Teil 1: Standardisierung

1.1 Weshalb gibt es Standardisierung? Aspekte der Standardisierung: Was soll/kann/muss standardisiert werden (Software, Hardware, Schnittstellen)? Vorteile und Nachteile? Was versteht man unter Innovation, inwieweit beeinflusst Standardisierung Innovation?

Standardisierung für Interoperabilität: standardisierte Interfaces, Fokus auf einfacher Bedienung, erhöht Anzahl der Kunden

Aspekte der Interoperabilität:

- Technisch: Hardware, Software, Vendor
- Geografisch: Operator, Land, Kontinent, Weltweit
- Rolle von Gateways: Technologien verbinden, Anzahl der (erreichbaren) User erhöhen

Metcalfe's Law: The value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2)

Innovation

- "... creation of better or more effective products, processes, technologies, or ideas that are accepted by markets, governments, and society …"
- "substantial positive change compared to incremental changes"
- Fehlende oder unzureichende Standardisierung gefährdet Innovation. Standardisierung hat aber geringen Einfluss auf Innovation.

1.2 Erklären Sie die Begriffe IETF Standards Track und Maturity Level und deren Notwendigkeit. Zählen Sie die entsprechenden Dokumente auf und beschreiben Sie deren Zweck (z.B. Beispiele für Einsatz).

IETF Standards Track RFC: RFCs die Internet Standards werden sollen
Maturity Levels:

- Proposed Standard
    - Einstiegsklasse der Maturity Klassifikation nach der RFC Anerkennung
    - sollen stabil und wohlverstanden sein
    - üblicherweise ist keine (Referenz-)Implementation vorhanden
    - Validierung durch Implementation
- Draft Standard
    - der nächste Abschnitt in der Entwicklung, es sind mindestens zwei unterschiedliche interoperable Implementationen von unterschiedlichen Code-Bases verfügbar
    - Operational Experience; wird wahrscheinlich ein Mature-Standard
- Internet Standard (Standard)
    - Rich Implementation und Operational Experience, Protokoll hat hohen Nutzen für Internet Community

Non(Off)-Standards Track RFC: RFCs, die noch nicht bereit sind für Standard Track oder nicht dafür vorgesehen sind
Maturity Levels:

- Experimental: als generelle Information der Internet Technical Community und zur Archivierung der Arbeit veröffentlicht
- Informational: als generelle Information der Internet Community veröffentlicht
- Historic: Spezifikation die durch neuere Spezifikation ersetzt wurde

1.3 Was versteht man unter einer 3GPP Release? Welche Komponenten hat eine 3GPP Dokumentennummer und wie ist sie strukturiert?

Release spezifiziert alle standardisierten Features, nicht auf IMS (IP Multimedia Subsystem) beschränkt
Es gibt Technical Specifications (TS, Standards) und Technical Reports (TR, "Best Practice").

3GPP Definition: "3GPP uses a system of parallel "releases" - to provide developers with a stable platform for implementation and to allow for the addition of new features required by the market."

3GPP Stages:
- abgeleitet von ITU-T
- Stage 1: Service Description von Service-User Standpunkt aus
- Stage 2: logische Analyse und Informationsfluss auf functional Element Level
- Stage 3: konkrete Implementierung von Protokollen

3GPP Dokumente sind spezifisch für ein bestimmtes 3GPP Release, innerhalb der gleichen Serie kann mehrmals die gleiche Nummerierung auftreten. Release wird üblicherweise in den Filenamen kodiert.

Nummerierungsschema: TS xx.yyy a.b.c
- xx: Seriennummer
- yyy: Spezifikation innerhalb der Serie
- a: 3GPP Release Nummer
- b: Major Version
- c: Minor Version
- z.B. TS 22.228 5.6.0
    - Dokument TS 22.228 für 3GPP Release 5, Version 6.0
    - Filename: 22228-560.zip

1.4 IETF: Beschreiben Sie die Aktivitäten der Standardisierungsorganisation im Detail: (a) Wofür steht die Abkürzung? (b) Schwerpunkt der Standardisierungs Aktivitäten? (c) Wer kann sich bei der Standardisierung beteiligen, wer kann Standards vorschlagen, Voraussetzungen um mitzuwirken? (d) Wie heißen die Standards und verwandten Dokumente ? (e) Beschreiben Sie den Standardisierungsprozess. (f) Was geschieht, wenn man einen Fehler in einem Standard dieser Organisation entdeckt? (g) Welche Versionierungsmechanismen gibt es?

(a) IETF: Internet Engineering Task Force

(b) treibende Kraft bei der Entwicklung von Internet Standards

(c) jeder kann einen RFC vorschlagen (wird zuerst Internet Draft)

(d)

- IETF Standards: RFC (Request for Comments), alle RFCs sind frei verfügbar, in Plain Text gehalten für Plattformunabhängigkeit
- IETF Drafts: Pre-RFC Stage, Internet Drafts
- RFC Classification: Standards-track RFC, Non-standards-track RFC, BCP (best current practice) RFC

(e)
Jeder kann einen RFC vorschlagen, indem er einen Internet Draft (ID) vorbereitet, dieser ID ist begrenzte Zeit (6 Monate) gültig, mit Unterstützung der Community kann der ID verfeinert und schließlich zum RFC werden, ID muss ebenfalls bestimmten Prozessen folgen, Drafts werden nicht archiviert, abgelaufene Drafts verschwinden, Drafts sollen nie referenziert werden

1. Konzepte, Ideen
2. Leute kontaktieren die geeignete IETF Arbeitsgruppe
3. jemand bereitet einen Internet Draft entsprechend den ID Anforderungen vor
4. ID wird veröffentlicht: Kommentare von Arbeitsgruppen-Mitgliedern und anderen Mitgliedern
5. bei Einigkeit und IESG (Internet Engineering Steering Group) Zustimmung wird RFC Editor für Publikation kontaktiert -> RFC
6. bei neuem Input oder Aufforderungen zu Änderungen zurück zu Punkt 3
7. Draft läuft ab

(f) entweder Errata (bekannte Fehler sind in Errata verzeichnet) oder neuer RFC

(g) ein RFC ändert sich nie, IETF hat keine Versionierungsmechanismen
Pro: RFC Nummer ist also eindeutig
Contra: dem Standardisierungspfad ist schwerer zu folgen

1.5 ITU: Beschreiben Sie die Aktivitäten der Standardisierungsorganisation im Detail: (a) Wofür steht die Abkürzung? (b) Schwerpunkt der Standardisierungs Aktivitäten? (c) Wer kann sich bei der Standardisierung beteiligen, wer kann Standards vorschlagen, Voraussetzungen um mitzuwirken? (d) Wie heißen die Standards und verwandten Dokumente ? (e) Beschreiben Sie den Standardisierungsprozess. (f) Was geschieht, wenn man einen Fehler in einem Standard dieser Organisation entdeckt? (g) Welche Versionierungsmechanismen gibt es?

(a) ITU: International Telecommunication Union

(b) Weltweit gültige Standards im Bereich der Telekommunikation: Telefon, Festnetze, ... (internationale Regelungen für die Nutzung von Frequenzen, Registrierung von Sende- und Empfangsfrequenzen)
ITU-T (Telecommunication), ITU-D (Development), ITU-R (Radiocommunication)

(c)
ITU-Mitglieder und Staaten, Jahresbeitrag notwendig

(d)
ITU Recommendations, X.yyy, X je nach Bereich, z.B. H.323, H für Audiovisual an Multimedia Systems, ITU Recommendations sind seit 2007 frei verfügbar
ITU Drafts

(e)

1. ITU Drafts werden innerhalb der SGs (Study Groups) bzw. WPs (Working Parties) ausgearbeitet und diskutiert
2. Review bei Meeting, wenn sie als ausgereift erachtet sind
3. bei Zustimmung wird ein Draft zur Genehmigung eingereicht, Final Review
4. wenn keine Mitglieder Einwände haben, wird der Draft genehmigt und wird zur Recommendation

(f) Versionierung

(g)

- es gibt Versionierungsmechanismen, keine bestimmte Versionsnummer, referenziert durch Approval Datum (mm/yy), z.B. H.323 (12/09), ältere Versionen werden ersetzt: H.323 (11/96), H.323 (02/98), …, H.323 (06/06)
- verschiedene Versionen des Standards können auf unterschiedliche Protokoll-Versionen zeigen (z.B. H.323 V1, H.323 V2, …)

1.6 ETSI: Beschreiben Sie die Aktivitäten der Standardisierungsorganisation im Detail: (a) Wofür steht die Abkürzung? (b) Schwerpunkt der Standardisierungs Aktivitäten? (c) Wer kann sich bei der Standardisierung beteiligen, wer kann Standards vorschlagen, Voraussetzungen um mitzuwirken? (d) Wie heißen die Standards und verwandten Dokumente ? (e) Beschreiben Sie den Standardisierungsprozess. (f) Was geschieht, wenn man einen Fehler in einem Standard dieser Organisation entdeckt? (g) Welche Versionierungsmechanismen gibt es?

(a) European Telecommunications Standards Institute

(b) Koordination und Produktion von europäischen Standards, um einen homogenen europäischen Telekommunikationssektor zu ermöglichen
zusätzlich sollen weltweit anwendbare Standards für Informations- & Kommunikationstechnologien entstehen (GSM, UMTS wurden erreicht)

(c) ETSI-Mitglieder, darunter sind Netzbetreiber, Diensteanbieter, Verwaltungen, Anwender und Hersteller

(d) Standards sind frei verfügbar von Homepage, bis vor kurzem nur für Mitglieder

ETSI Document Categories:

- ETSI Technical Specifications (ES): Standard Document
- ETSI Technical Guide (EG)
- ETSI Special Report (SR): informatives Dokument (best practice)
- ETSI Group Specifications (GS)

(e) ETSI Struktur:

- General Assembly: höchste Autorität
- Board: Vollzugsarm der General Assembly
- Technical Bodies: technische und spezielle Komitees, Projekte, Partnerprojekte
- Sekretariat

(f) Versionierung

(g) Number-based Versionierung (Major/minor Release)
z.B.:
ES 282 001 V2.0.0 (2008-03)
ES 282 001 V1.1.1 (2005-09)

1.7 3GPP: Beschreiben Sie die Aktivitäten der Standardisierungsorganisation im Detail: (a) Wofür steht die Abkürzung? (b) Schwerpunkt der Standardisierungs Aktivitäten? (c) Wer kann sich bei der Standardisierung beteiligen, wer kann Standards vorschlagen, Voraussetzungen um mitzuwirken? (d) Wie heißen die Standards und verwandten Dokumente ? (e) Beschreiben Sie den Standardisierungsprozess. (f) Was geschieht, wenn man einen Fehler in einem Standard dieser Organisation entdeckt? (g) Welche Versionierungsmechanismen gibt es?

(a) 3rd Generation Partnership Project

(b)
- weltweit anwendbare Standards für ein 3rd Generation Mobile System (UMTS, HSPA)
- Wartung und Entwicklung von GSM (Global System for Mobile Communication) Standards (inklusive Funk-Technologien wie GPRS, EDGE)
- verantwortlich für IMS (IP Multimedia Subsystem)
- standardisiert EPS (Evolved Packet System), besser bekannt als LTE (Long Term Evolution), Nachfolger von UMTS

(c) 3GPP Members sind: ETSI (Europa), ARIB (Japan), CCSA (China), ATIS (US), TTA (Korea), TTC (Japan)
aktive Unternehmen und Hersteller können mitwirken

(d) die Standards heißen Technical Specifications (TS), Technical Reports (TR), “Best Practice”

(e) 3GPP Stages:
- Stage 1: Service-Beschreibung aus der Sicht des Service-Users
- Stage 2: logische Analyse und Informationsfluss auf functional Element Level
- Stage 3: konkrete Implementierung von Protokollen zwischen physikalischen Elementen auf die die functional Elements gemapped wurden

(f) Versionierung

(g) TS xx.yyy a.b.c
xx … Seriennummer
yyy … Spezifikation innerhalb einer Serie
a … 3GPP Release Nummer (1=inform, 2=for approval)
b … Major Version (bei umfangreichen Änderungen erhöht)

c … Minor Version (bei redaktionellen Änderungen (editorial changes) erhöht)

z.B.
TS 22.228 5.6.0
Dokument TS 22.228 für 3GPP Release 5, Version 6.0
Dateiname 22228-560.zip

TS 22.228 6.10.0
Dokument TS 22.228 für 3GPP Release 6, Version 10.0
Dateiname 22228-6a0.zip

Teil 2: Vermittlungstechnologien

2.1 Gesetz von Metcalf: Wie lautet der Satz, welche Auswirkung hat er in Theorie und Praxis auf den Aufbau von Kommunikationsnetzen.

Metcalfe's Law: The value of a telecommunication network is proportional to the square of the number of connected users of the system (n^2).

2.2 Was versteht man unter In Band und Out of Band Signalisierung? Geben Sie Beispiele für Anwendung in der Telekommunikation, erklären Sie kurz Vorteile und Nachteile der Methoden.

In-Band-Signalling: Verbindungssteuerung am selben Kanal wie der eigentliche Telefonanruf, in analoger Telefonie verwendet, ist einfacher aber anfälliger für Störungen
Out-of-band-Signalling: eigener Signalisierungskanal zur Steuerung der Verbindung, bei ISDN verwendet (Data Channel und Signalling Channel - B- Channel und D-Channel), ist robuster, dafür höherer technischer Aufwand

2.3 Erklären Sie (kurz, evtl. mit Skizze) das Konzept der Paketvermittlung (packet switching)

Bei der Paketvermittlung wird eine logische Verbindung zwischen den Teilnehmern aufgebaut. Längere Nachrichten werden in einzelne Datenpakete unterteilt und als Datagramm über die virtuelle Verbindung übermittelt. Die Pakete durchqueren als unabhängige und eigenständige Einheiten das Netz und können in den Vermittlungsknoten zwischengespeichert werden.

