TTM4130 Kont eksamen 2004 Nettintelligens og mobilitet
Løsningsforslag

1. Mobilitet (20%)

1.1 Definisjoner

Definer følgende begreper (bruk en eller to setninger for hver)
SVAR fra kompendium side 57 og 58

a) Terminalmobilitet
tillater terminalen å forandre posisjon i nettet, mens tjenesten opprettholdes
b) Brukermobilitet
tillater brukeren adgang til sin tjenester uavhengig av hvilke (fysiske) terminaler han befinner seg på.
c) Sesjonsmobilitet
tillater brukeren å beholde en aktiv sesjon, selv når han bytter terminal (den kan bli midlertidig "parkert" , under skiftet av terminal).
d) Tjenestemobilitet (alternative betegnelser: programmobilitet, aktørmobilitet)
tillater programvaremoduler/aktører (kode, objekter, prosesser) å bli overført fra en maskin til en annen.
e) Personmobilitet tillater en person å benytte tjenester som er tilpasset egne preferanser, og brukere (abonnementer) uavhengig av fysisk plassering og spesielt utstyr
f) Rollemobilitet: rolleskifte eller brukerskifte
Personer kan skifte rolle, få adgang til bestemte preferanser, rettigheter og begrensinger avhengig av eget valg eller på grunn av inntruffet hendelse. Det kan være hensiktsmessig å benytte rolleskifte eller brukerskifte om denne egenskap (for ikke å belaste ordet "mobilitet" mer).

1.2 Sesjonsmobilitet

Beskriv sesjonsmobilitet, og hvilke problemstillinger som må løses.
SVAR fra kompendium side 59-60

I dette begrepet ligger at man har anledning til å ta med seg "sesjonen", samtalen, filoverføringen, eller hva det nå er man holder på med, fra et tilknytningspunkt til et annet. Sesjonsmobilitet har opprinnelig blitt tatt i bruk for å beskrive flytting av en TCP sesjon. I fremtidens multimedia-verden, kan en terminal ha mange slags sesjoner simultant. Et situasjon man ser for seg er at en bruker på et kontor ustyrt med fastterminal og med høy båndbredde også har en mobilterminal, med essensielt samme funksjonsutvalg, men med mindre båndbredde, med mindre skjerm, etc. Hvis brukeren nå har gående et sett av sesjoner på den en av disse terminalene, og så ønsker å bevege seg (reise seg å gå, eller han/hun ankommer sin faste arbeidsplass), så kan det være aktuelt å skifte "hele greia" over til den mest hensiktmessige terminal. Dette fordrer for TCP overføring, at man flytter IP adressen, og tilhørende portadresse, man bør også vite hvor langt man er kommet i en filoverføring etc.. Hvis det er snakk om en sanntidsoverføring, kan det bli aktuelt å justere kodingsrate/kodingsform for å tilpasse seg den nye båndbredden.
Man må altså:

1. flytte tilknytingspunkt,
2. skifter rutingsmønster,
3. holde rede på seksvensnummer, i informsasjonsstrømmene
4. evt. juster kodingrater
5. samt overføre et bilde av "tilstandsbildet" for den terminalen man forlater til den nye terminalen.

Funksjon 1 og 2 er relativt enkle å utføre, hvis de to aksessnettene det er snakk om har en hensiktsmessig sammenknyting. Funksjon 3 og 4. kan være en oppgave for medieovergang/-gateway (i alle fall kan den sikkert justere kodingsraten ned). Imidlertid vil den ideelle løsning for en-til-en forbindelse, kanskje ha vært å gi kilden for informasjonen nye sendingsparametre. Har man derimot en konferanseforbindelse (en kilde kommuniserer med flere), så er det mer naturlig å tenke seg evt. justeringer gjort i en medieovergang /konferansebro. Legg også merke til at vi må oppdatere den nye terminalen med alle "sesjoner" og deres tilstand. Dette bør kunne realiseres "lettvint", f.eks. ved at bruker velger en funksjon "flytt til min andre, tredje osv., terminal". Dette vil medføre et signaleringsforløp som flytter forbindelsen. Spørsmålet er bare så hva eller hvem skal man "snakke" med i denne forbindelse. En naturlig mulighet er å la hver bruker ha tilknyttet "hjemme-tjener", (Home Server), som til enhver tid holdes oppdatert om brukerens tilstand. Legg merke til at dette bare er en av mange mulige realiseringsmåter!
N.B. Dette er et altfor uttømmende svar (vil ikke kreve så mye for å få A).

1.3 Kontinuerlig eller diskret?

a) Gi noen eksempler på håndtering av mobilitet på kontinuerlig henholdsvis diskret basis.

SVAR: Handover i GSM er eksempel på kontinuerlig håndtering av (terminal)mobilitet
Handover mellom to basestasjoner i et DECT system representer også kontinuerlig terminalmobilitet. (kan forekomme f.eks. i et hussentralsystem med omfattende bruk ab trådløse telefoner)..
Roaming i GSM er diskret terminalmobilitet
Mobil IP ble også opprinnelig designet for diskret sesjonsmobilitet (arbeid er på gang med utvidelser som kan gi kontinuerlig mobilitet)

b) Indiker hvilke primær form ("kontinuerlig" eller "diskret") du anser terminalmobilitet, brukermobilitet, osv., for å være (ref liste under punkt 1.1).

- Hvis du i noen tilfelle anser begge former å være like aktuelle, angi også dette.

SVAR:

a)	Terminalmobilitet	kont og diskret
b)	Brukermobilitet	diskret
c)	Sesjonsmobilitet	diskret (opprinnelig) og kontinuerlig
d)	Tjenestemobilitet	diskret
e)	Personmobilitet	diskret
f)	Rollemobilitet	diskret

2. AAA (15%)

2.1 Generelt

a) Forklar hva hver av de tre "A"-ene står for.
SVAR:
AAA står for "Authentication", "Authorisation" og "Accounting". På norsk kan vi si:

- Sikker identifikasjon (autentisering) "Authentication"
- Tillatelse (autorisasjon) "Authorisation"
- Regnskapsføring "Accounting"

b) Kan du si noe om forskjellen på "accounting" og "billing"?
SVAR:
"Accounting" står for regnskapsføring: (I denne sammenheng) registrering av trafikk, hendelser, samt produksjon av bearbeidet underlag for fakturering justering av nettet, etc. .
"Billing" står for fakturering. Obs, man må også ha "billing" mellom forskjellige tjenesteleverandører.

2.2 AAA Basismodell

Gitt et scenario som vist i figur 12.1 (hentet fra kompendiet). Diskuter krav til funksjoner og sikkerhetsrelasjoner. Fiuren inneholder mange alternative navn/betegnelser. Du kan benytte FA for betjeningsnode og HA for hjemmeagent i din beskrivelse. Diskuter spesielt hvilke krav som følger av "roaming".

(Her spørres IKKE om en detaljert gjennomgang av mobil IP.)

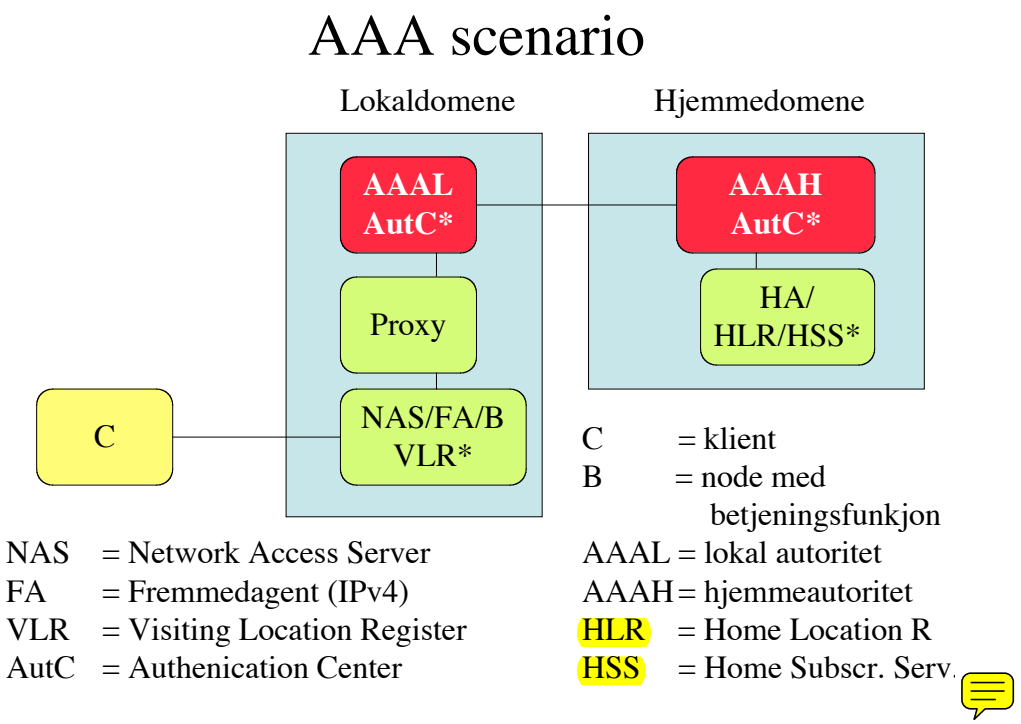
SVAR: (Hentet fra side 141 og etterfølende i kompendiet- Et så omfattende beretning som den som gis her kreves ikke for full uttelling)

