UNINETT

SIP infrastruktur

9. februar 2010

Innledning

Dette dokumentet beskriver UNINETT sin foreslåtte SIP infrastruktur. Dokumentet er et resultat av arbeid gjort i GigaCampus (2006-2009) og danner et utgangspunkt for UNINETT sitt videre arbeid på området. Campuskoordineringsaktivitet er fra og med 2010 et permanent fokusområde for UNINETT. SIP infrastruktur inngår her som et sentralt satsingsområde.

Dokumentet skisserer komponentene og anbefalinger til hvordan man praktisk gjennomfører en innføring og overgang til SIP. Den beskriver også et utvalg av mulige tjenester man kan innføre. Dokumentet er ment for UH-institusjoner som ønsker å vite mer om tankene bak, teknologien og prosessen for å ta del i SIP infrastrukturen.

Dokumentet har tre hovedkapitler og tre supplerende vedlegg.

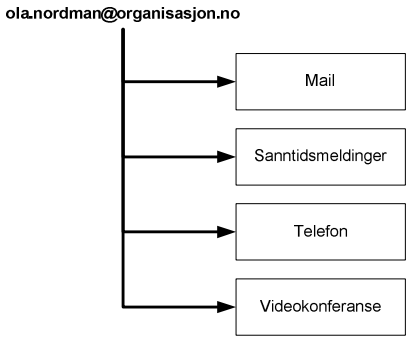
Dette dokumentet er et levende dokument og vil bli oppdatert og endret for å reflektere veivalg og praktiske erfaringer gjort bl.a. i forbindelse med pilotimplementasjoner.

Bakgrunn og motivasjon

Vi bruker i dag mange ulike former for elektronisk kommunikasjon som en-til-en, en-til-mange eller mange-til-mange. Eksempler på dette er mail, telefon, sanntidsmeldinger (IM), videosamtaler/konferanser og delte arbeidsflater. Dersom en skal prøve å se fremover i tid, kan vi skimte noen nye samarbeids- og kommunikasjonsformer, men vi kan være helt sikker på at det vil komme noen som vi ikke har klart å forutse.

En fellesnevner for alle disse er at det må opprettes en forbindelse mellom partene i kommunikasjonen og for å få det til så må man ha en form for adressering. Fra telefonen kjenner vi bruk av siffer. Det er unaturlig og vanskelig for et menneske å skulle forholde seg til masse tall. Internet med sine IP-adresser er et klassisk eksempel på hvor man ved hjelp av DNS har laget seg en oversettelse til noe som er letter og huske og bruke, nemlig ord, navn og benevnelser. Telefonnummer har vi måttet leve med siden sentralbord ble automatisert. Vanskeligere har det blitt jo flere siffer vi har fått i nummeret på grunn av en stadig voksende mengde apparater.

I mail har vi en mailadresse. Med IM varierer det med hvilken variant man bruker, men også der er det vanlig med en adresse på et format vi kjenner fra mail. Etter hvert som man får flere ulike tjenester så får man dessverre også flere ulike typer adresser å forholde seg til. Hadde det ikke vært greit om man kunne forhold seg til en og samme adresse for alle de ulike tjenestene?



SIP (Session Initiation Protocol) er en teknologi som åpner for masse muligheter. Med SIP er det mulig å ringe på navn i stedet for nummer. En SIP adresse er på et logisk format som kan tilrettelegges å være lik det man bruker for mail. Med en fornuftig navnekonvensjon kan den identifisere person, avdeling, organisasjon og land slik at den er lett å huske eller finne frem til.

Med SIP til å organisere kontakten så kan man legge ulike former for kommunikasjon mellom partene. En av de tjenestene som oftest blir assosiert med SIP er telefoni. Det er til gjengjeld en så tydelig og sterk tjeneste at det lett kan overskygge alle de andre mulighetene SIP kan tilby. IP-telefoni og ”VoIP” (Voice over IP) er begreper som har blitt mye brukt og ”misbrukt”. Man skal være klar over at dette kan innebære mange ulike typer løsninger som ikke nødvendigvis bruker SIP eller som er kompatible med andre systemer.

I vår kontekst ser vi på IP-telefoni som en kraftig berikelse av tjenesten gjennom å ”internettifisere” telefonien og åpne for flere teknologiske muligheter. At det på sikt også vil kunne føre til økonomiske besparelser er også en god motivasjon. Det er i dag ingen teknisk grunn til at telefoni og data trenger å være adskilt med separate linjer og forskjellig typer utstyr. Det er heller ingen grunn til at man må forholde seg til en gitt produsent til alt av utstyr, programvare og tjenester fordi det også er produsenten av sentralen. Kort fortalt flytter vi telefonilogikken ut til Internett og beriker samtidig tjenesten ved å kunne knytte det opp mot andre systemer og verktøy vi allerede har og i en verden som brukerne og IT-drift allerede er kjent med. For organisasjonen betyr det en økonomisk besparelse ved at kompetanse for drift

og utstyr for både IT og telefoni kan samles i samme avdeling. Ved å bygge opp en person-til-person infrastruktur, får vi også muliggjort dynamisk vekst mot andre former for kommunikasjonsmedier, som f.eks. video, uten at eventuelle begrensninger i mellomledd er til hinder.

I vår SIP infrastruktur ønsker vi å tilstrebe noen viktige prinsipper:

- **Mest mulig bruk av åpne standarder for å kunne sikre interaksjon mellom produkter og tjenester fra ulike produsenter.**
  Dette gir en konkurransesituasjon mellom produsentene og man får anledning til å sy sammen de produktene som passer en best ut i fra lokale hensyn. Det vil også kunne gi en raskere omlegging mot fremtidige tjenester.

- **Infrastrukturen skal ikke sette begrensninger for fremtidige tjenester.**
  Det er vanlig å se SIP satt opp til kun å skulle støtte telefoni. De systemene vil ha problemer med å tilpasse seg fremtidige krav som f.eks. videotelefoni og samtidig låse ute andre typer tjenester. Det kan tenkes at en i noen tilfeller ønsker å separere telefonitjenester fra andre typer tjenester. I de tilfellene kan telefoni separeres til f.eks. egne nettverk og bak dedikerte portaler. I SIP sin sanne ånd skal datakommunikasjonen gå direkte mellom partene mens signalering kan gå gjennom mellomledd. På den måten blir det opp til den enkelte klient hvilke tjenester den kan støtte og ikke en kunstig begrensning i et mellomledd.

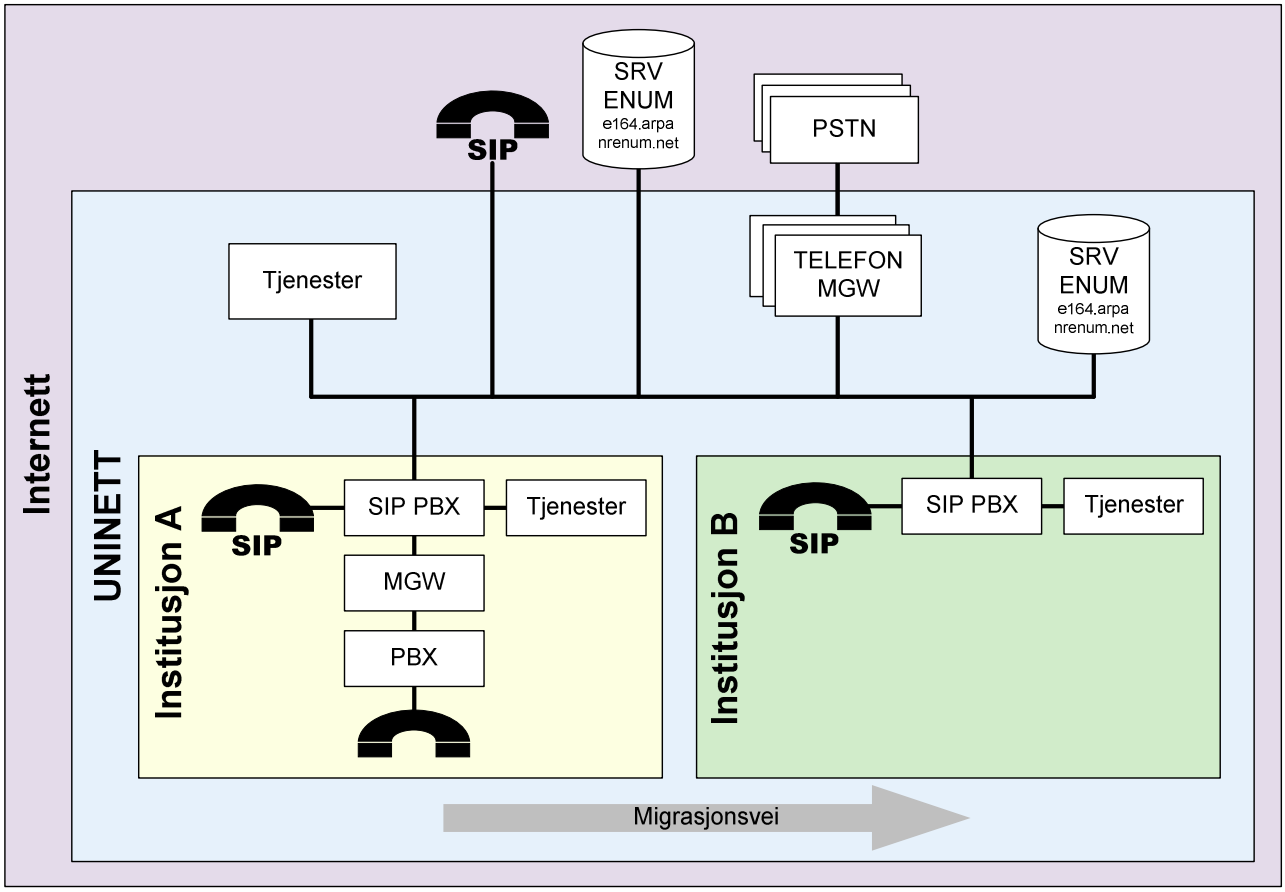
- **Den enkelte institusjon skal kunne ta i bruk tjenestene i den grad og med den utviklingstakt de selv ønsker.**
  Av forskjellige årsaker er det ikke alle som ønsker å ta i bruk SIP i sin lokale infrastruktur enda. Det vil naturlig nok også være mange som har investert store beløp i et telefonisystem og som ønsker at det fungerer ut sin beregnede levetid. Slike utgangspunkt trenger ikke nødvendigvis bety det samme som at man ikke kan ta del i noen av fordelene og tjenestene gjennom SIP. Infrastrukturen vi bygger skal ta hensyn til dette og også åpne for en gradvis migrering om ønskelig, dvs. at man teoretisk kan legge om ett og ett nummer i eget tempo.

Det er vårt mål at SIP blir en velkjent og ønsket teknologi i UH-sektoren hvor alle personer har en SIP-identitet og kan nås på tilgjengelige tjenester gjennom denne. Etter hvert som en får en SIP-identitet så vil det også bli mulig få kontakt med andre organisasjoner i Norge og utlandet som også bruker SIP. Det begynner å bli en del og det er tydelig fra utviklingen at det er denne veien verden går.

1. Infrastrukturen

UNINETT SIP infrastruktur er ikke en egen infrastruktur men SIP satt i system. Det er sammensatt av den enkelte institusjons SIP-tjenester, UNINETT-drevne SIP-tjenester og ikke minst en samordnet måte å gjøre ting på. Kjernen i infrastrukturen i så måte er UNINETT sin nettverksinfrastruktur hvor vi utnytter dens egenskaper med god kapasitet og redundans til å bære også SIP-baserte tjenester som f.eks. telefoni. Sistnevnte tjeneste får naturlig nok mye fokus i dette dokumentet.

I tegningen under har vi illustrert infrastrukturen. Fargede bokser representerer ulike nettverk/organisasjoner hvor man har plassert ulike entiteter og tjenester. En farget boks inne i en annen farget boks vil si at den er direkte tilknyttet ressursene til den utenpåliggende boksen.



Institusjonen (gul og grønn boks)

Telefonisituasjonen hos de forskjellige institusjoner kan være svært varierende. Det kan være en telefonisentral fra f.eks. Nortel, Alcatel, Ericsson eller Cisco. Noen er til dels over på VoIP og noen bruker kanskje allerede SIP via muligheter i sentralen. Men selv med forskjellig utgangspunkt og forskjellige ønsker om hva man vil ha internt, søker vi å lage en løsning hvor man kan knytte seg mot UNINETT SIP infrastruktur enten fullstendig eller gjennom en gradvis migrering. Dette kan gjøres ved å etablere en utenpåliggende enhet som ”homogeniserer” tilkoblingen mot SIP-infrastrukturen. Denne enheten har fått betegnelsen ”SIP PBX” i tegningen. Avhengig av hvilken type PBX man måtte ha fra før, kobles denne til ”SIP PBX” gjennom en ”Media gateway” (MGW) eller direkte med SIP. Institusjonen kan velge å legge til tilleggstjenester som f.eks. telefonsvarer, kalenderintegrasjon og telefonkonferansetjenester i en eller flere enheter som kalles ”Tjenester” i tegningen. Mange tjenester vil også kunne være tilgjengelig for klienter tilknyttet PBX gjennom MGW og SIP PBX.

