MULTIMEDIA KOMMUNIKATION

Teil 1: Standardisierung

1) Weshalb gibt es Standardisierung?

Interoperabilität (Fähigkeit zur Zusammenarbeit von verschiedenen Systemen, Techniken oder Organisationen) : standardisierte Schnittstellen (Interfaces), Fokus auf Benutzerfreundlichkeit, verbesserte Kundenerfahrung, Anstieg von Kundenanzahl

2) Aspekte der Standardisierung: Was soll/kann/muss standardisiert werden (Software, Hardware, Schnittstellen)? Vorteile und Nachteile?

Aspekte der Interoperabilität: Hardware und Software, Anbieter, Anwender, Staat, kontinental, trans-kontinental

Telekommunikationsstandardisierung ist sehr komplex – es gibt viele Standardisierungsorganistaionen und –foren, unterschiedliche Standardisierungsprozesse, viele Dokumenttypen, unterschiedliche Dokumentenbennenung und –nummerierungsschemen

3) Standardisierung: wählen Sie eine der vier in der Vorlesung näher besprochenen Standardisierungsorganisationen und beschreiben Sie deren Aktivität (alle folgenden Punkte betreffen diese gewählte Organisation):

a. **Wie heißt die Organisation, wofür steht die Abkürzung?**

Internet Engineering Task Force (IETF)
International Telecommunication Union (ITU)
European Telecommunications Standards Institute (ETSI)

3rd Generation Partnership Project (3GPP) - Mitglieder: ETSI (Europa), ARIB (Japan), CCSA (China), ATIS (US), TTA (Korea), TTC (Japan)

b. Beschreiben Sie den Schwerpunkt der Standardisierungs-Aktivitäten

Die **Internet Engineering Task Force** (**IETF**) ist eine Organisation, die sich mit der technischen Weiterentwicklung des Internets befasst, um dessen Funktionsweise zu verbessern. Ihr Auftrag ist die Erstellung hochqualitativer, relevanter technischer Dokumente, welche die Art und Weise beeinflussen, wie Menschen das Internet weiterentwickeln, benutzen und verwalten. Diese Dokumente umfassen Internetprotokollstandards, Beschreibungen momentan bekannter Verfahren sowie verschiedener Dokumente mit eher informativem Charakter. IETF kümmert sich um die kurzfristig zu lösenden Probleme des Internets, insbesondere um die Standardisierung der im Internet eingesetzten Kommunikationsprotokolle

Die Ziele der **ITU** sind Abstimmung und Förderung der internationalen Zusammenarbeit im Nachrichtenwesen durch:

- Internationale Zuweisung und Registrierung von Sende- und Empfangsfrequenzen und Rufzeichenblöcken
- Internationale Regelungen für die Nutzung von Frequenzen
- Koordinierung von Bemühungen zur Störungsbearbeitung im internationalen Funkverkehr
- Koordinierung der Entwicklung von Fernmeldeanlagen
- Vereinbarungen von Leistungsgarantien und Gebühren

(Weltweit gültige Standards im Bereich der Telekommunikation, Schwerpunkt Festnetze)

ETSI: ursprüngliches Ziel: Koordination und Produktion von europäischen Standards mit dem Hauptziel einen homogenen europäischen Telekommunikationssektor zu ermöglichen . Zusätzlich: Produktion von global einsetzbaren Standards für Informations- und Kommunikationstechnologien
Hauptleistungen im globalen Standard: GSM (Global System for Mobile Communication) und UMTS (Universal Mobile Telecommunications System)

3GPP: Produktion von global anwendbaren Standards für ein 3rd Generation Mobile System, Erhaltung und Entwicklung des GSM Standards inklusive entwickelter radio access. Technologien (zB GPRS, EDGE)
Verantwortlich für IP Multimedia Subsystems (ISM) – Haupt-NGN-Kandidat für den Ersatz gängiger mobiler cellular Netzwerke

c)Wer kann sich bei der Standardisierung beteiligen, wer kann Standards vorschlagen, Voraussetzungen um mitzuwirken?

IETF:
Der Entwurf jedes RFC, den man als Internet- Draft bezeichnet, wird innerhalb der IESG (Internet Engineering Steering Group) diskutiert. Ein Internet- Draft (typischerweise 6 Monate gültig) wird nur mit der Zustimmung der IESG als Internet-Standard, also als RFC, veröffentlicht. IESG arbeitet mit dem RFC- Editor zusammen, der für die Veröffentlichung von RFCs zuständig ist). Jeder kann einen neuen ID vorschlagen.

ITU:
(ITU Mitglieder - Jahresbeitrag)

ETSI:
Mitglied bei ETSI können Verwaltungen, Netzbetreiber, Hersteller, Anwender oder Dienstanbieter werden. Beispiele für ETSI-Standards: GSM, UMTS

3GPP
arbeitet eng mit ITU-T und ETSI zusammen. „aktive“ Unternehmen und Hersteller um technische Spezifikationen für die sog. dritte Generation (3G) der Mobilfunknetze – also für UMTS – zu entwickeln

d.Wie heißen die Standards und verwandte Dokumente bei der gewählten Organisation?

Die IETF-Dokumente werden als sog. RFCs (Requests for Comments) im Internet veröffentlicht. Der Entwurf jedes RFC nennt man Internet- Draft.

ITU: Recommendation, Draft

ETSI Technical Specifications (ES) - Standard Document, ETSI Technical Guide (EG), ETSI Special Report (SR), ETSI Technical Report (TR) – Informative Document ("best practice"), ETIS Group Specification (GS)

3GPP: Document stages: Architecture (Stage 1), Function (Stage 2), Implementation (Stage 3)
Technical Specifications – TS, Standards
Technical Report – TR, "best practice")

e. Beschreiben Sie (kurz!) den Standardisierungsprozess.

IETF:
1. Konzept, Idee
2. eine Gruppe von Leuten kontaktiert die entsprechende IETF Arbeitsgruppe
3. jemand bereitet/korrigiert einen Internet Draft entsprechend der formalen ID Anforderungen vor
4. ID wird veröffentlicht (Kommentare von Arbeitsgruppenmitgliedern, …)
5. Bei Übereinstimmung und IESG Zustimmung kontaktiert man den RFC Editor zur Veröffentlichung → RFC
6. bei neuem Input oder Änderungswünschen muss man wieder zu Punkt 3
7. Draft verfällt

ITU
1. ITU Draft wird ausgearbeitet und diskutiert innerhalb der SGs oder WPs
2. wenn beschlossen ist, dass es ausgereift ist erfolgt ein Review bei einem Meeting
3. Wenn es bewilligt wird, wird das Draft zur Anerkennung eingereicht und es erfolgt ein finaler Review.
4. wenn die Mitglieder keine Einwände haben wird dem Draft zugestimmt und es wird zu einer Recommandation.