Vorteile:

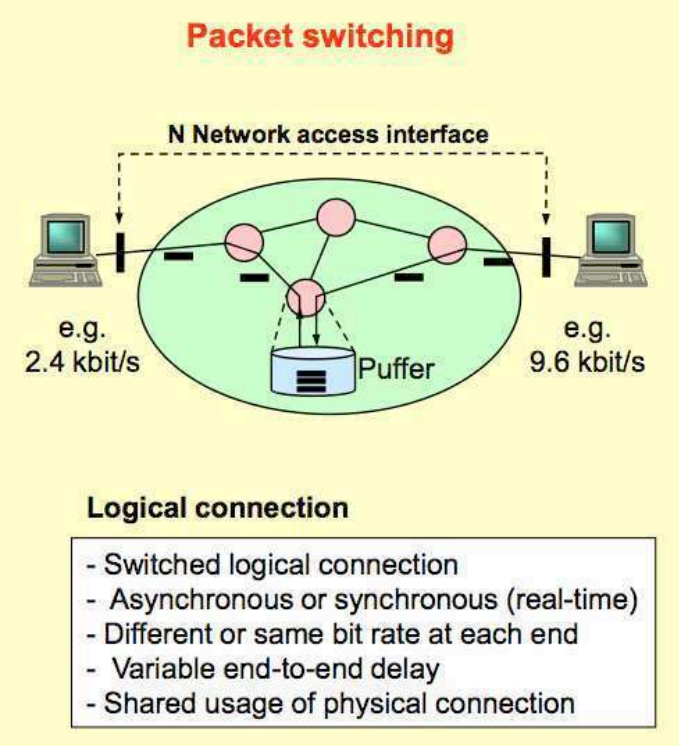
- kleine Pakete => kurze Wartezeiten für alle Teilnehmer und gute Netzauslastung, Übertragungsfehler können schnell erkannt und behoben werden
- faire Verteilung der Ressourcen
- fällt eine Vermittlungsstation aus wird der Datenstrom einfach umgelenkt

Nachteile:

- da die Übertragungsrouten nicht festgelegt sind, kann es zu Überlastungen an einzelnen Vermittlungsstationen kommen
- die Pakete müssen nicht in der gleichen Reihe beim Empfänger ankommen, wie sie gesendet wurden
- es kann keine konstante Bandbreite garantiert werden und es kann zu Schwankungen kommen
- da die Pakete gebuffert und in die Queues der Vermittlungsstationen kommen, ist der Delay variabel

Wird verwendet in:

Wireless: GPRS, UMTS, WLAN
Wired: IP, LAN, ATM (Asynchronous Transfer Mode), ...



2.4 Erklären Sie (kurz, evtl. mit Skizze) das Konzept der Leitungsvermittlung (circuit switching)

Bei der Leitungsvermittlung wird ein durchgeschalteter Übertragungskanal mit konstanter Bandbreite zugeordnet, der dieser Verbindung zur exklusiven Nutzung zur Verfügung steht (auch wenn keine Informationen übertragen werden).

Vorteile:

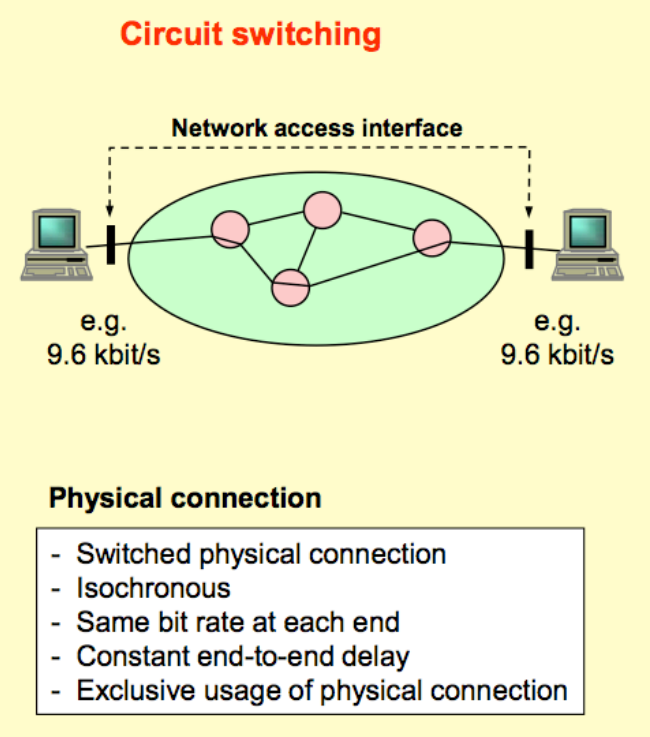
- konstante Bandbreite und Delay (Nachrichten müssen von Zwischenstationen nicht zwischengespeichert werden)
- keine zusätzlichen Header (Address-Informationen etc.) in den Nachrichten, keine Umordnung der empfangenen Daten

Nachteile:

- fällt eine Zwischenstation aus, so bricht die Verbindung zusammen
- Verschwendung von Ressourcen
- höhere Kosten

Wird verwendet in:
Wireless: GSM

Wired: PSTN, ISDN



2.5 Beschreiben Sie die wesentlichen Vor und Nachteile von Paketvermittlung und Leitungsvermittlung in Bezug auf Multimedia Kommunikation.

Bei der Leitungsvermittlung wird eine exklusive physikalische Verbindung zwischen den Teilnehmern aufgebaut. Die daraus entstehenden Vorteile sind der kleine und fixe Delay (kein Jitter), da kein Buffering in den Zwischenstationen nötig ist. Die Daten kommen beim Empfänger in der gleichen Reihenfolge an, wie sie abgesendet wurden. All diese Eigenschaften sind besonders für Multimedia-Kommunikation günstig. Der große Nachteil der Leitungsvermittlung ist, dass die Verbindung nicht aufrechterhalten werden kann, wenn eine der Zwischenstationen ausfällt. Im Falle der Paketvermittlung können die Daten über einen anderen Weg geroutet werden. Die Paketvermittlung bietet auch eine bessere Ausnutzung der Ressourcen, da die Verbindungen nicht exklusiv den Teilnehmern zur Verfügung stehen. Jedoch entsteht Overhead aufgrund von Adressierung.

2.6 Vergleichen Sie die Positionierung der Intelligenz und Kontrolle in Leitungs und Paketvermittelten Netzen.

Leitungsvermittlung: die Vermittlungsstellen sind für die Vermittlung der Verbindung zuständig, die Kontrolle für den Datenfluss liegt in den Vermittlungsstellen, Intelligenz ist in den Vermittlungsstellen untergebracht

Paketvermittlung: Intelligenz in den Endgeräten für die Verarbeitung der Pakete (die Pakete müssen die richtigen Header, Adressinformationen usw. enthalten, müssen beim Empfänger wieder geordnet und zusammengesetzt werden), die Zwischenstationen leiten die Pakete, entsprechend den Adressinformationen, einfach weiter

2.7 Was können Sie über die Verfügbarkeit (Availability) von leitungsvermittelten (Telefonie) und paketvermittelten (IP) Netzen sagen? Was versteht man unter den „five nines“?

Five nines bedeutet eine Availability von 99,999% (fünf mal die neun), dies entspricht einer Downtime von 5,26 Minuten im Jahr

Leitungsvermittlung hat eine Availability von 99,999% (“Carrier class” equipment and specifications), Leitungsvermittlung hat höhere Availability als Paketvermittlung

Paketvermittlung: bei Paketvermittlung werden “Carrier Class”, Business und Consumer Equipment gemischt verwendet, der Backbone Target hat eine Availability von >99,99%, die lokalen Netzwerke haben eine Availability von >99%

2.8 Wofür wird ICMP verwendet? Geben Sie ein Beispiel eines häufig verwendeten Programms, das auf ICMP aufbaut und erklären Sie dessen Funktionsweise.

ICMP … Internet Control Message Protocol

- dient zur Übertragung von Fehler- und Kontrollmeldungen bei fehlerhaftem IP-Betrieb
- benutzt IP-Datagramme um Meldungen zu versenden
- meldet keine Fehler bei den ICMP-Meldungen selbst
- reagiert nicht bei Fehlern der Prüfsumme eines IP-Datagramms
- meldet nur Fehler beim ersten fragmentierten Paket

Ping benutzt ICMP, Ping sendet einen ICMP-Echo-Request an die Zieladresse des zu überprüfenden Hosts, der Empfänger muss laut Protokollspezifikation eine Antwort zurücksenden, eine ICMP-Echo-Reply

2.9 IPv4 und IPv6: Erläutern Sie, welches die wesentlichen Gründe für die Einführung von IPv6 sind, welche Versäumnisse es bei der IPv4 Adressvergabe gab und welche Folgen diese hatten.

IPv4 (RFC 791) wurde 1981 veröffentlicht, damals erachtete man den Adressraum mit der Größe 2^{32} als groß genug, 1989 entwickelte Tim Berners-Lee jedoch das WWW (HTTP, HTML, Browser)
es würde jedoch noch immer genug Adressen geben, wenn sie nicht so ungleichmäßig verteilt

worden wären, die USA besitzen ca. 50-75% aller 4 Milliarden IPv4 Adressen, die University of California besitzt 250 Millionen IP Adressen, China hat 420 Millionen Internet User und 250 Millionen IP Adressen
viele (kleine) amerikanische Firmen bekamen damals Class A Adressen (das bedeutet 16,777,214 mögliche Hosts), es gibt insgesamt nur 126 Class A's
die Anzahl der benötigten IP Adressen wird weiter ansteigen: mobile Geräte, Smart Homes, steigende Weltbevölkerung … => IPv6
IPv4 Re-Distribution von ungenutzten Adressen: hoher administrativer Aufwand, nur eine zeitliche Verzögerung, vergebene IP-Adressen können rechtlich nicht zurückgefordert werden.
NAT, Network Address Translation: Mehrere private Rechner bekommen nur eine öffentiche Adresse, wobei diese Abbildung durch die 16bit breiten Portnummern auf ca. 65000 Rechner beschränkt ist.

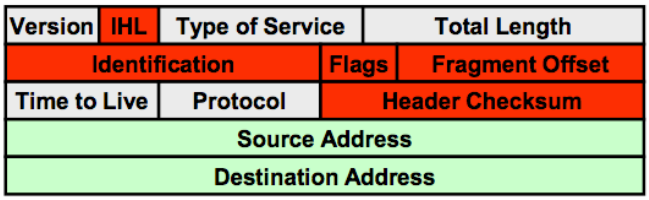
2.10 Welche Klassen von Anwendungen dominieren heute das Verkehrsvolumen in IP basierten Netzen? Für welche Entscheidungen können bzw. sollten Sie veröffentlichte Internet Statistiken als Grundlage verwenden? Worauf müssen Sie bei der Auswahl der Statistiken achten?

Peer to Peer dominiert das Verkehrsvolumen (70% des Traffics in Deutschland in 2007), HTTP auf Platz 2 mit 10%
Peer To Peer ist in der Statistik von 2008/09 auf Platz 1, mit 45-70% je nach Region
fast 75% des Traffics bei eDonkey waren für Videodaten, Musik auf Platz 2

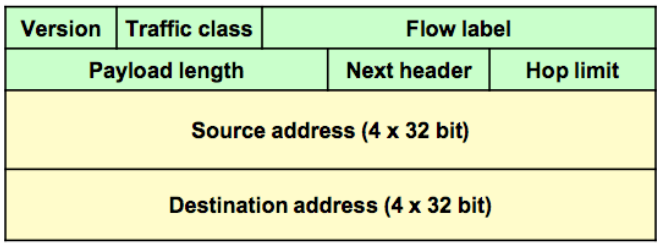
2.11 Welches sind die wesentlichen Eigenschaften bzw. Neuerungen von IPv6 verglichen mit IPv4 (high level Vorteile)?

- größerer Adressraum: 128 Bit Adressen anstatt 32 Bit Adressen
- zustandslose IPv6 Addressen Autokonfiguration: integriert, ersetzt zustandsorientiertes DHCP oder manuelle Konfiguration
- einfacheres IPv6 Header Format: fixe Standard Header Länge, keine Checksummen-Berechnung, signifikante Verbesserung in der Router-Performance
- Mobility und Security: integriertere Unterstützung für Mobile IPv6 und IPSec (Internet Protocol Security - Sicherheitsprotokoll, arbeitet im Gegensatz zu SSL direkt auf der Vermittlungsschicht, Layer 3 im OSI Modell)
- IPv6 Extension Headers: flexible Optionen, Extension ohne dass das IPv6 Protokoll geändert werden muss, optionale Unterstützung für größere Pakete (IPv6 "Jumbogramme")

2.12 Welche im IPv4 Header vorhandenen Felder wurden im IPv6 Header entfernt und welche kamen neu hinzu? Weshalb?



IPv4 Header (20-60 bytes)



IPv6 Header (40 bytes)

entfernte IPv4 Felder:

- Header Length: der IPv6 Header hat eine fixe Länge, somit wird dieses Feld nicht mehr benötigt
- Identification, Flags, Fragment Offset
    - werden benutzt, um fragmentierte Pakete wieder zusammenzusetzen
    - Identification: Fragmente des selben Pakets haben gleiche Nummer
    - Flags: zeigt an ob Paket fragmentiert ist
    - Fragment Offset: Eine Nummer, die bei fragmentierten Paketen besagt, ab welcher Position innerhalb des Paketes das Fragment anfängt.
    - die Informationen zur Fragmentierung werden in IPv6 im optionalen Extension Header angegeben
        - nur der sendende Host kann IPv6 Pakete fragmentieren
        - ist ein Paket zu groß muss der Absender die MTU (Maximum Transmission Unit) anpassen, Path MTU Discovery (ICMPv6)
- Header Checksum: entfernt, weil in IPv6 auf MAC- und Transport/Application Layern überprüft wird

Arbeit für Router wird minimiert, deren Hauptaufgabe war das Prüfen von Checksummen und Fragmentieren von Daten

IPv6 Header:

- Version (4 Bits): IP Version, 6 für IPv6
- Traffic Class (1 Byte): entspricht dem “Type of Service”-Feld in IPv4, für QoS verwendeter Wert, eine Art Prioritätsvergabe
- Flow Label (20 Bits): ebenfalls für QoS oder Echtzeitanwendungen verwendeter Wert, Pakete die zum gleichen Flow gehören, werden gleich behandelt
- Payload Length (2 Bytes):
    - Länge des IPv6-Paketinhaltes nach dem Basic IPv6 Header
    - inkludiert auch die Länge der Extension Headers
    - in IPv4 war der Header in der Payload Length auch enthalten
- Hop Limit (1 Byte): TTL Feld aus IPv4 wurde umbenannt, Wert wird von Router dekrementiert
- Next Header (1 Byte)
    - entspricht dem “Protocol Type”-Feld in IPv4
    - identifiziert den Typ des nächsten Headers, kann sein

- Protocol Data: wie in IPv4, bezeichnet Protokoll höherer Schicht, z.B. TCP, UDP
- IPv6 Extension Header: Next Header bezeichnet Typ des folgenden Extension Headers

- Source Address (128 Bit): IPv6 Adresse des sendenden Hosts
- Destination Address (128 Bit): destination Address muss nicht unbedingt die Adresse des schlussendlichen Empfängers enthalten, so wie in IPv4; existiert der Routing Extension Header so enthält die Destination Address die Adresse des nächsten Hops

2.13 Zählen Sie die von IPv6 unterstützten Adress bzw. Adressierungsarten auf und beschreiben Sie sie kurz.

IP-Adressen beziehen sich auf bestimmte Hosts (bzw. ein Interface von einem Host)

die von IPv6 unterstützen Adressarten:

- Unicast address: bezeichnet ein einziges Interface
- Multicast address: bezeichnet eine Gruppe an Interfaces, die Nachrichten werden von allen Mitgliedern der Gruppe empfangen
- Anycast address: ist mehreren Interfaces zugeordnet, die Nachricht wird an eines dieser (an das nächstgelegene) dieser Interfaces gesendet

2.14 Weshalb gibt es in IPv6 kein Broadcast mehr? Wodurch wurde IPv4 Broadcast ersetzt?

die Broadcast-Adressen aus IPv4 werden durch die Multicast- oder Anycast-Adressen ersetzt (Nachricht wird an die all hosts Multicast-Adresse gesendet)

2.15 Was bedeutet ARP bzw. RARP, wofür wird das Protokoll verwendet? Welches Protokoll/welche Funktionalität ersetzt ARP und RARP in IPv6?