Grunnkonseptet er at samtlige telefonbrukere får en identitet i ”SIP PBX” som er på formen av vedkommendes mailadresse. I tillegg vil samtlige telefonbrukere også være nåbar via nummeret brukt som SIP-adresse. Personer med SIP-konto, kan i tillegg logge seg på ved hjelp av sitt vante brukernavn. Ved å gjøre det har man lagt grunnlaget for at alle brukere kan nås på en SIP-adresse. Håndteringen av en henvendelse på en slik adresse vil være avhengig av typen tjeneste det dreier seg om.

Hva slags programvare eller utstyr som velges, skal i så stor grad som mulig være opp til den enkelte institusjon. Det vil si at institusjonen selv velger hvilken type SIP-løsning man vil ha såfremt den støtter de nødvendige standarder og metoder. Det er verdt å merke seg at virtuelle maskiner ikke er egnet til bruk i telefoniløsninger. Til dette er det best med dedikert nettverkskort som har gode drivere. UNINETT vil være behjelpelig med å installere og konfigurere en grunnpakke med modulene SIP PBX, Tjenester og om nødvendig MGW basert på programvare med åpen kildekode.

Under den gule og grønne boksen er det en grå pil som angir migrasjonsvei. Dette er for å symbolisere en ønsket utvikling innen telefonien hos institusjonen. Med en SIP PBX og kanskje også Tjenester på plass, er veien åpen for å kunne velge enten en gradvis eller fullstendig migrering over til en ren SIP-basert løsning hvor også samtlige klienter benytter SIP. Med alle brukere over på SIP-apparater er det i mange tilfeller ikke lenger behov for hussentralen og den kan fases ut som en naturlig del av prosessen.

UNINETT vil kunne stå for drift og vedlikehold av systemene på SIP PBX, MGW og til dels Tjenester gjennom et sentralt driftsopplegg.

UNINETT (lys blå underliggende boks)

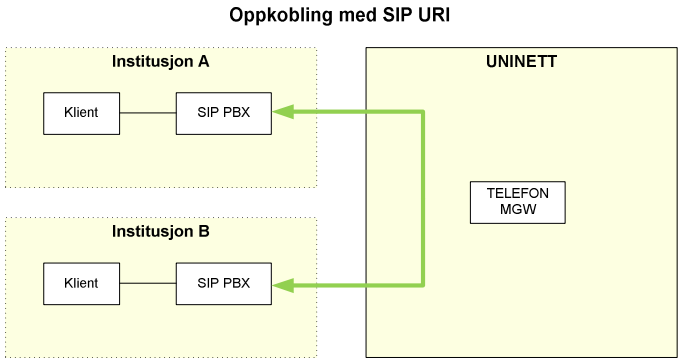
UNINETT vil sørge for drift av sentrale tjenester, DNS (SRV og ENUM) og ikke minst knutepunktene mot telefonileverandøren. I tegningen er sistnevnte merket som ”TELEFON MGW”.

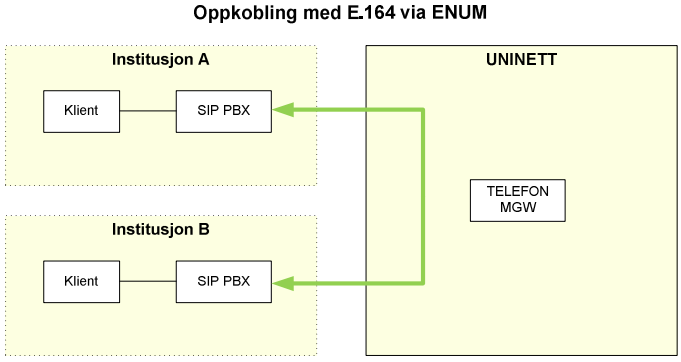
Sentrale tjenester vil i første rekke være tjenester hvor det er mest formålstjenlig å ha en sentral, felles driftløsning. Det kan også tenkes at det er institusjoner som ikke har anledning til å drifte egne lokale tjenester som f.eks. telefonsvarer og telefonkonferanseløsning. I de tilfeller er det teknisk sett uproblematisk at UNINETT drifter slike tjenester i en sentral løsning.

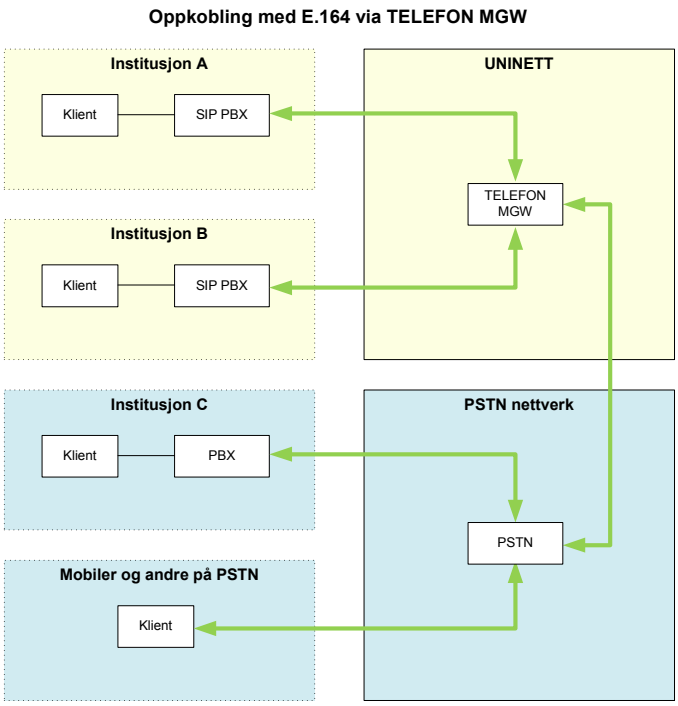
DNS er viktig i denne infrastrukturen. SRV brukes til å finne de ulike servere som skal håndtere tjenestene og ENUM brukes for å finne frem til hvor nummer kan nås. DNS forenkler veldig den praktiske administrasjon av infrastrukturen og gjør løsningen dynamisk. DNS er allerede etablert med god redundans i mange ledd.

TELEFON MGW er en svært viktig komponent. Alle innkommende samtaler fra telefonileverandøren til institusjonene og alle utgående samtaler fra institusjonene til en telefon som ikke er tilgjengelig over SIP, vil gå gjennom denne noden. Med andre ord vil alle institusjoners SIP PBX sette denne noden som neste hopp dersom nummeret som ringes ikke er tilgjengelig over SIP. TELEFON MGW er en B2BUA (”MGW”) mellom institusjonene og telefonileverandøren (PSTN), dvs. den fremstår som samtalens endepunkt fra begge sider. Det gjør at all ikke bare signalering men også tale går gjennom denne noden.

Illustrasjonene under viser hvordan signalering skjer ut i fra forskjellige forutsetninger mellom partene.







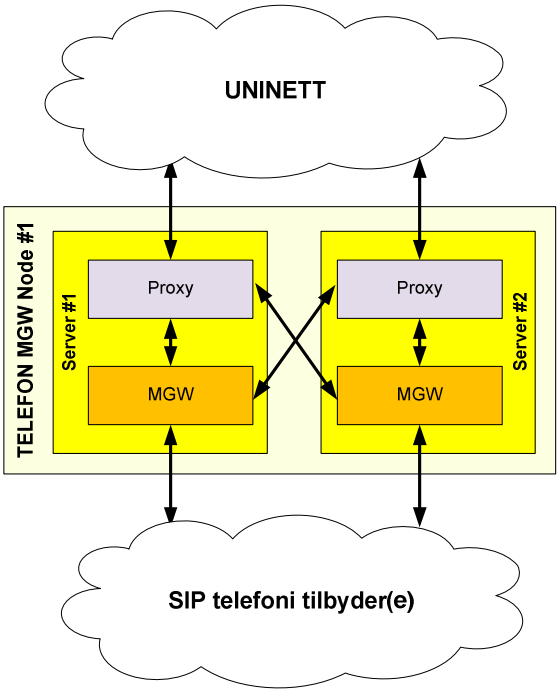
Logikken i TELEFON MGW er laget for å benytte ENUM. Det vil si at alle henvendelser på nummer blir gjort om til E.164 format der det ikke allerede er slik, og sjekket mot ENUM. I Norge har vi anledning til å bruke det offisielle ENUM treet e164.arpa, men UNINETT har også anledning til å ta del i treet nrenum.net. Målet er kun å måtte forholde oss til e164.arpa og det er uheldig å måtte bruke tid på å slå opp i flere trær, men så lenge vi ser at vi har mulige forbindelser i andre trær så må vi vurdere om det ikke skal inkluderes i søket. ENUM oppslag foretatt i TELEFON MGW begrenser seg til e164.arpa og nrenum.net.

Som et minimum blir samtlige nummer som rutes inn via TELEFON MGW lagt inn i ENUM. En institusjon kan også velge å gjøre seg nåbar via ENUM selv om samtalen ikke er rutet fra PSTN til TELEFON MGW. Det vil si at andre institusjoner som bruker ENUM aktivt da vil gå veien om Internett i stedet for å ringe via PSTN. UNINETT tar på seg oppgaven med å registrere nummerserier på vegne av institusjonen som en del av prosessen med institusjonens tilknytning til TELEFON MGW.

Med TELEFON MGW blir det mulig å logge samtlige innkommende og utgående samtaler i en Call Detail Recording (CDR) hvor bl.a. fra-nummer, til-nummer og samtalens varighet blir lagret. Denne CDR vil være tilgjengelig for autoriserte personer fra den enkelte institusjon gjennom et webgrensesnitt og sikret med FEIDE. Her vil der være mulig å gjøre søkeutvalg for å få generere lister som f.eks. kan avstemmes med telefonregningen fra telefonileverandøren.

Sikkerheten er svært viktig for TELEFON MGW på mange måter. Det er sikkerhet mot nedetid, hacking, uautorisert telefonibruk og også sikkerhetsfunksjoner som skal hjelpe den enkelte institusjon i administrasjon av telefonien.

TELEFON MGW noden er konstruert med tanke på optimal oppetid. Det vil si at redundans er til stede i mange ledd, både fysisk og logisk. Tegningen viser hvordan en node er logisk konstruert.



Hver TELEFON MGW node består av to aktive og gjensidig dynamisk redundante servere hvor hver server har redundant strømforsyning og disk. Hver server kjører begge de samme tjenestene på hvert sitt separate nettverkskort. Dersom en av tjenestene skulle bli utilgjengelig, vil den tilsvarende tjenesten hos den andre serveren automatisk bli foretrukket. Skulle begge like tjenester bli utilgjengelig, vil tjenestene hos en annen node automatisk bli foretrukket. Hvis hele noden skulle bli utilgjengelig, vil tilsvarende en annen node bli foretrukket. Denne prioriteringen er til dels gjort ved hjelp av vektede SRV-innslag i DNS. Teknisk kan TELEFON MGW ha eksterne databaser, men av hensyn til oppetid og kortest mulig responstid/oppslagstid så er databasene lokal og ikke avhengig av andre systemer. Databasene oppdateres fortløpende mellom enhetene.

Flere TELEFON MGW noder er plassert forskjellige steder i landet. Ved å utnytte den gode redundansen UNINETT har i sitt nett i kombinasjon med strategisk plasserte enheter så skal det svært mye til for at TELEFON MGW-tjenesten skal bli utilgjengelig. Et tenkt scenario i en fullt utbygd infrastruktur kan være redundante noder i Tromsø, Trondheim, Oslo og Bergen. I første omgang er det redundante enheter i Trondheim og Oslo. En forutsetning er at også telefonileverandøren har den nødvendige redundans i sitt nettverk. En slik løsning åpner også for at belastningen fordeles regionalt og således utnytte samtlige TELEFON MGW noder.

Sikkerhet mot hacking er vanskelig men vi begrenser risikoen ved å begrense hvilke IP adresser som får lov til å kommunisere med enheten. Gjennom routerfilter og iptables gjør man en avgrensing som gjør at kun ønskede IP eller subnett får kommunisere med TELEFON MGW og da kun med ønskede porter. Hva som er nødvendig må vurderes i hvert enkelt tilfelle, men i utgangspunktet må det sperres for alt men åpnes for RTP og SIP til/fra de adresser hos institusjonen som skal kunne føre en telefonsamtale. Det må også åpnes tilsvarende for telefonileverandørens kontaktpunkt. Øvrige adresser vil kunne stenges ute fordi det ikke vil være aktuelt for utenforliggende nett å bruke TELEFON MGW. Legitime mobile brukere fra andre nett må få gjort telefoni tilgjengelig gjennom lokale løsninger som VPN eller en B2BUA med ekstra sikring hos institusjonen. Etter å ha blitt gjort oppmerksom på risiko og konsekvenser, må den enkelte institusjon stå som ansvarlig for å velge ut hvilke adresser som skal tillates brukt mot TELEFON MGW. Det er fordi et eventuelt misbruk vil medføre økonomiske konsekvenser for den rammede institusjon. Administrasjon av CDR gjøres via en frittliggende webserver.

