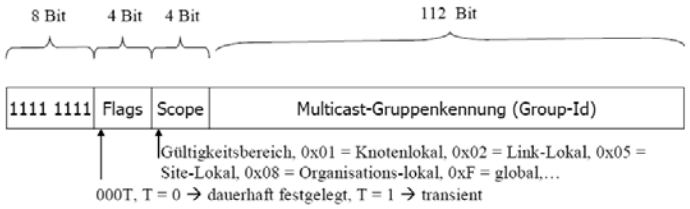
Lokale IPv6-Adressen *(Präfix: FEC0 … FEFF) (Unique-Local IPv6-Adresse)*

Eine lokale IPv6-Adresse ist im Gegensatz zu einer Site-lokalen Adresse auch global eindeutig. Dies hat den Vorteil, dass ein versehentliches Routing mit dieser Adresse in das globale Internet nicht zu einem Adresskonflikt führen kann. Für diesen Adresstyp wurde die sog. Global Identification eingeführt. Nach einem Präfix FC00::/8 folgt die 40 Bit lange global Identification und danach kommen die Subnet- und Interface-Identification. Die global Identification wird von einer Registrierungsstelle vergeben.

-> Global eindeutige lokale Adressen, die nicht zum Routen bestimmt sind, und zukünftig die Site-Lokalen Adressen ersetzen sollen (die zu Problemen geführt haben).

Multicast-Adressen

Multicast-Nachrichten werden z.B. für das Neighbor Discovery, DHCP und zur Routing-Unterstützung eingesetzt. Sie dürfen nicht als Absender-Adressen verwendet werden und sind folgendermaßen aufgebaut:



Beispieladressen:
FF01::1 – alle Multicast-Adressen im Knoten (Paket verlässt Knoten nicht)
FF01::2 – alle IP-Router des Knotens

Das Format-Präfix ist FF00/8 (bzw. 11111111), anschließend folgt ein Feld namens Flag, das einzeigt, ob es sich um eine temporäre oder well-known Multicast-Adresse handelt (im 4. Bit, die anderen drei Bits sind noch ungenutzt). Der Scope kennzeichnet den Gültigkeitsbereich, wie z.B. knoten-lokal, link-lokal, site-lokal, organisations-lokal oder global. In der Group-ID wird dann schließlich die Multicast-Gruppe identifiziert.

Sicherheitsmechanismen in IPv6

- Authentifizierung und Verschlüsselung sind bereits im Protokoll spezifiziert
- MD5-Algorithmen zur Authentifizierung der Partner
- Verschlüsselung der Nutzdaten mittels DES

Neighbor-Discovery

Das Neighbor-Discovery Protocoll (ND-Protokoll) dient zur Unterstützung der automatischen Konfiguration von Endsystemen. Links meinen Netzwerkanschlüsse und Link-Adressen meinen die Adresse des Netzwerkanschlusses. Das Protokoll ist sowohl für LANs als auch verbindungsorientierte Netze (wie ISDN, ATM) konzipiert. In einem Ethernet-LAN ist die Link-Adresse eine MAC-Adresse, in einem ISDN-Netzwerk die ISDN-Rufnummer.

Das Protokoll ermöglicht

- das Auffinden von Routern im gleichen Link (Subnetz) (Router Discovery)
- die dynamische Zuordnung von Konfigurationsparametern (MTU, Hop-Limit, …) (Parameter Discovery)
- die automatische IP-Adresskonfiguration zur Laufzeit (Neighbor Solicitation)
- die dynamische Adressaufkösung für Layer2-Adressen (wie heute im ARP-Protokoll)
- die optimale MTU muss gefunden und zur Laufzeit zwischen Sender und Empfänger optimiert werden (Path MTU Discovery)

Beispiel: Router Discovery (via ICMP)

Wenn ein Client einen Router sucht, sendet es eine Router-Solicitation-Nachricht über Multicast an die Adresse FF02::2. Damit werden alle Router angesprochen und diese Antworten mit einer Router-Advertisement-Nachricht. Somit kann der verantwortliche Router aufgefunden werden.

Beispiel: Parameter Discovery

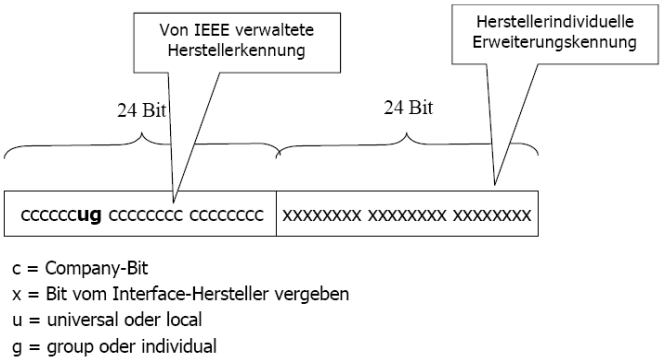
Ein Client kann zum Startzeitpunkt eine Router-Solicitation-Nachricht an die feste Multicast-Adresse FF02::2 senden, wobei die Router dann mit einer Router-Advertisement-Nachricht antworten.
Dabei können folgende Parameter übertragen werden: Max-Hop-Limit, Retransmission-Timer, die MTU-Size, ….