ARP … Address Resolution Protocol
RARP … Reverse Address Resolution Protocol

wird fast ausschließlich in Zusammenhang mit IPv4 verwendet, IPv6 hat dafür NDP (Neighbor Discovery Protocol), ARP ist ein Network-Layer-Protokoll, löst die IP-Adresse auf die zugehörige MAC-Adresse auf, wird meistens benutzt um IP-Pakete auf Ethernet-Frames abzubilden, ARP Request wird vom Host generiert um die MAC Adresse des Next Hops (Adresse des nächsten IP-Router) zu bestimmen

Da IPv4-Adressen nur aus 32 Bits bestehen, sind sie nicht in der Lage, MAC-Adressen zu speichern. Aus diesem Grund besteht keine feste Beziehung zwischen MAC-Adressen und IP-Adressen. Bevor ein Rechner im Ethernet an einen Rechner im selben Subnetz ein IP-Paket sendet, muss er die Information in einen Ethernetframe verpacken. Dazu muss er die MAC-Adresse des Zielrechners kennen und im entsprechenden Feld des Ethernetframes einfügen. Ist ihm diese nicht bekannt, kann er das IP-Paket nicht zustellen. Stattdessen ermittelt er dann mit Hilfe des ARP zunächst die MAC-Adresse des Zielrechners.

RARP ermöglicht die Zuordnung von MAC-Adressen zu IP-Adressen, wird verwendet wenn IP-Adresse nicht bekannt ist

RARP sendet dazu ein *RARP Request*-Broadcast mit der eigenen MAC-Adresse als Inhalt an die am Netzwerk angeschlossenen Rechner. Ein RARP-Server, welcher alle Zuordnungen IP- zu MAC-Adressen kennt, sendet daraufhin eine Antwort mit der IP-Adresse an die anfragende MAC-Adresse (*RARP-Reply*).

2.16 Welche Adressierungsform (addressing mechanism) wird in IPv4 Netzen und welche in Telefonienetzen verwendet? Wie wird in den IETF Standards die Entität (Instanz) genannt, die man mit einer IPv4 oder IPv6 Adresse adressiert? Was ist die physikalische Entsprechung (in einem Computersystem)?

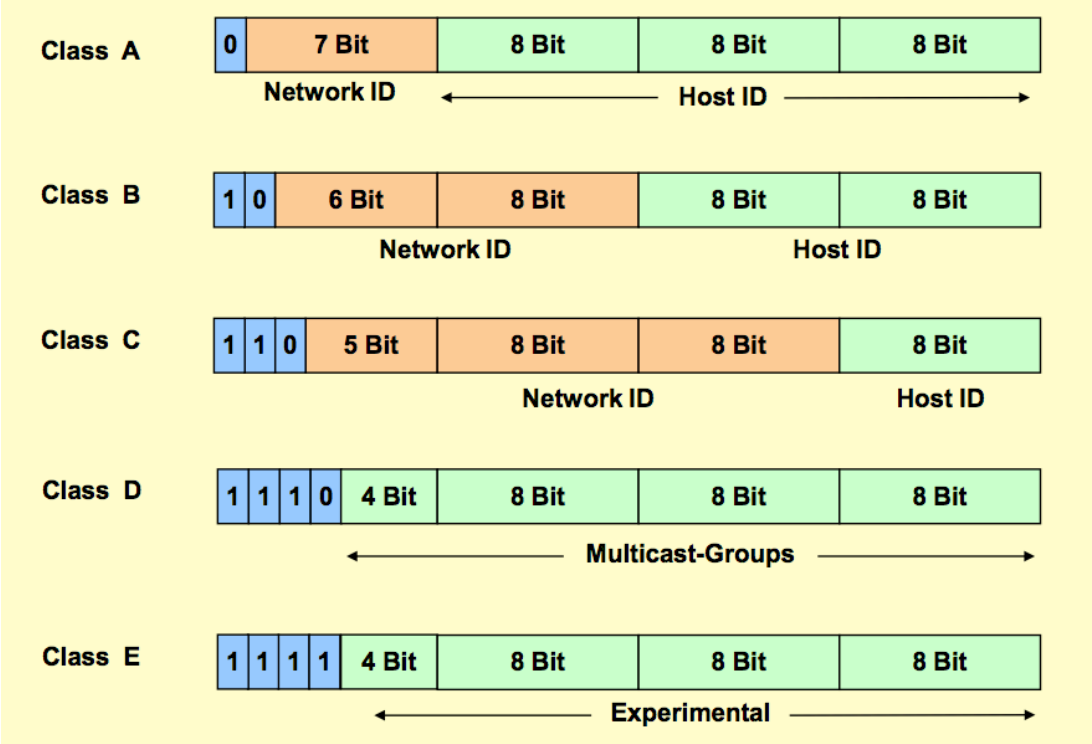
Eine IPv4 Adresse besteht aus 4 Blöcken zu je 8 Bit, entweder geschrieben als 3 Dezimalzahlen getrennt durch Punkte oder als 32 Bit Hexadezimalzahl.
Es gibt verschiedene Netzwerkklassen, unterschieden durch die maximale Anzahl an möglichen Netzen und möglichen Hosts.

Entitäten heißen bei IETF Interfaces (http://www.faqs.org/rfcs/rfc2460.html), die physikalische Entsprechung ist ein Netzwerkmodul.

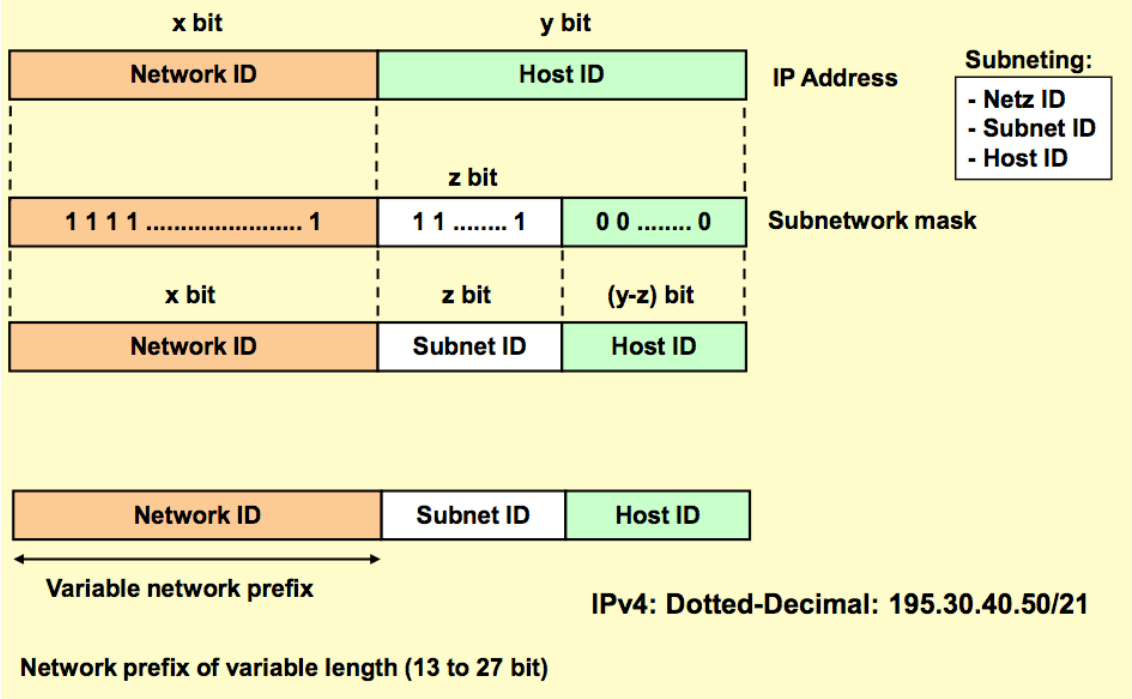
2.17 Wie viele IPv4 Adressen und wie viele IPv6 Adressen gibt es ungefähr? Wie viele Bit werden für die Speicherung einer IPv4 bzw. einer IPv6 Adresse benötigt?

IPv4: 32 Bit, 2^{32} Adressen = 4 294 967 296 Adressen (~4 Milliarden Adressen)
IPv6: 128 Bit, 2^{128} Adressen = 3,402823669209387e+38 Adressen (~$3{,}4 \cdot 10^{38}$ Adressen)

2.18 Welche Klassen von IPv4 Adressen gibt es? Wo liegt das Problem dabei, wie funktioniert Classless Inter Domain Routing und was ist der wesentliche Vorteil davon? Geben Sie ein Beispiel für die Adress Notation bei CIDR.



Das starre Adressenschema der klassischen IP-Adresse in Netzwerk- und Host-Teil verhindert eine flexible Anpassung und schränkt den gesamten Adressraum wesentlich ein. Da die Anzahl an IP-Adressen begrenzt ist, hat man bei der IPv4-Adresse das Verfahren des Classless Interdomain Routing (CIDR) eingeführt, das den zur Verfügung stehenden 32 Bit umfassenden Adressraum effizienter ausnutzt. Dieses CIDR-Verfahren wird auch bei IPv6 verwendet.
Das CIDR-Verfahren löst die starren IP-Adressstrukturen und basiert auf Subnetzmasken. Die Subnetzmaske teilt die IP-Adresse in den Netzwerkteil und den Hostteil auf.
In der Notation werden diese Subnetzmasken durch einen Suffix angegeben, der mit einem Schrägstrich an die IP-Adresse angehängt wird. Das Suffix bestimmt die Anzahl der 1-Bit-Werte in der IP-Adresse, beginnend beim ersten Bit im ersten Byte.
Bsp.: 172.17.0.0/17 entspricht 172.17.0.0/255.255.128.0



2.19 Welche Notationen werden für IPv4 Adressen verwendet und welche für IPv6? Geben Sie mindestens je ein Beispiel. Weshalb kann man höchstens eine zusammenhängende Nuller Gruppe in einer IPv6 Adresse ersetzen?

IPv4 Adressen werden geschrieben als 4 durch Punkte getrennte Dezimalwerte (192.168.0.1) oder als eine 32 Bit Hexadezimalzahl (0xC0A00001). IPv6 Adressen bestehen aus acht 16 Bit Blöcken in hexadezimaler Schreibweise durch Doppelpunkte getrennt. (2001:0629:2600:0:0:0:0:5113). Eine zusammenhängende Nullergruppe kann in einer verkürzten Schreibweise entfallen. (2001:0629:2600::5113, ersetzt durch zwei aufeinanderfolgende Doppelpunkte). Dies ist möglich weil die Anzahl der Blöcke immer genau 8 sein muss. Die auf 8 fehlenden Blöcke werden dann einfach mit Nullen aufgefüllt. Bei mehr als einer Komprimierung dieser Art wäre eine Rekonstruktion nicht mehr möglich, da die Anzahl der Zusammenhängenden Null-Blöcke nun nicht mehr eindeutig wäre.

2.20 Wie wird eine IPv6 Adresse in eine URL eingebunden? Weshalb?

IPv6 Adressen werden zwischen eckigen Klammern eingebunden. Der Grund hierfür ist, dass ansonsten der URL-Parser den Unterschied zwischen Adresse und Port (aufgrund der gleichen Schreibweise mit Doppelpunkt) nicht mehr erkennt.
Bsp: http://[2001:0629:2600::5113]:8080/

2.21 Erklären Sie kurz „Private Netze“ im Zusammenhang mit IPv4 Adressen. Welche Vorteile

und welche Nachteile hat diese Adressierungsform?

Um für private Netze nicht einen IP-Bereich beantragen zu müssen, gibt es sogenannte private IP-Adressen:
Class A: 10.0.0.0–10.255.255.255 (10.0.0.0/8)
Class B: 172.16.0.0–172.31.255.255 (172.16.0.0/16 - 172.31.0.0/16)
Class C: 192.168.0.0–192.168.255.255 (192.168.0.0/24 - 192.168.255.0/24)

Adressen aus den oben angegebenen Bereichen können für interne Netze frei genutzt werden. Da mit diesen Adressen kein Internetzugang möglich ist (sie werden nicht geroutet), können beliebig viele LANs diese Adressen verwenden.

Bei der Einteilung des Adressraums aller gültigen IP-Adressen wurden ursprünglich Netzklassen festgelegt und entsprechend für jede Klasse ein "privater Adressraum" reserviert.

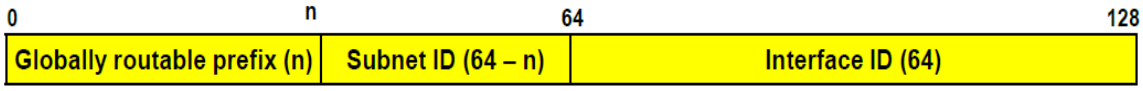
Ein Vorteil ist die Einsparung von öffentlichen IP-Adressen, ein privates Netz trägt nach außen hin nur eine Adresse, damit verbunden ist auch ein gewisser Grad an zusätzlicher Sicherheit (Stw. NAT) Nachteil: erhöhter Aufwand.