ETSI
General assembly: höchste entscheidungsbefugte Autorität
Board: Vollzugsarm der general assembly
Technical Bodies: technische und spezielle Komitees, Projekte, Partnerprojekte Sekretariat

3GPP
Stufe 1: Servicebeschreibung von der Sicht eines Servicebenutzers
Stufe 2: logische Analyse und Information fließen auf einem funktionalen Elementlevel
Stufe3: konkrete Implementation der Protokolle zwischen Physikalischen Elementen auf denen die funktionalen Elemente gemapped wurden

f. Was geschieht, wenn man einen Fehler in einem Standard dieser Organisation entdeckt?

IETF
Wenn ein Fehler gefunden wird Errata bzw. es wird ein neuer RFC Standard geschrieben. Ein veröffentlichtes RFC wird niemals geändert.

alle anderen haben Versionierungsmechanismen

g. Welche Versionierungsmechanismen gibt es für Standards dieser Organisation?

IETF hat keine Versionierungsmechanismen.

ITU: Primitiv, eindeutige Kennzeichnung über Jahr- und Monat der Verabschiedung des Standards

ETSI: Nummer basierte Versionisierung. (major / minor releases))

3GPP: Dokument Notation: TS xx.yyy a.b.c
Gültig für beide Technical Specification und Technical Reports
xx: series number, yyy: specification within series
a: 3GPP Release (if > 3; 1=inform, 2=for approval), b: Major version, c: Minor version

Teil 2: Vermittlungstechnologien

1) **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.**

Analoge Telefonie (In-Band) - Einfachheit, anfällig für Störungen

Digitale Telefonie (ISDN, eigener Signalisierungskanal, Out-of-Band) - Eigene Signalisierung, Störfreiheit, dafür höhere technische Komplexität.)

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

File von Computer A zu Computer B -> File in kleine Pakete aufgeteilt (jedes Paket enthält Ursprung (Start), Ziel, und Platz im Originalfile) -> Pakete auf Routen verschickt -> am Ziel wieder zusammengebaut

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

ein durchgeschalteter Übertragungskanal mit konstanter Bandbreite zugeordnet wird, der dieser Verbindung dann zur exklusiven Nutzung zur Verfügung steht, auch wenn keine Informationen übertragen werden.Das wohl bekannteste Netz, das Verbindungen mit Leitungsvermittlung herstellt, ist das klassische Telefonnetz.Die Verbindung wird im Regelfall aufgrund der von der rufenden Endstelle eingegebenen Zielinformation aufgebaut, bevor der eigentliche Nachrichtenaustausch beginnen kann. Nach Beenden des Nachrichtenaustausches erfolgt ein Abbau der Verbindung. Die Steuerung des Auf- und Abbaus der Nachrichtenverbindungen wird von den Vermittlungsstellen vorgenommen. Sie tauschen zu diesem Zweck mit den Endstellen bzw. untereinander Steuerinformationen aus, was als Zeichengabe oder Signalisierung bezeichnet wird.

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

Paketvermittlung: fehlertolerant, flexibel auf Last reagierend, skaliert gut – jedes Paket muss einzeln geroutet werden, daher Overhead, bzw. Best-effort-Service und Jitter. shared usage of physical connection, different or same bit rate at each end

Leitungsvermittlung: Verbindungsaufbau zeitintensiv, Ressourcen müssen dediziert alloziert werden und stehen anderen Teilnehmern nicht mehr zur Verfügung. Dafür aber garantierte Bandbreite, konstanter Delay, kein Jitter. same bit rate at each end

5) Vergleichen Sie die Positionierung der Intelligenz und Kontrolle in Leitungs- und Paketvermittelten Netzen.

Paketvermittlung: Intelligenz bei den Endgeräten
Leitungsvermittlung: Intelligenz im Kernnetz

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

Leitungsvermittlung: 99,999%
Paketvermittlung: ca. 99% LAN, 99,99% Backbone

five-nines: sehr hohe Verfügbarkeit 99,999 % - ca. 5 Minuten pro Jahr nicht verfügbar)

7) Wofür wird ICMP verwendet? Geben Sie ein Beispiel eines häufig verwendeten Programms, das auf ICMP aufbaut.

Internet Control Message Protocol (ICMP):
RFC 792, ICMP reagiert mit Fehler- und Kontroll-Meldungen bei fehlerhaftem IP Betrieb, ICMP 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

Übertragung von Steuerung und Status der Information, aktuell ist ICMP eine adressierbare Applikation bei gut gewussten Ports, Aber nicht geeignet als Transport Protokoll, typischerweise implementiert innerhalb operating systems/IP stacks
Beispiel für Programm: PING

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

IPv6 Adressen werden eingeführt weil bald keine IPv4 Adressen mehr zur Verfügung stehen. Versäumnis: es wurde nicht mit so einer rasanten Wachstum des Internets gerechnet. Durch die mit der Zeit mehrmals geänderte Vergabepraxis von IPv4-Adressraum ist dieser inzwischen stark fragmentiert, d. h. häufig gehören mehrere nicht zusammenhängende Adressbereiche zur gleichen organisatorischen Instanz.
lange Routingtabellen, Prozessorbelastung durch Prüfsummenberechnung, Probleme beim Unterstützen von neuen Services

9) Welches sind die wesentlichen Eigenschaften bzw. Neuerungen von IPv6 verglichen mit IPv4?

Vergrößerung des Adressraums
IPv6-Adressen werden gewöhnlicherweise hexadezimal (IPv4: dezimal) notiert, wobei die Zahl in acht Blöcke zu jeweils 16 Bit unterteilt wird. Diese Blöcke werden durch Doppelpunkte (IPv4: Punkte) getrennt notiert
Autokonfiguration von IPv6-Adressen (stateless)
Mobile IP und vereinfachtes Renumbering (Umnummerierung)
Dienste wie IPSec, QoS und Multicast werden von Haus aus unterstützt
Vereinfachung und Verbesserung des Protokollrahmen, genauer gesagt der Kopfdaten. Diese Informationen sind für Router sehr wichtig.