MAC-Adressen – IEEE 802.3

Die MAC-Adressen (Media Access Control) werden bei der Herstellung zugewiesen, sie sind global eindeutig und kennzeichnen

Aufbau:

- Firmenkennung (24 Bit)
- Platinenkennung / Erweiterungskennung (24 Bit)



Bestandteile:

u-Flag: universal (von IEEE oder lokal vom Netzwerkadministrator verwaltete Adresse)

g-Flag: Unicast- oder Multicast-Adresse

u = 0 und g = 0 bedeutet: Standard-Netzwerk-adapteradresse, also eine universell verwaltete MAC-Unicastadresse.

IEEE EUI-64 Adresse: Neuer Standard der MAC-Adressen, Erweiterungskennung ist nun 40 Bit. Die u und g-Flags und der Aufbau sind ansonsten identisch.

Exkurs: IPv6-Migration

Das Internet wird nicht Zug um Zug umgestellt, sondern es ist eine Koexistenz bei der Migration mit IPv4 erforderlich. Daher werden die Router so ausgelegt, dass sie beide Protokolle beherrschen (Dual-IP-Stack) – ein IPv4-Netzwerk muss in eine IPv6-Umgegunb integriert werden können und ein IPv6-Netz muss an ein IPv4-Netz angeschlossen werden können.

Neben dem IP-Protokoll müssen auch höherwertige Protokolle, wie DNS, TCP oder UDP angepasst werden, da beispielsweise die IP-Adressen zur Prüfsummenberechnung anders sind.

Exkurs: Anpassung wichtiger Protokolle an IPv6

Bei der Nutzung von IPv6 müssen auch einige Steuer- und Routingprotokolle angepasst werden.

RIPng (next Generation).Hier bleibt eigentlich alles gleich bis auf dass die Unterstützung der neuen Adresslänge. Fener wird anstatt der Subnetzmaske die Präfixlenge der Subnetzmaske gespeichert. Dadurch ist es möglich, dass RIPng in Netzwerken verwendet wird, in denen mehrere Präfixlengen verwendet werden.

OSPFng ist eine Anpassung von OSPF an IPv6, jedoch gibt es Prinzipiell keine großen Änderungen außer den notwendigen Anpassungen

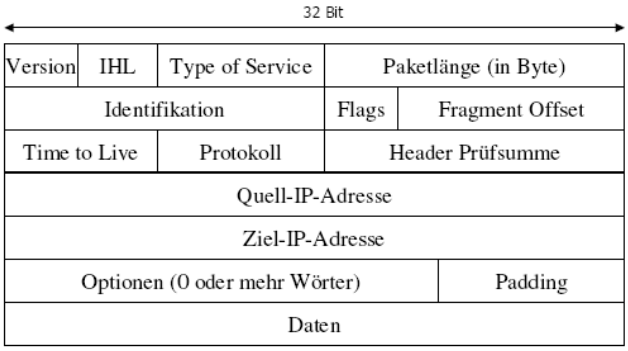
ICMPv6 ist die Anpassung an IPv6 mit einigen Zusatzfeatures, da beispielsweise die automatische Adresskonfiguration unterstützt wird. Außerdem wurden die ICMP-Typangaben neu organisiert und einige neuen Nachrichtentypen wurden hinzugefügt.

ARPv6 ist im Prinzip nicht mehr notwendig, da die MAC-Adressen in die Interface-Ids eingetragen sind und von daher statisch festgelegt werden können.

DHCPv6 wird für die statische Autokonfiguration verwendet und hat einige Erweiterungen erfahren (siehe Aufgabe 51).

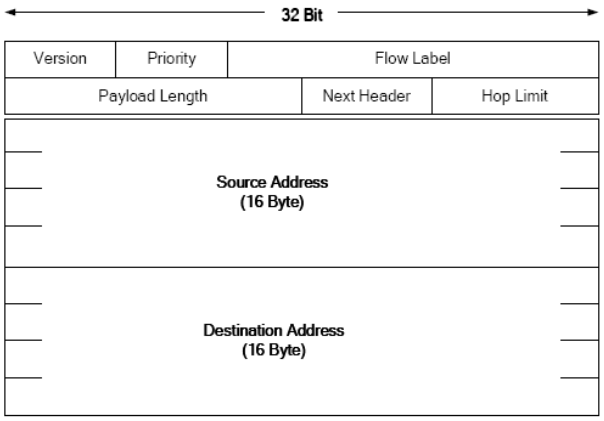
Header

IPv4-Header



- Version: IP-Version (4)
- IHL: Länge des IP-Headers (20 – 60 Byte), gemessen in 32-Bit Worten
- Type of Service (wie Priorität oder Servicetyp) – wird nicht benutzt
- Paketlänge (Gesamtlänge Datenpaket (Header + Nutzdaten)
- Identifikation: Alle Fragmente eines Datagrams erhalten hier die selbe ID
- Flags wie DF, MF (Disable Fragmentation, More Fragments)
- Fragment Offset zur Ermittlung der relativen Lage eines Fragments
- TTL – Paketlebensdauer
- Protocoll – definiert das darüberliegende Protokoll
- Header-Prüfszumme zur Fehlererkennung im Header
- Quell- IP und Ziel-IP zur Adressierung
- Optionen, wie loses oder striktes Routing mit oder ohne Pfadvorgaben (nicht benutzt)
- Padding – das Datagramm wird bei Bedarf zur nächsten 32 Bit mit Nullen aufgefüllt (durch dieses Feld)
- Daten: Nutzdaten der höheren Schicht

