VoIP

Inledning

Sammandrag

Voice over IP, även kallat VoIP, är ett idag växande begrepp. Det hela handlar om att föra över röster/ljud över datornätverk, vilket möjliggör att man prata med varandra över Internet. VoIP är ingen teknik i sig utan bara ett sammanfattande namn för tekniker som gör att man kan prata med någon över Internet.
Tre populära tekniker som används idag är SIP, H.323 samt Skype.

Det finns båda nackdelar och fördelar med VoIP. En av de största nackdelarna med VoIP är man inte kan garantera ljudkvalitén helt enkelt på grund av inte bandbredden räcker till eller att det är problem med nätverket. Ett annat problem handlar om att vissa larmnummer inte fungerar som dom ska.
Några av de största fördelarna är att det är går att använda över befintlig nätverksutrustning samt att det är mer eller mindre mobilt. Tack vare att de flesta VoIP-tekniker är mobila behöver inte användaren ha ett ”IP-telefonnummer” per dator utan kan uppdatera en lokaliseringsdatabasen med det IP-nummer användaren har för tillfället.

Syfte

Syftet med rapporten är att belysa och inspektera det idag allt mer populära VoIP-tekniken. Dels varför VoIP används och sedan hur teknikerna bakom ser ut. Denna kunskap kan vara mycket viktigt när man själv skall implementera något idag existerande protokoll eller om man skall ta fram ett nytt.

Metod

Vi har gått igenom diverse litteratur och tekniska referensdokument. Dessa har vi sedan sammanställt till en rapport

Avgränsningar

Vi har valt att fokusera på en övergripande bild av VoIP samt detaljbeskriva VoIP-protokollen SIP respektive H.323. Dessutom har vi tittat närmare på hur framtiden ser ut för VoIP och vilka tänkbara förändringar vi kan tänkas få se.

Introduktion till VoIP

VoIP eller Voice over IP handlar om att man skall kunna föra röster(ljud) över datornätverk. Detta område har funnits sedan 1995 men det är först under de senaste 6 år som den största utvecklingen och populäriteten har ökat. Dels tack vare att allt fler fick snabbare Internetuppkopplingar under denna tid, dels tack vare att olika hårdvaruföretag började släppa så kallade VoIP-telefoner. Dessa VoIP-telefoner möjliggjorde att man slapp använda datorn utan kunde använda telefonen direkt från ett nätverksuttag.
Ytterligare en faktor som har motiverat användning av VoIP på senare tid, har varit möjligheten att kunna kommunicera till en vanlig telefon.

VoIP är inte något speciellt protokoll för ljudöverförning utan istället ett samlingsnamn för tekniken. Några protokoll som används vid Voice over IP är Session Initiation Protocol (SIP), H.323 samt Skype.

Fördelar och nackdelar

Fördelarna med VoIP jämfört med traditionell telefoni är många. Med VoIP går det att använda det befintliga nätverket till att överföra ljud mellan olika klienter. Den största fördelen med VoIP är att det är ett mycket billigt alternativ jämfört med vanlig telefoni. Andra fördelar är att VoIP är flexibelt. Det går att, som användare, sitta på olika platser och vara nåbar eller ringa med samma ”telefonnummer” oavsett var man är placerad. Det är också mycket lättare att använda olika tilläggstjänster. Med VoIP tätt sammankopplat med det vanliga datorsystemet kan tillsyn, kontroll och andra administrativa tjänster lätt sammankopplas. Statistik och information om hur och till vem VoIP används är lättillgängligt och administratörer kan på ett enkelt begränsa och reglera VoIP-trafiken i nätverket.
Nackdelarna med VoIP är att nätverket inte är självförsörjande av el och vid strömavbrott slutar tjänsten att fungera. Detta är något som inte drabbar den traditionella telefonin.
Den vanliga telefonin har också en lång historia och fungerar med hög tillförlitlighet. Kunder är inte villiga att byta till en motsvarande tjänst med lägre tillförlitlighet. Tillförlitligheten är VoIP största nackdel. Quality of Service (QoS) är något som det ofta pratas om i smaband med VoIP. För att VoIP skall ha möjligheten måste tillförlitligheten och QoS säkras.

