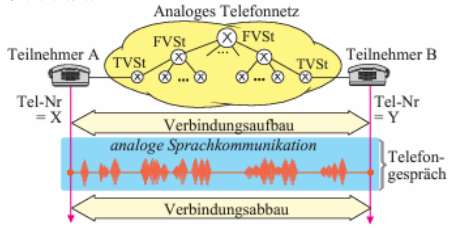
1 PSTN

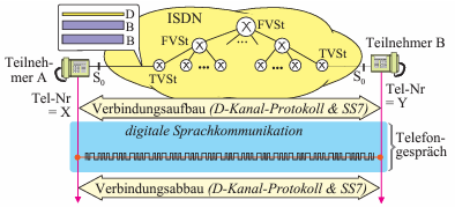
(Public Switched Telephone Network)
-300-3400Hz Sprachsignalen
-bis 4000Hz mit Signalen
-Öffentlichesnetz



-TVSt (Teilnehmer Verbindungsstelle)
-OVSt (Orts-VSt) - FVSt (Fern)

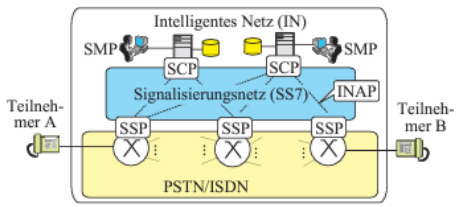
2 ISDN

(Integrated Services Digital Network)
-Vor der Kommunikation muss eine Verbindung aufgebaut werden. (auch abgebaut)
-Nach Verbindungsaufbau ist eine feste Bandbreite vorhanden.
-Digitalisierung bereits im Telefon
-Da reine Datenübertragung ⇒ andere Dienste wie Fax oder allgemeine Dateneinrichtungen.
-2xB-Kanal a 64kBit/s (Datenkanal)
-1xD-Kanal a 16kBit/s (Signalisierungskanal)
-Verbindungsaufbau über D-Kanal mittels SS7 (Signalling System No.7)
-Circuit Switched (Internet ist Packet Switched)



3 IN (Inteligentes Netzwerk)

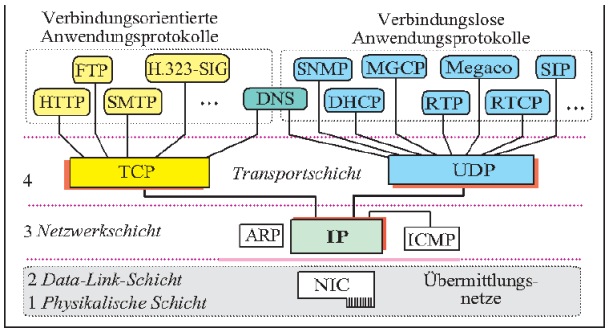
IN ist nötig da ISDN ein reines Übermittlungsnetz ist. Es verbindet z.B. ein normales Tel mit dem ISDN.
Vorhanden sind:
-SSP(Service Switching Point)
IN-Modul (Wird zur Kommunikation mit anderen IN-Komponenten eingesetzt)
-SCP(Service Control Point)
Server des IN's
-SMP(Servoce Management Point)
Dienstverwaltungspunkt. Richtet dienste ein, verwaltet sie und überwacht sie
-Kommunikation zwischen SSP+SCP nach INAP (Itelligent network application protocol (Teil des SS7))