10) Zählen Sie die von IPv6 unterstützten Adress- bzw. Adressierungsarten auf und beschreiben Sie sie kurz.

Wie können die Päckchen verschickt werden ?
Unicast Adressierung: Ein Paket wird einem Interface zugestellt
Multicast Adressierung: Ein Paket wird mehreren Interfaces zugestellt.
Anycast Adressierung: Ein Paket wird den nächst nähren Interfaces zugestellt (basierend auf der Routing Distanz)

An wen können die Päckchen verschickt werden ?

Link-local: An alle Knoten im selben Subnetz
Site-local: An alle Knoten in der Organisation
Global: An alle IPv6 Knoten

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

IPv6 verfügt über Multicast Adressierung, d.h. man braucht keine eigene Adresse (Broadcast Adresse) mehr an die man ein Päckchen schicken muss, sondern verwendet einfach einen Multicast an den Link-Local (alle Knoten im selben Subnetz)

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

Adress Resolution Protocol (ARP): Netzwerklayer Protokoll, löst die IP Adresse auf die zugrundeliegende MAC Adresse auf, meistens benutzt für das Mappen von IP Paketen auf Ethernet Frames, ARP request generiert vom Host um MAC Adresse für nächsten Hop (Adresse des nächsten IP Routers) zu bestimmen

Das Reverse Address Resolution Protocol (RARP) ist ein Netzwerkprotokoll, das die Zuordnung von Hardwareadressen zu Internetadressen ermöglicht. Es gehört zur Vermittlungsschicht der Internetprotokollfamilie

Insbesondere wird das Address Resolution Protocol (ARP) durch das Neighbor Discovery Protocol (NDP) ersetzt.

13) Welche Adressierungsform wird in IPv4-Netzen und welche in Telefonienetzen verwendet?

IPv4 benutzt 32 bit Adressen; werden dezimal in vier Blöcken geschrieben
Telefonienetz ist nur nummernbasiert.

14) 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)?

Node ... Ein Gerät das IPv6 implementiert.
Ein Node kann entweder ein Router oder ein Host sein.
Ein Router ist ein Gerät das IPv6 Pakete weiterleitet, welche nicht an sich selbst adressiert sind.
Ein Host ist ein Node der kein Router ist.

Interface ... Ein Anbaugerät eines Nodes zu einem Link. (Netzwerkkarte)

15) 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?

2^{32} (≈ 4,3 Milliarden = $4{,}3 \cdot 10^{9}$) bei IPv4
2^{128} (≈ 340 Sextillionen = $3{,}4 \cdot 10^{38}$) Adressen bei IPv6

IPv6-Adressen sind 128 Bit lang (IPv4: 32 Bit)

16) 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.

Class A: Netze 0.0.0.0/8 bis 127.255.255.255
0 … 8-Bit-Netz 24-Bit-Host

Class B: Netze 128.0.0.0/16 bis 191.255.255.255
1 0 … 16-Bit-Netz 16-Bit-Host

Class C: Netze 192.0.0.0/24 bis 223.255.255.255
1 1 0 … 24-Bit-Netz 8-Bit-Host

Class D: Multicast-Gruppen 224.0.0.0/4 bis 239.255.255.255
1 1 1 0 28-Bit-Multicast-Gruppen-ID

Class E: Reserviert 240.0.0.0/4 bis 255.255.255.255
1 1 1 1 28 Bit reserviert für zukünftige Anwendungen

Zwei Host-Adressen fallen immer weg – die erste Adresse (zum Beispiel 192.168.0.0) bezeichnet das Netz selber, die letzte Adresse (zum Beispiel 192.168.0.255) ist für den Broadcast (alle Teilnehmer werden angesprochen) reserviert. Früher gab es fest vorgeschriebene Einteilungen für Netzwerkklassen mit einer festen Länge. Da diese Einteilung sehr unflexibel ist, wird seit 1993 vor allem im WAN hauptsächlich das Classless Inter-Domain Routing-Verfahren durchgeführt,

Classless Inter-Domain Routing (CIDR) beschreibt ein Verfahren zur effizienteren Nutzung des bestehenden 32-Bit-IP-Adress-Raumes für IPv4. Es wurde 1993 eingeführt (RFC 1518, RFC 1519, RFC 4632), um die Größe von Routingtabellen zu reduzieren und um die verfügbaren Adressbereiche besser auszunutzen.

Mit CIDR entfällt die feste Zuordnung einer IPv4-Adresse zu einer Netzklasse, aus welcher die Präfixlänge hervor ging. Durch die zusätzliche Angabe einer Netzmaske wird jetzt die IP-Adresse in den Netzwerk- und Hostteil aufgeteilt.

Bei CIDR führte man als neue Notation so genannte Suffixe ein. Das Suffix gibt die Anzahl der 1-Bits in der Netzmaske an. Diese Schreibform, z. B. 172.17.0.0/17, ist viel kürzer und im Umgang einfacher als die Dotted decimal notation wie 172.17.0.0/255.255.128.0 und ebenfalls eindeutig.

17) Welche Notationen werden für IPv4-Adressen verwendet und welche für IPv6? Geben Sie mindestens je ein Beispiel.

IPv4.....192.168.0.23 (Dezimal, Punkte)
IPv6 ..... `2001:0db8:85a3:08d3:1319:8a2e:0370:7344` (hexadezimal, Doppelpunkte)

18) Weshalb kann man höchstens eine zusammenhängende Nuller-Gruppe in einer IPv6-Adresse ersetzen?

Es darf höchstens eine zusammenhängende Gruppe aus Null-Blöcken in der Adresse ersetzt werden. Die Adresse 2001:db8:0:0:8d3:0:0:0 darf demnach entweder zu 2001:db8:0:0:8d3:: oder 2001:db8::8d3:0:0:0 gekürzt werden; 2001:db8::8d3:: ist unzulässig, da dies fälschlicherweise z. B. auch als 2001:db8:0:0:0:8d3:0:0 interpretiert werden könnte

19) Wie wird eine IPv6-Adresse in eine URL eingebunden? Weshalb?

