



# GIGACAMPUS 2006–2009

SAMORDNET NETTBYGGING PÅ NORSKE UNIVERSITETER OG HØGSKOLER



# INNHold

Forord .....	5
Leserveiledning .....	6
<b>Sammendrag .....</b>	<b>8</b>
<b>Bakgrunn.....</b>	<b>12</b>
2.1 Nasjonal og internasjonal forskning stiller krav .....	12
2.3 Moore's lov .....	14
2.4 Europeisk satsing.....	16
2.5 Etablert samarbeidskultur .....	16
2.6 Økonomiske besparelser .....	17
<b>Visjon.....</b>	<b>20</b>
<b>Hovedmål .....</b>	<b>24</b>
<b>Satsingsområder .....</b>	<b>26</b>
5.1 Fysisk infrastruktur .....	27
5.2 Høykapasitetsnett .....	29
5.3 Mobilitet .....	32
5.4 Person til person-kommunikasjon .....	36
5.5 Sikkerhet.....	40
5.6 Drift og overvåking .....	44
5.7 Ende til ende-kvalitet.....	46
<b>Sentrale prosesser.....</b>	<b>50</b>
6.1 UNINETT fagstyrke.....	50
6.2 Innkjøpssamarbeid .....	51
6.3 Prosjektstøtte for felles verktøy og løsninger.....	51
6.4 Implementasjons- og driftsstøtte.....	52
6.5 Kompetanseheving .....	53
<b>Dokumentasjon og erfaringsspredning.....</b>	<b>56</b>
<b>Organisering og forankring .....</b>	<b>58</b>
<b>Koordinering med andre satsinger .....</b>	<b>60</b>
<b>Finansiering .....</b>	<b>64</b>
<b>Behov for nye krafttak.....</b>	<b>65</b>
<b>Vedlegg.....</b>	<b>68</b>
<b>Ordliste.....</b>	<b>72</b>

VÅR VISJON ER EN KOORDINERT IKT-INFRASTRUKTUR PÅ  
CAMPUS I INTERNASJONAL TOPPKLASSE, SOM INVITERER  
TIL INNOVASJON, SAMARBEID OG EFFEKTIV FORSKNING  
OG UTDANNING.

## FORORD

Oppgradering av forskningsnettet i Norge har fortsatt i hele 2005 og vi nærmer oss målet med gigabitkapasitet til alle universiteter og høyskoler i 2006. Som i de øvrige nasjonale forskningsnettene i Europa, opplever vi nå at det svakeste leddet i kommunikasjonsskjeden mellom sluttbrukerne er blitt campusnettene. Campusnettene er ikke rustet for gigabitkapasitet, og har heller ikke tilfredsstillende funksjonalitet for blant annet sikkerhet, nettovervåking, kontroll og trådløse nett. Infrastrukturen på campus som vi bygde opp fra begynnelsen av 1990-tallet holder ikke lenger mål, og vi er nødt til å gjøre et felles løft for at campusnett og forskningsnett igjen skal være på samme nivå.

For at sentral nasjonal koordinering skal få best effekt, må vi gjennomføre endringene i campusnettene på en standardisert måte. Vi må finne fram til felles tekniske løsninger og felles omforente driftsløsninger så langt dette er praktisk mulig. For å kunne realisere dette har UNINETT utformet et 4-års utviklingsprogram, GigaCampus, som presenteres her:

GigaCampus har fått sentrale tilskudd i statsbudsjettet for 2006, og det er i tillegg gitt øremerkede midler til det enkelte universitet og høyskole. Et eksternt dominert programstyre blir nå etablert og detaljplaner er under utarbeidelse. UNINETT har under forprosjektperioden i 2005 opprettet et antall arbeidsgrupper med nøkkelpersoner fra UNINETT og institusjonene i sektoren. Arbeidsgruppene vil bestå av de dyktigste ressurspersonene i hele sektoren. Kompetanseoverføring og tekniske avklaringer skjer i felles arbeidsgruppemøter, og resultatene konkretiseres i tekniske anbefalinger som benyttes av GigaCampus og institusjonene selv. Nye arbeidsgrupper og oppgaver kan komme til underveis i programmet.