Uautorisert telefonibruk kan raskt bli en svært dyr konsekvens av utilstrekkelig beskyttelse mot hacking eller utro tjenere. Det hjelper heller ikke å sikre TELEFON MGW mot hacking dersom problemet er at en i

utgangspunktet lovlig bruker ringer mange dyre nummer. Begrensninger i hvilke IP-adresser som får benytte TELEFON MGW vil avgrense dette problemet mye, men det kan også være at den lokale SIP PBX blir hacket eller at misbruket skjer fra innsiden, f.eks. via en hacket PC. Til hjelp mot dette trenger vi "fraud detection" systemer. Fordi vi har en CDR har vi en oversikt over samtalehistorikken. Ut i fra dette lages rutiner som leter etter samtalemønster og dersom dette oppdages, kan ansvarlige hos institusjonen varsles. Det kan være f.eks. at ett og samme nummer overstiger en gitt kostnadsgrense, unormalt mange oppringninger innenfor en tidsperiode, absolutt sperre for alle samtaler til et gitt land, varsel dersom samlede samtalekostnader overskrider budsjett, o.l. Administrasjon av dette kan gjøres av den enkelte institusjon via webgrensesnitt beskyttet med FEIDE. Bakenforliggende systemer holder rede på status gjennom modulbaserte rutiner og flagger treff for videre behandling og respons. Et minimum regelsett etableres som standard med varsling hos lokale ansvarlige.

Sperre og filter i TELEFON MGW må ses på som en "siste skanse" med tanke på å hindre dyrt misbruk og beholde oversikten over telefonibruken. Det er den lokale SIP PBX som skal håndtere de primære reglene for hvordan samtaler skal håndteres og eventuelt begrense tilgjengeligheten til og fra visse nummer.

På sikt kan TELEFON MGW få en viktig rolle hvor man kan håndtere flere telefonileverandører samtidig. Det kan tenkes at avtaleverket gir institusjonene anledning til å velge telefonileverandør etter hvor man skal ringe. F.eks. kan det være at leverandør A er gunstigst for nasjonale samtaler mens B er gunstigst for samtaler til utlandet. Det kan også være at man kan få til avtaler for mobiltelefoni hvor man bruker ulike telefonileverandører avhengig av hvilken operatør nummeret ligger hos. TELEFON MGW vil kunne håndtere slikt sømløst for institusjonen og brukeren.

Internet (grå underliggende boks)

Utenfor UNINETT vil det forekomme stadig flere SIP-baserte klienter som vil kunne ta kontakt med klienter i vår infrastruktur uten å måte gå igjennom telefoninettet. I DNS med ENUM vil de bli enkelt å bli nådd og nå disse. For de med tilsvarende infrastruktur som oss, vil dette skje sømløst og uten at brukeren trenger å forholde seg til noe spesielt. Unntaket er dersom man begynner å benytte seg av SIP URI fremfor telefonnummer.

PSTN er telefonileverandøren. Det kan være flere av disse samtidig som tilbyr gunstigst mulig priser for hvert sitt fokusområde som f.eks. telefoni innenlands, mobiltelefoni og utenlandssamtaler. PSTN vil ligge på sitt eget IP nettverk. Vi må kreve at de har den nødvendige kvalitet og redundans i sitt nettverk for å tilfredsstille våre behov.

2. Migrering

Overgangen fra PBX til SIP PBX kan gjøres gradvis gjennom en migreringsprosess. Det vil være opp til den enkelte institusjon hvor raskt denne prosessen skal gå og det er ikke gitt at alle trinn må følges slavisk. Man kan også velge å hoppe over enkelte trinn.

Migreringen er en prosess som for de fleste vil kunne strekke seg over flere år. Mye av arbeidet ligger i planlegging, tilrettelegging og etablering av grunnkomponentene i organisasjonen. Etter det vil man kunne få en gradvis tilpasning frem til en endelig utfasing av den gamle PBX. Et viktig mål med prosessen er at brukerne hele veien merker minst mulig til overgangen. Det er en fordel om brukeren i overgangen også blir gjort kjent med de utvidede mulighetene den nye teknologien gir, bl.a. gjennom nye tjenester. Det er også viktig at man merker seg detaljene og ikke undervurderer tiden det kan ta for å få de små ting i orden.

UNINETT vil hjelpe med å legge til rette for migrasjonen slik at prosessen blir så enkel som mulig, samtidig som de lokale ansvarlige får den nødvendige opplæring for videre drift og vedlikehold.

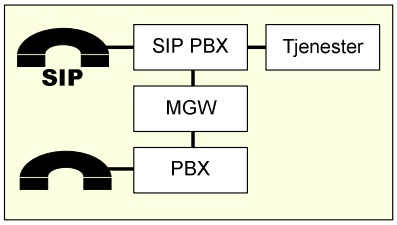
Komponentene

Den grunnleggende og viktige komponenten i en ny lokal SIP infrastruktur er entiteten ”SIP PBX”. Det er SIP ruteren som holder rede på innkommende og utgående henvendelser, og den fungerer som registrar for SIP-brukere. Det endelige målet er at alle telefonibrukere vil koble seg til mot denne med et SIP-apparat.

En annen viktig entitet er ”MGW” som er bindeleddet mellom SIP-verden og det lokale telefonisystemet.

Til slutt har vi ”Tjenester” som er en entitet som kan gi lokale tjenester som telefonsvarer, konferansesystem, automatiserte telefonimeldinger, kalenderintegrasjon, osv.

Illustrasjonen under viser hvordan disse entitetene henger sammen hos en institusjon:



I praksis kan entitetene i svært mange tilfeller slås sammen og kjøres på en og samme server.

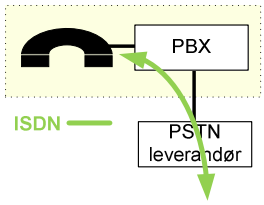
Migreringsalternativer

Som tidligere nevnt er et viktig mål at brukeren skal merke minst mulig til migreringsprosessen. For å gi et bilde av hvordan en migreringsprosess kan arte seg i praksis, gis det her en oversikt over to mulige scenarioer man har for å nå dette målet. Det kan godt være flere varianter for mulighetene er mange. Et sted på veien må man velge når brukeren skal få et SIP-apparat eller om han i det hele tatt skal ha et SIP-apparat eller beholde det eksisterende.

A - Holde på PBX-apparatene så lenge som mulig	B - Bytte til SIP-apparat så tidlig som mulig
1. Utgangspunktet	1. Utgangspunktet
2. Innfasing av SIP PBX, MGW og Tjenester	2. Innfasing av SIP PBX, MGW og Tjenester
A3. Endre rute for utgående anrop	B3. Bytte ut apparat
A4. Portere nummer til SIP	B4. Endre rute for utgående anrop
A5. Bytte ut apparat	B5. Portere nummer til SIP
6. Fjerne MGW og PBX, si opp ISDN	6. Fjerne MGW og PBX, si opp ISDN

1. Utgangspunktet

Som utgangspunkt har man gjerne en lokal PBX med tilhørende apparater. PBX kan være f.eks. fra Alcatel, Ericsson, Nortel, Cisco, e.l. Alle samtaler til andre lokale apparater går enten via PBX eller direkte mellom apparater men med PBX for å styre samtalene. Samtaler med PSTN (”bylinje”) går enten via ISDN (PRI) eller SIP med PBX som gateway.

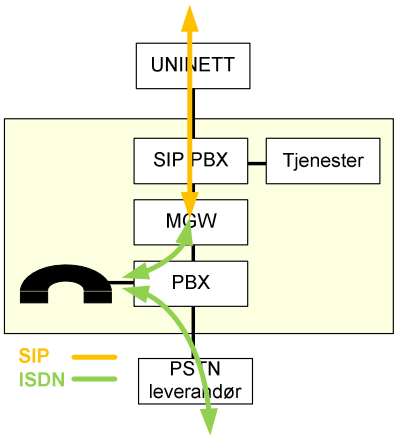


2. Innfasing av SIP PBX, MGW og Tjenester

Med SIP PBX og MGW på plass er institusjonen nåbar via SIP over Internet. Da får man umiddelbart en del muligheter selv før man har laget en eneste SIP-bruker og uten at det får noen praktisk endring av bruksmåten for eksisterende brukere.

- Institusjonens telefonibrukere kan få en SIP-adresse (SIP URI) på f.eks. email form og gjøres nåbar via Internet.
- Institusjonens telefonnummer kan registreres i ENUM og lenkes mot fasttelefonene på PBX. En slik handling får som konsekvens at alle institusjoner som bruker ENUM for utgående anrop vil forvente at dette fungerer. I motsatt fall vil de ikke være i stand til å nå frem.
- Institusjonens telefonibrukere kan settes opp til å ringe ut via ENUM og Internet dersom det er tilgjengelig, eventuelt med innvalgsnummer.
- Dersom man også implementerer ”Tjenester” så kan institusjonens telefonibrukere benytte seg av dette. Nummer for tjenesten fra lokal nummerserie settes opp til å rutes ut via MGW.

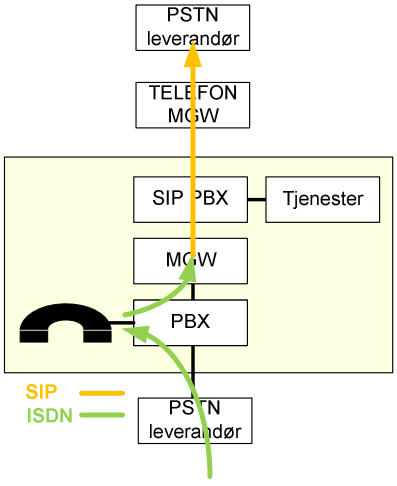
Enkelte institusjoner har satt sine IP-kapable telefoner og/eller PBX på et RFC 1918-nett (privat nett). Noen PBX har mulighet for SIP-tilknytning men har kanskje ikke kompatibelt nok implementert bruk av SIP. De fleste PBX har bare ISDN. I alle disse tilfellene anbefaler vi bruk av MGW fordi man da har muligheten til å spesialtilpasse tilkoblingen og samtidig standardisere grensesnittet videre ut mot verden på en kompatibel form. I tillegg har det den ekstra fordelen at det vil kunne la eksisterende PBX stå så urørt som mulig. Samtaler til og fra PSTN går som før.



A. Holde på PBX-apparatene så lenge som mulig

A3. Endre rute for utgående anrop

Fremdeles med telefon tilkoblet PBX er det mulig å gjøre om på samtalerutingen for en eller flere telefoner. Innkommende anrop kommer via ISDN og blir rutet frem på vanlig måte. Utgående anrop styres til MGW og videre til SIP PBX. Nå må SIP PBX tilkobles TELEFON MGW og det gjør det mulig å nå bylinje via SIP. For hverken lokal bruker eller mottaker på PSTN vil det ikke være noen opplevd forskjell på dette og ren ISDN, men den lokale brukeren har kommet ett skritt videre mot å bli konvertert til SIP. Samtaler til andre nummer på PBX håndteres av PBX som vanlig.

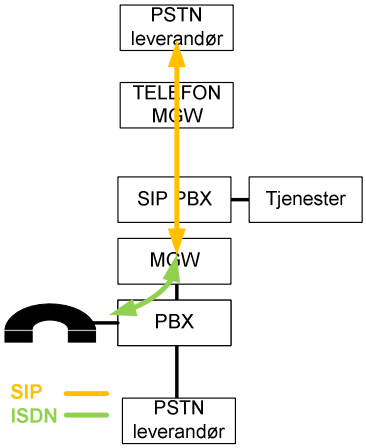


A4. Portere nummer til SIP

Når en bruker er i stand til å bruke SIP-veien for utgående samtaler, er tiden kommet for å portere nummeret fra ISDN til SIP. I praksis vil det si at innkommende anrop kommer via TELEFON MGW i stedet for lokal ISDN. Denne porteringen kan teknisk sett gjennomføres med ett og ett nummer, men det vil i praksis være mer hensiktsmessig å ta flere større bolker (f.eks. avdeling for avdeling, nummerserie for nummerserie) eller alt på en gang.

For både bruker og innringere vil dette fortone seg som helt sømløst. Samtaler kommer inn via ISDN helt frem til det øyeblikk leverandøren har portert. I det øyeblikk vil samtaler komme inn via TELEFON MGW.

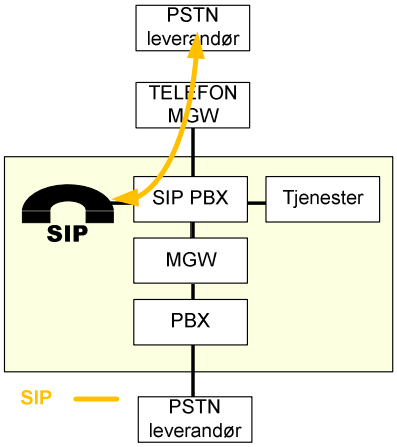
Hverken innringer eller bruker vil i praksis oppleve noen forskjell. PBX vil som vanlig sørge for riktig ruting av interne telefoner.