In einer URL wird die IPv6-Adresse in eckige Klammern eingeschlossen, z. B.:http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]/

Diese Notation verhindert die fälschliche Interpretation von Portnummern als Teil der IPv6-Adresse

20) Erklären Sie kurz „Private Netze“ im Zusammenhang mit IPv4-Adressen. Welche Vorteile und welche Nachteile hat diese Adressierungsform?

Private IP-Adressen gehören zu bestimmten IP-Adressbereichen, die im Internet nicht geroutet werden. Sie können von jedem für private Netze wie etwa LANs verwendet werden.
Die Idee, private Adressbereiche festzulegen, entstand aus dem Wunsch, ohne unnützen administrativen Mehraufwand lokale Netzwerke pflegen zu können.

Konfiguriert ein Administrator aus Unkenntnis einen öffentlichen, bereits Nutzern zugeordneten IP-Adressbereich in einem privaten Netz, so kann das Netz nicht auf den entsprechenden Bereich im Internet zugreifen. Außerhalb des privaten Netzes ergeben sich keine Schwierigkeiten.

Umgekehrt führt die Verwendung von privaten Adressbereichen regelmäßig zu Problemen, wenn etwa Firmen-LANs per VPN miteinander verbunden werden sollen und beide Standorte dieselben Netze verwenden

21) Durch welches Konzept wurden Private IPv4 Netze in IPv6 ersetzt?

Für private Adressen gibt es die *Unique Local Addresses* (ULA), beschrieben in RFC 4193. Derzeit ist nur das Präfix fd für lokal generierte ULA vorgesehen, mit dem Präfix fc werden in Zukunft wahrscheinlich global zugewiesene eindeutige ULA gekennzeichnet. Eine Beispiel-ULA wäre fd9e:21a7:a92c:2323::1. Hierbei ist fd der Präfix für lokal generierte ULAs, 9e:21a7:a92c ein einmalig zufällig erzeugter 40-Bit-Wert und 2323 eine willkürlich gewählte Subnet-ID.

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

0:0:0:0:0:ffff::/96 (80 0-Bits, gefolgt von 16 1-Bits) steht für *IPv4 mapped (abgebildete)* IPv6 Adressen. Die letzten 32 Bits enthalten die IPv4-Adresse. Ein geeigneter Router kann diese Pakete zwischen *IPv4* und *IPv6* konvertieren und so die neue mit der alten Welt verbinden.

2000::/3 (also alle Adressen von 2000:… bis 3fff:…) stehen für die von der IANA vergebenen globalen Unicast-Adressen, also routbare und weltweit einzigartige Adressen.

2001-Adressen werden an Provider vergeben, die diese an ihre Kunden weiterverteilen.

Adressen aus 2001::/32 (also beginnend mit 2001:0:) werden für den Tunnelmechanismus Teredo benutzt.

Adressen aus 2001:db8::/32 dienen Dokumentationszwecken, wie beispielsweise in diesem Artikel, und bezeichnen keine tatsächlichen Netzteilnehmer.

2002-Präfixe deuten auf Adressen des Tunnelmechanismus 6to4 hin.

Auch mit 2003, 240, 260, 261, 262, 280, 2a0, 2b0 und 2c0 beginnende Adressen werden von Regional Internet Registries (RIRs) vergeben; diese Adressbereiche sind ihnen z. T. aber noch nicht zu dem Anteil zugeteilt, wie dies bei 2001::/16 der Fall ist.[20]

3ffe::/16-Adressen wurden für das Testnetzwerk 6Bone benutzt; dieser Adressbereich wurde gemäß RFC 3701 wieder an die IANA zurückgegeben

23) 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.

Im Gegensatz zu IPv4 (Protokolltyp 4) hat der IP-Kopfdatenbereich (Header) bei IPv6 (Protokolltyp 41) eine feste Länge von 40 Bytes (320 Bits). Optionale, seltener benutzte Informationen werden in so genannten Erweiterungs-Kopfdaten (engl.: *Extension Headers*) zwischen dem IPv6-Kopfdatenbereich und der eigentlichen Nutzlast (engl. *Payload*) eingebettet.

Die meisten IPv6-Pakete sollten ohne *Extension Headers* auskommen, diese können bis auf den *Destination Options Header* nur einmal in jedem Paket vorkommen. Befindet sich

nämlich ein *Routing Extension Header* im Paket, so darf davor ein weiterer *Destination Options Header* stehen. Alle *Extension Headers* enthalten ein *Next-Header*-Feld, in dem der nächste *Extension Header* oder das *Upper Layer Protocol* genannt wird.

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

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

Stateless Adress Autoconfiguration - Geräte weise sich selbst eine Adresse zu und über diese Vergabe wird kein Buch geführt

Mittels des Autokonfigurationsprozesses kann ein Host vollautomatisch eine funktionsfähige Internetverbindung aufbauen. Dazu kommuniziert er mit den für sein Netzwerksegment zuständigen Routern, um die notwendige Konfiguration zu ermitteln.

Zur initialen Kommunikation mit dem Router weist sich der Host eine link-lokale Adresse zu, die im Falle einer Ethernet-Schnittstelle etwa aus deren Hardware-Adresse berechnet werden kann. Damit kann ein Gerät sich mittels des Neighbor Discovery Protocols (NDP, siehe auch ICMPv6-Funktionalität) auf die Suche nach den Routern in seinem Netzwerksegment machen. Dies geschieht durch eine Anfrage an die Multicast-Adresse ff02::2, über die alle Router eines Segments erreichbar sind (*Router Solicitation*).

Ein Router versendet auf eine solche Anfrage hin Information zu verfügbaren Präfixen, also Information über die Adressbereiche, aus denen ein Gerät sich selbst *Unicast*-Adressen zuweisen darf. An ein solches Präfix hängt der Host den auch für die link-lokale Adresse verwendeten Interface Identifier an.

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

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

28) Beschreiben Sie kurz Notwendigkeit und Funktionsprinzip von Fragmentierung bzw. Re-Assembling in IPv4-Netzen.

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

Teil 3: Transportebene

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

Verbindung bzw. Adressierung von Applikationen auf Hosts
notwendig für Fehlerkontrolle, Überlastschutz, Flusskontrolle

2) Welches 5-Tupel beschreibt eine Verbindung im Internet Protokoll Stack eindeutig?

(<SenderIP, SenderPort, DestIP, DestPort, Protocol>)

3) Beschreiben Sie kurz die wesentlichen Eigenschaften, Vorteile, Nachteile und Einsatzbereiche von UDP in Bezug auf Multimedia-Kommunikation (Signalisierung und Medienübertragung).