2.22 Durch welches Konzept wurden Private IPv4 Netze in IPv6 ersetzt?

Das Konzept der privaten Netze wurde ersetzt durch die “Unique Local Address/Unicast”. Adressen mit dem Prefix FC00::/7 sind für zukünftige Anwendungen vorgesehen und sind beabsichtigt weltweit eindeutig zu sein. Adressen mit beginnendem FD00::/7 können für private Netze frei verwendetet werden. Der Standard (RFC 4193) sieht dabei einen Algorithmus für die Erzeugung einer 40-Bit Pseudo-Zufallszahl vor, die an den Prefix zusammen mit einer 16-Bit Subnetz ID angehängt wird und gemeinsam die Netzwerkadresse bilden.

2.23 Beschreiben Sie Funktionalität und Aufbau einer „Global Unicast Address“ in IPv6

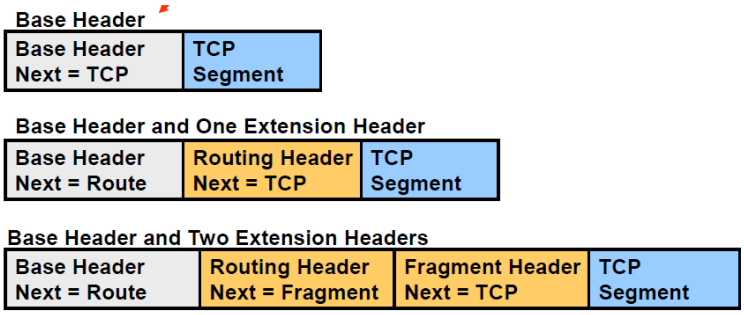
Zu sehen ist das Format einer Global Unicast Adresse.



Für den End-User sind als Prefix 64 Bit vorgesehen. Es bleiben damit 64 Bit für die Interface-ID. Internet Service Providern werden Prefixe der Größe 32 zugesprochen, die davon Adressen ihren Kunden zuweisen können. Für größe Unternehmen ist /48 vorgesehen, in seltenen Fällen auch kleiner.
Prefix 2000::/3 steht für alle derzeit von der IANA vergebenen Globalen Unicast Adressen. An Providern vergebenen Adressen sind 2001::

2.24 Beschreiben Sie den Sinn und die Funktionalität von Extension Headers in IPv6. Geben Sie Beispiele von Standard IPv6 Extension Headers bzw. von optionalen Extension Headers und beschreiben Sie kurz deren Einsatzbereich.

Die Headerlänge bei IPv6 ist auf 40 Byte fixiert. Optionale, seltener verwendete Header-Informationen werden in Form von Extension-Headern an den Base Header angehängt.
Ist ein Extension Header im IPv6-Header vorhanden, so wird dies im Feld "Next Header" des Base Headers gekennzeichnet. Es wird der jeweils nachfolgende Headertyp in das Feld eingetragen



Sechs Headertypen müssen zwingend in IPv6 implementiert sein, von denen jeder maximal einmal im gesamten Header vorkommen darf:

- Hop-by-hop Options Header
  Trägt von Routern am Übertragungsweg benötigte Information.
- Routing Header
  Folge von Routern, die angesteuert werden müssen, durch diesen Mechanismus kann ein bestimmter Pfad durchs Netz bestimmt werden.
- Fragment Header
  Fragmentierung in IPv6 geschieht ausschließlich beim Sender, einzelne Knoten im Pfad dürfen Pakete nicht (weiter) fragmentieren. Die Pfad-MTU muss vor Übertragung großer Daten bestimmt werden.
- Destination Options Header
  Enthält Information die ausschließlich vom Empfänger verarbeitet werden soll. Dieser Header kann zweimal vorkommen (Hop-by-Hop & End-to-End).
    - Hop-by-Hop: Header steht vor Routing Header, Information ausschließlich für Router
    - End-to-End: Header Steht vor Protokoll-Segment, Information ausschließlich für Empfänger.
- Authentication Header
  Integritätsschutz, Verifizierung der Herkunft der Daten, Schützt den Destination Options Header, Nutzdaten, Basis-Header, mit Ausnahme von Hop-Limit.
- Encapsulating Security Payload Header
  Verschlüsselungsinformation bezüglich Sicherheit der Nutzdaten.

Und weitere optionale Extension Header, zB. Extension Header für Mobile IPv6

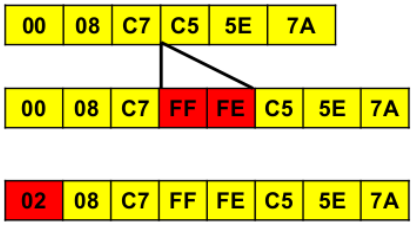
2.25 Welche Merkmale von IPv6 Paketen erlauben eine effizientere Weiterleitung in Routern? Vergleichen Sie den Aufbau des IPv4 – Headers mit dem von IPv6.

Vgl. Frage 2.12
Die Headerlänge ist konstant 40 Byte. Das Checksummenfeld wurde entfernt, diese werden nur noch auf MAC und Transport/Application-Ebene berechnet. Die Fragmentierungsinformation ist nur noch als eigenständiger Extended Header ausgeführt. Es ist nur noch Endgeräten erlaubt Pakete zu fragmentieren. Diese Tatsache und das Weglassen der Checksummenberechnung reduziert die Anforderung an Rechenleistung von Routern.

2.26 Was verstehen Sie unter SLAAC? Beschreiben Sie wesentlichen Schritte von SLAAC in IPv6.

SLAAC … Stateless Address Auto Configuration
Host kann vollautomatisch eine funktionsfähige Internetverbindung aufbauen, dazu kommuniziert er mit den für sein Netzwerksegment zuständigen Routern, um die notwendige Konfiguration zu ermitteln

- Schritt 1:
  - der Host weist sich eine link-lokale Adresse zu, dazu wird die 48 Bit MAC-Adresse in einen 64 Bit Interface Identifier konvertiert: 0xFFFE wird zwischen 3. und 4. Byte der MAC Adresse eingefügt und das low-order Bit 2 des ersten Bytes wird auf 1 gesetzt



- Schritt 2:
  - Node verwendet NDP (Neighbor Discovery Protocol) um Router zu finden (basiert auf ICMPv6)
  - geschieht durch Anfrage an Multicast-Adresse FF02::2, über die alle Router eines Segments erreichbar sind (Router Solcitation)
  - Router versendet daraufhin Router Advertisements (RA), die Informationen zu den verfügbaren Präfixen enthalten, also Information über die Adressbereiche, aus denen ein Gerät sich selbst Unicast-Adressen zuweisen darf
  - Node bildet sich selbst eine global routbare Unicast-Adresse indem er an das Präfix den Interface Identifier anhängt
- Schritt 3:
  - Duplicate Address Detection (DAD)
  - die gewählte Adresse muss einzigartig sein, dies muss überprüft werden, der

Vorgang läuft ohne Benutzereingriff via NDP (Neighbour Discovery Protocol) ab

2.27 Welche schwerwiegende Risiken birgt die IPv6 Autokonfiguration und welche Maßnahmen wurden getroffen um alternative Lösungen anzubieten?

zu den global routbaren Unicast-Adressen könnte die MAC-Adresse ausfindig gemacht werden, womit es möglich wäre E-Mails auf einen bestimmten Computer/User zurückzuverfolgen und es können Profile für bestimmte User angelegt werden, was ein großes Problem der Privatsphäre darstellt

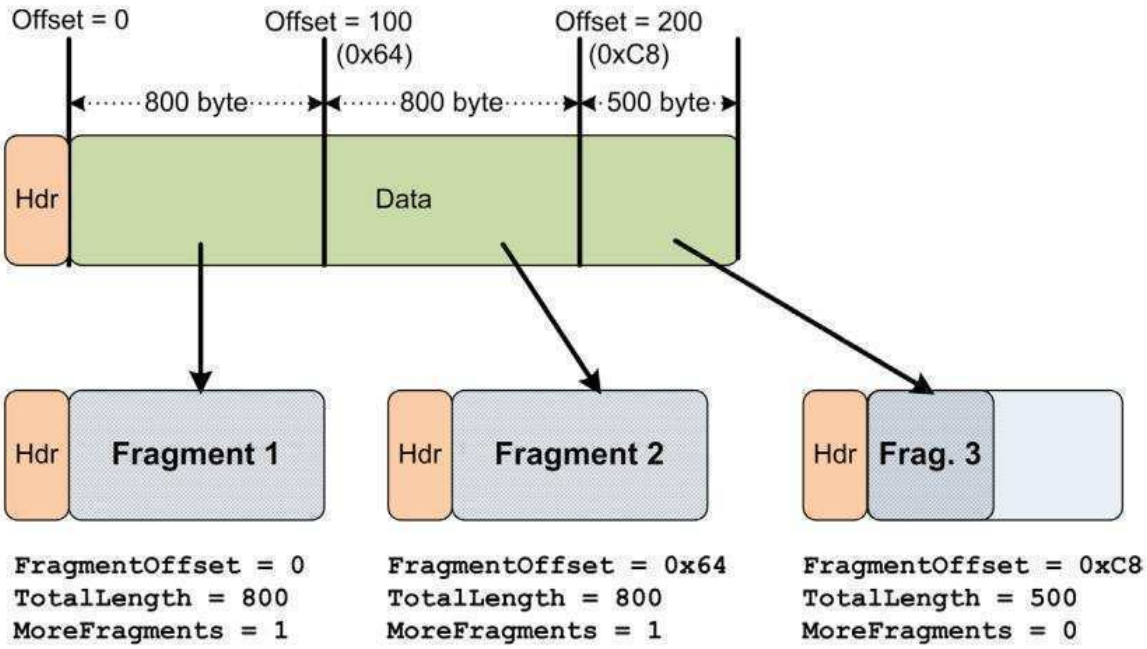
Abhilfe: Privacy Extension für SLAAC in IPv6: dem Host wird eine zufällige Interface-ID zugewiesen, die nach einer bestimmten Zeitdauer geändert wird
Alternativen: DHCPv6, statisch konfigurierte IPv6 Adressen

2.28 Wie entscheidet der IPv4/IPv6 Stack bei einem eingehenden Paket, an welchen darüberliegenden Transport Protokollstack die Daten weitergereicht werden?

Anhand des Protocol-Feldes in IPv4 oder des Next-Header-Feldes in IPv6. Die verschiedenen Protokolle sind durch Nummern gekennzeichnet.

2.29 Beschreiben Sie kurz Notwendigkeit und Funktionsprinzip von Fragmentierung bzw. Re Assembling in IPv4 Netzen.

Die Datenpaketgrößen in IP-Netzen sind nicht fest vorgeschrieben. Fragmentierung wird dann notwendig, wenn das zu sendende Datenpaket zu groß für einen physikalischen Datenblock (bzw. MTU...Maximum Transmission Unit) ist.



Beim Reassembling wird die Reihenfolge der Pakete durch den Offset bestimmt. Der Speicher für das gesamte Paket muss zuvor Alloziert worden sein.

2.30 Welche wesentlichen Neuerungen gibt es bei IPv6 bezüglich Fragmentierung? Vergleichen Sie die Fragmentierung bei IPv4 und IPv6.

Siehe auch Frage 2.25 und 2.12. Es dürfen nur noch sendende Hosts Pakete fragmentieren. Ist die Paketgröße größer als eine am Pfad vorkommende MTU (Maximum Transmission Unit einer Verbindungsstrecke, so wird vom vorangehenden Knoten (bspw. Router) eine ICMPv6-Fehlernachricht Fragment generiert. Der sendende Host passt auf Erhalt die Paketgröße entsprechend an und die Daten werden nochmals gesendet. Auch der Extension Header Fragment wird entsprechend angepasst bzw. eingefügt.

Die minimale MTU bei IPv6 ist 1280 Byte, sind kleinere Paketgrößen erfordert, muss auf Link Layer-Ebene fragmentiert werden.
IPv6/IPv4 Interworking: Eine kleinere IPv4 als IPv6 MTU führt zu einer ICMPv6 Fehlermeldung (Packet too big). Der IPv6/IPv4 Umsetzer bedient sich des IPv6 Fragmentation Extension Headers, um die Daten zu fragmentieren.

Teil 3: Transportebene

3.1 Welche Aufgabe erfüllt die Transportebene, weshalb ist sie zur Kommunikation notwendig?

vierte Schicht des OSI-Modells, bietet den Applikationen End-to-End Communication Services

Aufgaben:

- Segmentierung des Datenstroms und richtiges wiederzusammensetzen der Pakete beim Empfänger (Ordering)
- Flow Control
- Reliability (ACKs und NACKs)
- Multiplexing
- verbindungsorientierte Kommunikation (TCP)
- bietet den anwendungsorientierten Schichten 5 bis 7 einen einheitlichen Zugriff, so dass diese die Eigenschaften des Kommunikationsnetzes nicht zu berücksichtigen brauchen

Protokolle: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), SCTP (Stream Transmission Control Protocol), DCCP (Datagram Congestion Control Protocol)

3.2 Welches 5 Tupel beschreibt eine Verbindung im Internet Protokoll Stack eindeutig?

<Sender IP, Sender Port, Recv IP, Recv Port, Protocol>

z.B.: <128.131.101.5, 13384, 193.99.144.85, 80, TCP>

Die Port-Nummer wird vom Protokoll unterschieden, z.B. kann am gleichen Host eine Applikation über TCP am Port <n> kommunizieren während eine andere Applikation den gleichen Port <n> mit UDP benutzt

3.3 Beschreiben Sie kurz die wesentlichen Eigenschaften, Vorteile, Nachteile und Einsatzbereiche von UDP in Bezug auf Multimedia Kommunikation (Signalisierung und Medienübertragung). Welches sind die typischen Einsatzbereiche von UDP in der Praxis?

Eigenschaften: verbindungslos, best effort, nur kleine Erweiterung der Funktionalität von Layer 3: Weiterreichung der Daten an Application Layer, gleiche Adressierung wie in TCP (Portnummer, Socket, Verbindung), einfach zu implementieren

Nachteile: Übertragung von Datagrammen ist unreliable, die Eigenschaften von IP bleiben erhalten, d.h. Pakete können verloren gehen, dupliziert sein, umgeordnet sein, … (Applikation muss sich darum kümmern)

Vorteile: kaum Overhead

benutzt für Streaming Applications, Pakete müssen nicht durch ACKs bestätigt werden und bei

Verlust eines Paketes muss es nicht erneut gesendet werden, bei Echtzeitanforderungen sind weggefallene Pakete angemessener als Pakete die zu spät ankommen

3.4 Beschreiben Sie kurz die wesentlichen Eigenschaften, Vorteile, Nachteile und Einsatzbereiche von TCP in Bezug auf Multimedia Kommunikation (Signalisierung und Medienübertragung). Welches sind die typischen Einsatzbereiche von TCP in der Praxis?