IPv6-Header

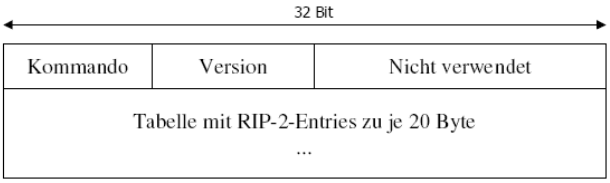


Der IPv6-Header besteht aus folgenden Feldern:

- Version: Versionsnummer des Internet-Protokolls
- Priorität: Information für Router, der Interessant bei Überlastsituationen ist (z.B. Kennzeichnung vom Verkehr mit hohem Durchsatz, oder geringer Verzögerung, oder Verkehrsarten ohne Staukontrolle, wie Videoanwendungen)
- Flussmarke: Identifikation des Flusses, wird vom Quellknoten eingetragen. Ein Fluss wird mit Zieladresse + Flussmarke identifiziert und dient dem Aufbau von Pseudoverbindungen mit definierten QS-Merkmalen (wie Verzögerung und Bandbreite). Ziel: Kombination von virtuellen Verbindungen mit der Flexibilität von Datagramm-Netzen
- Payload-Length: Nutzdatenlänge ohne die 40 Byte des IPv6-Header
- Next-Header: Verweis auf einen Erweiterungsheader – der letzte Erweiterungsheader muss auf die den Protokolltyp der höherliegenden Schicht verweisen (wie IPv4-Protocoll Headerteil, z.B. FTP)
- Hop-Limit: Lebenszeit des Paketes (gemessen in TTL)
- Source- und Destination Adresse

RIP-2

- Kommando: RIP-Request oder Response
- Version (des RIP-Protokolls)



- Adressierungsart: bei IP-Adressen immer den Wert 0x02
- Route Tag: dient zur Kennzeichnung der Herkunft, wie BGP-Router
- IPv4-Adresse der Route
- Subnetzmask: SNM der Adresse (CIDR, VLSM)

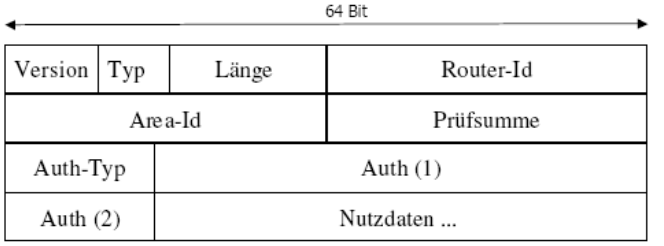
RIP-2-Entry:

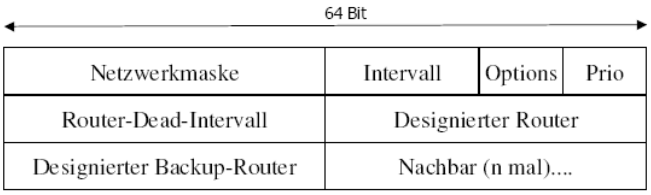
Address-Family-Identifier	Route-Tag
IPv4-Adresse	
Subnet-Mask	
Next-Hop	
Metrik	

- Metrik: Anzahl der Hops
- Next Hop: hiermit kann der Router eine direkte Route zu einem Host bekannt geben (Host-Route). Ankommende IP-Pakete an den Host werden direkt übertragen.

OSPF

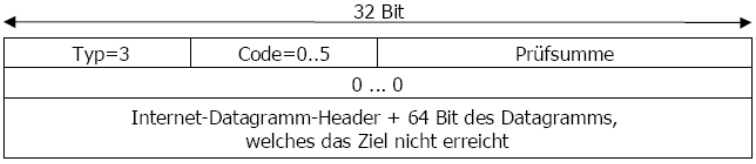
- Version: Wert 2
- Typ: Hello-PDU, …-PDU, …
- Länge: Gesamtlänge der PDU
- Router-ID
- Area-ID: Area, in der Paket erzeugt wurde
- Prüfsumme
- Auth-Typ: Art der Identifikation
- Auth (1) und Auth (2): Authentifizierungsdaten
- Nutzdaten





ICMP

- Typ der Nachricht
- Code
- Prüfsumme
- Daten: IP-Header + 64 Bit des ursprünglich übertragenen Datagramms



ARP

- Hardware-Typ: Adresstyp 1 = Ethernet
- Protokoll-Typ: Adresstyp des höherliegenden Protokolls (IP)
- HLEN: Länge der Hardware-Adresse
- PLEN: Länge der Schicht3-Adresse
- Restliche Felder: Adressdaten