UDP (User Datagram Protocol): verbindungslos, packet stream, multicast support, nicht zuverlässig-optionale Fehlererkennung, keine Fehlerkorrektur und keine Sequenzierung.
Im Gegensatz zu TCP übermittelt man bei UDP Daten verbindungslos, d.h. ohne vorher eine virtuelle Verbindung aufzubauen. UDP gibt keine Garantie für die korrekte Übermittlung der Daten. UDP realisiert nur eine einfache Fehlerkontrolle. Bei UDP werden keine Quittungen verwendet, um beim Quellrechner eine erneuerte Übermittlung der am Zielrechner mit Fehlern empfangenen und demzufolge verworfenen UDP-Pakete zu veranlassen. Deswegen wird UDP vom RTP für die Übermittlung von Echtzeitmedien wie Audio und Video und vom SIP verwendet.

4) Welches sind die typischen Einsatzbereiche von UDP in der Praxis?

für Streaming Applikationen verwendet

5) Beschreiben Sie kurz die wesentlichen Eigenschaften, Vorteile , Nachteile und Einsatzbereiche von TCP in Bezug auf Multimedia-Kommunikation (Signalisierung und Medienübertragung).

(TCP (Transmission Control Protocol): verbindungsorientiert, byte stream, nur 1:1 Kommunikation, zuverlässig.
Ermöglicht es, virtuelle Verbindungen zwischen den kommunizierenden Rechnern auf- und abzubauen. Unter einer virtuellen Verbindung ist eine Vereinbarung zwischen zwei Applikationen zu verstehen, die vor der eigentlichen Kommunikation stattfindet und ihren Ablauf regelt. Somit stellt ein verbindungsorientiertes Transportprotokoll dar. Weil es mittels Fehlerkontrolle eine zuverlässige Datenübermittlung gewährleistet, kann TCP als Sicherungsprotokoll zwischen zwei Rechnern, die nicht direkt miteinander verbunden sind, angesehen werden.

6) Welches sind die typischen Einsatzbereiche von TCP in der Praxis?

Beispielsweise wird TCP als fast ausschließliches Transportmedium für das WWW, E-Mail und viele andere populäre Netzdienste verwende

7) Beschreiben Sie den Aufbau einer TCP-Verbindung. Weshalb ist dieser Aufwand notwendig?

Der Client, der eine Verbindung aufbauen will, sendet dem Server ein SYN-Paket (von engl. synchronize) mit einer Sequenznummer x. Der Server (siehe Skizze) empfängt das Paket. Ist der Port geschlossen, antwortet er mit einem TCP-RST, um zu signalisieren, dass keine Verbindung aufgebaut werden kann. Ist der Port geöffnet, bestätigt er den

Erhalt des ersten SYN-Pakets und stimmt dem Verbindungsaufbau zu, indem er ein SYN/ACK-Paket zurückschickt. Der Client bestätigt zuletzt den Erhalt des SYN/ACK-Pakets durch das Senden eines eigenen ACK-Pakets mit der Sequenznummer x+1. Aus Sicherheitsgründen sendet der Client den Wert y+1 (die Sequenznummer des Servers + 1) im ACK-Segment zurück. Die Verbindung ist damit aufgebaut.

Aufwand ist notwendig damit sichergestellt werden kann dass die gesendeten Pakete alle ankommen.

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

Sequenznummern für Sender und Empfänger – Erkennen von Paketverlusten, Flusskontrolle

9) Was ist die wesentliche Ursache für die „Sägezahnkurve“ bei der Übertragung mit TCP?

congestion marks bzw drosseln der übertragungsrate

10) Welches Transport-Protokoll wird für Echtzeit-Datenübertragung verwendet? Weshalb?

Für Echtzeit- Datenübertragung wird UDP bzw. DCCP verwendet.
UDP: sehr schlankes Protokoll, minimum Overhead, gut für MM- Datenübertragung – aber best effort, kein Fehlerschutz, Datagramm kann verloren/ umgeordnet/ dupliziert werden

11) 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.

Verlust eines Paketes erzwingt Warten auf dieses Paket trotzdem die darauf folgenden Pakete schon vorhanden sind

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

SCTP: Multi-Streaming, Multi- Homing, Message Boundary Preservation, Schutz gegen Syn-Flooding.
DCCP: Sequence numbers, Flow- Control für Sender Rate adaption

Teil 4: DNS, ENUM, SIP, usw.

1) **Wie war im Internet die Funktionalität von DNS VOR der Definition von DNS implementiert/realisiert?**

File in /etc/hosts, periodische Syncs mit zentralem File

2) **Was sind die wesentlichen Aufgaben von DNS? Was waren die wesentlichen Ziele bei der Definition von DNS?**

Mapping von Names auf verschiedenste Resources. Wesentliches Ziel: allgemeine Anwendbarkeit, Skalierbarkeit, Performance, eindeutiger Namensraum

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

Domain-Namensraum: Der Domain-Namensraum hat eine baumförmige Struktur. Die Blätter und Knoten des Baumes werden als Labels bezeichnet. Ein kompletter Domainname eines Objektes besteht aus der Verkettung aller Labels eines Pfades.

Nameserver: Nameserver sind zum einen Programme, die Anfragen zum Domain-Namensraum beantworten, im Sprachgebrauch werden allerdings auch die Rechner, auf denen diese Programme laufen, als Nameserver bezeichnet.

Resolver: Resolver sind einfach aufgebaute Software-Module, die auf dem Rechner eines DNS-Teilnehmers installiert sind und die Informationen von Nameservern abrufen können. Sie bilden die Schnittstelle zwischen Anwendung und Nameserver.

4) Definieren Sie folgende DNS-Konzepte: DNS Zone, DNS Resolver, Root Server. Was versteht man unter einer DNS Zone? Was versteht man unter einem DNS Resolver?

DNS Zone: Die Informationen im Nameservern im DNS werden in Form atomarer Einheiten – die sog. Resource Records (RRs) bilden – abgespeichert. Ein Nameserver beinhaltet die RRs des ihm dauerhaft zugeordneten Namensraums, der typischerweise als Zone bezeichnet wird.