A5. Bytte ut apparat

Når samtaler både inn og ut går via SIP så kan man velge å gi brukeren en fullverdig SIP-konto med de muligheter det gir, og et SIP-apparat. Når man har kommet hit, har alle andre SIP-messige forberedelser blitt gjort slik at det eneste PBX i realiteten gjør er å fungere som en stor "SIP-adapter" for det gamle telefonapparatet og er dermed overflødig.

Med mindre det gamle apparatet kan konverteres til SIP, vil brukeren nå oppleve å få et nytt apparat på pulten. Brukeropplevelsen utover dette vil være som før. Det er også et alternativ at PBX består som "SIP-adapter" for noen apparater av økonomiske eller praktiske hensyn.

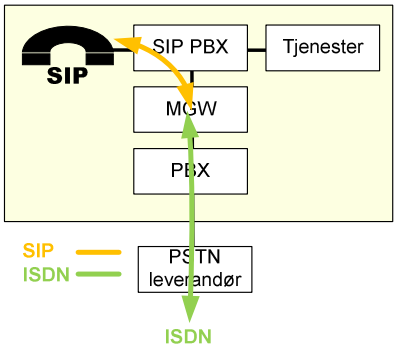


B. Bytte til SIP-apparat så tidlig som mulig

B3. Bytte ut apparat

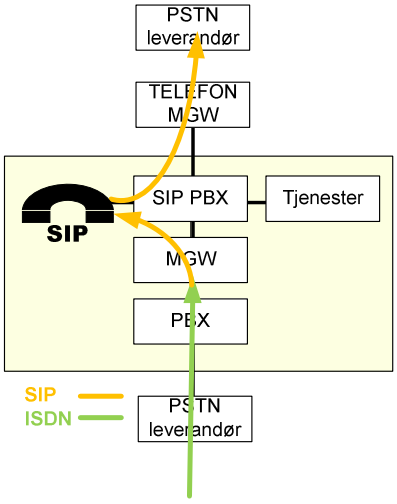
Etter at SIP PBX og MGW er på plass, kan man velge å gi brukeren en fullverdig SIP-konto med de muligheter det gir, og et SIP-apparat. PBX settes opp til å videresende alle anrop til det aktuelle nummer til MGW, som igjen sørger for riktig ruting til SIP PBX og til slutt brukeren. På samme måte kan alle utgående anrop fra brukeren settes opp i SIP PBX til å gå til MGW som sender det videre til PBX som igjen ruter det lokalt eller sender det til PSTN-leverandør over PRI.

Bortsett fra et annet apparat, vil ikke brukeren merke noen stor praktisk forskjell i bruken av telefonen.



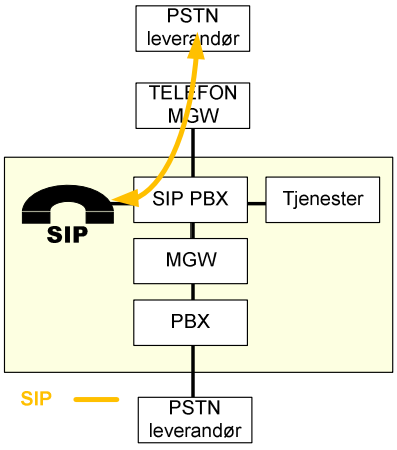
B4. Endre rute for utgående anrop

Innkommende anrop kommer via ISDN og blir rutet frem på vanlig måte. Utgående anrop styres til SIP PBX. Nå må SIP PBX tilkobles TELEFON MGW og det gjør det mulig å nå bylinje via SIP. For hverken lokal bruker eller mottaker på PSTN vil det ikke være noen opplevd forskjell på dette og ren ISDN. Samtaler til andre lokale nummer på PBX håndteres av MGW til PBX.



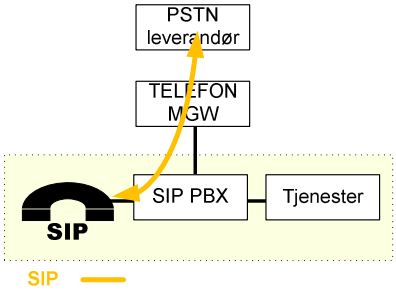
B5. Portere nummer til SIP

Dette punktet vil være nesten identisk med A-2 med unntak av utgangspunktet for apparatet.



6. Fjerne MGW og PBX, si opp ISDN

Når alle apparater er fjernet fra PBX er både denne og MGW overflødige og kan fjernes. Når ikke lenger ISDN-forbindelsen til PSTN benyttes kan også denne sies opp eller endres til et minimum dersom man ønsker en form for lokal backup. En lokal PRI-forbindelse til PSTN-leverandør kan selvsagt også kobles direkte mot MGW så PBX trengs ikke for den grunn alene.



Etter hvert som UNINETT hjelper institusjoner med å innføre en SIP infrastruktur så vil den praktiske erfaringen bidra mye til å heve kompetansen. Et dokument for plan og gjennomføring vedlikeholdes av UNINETT for å dokumentere denne erfaringen og lette prosessen for senere institusjoner.

Se Vedlegg C (side29) for en mer detaljert migrasjonsprosess i 15 steg.

3. Tjenester

Med tjenester menes i denne kontekst tilbud for brukerne utover vanlig telefonering. Ved å flytte telefoni over til IT-domenet så åpner det straks for en mengde muligheter for kobling mot andre systemer og man kan tilby det med et grensesnitt brukeren er vant med fra før.

Dette er ikke en utfyllende oversikt, men eksempler. Noen er det hensiktsmessig at UNINETT tilbyr, mens andre kanskje faller mer under lokalt ansvar.

Oversikt over omtalte tjenester
Punktene er ment som referanser og ikke som en prioritert rekkefølge.

1. Telefonsvarer
2. Mobilitet
3. Oppslagstjeneste/opplysningstjeneste
4. Konferansetjeneste
5. Web-administrasjon av egen bruker/profil
6. Sentralbord
7. Taletjenester
8. Klikk-og-Ring (Click-2-Call)
9. Oppslagsdirigering ved innkommende anrop
10. Studenttjeneste
11. Nødsamtaler
12. Telefoner for personer med særlig behov
13. Tilbakering når ledig
14. Alarm ved anomalideteksjon

1. Telefonsvarer

Nåbarhet er et viktig tema innenfor telefonien. Dersom mottaker ikke kan nås, anser mange det som en nyttig tjeneste å få høre mer om f.eks. når vedkommende kan ventes tilbake og eventuelt legge igjen en beskjed.

Med tilgjengelige programmer basert på åpen kildekode og i samarbeid med SIP PBX, kan dette enkelt implementeres for både brukere med SIP-klienter og brukere tilknyttet en samarbeidende PBX. Den innkommende samtalen kan rutes til en annen destinasjon etter definert tid med ringing uten svar. Dersom denne andre destinasjonen er telefonsvarersystemet, vil man f.eks. kunne sette opp felles svar for organisasjonen/avdelingen og/eller personlig svar for den det gjelder. Her kan man også om ønskelig sette opp et menysystem for innringer. Svaret kan også baseres på resultatet fra spørringer mot eksterne systemer, som f.eks. kalendersystemer, slik at svaret varierer med tid og status til den det søkes. Dersom det legges igjen en beskjed, kan denne sendes som vedlegg i email til den som prøves nådd.

Det kan tenkes at UNINETT etablerer en enklere form for felles svartjeneste som institusjonene kan benytte seg av. Det vil si at UNINETT er vertskap for det tekniske systemet mens institusjonen oppfører denne tjenesten som mottaker for ikke besvarte anrop. Den enkelte institusjon kan allikevel legge inn både felles svar og personlige svar for den enkelte oppringte.

2. Mobilitet

En av styrkene til SIP er å kunne ta klienten med seg mellom ulike IP-nettverk. I utgangspunktet er dette mulig men blir i flere tilfeller umuliggjort på grunn av begrensninger i nettverket, som NAT, brannmurer, andre filter og kanskje også bevisst konfigurasjon av tjeneren.

NAT og brannmurer/filter fungerer gjerne i praksis slik at samtalene går ut, men man hører ingenting. Det kan også være at klienten ikke klarer å koble seg til tjeneren i det hele tatt. Det kan argumenteres for at det blir bedre sikkerhet av å begrense hvor brukere kan registrere sine brukere fra. Typisk ønsker man kanskje at man kun skal kunne koble seg opp fra godkjente IP-adresser.

For å gjenopprette mobiliteten, må man derfor i mange tilfeller sette opp en ekstra tjeneste til dette formålet. Denne tjenesten kan settes opp til spesiell håndtering av NAT- og brannmur traversering og den kan settes opp med en ekstra sikring av brukerkontoene som kanskje ikke er ønskelig for lokale forhold. Slik ekstra sikkerhet kan være eget brukernavn og passord til denne mobile kontoen, begrensninger i nummer som kan ringes, krav om pin-kode ved oppringning av nummer som koster penger å ringe. Det kan også settes ekstra krav som kryptering. For innringer vil denne mobiliteten være transparent.

Siden dette er en tjeneste som gir tilgang til lokale ressurser og bruker av lokale midler (telefonutgifter), hører ansvaret for driften naturlig hjemme hos den enkelte institusjon. UNINETT er behjelpelig med konfigurasjon og å opparbeide driftsrutiner.

3. Oppslagstjeneste/opplysningstjeneste

Med en kobling mot en nummerdatabase kan man få automatisk lagt inn ”Caller ID” med navn på både innkommende og utgående anrop. Dermed vil brukeren f.eks. kunne se på navn hvem det er som ringer og det vil kun fremkomme i en eventuell samtalelogg man måtte ha.

Kilden til denne informasjonen kan enten være en lokal database, f.eks. en privat telefonliste som brukeren selv holder, det kan være URDB eller abonnement på opplysningstjeneste fra en leverandør av dette. Det kan også være en kombinasjon av disse.

SIP PBX kan sørge for at oppslag blir gjort automatisk for innkommende samtaler. Det kan også løses som at bruker har en spesiell knapp på sitt apparat som foretar oppslag etter ønske for både innkommende samtaler og samtalelogg. Det kan også tenkes at man ikke begrenser seg til nummer og navn men også annen tilgjengelig informasjon og at dette sendes den oppringte i form av mail eller IM.

En slik tjeneste vil i første omgang være noe som den enkelte institusjon må tilby på grunn av praktiske lokale tilpasninger, men det kan også være noe UNINETT kan bidra med.

4. Konferansetjeneste

En flerparts telefonkonferanse er en enkel og gratis tjeneste satt opp ved hjelp av programvare basert på åpen kildekode. Her etablerer man typisk noen faste telefonnummer for innringere til en konferanse. Disse kan gå direkte til et konferanserom eller til en felles ”resepsjon”. Konferanserom kan velges ut i fra predefinerte eller dynamisk opprettet. De kan også passordbeskyttes.

Med et IP-basert konferansesystem kan man inkludere innringere med forskjellige teknologier og sette dem sammen. Innringere fra det tradisjonelle telefoninettet kan nå konferansen på oppgitte telefonnummer, SIP-brukere når den også via SIP til en dedikert adresse (f.eks. konferanse@uninett.no) og det kan også opprettes kontaktadresser for H.323-klienter. Man trenger ikke nødvendigvis være en registrert SIP-bruker hos en organisasjon for å ta del i konferansen. En person kan f.eks. bruke en softwarebasert SIP-klient i Person-til-Person modus og ringe konferansen direkte. For deltakere fra andre land vil det altså kunne bety store besparelser i telefonikostnader og dermed også en attraktiv tjeneste å kunne tilby.

Det vil være naturlig for UNINETT å etablere en slik konferansetjeneste for sektoren, men det er lite ressurser som skal til for å etablere en slik tjeneste lokalt.

5. Web-administrasjon av egen bruker/profil

Det vil være aktuelt å bygge en webbasert tjeneste der den enkelte bruker selv er i stand til å justere aspekter ved sin konto og telefonibruk. Dette kan velges å gjøres avansert eller man kan holde det enkelt. Web-tjenestene kan f.eks. beskyttes med FEIDE pålogging for å få en personlig innlogging.

Aktuelle justerbare parametre og opplysninger til brukeren kan være:

- Kontoinformasjon (brukernavn, tilkoblingsdetaljer, telefonnummer, beskrivelse, o.l.)
- Passord (endre)
- Status (Ikke pålogget, Tilgjengelig, Opptatt, Viderekoblet)
- Viderekobling (etter antall ring, til hvilket nummer, telefonsvarer, o.l.)
- Siste X samtaler inn/ut/ikke besvart
- Oversikt over egne telefonkostnader
- Kalendertilkobling (lenke til kalenderinformasjon)
- Administrere egen telefonsvarer (meldinger, status, o.l.)
- Administrasjon av personlig telefonkatalog (Click-2-Call, Caller-ID oppslag inn/ut)

Dette kan altså være en slags ”Min side” hvor brukeren vet å finne alle de nødvendige opplysninger om sin egen telefoni. UNINETT kan være behjelpelig til i første omgang å realisere skreddersydde prototyper av slike systemer.