Quality of Service (QoS)

För att kunna använda VoIP är det viktigt att nätverket uppfyller vissa krav och klarar att leverera en realtidsöverföring av ljudet mellan klienterna. Vanliga paket, innehållande data, är ofta inte lika känsliga för fördröjningar som när man pratar över VoIP. Redan vid små fördröjningar i samtalet kan detta upplevas mycket störande och användarna får svårt att kommunicera med varandra.
Traditionella telefonnät, så kallade Public Switched Telephone Network (PSTN), kopplar upp en förbindelse mellan klienter som inte delas av andra så länge kommunikationen pågår. Detta är svårt att göra i paketbaserade nätverk och omöjligt att göra över Internet. PSTN har den fördelen, jämfört med VoIP, att garantera en bandbredd med låg fördröjning genom hela kommunikationen.
I samband med VoIP talas det om Quality of Service (QoS). QoS är ett begrepp som vanligtvis innefattar sex punkter med egenskaper för att säkerställa en VoIP-kommunikation. Begreppet är svårdefinierat men här är ett försök av Goralski och Kolon att definiera QoS:

”Möjligheterna för ett nätverk att garantera och upprätthålla vissa nivåer av prestanda för varje enskild applikation med hänsyn till de specificerade behov varje användare har”.

De sex punkterna som kan innefattas i QoS är bandbredd, fördröjning, jitter, informationsförlust, tillförlitlighet och säkerhet.
Bandbredd tillsammans med fördröjning är de två viktigast parametrarna i begreppet QoS. Bandbredd är de antal bitar per sekund som finns tillgänglig för en applikation att skicka information till en annan klient. I ett nätverk delas bandbredden mellan olika klienter och applikationer och den enskildes bandbredd variera beroende av trafikmängden på nätverket.
Fördröjning är kopplat till bandbredden, då vid mindre bandbredd ökar fördröjningen och vid ökad bandbredd ger minskad fördröjning. Fördröjningen är den tid det tar för information att överföras från källan till destinationen.
Jitter är variationen i fördröjningen på nätverket och realtidsöverföringar är mycket känsliga för jitter. För att få en bra realtidskommunikation krävs det att det är lite jitter på överföringskanalen.
Informationsförlust i små mängder är inget större problem i samband med realtidsöverföring. Om ett paket försvinner kan applikationen hoppa över det paketet och ta efterföljande i stället utan att användaren upptäcker informationsförlusten.
Tillförlitlighet är viktigt i samband med VoIP. Om VoIP skall ersätta traditionell telefon är det viktigt att tillförlitligheten är hög. Oförutsedda händelser inträffar men det är viktigt att underhålla nätverken, bygga med redundans och snabbt kunna åtgärda problem när de uppstår.
Säkerhet är också en viktig aspekt vid kommunikation över Internet. Internet är öppet och den väg pakten går är oskyddad och kan avlyssnas av andra. Därför är kryptering och andra säkerhetsmekanismer viktiga i samband med realtidskommunikation. För att säkerställa att endast deltagande parter deltar kommunikationen måste säkerhetsmekanismer implementeras.

I IPv6 som är den nya och kommande IP-standard finns mer mekanismer för att säkerställa och använda olika nivåer av QoS. Det går, med IPv6, att garantera en viss bandbredd och säkerställa att jitternivån är låg och jämn. Detta är viktiga egenskaper för att VoIP ska växa och, på allvar, kunna konkurrera med traditionell telefoni.

VoIP-protokoll

SIP - Session Initiation Protocol

Introduktion

SIP är ett relativt nytt protokoll som standardiserades 1999 som ett protokoll för etablera VoIP-sessioner. SIP påminner mycket om HTTP-protokollet. Båda protokollen jobbar i applikationslagret i OSI-modellen, de är båda textbaserade vilket gör de lättläsliga.
SIP är ett så kallat peer-to-peer protokoll vilket betyder att det inte krävs mycket annat förutom mjukvara hos ändnoderna. Detta gör SIP väldigt skalbart.

SIP är inte i själv ett protokoll som implementera VoIP utan används för att initiera en session. Således behövs fler delar/protokoll för att kunna åstadkomma VoIP.

Teknik

SIP består av två huvudsakliga komponenter; User Agents samt nätverksservrar. User Agents är mjukvaran som finns hos ändnoderna i systemet, det vill säga hos dem som skall kommunicera med varandra. Programvaran i ändnoderna är uppdelad i två bitar. Den ena biten används som klient (UAC = User Agent Client) som används för att initiera en session. Den andra biten används som server (UAS = User Agent Server) och tar emot initieringen från klienten och skickar ett meddelande till klienten huruvida serversidan vill upprätta en session.