DNS Resolver: Ist der lokale Agent, der die DNS Abfragen bearbeitet. Er leitet Abfragen an den lokalen DNS-Server: z.B. Wie lautet die IP-Adresse für www.informatik.hs-fulde.de und erhält am Ende vom lokalen Nameserver die dem Rechner z.B. www.informatik.hs-fulda.de zugeordnete IP-Adresse und kann somit ein IP-Paket an den Rechner srv1 in der Subdomain informatik.hs-fulde.de senden.

Root Server: Der DNS-Baum besitzt ganz oben eine einzige Wurzel (Root), die man einfach Root nennt. Für den Namen Root ist „.“ (Punkt) reserviert

Frage 5+6 siehe oben!

7) **Wie findet ein Client bei der Namensauflösung den ersten zu kontaktierenden DNS Server?**

Der DNS Client ist eine Software auf dem Rechner eines Benutzers, mit deren Hilfe DNS-Server – als Nameserver bezeichnet – abgefragt werden, um Rechnernamen in IP-Adressen zu übersetzen. Der DNS-Server ist ein Programm in einem dedizierten Rechner, das auf eine entsprechende Datei – Resource Record (RR) genannt – zugreift, um die Anfragen des Clients zu beantworten

8) 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).

Art der Ressource – A, AAAA, CNAME, SRV, NAPTR

9) 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

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

E.164 Number Mapping – Aufläsung von E.164-Telefonnummern im IP-Netz, Mapping zu URIs – ist in DNS integriert

11) Nennen und vergleichen Sie die wesentlichen Merkmale von Telekom- und Internet-Architektur.

Telekom Architektur: Leitungsvermittlung, verbindungsorientiert, ITU-Standard, Long setup times – End-zu-End Verbindung muss erstellt werden, eine Menge von internal states (in jedem switch und anderen Netzwerkknoten), Services sind im Netzwerk integriert, zentralisierte Steuerung. High availabilty: 99,999% (5 Minuten pro Jahr nicht erreichbar)

Internet Architektur: Paketvermittlung, verbindungslos, IETF-Standard, begrenzte internal states, Services können von jedem hinzugefügt werden, (services by any node, users control their choice of services), keine zentralisierte Steuerung, high availability: backbone – 99,99% (50 Minuten pro Jahr nicht erreichbar), lokales Netzwerk: 99% (ein paar Tage im Jahr nicht erreichbar)

12) Wofür steht SIP? Erklären Sie die wesentlichen Funktionen, die SIP erfüllt.

Das **Session Initiation Protocol** (**SIP**) ist ein Netzprotokoll zum Aufbau, zur Steuerung und zum Abbau einer Kommunikationssitzung zwischen zwei und mehr Teilnehmern. Das Protokoll wird u. a. im RFC 3261 spezifiziert. In der IP-Telefonie ist das SIP ein häufig angewandtes Protokoll.

13) Genügt SIP um Telefongespräche über IP zu führen? Begründen Sie ihre Antwort!
Nein, weil es bloß die Kommunikationsmodalitäten aushandelt. Daten für Kommunikation müssen mit anderen Protokollen ausgetauscht werden. (zB SDP)

14) Mit welchen Transport-Protokollen ist SIP einsetzbar?

für die Medienübertragung wird das *Realtime Transport Protocol verwendet*

15) 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: Seine Aufgabe besteht darin, den Absender, von dem er den Request INVITE empfangen hat – wie z.B. IP-Telefon, Proxy-Server-, darüber zu informieren, in welcher Fremd-Domain sich der Angerufene aktuell aufhält. Ein Redirect Server informiert somit den Absender nur darüber, zu welcher Domain die bereits initiierte Session aufgebaut bzw. weitergeleitet werden soll.

Proxy Server: Seine wesentliche Aufgabe ist die Unterstützung der Mobilität, damit ein Benutzer – der Angerufene – sich zwischen verschiedenen DnS- Domains „bewegen“ und trotzdem erreichbar sein kann. Der Angerufenen kann seinen Heimat- Domain, die dem Anrufenden aus dem SIP-URI des Angerufenen bekannt ist, verlassen und sich als Gast innerhalb einer anderen Fremd-Domain aufhalten, die dem Anrufenden noch nicht bekannt ist. Ist der Angerufene in eine Fremd-Domain „umgezogen“, kommen beim Aufbau einer Session für die VoIP- Kommunikation mehrere SIP-Server zum Einsatz, mit deren Hilfe die ankommenden Anrufe in die Fremd- Domains weitergeleitet werden.

Weiterleitung eines Requests zu einem anderen Server oder User Agent und kann auch Requests zu mehreren Servers weiterleiten (forking proxy)

Stateless Proxy: leicht zu implementieren, fast processing of SIP messages, kann TCP nicht unterstützen, eigene provisional responses (1xx) müssen nicht generiert werden, kann für billing, forking, application control… nicht verwendet werden

Transaction Stateful Proxy: speichert den Zustand von jedem SIP transaction (wird für forking benötigt), kann eigene provisional responses (1xx) generieren, unterstützt TCP und UDP, kann für billing, forking, application control… nicht verwendet werden

Call Stateful Proxy: speichert den Zustand von jedem Call, wird für billing und für application control benötigt

AAA: Athentication, Authorization, Accounting

Registrar: Dieser Server stellt eine funktionelle Komponente dar, die in der Regel in einem Proxy-Server bzw. in einem Redirect- Server untergebracht wird. Der Registrar einer Internet- Domain enthält Angaben hinsichtlich der aktuellen Lokation von Benutzern seiner Domain.

Back-to-Back User Agent (B2B UA): Erweiterung von SIP-Proxy um zusätzliche Funktionen – wie z.B. für die Erfassung von anfallenden Gebühren. Im Unterschied zu einem „normalen“SIP-Proxy ist B2BUA in der Lage, nicht nur SIP-Responses, sondern auch SIP-Requests zu generieren, zu berarbeiten und hierbei auch ihre Body-Teile zu interpretieren. Daher kann er auch die Medienströme auf eine bestimmte Art und Weise beeinflussen. Ein B2BUEA enthält sowohl einen UAC als auch einen UAS und kann dadurch als UAC und als UAS dienen.
Beim Einsatz von B2BUAs bei VoIP Service Provider verlaufen in der Regel auch die Sessions über die beteiligten B2BUAs. Damit lässt sich der Verlauf der Kommunikation kontrollieren, und die anfallenden Gebühren können erfasst werden.