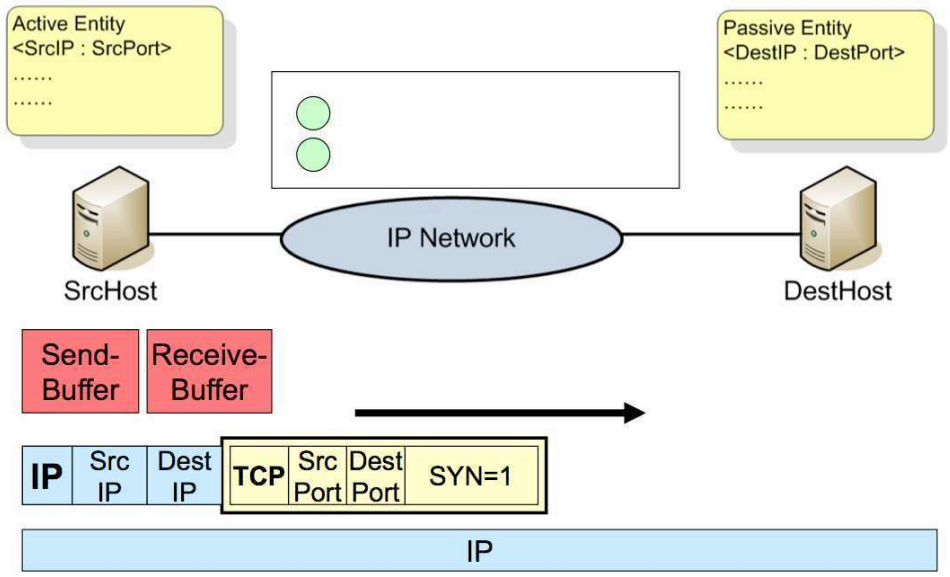
- Bi-Direktional verbindungsorientiert
  - Full-Duplex
  - Verbindungsaufbau
- Reliable
  - korrekte Ordnung der Pakete
  - Datenintegrität (Checksummen-basierender Verwurf von fehlerhaften Segmenten)
  - Sequence Counter
- Flow Control (Empfänger kontrolliert Datenfluss)
- End-to-End Connection
- Sequence Counters
- transparente Retransmission Mechanismen im Falle von Paketverlust

Nachteile: keine Übertragung von strukturierten Daten, Datenpaket-Limits bleiben nicht erhalten, mehrere Security-Defizite

3.5 Beschreiben Sie den Aufbau einer TCP Verbindung. Weshalb ist dieser Aufwand notwendig?

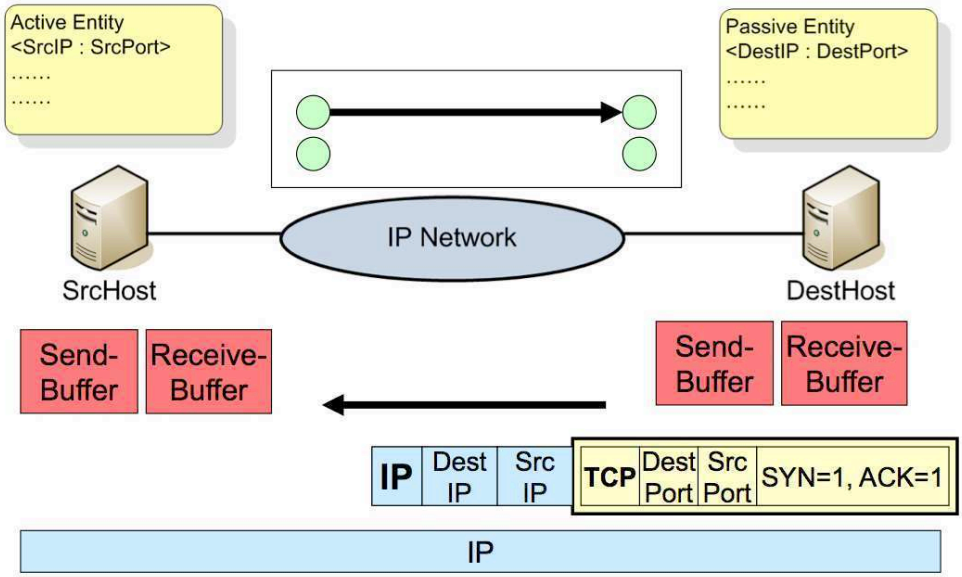
Schritt 1:

1. Aktive Entität initiiert Verbindung
2. Sende/Receive-Buffer werden allokiert
3. der Client der Verbindung aufbauen will sendet SYN Paket mit Sequenznummer x (für die Sicherstellung einer vollständigen Übertragung in der richtigen Reihenfolge und ohne Duplikate)
   - von <SrcIP>:<SrcPort> zu <DestIP>:<DestPort>



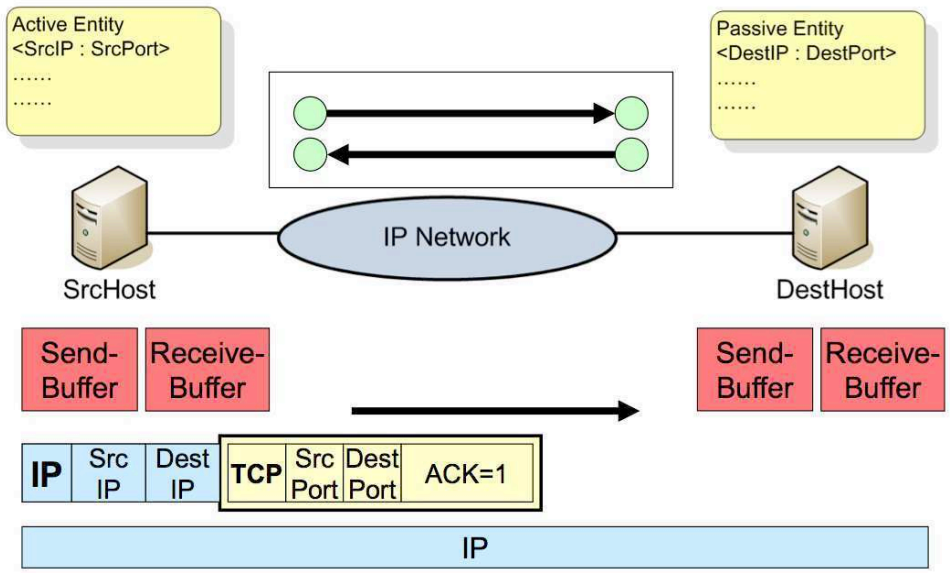
Schritt 2:

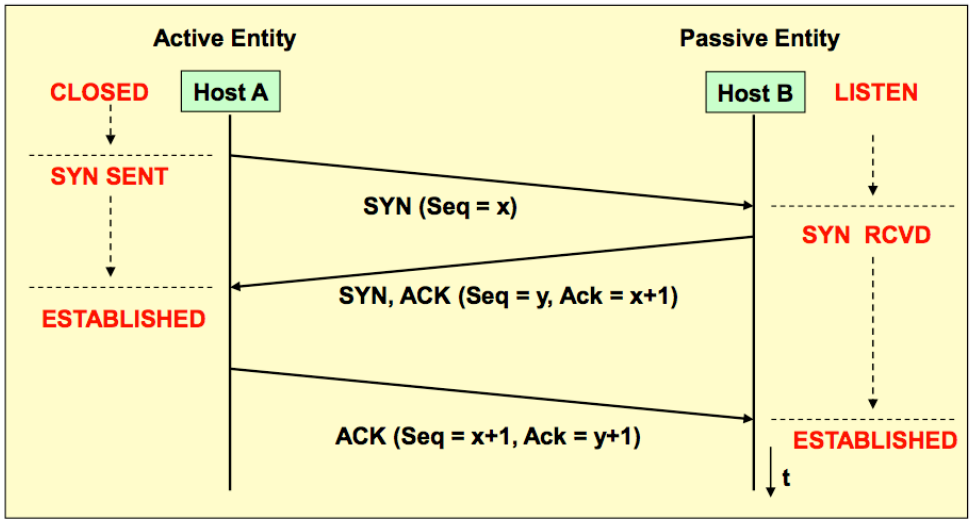
1. Host empfängt SYN Paket
2. TCP/IP Stack allokiert Sending/Receiving Buffers
3. SYN-ACK Paket wird zurück gesendet
    - von <DestIP>:<DestPort> nach <SrcIP>:<SrcPort>



Schritt 3:

1. der Initiator der Verbindung nimmt SYN-ACK an und bestätigt mit ACK
2. die logische TCP Verbindung ist jetzt aufgebaut und bereit zum Datenverkehr





Aufwand ist notwendig um sicherzustellen, dass auch alle Pakete ankommen.

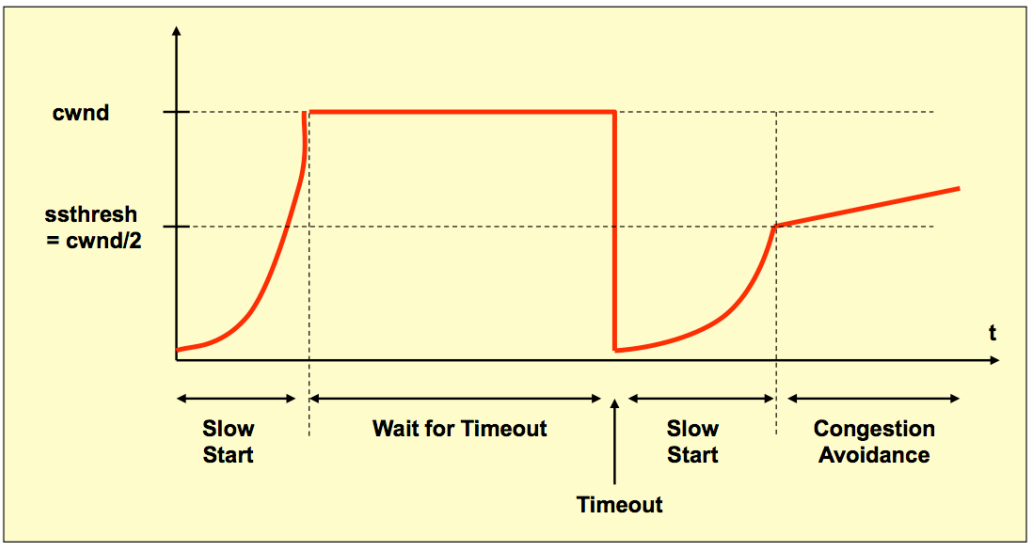
3.6 Welche Informationen werden beim Aufbau einer TCP Verbindung zwischen Sender und Empfänger ausgetauscht. Weshalb?

Vor der effektiven Kommunikation muss eine virtuelle Verbindung aufgebaut werden, weil die Verbindungsparameter ausgehandelt werden müssen.
Sequenznummern werden zwischen Sender und Empfänger synchronisiert, Ressourcen (Sende/Empfangs-Buffer) werden allokiert, Segment- und Window-Größe werden ausgehandelt

3.7 Was ist die wesentliche Ursache für die „Sägezahnkurve“ bei der Ubertragung mit TCP?

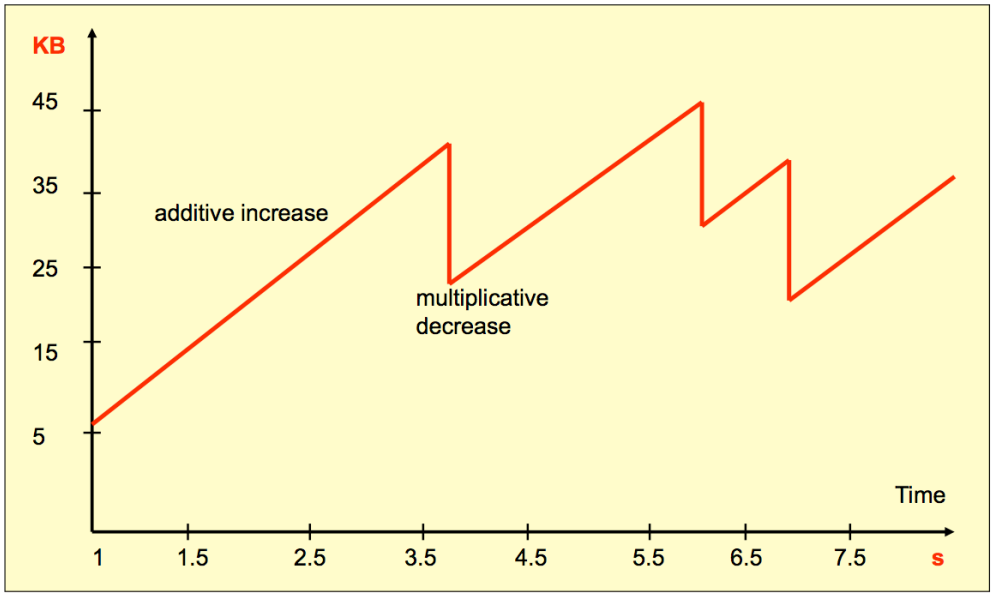
Congestion Control: Wird eine Verbindung stark belastet, werden immer mehr Pakete verworfen, die entsprechend wiederholt werden müssen. Durch die Wiederholung steigt wiederum die Belastung, ohne geeignete Maßnahmen kommt es zu einem Datenstau.
Normalerweise wird eine TCP/IP-Verbindung langsam gestartet (Slow-Start) und die Senderate schrittweise erhöht, bis es zum Datenverlust kommt. Ein Datenverlust verringert die Senderate, ohne Verlust wird sie wiederum erhöht. Insgesamt nähert sich die Datenrate so zunächst dem jeweiligen zur Verfügung stehenden Maximum und bleibt ungefähr dann dort. Eine Überbelastung wird vermieden.