Den andra huvudsakliga komponenten i SIP-protokollet är speciella servrar som håller koll på var olika användare/ändnoder finns. Så när en användare loggar in på systemet så sparas information om användaren ifråga, exempelvis IP-adress och personuppgifter.

Kommunikationen mellan User Agent Client och User Agent Server går till så att UAC skickar en förfrågan till UAS. Servern tolkar sedan förfrågan från klienten och svarar med ett lämpligt svarsmeddelande. Med andra ord så är det alltid klienten som inleder kommunikationen med servern och inte tvärt om.
SIP har specificerat några givna meddelanden som en förfrågan kan bestå av.
INVITE – används för att etablera/initiera en session. När ett INVITE skickas kopplas också ett unikt ID till den framtida sessionen som möjliggör att två noder kan ha en eller flera sessioner samtidigt.
ACK – används för att bekräfta att man verkligen vill etablera en anslutning. ACK skickas av klienten när denna har mottagit ett positivt svarsmeddelande från UAS.
BYE – används för att avsluta en etablerad session.
OPTIONS – används för att undersöka vilka inställningar som den mottagande användaragenten har. Fungerar i princip som ett INVITE-meddelande men utan att etablera en session.
CANCEL – skickas för att avbryta en viss session.
REGISTER – används för att registrera en klient hos en server som håller reda på vart olika klienter befinner sig på nätverket.
INFO – används för att skicka olika typer av informationsmeddelanden, exempelvis att kryptering skall aktiveras. SIP har som HTTP specificerat olika grupper av svarsmeddelanden. Ett svarsmeddelande skickas alltid efter en förfrågan, exempelvis ett INVITE-meddelande.
100 – 199 är så kallade upplysningsmeddelanden om vad som händer. Om person A skickar ett INVITE-meddelande till person B kan exempelvis så skickas upplysningsmeddelandet 180 till A. 180 betyder att det ringer hos den som tar emot INVITE-meddelandet (i exemplet person B).
200 – 299 är svarsmeddelanden på att något har lyckats. Exempelvis betyder 200 just OK och kan skickas som ett svar på ett INVITE-meddelande.
300 – 399 används för olika typer av vidarepekningar.
400 – 499 är svarsmeddelanden för att indikera att det har skett ett klientfel någonstans. Svarsmeddelandet 404 betyder precis som svarsmeddelandet för HTTP att en URL inte kunde hittas.
500 – 599 är svarsmeddelanden för att informera om problem och fel hos servern. Exempelvis så är svarsmeddelandet 500 internt serverfel.
600 – 699 är den sista gruppen av svarsmeddelanden och används för att globala problem såsom att en server är upptagen.

Samarbetande protokoll

Som nämndes i introduktionen om SIP så är SIP i sig själv inget multimediaprotokoll utan används för sätta upp en session. Exempel på protokoll som SIP interagerar med är SDP och RTP.
SDP står för Session Description Protocol. SDP beskriver den multimediasession som SIP skall initiera. Exempel på sådant som beskrivs med hjälp av SDP är vilka codec som skall användas och vilka IP-portar som skall användas.
SDP skickas exempelvis alltid med när ett INVITE-meddelande skickas.
RTP står för Real-time Transport Protocol och är det protokoll som faktiskt skickar och hanterar ljudet över nätverket.

Exempelsession

Här kommer en liten exempelsession som visar vad som händer när två användare skall etablera en SIP-session.

Ponera att användare Alice vill starta en session med användare Bob
Alice börjar då det hela med att skicka ett INVITE-meddelande till Bob som bland annat innehåller ett SDP-meddelande som specificerar vilka codec och liknande som skall användas när sessionen väl sats upp.
Bob tar emot INVITE-meddelandet från Alice och skickar ett svarsmeddelande innehållandes 200:OK för att bekräfta att han vill delta i denna session. Skulle Bob välja att inte delta i sessionen skickar han istället ett svarsmeddelande som indikerar just detta.
Alice tar emot svarsmeddelandet från Bob. Om Bob skickade 200:OK bekräftar Alice detta med ett ACK-meddelande.
Bob tar emot ACK-meddelandet och starta multimediasessionen enligt de instruktioner som beskrevs med hjälp av SDP-meddelandet i INVITE.