4 TCP/IP

4.1 ISO/OSI-LAYER

Layer #	Layer Name	Misc. examples	TCP/IP suite
7	Application	HL7, Modbus, CDP	NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, SMPP, SMTP, SNMP, Telnet,
6	Presentation	TDI, ASCII, EBCDIC, MIDI, MPEG	MIME, XDR, SSL, TLS (Not a separate layer)
5	Session	Named Pipes, NetBIOS, SAP, SDP	Sockets. Session establishment in TCP. SIP. (Not a separate layer with standardized API.)
4	Transport	NBF, nanoTCP, nanoUDP	TCP, UDP, IPsec, PPTP, L2TP
3	Network	NBF, Q.931	IP, ARP, ICMP, DHCP, RIP, OSPF, BGP, IGMP, IS-IS
2	Data Link	802.3 (Ethernet), 802.11a/b/g/n MAC/LLC, 802.1Q (VLAN), ATM, HDP, FDDI, Fibre Channel, Frame Relay, HDLC, ISL, PPP, Q.921, Token Ring	PPP, SLIP
1	Physical	RS-232, V.35, V.34, I.430, I.431, T1, E1, 10BASE-T, 100BASE-TX, POTS, SONET, DSL, 802.11a/b/g/n PHY	



Physial-Layer: -ist für das Schicken/Empfangen von Bits zuständig
Link-Layer: -schicht/empfängt Frames (mehere Bits)
-sorgt dafür, dass Devices senden/empfangen kann (einen Slot kriegt → MAC)
Network-Layer: -ist für den Datenverkehr ausserhalb des eigenen Subnetzes zuständig

-Anwendungsprotokolle sind in den Applikationen
-InternetProtocol legt fest, wie die Daten als Datenpakete (sog. IP-Packete) übermittelt werden.
-ARP (Address Resolution Protocol) liefert für die ensprechende IP-Adr. die MAC-Adr.
-ICMP (Internet Control Message Protocol) überträgt Fehlermedungen und andere Steuerinfos
-TCP (Transmission Control Protocol) Virtuelle Verbindung durch Fehlerkontrolle geschützt.
  -HTTP (Hypertext Transfer Protocol)
  -FTP (File Transfer Protocol)
  -SMTP (Simple Mail Transfer Protocol)
  -H.323-Signalisierung (H.255.0 & H.245 (auf und abbau der Verbindung))

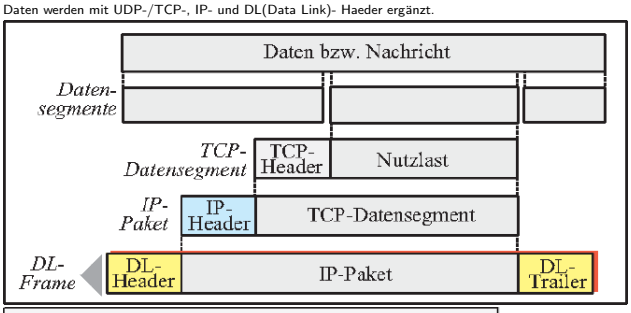
-UDP (User Datagram Protocol) verbindungslose Datenübermittlung. nicht sicher
  -DHCP (Dynamic Host Configuration Protocol)
  -SNMP (Simple Network Management Protocol)
  -RTP (Real-time Transport Protocol)
  -RTCP (RTP Control Protocol)
  -SIP (Session Initiation Protocol)
  -MGCP (Media Gateway Control Protocol)