12.1 AAA Basismodell

I dette kapitlet prøver vi beskrive hovedegenskapene til et grunnleggende skjema for AAA tjenere. Generelt kan vi tenke oss et scenario som vist i figur 12.1. I Internett vil en klient som hører til et administrativt domene (kalt hjemmedomenet) ofte trenge ressurser tilknyttet et annet administrativt domene (kalt fremmeddomenet). En agent i fremmeddomenet som betjener klientens forespørsler vil sannsynligvis kreve at klienten foreviser noen fullmakter som kan autentiseres, før tilgang gis. Disse fullmakter kan være slik at de kan tolkes i fremmeddomenet, men mange ganger vil de være gitt og kunne autentiseres kun av funksjoner i hjemmeområdet. De kan f.eks. benyttes for å sette opp en sikker forbindelse til den mobile node.

Betjeningsnoden har ofte ikke direkte adgang til data som trengs for å sluttføre transaksjonen. Men det forutsettes at den konsulterer en autoritet (som regel i det

samme administrative domenet) for å skaffe seg bevis for klienten har akseptable fullmakter. Siden betjeningsnoden og den lokale autoritet tilhører samme administrasjon antar man at de har etablert eller er i stand til å etablere med tilstrekkelig varighet, en sikker kanal som tillater utveksling av info relatert til adgangskontroll, samtidig som kanalen holdes skjult (i det minste) for besøkende node.



Figur 12.1: AAA tjenere i hjemme- og lokal-domenene (uttrykk merket med *, er alternative GSM/UMTS betegnelser)

Lokal autoritet har ikke alltid nok informasjon, for å kunne verifisere klientens fullmakter . Imidlertid forutsettes det at AAAL (i motsetning til betjeningsnoden) kan forhandle seg frem til en verifikasjons ved hjelp av eksterne autoriteter. De lokale og eksterne autoriteter bør utstyres med tilstrekkelige sikringsverktøy og sikkerhetsassosiasjoner, fortrinnsvis slik at de uten assistanse fra tredjepart kan forhandle fram autorisasjon som gir klienten adgang til de forspurte ressurser (eller noen av dem). I mange tilfelle vil autorisasjon bare være avhengig av en autentisering av klientens fullmakter. Betjeningsnoden vil normalt gi adgang til de forespurte ressurser så snart autorisasjon er gitt.

Det hører med til bildet at det kan være mange betjeningsnoder i et hvert AAAL og at et AAAL kan innholde mange klienter fra mange forskjellige hjemmedomener. Ethvert hjemmedomene må bringe tilveie en AAAH som kan sjekke ut tilsendte fullmakter tilhørende klienter administrert i eget domene. Figur 12.1 angir implisitt et skjema en virkemåte for informasjonssikring og det er viktig å fastlegge de spesielle sikkerhetsassosiasjoner som blir antatt som forutsetning her.

For det første er det er naturlig å anta at klienten har en etablerte sikkerhetassosiasjon med AAAH, siden dette (sånn omtrent) må være hva som menes, når vi sier at klienten hører til hjemmedomenet.

For det andre, sett ut fra figur 12.1 så er det klart at AAAL og AAH må dele en sikkerhetsassosiasjon, for å kunne stole på svar på autentiseringsønsker, autorisasjoner osv., eller på regnskapsdata som blir utvekslet. Å kreve slike tosidige sikkerhetsavtaler blir i det lang løp tungvint. AAA rammeverket bør derfor gi mer skalerbare mekanismer som antydet nedenfor.

Til sist viser figuren at betjeningsnoden på en naturlig måte kan ha en sikker kanal til AAAL. Dette er nødvendig for å få skjemaet til å virke, fordi betjeningsnoden må vite om det er lovlig å tilordne lokal ressurser til klienten.

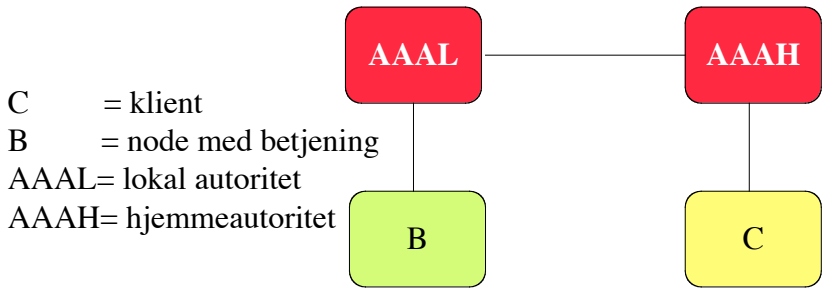
RADIUS protokollen anvendt i dagens internett, kan brukes som et implementeringseksempel på en slik sikkerhetsarkitektur. Den kan brukes for å gi mobile datamaskinklienter adgang via en lokal ISP (forskjellig fra "hjemme-ISPen"). ISP-en må forsikre seg om at den mobile klienten kan betale for tilgangen. Så snart klienten har oversendt sine fullmakter, kontakter ISPen derfor klientens hjemmeautoritet for å få verifisert signatur, og få en forsikring om betaling. I et slikt tilfelle kan betjeningsnoden realiseres som en NAS (Network Access Server) og de lokale autoriteter og hjemmeautoriteten kan bruke RADIUS tjenere. Fullmakter som gir autorisasjon hos en betjeningsnode bør (helst) være ubrukbar for fremtidige autorisasjoner hos samme eller andre betjeningsnoder.

Fra beskrivelsen og eksemplet ovenfor kan vi identifisere flere krav:

- Enhver lokal betjeningsnode bør ha en sikkerhetsrelasjon med den lokale AAA tjener (AAAL).
- Lokal autoritet må dele, eller dynamisk etablere sikkerhetsrelasjoner med eksterne autoriteter som er i stand til a sjekke klientfullmakter.
- Betjeningsnoden må kunne holde rede på tilstand for klientforespørsler mens lokal autoritet kontakter passende ekstern autoritet.
- Siden den mobile node ikke nødvendigvis starter sin "karriere" med å være tilstede i eget hjemmedomene, så må den være i stand til å bringe til veie fullstendige, men uforfalskbare fullmakter uten noen gang å ha vært i kontakt med hjemmedomenet.
- Siden den mobile nodes fullmakter/adgangstegn må holdes uforfalskbare, så må ikke mellomliggende noder (enten de nå er betjeningsnoden eller AAAL) være i stand til å lære noe om beskyttet sikret informasjon som setter dem i stand til å rekonstruere og gjenbruke fullmakter.

Ut fra det siste kravet så kan vi se årsaken til det naturlige krav om at klienten må kunne dele eller dynamisk kunne etablere en sikkerhetsassosiasjon med ekstern autoritet i hjemmedomenet. Ellers blir det teknisk sett ugjørlig (med nettverks-topologi som vist) for klienten å produsere uforfalskbare signaturer som kan verifiseres av AAAH. Figur 12.2 illustrere de naturlige sikkerhetsassosiasjon vi får med vårt skjema. Bemerk at i følge senere diskusjon, så kan man innføre en tiltrodd 3.dje part mellom AAAL og AAAH for å sikre et mer skalerbart system.