Slow Start und Congestion Avoidance

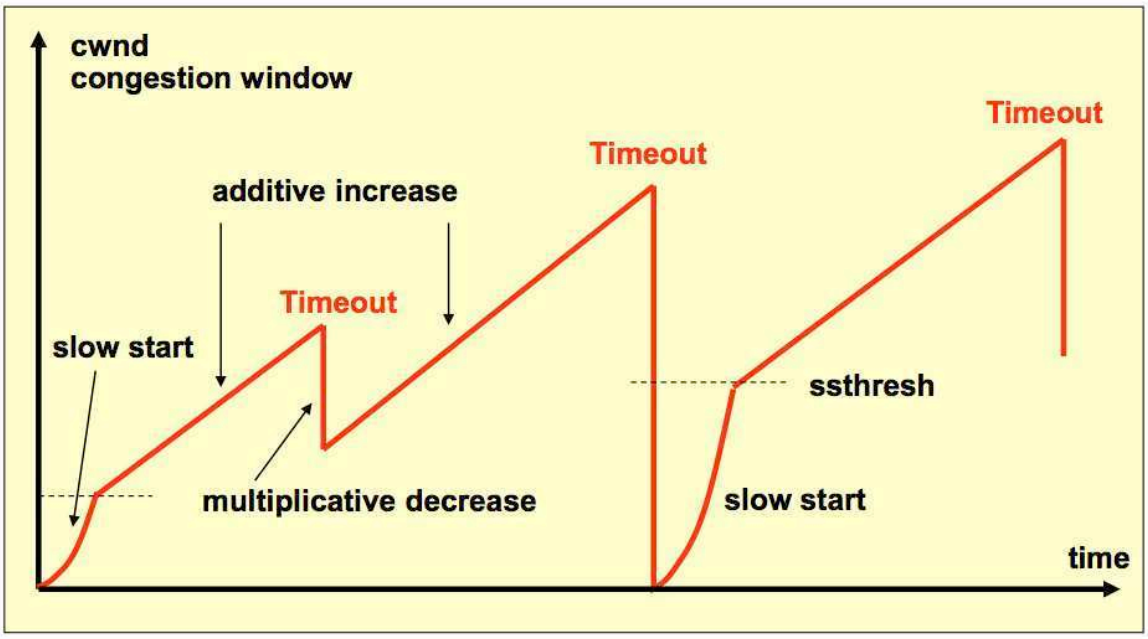


es wird zunächst mit der Übertragung von kleinen Datenmengen begonnen, mit jedem erhaltenen ACK wird das Congestion Window vergrößert

- Additive Increase, Multiplicative Decrease
    - Window wird für jeden Roundtrip um 1 vergrößert, lineares Wachstum
    - Window wird um Faktor 2 des vorherigen Slow Start Threshhold vergrößert wenn Verlust angenommen wird (ACK nicht rechtzeitig erhalten) => bei häufigen Verlusten wächst das Fenster nur langsam
- Congestion Control Window wird anfänglich auf 2 x MSS (Maximum Segment Size) gesetzt



TCP Slow Start with AIMD Control



ssthresh = Slow Start Threshold
= cwnd / 2 upon every timeout

AIMD: Additive Increase Multiple Decrease

3.8 Welches Transport Protokoll wird für Echtzeit Datenübertragung verwendet? Weshalb?

siehe auch 3.3

UDP
Pakete müssen nicht durch ACKs bestätigt werden und bei Verlust eines Paketes muss es nicht erneut gesendet werden, bei Echtzeitanforderungen sind weggefallene Pakete angemessener als Pakete die zu spät ankommen

3.9 Nennen Sie den (einen) wesentlichen Grund, weshalb TCP nicht für die Übertragung von Echtzeitdaten geeignet ist. Skizzieren Sie ein konkretes Szenario, das den Problemfall verdeutlicht.

ACKs sind nötig

Wenn ein Paket verloren geht, wird auf dieses gewartet obwohl die darauf folgenden Pakete schon da sind.

3.10 Was für wesentliche Vorteile bieten SCTP und DCCP gegenüber den traditionellen Transportprotokollen TCP bzw. UDP?

SCTP … Streaming Control Transmission Protocol
Multi-homing (ein Host mit mehreren Zugängen zum Internet), Multi-streaming, verbesserte SYN-Flood Protection, abstimmbare Parameter (Timeout, Retransmissions, …), Message Boundary Preservation

DCCP … Datagram Congestion Control Protocol
Congestion Control, Sequence Numbers

Teil 4: DNS, ENUM, SIP, usw.

4.1 Wie war im Internet die Funktionalität von DNS VOR der Definition von DNS implementiert/realisiert?

Vor DNS wurden Domainnamen und zugehörige IP-Adressen in einer Textdatei “hosts.txt” gespeichert. Diese Datei wurde vom Network Information Center (NIC) instandgehalten und über FTP zur Verfügung gestellt.
Das schnelle Wachstum des Internets jedoch verlangte nach einer alternativen Lösung, da der Download von hosts.txt einen Internetverkehr proportional der Zahl der Internetuser verursachte.

4.2 Was sind die wesentlichen Aufgaben von DNS? Was waren die wesentlichen Ziele bei der Definition von DNS?

“…provide a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internets, and administrative organizations…” (RFC 1035)

Die Auflösung von Domainnamen (www.example.com) in IP-Adressen. Es besteht eine Vereinfachung darin, dass Namen leichter zu merken sind als IP-Adressen. Ein Vorteil ist, dass die IP-Adresse hinter einem Domainnamen einfach geändert werden kann ohne dass man als User etwas davon merkt. Durch die Mehrfachzuweisung von IP-Adressen zu Namen, kann Load-Balancing betrieben werden.

Auch ein Reverse-Lookup ist möglich.

Ziele:

- Konsistenter Namespace, keine Abhängigkeit von Network-ID, Adressen, Routes als Teil des Namens
  - Verteilte Datenbank mit lokalem Caching, Hauptgrund: Größe und Aktualisierungshäufigkeit, lokales Caching verbessert Performance
  - allgemeines Konzept, nicht an eine Anwendung gebunden, verschiedene Ressourcetypen
- Unabhängig vom Transportsystem

4.3 Beschreiben Sie die Architektur (Komponenten) von DNS und die DNS spezifischen Begriffe.

Domain-Namespace:
Der Domain Namespace hat Baumstruktur. Seine Blätter heißen Labels. Ein kompletter Domainname eines Objekts besteht aus der Verkettung aller Labels eines Pfades. Ein Domainname wird immer von Rechts nach Links aufgelöst. Die erste Ebene oberhalb der Wurzel (root) heißt Top-Level-Domain (.com, .at,...), eine Ebene darüber Second-Level Domain (.ac,...)

Nameserver:

Sind meist Programme, die Anfragen zum Domain-Space beantworten.

Resolver:
Sind auf einem lokalen Rechner installierte Softwaremodule, die DNS-Anfragen von Anwendungen übernehmen, eventuell ergänzen, und an einen DNS-Server weiterleiten. Der Resolver kennt zumindest einen DNS.

DNS-Clients:
nslookup, dig

4.4 Wie findet ein Client bei der Namensauflösung den ersten zu kontaktierenden DNS Server?

Der erste DNS Server ist beim Client vordefiniert (meist vom Provider).

4.5 Wofür wird der DNS Record Type benötigt, geben Sie mindestens fünf Beispiele für DNS Record Types (bevorzugt solche, die für Multimedia Kommunikation von Bedeutung sind).

A	gibt eine 32-bit IPv4 Adresse zurück, meistens verwendet um Domainnamen IP-Adressen von Hosts zuzuordnen.
AAAA	Gibt eine 128-bit IPv6 Adresse zurück
CNAME	Canonical Name Record, Namens-Alias, Der DNS Lookup wird unter dem neuen Namen durchgeführt
NS	Name Server Record, Verweist eine DNS-Zone an die angegebenen Authoritative Name Server
PTR	Pointer Record, Pointer zu einem Canonical Name Record, wird verwendet, um Reverse Lookup zu implementieren.

4.6 Zwei wesentliche architekturelle Konzepte in der Implementierung von DNS ermöglichen die notwendige (Steigerung der) Performance für den weltweiten Einsatz. Welches sind diese?

Caching, Verteilte Implementierung, ggf. hierarchische Struktur

4.7 Wofür steht ENUM, wofür wird es benötigt und in welchem Zusammenhang steht es mit dem DNS?

ENUM … E.164 NUmber Mapping
Wird verwendet um Telefonnummern in Internetadressen zu übersetzen.
Bsp.: Lookup +43 1 58801 38813
+ und Leerzeichen entfernen, Zeichenfolge umkehren, Punkte einfügen und Domain-Suffix
“e164.arpa” anhängen

→ 3.1.8.8.3.1.0.8.8.5.1.3.4 .e164.arpa
TLD ist .arpa, SLC ist .e164
Der so generierte Domainname folgt einem Pfad im DNS

4.8 Wofür steht SIP? Erklären Sie die wesentlichen Funktionen, die SIP erfüllt. Genügt SIP um Telefongespräche über IP zu führen? Mit welchen Transport Protokollen ist SIP einsetzbar?

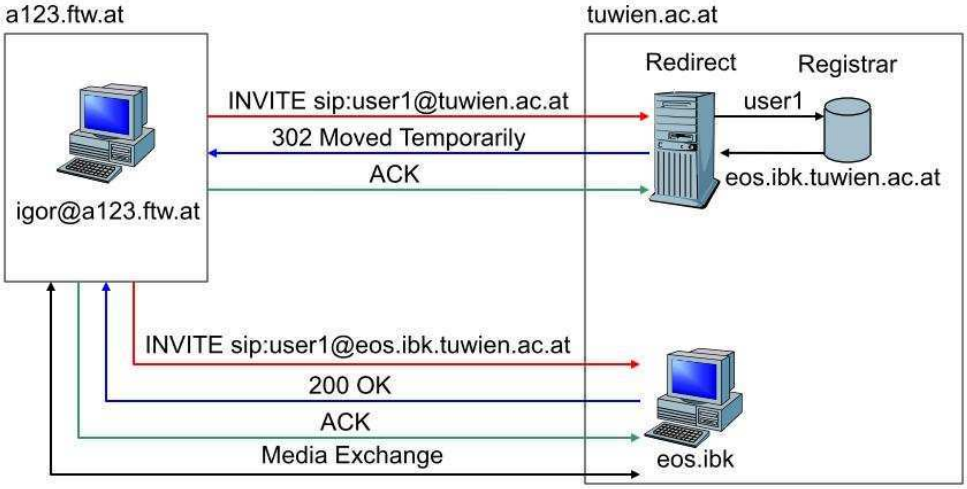
SIP … Session Initiation Protocol
Dient als IP Signalisierungsprotokoll im VoIP-Bereich.

- Verbindungsauf- und abbau
- Konferenzschaltungsmanagement
- Namens und Adressierungsinfrastruktur
- Flexibles Erstellen von Services
- Benutzerauthentifizierung

SIP dient nur zur Signalisierung, zur Sprachübetragung wird bspw. RTP verwendet.
Protokoll-Unabhängig, funktioniert mit TCP oder UDP.

4.9 Welche Server Typen gibt es in SIP (bezogen auf die Speicherung von Zustandsinformation in den Servern)? Nennen Sie für jeden dieser Server Typen mindestens ein Anwendungsgebiet.

- Redirect Server: Ist ein User Agent, der 3xx Responses auf empfangene Requests generiert. Clients werden somit auf eine alternative URI umgeleitet.



- Proxy Server: Ist eine vermittelnde Einheit, die sowohl als Server als auch als Client dient und im Auftrag von weiteren Clients Requests weiterleitet. Ein Proxy dient hauptsächlich zum Zwecke des Routings. Des weiteren ist es auch möglich Proxies zur Durchsetzung von Richtlinien einzusetzen (prüfen, ob ein User berechtigt ist einen Anruf zu tätigen)

    - Stateless Proxy: Leitet SIP Requests und Responses weiter. Leicht zu implementieren, schnelle Verarbeitung von SIP-Nachrichten. kein Billing, Forking, etc. möglich, TCP nicht unterstützt, kann keine provisional-Nachrichten (1xx) erzeugen.
    - Transaction Stateful Proxy: Speichert den Zustand jeder SIP-Transaktion (für Forking, jedoch kein Billing), kann eigene Provisional Responses erzeugen, TCP und UDP unterstützt.
    - Call Stateful Proxy: Speichert den Zustand jedes SIP-Calls (für Billing)
- Proxy-Server AAA: Authentication, Authorization, Accounting
    - A … Authentication: Überprüfe Identität, Passwort, digitale Zertifikate
    - A … Authorization: Prüfe, ob User die nötigen Rechte besitzt um eine Aktion durchzuführen, SIP-Proxys können basierend auf User-Informationen den Zugriff auf bestimmte Services erlauben oder verweigern.
    - A … Accounting: Charging und Billing für bestimmte Services und Benutzer, die Dauer eines Anrufes muss genau bestimmt werden (200 OK bis BYE), Stabilitätsprobleme: einer der UA stürzt ab, der Anruf dauert unendlich lange. Der Proxy-Server stürzt ab, alle Informationen wie die Anrufdauer gehen verloren. Abhilfen: UA-Polling, Intermediate Tickets, bei UA-Absturz auf ein BYE des zweiten UA warten, Re-Registrierungen
- Registrar: Unterstützt nur REGISTER-Requests, besitzt eine lokale Datenbank mit registrierten Usern. Stellt die Benutzerdaten für Proxy-Server und Redirects zur Verfügung. Meistens sind Registrare gemeinsam mit einem Proxy oder Redirect-Server in derselben Einheit kombiniert. Die Schnittstelle zwischen Registrar und Proxy bzw. Redirect-Server ist in SIP nicht standardisiert!
- Back-to-Back User Agent (B2BUA): Ist eine logische Einheit, die Requests empfängt und sie wie ein UAS verarbeitet. Um zu bestimmen wie der Request beantwortet werden soll, verhält sich der B2B UA wie ein UAC. Wird verwendet für Topology-Hiding.
- Forking: Ein User ist mit mehreren UA (mehrere Adressen) im System registriert. Der Proxy sendet ein INVITE an alle Stellen. Sobald ein 200 OK zurückkommt, sendet er einen CANCEL Request an alle übrigen Stellen.

4.10 Beschreiben Sie die wesentlichen Eigenschaften des SIP Protokolls (Nachrichtenformat, Codierung, Nachrichtentypen)

2 Typen von Nachrichten: SIP Request und SIP Response

Das Nachrichtenformat besteht aus textuellen Beschreibungen und gliedert sich in
Startzeile, ein oder mehrere Message-Header-Zeilen, Leerzeile, Body (optional)
Manche SIP-Header beschreiben den Message-Body (content-type, content-length)
SIP-Message-Body enthält üblicherweise ein Session Description Protokoll.

4.11 Wie kann man SIP Nachrichten vom Typ her klassifizieren (angelehnt an HTTP)? Welche

Klassen/Kategorien von SIP Responses gibt es (angelehnt an HTTP)?