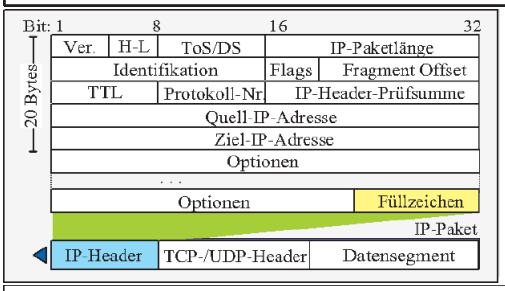
4.2 Subneting

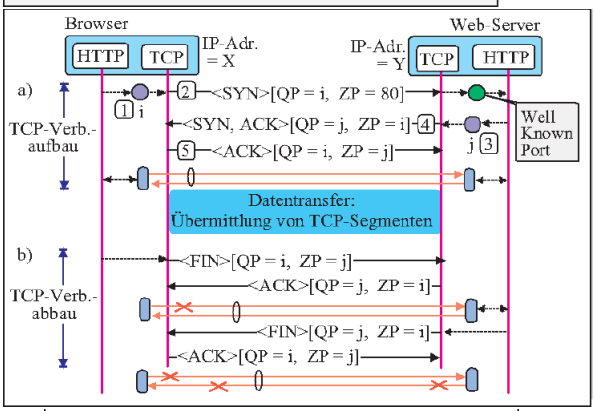
	Dezimal				Binär			
IP-Adresse	192	168	0	1	1100 0000	1010 1000	0000 0000	0000 0001
Subnetmaske	255	255	255	0	1111 1111	1111 1111	1111 1111	0000 0000
Subnet	192	168	0	0	1100 0000	1010 1000	0000 0000	0000 0000
Stationsadresse	0	0	0	1	0000 0000	0000 0000	0000 0000	0000 0001

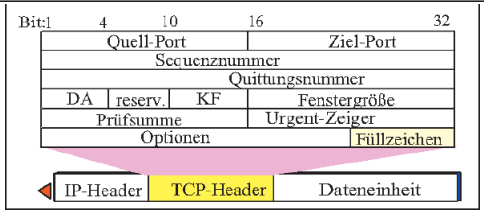
4.3 IP-Pakete

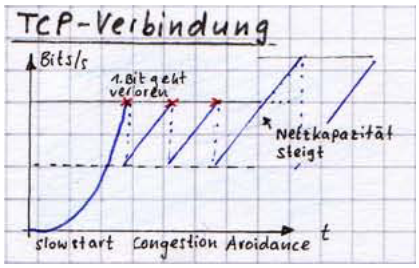
Daten werden mit UDP-/TCP-, IP- und DL(Data Link)- Haeder ergänzt.





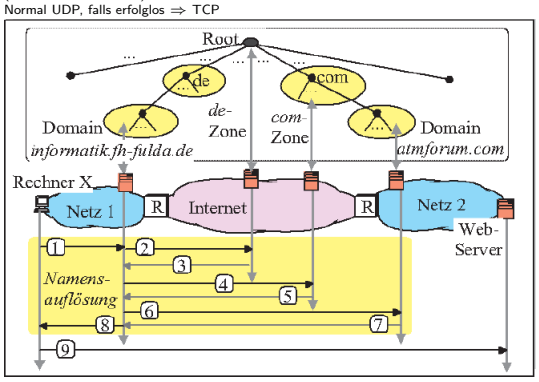






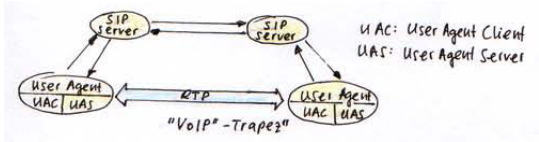
5 DNS

(Domain Name Service)
Normal UDP, falls erfolglos ⇒ TCP



6 VoIP

Es wird RTP und RTCP verwendent.



7 QoS-Anforderungen bei VoIP

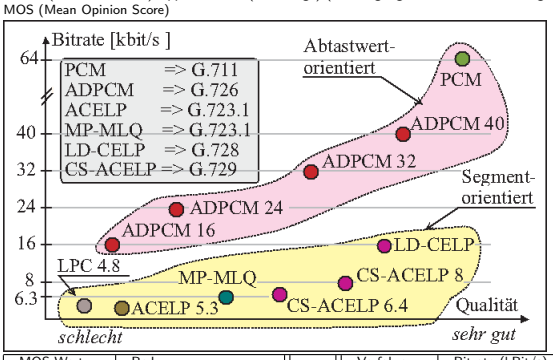
Quality of Service (Dienstgüte)
Zeitverhältnisse im Bitstrom müssen bei Sender und Empfänger gleich bleiben. (Isochronität)
Sie ist definiert durch:
Bandbreite
End zu End Verzögerungen (Delay)
Schwankungen von Übermittlungszeiten (Jitter) $t_{ü}$
Paketverluste (Packet Loss Rate)
Konzepte:
DiffServ (Differentiated Services)prioritäts IP-Packete
Management von Warteschlangen (Queue's)
RSVP (Resource reServVation Protocol) Reservation von Resourcen