6. Sentralbord

Sentralbordets funksjon er viktig som organisasjonens ”ansikt utad” for den som ringer inn. Det forventes at sentralbordet er i stand til å lede innringer videre til best egnede destinasjon, om det så er rolle eller bestemt person. Sentralbordet må med andre ord ha kontroll på funksjon og tilgjengelighet for de som skal kunne nås på telefon. Det har ofte også en rolle som opplysningstjeneste.

Hvilket krav man har til lokalt sentralbord vil være forskjellig fra institusjon til institusjon. Noen vil ha et automatisert talemenysystem, f.eks. i kombinasjon med gruppeoppringning, mens andre vil ha en menneskelig svartjeneste med full kontroll på alle samtalestatuser. Det er viktig at den enkelte institusjon utarbeider en kravspesifikasjon på hva de ønsker fra et sentralbord. For noen kan det være en lik løsning som den de allerede praktiserer, for andre en omlegging.

Man skal være klar over at SIP i motsetning til tradisjonell PBX, er en mer distribuert løsning hvor det ikke uten videre er anledning til å se status, monitorere eller ”hente inn” samtaler. Dersom slike ting er i kravspesifikasjonen så må det tas spesielt hensyn til det under byggingen av den lokale infrastrukturen. En mellomløsning kan f.eks. være at slike spesielle løsninger blir implementert for den gruppen telefoner det ønskes for, mens de øvrige bruker en vanlig SIP-modell. Enkle funksjoner som å sette over en samtale er uproblematisk, mens funksjoner som å komme tilbake til sentralen kan implementeres f.eks. via en svartjeneste.

Det finnes ferdige sentralbordløsninger å få kjøpt, eller man kan utvikle noe selv dersom man bare trenger noen enklere ting. Hvordan det best løses vil være spesielt for hvert enkelt tilfelle. UNINETT kan bistå i prosessen med å finne en egnet løsning.

7. Taletjenester

Med taletjenester menes her muntlige beskjeder av ulik art som gis den som ringer. Dette kan være at taster seg igjennom et talemenysystem (IVR), det kan være opplysningstjenester om status og resultater som karakterer, fravær, været og trafikken.

Dette er tjenester som er nært beslektet med talepost- og konferansesystemet og kan utvikles ved hjelp av samme plattform. Noen av disse tjenestene kan tenkes gjort tilgjengelig av UNINETT, andre vil være mer spesifikke den enkelte institusjon.

8. Klikk-og-Ring (Click-2-Call)

Det vil i mange sammenhenger være praktisk for en bruker å kunne få en samtale satt opp ved bare å klikke på nummeret i f.eks. en webside. Når brukeren klikker på nummeret, begynner telefonen å ringe. Når brukeren tar røret, ringes det klikkede nummeret.

Dette er praktisk i tilfeller hvor man f.eks. ønsker å ringe et nummer man har funnet på en opplysningstjeneste, webside, e.l. Det kan implementeres ved hjelp av plug-in i populære weblesere eller formulert ved hjelp av en spesiell URL i egne websider.

Dette vil være et lokalt tilbud, men UNINETT kan være behjelpelig med den tekniske løsningen.

9. Oppslagsdirigering ved innkommende anrop

For typisk driftssenter o.l. kan det være praktisk at relevante skjema og databaser på skjermen til den oppringte får gjort automatiske oppslag basert på nummeret som ringer. Da kan mye være klart allerede før man svarer.

SIP PBX kan etter visse kriterier settes til å kalle andre systemer. Andre systemer kan i dette tilfellet være rutiner som sender nødvendig beskjed til mottakers maskin som igjen gjør de nødvendige oppslag.

Dette vil være institusjonsspesifikke løsninger, men UNINETT kan bidra med teknisk assistanse til hvordan å løse det tekniske.

10. Studenttjeneste

Studenter kan gis en SIP-konto basert på den vanlige brukeren man benytter ved institusjonen. Dette kan være begrensede konti som får ringe gratis innad i institusjonen og alle andre institusjoner tilkoblet denne infrastrukturen eller ENUM. Dette kan f.eks. sys sammen med en pre-konfigurert softwarebasert klient som gjør det enkelt for studenten å ta i bruk. Her kan man også koble sammen med andre teknologier for samarbeid og IM. Sett at man hadde en Jabber-server på institusjonen som var koblet til SIP-profilen og SIP-klienten. Da vil studenten kunne få tilgang til alle de nødvendige lokale ressurser gjennom tale og IM gjennom en og samme klient. Relevante kontaktlister og IM-grupper kan automatisk legges ut til den enkelte bruker og oppdateres dynamisk etter behov, kanskje også med forbindelse til en personlig ”Min side” på den lokale webtjeneren.

Slike løsninger eksisterer og har blitt tatt i bruk noen steder i utlandet.

11. Nødsamtaler

En grunnleggende funksjon, men den kan løses på ulike måter og med ulik grad av sikkerhet. Man kan f.eks. rute alle nødsamtaler ut på en lokal ISDN (et enkelt BRI-abonnement) dersom Internet ikke er tilgjengelig eller man kan la alle nødsamtaler gå til PSTN-leverandør på vanlig vis. Hos PSTN-leverandør er det en kobling mellom nummer og adresse og det er PSTN-leverandør som er ansvarlig for å sørge for at denne informasjonen kommer frem til nødsamtalen.

Eksperimentelt jobbes det med integrasjon mellom nettverksinformasjon og posisjonering (som GPS) i forbindelse med SIP. På denne måten kan detaljert lokasjonsinformasjon sendes til nærmeste nødsentral.

12. Telefoner for personer med særlig behov

Det finnes en mengde muligheter og løsninger for personer med særlige behov. Å kunne koble telefonen til Internet åpner for muligheter som kan tilpasses det spesifikke behov og kan om nødvendig skreddersys. Det kan være f.eks. billedtelefon (håndtegn/leppelesing), braille-teksting, teleslynge for telefonapparater, talesyntese, osv.

13. Tilbakering når ledig

Når den du ringer er opptatt, kan man velge at telefonen automatisk ringer deg opp når vedkommende har blitt ledig. Først ringer din egen telefon og når du tar røret, ringer det hos mottakeren. En kjekk funksjon

mot PSTN-verden og andre med kun en tilgjengelig linje. For SIP-brukere har man flere ”linjer” og vil alltid være ”tilgjengelig” med unntak av dersom samtlige egne klienter har koblet seg av.

14. Alarm ved anomalideteksjon

Ved å ha full kontroll på samtaleflyten og en god CDR, kan man følge med på ringemønster. Man kan lage funksjoner som detekterer ulike mønster i samtaleflyten og på den måten finne ut om det er unormale samtalemønster man bør merke seg. F.eks. et nummer ringer et utenlandsnummer 10 ganger på rad i løpet av kort tid, burde kanskje undersøkes nærmere eller kanskje til og med automatisk sperres. Ansvarlige kan også tenkes å få satt opp deteksjon med varsel når man nærmer seg rammene til et utgiftsbudsjett, e.l.

Vedlegg A – SIP, en teknisk innføring

Dette vedlegget gir en teknisk innføring i SIP, SRV og ENUM på et overordnet nivå.

SIP

Session Initiation Protocol (SIP) er en standard beskrevet i IETF RFC. Det er egentlig en mengde RFC, over 100 stykker. Det heter seg at noe av det fine med standarder er at det er så mange å velge mellom, men for SIP så har det dessverre blitt slik at det er en såpass stor frihet i implementasjonen at man kan finne flere ulike SIP løsninger som i praksis ikke er så veldig kompatible med hverandre. Dette gjelder både utstyr som telefoner og programvare. I tillegg finnes det flere produkter på markedet som har lånt til dels kraftig fra SIP men har lagt til egne komponenter og i praksis gjort det til en proprietær løsning. Alt dette gjør at det er viktig at man er bevisst på at de produktene man satser på fungerer som forventet.

Til hjelp for både utviklere og brukere har det blitt utviklet noen initiativ for hvordan man bør implementere SIP.

- A Hitchhiker's Guide to the Session Initiation Protocol (SIP)
  http://tools.ietf.org/html/draft-ietf-sip-hitchhikers-guide-05
  Denne gir en veiledning om hvilke RFC som skal brukes til hva.

- SIPConnect
  http://www.sipforum.org/content/view/273/227/
  Dette initiativet I regi av SIP Forum har som mål å få standardisert måten utviklere og produsenter implementerer SIP I sine produkter. De har en lang rekke medlemmer blant produsenter og andre og har fått en del tyngde i SIP-verdenen. De har også ” SIPconnect Compliant Certification Program” som sjekker kompatibilitet innenfor retningslinjene. For sluttbrukere vil det være et poeng å kreve at utstyr og programvare følger spesifikasjonene i SIPConnect.

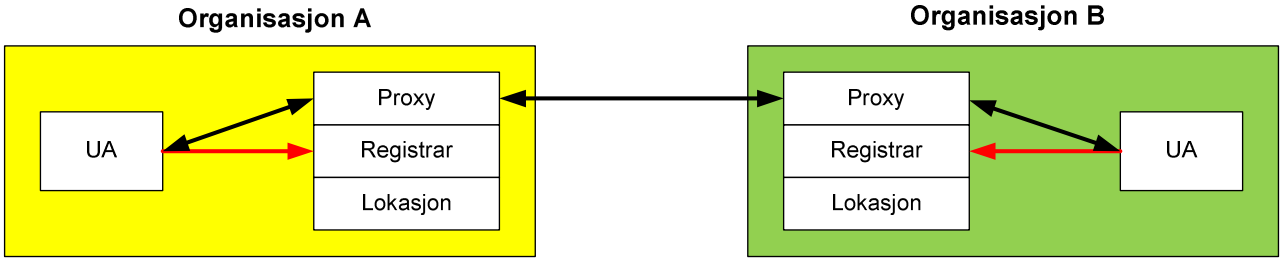
I tillegg har UNINETT noen utkast til UFS på temaet:

- UFS123 - Krav til telefoni-ruting i UH-sektoren
  https://ow.feide.no/_media/gigacampus:ufs_123_-_utkast_1_-_krav_til_telefoni-ruting_i_uh-sektoren.pdf
- UFS124 - Krav til telefoni-tjenester i UH-sektoren
  https://ow.feide.no/_media/gigacampus:ufs_124_krav_til_telefonitjenester_i_uh_sektoren.pdf

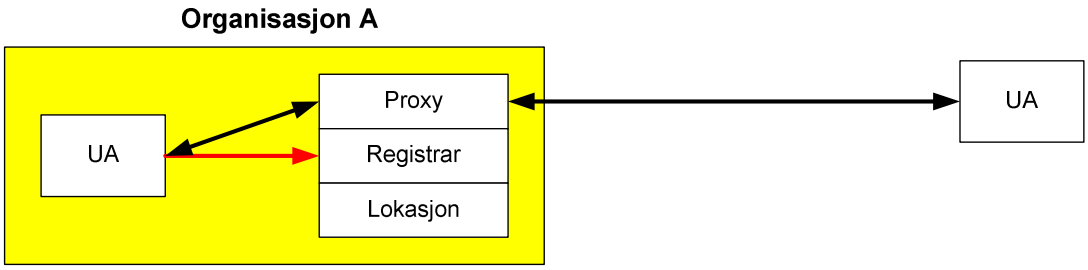
Kort fortalt så er SIP en signaleringsprotokoll som forhandler og etablerer kontakt mellom enheter kalt User Agent (UA). Det kan gå direkte mellom to UA eller via en Proxy som viser veien videre. Det kan også skje gjennom etapper hvor en enhet terminerer forbindelsen på hver sin side av seg selv ved å være en UA på hver side (Back-to-back UA – B2BUA). Når man er en del av en organisasjon, er det vanligste å bruke en Proxy slik at man kan få en adressering på formatet <bruker@organisasjon.no> for alle brukerne i den organisasjonen. Brukerne vil da registrere seg hos en Registrar som gjerne også holder rede på brukerens faktiske Lokasjon i nettverket. Uten en Proxy og Lokasjon så ville UA ha måtte bruke IP/Alias for til hverandre for å oppnå kontakt. Ved å bruke en Proxy i kombinasjon med en Registrar, kan man også legge til begrensninger ved bruken av enkelte tjenester, som f.eks..å kreve identifikasjon og tillatelse før en får ringe kostnadsbærende samtaler. En server med Proxy, Registrar og Lokasjon er ofte den samme enheten, spesielt i mindre organisasjoner.

- User Agent (UA) – Der kommunikasjonen terminer. Som oftest klienten en bruker benytter. Det kan være programvare på PC eller et dedikert apparat.
- Proxy – Sørger for ruting av SIP

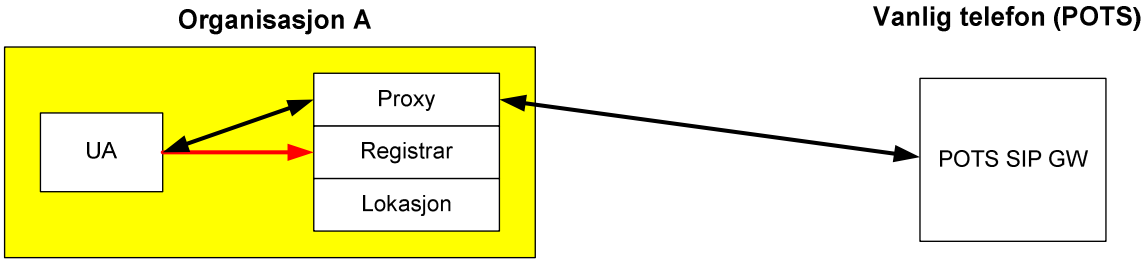
- Registrar – Sørger for autentisering og registrering av brukere
- Lokasjon – Sørger for å holde rede på hvor i IP-nettet de ulike registrerte UA befinner seg.