Om någon vill avsluta sessionen skickas ett BYE-meddelande som sedan bekräftas med ett 200:OK-svarsmeddelande.

Säkerhet

Säkerhetsstödet i SIP bygger på 3 områden, nämligen kryptering, autentisering samt integritet.

Kryptering

Om man är ute efter total kryptering av de olika värdena som IP-adresser, port nummer och liknande som finns i ett SIP-meddelande så krävs det skydd på under applikationslagret. Exempelvis så erbjuder IPSec denna typ av skydd.

Vill man dock inte kryptera under applikationslagret och kan leva med att viss information visas så erbjuder SIP möjligheter för detta. Sådant som då inte kan krypteras är de delar av meddelandet som krävs för att det skall kunna skickas på nätet, exempelvis till- och från adresser.

Autentisering

Används för att en användaragent kan bevisa för en annan användaragent eller en SIP-server att denne känner till en delad hemlighet och på så bevisa vem han är.
Integritet

SIP har stöd för att signera bitar eller hela SIP-meddelanden för att garantera dess integritet. På så sätt kan man vara säker på att inte någon modifierat eller att någon av förneka att denne har skickat ett meddelande.

H.323

Introduktion

H.323 är en internationell standard för multimediakommunikation över nätverk som är paketförmedlande. H.323 är ett ”paraplyprotokoll” för en samling protokoll för att kommunicera röstsamtal, videokonferenser och data över olika nätverk i realtid. Protokollen togs fram av ITU (International Telecommunication Union) 1996 och är en av de stora standarderna som används för att kommunicera VoIP. H.323 uppdateras kontinuerligt och har idag nått till version 5 (H.323v5).

Teknik

H.323 är en stor och flexibel standard som innebär att det finns stor valmöjligheter att anpassa systemet efter behov. Minimikravet för H.323 specificerar ett antal protokoll för att, i realtid, överföra röstkommunikation mellan två punkter över ett paketbaserat nätverk utan att garantera någon kvalitetsnorm. H.323 specificerar, utöver minimikraven, också ett antal andra egenskaper.
I ett H.323-system finns möjligheten till att kommunicera multimedia till en eller flera olika klienter.
H.323 kan kommunicera över olika typer av nätverk och behöver inte ha IP-protokollet som bärare. H.323 ger också klienterna möjlighet att förhandla om vilka ljud-codec, och om önskat, video-codec som skall användas i kommunikationen. H.323 specificerar ett antal olika codec för ljud och video men det är inget som hindrar klienterna att använda andra så länge båda stödjer dessa.
I H.323-system finns också möjligheten att styra över hur många kommunikationer och hur mycket bandbredd dessa får användas samtidigt.
H.323 innehåller också protokoll för att göra kommunikationen säker.

Generellt består ett H.323-system av fyra olika komponenter. Termminaler, gateway, gatekeeper och multipoint control units (MCU).

Terminaler

En terminal är en ändpunkt som kommunicerar med en eller flera andra terminaler. Vanligtvis är det en applikation i datorn, ibland kallad Softphone, som agerar terminal men det kan också vara en fysisk IP-telefon.
Alla terminaler måste stödja H.245, Q.931, RAS och RTP protokollen. H.245 är ett kontrollprotokoll som tillåter kommunikation på kanalen. Q.931 behövs för att skapa en anslutning. Registration Admission Status (RAS) används för kommunikation mellan klienten och gatekeepern. Real Time Transport Protocol (RTP) är transportprotokollet som bär paketen mellan klienterna. H.323 kräver bara att en terminal stödjer ljudöverföring men terminalerna kan med video codec och T.120-protokollet också kommunicera video och data.

Gateway

En H.323-gateways uppgift, som ändpunkt i nätverket, är att möjliggöra realtidskommunikation mellan två klienter i olika nätverk. En H.323-gateway används också till att kommunicera mellan olika typer nätverk och fungerar som ett interface mellan vanlig traditionellt telefonnät och paketbaserade nätverk. En gateway är också kapabel till att översätta olika video-codec till ljud-codec. Klienter inom samma nätverk kan kommunicera med varandra utan hjälp av en gateway, men skall kommunikationen ske mellan olika nätverk är en H.323-gateway nödvändig.