8 Enum-Konzept

Damit Telefonnummern auch als Adressen für die Nutzung der Inernet-Dienste verwendet werden können.
mailto:pafswip.de
sip:pafswip.de

9 Sprachcodierung

PCM(Pulse Code Modulation)(G.711) 8000 Samples pro Sec. 16 Bit Gleichförmig
DPCM (Differntial PCM) Approximation (vorhersage) (übertragung der Differenz ⇒ weniger BIT)
MOS (Mean Opinion Score)

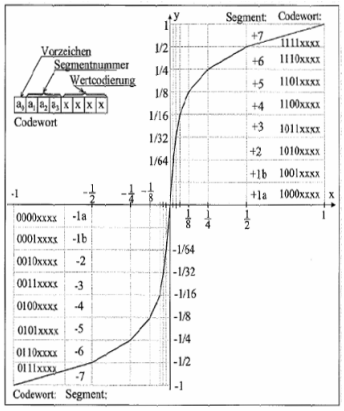


MOS-Wert	Bed.
5 = Excellent	keine Verständnisprob
4 = good	kein Anstrengung nötig
3 = fair	leichte Anstrengung
2 = poor	Anstrengung
1 = bad	nichts

Verfahren	Bitrate (kBit/s)	MOS-Wert
PCM	64	4.3-4.5
ADPCM	16/24/32/40	3.4/3.6/3.9/4.2
CS-ACELP	8/6.4	4.0/3.8
LD-CELP	16	4.0-4.1
ACELP	5.3	3.5
MP-MLQ	6.3	3.7

9.1 G.711

-Bitrate: 8000kHz @ 8Bit = 64kBit/s=8kBytes/s
-normally 10ms ⇒ 80Bytes/frame
-⇒ 960Bity/10ms = 96kBits/s bidirectional



9.2 GSM

-Bitrate: 13kBit/s
-Frame size: 20ms= 260Bits/Frame
-Packetsize: normally 20ms= 40·8+260=580Bits/packet ⇒ 580/20ms=29kBits/s bidirectional
-encoder MIPS:3.5 / Decoder MIPS: 2.1

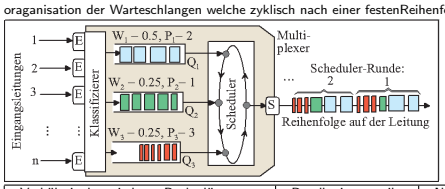
10 Queue-Management

10.1 FIFO

10.2 PQ (Pririty Queueing)

10.3 CQ (Custom Queueing)

oraganisation der Warteschlangen welche zyklisch nach einer festenReihenfolge geleert werden.



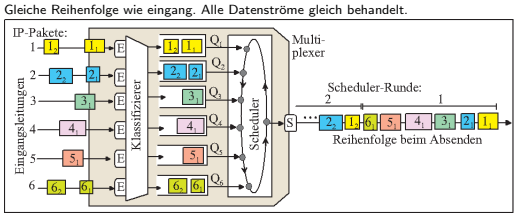
Verhältnis der mittleren Packetlängen	Bandbreitenanteil	Normalisieren (aufrunden) (Anzahl bearbeiteter Packete)
Packetstrom1 (W=0.5): 500/500=1	0.5· 1=0.5	0.5/0.4175 = 1.19⇒ 2
Packetstrom2 (W=0.25): 500/300=1.65	0.25· 1.65=0.4175	0.4175/0.4175 = 1⇒ 1
Packetstrom3 (W=0.25): 500/100=5	0.25· 0.5 = 1.25	1.25/0.4175 = 2.99 ⇒ 3

10.4 CBQ (Class Based)

IP-Packete werden Klassen zugeordnet

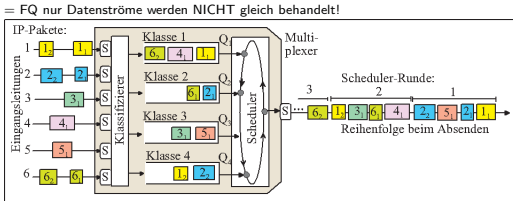
10.5 FQ (Fair Queueing)

Gleiche Reihenfolge wie eingang. Alle Datenströme gleich behandelt.