Sikkerhetsassosiasjoner



Figur 12.2: Sikkerhetsassosiasjoner

I flere RFCer betraktes en sikkerhetsassosiasjon på simpleks basis (enveis), dvs. den dekker bare trafikk i en retning. For å beskytte toveis trafikk må man definere en assosiasjon for hver retning. En sikkerhetsassosiasjon består i en virksom avtale om å bruke en gitt oppskrift for sikring (dette kan for eksempel medføre delt kjennskap til nøkler).

Til kravene ovenfor spesifiseres det tilleggsbetingelser som har sin bakgrunn i driftserfaring med dagens protokoller for mobilhåndtering (roaming):

- En betjeningsnode må kunne håndtere forespørsler fra mange klienter samtidig.
- Betjeningsnoden må beskytte mot ”replay attacks”.
- Utstyr for betjeningsnode bør være så billig som mulig, siden det vil bli installert mange kopier for å kunne håndtere mange samtidige klienter. ,
- Betjeningsnodene bør bli konfigurert til å kunne innhente autorisasjon fra en tiltrodd lokal AAA tjener for QoS krav fra klienter.

Nodene i to separate administrative domener må ofte foreta seg flere ting for å identifisere kommuniserende partnerer eller skjerme kommunikasjonen mellom dem. Dette beskrives ikke her. Legg derimot merke til at nødvendige sikkerhetsassosiasjoner mellom mobile IP enheter får en sentral betydning når det gjelder design av en passende AAA infrastruktur. Det har vist seg hensiktmessig å ustyre B med mulighet for å terminere/avbryte tjenestetilgang basert på anmoding fra AAAH eller AAAL.

AAA Protokoll ”Roaming” krav

Basert på erfaring fra ISP-er som har administrert nett-tilgang basert på RADIUS protokollen har følgene tilleggskrav kommet opp (fremstillingen her er sterkt forkortet i forhold til originalen):

- Digitale sertifikater bør kunne fraktes i en AAA melding (for å unngå for mange meldingsrunder). AAA infrastruktur bør også kunne assisterer med hensyn på validering av fullmakter, slik at fremmedagenten og hjemmeagenten blir avlastet dette.
- Støtte for beskyttelse mot ”replay” og støtte for ”ikke-fornekt” for alle meldinger som gjelder autorisasjon og regnskapsdata.
- Støtte for regnskapsføring, både bilateralt og via megler, dvs. AAA noder med ”clearinghouse”-funksjon. Sanntids regnskap må bli støttet, og alle regnskapsmeldinger må innholde tidsstempel.

3. Metaprotokoll (10%)

3.1 Begrunnelse

Tiphon modellen prøver å legge opp til et generelt og fleksibelt rammeverk for fremtidig utvikling (og vedlikehold) av systemspesifikasjonen ved å benytte noe som kalles metaprotokoller.

a) Diskutere hva som menes med en metaprotokoll og
b) Hvilke fordeler som oppnåes.

SVAR: - både på a og b, hentet fra side 34 og 35 i kompendiet.
Litt om Tiphonmodellen.

I release 4 av Tiphon undersøker man hvordan man kan realisere telefonitjenester i heterogene omgivelser. Man har utviklet en generell metodikk som tillater en å lage tjenester uavhengig av den spesifikke netteknologi (f.eks. linje- eller pakkesvitsjing). Man har funnet fram til en felles omsluttende metodikk og en generisk meta-protokoll, dvs. et domeneuavhengig protokollrammeverk.

Arkitekturer støtter systemer hvor anrop kan traverserer mange operatørers nett, som kan anvende forskjellige transportprotokoller og signaleringssystemer. For å oppnå dette, så skaper man en transportuavhengig, funksjonell modell for operatørdomenet. Dette skaper en løsning hvor man for eksempel kan adressere introduksjon av nye tjenester uavhengig av samvirke mellom forskjellige transportmodi. Man foreslår en modell som grupperer transportrelaterte og applikasjonsrelaterte funksjoner i forskjellige plan. Disse planene blir igjen delt i lag. Elementer i disse lagene kan brukes som byggesteiner for framtidige generasjoner av liknende tjenester. Meta-protokollene blir anvendt til å lage profiler for protokoller assosiert med enhver gitt kommunikasjonsteknikk. Ved å mappe denne ”meta-protokollen” til det spesifikke nettløsningen, så kan man sikre en effektiv veg for å realisere sammenkobling ende til

ende.

Ved å anvende denne tilnærmingen får man en arkitektur for pakkesvitsjet telefoni som kan anvendes for et tjenestetilbud tilsvarende det man har i tradisjonelle telefonnett, og som kan tilby en utviklingsvei over mot bredbåndsapplikasjoner så vel som mobile anvendelser.

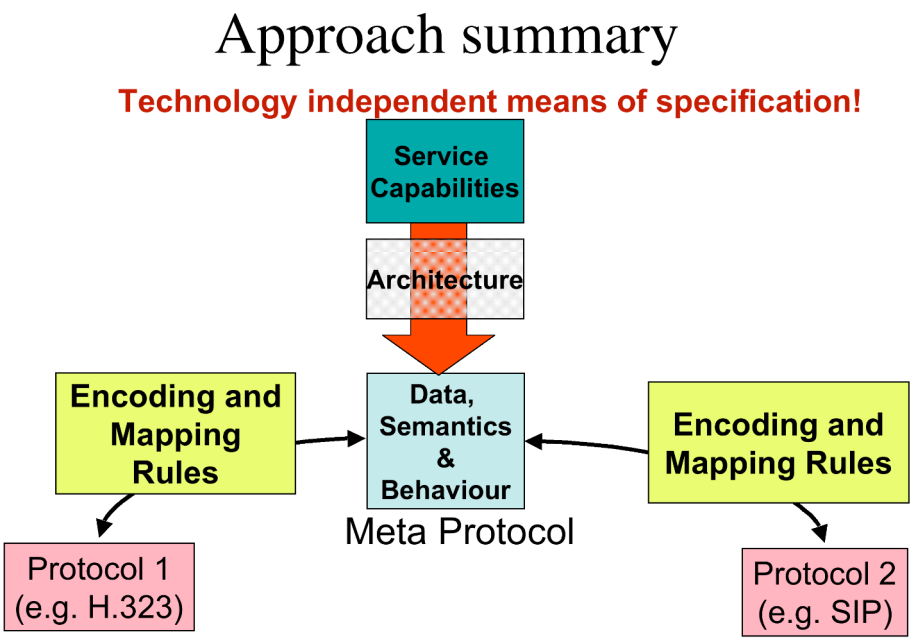
Tjenester og anvendelser som, multimediekonferanse, "instant messaging" og e-handel går lenger enn det som dekkes av dagens offentlige telefontjeneste (PSTN) eller basis internett-tilkobling. Disse vil bli behandlet i en senere utgave av Tiphon.

Introduksjon til TIPHON metaprotokollen

I telekommunikasjonsindustrien har man en lang tradisjon for å utvikle spesielle protokoller for de individuelle tjenestene. Ofte brukte man forskjellige versjoner av den samme protokollen eller man hadde sameksistens av mange protokoller som løste det samme problem. Når det gjelder mulig samvirke, så representerte en slik flora av protokoller en betydelig utfordring, fordi hver av dem antar at de meldinger og grensesnitt som definere tjenestene er tilgjengelig. Konsekvensen er ofte at tjenestedefinisjonene blir litt forskjellige på hver sin side av et samarbeidspunkt, ofte på en litt subtil måte. Dette betyr at samvirke er et komplisert problem som medfører et stor antall kompromisser. For å være litt mer konkret, hvis *n* protokoller skal samvirke så trenges det utviklet *n x (n-1)* "samarbeidsoppskrifter" .
TIPHON Release 3 innfører bruk av en metaprotokoll som håndterer kompleksiteten ved multiprotokoll samvirke. En metaprotokoll beskriver meldinger som skal sendes, deres informasjonsinnhold og oppførselen til systemene – når meldinger skal sendes og når de skal mottas. En slik metaprotokoll er ikke designet for realisering direkte, men tjener som en referanse for andre protokoller. Her kan man definere realiseringer for *n* forskjelllige virkelige protokoller ved hjelp av *n* avbildninger eller "mappinger". Slike realiseringer vil man da lett få til å samarbeide, siden deres oppførsel og informasjonsinnhold er en realisering av den sammen metaprotokoll. Figur 5.1, illustrerer prosessen. Samvirkeprosesser blir definert ved hjelp av regler for koding, mapping av meldinger og modifikasjon av tilstander i samvirkepunktene. Mappingen eller avbildningen må også ta hensyn til oppførselen i de underliggende transportlag og beskytte mot meldingstap. Det er en komplisert oppgave å utarbeide en slik avbildning. En rekke slike avbildninger er nå publisert. Mer detaljerte opplysinger om metodikken kan finnes i ETSI TS 101 882-1[1]

Det blir imidlertid ikke alltid mulig å anvende en metaprotokoll for å generere en fullstendig avbildning over til en gitt protokoll. Dette resulterer enten i at man må definere utvidelser til den eksisterende metaprotokollen, eller mangler ved den valgte protokoll.