Kommunikasjonen mellom UA går I dette eksempelet via en Proxy hos den respektive organisasjon men forutsetter at UA har registrert seg først.



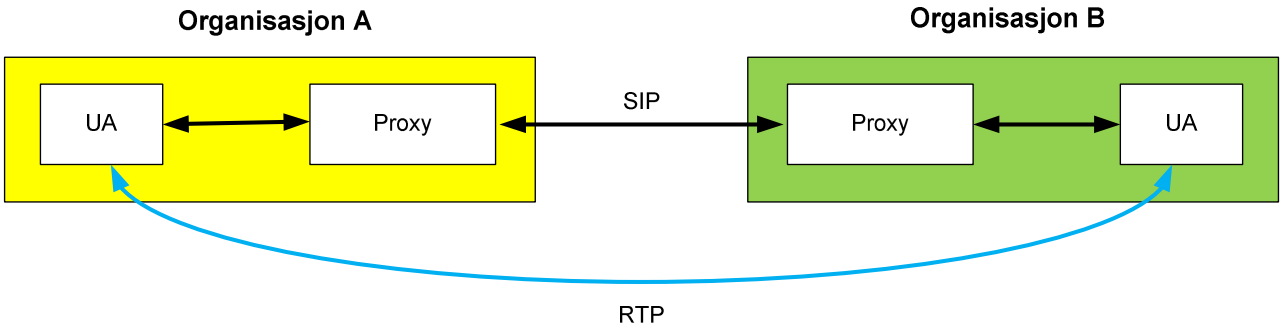
Det er fullt mulig å kommunisere med en UA som ikke tilhører en organisasjon, altså direkte.



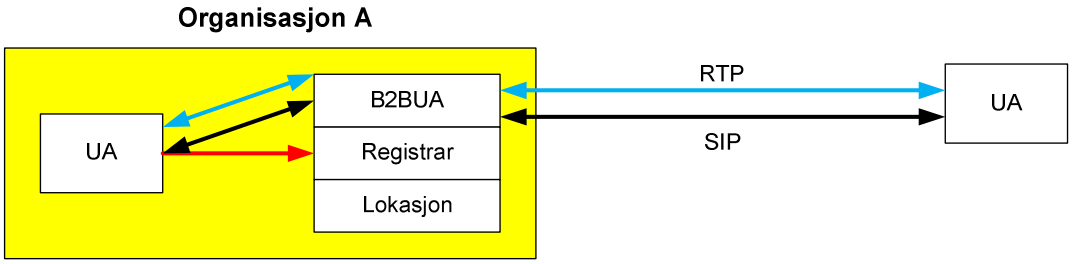
Dersom man skal ringe en ”bylinje” så er det bare et spørsmål om å få Proxy til å rute henvendelsen til en slik tjeneste dersom brukeren er autorisert til handlingen.

SIP handler også om å formidle direkte kontakt mellom partene i kommunikasjonen. Når UA har funnet hverandre så kan resten av SIP-kommunikasjonen gå direkte mellom dem uten å gå via Proxy. Dersom man imidlertid bruker funksjonen ”Strict Outbound Proxy” så er brukerne tvunget til å gå via Proxy hele tiden. Det kan også ha sine fordeler i enkelte sammenhenger.

Denne SIP protokollen etablerer kontakten og forhandler frem mulige kommunikasjonsformer, men det er viktig å merke seg at SIP ikke gjør selve kommunikasjonen over tjenesten som er forhandlet frem. Det er en kommunikasjon som blir satt opp som et resultat av forhandlingene og som bare vedlikeholdes av SIP. I SIP telefoni handler det om to separate RTP-strømmer som går den ene og den andre veien direkte mellom UA. Porten det sendes mot er forhandlet frem i SIP og kan variere innenfor et område som er definert i den enkelte UA. Dette har relevans for oppsett av brannmurer og filter.



Dette eksempelet viser hvordan RTP vil ta en direkte vei mellom UA

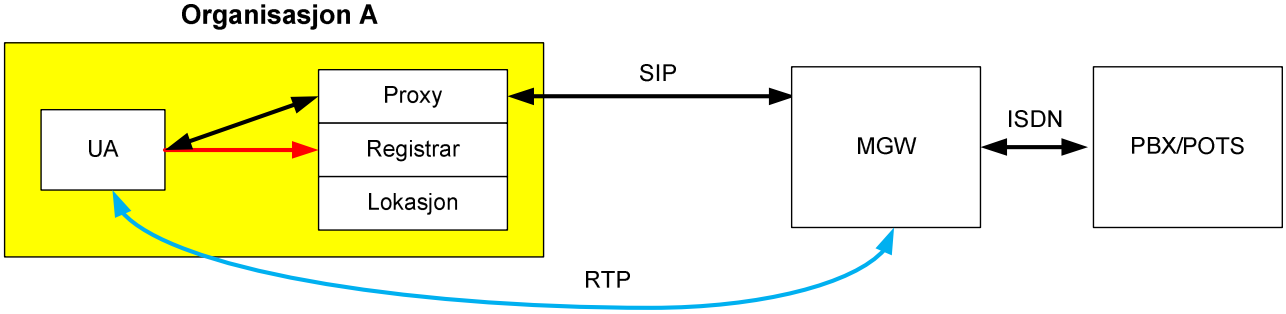


I tilfeller hvor vi opererer med en B2BUA, så vil den terminere RTP i seg selv for så å opprette en ny forbindelse frem til den andre UA. B2BUA vil i et slikt oppsett også kunne fungere som Registrar og Lokasjon og er ofte å se i konfigurasjoner der man kun ser på telefoni og ønsker en løsning i forbindelse med brannmurer e.l. Det er viktig å merke seg at en slik løsning setter kraftige begrensninger på hva man kan bruke SIP til og vil kunne representere et hinder mot ideen om en fremtidsrettet løsning dersom den ikke brukes riktig.

SIP kan gå både over UDP og TCP men UDP er mest vanlig. RTP går over UDP. Mens SIP har sine faste porter så kan RTP portene endre seg fra gang til gang. Det er ingen standard for hvilke porter dette skal være, men det har utviklet seg en anbefaling på hva det bør være og de fleste produkter har eller kan justeres til å bruke disse.

- 5060 UDP SIP signaleringsport
- 5061 TCP SIP signaleringsport
- 16384-16485 UDP primær RTP mediestrøm
- 49152-49162 UDP alternativ RTP mediestrøm

Så langt har det blitt presentert en ren SIP/RTP-modell som utgjør en viktig del av infrastrukturen. For å kunne kommunisere med parter som ikke bruker SIP/RTP, må vi ha en oversetter. Det kalles en Media Gateway (MGW). I telefoni finner vi som regel den mot telefonsentraler (PBX) og PSTN.



I dette oppsettet vil Proxy sørge for at UA har den nødvendige autorisasjon for å kunne kommunisere med MGW. MGW vil oppfattes som en UA som terminerer både SIP og RTP hos seg mens den på andre siden har en annen form for forbindelse mot f.eks. et ISDN-system. Dette kan altså være mot egen telefonsentral eller direkte på lokalt leide ISDN-linjer. Motsatt vei vil det hos MGW være en mekanisme for å finne ut hvor en PBX/PSTN originerende samtale skal for å nå UA. En MGW trenger ikke nødvendigvis kun ha SIP/RTP og ISDN men kan like gjerne ha H.323, SCCP (”Skinny” VoIP protokollen til Cisco) eller analoge linjer.

Med en MGW kan man altså knytte sammen den eller de telefonsentralene man måtte ha mot SIP. Det vil si at selv om det utstyret man ikke har støtter SIP, kan man få til en form for SIP støtte allikevel ut til andre former for telefoner ved å sette en MGW foran. Brukeren vil ikke merke noen forskjell i praksis bortsett fra en økning i mulige tjenester.

I en SIP infrastruktur kunne man ha satt opp statisk ruting mellom alle Proxy, men det er ikke skalerbar og veldig tungvindt. DNS er derfor en viktig støttespiller også for SIP når man skal finne frem til andre UA og tjenester.

NAPTR

NAPTR poster (RFC 3403) definerer hvilke protokoller som er tilgjengelig for en tjeneste hos en domene. Ved å foreta en spørring etter en NAPTR-post for domenedelen av adressen kan vi få svar på hva som støttes.

NAPTR poster er på formen "domain-name TTL Class NAPTR order preference flags service regexp target"

F.eks.: "*organisasjon.no. IN NAPTR 60 50 "s" "SIP+D2U" "" _sip._udp.organisasjon.no*."

I denne sammenheng vil D2U bety UDP og D2T bety TCP. I tillegg har vi D2S som betyr SCTP.

SRV

SRV (RFC 2782) er neste operasjon. Dersom en NAPTR finnes, vet klienten hvilke protokoller som støttes og kan finne SRV basert på det. Dersom det ikke er noen NAPTR eller at NAPTR ikke brukes, baserer klienten seg på oppslag etter egne foretrukne protokoller. Som for NAPTR spør man i SRV etter domene. Svaret skal bli den konkrete adressen til tjenesten.

SRV poster er på formen: "_Service._Proto.Name TTL Class SRV Priority Weight Port Target"

F.eks.: "*_sip._udp.organisasjon.no 3600 IN SRV 10 10 5060 sip.organisasjon.no*"

Denne adressen peker som oftest til organisasjonens primære SIP proxy som igjen eventuelt vil rute henvendelsen videre innover i sin organisasjon.

ENUM

ENUM (RFC 3761) er den siste viktige DNS komponenten. ENUM er en utvidelse av DNS som gjør det mulig å slå opp telefonnummer i E.164 format for å se om de finnes tilgjengelig på Internet.

NORID har skrevet mer E.164 og ENUM.
http://www.norid.no/enum/ENUMfokus2005.html
http://www.norid.no/enum/om_enum.html

SIP.edu har en ”kokebok”: http://web.mit.edu/sip/sip.edu/dns.shtml

ENUM er knyttet til et toppnivå som på verdensbasis foretrekkes å være e164.arpa. I Norge har dette fremdeles prøvestatus i påvente av utbredt bruk. Det er imidlertid ingenting i veien for å registrere seg i andre ENUM-trær. For UNINETT medlemmer er også nrenum.net tilgjengelig og når en del andre

akademiske organisasjoner i Europa, og e164.org er tilgjengelig for hvem som helst. Det er imidlertid viktig at det er høy kvalitet på de registrerte innslag, noe som betinger et registreringssystem under god kontroll. Det er også ønskelig med så få trær som mulig, helst bare ett, da oppslag tar tid. Selv om det er bare litt tid så blir det mer en ønskelig dersom man skal sjekke flere.

Man slår opp et fullt kvalifisert E.164 nummer som da betyr at landskoden skal inkluderes. F.eks. nummeret til sentralbordet hos UNINETT er 73557900 så et fullt kvalifisert E.164 nummer blir +4773557900.

I DNS lagrer man et nummer eller nummerserie som et domene. Numrene oppføres ”baklengs” slik man gjør med domener.

```
$ORIGIN 9.7.5.5.3.7.7.4.e164.arpa.
$TTL 86400
@       3600    IN      SOA     biff.uninett.no. hostmaster.uninett.no. (
; $Revision: 1.10 $
                                2009010101 ; Serialnumber
                                28800   ; Refresh, 8 hrs
                                3600    ; Retry, 1 hr
                                604800  ; Expire, 1 week
                                86400 ) ; Minimum (& default) TTL, 1 day
; Name servers:
                        NS      biff.uninett.no.
                        NS      nn.uninett.no.
;
; Domain data:
;
0.0                     NAPTR   10 10 "u"  "sip+E2U" "!^\\+*(.*)$!sip:\\4773557900@uninett.no!" .
0.0                     NAPTR   20 10 "u" "smtp+E2U" "!^\\+*(.*)$!mailto:post@uninett.no!" .
1.0                     NAPTR   10 10 "u"  "E2U+SIP" "!^\\+*(.*)$!sip:\\4773557901@uninett.no!" .
```

For å begynne å bruke ENUM må man få delegert de DNS-soner som tilsvarer de nummerseriene man bruker. Dette gjøres via sin registrar eller via NORID på vanlig måte.

Det er viktig ikke å begynne å publisere ENUM-informasjon før man faktisk er nåbar på de kontaktadressene man publiserer. De finnes flere rundt om i verden som bruker ENUM og som stiller forventninger til at kontaktinformasjonen fungerer.

Det er anbefalt at man ikke registrerer en brukers adresse direkte mot et gitt nummer i ENUM men heller registrerer mot et Alias som håndteres av SIP Proxy. F.eks. å knytte nummeret +4773557900 til 4773557900@uninett.no fremfor ola.nordman@uninett.no. Dette gir lettere administrasjon med oppdatering i tilfelle nummeret overtas av noen andre og det gir bedre sikring mot mail-hamstring fra DNS til uønskede formål.