10.6 WFQ (Weighted Fair Queueing)

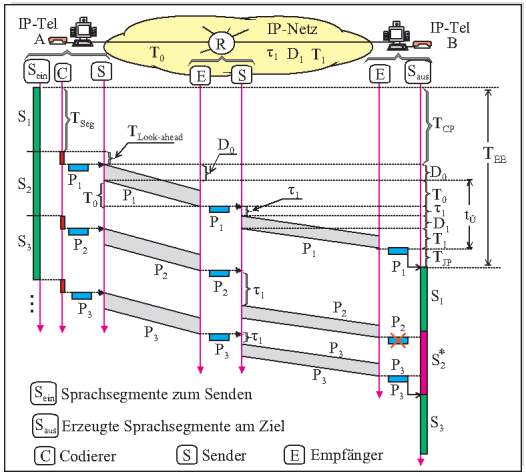
= FQ nur Datenströme werden NICHT gleich behandelt!



10.7 CBWFQ (Class-based)

um Class erweitertes WFQ

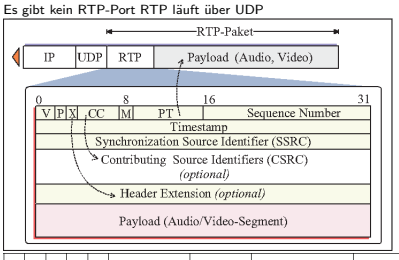
12 timing



$T_{Segment}$: Aufnahmezeit
$T_{look-ahead}$: Codierungszeit
T_{CP}: $T_{look-ahead} + T_{Segment}$
D_0: Serialisierungsverzögerung D_0 = Paketgrösse [BIT]/Übertragungsrate [Bit/s]
T_0: Zeit um Packet zum Router zu schicken
τ_1: Zufällige Wartezeit in Queues
D_1: Zeitverlust im Router
T_1: Zeit um Packet zum empfänger zu schicken
$t_{\ddot{u}}$: Übertragungszeit, $t_{\ddot{u}} = T_0 + \tau_1 + D_1 + T_1$
T_{SP}: Zeit im Jitter-Ausgleichsbuffer (oft:$T_{SP} = 2 \cdot T_{Seg}$)

11 RTP

Es gibt kein RTP-Port RTP läuft über UDP



V	Version	2 Bit	Derzeit gilt Version 2 (RFC3550, July 2003)					
P	Padding	1 Bit	Gesetzt, falls die Payload hinten mit 0 noch aufgefüllt wird.					
X	eXtension	1 Bit	Gesetzt, falls eine optionale Header Extension vorhanden ist					
CC	CSRS Count	4 Bit	Anzahl von im Feld CSRC enthaltenen Quell-Identifikatoren					
M	**Marker**	1 Bit	Oft verwendet zur Angabe des 1. RTP Paketes einer Übertragung					
PT	**Payload-Type**	7 Bit	Hier wird angegeben um welches Format es sich beim transportierten Medium als Nutzlast handelt. Zum einen, ob es sich um Audio, Video oder andere Daten handelt, und zum andern, mit welchem Verfahren die Daten kodiert wurden.					
Sequence Number		16 Bit	Jedes Paket wird mit einer Sequenz Nummer versehen, die es dem Empfänger erlaubt, die Pakete in die richtige Reihenfolge zu bringen und festzustellen, ob ein Paket verloren wurde.					
Timestamp		32 Bit	Der Zeitstempel dient dazu, den Zeitpunkt der Generierung der Payload anzugeben. Er ist von der Payload-Type abhängig und wird bei Audio meistens *in Samples* angegeben. Bei Audio gibt der Timestamp an, das wievielte Sample eines Streams das erste Sample im Paket ist.					
SSRC	Synchronisation Source Identifier	32 Bit	Zur Unterscheidung der Quelle eines Medienstromes. SSRC bleibt für einen Medienstrom immer konstant. Zwei verschiedene Quellen (Mikrophon, Kamera....) müssen unterschiedliche SSRC haben.					