[1] Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Part 1: Meta-protocol design rules, development method, and mapping guideline



Figur 5.1: Samvirke definert ved hjelp av meta-protokoll.

Mer formelt, så definerer TIPHON meta-protokollen en funksjonalitet på applikasjonslagsnivå som omfatter en mengde applikasjoner som anses nødvendige i neste generasjons telefoni. Den tilveiebringer et funksjonsrepertoar som støtter telefonianvendelser på en protokoll- og transportuavhengig måte. Meta-protokollen består av tilstandsmaskiner som kan utføre anropsbehandling/sesjonsstyring. Forskjellige standard (og ikkestandardiserte) protokoller kan bli mappet inn i dette funksjonsrepertoaret for å realisere samvirke. Metaprotokollen kan bli implementert fullstendig i den hensikt å utvikle applikasjonstjenere, eller den kan bli brukt som et verktøy for å utvide supplere eksisterende protokoller og sørge for samvirke mellom dem.

4. Litt av hvert (20%)

a) Hva er TMN og hva brukes det til?
SVAR:
TMN står for Telecommunication Management Network, dette er et administrasjonssystem utviklet av ITU-T (M.3010) for telenett. System definer en informasjonsarkitektur, en funksjonell arkitektur, og en fysisk arkitektur, med tilhørende grensesnitt.(se kapitel 14.4). M.3010 danner basis for (nesten) alle nettadministrasjonssystemer som er i drift (for PSTN og ISDN nett). Og vil også bli tatt i bruk for NGN.

b) Skisser arkitektur for signaleringssystem nr. 7 (SS7)
SVAR Fra kompemdium kap 4 (mer utfyllende en det som kreves).
Telesystemene er viktige for samfunnet (og også for operatørene), derfor har det vært strenge krav til disse felleskanalsystemene med hensyn oppetid, feilfrihet osv..
Strengere enn tilsvarende krav til tidligere dataoverføringssystemer. Disse krav gjorde

at man valgte å definere protokoller og funksjoner helt fra grunnen i det første store felleskanalsystem for den "digitale æra", nemlig Signaleringssystem nr. 7 (SS7). SS7 brukes fortsatt i stor utstrekning, og vil sannsynligvis bli modifisert og tilpasset også til morgendagens nett. SS7 nett og protokoller benyttes som hjelpemiddel til å effektuere:

- Basis anropsstyring, administrasjon og nedkobling.
- Mobile tjenester, som i GSM, for å realisere "roaming", autentisering etc.
- Portabilitet av lokalnummer
- Håndtering av ikke-geografiske nummer, og "grønne nummer", slike som 800 xxx
- Utvidet tjenesterepertoar: medflytting, overføring av samtale til annen abonnent, vise nummeret til den som har ringt, manøvrering av treparts samtaler, osv.
- Sikre effektiv og sikker kommunikasjon på en global basis.

Legg merke til at det ovenfor står hjelpemiddel til å effektuere. SS7 skaper, på en måte språket (ved sine definerte meldingsformer) og kommunikasjonssystemet (ved det fysiske system) som sikrer at meldingen blir overført. For å realisere funksjoner som angitt, trenger vi også enheter i nettet som tolker disse meldingene og reagerer på en hensiktsmessig måte. Slik prosessering kan være realisert i enheter som SCP (Service Control Point) i IN, HLR (Home Location Register) og AuC (Authentication Center) i GSM, osv. Dette for å understreke at SS7 ikke "fikser alt". Det stilles store krav til pålitelighet og datasikkerhet i et slikt signaleringssystem. SS7 ble påbegynt i en tid da sambandskvaliteten var vesentlig dårligere enn i dag. Det var derfor naturlig "å sikre dataoverføringen godt", dette ble gjort ved å skreddersy rutiner helt fra fysisk lag og opp.

SS7 rekommandasjonen kan således deles i to:

- "Message Transfer Part",
  som beskriver virkemåte på fysisk lag, linklag og nettverkslag, og

- en "User Part" (forfatters betegnelse),
  som består av 3 "hovedsøyler": "ISDN User Part" (ofte gjengitt som ISUP), "Telephone User Part" (TUP) og en sammensatt med "Signaling Connection Control Part" (SCCP) i bunnen og "Transaction Capabilities Application Part" (TC eller TCAP) over.

Arkitekturen, ifølge ITU-T er illustrert i figur 4.2

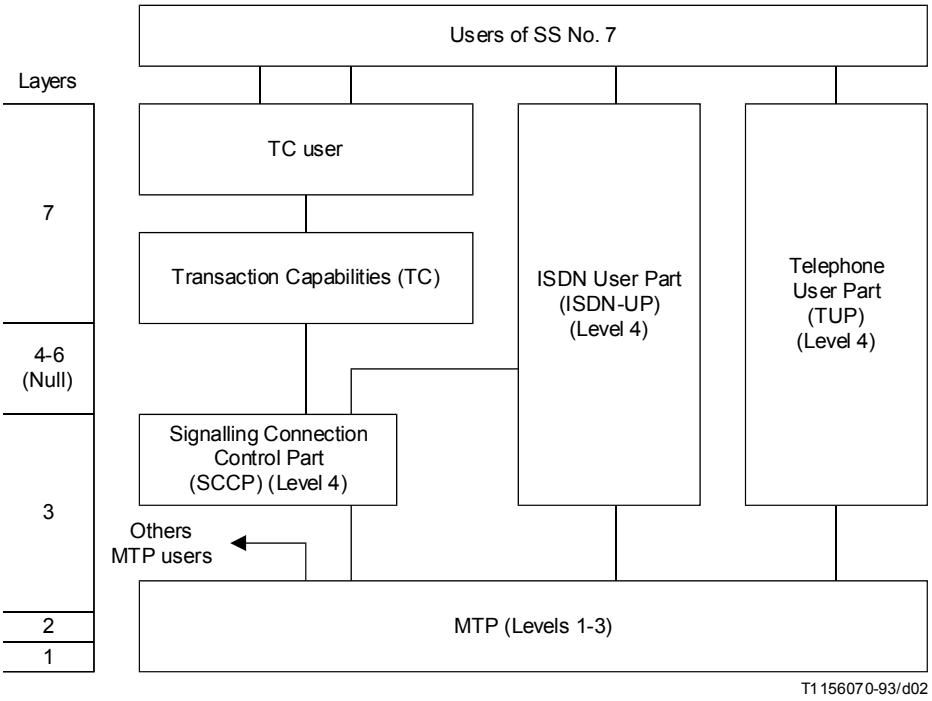


FIGURE 2/Q.700

Architecture of SS No. 7

Figur 4.1 Arkitektur for Signaleringssystem nr. 7, hentet fra T-Req-Q.700

Message Transfer part

Message Transfer Part (MTP) funksjonalitet sørger for at informasjon fra User Part kan bli transportert "tverrsover" SS7 nettet til ønsket mottaker.

Hensikten er å tilveiebringe:

a) Pålitelig transport og levering av "User Part" signaleringsinformasjon tverrsover SS7 nettet;
b) Evne til å reagere på system and nett feil som vil ha følger for punkt a) og ta nødvendige aksjoner for sørge for at a) allikevel blir utført.