Flere andre av våre øvrige aktiviteter vil være premissleverandører til GigaCampus. FEIDE-prosjektet utvikler strategier for hvordan elektronisk autentisering kan realiseres for alle ansatte og

studenter/elever ved norske utdanningsinstitusjoner. I GigaCampus-regi vil FEIDE blant annet levere løsninger for hvordan identifisering av brukere i trådløse nett kan realiseres på campus. UNINETT's Samson-prosjekt vil levere tjenermaskiner til GigaCampus for instrumentering av campusnettet og for administrasjon av ulike samarbeidstjenester som f.eks. videokonferanser.

UNINETT vil også neste år delta tungt i det europeiske GÉANT2-prosjektet. Nesten all vår virksomhet i dette prosjektet inngår direkte som delaktiviteter i GigaCampus. Med GigaCampus har vi startet en satsing som vekker internasjonal interesse, og som flere land følger nøye med på.

Petter Kongshaug  
administrerende direktør  
UNINETT

## LESERVEILEDNING

Kapittel 5 Satsingsområder forutsetter at leseren har inngående kjennskap til IKT-faglige begreper.

Bakerst finnes en ordliste som beskriver både forkortelser og faglige begreper som brukes underveis i teksten. I teksten er disse ordene **merket med rødt**.



# SAMMENDRAG

## SAMMENDRAG

UNINETT lanserer et fireårig program: GigaCampus 2006–2009. Universitets- og høyskolerådet stiller seg bak og programmet har støtte og bevilgning gjennom statsbudsjettet for 2006.

Vår visjon er en koordinert IKT-infrastruktur på campus i internasjonal toppklasse, som inviterer til innovasjon, samarbeid og effektiv forskning og utdanning.

GigaCampus har et avgrenset og målrettet fokus på kommunikasjonsinfrastruktur. I samarbeid med sektoren skal programmet sørge for standardisert opprusting av campusnettene og den lokale IKT-kompetansen ved landets universiteter og høyskoler. GigaCampus skal gi grobunn for fremtidens IKT-tjenester, og programmet skal svare på de utfordringer og krav som forskning, undervisning og administrasjon stiller. Dette omfatter også de særlige behov en sterkt voksende **eVitenskap** fører med seg.

Programmet arbeider mot sju definerte hovedmål. I 2009 skal:

- norsk UH-sektor ha et høykvalitets og feiltolerant datanett med gigabitkapasitet til de fleste arbeidsstasjoner. Særlige brukergrupper skal tilbys høyere kapasitet.
- landets studenter, forskere og øvrige ansatte sømløst kunne bevege seg på campus med trådløs nettilgang fra PC-er og håndholdte enheter som blant annet **PDA**-er.
- IP-basert person til person-kommunikasjon være tilgjengeliggjort. Det skal være enkelt å etablere sanntids tale- og videosamtaler over nett.
- UH-sektorens sikkerhetsarbeid være godt koordinert. Lokale sikkerhetsteam (IRT, Incident Response Teams) skal være etablert og felles rammeverk for sikkerhetspolicy tatt i bruk.

- proaktiv drift ha et sterkere fokus. Felles standarder og anbefalinger skal være implementert og verktøy og løsninger skal være bredt anvendt i sektoren.
- gode virkemidler fange opp og utbedre kvalitetsmessig forringelse av tjenester. Vi skal ha et særlig fokus på å ivareta sanntidskrav.
- et bredt anlagt og omfattende kompetanseløft være gjennomført. Sektorens samarbeidsvilje og -evne skal stå sterkt. Kostnadseffektive drifts- og utviklingsmodeller skal fungere og et formålstjenlig innkjøpsamarbeid skal være på plass.

GigaCampus har sju satsingsområder:

1. Fysisk infrastruktur
2. Høykapasitetsnett
3. Mobilitet
4. Person til person-kommunikasjon
5. Sikkerhet
6. Drift og overvåking
7. Ende til ende-kvalitet

Satsingsområdene beskrives nærmere i kapittel 5.

GigaCampus skal ha et tydelig fokus på kompetansebygging. Kurs, konferanser og andre opplæringstiltak står sentralt og vi skal bidra til at IKT-kompetansen ved hvert enkelt universitet og høyskole skal økes betraktelig i programperioden. Dokumentasjon og erfaringsspredning er en viktig del av programmet. Eksterne og interne websider skal inneholde oppdatert og god informasjon om programmets resultater og planer.