13 Key-Management

13.1 Masterkeying

1 Die 2 Teilnehmer (A=initiator, B=Responder) denken sich eine Zahl (X_A und X_B) aus (bleibt geheim).
Es wird $Z_{A,B} = g^{X_{A,B}} \bmod p$ berechnet und dem Partner mitgeteilt.
2 Initiator Berechnet:
$S_A = (Z_B)^A \bmod p = (g^B \bmod p)^A \bmod p = (g^B)^A \bmod p = g^{AB} \bmod p$
3 Responder Berechnet:
$S_B = (Z_A)^B \bmod p = (g^A \bmod p)^B \bmod p = (g^A)^B \bmod p = g^{AB} \bmod p$
4 $S_A = S_B$ somit haben wir das geheime Schlüsselmaterial. Master Key dieser wird verwendet um die Sessions-Key zu erzeugen.

13.2 DES

-(Data Encryption Standard)(1976)
-symmetrischer Verschlüsselungsalgorithmus (Gleicher Schlüsser für die Codierung und Decodierung)
-Blockchiffre (Blockweises Codieren mit dem Schlüssel)
-Blockgrösse 64Bit, (64-Bit Klartext ⇒ 64-Bit CHiffretext) (Schlüssel=64Bit)
-eingentlich nur 56Bit da pro Byte ein Paritätsbit enthalten ist.
-entschlüsselung mit den gleichen Schlüsseln einfach umgekehrte rheienfolge

13.3 3DES

- $-DES-DES^{-1}-DES-$
-mit 192Bit (168 gebrauchten)
-Schlüsselkomplexität um den Faktor 2^{112}
-hoher Rechenaufwand

13.4 AES

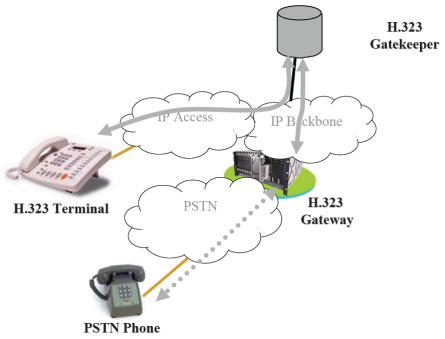
-Advanced Encryption Standard, Rijndael-Algorithmus (2000)
-DES-Nachfolger
-Symmetrische Verschlüsselung
-Blockgrössen von 128, 192 oder 256 Bit

13.5 RAS

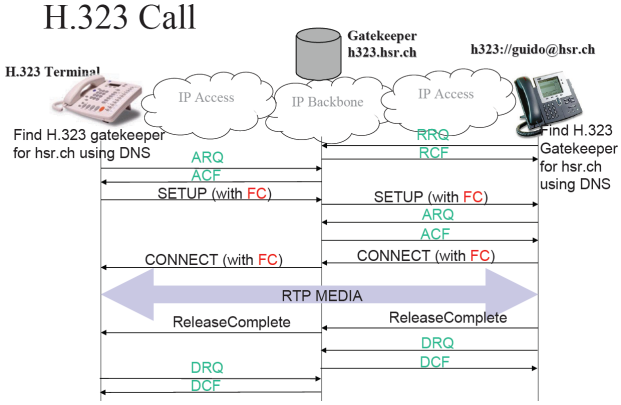
14 H.323

ITU-T H.323 umbrella standard
-based on ITU-T H.320
–H.225.0 (RAS&Q.931) for call setup
–H.245 for logical channel management