Vedlegg B – SIP og sikkerhet

Dette vedlegget beskriver noen betraktninger rundt temaet sikkerhet på VoIP og telefoni generelt. Under det vide begrepet "sikkerhet" hører både pålitelighet og informasjonssikring.

Sikkerhet

Sikkerhet er noe man hører mye omtalt i forbindelse med VoIP. Når man snakker om telefoni så blir sikkerhet ofte et viktig tema fordi telefoni er en tjeneste som er svært viktig operativt, kan være sensitivt innholdsmessig og fort kan koste penger i tilfelle misbruk. Sikkerhet i telefonien er derfor et tema som bør tas på alvor.

Hva som vektlegges av sikkerhet kan variere stort fra organisasjon til organisasjon og kanskje også innenfor ulike avdelinger og grupper i organisasjonen. Organisasjonens kravspesifikasjon må derfor legges til grunn i sikkerhetsarbeidet. Første steg blir så å utarbeide en sikkerhetspolicy. Med utgangspunkt i disse dokumentene bygger man så en telefoniløsning som tilfredsstiller disse kravene, herunder også retningslinjer for drift/administrasjon og monitorering/overvåkning av tilstander.

Sikkerheten kan deles inn i to hovedkategorier:

1. **Pålitelighet** – Tjenestens evne til å fungere når man forventer det. Her må man sette opp alle relevante eventualiteter og spesifisere kravene til hvordan systemet skal fungere i tilfelle den eventualiteten inntreffer. Slike eventualiteter kan være:
    - Strømbrudd
    - Kabelbrudd
    - Utstyrsfeil
    - Utilgjengelig pga. hacking, og liknende
    - Osv.
2. **Informasjonssikkerhet** – F.eks. i hvilken grad tjenesten er i stand til å beskytte den informasjonen den formidler og beskytte mot misbruk/uautorisert bruk. Slike eventualiteter kan være:
    - Integritet
    - Konfidensialitet
    - Ansvarlighet
    - Osv.

Felles for begge kategorier er at eventualiteten kan knyttes direkte mot systemet for telefonien, eller i utenforliggende forhold hvorav noen er utenfor ens egen kontroll. F.eks. på grunn av avhengighet til eksterne ressurser. At man ikke kan ringe noen i Danmark fordi alle linjer inn i Danmark har blitt gravd over, er kanskje ikke en relevant eventualitet å sikre seg mot. Svært ofte er sikkerhet også et spørsmål om økonomisk avveining. Klarer man seg f.eks. med en telefonsentral eller må man ha to for redundans? Skal man ha en fibertilknytning til bygningen eller skal man ha en på hver side av bygget? Dersom lokal ruter går ned slik at nettforbindelsen blir brutt, har det praktisk konsekvens for telefonien eller er det ikke noe vits i telefonen heller dersom man ikke har dataverktøyet tilgjengelig? For informasjonssikkerhet kan man f.eks. vurdere faren for avlytning i forhold til hvor beskyttelsesverdig informasjonen er.

Vi har nevnt retningslinjer for drift/administrasjon og monitorering/overvåkning. Dette er viktig for å kunne opprettholde kravene i kravspesifikasjon og sikkerhetspolicy. Gjennom systemets levetid vil det være endring i interne og eksterne forhold som kan gå på bekostning av sikkerheten i systemet. F.eks. kan det være ønskelig med en jevnlig revisjon av sikkerheten, krav til en viss sertifisering eller test av klientene eller ny versjon av programvaren på klienten som skal tas i bruk, o.l. Når man får telefonien tilknyttet et datanett med dens muligheter, får vi også mange muligheter for å drive monitorering og overvåkning av bruken. Her kan man spesifisere krav som varsling ved unormal bruk av telefon, f.eks. dersom en klient plutselig ringer et teletorgnummer i utlandet tre ganger på rad så får administrator en mail og etter ti ganger så sperres brukeren.

Som nevnt har ikke alle de samme behov så det gjelder å ha en realistisk plan som passer de lokale forhold. Det kan også være juridiske forpliktelser som betinger noen krav.

Før man angriper problematikken så er det viktig å være klar over at sikkerhet på telefoni ikke er et nytt tema som har kommet med VoIP. Sikkerhetsproblemer har eksistert så lenge telefonien har eksistert. VoIP har potensialet til å løse noen av problemene men introduserer kanskje også noen nye.

Her er noen eksempler:

- Kabelbrudd – Dette kan skje like gjerne med en dedikert telefonikabel som for en datakabel. Spørsmålet er om man har en redundans i kabelen eller en alternativ kommunikasjonsform.
- Strømbrudd – Telefonileverandøren har formodentlig UPS i sitt nett og det vil være irrelevant om man kommer via IP eller ISDN. Lokal PBX har gjerne UPS også, og det kan man selvsagt også sette på systemer som VoIP er avhengig av. med. Man kan også vurdere alternative kommunikasjonsformer. Vær klar over at de færreste mobiltelefonantenner har UPS så mobiltelefonnettet mange steder i landet vil ikke fungere i tilfelle strømbrudd.
- Denial of Service (DoS) – Dette er ikke et fenomen utelukkende for datanett. Med enkle midler er det i dag effektivt å utføre DoS-angrep mot en hvilken som helst bedrifts telefonnett ved å ringe ustanselig til alle nummer. SPIT (SPAM over telefon) er også uavhengig av hvilken telefoniteknologi man selv bruker. Før var slike angrep uaktuelle på grunn av kostnaden for innringer. Med hackede telefonsentraler og IP-telefoni kan slikt i dag gjøres fra utlandet på bestilling.
- Hacking av telefonsentralen – Man kan skille mellom direkte hacking av telefonsentralen som har et administrasjonsgrensesnitt over IP, og utnytting av svakheter i teknologien eller konfigurasjonen. Mange moderne PBX har et administrasjonsgrensesnitt på IP selv om systemet selv ikke bruker VoIP. Dette har vi sett eksempler på har blitt hacket og man kan da utsettes for avlytning og/eller misbruk. Utnytting av svakheter i teknologien så vi allerede på tidlig 70-tallet med ”Captain Cruch” phone phreaking og det etter hvert mer utbredte ”Blueboxing”. Det er fremdeles en aktuell problemstilling at noen ved hjelp av modem og DTMF utforsker svakheter i konfigurasjonen til telefonisystemet for å komme til linjer som ikke var tiltenkt tilgjengelig utenfra.
- Avlytning – Før som nå er man avhengig av å få en tilkobling til kabelen som fører taletrafikken, eller hacke en telefonsentral. På analoge linjer er det så enkelt som å koble en båndopptaker direkte til kabelen. På ISDN krever det litt mer utstyr og kompetanse men er langt fra vanskelig. På VoIP må man sniffe de aktuelle nett og tolke datastrømmen, noe som sjeldent er vanskelig. På VoIP har man heldigvis også muligheten til kryptering om nødvendig.
- Sosial manipulering (Social Engineering) – En ofte undervurdert fare som sjeldent har noen direkte sammenheng med teknologi. Enkleste måte å få tak i sensitiv informasjon kan noen ganger være å rett og slett spørre.

Noen argumenter mot å ”internettifisere” telefonien er også at man fra å nyte ”security through obscurity” ved å ha systemer som krevde særskilt innsikt, går til en verden hvor langt flere har kompetanse og til å gjøre uønskede ting. Internet gjør det også raskt, enkelt og i praksis trygt for uønskede å teste systemer for svakheter. DoS er ikke et ukjent fenomen i Internet-verden og trafikkflyten kan det være en utfordring å holde sikker mot manipulering og avlytning. Til gjengjeld kan man dra nytte av en redundans og overvåkningsteknologi i eget nettverk som kanskje overgår telefonileverandørens. Verktøy for gjensidig autentisering og kryptering kan gjøre det mulig å sikre både mot misbruk, manipulering og avlytning. Ikke minst får man tilgang til testverktøy, administrasjonsverktøy og overvåkningsverktøy som kan reagere raskt i tilfelle noe utenom det vanlige skulle skje.

Vedlegg C - Migrasjonsprosessen steg for steg

For praktisk gjennomføring er det nyttig å ha gjort litt grunnarbeid på forhånd og ha en plan for prosessen. Under følger et forslag til en slik prosessplan.

UNINETT vil i samarbeid med piloter, forene teori med praksis og vil i løpet av det arbeidet høste erfaringer som vil føre til en grundigere og bedre migreringsplan enn det som fremkommer i dette dokumentet.

Oversikt over punktene

1. Kartlegging av eksisterende telefonisystem / dokumentering
2. Etablering av SIP PBX
3. Etablering av MGW
4. Etablering av tjenester
5. Kobling mot TELEFON MGW med prøvenummer
6. Etablering av brukerdatabase for SIP brukere til test
7. Etablere prøveklienter
8. Testing av lokal infrastruktur alle veier
9. Etablering av brukerdatabase for alle SIP brukere
10. Etablering av provisjoneringstjeneste
11. Omlegging av et utvalg brukere for en testperiode
12. Individuavhengige klienter
13. Dokumentasjon/Konkretisere roller
14. Sette infrastrukturen i drift
15. Fase ut PBX og MGW

1. Kartlegging av eksisterende telefonisystem / dokumentering

Det er viktig å vite hva man har og hvordan det fungerer.

Dokumenter:

- Alle nummer/serier, hva de brukes til og om nødvendig lokasjon. Kontor, møterom, fax, porttelefoner, heistelefoner, osv.
- Type apparater og antall
- Type PBX, programvareversjon og tilhørende utstyr.
- Ringegrupper og spesialnummer
- Hvordan sentralbordet brukes i praksis.
- Spesielle løsninger

Med støtte i denne dokumentasjonen skal man så skrive en kravspesifikasjon til det nye systemet med tanke på telefoni. I noen tilfeller vil det være snakk om å duplisere en eksisterende funksjonalitet, i andre tilfeller kan det være å droppe funksjonaliteter som blir lite eller ikke brukt eller å legge til ny ønsket funksjonalitet.

Det må påregnes en god del tid til denne prosessen. Manglende oppføringer kan føre til komplikasjoner og ekstra tap av tid senere i prosessen.

2. Etablering av SIP PBX

Dette er kjernen i den lokale infrastrukturen. Den kan gjerne komme tidlig på plass og arbeidet på den vil være en kontinuerlig prosess. Det er viktig å velge en god hardware som gir ønsket grad av redundans og som håndterer mengden av UDP trafikk tilfredsstillende. Prinsipielt er dette en PC med minimum ett nettverkskort. Vi anbefaler Ubuntu Server 8.04LTE som operativsystem og OpenSER/KAMAILIO som SIP Proxy.

Den må i første omgang ha grunnleggende konfigurasjon for å håndtere samtaleruting og registrering av brukere, dvs. kobling mot en brukerdatabase. I forbindelse med samtalerutingen legges det inn eventuelle begrensninger i hva brukerne får lov til å ringe og ikke.

Sikkerhet må ivaretas ved hjelp av sikring av OS og nødvendige filter i f.eks. iptables og/eller router.

3. Etablering av MGW
En media gateway må stå mellom SIP PBX og lokal PBX. Det er en eller flere maskiner hver med ett eller flere PRI-kort som er koblet mot PRI-kort i PBX. Gjennom IP er den i den andre enden koblet mot SIP PBX. MGW kan også bruke SIP i stedet for PRI mot PBX.

Hvorvidt dette er dedikert hardware eller om MGW maskinen kan være den samme som SIP PBX maskinen må vurderes i hvert enkelt tilfelle. Mindre institusjoner er muligens tjent med å slå dem sammen mens større bør skille dem. Utover det anbefaler vi bruk av Asterisk og Digium PRI-kort som er godt støttet i Asterisk.

MGW settes opp til å videreformidle innkommende samtaler på den ene siden til å gå til den andre siden og på den måten holder kompleksiteten i konfigurasjonen til et minimum. Selve samtalerutingen er SIP PBX sin oppgave å håndtere.

PBX på sin side må settes opp med nødvendig bestykning av PRI-kort for kobling mot MGW. Konfigurasjonen kan gjøres slik at alle samtaler som ikke skal til et annet PBX-tilkoblet apparat går ut på PRI-forbindelsen. Innkommende samtaler til PBX gjennom PRI-forbindelsen vil kun være til de apparater som er tilkoblet PBX. I praksis kan man si at MGW+PBX blir som en stor SIP-konverteringsenhet (ATA) for enheter som ikke håndterer SIP. Merk at denne konfigurasjonen selvsagt ikke kan gjøres før SIP PBX er tilkoblet TELEFON MGW og at telefonileverandøren har rutet om organisasjonens nummer til å gå over SIP til TELEFON MGW. I en testfase kan man i PBX plukke ut spesifikke nummer som skal rutes ut via MGW.

I noen tilfeller kan det være at man har en PBX som kan SIP. I så fall kan det være at MGW kan sløyfes, men det må i så fall testes ut i hvert tilfelle. Ikke alle leverandørers SIP håndteres på ønsket måte.