Gatekeeper

En gatekeeper är den viktigaste delen i ett H.323-system. Gatekeepern fungerar som styrenhet eller central punkt inom nätverket och tillhandahåller nödvändiga tjänster till klienterna. I ett H.323-system kan klienterna få ”alias-adresser” som gatekeepern kan översätta och använda för att inleda en kommunikation mellan två klienter. Gatekeepern kan också auktorisera kommunikationer mellan klienter baserat på ett antal regler samt att övervaka nätverket och bara tillåta ett visst antal pågående kommunikationer samtidigt.

Multipoint Control Units (MCU)

MCU är en ändpunkt i nätverket som möjliggör kommunikation mellan flera klienter samtidigt. När en konferens pågår skickas paketen till MCUen som hanterar och skickar paketen vidare till berörda klienter. Trafiken på nätverket minskas då inte klienter skickar paket mellan varandra utan via MCU-eneheten.

Kontroll och signalering

RAS (Registration, Admission and Signaling)
RAS-kanalen används för kommunikation mellan klienten/terminalen och gatekeepern. RSA-meddelanden skickas över UDP och rekomenderas därför att använda time-out och paketräknare för att upptäcka fel. RSA används när klienter skall upptäcka och registrera sig hos gatekeepern. Klienten multicastar ett Gatekeeper Request (GRQ) meddelande och väntar på ett Gatekeeper Confirmation (GCF) meddelande men nödvändig information för att klienten skall kunna registrea sig hos Gatekeepern.
När klienten känner till gatekeepern kan klienten registrerar sig genom att skicka uppgifter om sig själv. Om gatekeepern godkänner klienten säkerställer gatekeepern att klientens uppgifter är korrekta och att klientens alias-adresser översätts till en unik och giltig adress.
För att en klient skall få giltig information om andra klienter skickas ett Location request (LRQ) meddelande, innehållande den sökta klientens alias-adress, till gatekeepern som svarar med klientens verkliga adress.
RSA innehåller också funktionaliteten för att kontrollera hur många kommunikationer som pågår och mekanismer för att begränsa användandet av bandbredd.

Kontrollmeddelanden

Kontrollmeddelanden kan skickas direkt mellan klienter eller via gatekeepern och sköter initialisering och upp- och nerkoppling av kommunikationen. Kontrollmeddelandena som

skickas direkt mellan klienter använder TCP för att få en pålitlig kommunikation och kontrollmeddelanden som skickas vi gatekeepern använder RSA-kanalen.

Media- och konferenskontroll

H.245-protokollet används efter att ett samtal initialiseras och förhandlar och sätter upp mediakanaler mellan klienterna. Mediakanalerna använder sig av Real Time Transport Protocol (RTP) som bärare och används till att förhandla hur kommunikationen skall användas. Mediakanalerna ger också möjlighet till att möjliggöra konferenssamtal mellan flera parter samtidigt.

Uppringningsprocess

För att en klient skall komma i kontakt med en annan klient krävs olika steg för att kommunikationen skall sättas upp. Först måste klienten upptäcka och kontakta gatekeepern. När gatekeepern är känd registrera sig klienten hos gatekeepern. Klienten kontaktar gatekeepern för att få information om önskad klient och påbörjar kommunikationen. Klienterna förhandlar med gatekeepern för att komma överens om hur kommunikationen skall gå till. När detta är gjort startas kommunikationen mellan klienterna. När klienterna kommunicerat färdig avslutas kommunikationene av klienterna eller gatekeepern.

Säkerhet

H.323-standarden innehåller protokollet H.325. H.325 innebär att autentisering säkerställs av gatekeepern genom att kontrollera berörda klienter. H.325 ger också möjligheten att använda krypterad överföring mellan klienterna för att skydda kommunikationen från avlysning. Vid kryptering används något av de befintliga protokollen IP Security (IPsec) eller Transport Layer Protocol (TLS). Det finns också en mekanism i gatekeepern för att klienter inte skall kunna neka att de deltagit i en kommunikation.

Skype

Introduktion

Skype är ett nytt företag som grundades 2003 men som redan fått mycket publicitet och användare. Skype är en VoIP programvara som ger användaren möjlighet att ringa gratis överallt. Det som krävs är en Internettuppkopplad dator samt att mottagaren också sitter vid en uppkopplad dator. Skype erbjuder också tjänster, till en jämförelsevis låg kostnad, för att ringa mellan datorer och vanliga telefonnätet.
I delar av värden har Skype också lanserat en tjänst som gör det möjligt att ringa från det vanliga telefonnätet till en Skype-klient. Denna tjänst är under uppbyggnad men kommer snart lanserar över hela världen.