I sum realiserer MTP en oppsetningsfri (eller "forbindelsesløs") overføring med bibehold av intern sekvens. Kombinasjonen av MTP og SCCP (Signalling Connection Control Part) kalles av og til Network Service Part (NSP) og leverer samlet en tjeneste som svarer til nivå 3 i OSI modellen. (En "ren" avbilding over til OSI modellen er ikke helt enkel i dette tilfelle!)

"Brukere" av MTP er SCCP, Telephone User Part (TUP), Data User Part (DUP) (Recommendation Q.741) og ISDN User Part (ISUP) (Recommendation Q.761-Q.766).

SS7 nett kan altså brukes til å sammenbinde mange slags kommunikasjonssystemer. Det representer et slags pakkesvitsjet datanett, som også har fått definert sine egne rutere.
Disse kalles STP Signal Transfer Points, og benyttes blant annet for følgende formål:

- Reduksjon av antall signaleringslinker som kreves (mer ”stjerne” enn ”full maske”).
- For å kunne fordele signaleringslasten på flere mottakere avhengig av feiltilstand eller trafikk (f.eks. fordeling til en av flere mulige ”Service Control Points”, se kapitel 6).
- For å foreta adresseoversetting (mellom nett med forskjellige intern struktur på SS7 adresser – svarene f.eks. til forskjellige generasjon av nett)
- For å filtrere SS7 meldinger fra andre nett (brannmurfunksjon).

For 3 generasjons mobilnett, hvor man også planlegger å bruke SS7, har man valgt å erstatte MTP (Message Transfer Part) med IP versjon 6. Imidlertid lar ikke SCCP seg enkelt innpasse i dette skjemaet, og verken TCP eller UDP gir nok støttefunksjoner til punktene a) og b) ovenfor. – Man arbeidet lenge med et ”påbygg” til en av disse protokollene. Men i samarbeid med IETF har man nå kommet fram til en ny transportprotokoll SCTP eller ”Stream Control Transport Protocol”, som kommuniserer direkte med IP laget (altså er på samme protokollnivå som TCP og UDP). Denne vil bli brukt som transportmekanisme for SS7 (User parts) i fremtidige nett.

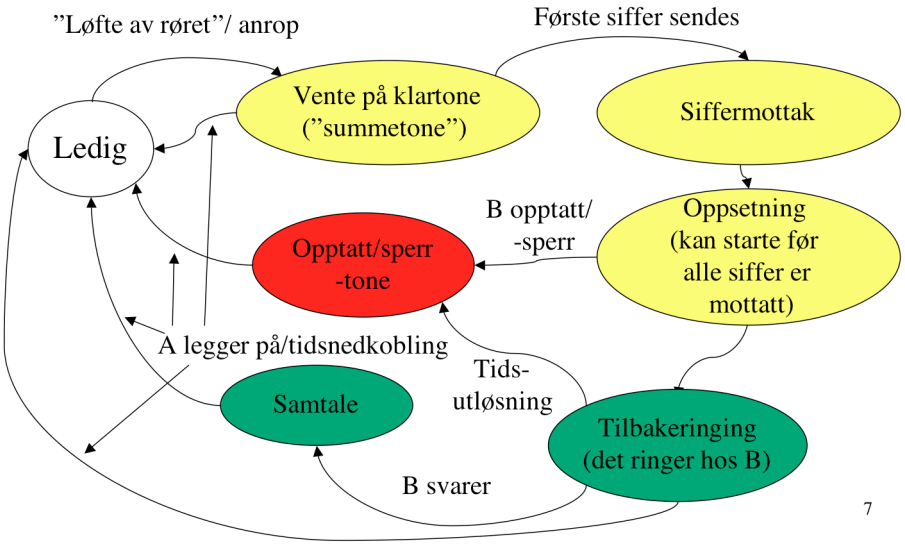
c) Hva brukes SS7 til? - Benytter TMN SS7?

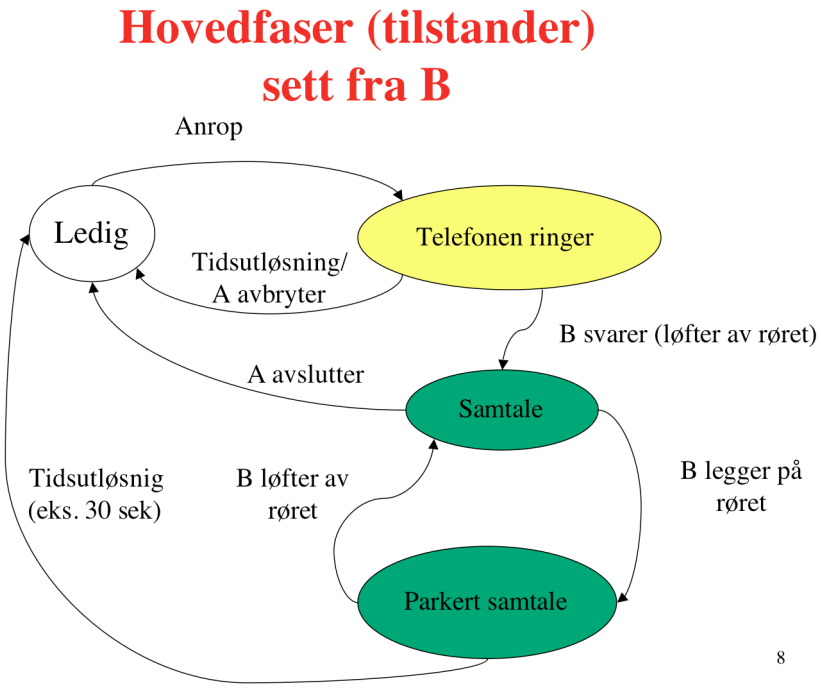
SVAR: Første del stort sett besvart ovenfor. TMN benytter seg ikke av SS7, men har vært spesifisert med bruk av X.25 Virtuell linjesvitsjing på datalinker mellom nettnodene.

d) Skisser og tegn en tilstandsmodell for hovedfasene til en ”basic” PSTN telefonsamtale referert til både A side (en tegning) og B side (en tegning).

SVAR: (hentet fra kompendium)

Hovedfaser (tilstander) sett fra A





Figur 3.3 Hovedfaser sett fra B-siden

e) **Hvilken funksjonalitet ligger innebygget i et SSP (”Signaling Switching Point”).**

SVAR:

Evne til å analysere siffer (nummer) informasjon for å avgjøre om et anrop trenger assistanse fra IN. Hvis ja, evne til å parkere videre anropsoppsett, initiere henvendelse med IN, og deretter koble opp i følge det svar man får. (Kan medføre oppkobling mot Intelligen Periheral). - Dette er hovedfunksjonene som omfatter implementering av de standardiserte funksjonene SCF (Service Control Function), SSF (Service Switching Function) og CCF (Call Control Function). I tillegg kan en SSP ut fra praktiske formål innholde en rekke andre funksjoner som CCAF, SRF, SDF etc.

f) **Hvordan er NAI (Network Access Identifier) bygget opp og hvilke fordeler /ulemper ser du ved å bruke denne framfor IP adressen som referanse ved mobilhåndtering?**

SVAR hentet fra kompendiet kapitel 10, dette er mye mer en det som trengs. !

NAI - Identifikasjon av mobile brukere i Internett.

I Internet sammenheng er det en økende forståelse for at en person/bruker kan bevege seg mellom mange IP adresser. Med hensyn på AAA funksjoner kan det ofte være viktigere å verifisere brukeren enn utstyret. For å oppnå dette trenger man, på samme måte som i GSM/UMTS sammenheng, å definere et globalt navnerom for brukeridentiteter. Syntaks er formelt beskrevet i RFC. 2486 “Network Access Identifier”. Formatet er på formen:

<brukernavn>@<fullt kvalifisert domenenavn>

hvilket tilsvarer en e-post adresse. Legg merke til at domenenavnet er med. Dette gir et hierarkisk navnerom. Brukernavnet forutsettes å være entydig innen det oppgitte domene. Ved autentisering kan en lokal AAA tjener bruke domenenavnet for å finne hjemmeområdet til brukeren, og derved finne adressen til den AAAH tjener hvor brukeren er "kunde". Grovt sett kan vi si at NAI har samme funksjon i Internet som IMSI i UMTS/GSM.