Layers
V1+2 ⇒ H.245+Q.931 über TCP, RAS über UDP
V3+4 ⇒ H.245+Q.931 über UDP/TCP, RAS über UDP

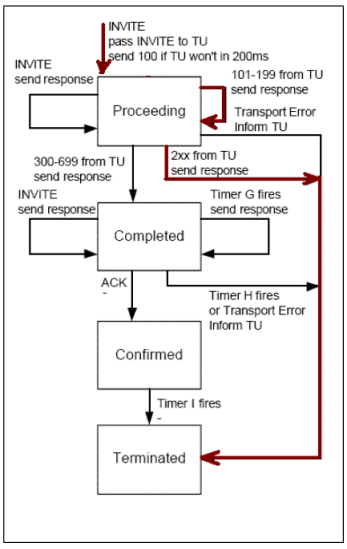


H.323 Call

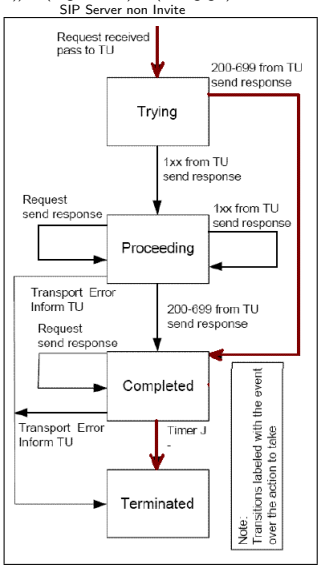


ARQ (Admission-ReQuest), ACF (Admission-ConFirm(ation)), R (Registration-), D (Disengage-)

SIP Server Invite

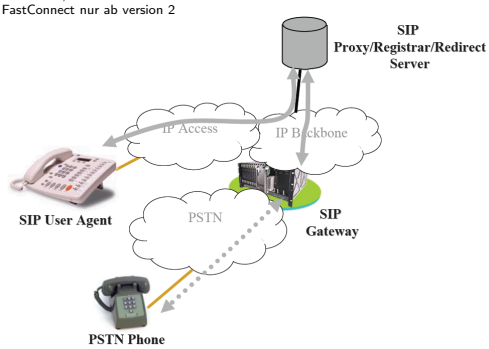


SIP Server non Invite

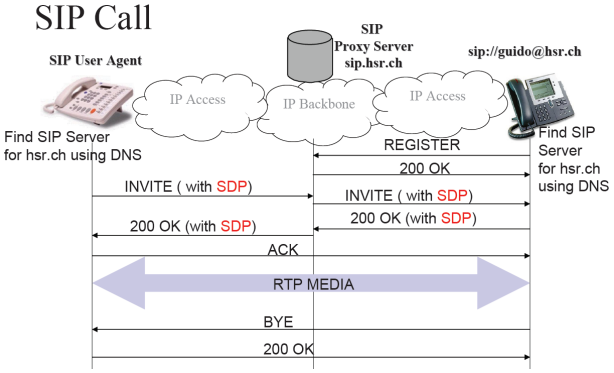


15 SIP

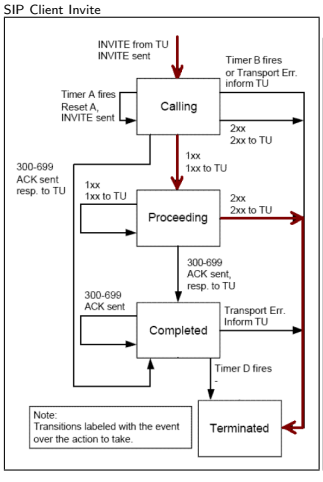
-based on HTTP and SMTP ideas
–Request/Peply model for call setup
–SIP carries SDP for session description
Über TCP/UDP wobei UDP normal ist
FastConnect nur ab version 2



SIP Call



SIP Client Invite



SIP Client non Invite