4. Etablering av tjenester
I de tilfeller hvor man ønsker lokale telefonitjenester, kan man begynne å etablere denne tjenesten i parallell med SIP PBX. Typiske basistjenester er telefonsvarer og telefonkonferanser. Utover dette er det opp til lokale behov og kreative evner.

Dette kan være en eller flere maskiner eller det kan være en egen prosess på SIP PBX i noen tilfeller. Lokale forhold og preferanser avgjør dette. Vi anbefaler bruk av Asterisk som tjenesteplattform da det er en terminerende instans med svært mange utvidelsesmuligheter.

Tjenester vil kunne være tilgjengelig både for SIP brukere og brukere av vanlig telefoni såfremt man har en SIP PBX til å rute samtalene.

5. Kobling mot TELEFON MGW med prøvenummer
Med SIP PBX på plass kan man med hjelp fra UNINETT få etablert noen prøvenummer og koble seg mot TELEFON MGW. Dette innebærer litt konfigurasjon av TELEFON MGW, SIP PBX og filter slik at partene kjenner hverandre.

Dette er første fase for å kunne teste at infrastrukturen fungerer tilfredsstillende.

6. Etablering av brukerdatabase for SIP brukere til test
SIP PBX må ha en brukerdatabase for å kunne autentisere og holde rede på legitime brukere.

I første omgang kan det være lurt å bruke noen fiktive testbrukere i forbindelse med prøvenummer mot TELEFON MGW. Dette vil være brukere en kan eksperimentere litt med for å se om systemene reagerer som forventet.

Dette er andre fase for å teste infrastrukturen

7. Etablere prøveklienter

For å kunne teste infrastrukturen tilfredsstillende trenger man et utvalg relevante klienter til å teste registrering og bruk av telefonitjenestene til SIP. Relevante klienter kan være ulike typer bordtelefoner, trådløse telefoner, mobiltelefoner med SIP og softwarebaserte klienter. Disse må kunne registrere seg med testbrukeren mot SIP PBX fra ønskede IP subnett og kunne kommunisere med RTP til andre SIP klienter både i og utenfor organisasjonen og med TELEFON MGW.

Dette er tredje fase for å teste infrastrukturen.

8. Testing av lokal infrastruktur alle veier

I siste fase av testingen bruker vi en kombinasjon av etablerte testbrukere, brukere fra PBX og eksterne telefonnummer (f.eks. mobiltelefon) til å teste at infrastrukturen fungerer som ønsket alle veier og at tjenester fungerer som ønsket.

9. Etablering av brukerdatabase for alle SIP brukere

Når infrastrukturen er testet og fungerer tilfredsstillende, kan man etablere en endelig brukerdatabase for alle SIP brukere.

Det bør være en kilde for brukerdata å bruke som grunnlag for så å supplere med nødvendig tilleggsinformasjon. I første omgang kan brukere genereres automatisk med f.eks. allerede etablert brukernavn i kombinasjon med et automatisk generert passord av tilfredsstillende kompleksitet. BAS er et eksempel på en slik kilde. Til senere administrasjon og vedlikehold kan man tenke seg en web side beskyttet med FEIDE hvor den enkelte bruker kan gå inn å justere på parametere som viderekobling, tid før telefonsvarer, generering av nye passord for klienter, o.l.

Samtlige brukere bør som et minimum ha et brukernavn som allerede er etablert men med Alias til navn på form som mailadressen og telefonnummeret.

F.eks.

Brukernavn:	olan@institusjon.no
Alias 1:	ola.nordman@institusjon.no
Alias 2:	73557900@institusjon.no

Passord bør være på minimum 12 tegn og kun være alfanumeriske med en god blanding av store og små bokstaver. Av sikkerhetsmessige hensyn bør ikke brukeren selv få anledning til å lage disse passordene. Passordet bør heller ikke brukes av andre systemer.

Samtlige av institusjonens telefonibrukere kan registreres i denne databasen, selv de som er tilkoblet gammel PBX. SIP PBX vil dermed sørge for at også eldre telefoner får en nåbarhet over SIP og dra nytte av mange av tjenestene.

I brukerdatabasen må det også legges brukere for telefoner som ikke er knyttet mot et individ, slik som møteromstelefoner, resepsjon, porttelefon, fax, osv. Som SIP-klienter må de ha et brukernavn og passord, samt alias som gjør det lett å finne frem til via SIP.

F.eks.

Brukernavn:	faxresepsjon@institusjon.no
Alias 1:	fax.resepsjonen@institusjon.no

Alias 2: 73557901@institusjon.no

Slike brukere må administreres spesielt av de rette ansvarlige.

10. Etablering av provisjoneringstjeneste

Provisjonering er automatisk oppsett og konfigurasjon av en klient. Det kan bety vesentlig lettere administrasjon dersom en provisjoneringstjeneste er optimalt satt opp. Ideelt vil det være mulig å plugge en helt fabrikkny telefon i nettverkskontakten og få den automatisk ferdig satt opp og klar for brukeren.

Ulike telefoner har ulike måter å gjøre dette på så metode og rutine vil være forskjellig avhengig av merke og modell. Ut i fra switchporten en telefon blir satt inn i eller telefonens MAC-adresse, som gjerne er oppført på telefonen og/eller esken, kan man i kombinasjon med brukerinformasjon i brukerdatabasen skreddersy en automatisk konfigurasjon med ønskede parametre.

Det bør vurderes hvordan en bruker kobles mot en gitt klient også. Man kan f.eks. ha løsninger hvor selve klienten er registrert som en egen entitet og hvor brukeren via apparatet selv melder seg inn (og ut) på den aktuelle telefonen eller løsninger hvor brukeren er direkte registrert via apparatet. Her finnes det flere varianter som kan vurderes etter institusjonens ønsker og behov.

11. Omlegging av et utvalg brukere for en testperiode

I en overgangsperiode vil det være fornuftig å prøve ut det nye systemet med en liten gruppe individer som kan komme med tilbakemeldinger om hvordan systemet fungerer. Det er mange steder hvor det kan ligge feil å lure og som til tross for testing i forkant ikke vil manifestere seg før man har brukt systemet slikt det var tiltenkt.

Ting man bør være oppmerksom på er:

- Kan brukerne registrere seg mot SIP serveren (Brukerdatabase/konfigurasjon)
- Filter som forhindrer fri ferdsel for RTP (Typisk tale kun en vei)
- Nummer som ikke kan nås når man ringer ut (Er nummerplanen riktig satt opp? MGW? ENUM?)
- Nummer som ikke kan nås når man ringer inn (Riktig nummerplan? MGW? ENUM?)
- ”Støy” på linjen, dårlig kvalitet på lyden? Ekko? Merkbar forsinkelse av lyden? (Kapasitetsproblemer i nettverket? Riktig CODEC-valg? Ekko-kansellering?)
- Virker alle oppsatte tjenester?
- Holder samtalen seg oppe eller blir den avbrutt etter en viss tid.
- Fungerer sikkerhetstiltakene? Går det å ringe nummer det ikke skal ringes til? Slår filter og advarsler til om man overstiger satte grenseverdier?

På denne måten får man forhåpentligvis luket ut de fleste feil før man går inn i en driftsfase.

12. Individuavhengige klienter

Veldig mange telefoner og telefonnummer er knyttet mot et gitt individ som utfyller en bestemt rolle. Disse er som regel grei å forholde seg til fordi man kan ha en konto og telefon som er basert på individet. Det er imidlertid ikke uvanlig å finne telefoner som har en mer generell eller spesifikk rolle som ikke er knyttet mot et individ. Det er heller ikke sikkert at å finne en SIP-erstatning er trivielt. Det er derfor viktig at institusjonen går igjennom alle disse telefonløsningene og finner den løsningen som er optimal i hvert enkelt tilfelle.

Dette utvalget er ikke utfyllende men ment å gi noen eksempler:

- Møterom – Kan ofte være en vanlig SIP-bordtelefon men tilknyttet en ”møteroms”-bruker.
- Resepsjon Gjerne et litt spesielt apparat med flere linjer og indikasjoner på status på andre linjer. Det kan også være snakk om at den skal fungere i forbindelse med en applikasjon eller utelukkende som en applikasjon (softphone). Funksjoner som overføre, viderekoble, monitor, o.l. kan være viktig. Slike behov må vurderes for hvert enkelt tilfelle for å finne den løsningen som passer best.

- FAX – FAX over SIP med ATA eller alternativ løsning med FAX over Internet.
- Porttelefon – Gjerne analogt. Erstattes med en ren SIP-løsning eller kobles via en ATA
- Heistelefon – Gjerne analogt. Erstattes med en ren SIP-løsning eller kobles via en ATA

13. Dokumentasjon/Konkretisere roller

Å dokumentere systemet er viktig for den videre drift. Det er nyttig for feilsøking, opplæring og videre utvikling. Like viktig er det å oppdatere dokumentasjonen når endringer gjøres.

Driftsdokumentasjon trengs for å kunne ivareta den daglige drift. F.eks. hvilke systemer skal være oppe? Hva gjør man for å legge til en ny telefon? Hvordan flytter man en bruker fra PBX til SIP? Hvordan oppdaterer man systemet til nyere versjon? Hvem kontaktes for å gjøre hva?

Det er også viktig å tydeliggjøre hvem som har ansvaret for de ulike områdene av teknologien slik at henvendelser og aksjoner kan gjøres så effektivt og rimelig som mulig.

Brukere av systemet må heller ikke glemmes. En telefon klarer de flest å bruke, men det kreves kanskje litt mer innsikt for å kunne utnytte alle mulighetene SIP gir. Spesialfunksjoner som f.eks. resepsjonen krever mest sannsynlig utvidet opplæring. Web-sider med hjelp til selvhjelp kan også være et nyttig verktøy.

14. Sette infrastrukturen i drift

Når dokumentasjonen er i orden og praktiske prøver med pilotbrukere har vist seg tilfredsstillende, kan systemet få en endret status til drift.

Fra da av vil man kunne flytte over brukere fra gammel PBX til SIP i det tempo man selv ønsker. Opplæring av brukerne vil være en kontinuerlig prosess.

Administrasjon gjøres i henhold til dokumentasjonen som igjen oppdateres og justeres etter behov.

15. Fase ut PBX og MGW

Som en naturlig konsekvens av at alle telefoner og brukere har migrert fra PBX til SIP, kan PBX fases ut og med den også MGW.

Forkortelser

ATA	Analog Telephone Adapter. Enhet som fungerer som en SIP UA i den ene enden og en analog telefontilkobling i den andre enden. Gjør at analoge telefoner kan bruke SIP. Kan også brukes for FAX. Det finnes også måter for å koble til ISDN-telefoner, for eksempel via et ISDN-kort i en vanlig PC.
B2BUA	Back-2-Back User Agent. En «endestasjon» (sender/mottaker) i SIP-terminologi er en User Agent. Når man sier det er en B2BUA så er den en mer eller mindre «usynlig» bru mellom to andre parter men fremstår teknisk som de respektive parters samtalepartner. Både SIP-strømmen og RTP-strømmen kanaliseres gjennom en B2BUA.
CDR	Call Detail Record – en beskrivelse av samtaler som har funnet sted, som fra, til, tidspunkt, varighet, m.m.
ENUM	Registrering av telefonnummer i E164-format i DNS slik at man kan gjøre oppslag (resolve) til en SIP URI dersom denne er tilgjengelig.
MGW	Media GateWay. Fungerer som oftest som et bindeledd og «oversetter» mellom to ulike kommunikasjonsteknologier. En MGW kan også fungere som en portal hvor en ønsker å ha full kontroll på trafikken som strømmer igjennom. Det innebærer også selve talestrømmen.
PBX	Private Branch Exchange. Betegnelse for en privat telefonsentral/hussentral. I tradisjonell forstand er det en enhet hvor organisasjonens telefoner er fysisk tilkoblet. Mot PSTN er det tilknytning via for eksempel PRI.
PRI	Primary Rate Interface. En telekommunikasjonsstandard for bærer av flere tale og/eller datakanaler i form av ISDN (64 Kbps). En PRI er gjerne tilkoblet en E1-forbindelse som er på 2.048 Mbps, noe som i Norge gir oss 30 B-kanaler (ISDN tale/data) og 1 D-kanal (kontroll) i PRI.
PSTN	Public Switched Telephone Network. Betegnelsen for det verdensomspennende (for det meste digitale) telefoninettverket som består av fasttelefoner og mobiltelefoner.
RTP	Real-Time Transport Protocol. Brukes for datastrømmen i en SIP-samtale. En hver vei mellom partene.
SIP	Session Initiation Protocol. En samling IETF RFC som beskriver person-til-person signalering, som oftest i den hensikt å opprette en direkte tale- og/eller videostrøm mellom partene (SIP UA).
SIP Proxy	Kan også kalles en SIP ruter.
SIP Registrar	En tjeneste hvor UA kan autentisere seg og knytte seg til som del av et SIP-domene.
SIP UA	SIP User Agent. Det man kan oppfatte som klienten eller «telefonapparatet» i SIP-verden.
SIP URI	SIP Uniform Resource Identifier. En adresse i SIP-format. F.eks. på formen SIP:ole@uninett.no