Types of Status Code in SIP Responses
– Provisional (1xx) - request received, continuing to process the request
– Success (2xx) - the request was accepted
– Redirection (3xx) - further action needs to be taken to complete the request
– Client-Error (4xx) - the request contains bad syntax or cannot be fulfilled at this server
– Server-Error (5xx) - the server failed to fulfil the request
– Global-Failure (6xx) - the request cannot be fulfilled at any server

4.12 Wie bezeichnet der SIP Standard einen SIP Endpunkt (ein Endgerät)? Welche zwei Rollen kann das Endgerät spielen? Was für einen Zweck hat diese strenge logische Trennung?

UAC … User Agent Client, Tätigt Anrufe
UAS … Wartet auf Anrufe und übernimmt, oder lehnt ab

Einerseits wegen der erleichterten Implementierung, (UAC Requests, UAS Responses), und auch aus Verrechnungsgründen.

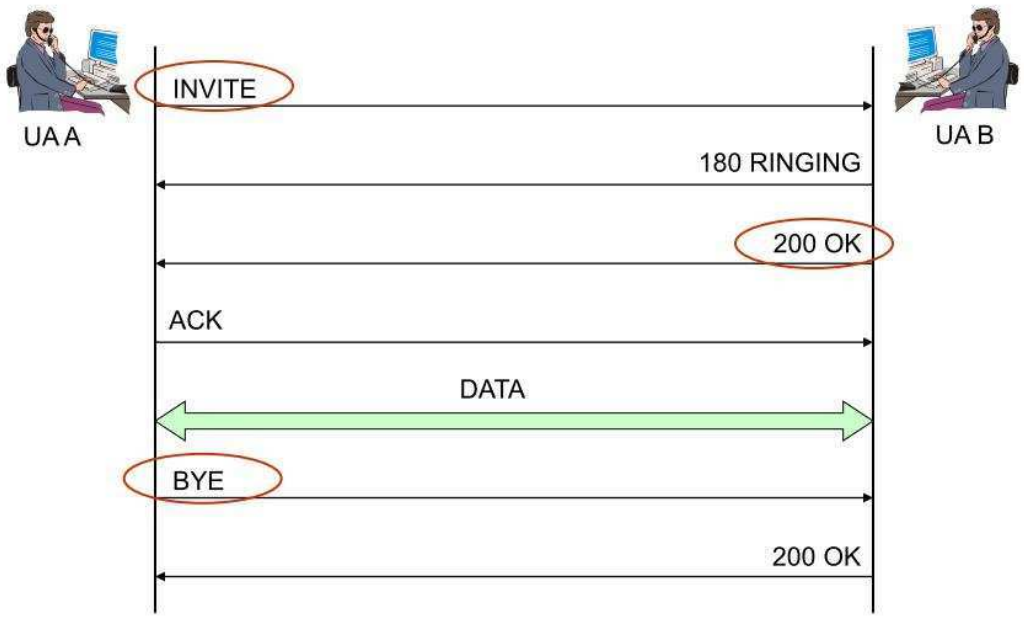
4.13 Erläutern Sie das Kommunikationskonzept von SIP d.h. benennen und erläutern Sie die von SIP definierten Gruppen von Nachrichten.

Message – Request/Response – Transaktion (Request mit dazu gehörigen Responses),
Dialog (alle Transactions vom Aufbau bis Abbau), Call (einer oder mehrere Dialoge)

4.14 Wie lautet die genaue Bezeichnung der Adresse in SIP? Geben Sie ein Beispiel einer SIP Adresse.

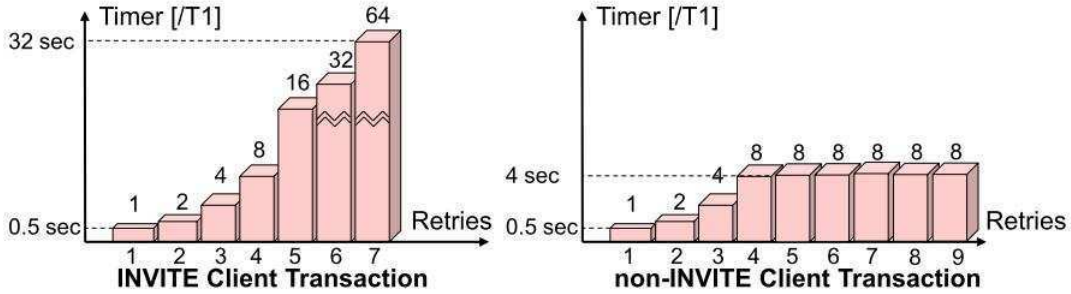
Host muss inkludiert sein, User Name und Portnummer können inkludiert sein
Syntax: sip:user:password@host:port;uri-parameters?headers (z.B. sip:jiri@iptel.org
oder sip:+4315880138813@ibk.tuwien.ac.at:port=5060;user=phone)

4.15 Beschreiben Sie den Ablauf des Verbindungsaufbaus in SIP in Form eines Sequenzdiagramms (Requests, Responses, Nachrichtenbezeichnung).



4.16 Welche Mechanismen verwendet SIP um Paketverluste auszugleichen? Welchen Unterschied gibt es diesbezüglich für Invite und Non Invite Transaktionen? Weshalb?

Verloren gegangene Pakete werden nochmals gesendet, bei unzuverlässigem Transportprotokoll (UDP) benötigt.
Der Wert des Retransmit-Timers wird bei jeder Wiederholung um einen Faktor 2 verdoppelt (bei INVITE Requests).



4.17 Welche Funktion erfüllt die Registrierung in SIP?

User Contact Information, Verfügbarkeit, Authentifizierung

4.18 Auf welche Arten kann eine bestehende SIP Registrierung gelöscht? Welche Nachricht wird dafür verwendet? Wie wird die Registrierung eines UA und wie die aller registrierten UA eines Users gelöscht?

Es wird ein REGISTER Request mit Expires:0 gesendet. Wenn alle registrierten UA eines Users de-registiert werden sollen, so muss im REGISTER-Request-Header eine einzelne Contact-Zeile mit Wildcard (*) angegeben werden. Dies ist nur gültig wenn Expires auf Null gesetzt ist.

4.19 Beschreiben Sie das Routing in SIP. Anhand welcher Information und wie genau erfolgt das (SIP) Routen von ersten Anfragen (Requests) vom Absender zum Empfänger? Welche Information bestimmt die Route der dazu gehörigen Antworten (Responses)?

Via Header im Request: Wird verwendet, um die Route des Requests zu verfolgen, die Reihenfolge der Via-Header ist wichtig

1. Der UA, der den Request generiert, speichert seine eigene Adresse als erste Via-Header-Zeile
2. Jeder weiterleitende Proxy fügt seine Adresse davor hinzu
3. Dank der Via-Header kann die Route für den Response zurückverfolgt werden.
4. Dazu wird der Via-Header des Requests in den Response-Header kopiert
5. Die Response wird vom UAS an die erste Adresse im Via-Header gesendet.
6. Jeder Proxy entfernt seine (oberste) Adresse und leitet die Response an die nächste Adresse weiter.

4.20 Mit welchen Mitteln kann man eine feste Wegwahl der Anfragen (Requests) bzw. der Antworten (Responses) in SIP erzwingen?

Record Route Header:
Call Stateful Proxies müssen im Pfad für alle weiteren Requests bestehen bleiben.

1. Ein CS-Proxy kopiert seine Adresse an die erste Stelle in den Record Route Header.
2. Der UAS kopiert den Record-Route Header in die Final Response und gelangt so zum UAC.
3. Der UAC kopiert den Record-Route-Header in invertierter Reihenfolge in den Route-Header. Alle weiteren Requests beinhalten den Route-Header und es werden alle Proxies in der Record-Route erreicht.

4.21 Erklären Sie mittels Sequenzdiagrammen das unterschiedliche Verhalten der drei in SIP vorgesehenen Proxy Varianten.

Forwarding Proxy, Redirect Proxy, Forking Proxy
-Stateless Proxy
-Transaction Stateful Proxy
-Call Stateful Proxy

4.22 Welche Protokolle werden typischerweise gemeinsam mit SIP für Multimedia Kommunikation eingesetzt? Weshalb?

RTP: Über eine zwischen zwei Rechnern aufgebaute SIP-Session können verschiedene Medien (Sprache, Video, Daten) mit Hilfe des Protokolls RTP transportiert werden.
SDP: Bei SIP werden u.a. folgende Eigenschaften der initiierten RTP-Session nach dem Protokoll SDP ausgehandelt:
- Welche Medien sollen übermittelt werden?
- Wie werden die einzelnen Medien codiert?
- Welcher Port wurde dem Protokoll RTP zugewiesen?

4.23 Was bedeutet SDP? Wie unterstützt SDP den Verbindungsaufbau und welche Rolle spielt es genau?

SDP … Session Description Protocol, SIP Unterstützung von SDP ist verpflichtend. Aufgabe von SDP in SIP ist der Austausch von Medienstream-bezogenen Informationen, textbasierend definiert durch die Multiparty Multimedia Session Control (MMUSIC) WG der IETF

- IP-Adresse
- UDP or TCP Port (meistens UDP wegen RTP)
- Medientyp (audio, video, interactive whiteboard, ...)
- Mediencodec (PCM μ-Law, G.729, H.261, ...)
- Session spezifische Information (nicht verpflichtend in SIP)
  Betreff der Session
  Start- und Stop-Zeit
  Besitzerinformation

4.24 Beschreiben Sie die Probleme von SIP im Zusammenhang von NAT/Firewalls. Welche Lösungen gibt es?

NAT übersetzt private IP-Adressen und Ports in globale.

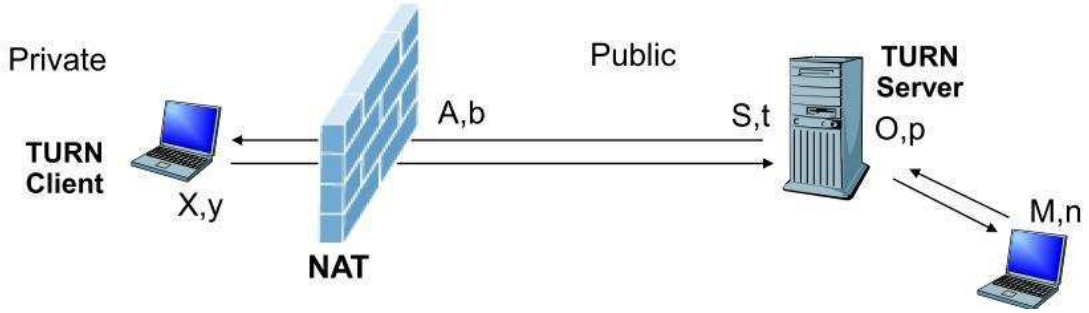
SIP Signalisierungsproblem:
Problem ist, dass bei der SIP Signalisierung in den SIP-Headern die falsche private IP-Adresse und Portnummer enthalten ist.

Media Traversal Problem:
IP Adressen und Ports in INVITE und OK Messages sind privat und nicht global. Die RTP Datenströme müssen für den globalen Verkehr initiiert werden, RTCP Real Time Control Protocol

Abhilfen:
- Application Level Gateway ALG, Der Service ist im NAT vorhanden

NAT arbeitet auf Application layer und modifiziert die SIP-Nachrichten, ändert IP-Adressen und Portnummern in den SIP und SDP-Headern, (Request-URI,VIA,RECORD-ROUTE,ROUTE,FROM,TO,CONTACT)
Einschränkungen sind: Erweiterbarkeit, Sicherheit, Stabilität

- IETF STUN Lösung: (Session Traversal Utilities for NAT)
  STUN Protokoll bestimmt die globale IP-Adresse des NAT, funktioniert NICHT mit symmetrischen NAT, funktioniert nicht wenn sich beide clients hinter derselben NAT befinden, alle Clients müssen STUN-fähig sein, wird bereits von vielen Endgeräten unterstützt
- TURN-Server



Jeder involvierte Client muss TURN/STUN-fähig sein, behebt das symmetric-NAT Problem, Medienströme fließen über den TURN-Server, das erfordert höheres QoS wegen
zusätzlichen Verzögerungen.

- ICE, Interactive Connectivity Establishment

Protokol für NAT (Network Adress Translator),

4.25 Wie wird eine RTP Verbindung in SIP aufgebaut? Wie werden die entsprechenden Verbindungs Parameter (z.B. Codecs) festgelegt?

Mit SIP-INVITE-Request + SDP Body

4.26 Gibt es die Möglichkeit, Parameter einer bereits mittels SIP aufgebaute RTP Verbindung zu modifizieren? Begründen und beschreiben Sie die Mechanismen, die die Modifikation verhindern oder ermöglichen.

Ja, es ist ein erneuter Austausch der Medieninformationen nötig, mittels Re-Invite. Sind die Medienströme am jeweiligen UA nicht unterstützt, so antwortet dieser mit 405 Not Acceptable. Ansonsten folgt ein 200 OK und ACK.

4.27 Auf welches Transport Protokoll setzt RTP auf? Welche für Echtzeit Datentransport wesentlichen Informationen enthält der RTP Header?

RTP setzt auf UDP auf
Anforderungen an ein Echtzeitprotokoll sind:

- Die Daten müssen mit der selben Zeitlichen Relation empfangen werden mit der sie gesendet werden.
- Jitter und Delay muss abgefangen werden
- Der Datenstrom muss konstant sein
- Pakete, die zu spät ankommen können verworfen werden (Packet Loss)

Die Vorteile von UDP gegenüber TCP sind:

- Slow-Start Algorithmus in TCP verhindert einen konstanten Datenstrom, TCP Retransmissions verzögern den Stream, Nur Forward Error Correction ist möglich in TCP
- UDP-Header sind kleiner als TCP-Header, geringerer Overhead
- UDP ist leichter zu implementieren, erlaubt schnellere Bearbeitung
- UDP ermöglicht Multicast, mehrere Empfänger können den selben Stream empfangen

Nachteile von UDP:

- Keine Korrektur der Paketreihenfolge
- Keine Erkennung von Paketverlusten
- Jitter (wegen verschieden langen Übertragungswegen)

RTP wurde ausgehend von UDP entwickelt um eine Reihe von Echtzeit-Multimediaströmen zu transportieren und die Unzulänglichkeiten von UDP zu beseitigen.