Teknik

Skype använder ett eget protokoll för VoIP. Grundarna bakom Skype utvecklade Peer-to-Peer (P2P) nätverket KaZzA. VoIP-protokollet som används i Skype är inte offentligt men det bygger på P2P-teknik som delvis användes i KaZzA. Genom att använda P2P-teknik och Global Index (GI), ett system med ”super-noder” som kommunicerar med varandra, kräver inte systemet stora och dyra servrar. Super-noderna kommuncerar med varandra och utbyter information om användarna. Varje nod i systemet får på så vis tillgång till alla tillgängliga användare om så önskas.

Säkerhet

All Skype-trafik är krypterad med AES-256 krypteringssytem och använder sig av RSA för hantering av AES-nycklar. Hur kommunikationen går till är inte offentligt men Skype hävdar att kommunikationen är säker.

H.323, SIP och Skype

Skillnaden mellan de olika protokollen är stor. H.323 är designat av ITU och möjliggör multimediakommunikation i realtid över paketbaserade nätverk. SIP är utvecklat av IETF för att transportera realtidsljud över Internet. Skype är ett företag som själva utvecklat ett protokoll för VoIP-kommunikation som bygger på P2P-teknik. Skype använder ett ickeoffentligt protokoll och kan därför inte jämföras med de två andra protokollen.

H.323 är en komplex standard som använder många olika typer av meddelande för att starta och upprätthålla en kommunikation. Det skickas mycket data mellan berörda klienter som inte har med själva mediainnehållet att göra.
SIP är däremot utvecklat för Internet och använder många mekanismer från http-protokollet för att skicka nödvändig information. H.323 definierar och skickar ett hundratal detaljer medan SIP endast använder sig av 37 headers innehållande ett fåtal parametrar. SIP använder sig av, till skillnad från H.323, av textbaserad representation och kan därför använda mekanismer från HTTP.
H.323 var i första hand utvecklat för att användas inom ett nätverk och skalbarheten är begränsad. H.323 har dock vidareutvecklats och går att använda mellan olika nätverk men på bekostnad av effektivitet. SIP är utvecklat för Internet och skalbarheten är därför mycket god.

VoIP i framtiden

De senaste åren har VoIP ökat kraftigt. Det finns ett flertal olika operatörer som erbjuder VoIP och stadsnäten i Sverige byggs ut för att kunna hantera VoIP. Det finns också ett flertal system som är gratis för användaren att ladda ner och använda tillsammans med en Internetuppkopplad dator.
På sikt bör tekniken förbättras och göras tillgänglig på fler platser och tillgängligt till fler användare.

Fjärde generationens mobilsystem (4G)

Fjärde generationens mobilsystem (4G) är under utveckling och visionen är att skapa ett heltäckande och snabbt mobilt nätverk baserat på IPv6. Tanken är att man använder sig av samma nätverk över allt till alla olika enheter som behöver kommunicera. Detta innebär att VoIP kommer att användas av alla mobiltelefonsanvändare och möjliggör för användaren att använda sin mobiltelefon som hemtelefon med sin egen anslutning, via en trådlösa accesspunkt, till Internet. Blir detta verklighet och operatörerna kan enas om en, för användaren, acceptabel affärsmodell kommer användandet av VoIP ta över efter det traditionella telefonisystemet.

Referenser:

Khasnabish, B., 2003, Implementing Voice Over IP [0471216666], John Wiley & Sons

Swale, R., 2001, Voice over IP: Systems and Solutions [0852960247], Institution of Electrical Engineers

Gough, M., 2006, Skype Me! From Single User to Small Enterprise and Beyond [1597490326], Syngress Publishing

Goralski, W., 2000, IP Telephony [007135221X], McGraw-Hill

Sinnreich, H., 2001, Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol [0471413992]

Forge, S, 2004, Is Fourth Generation Mobile Nirvana or Nothing

Mathiasson L, Mälarberg K, 2001, Göteborg, IP-TELEFONI – 2000-talets kommunikationsmedium

http://www.cse.wustl.edu/~jain/cis788-99/ftp/voip_protocols/index.html
Voice over IP : Protocols and Standards

http://www.cse.wustl.edu/~jain/cis788-99/ftp/voip_protocols/index.html
H.323 and Associated Protocols

Stawreberg, F, 2004, Göteborg, IP TELEFONI I STADSNÄT