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

Das Nachrichtenformat besteht aus textuellen Beschreibungen und gliedert sich in Startzeile, Kopf, Leerzeile, Body

2 Typen von Nachrichten: SIP Request und SIP Response

17) Wie kann man SIP-Nachrichten vom Typ her klassifizieren (angelehnt an HTTP)?

2 Typen von SIP Nachrichten: SIP Request und SIP Response
beide Nachrichtentypen beinhalten folgende Komponenten: Startline, verschiedene Messageheader, Emptyline (CRLF), einen optinalen Nachrichtenbody (zB SDP)

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

Provisional (1xx) – Anfrage erhalten, fortfahren mit Verarbeitung des Anfrage
Success (2xx) –die Anfrage wurde akzeptiert
Redirection (3xx) – weitere Aktionen müssen gemacht werden um die Anfrage zu vervollständigen
Client-Error (4xx) – die Anfrage beinhaltet schlechte Syntax oder kann nicht ausgeführt werden auf diesem Server
Server-Error (5xx) – der Server konnte die Anfrage nicht ausführen
Global Failure (6xx) – die Anfrage kann auf keinem Server ausgeführt werden

19) 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?

User Agent, UA – UAC, UAS, vereinfachte Protokollmaschinen und Implementierung

20) 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

21) 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)

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

Einfacher Anruf ohne Proxy:
Invite → Ringing → OK → ACK → Data → BYE → OK

23) Welche Mechanismen verwendet SIP um Paketverluste auszugleichen?

Timers und Retransmissions

24) Welche Funktion erfüllt die Registrierung in SIP?

Ein Benutzer sollte (technisch gesehen) die Möglichkeit haben, verschiedene Rechner – nicht nur in seiner Domain, sondern auch in anderen Domains – als sein IP- Telefon nutzen zu können. Um eine derartige Mobilität von Benutzern bei VoIP mit SIP zu unterstützen, kann ein Benutzer einen permanenten SIP- URI in seiner Heimat- Domain (als Address of Record (AoR) bezeichnet) und einen vorläufigen SIP-URI – sogar in einer Fremd-Domain – besitzen.
Unter einer Registrierung bei SIP versteht man daher einen Vorgang, bei dem ein Benutzer auf dem SIP-Registrar eine Zuordnung AoR aktueller SIP-URI speichern lässt. Damit teilt er dem Registrar mit, dass er aktuell nicht unter seinem AoR erreichbar ist, sondern vorläufig unter dem angegebenen aktuellen SIP-URI

25) 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)?

Über DNS oder Route-Header wird jeweils der nächste SIP-Hop bestimmt, alle Knoten tragen sich im Via-Header ein. Route der Response ist inverse Via-Route

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

27) Erklären Sie mittels Sequenzdiagrammen das unterschiedliche Verhalten der drei in SIP vorgesehenen Proxy-Varianten.

Forwarding Proxy, Redirect Proxy, Forking Proxy

28) Welche Protokolle werden typischerweise gemeinsam mit SIP für Multimedia-Kommunikation eingesetzt? Weshalb?

Als Transportprotokoll können UDP, TCP, SCTP und DCCP verwendet werden, wobei standardmäßig UDP genutzt wird, da der Aufbau einer Session effizienter und viel schneller ist.
RTP: Über eine SIP zwischen zwei Rechnern aufgebaute 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?

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

Session Description Protokoll (SDP)

definiert durch Multiparty Multimedia Session Control (MMUSIC) WG der IETF
SDP: beschreibt Multimedia Sessions, textbasiert, es ist mehr ein Sessionbeschreibungsformat als ein Protokoll

30) Beschreiben Sie die Probleme von SIP im Zusammenhang von NAT. Welche Lösungen gibt es?

ALG (Application Level Gateways - Service innerhalb des NAT) oder andere Vorkehrungen notwendig um SIP über NAT zu bringen – IP-Adresse und Portnummer in SDP-Info enthalten)
STUN, TURN, ICE,….

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

Es muss zuerst eine Session aufgebaut werden und danach findet die Sprachübermittlung statt. Nach Ablauf der Kommunikation muss die bestehende Session wieder abgebaut werden, um die vorher belegten Netzressourcen freizugeben.
Die Verbindungs- Parameter werden mittels SDP festgelegt.

32) 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.

33) Auf welches Transport-Protokoll setzt RTP auf?

RTP ist ein Paket-basiertes Protokoll und wird normalerweise über UDP betrieben.

34) Welche für Echtzeit-Datentransport wesentlichen Informationen enthält der RTP-Header?

Jedes RTP-Paket enthält einen RTP-Header und einen Payload-Teil.

PT (Payload-Type, Nutzlasttyp): Hier wird angegeben, um welches Format es sich beim als Nutzlast transportierten Medium handelt, d.h. nach welchem Verfahren dieses Medium codiert wurde.

Timestamp: Der Zeitstempel ist vom Payload-Typ abhängig und gibt den Zeitpunkt des Beginns des ersten Payload-Oktetts im RTP-Paket an. Der Zeitstempel wird benötigtl, um beim Empfänger Schwankungen der Übertragungszeit (sog. Jitter) von RTP-Paketen ausgleichen zu können.
Sequence Number: Jedes RTP-Paket wird mit einer Sequenznummer versehen, die es dem Empfänger erlaubt, den Verlust von Paketen festzustellen bzw. die richtige Reihenfolge der Pakete wiederherzustellen, falls sie in einer falschen Reihenfolge angekommen sind. Der Anfangswert der Sequenznummer wird zufällig ausgewählt, um eine unbefugte Entschlüsselung zu erschweren.

Optional: CSRC (Contributing Source Identifier), Header Extension

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

36) Welche Funktion erfüllt der Jitter-Buffer in der Echtzeitkommunikation? Welche Vorteile und welche Nachteile hat er?

Ausgleich von Jitter, d.h. variablem Delay in paketvermittelten Netzen. Ermöglicht Verbergen von Verlusten bzw. spät eintreffenden Paketen, erhöht E2E- Delay

37) Welche Information im RTP-Header ist für die Bearbeitung des RTP-Pakets im Jitter Buffer wesentlich?