Zwei der wichtigsten Eigenschaften von RTP sind:

- Sequenznummerierung der Pakete
- Timestamp des ersten Samples, Synchronisation und Jitter-Berechnung

Einige wichtige Header-Felder:

- Payload-Type (PT): Kennzeichnet den Medientyp
- Sequence Number (16 bit), Zufälliger Wert für das erste Paket, für jedes weitere Paket inkrementiert, Paketverlusterkennung, Herstellung der Paketreihenfolge
- Timestamp (32 bit), Zeitpunkt des ersten Samples, Auflösung wir durch den Medientyp bestimmt, Jitterberechnung und Synchronisation

4.28 Beschreiben Sie in Stichworten die notwendigen Schritte/Komponenten um Sprache in paketvermittelten Netzen (IP) zu übertragen (Kette vom Sender zum Empfänger).

Encoder - Packetizer - Transport Control - Network - Transport Control - Reassembly - Decoder

4.29 Welche Funktion erfüllt der Jitter Buffer in der Echtzeitkommunikation? Welche Vorteile und welche Nachteile hat er?

Durch Jitter kann es passieren, dass Pakete mit einer höheren Sequenznummer vor Paketen

mit einer niedrigen Paketnummer ankommen. Der Jitter-Buffer soll Jitter ausgleichen. Problem: Es wird eine zusätzliche künstliche Verzögerung eingeführt.

4.30 Welche Information im RTP Header ist für die Bearbeitung des RTP Pakets im Jitter Buffer wesentlich?

Timestamp und Sequenznummer

4.31 Folgen SIP Signalisierungsdaten und RTP Mediendaten gleichen oder unterschiedlichen Routen? Weshalb? Wer bestimmt die verwendeten Zwischenknoten?

Normalerweise gleichen Routen, mitunter jedoch unterschiedlich. Route für Stateful Proxies wird umgangen und direkt gesendet. Media IP kann von Session IP abweichen (Video-Streaming).

4.32 Wie kommunziert ein SIP Endgerät mit einem Gerät im PSTN bzw. umgekehrt? Welche technischen Voraussetzungen müssen dafür erfüllt sein (Signalisierung, Medienstrom)?

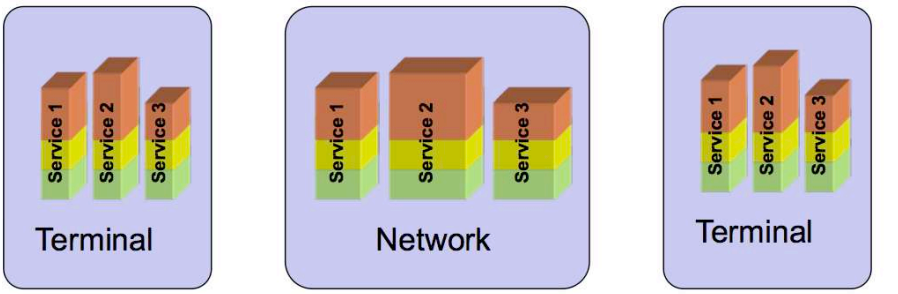
Via SIP-Proxy und IP/PSTN-Gateway auf PSTN-Switch, PCM Sprachdaten
Von PSTN-Switch zu Telefon analog

Teil 5: IMS

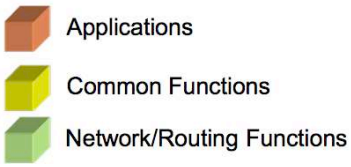
5.1 Welche Vorteile und Nachteile bietet eine "All IP" Infrastruktur gegenüber derzeitigen Kommunikationsnetzen? Nennen und vergleichen Sie die wesentlichen Merkmale von Telekom und Internet Architektur.

Eine einzige Infrastruktur für beliebige Dienste (horizontale Architektur), Kostenersparnis und einfache Realisierung von Diensten. Nachteil: bessere Optimierung vertikaler Dienste, höherer Overhead

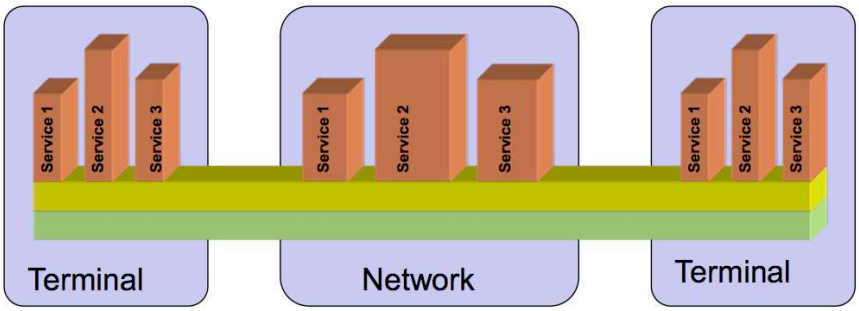
5.2 Was versteht man unter Vertikalen bzw. Horizontalen Dienste (Service) Architekturen?

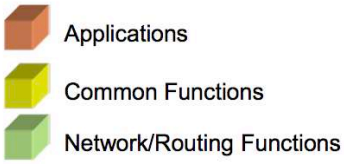


- Topics
  - Application complexity
  - Security
  - Roaming



Vertikale Service Architekturen:
alle Layer werden neu implementiert





Horizontale Service Architekturen:
die Network/Routing Functions und gemeinsamen Funktionen werden überall eingesetzt und nur die Applikationen sind gänzlich unterschiedlich

5.3 Welche entscheidenden Änderungen bringt das All IP Konzept bezüglich Rollenverteilung im Telekommunikationsmarkt mit sich? Welche Risiken birgt das für bestehende Telekommunikationsunternehmen?

Traditionelle Telekommunikationsunternehmen “besitzen” Kunden.
Sie übernehmen 2 Rollen:

- Service Provider (Voice, IP)
- Access Provider

Der Wert eines Telekommunikationsunternehmens wird sehr stark durch die Anzahl der Kunden bestimmt. “Demjenigen der die Rechnung ausstellt, gehört der Kunde”.
Für Telekommunikationsunternehmen besteht das Risiko “just another Bit-Pipe” zu werden, d.h. selbst keine Services anzubieten, sondern Services anderer Anbieter zum Kunden zu transportieren (und nicht davon zu profitieren).

5.4 Was ist IMS? Wer standardisiert IMS? Welche anderen wichtigen Technologien werden von der gleichen Organisation standardisiert? Welche Bereiche umfassen die IMS bezogenen Standards?

IP-Multimedia-Subsystem, Ziel von IMS ist ein standardisierter Zugriff auf Dienste aus unterschiedlichen Netzwerken.

- IMS ist ein architektonisches Framework
- Overlay-Network für bereits bestehende Packet- und Circuit-Switched Netzwerke
- Unterstützt IP-basierendes interaktives Multimedia
- End to End QoS
- IPv6 verpflichtend
- Die Signalisierung basiert auf IETF Protokolle (SIP, Diameter)
- Integration mit PSTN (Public Switched Telephone Network)

Wird standardisiert von 3GPP (3rd Generation Partnership Project), Standardisierungsgremium im Mobilfunkbereich, konkret: GSM, UMTS, LTE und der IETF (Internet Engineering Taskforce).
IETF Standardisierung sichert nicht die Interoperabilität, Bsp.: SIP-RFC Clients müssen nicht denselben Codec unterstützen.
Nur die Interfaces und Ressourcen werden standardisiert. Keine Standardisierung von Multimedia-Anwendungen.

5.5 Zählen Sie die wesentlichen Komponenten der IMS Architektur auf und beschreiben Sie (kurz!) deren wesentliche Aufgaben – Schwerpunkt SIP Proxies und IMS Datenbanken.

Call Control Einheiten:

- CSCF: Call-Session Control Function
- Proxy CSCF (P-CSCF)
- Interrogating CSCF (I-CSCF)
- Serving CSCF (S-CSCF)

Database Coponents:

- Home Subscriber Server (HSS)
- Subscriber Location Function (SLF)

Application Server:

- SIP-AS
- OSA-SCS
- IM-SSF

Media Ressource:

- MRFC
- MRFP

PSTN-Connectivity:

- BGCF
- MGCF
- SGW
- MGW

P-CSCF:
Verifiziert die Korrektheit und Integrität von SIP-Nachrichten, baut eine sichere Verbindung zum Ueser Equippment auf, komprimiert u. dekomprimiert Signalisierung, Abrechnungen

I-CSCF:
SIP-Proxy, Befindet sich am Rand einer Verwaltungszone, ist in DNS registriert, Leitet SIP-Requests an Ziele innerhalb seiner Verwaltungszone weiter, Empfängt Routing-Information von HSS, Kann für Topolgy-Hiding verwendet werden, weist einem Benutzer die S-CSCF zu

S-CSCF:
SIP-Registrar, Proxy, “Gehirn” von IMS, I-CSCF weist eine S-CSCF einem Benutzer während dem ersten IMS-Registrierungsvorgang zu, Registriert und Authentifiziert IMS-Benutzer

Datenbanken:
HSS: Speichert Benutzerdaten (Registrierungsdaten, Authentifizierungstokens, Initial Filter Criteria), S-CSCF alloziert für den Benutzer
SLF: Subscriber Location Function, wird benötigt, wenn ein Anbierter mehr als eine HSS verwendet, Bildet die Benutzeridentität auf dem HSS ab, der die Benutzerdaten speichert.

Application Server:
Führt die IMS-Services aus (AAM, Call-Redirect,..) wird vom Betreiber, oder von einem Drittanbieter zur Verfügung gestellt. Kommunizieren über SIP mit dem S-CSCF.
Media Ressource:
Bietet Ressourcen und Steuerung für Medienströme in IMS

CS-Interworking:
Interface zu CS-Netzwerken (PSTN)

5.6 Vergleichen Sie IMS mit IETF SIP, besprechen Sie Vorteile und Nachteile der beiden Ansätze.

?Bei IMS Zugriff auf Registrar immer über Proxy, Adresse wird von Proxy vergeben.
IMS aufwendiger als SIP, auch Multimedia in IMS, Unterteilung der Netze je nach Anbieter?

5.7 Mit welchem (aus der Mobil Telekommunikation bekannten) Konzept möchte IMS weltweite Verfügbarkeit erreichen?

GSM/GPRS Konzept wird wiederverwendet – Home network, visited network (ROAMING)
GGSN (Gateway GPRS Support Node) immer im gleichen Netz wie P-CSCF

Home Network: Infrastruktur die vom Heimnetzbetreiber zur Verfügung gestellt wird.
Visited Network: Infrastruktur eines Anbieters mit Roamingvertrag mit dem Heimnetzanbieter.

5.8 Welche zwei wesentlichen Topologien kennt IMS bezogen auf Positionierung der Signalisierungskomponenten in Heim und Fremdnetzen? Welches sind die Vor und Nachteile der beiden Varianten?

Visited Network GGSN (Gateway GPRS Support Node) – P-CSCF und GGSN im Visited Netz, Medien-Daten werden direkt geroutet, keine Kontrolle.
Home Network GGSN: P-CSCF u. GGSN im Home Network, Medien über Home Network geroutet, gute Kontrolle, hoher Overhead, hohe Verzögerung

5.9 Welche IMS Komponenten sind beim Routing einer SIP Nachricht im IMS Netz immer im SIP Signalisierungspfad?

End-2-End SIP-Session in IMS:
P-CSCF - I-CSCF (+HSS) - S-CSCF - I-CSCF (+HSS) - S-CSCF - P-CSCF

5.10 Auf welchen Komponenten werden Dienste (Services) in IMS implementiert? Welche Komponente bindet diese Dienste in den Signalfluss ein (mittels welcher Mechanismen).

Auf Application-Server, werden vom Betreiber oder von einem Drittanbieter zur Verfügung gestellt.

- SIP-AS, Native IMS/SIP Application Server
- OSA-SCS
- IMS-SSF

Alle drei Application-Server-Typen kommunizieren per SIP-Interface mit dem S-CSCF.

5.11 Was versteht man unter IFCs? In welcher IMS Komponente sind sie gespeichert? Erläutern Sie die Beziehung zwischen IFC, AS und S CSCF.

Initial Filter Criteria - sind im HSS gespeichert, bei Registrierung eines Benutzers, lädt der S-CSCF die Benutzerdaten vom HSS. Die Filter Criteria bestimmen die Services, die vom User ausgeführt werden dürfen. Bsp. INVITE. Wird die Anfrage bestätigt (Trigger wird ausgelöst), geht der Request weiter zum AS.

5.12 Was versteht man in IMS unter Identitäten? Beschreiben Sie kurz die bei IMS definierten und verwendeten Typen/Arten von Identitäten, bzw. deren Notwendigkeit. Wo ist die Information bezüglich Identität eines IMS Nutzers gespeichert?

Identitäten sind unbedingt erforderlich, um Benutzer eindeutig zu identifizieren (vgl. Telefonnummer, oder GSM-IMSI).

Es gibt 3 Arten von Identitäten:

- Public ID: Wird benötigt, um kontaktiert zu werden, mehrere Public IDs können dem selben Benutzer zugewiesen sein (bspw. SIP-URI, und Tel-URL). Zumindest eine SIP-URI oder Tel-URL ist einem Benutzer zugewiesen.
- Private ID: für IMS-interne Identifikation, öffentlich nicht sichtbar, dem User unbekannt, benötigt für IMS-Authentifizierung
- Public Service ID: Ähnlich der Public ID, jedoch nicht einem Benutzer zugewiesen, sondern einem Service, SIP-URI, oder Tel-URL, typischerweise von einem AS gehostet. Public Service-IDs werden nicht authentifiziert, es gibt keine zugehörige Private-ID.

Auf HSS gespeichert.

5.13 Wofür benötigt man eine temporäre Identität in IMS?

Wird in IMS ein Terminal mit einer UICC (Universal Integrated Circuit Card) ohne ISIM (IP Multimedia Services Identity Module) betrieben, so wird aus der USIM eine Temporary Public ID und Temporary Private ID gebildet, die es erlauben mittels REGISTER den Benutzer am Heimnetz zu registrieren. Wird nur während der Registrierung und De-Registrierung verwendet.

5.14 Welche beiden wesentlichen, in der Vorlesung vorgestellten Varianten von Vergebührung (Charging) unterstützt IMS? Wo liegt der Unterschied? Welches der beiden Systeme ist aus technischer Sicht anspruchsvoller (Begründung!)?

- Offline-Charging

Vergebührungsinformation wird hauptsächlich NACH einer Sitzung gesammelt. Der User erhält

Rechnungen monatlich.

- Online-Charging

IMS-Einheiten interagieren mit dem Online-Vergebührungssystem, es wird in Echtzeit vergebührt

Online-Charging ist anspruchsvoller, da sie in Echtzeit abgewickelt werden muss.