Med hensyn på det fremtidige IP baserte Multimedia Kjernenett (IM CN) så opererer man med i 3 typer IP adresser eller identiteter:

Privat brukeridentitet
Denne tilordnes av hjemmeoperatøren og brukes for all håndtering av abonnement og regninger. Den identifiserer "brukeren". Den har en form som beskrevet i RFC 2486 (typisk "bruker@tele.com"), den blir permanent tilordnet til brukeren (abonnementet). Denne identiteten vil blant annet bli

- lagret i HSS.
- funnet av og mellomlagret av S-CSCF under registrering

Offentlig brukeridentitet.
Dette er den gyldige "anropsidentiteten", den offentlige adressen som kan stå på et visittkort. Denne formen for id. kan inneholde et telefonnummer eller være utformet i følge internetts navneskjema. Minst en slik skal være lagret i ISIM (IP Multimedia Identity Module)applikasjonen på USIM en.
Denne skal ha form som en SIP URL (som definert i RFC 3261 og RFC2396 eller eventuelt foreligge i "tel:"-URL formatet som angitt i RFC 2806)

Temporær offentlig brukeridentitet:
For tidlige anvendelser (før release 5) har man innført en mulighet for å la systemet sette sammen en "temporær offentlig brukeridentitet". Det er lagt en del begrensinger på denne formeren for brukeridentitet, blant annet vil den aldri komme tilsyne i apparatets display, den skal ikke bruke på visittkort etc. Men det blir en slags "katalogadresse", for nettinterne formål. Identiteten vil bli utledet på grunnlag av IMSI og bli lagret på USIM og i HSS.

Diskusjon (ikke hentet fra kompendiet).
NAI tilsvarer IMSI og er velegnet til håndtering av roaming. Mobil IP har i utagangspunkt samme funksjon. I praksis vil man sannsynligvis komme til å bruke NAI som indentifikator for abonnement. IP adresse kan tilordnes dynamisk når brukere registrerer seg.

5. Stateless Network Control (10%)

a) **List opp og diskuter argumenter for hvorfor et fremtidig kjernenett (NGN) bør fremstå mest mulig som "tilstandsfritt".**

SVAR: (forsøk på)

Et nett med liten monitorering av tilstander er lettere å bygge opp for store hastigheter. Mye mindre ressurers trengs for registrering og monitorering av tilstander. Et nett med en enkel transportmekanisme blir også mer fleksiblet med hensyn på fremtidig tjenesteutvalg. Se ellers artikkelen "Dawn of the Stupid Network". Dette alternativ forskyver" intelligensen" til kanten av nettet

b) **List opp og diskuter argumenter for at fremtidens kjernenett må/bør utbygges med omfattende tilstandsstyring/monitorering.**

SVAR:

Et "dumt" nett kan lettere bli utsatt for jamming, ukontrollert trafikkpåtrykk som kan gi "Denial of Service". Det kan være vanskeligere å garanterer/sikre tenestekvalitet i et "dumt" nettt. Og til slutt: Tradisjonelle teleoperatører liker å holde på sin markedposisjon, betaling for en ren transportjenester vil sannsynligivis ikke gi store fortjenestemarginer.

En kan også referer til, både for både a) og b) diskusjon om Internettscenariet ("dumt" nett) og teleoperatørscenariet ("tilstandsrikt" nett) slik den er gjengitt på side 33 i kompendiet:

- **"Internettscenariet"**
  - Sammenkoblede nett vil i hovedsak sørge for å koble sluttbrukere effektivt sammen, vil frakte datapakker mellom "smarte" terminals og vil etablere ende-til-ende sesjoner styrt av terminal, når dette er nødvendig.
  - Tjenester frembringes i hovedsak ved samvirke mellom sluttbrukerutstyr (som illustrert blant annet ved tjenestene til "telio.no" og i MicroSoft Network).
  - Tradisjonelle operatørbaserte tjenester vil ha synkende markedsandeler.

- **"Teleoperatørscenariet"**
  - Tjeneste vil primært bli produsert i sammenkoblede nett, som vil være drevet av "multimedieoperatører". Man vil anvende smarte og "dumme" terminaler i en hensiktmessig blanding. Operatørene vil styre sluttbrukertjenestene, basert på brukernes ønsker (som signaleres til nettet).
  - Nåværende telenett vil utvikles slik at de kan støtte multimedia og skape en plattform for nestegenerasjons nett (NGN).
  - Mye av tjenesteutvikling/etablering vil komme fra offentlig nettoperatører. Slik tjenesteutvikling og realisering vil bli støttet ved høynivå tjenester/funksjoner utviklet for åpne, standardiserte grensesnitt.

- **Hvis Internettscenariet blir dominerende, får vi følgende situasjon:**
  - Ende-til-ende samvirke vil avhenge av terminalutstyrets evne til å virke sammen.
    - Erfaringer fra databransjen har vist at dette ikke vil være selvsagt og det er sannsynlig at ulike proprietære løsninger vil konkurrere og at mulighet for å koble enhver sammen vil bli mistet.

        - Samvirke med PSTN vil være relativt enkelt å oppnå, men adgang fra PSTN til det nye nettet vil sannsynligvis være mer problematisk.
    - ETSIs mulighet for å definere standarder for fremtidige nett av denne typen vil være begrenset.

- **Hvis Teleoperatørscenariet blir dominerende, får vi en litt annen situasjon:**
    - Ende-til-ende samvirke vil være avhengig av arkitekturene i de nye nettene og av de samarbeidsavtaler som er inngått.
    - ETSIs rolle i å etablere standarder for detter rammeverket vil være betydelig (og er basis for mye av nåværende arbeid).

6. VoIP og samdrift med PSTN (25%)

6.1 Protokollarkitekturer

Gi en kortfattet beskrivelse/skisse – (illustrer gjerne med figurer) følgende "standarder":

a) SIP protokollen

SVAR: Se kompendiet sidene 77 til 81 (se vedlegg)

b) H.323

SVAR: Passende utdrag av presentasjonen gitt i vedlegg D (**http://www.swrich.ch/vconf/ws2003/h323_basics_handout.pdf**). Fremstillingen bør inneholde en oversikt over de komponenter som inngår (f.eks. "Gatekeeper") og hvilke protokoller som anvendes (f. eks. RAS, Q931, H245 etc).

(Maks 4 sider på hver).

For SIP kan man stort sett nøye seg med å referere til "Internet" versjonen (man kan slippe å betrakte 3GPP)

6.2 Samvirkeproblematikk

Hvilke samarbeidsproblemer må løses ved samtrafikk mellom

a) Nett basert på henholdsvis SIP og H.323,
b) PSTN/ISDN og nett basert på SIP,
c) PSTN/ISDN og nett basert på H.323?

Du kan (stort sett) svare på b) og c) samtidig.
Diskuter også hvilke faktorer som spiller inn med hensyn av valg av punkt for overgang. - Med et globalt internett og et globalt PSTN, hvilket samtrafikkpunkt skal man velge (hvor bør det ligge)?

SVAR: Se kapitel 13, særlig sidene 160-164.
H.323 vil gi en noe enklere realisering av samdrift med PSTN/ISDN på styringssiden, siden H.323 her baserer seg på tradisjonelle "teleprotokoller". Ved samtrafikk mellom

SIP og H.323 er det i hovedsak signaleringsprotokollene som må oversettes, mediet kan (betinget) være formattert og kodet på samme vis.

Det er flere faktorer som vil være avgjørende for valg av overgangspunkt:

- Regulatoriske forhold,
- Tjenestekvalitet (linjesvitsjet nett kan i dag tilby en bedre garanti for tjenestekvalitet Dette medfører at man bør velge lengst mulig veg med linjesvitsjing).
- Pris (internett gir mye billigere transport- minimaliser linjesvitsjet strekning.

I praksis må man velge å balansere de forskjellige hensyn.