Timestamp, 32 bit
Der Zeitstempel gibt den Zeitpunkt des ersten Oktets des RTP-Datenpakets an. Der Zeitpunkt muss sich an einem Takt orientieren, der kontinuierlich und linear ist, damit die Synchronität des Streams sichergestellt und Laufzeitunterschiede der Übertragungsstrecke (Jitter) ermittelt werden können. Der Startwert sollte wie die Sequenznummer ein zufälliger Wert sein. Aufeinanderfolgende Pakete können den gleichen Zeitstempel haben, wenn die transportierten Daten z. B. zum selben Videoframe gehören. Pakete mit aufeinanderfolgenden Sequenznummern können aber auch nicht aufeinanderfolgende Zeitstempel enthalten, wenn wie z. B. bei komprimiertem Video Übertragungs- und Wiedergabereihenfolge nicht übereinstimmen.

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

Über DNS oder Route-Header wird jeweils der nächste SIP-Hop bestimmt, alle Knoten tragen sich im Via-Header ein. Route der Response ist inverse Via-Route

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

PSTN-SIP Gateway notwendig, setzt SIP Signalisierung auf ISDN/ISUP um. Gateway ist auf der einen Seite UA, auf der anderen CS-Teilnemer. Medien werden in Media Gateway terminiert, ggf. Transcoding notwendig

Teil 5: IMS

1) Welche Vorteile und Nachteile bietet eine "All-IP"-Infrastruktur gegenüber derzeitigen Kommunikationsnetzen?

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

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

Vertikal: Stovepipes, alle Layer werden neu implementiert in Server und Terminal
Horizontal: Middleware- Ebene in Terminal und Server unterstützt Entwickler

3) Wer standardisiert IMS? Welche anderen wichtigen Technologien werden von der gleichen Organisation standardisiert?

Das Konzept von IMS und seine Protokolle wurden im 3GPP (Third Generation Partnership Program) und von der ETSI-Arbeitsgruppe TISPAN (Telecommunication and Internet Converged Services and Protocols for Advanced Networking) weiterentwickelt und in verschiedenen ETSI- Dokumenten spezifiziert.
Von dieser Organisation wird UMTS, GSM, … standardisiert

4) Was ist IMS? Welche Bereiche umfassen die IMS-bezogenen Standards?

Das **IP Multimedia Subsystem** (**IMS**) ist eine Sammlung von Spezifikationen des 3rd Generation Partnership Project (3GPP). Ziel von IMS ist ein standardisierter Zugriff auf Dienste aus unterschiedlichen Netzwerken. IMS unterstützt aber auch bestehende Netze wie GSM oder das herkömmliche analoge und das digitale (ISDN-)Telefonnetz. Typische Dienste sind VoIP-Telefonie oder Präsenzinformationen. Das Basisprotokoll von IMS ist das SIP, welches über ein dediziertes IP-Netz Verbindungen zwischen den Teilnehmern aufbaut.

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

ein Release spezifiziert die Gesamtmenge der standardisierten Features – nicht beschränkt auf IMS; deckt Architektur, Services, Access, Core,… ab
3GPP Dokumentnamen folgen einer speziellen Notation – Valide Nummerierung sowohl für TS als auch für TR

TS xx.yyy → xx: Seriennummer; yyy: Spezifikation innerhalb der Serie (zB TS 22.228: Service Anforderungen für das IMS Core Netzwerk) Technical Reports (TR, best-practice)

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

P- CSCF (Proxy Call-Session Control Function): SIP Proxy, First Point of Contact to User Equipment, Inbound/ Outbound Proxy für UE, Verifiziert SIP Nachrichten Richtigkeit, generiert Gebühren Aufnahmen

I- CSCF (Interrogating CSCF): SIP Proxy, an der Spitze von der administrativen Domäne lokalisiert, im DNS registriert, routet SIP requests to den Destinationen innerhalb der administrativen Domäne, fragt Routing Informationen beim HSS ab
S- CSCF (Server CSCF): SIP Registrar, Proxy, "Brain" vom IMS, registriert IMS user, nach der Registration ist S-CSCF für routing von allen signalling traffic für den betreffenden user verantwortlich.
UE: (User Equipment)
HSS (Home Subscriber Server): speichert User Data
AS (Application Server)- evtl.): führt IMS Services aus

7) **Vergleichen Sie IMS mit IETF SIP, besprechen Sie Vorteile und Nachteile der beiden Ansätze.**

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

Heimnetz und Fremdnetz, Home Network und Visitied Network, bzw. Roaming – Verwenden der Infrastruktur anderer Betreiber

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

10) Welche IMS-Komponenten sind beim Routing einer SIP-Nachricht im IMS-Netz immer im SIP- Signalisierungspfad?

Anrufkontrolleinheiten: CSCF (Call-Session Control Function)

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

Application Server – AS.S-CSCF bindet Dienste ein, mittels Initial Filter Criteria

12) 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, in HSS gespeichert und in S- CSCF geladen. IFCs werden von S- CSCF geladen und von dieser verwendet, um AS in IMS/SIP Signalisierungspfad einzubinden

13) 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?

URIs (Uniforum Ressource Identifier) die aus Zahlen (zB. Telefonnummern) oder alphanumerischen Zeichen (zB SIP Adresse) bestehe können

öffentliche Identität: Identität benötigt um User zu kontaktieren - Telefonbenutzer sind möglicherweise nicht fähig die sip URI zu wählen), verschiedene öffentliche Identitäten sind möglicherweise dem selben User zugeteilt (abhängig von der Userrolle, zB Geschäftsidentität und Personalverwendungsidentität), Tendenz (Zumindest eine SIP URI und eine Tel URL sind einem User zugeteilt

private Identität: für IMS interne User / Terminal Identifikation - Format: username@operator.com), nicht öffentlich sichtbar, nicht für routing verwendet, User nicht bekannt

öffentliche Service Identität: ähnlich der öffentlichen Identität aber nicht einem Service anstatt zu einem Subscriber zugewiesen - SIP URI oder Tel URI (sip: chatroom13@operator.net, tel: +43-800-100100), typischerweise gehosted durch einen Applikationsserver, öffentliche Service Identitäten sind nicht autentifiziert

Private Identity: Systeminterne Identifikation, Public Identity: Sichtbarkeit User nach außen hin. Weltweit eindeutige Identifizierung. Gespeichert in SIM und HSS

14) Wofür benötigt man eine temporäre Identität in IMS?

15) 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!)?

Online Charging – Prepaid,
Offline Charging – Postpaid.
Online- Charging ist anspruchsvoller, Bearbeitung in Echtzeit notwendig