Vedlegg:

Disse sidene er ekstrahert fra kompendiets side 77-81 (obs tatt fra PDF format tilbake til MS Word- dette kan ha forårsaket litt urydding layout)

Kapitel 9 SIP og mobilitetshåndtering ved hjelp av SIP

Session Initiation Protocol ble opprinnelig utviklet av gruppen MMU i IETF Protokollen kan brukes til å sette opp som navnet sier, sesjoner i Internett. En slik sesjon kan være en multimedia-sesjon med to eller flere parter. SIP kan brukes primært for styring (signalering) av oppsett, men kan også benyttes for å gjøre endringer underveis, gi ordre om nye mediestrømmer, om ny posisjon i nettet, eller liknende. Altså SIPs funksjoner dekker følgende:

. • **Lokalisering av bruker**: finne endesystemet som skal brukes for kommunikasjon

. • **Brukertilgjengelighet:** bestemme villighet av anropt bruker med hensyn til deltagelse i kommunikasjon;

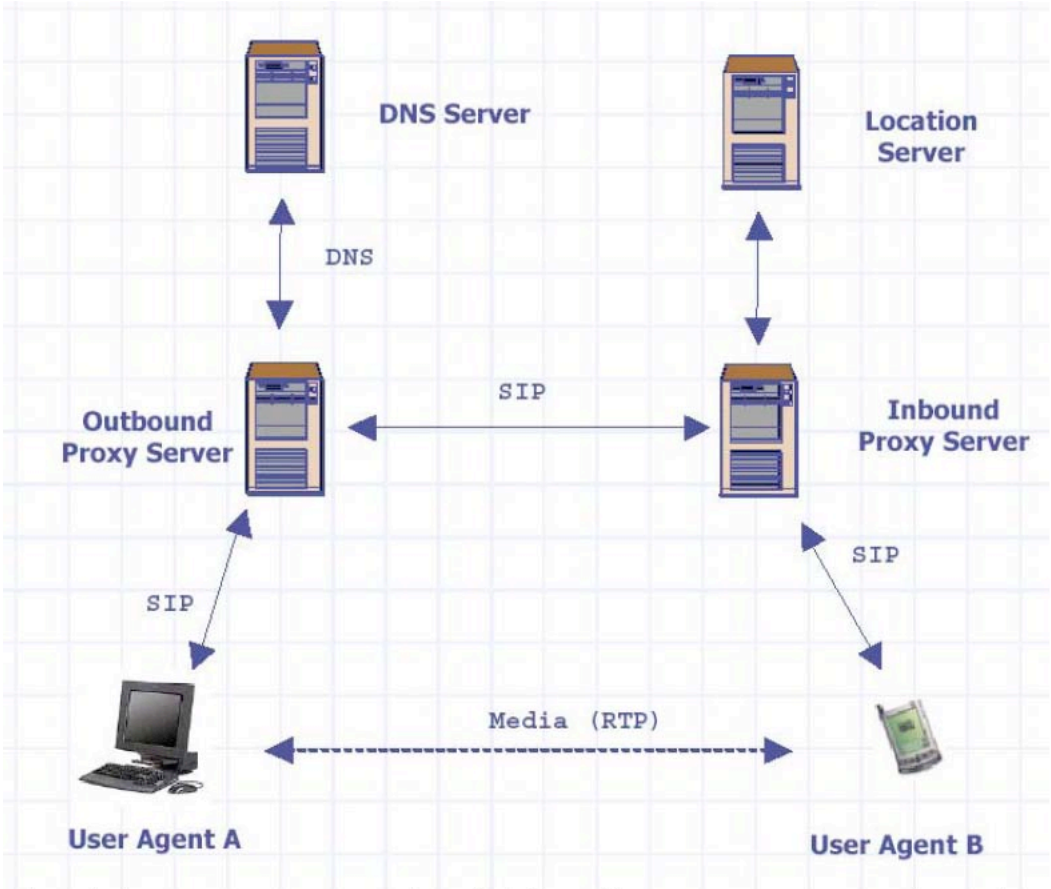
. • **Brukerprofil**: bestemme medieformer og parameter for disse som skal benyttes;

. • **Oppsetting av sesjon**: "ringing", etablering av sesjons-parametre for både anropt og anropende bruker;

. • **Sesjonsadministrasjon:** inkludert overføring og avsluting av sesjoner, modifikasjon av sesjonsparameter og igangsetting av tjenestene..

SIP beskriver selve arkitekturen for “signaleringssystemet”, i dette tilfelle. SDP ”Session Description Protocol” kan bli benyttet for å beskrive innhold i signaleringsmeldingene. Legg merke til at SIP som sådan, ikke frakter “nytteinfo” mellombruker. Men en “Invite” melding kan inneholde et bilde (f.eks. i JPEG), av den som kaller opp. Mediestrøm forutsettes håndtert ved hjelp av RTP eller liknende. 3GPP konsortiet har valgt å basere seg på SIP for oppsetning. Tilpasning til denne arkitekturen skal behandles senere, først gis en kortfattet introduksjon til SIP. Det er lagt stor vekt på gjenbruk av Internett begreper og prinsipper. Det finnes nå mer en 30 RFCer med spesifisering av forskjellig sider ved SIP. Flere handler om samvirke med PSTN.

Arkitekturen består i hovedsak av 3 typer entiteter: SIP brukeragent, SIP proxy-tjener, DNS, og lokasjonstjener. En oversikt er vist i figur. 9.1



Figur 9.1 Nett-elementer som inngår i SIP. (SIP servere kan egentlig realiseres både som proxy og som "Redirect Servers" – som gir det svar de kan gi, direkte tilbake til den som spør).

Abonnenten/brukeren forutsettes tildelt en identitet, i form av en
SIP Uniform Resource Indicator (URI)
Denne har samme formen som en email adresse: bruker@domene

Det finnes to URI skjema:

. • sip:henry@siptest.wcom.com er en SIP URI. Den mest vanlige formen, ble introdusert i RFC 2543,

. • sips:henry@siptest.wcom.com er en sikker (Secure) SIP URI . Nytt skjema ble introdusert i RFC 3261. Denne formen benytter TLS (se RFC2246) over TCP som transportmekanisme

Og to typer SIP URIs:

. • Address of Record (AOR) (identifiserer en bruker)
sip:henry@wcom.com (trenger DNS SRV records for å finne SIP tjener for wcom.com domenet)

. • Fully Qualified Domain Name (FQDN) (identifiserer en ustyrsenhet)
sip:henry@127.24.45.4 eller sip:henry@cube43.lab.wcom.com

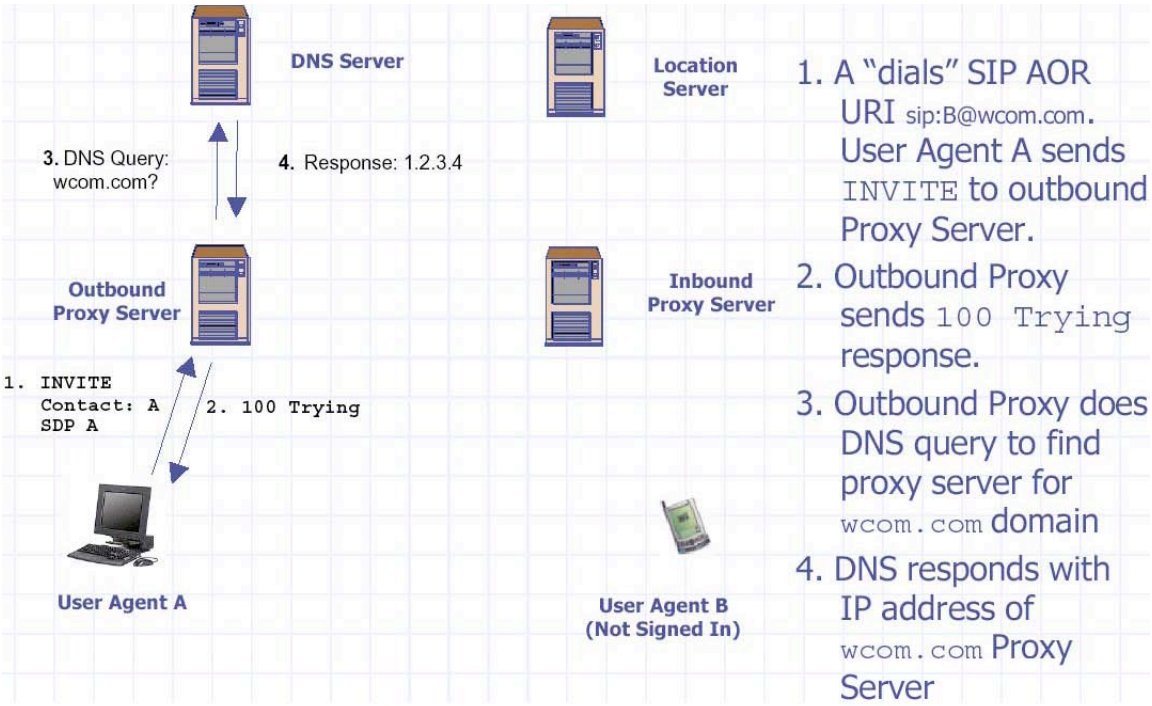
SIP meldinger: Meldingsutveksling er basert på klient, tjener prinsippet. Vi får da forespørsler/"requests" og svar/"responses", en oversikt er gitt nedenfor:

SIP Requests and Responses

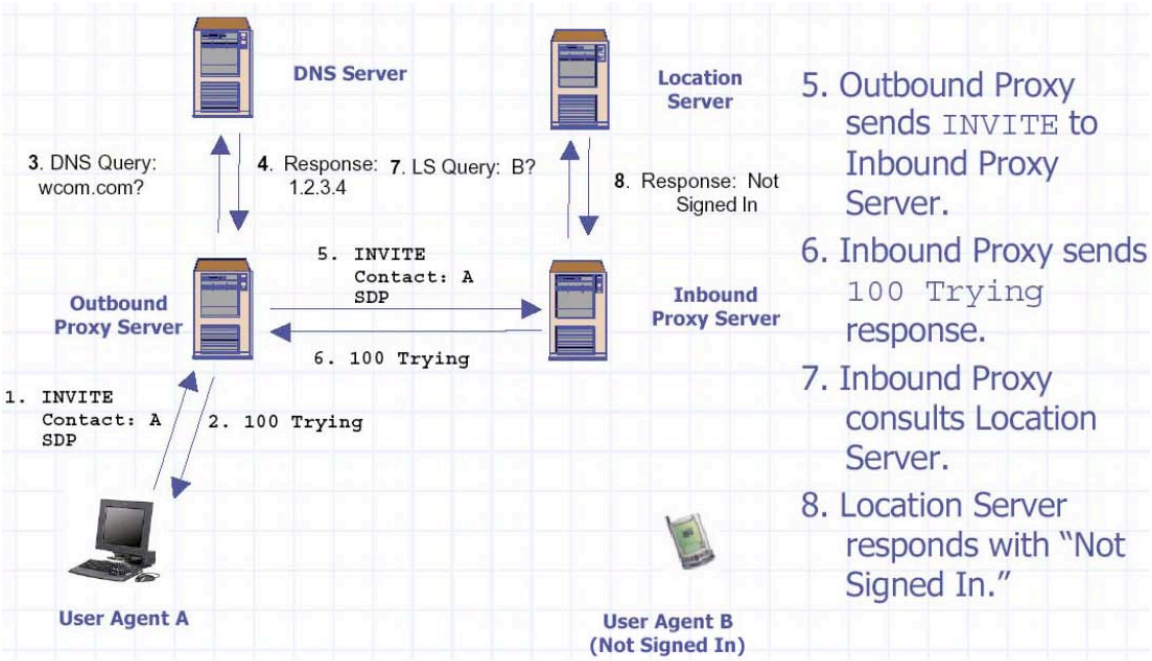
SIP Request typer blir kalt "methods".
SIP Responser bruker numeriske koder:
"Methods" i basisspesifikasjonen:
Klasser:

- **INVITE** **1xx** Informational
- **ACK** **2xx** Final
- **OPTIONS** **3xx** Redirection
- **CANCEL** **4xx** Client Error
- **BYE** **5xx** Server Error
- **REGISTER** **6xx** Global Failure **(Eksempel: 404 Not Found)**

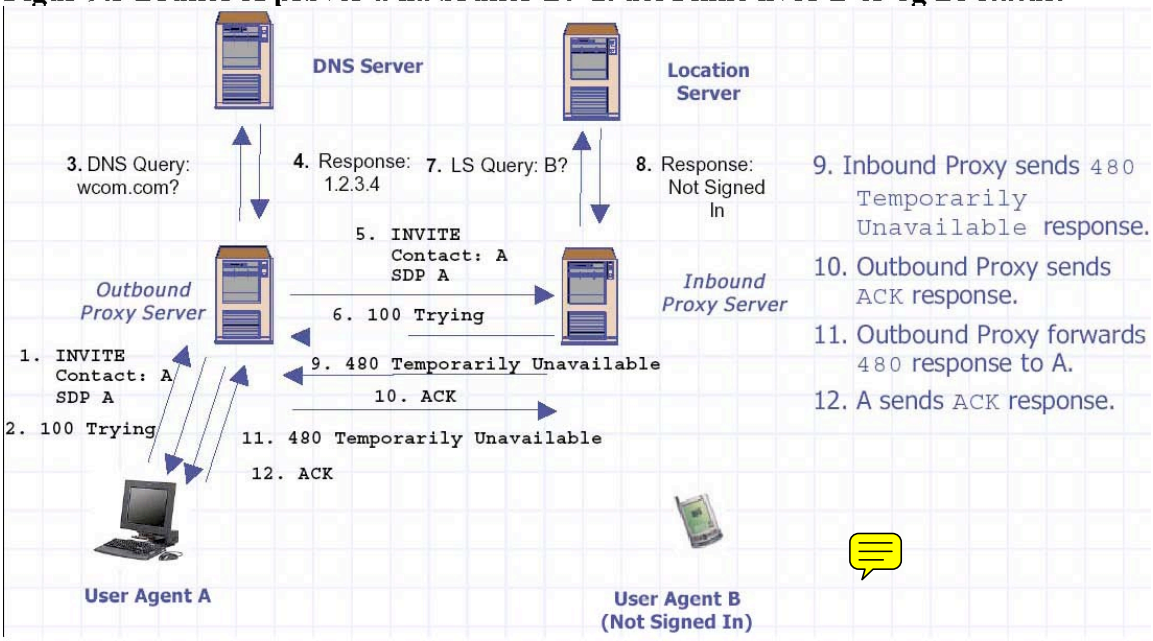
Eksempel på oppkoblingsforsøk (mislykket!) er gjengitt på figuren 9.2 – 9.4



Figur 9.2 Bruker A prøver å nå bruker B (som for øyeblikket ikke er logget på): 1.ste del finne "hjemmeserver" for B



Figur 9.3 Bruker A prøver å nå bruker B: 2. del Finne hvor B er og Bs status.



Figur 9.4 Bruker A prøver å nå bruker B: 3. del beskjed tilbake til A, om at B ikke er tilgjenglig

A kan, når han får denne beskjeden, f.eks. sende en melding til Bs location server, med anmodning om å bli varslet når B blir tilgjengelig. PCer. Portable PC-er, PDA-er og alt annet ustyr som kan bruke IP/UDP (og RTP for transport) kan ha bruker agenter. En bruker agent kan både sende og svare på "requests" (virke både som klient og tjener). En overgang mot PSTN vil inneholde en "brukeragent". Legg merke til at ikke alle signaleringsmeldinger behøver gå "innom" proxyene. De brukes bare når det behøves, eller det kan være foreskrevet av nettadministrator. Normalt vil f.eks. en "ack" på en oppkobling, kunne gå direkte.

SIP tjenerne kan realiseres som:

. • tilstandsløse tjenere
. • med tilstandsbeskrivelse for enkelttransaksjoner, eller

. • med tilstandsbeskrivelse for hele sesjoner

En proxy server kan ”forke”. Dvs, den kan videresende en forespørsel i flere retninger simultant. I et slikt tilfelle bør den han ”hukommelse” for denne transaksjon, for å hindre at multiple svar i å nå den som opprinnelig spurte. (Men dette er ikke nødvendig, det går an å konfigurer slik at responsene sendes direkte til spørrer, som da må sile svarene.)

Det finnes foreløpig spesifikasjon for to typer signaleringsoverganger: SIP-PSTN og SIP-H.323. (Vi skal beskrive H.323 senere).