GigaCampus skal bygge videre på sektorens gode samarbeidsklima. Programmet tar initiativ til UNINETT fagstyrke, en ny og drivende faglig allianse som målrettet skal utarbeide anbefalinger og veiledninger med basis i sektorens **beste praksis**. UNINETT fagstyrke organiseres gjennom arbeidsgrupper der



aktiv deltagelse fra sektoren er essensielt. Fagstyrken koordineres med andre nasjonale og internasjonale arenaer som eVITA, GÉANT2, TERENA, Q2S og IETF. Med internasjonal kontaktflate og som brobygger mellom operative miljø og FoU, skal UNINETT fagstyrke bane vei for de beste løsninger.

Fremfor alt skal GigaCampus være resultatorientert og kostnadseffektiv. Basert på fagstyrkens anbefalinger skal konkrete og målbare resultater settes ut i live i sektoren. GigaCampus skal være pådriver for felles verktøy og løsninger. Der det er rasjonelt og formålstjenlig, skal GigaCampus sørge for felles innkjøpsavtaler.

GigaCampus programledelse legges til UNINETT. Programledelsen rapporterer til programstyret, som vil ha bred deltagelse fra IKT-ledelsen ved universiteter og høyskoler. Programstyrets viktigste oppgave blir å påse at bevilgede midler brukes rettferdig i sektoren.

Over statsbudsjettet for 2006 er tilsammen 27,6 millioner kroner bevilget GigaCampus. Midlene vil bli disponert rasjonelt og hensiktsmessig i tråd med programmets intensjoner. En reell kollektiv besparelse skal påvises. Vi innser at 2006-bevilgningen ikke er tilstrekkelig for å nå alle programperiodens mål. Vi erkjenner også at den betydelige veksten i ressursbehov knyttet til IKT bare vil fortsette.





# BAKGRUNN

## BAKGRUNN

I dette kapitlet beskrives bakgrunnen for Giga-Campus og hvorfor UNINETT har fremmet programmet.

GigaCampus er et kollektivt initiativ for å løfte den nettverksmessige infrastrukturen ved alle norske universiteter og høyskoler. Satsingen vil gå side om side med en videre utbygging av det nasjonale forskningsnettet. GigaCampus er et fireårig program, og vi ser her på mange av de utfordringer som vil møte oss i perioden 2006-2009.

*«We can only see a short distance ahead, but we can see plenty there that needs to be done.»*

(Alan Turing)

Det er umulig å forutse alle fremtidens behov. Innovasjonsraten innen datakommunikasjon er eksponensiell, og vi befinner oss midt inne i en kommunikasjonsrevolusjon. Dette i seg selv tilsier at vi må ha et sterkt fokus på underliggende infrastruktur. Vi må være forberedt på det som kan og vil møte oss. Her ligger muligheter som norske universiteter og høyskoler bør og skal gripe – nye muligheter for forskning, undervisning og formidling.

GigaCampus har støtte gjennom statsbudsjettet for 2006, der følgende formulering er gitt:

«Det er særst viktig at campusnetta vert utvikla i takt med trafikkveksten og ytingskrava i sektoren, slik at tenestene når fram til brukaren på ein hurtig og sikker måte. GigaCampus-programmet vil, i tillegg til å auke trafikkapasiteten, heve sikkerheita, betre trafikkovervakinga, stimulere utviklingsmiljø, samt samordne infrastrukturen. Ei slik standardisering vil fremme kostnadseffektive og gode fellesløyningar, og ein robust nasjonal nettstruktur er ein føresetnad for at sektoren kan gi best mogeleg undervisning og arbeide med avansert forskning.»

«GigaCampus-programmet vil vere eit samarbeidsprosjekt mellom UNINETT og universitets- og høyskolesektoren.»

## 2.1 NASJONAL OG INTERNASJONAL FORSKNING STILLER KRAV

Stortingsmeldingen «Vilje til forskning» fra 2005 legger frem de nye prioriteringene for norsk forskningspolitikk, og her vektlegges betydningen av informasjons- og kommunikasjonsteknologi. IKT skal prioriteres som ett av tre teknologiområder og anses å være et uvurderlig redskap for forskning. Videre heter det at datakommunikasjon har bedret tilgjengeligheten for forskningsresultater dramatisk og økt kunnskapsutvekslingen over landegrensene.

Meldingen legger vekt på å styrke internasjonalt forskningssamarbeid og støtter her oppunder Bologna-avtalen, som er en europeisk deklarasjon om høyere utdanning som Norge undertegnet i 1999. Bologna-avtalen tilsier mer samarbeid mellom universitetene internasjonalt. Strukturelle hindringer for mobilitet for forskere og studenter skal fjernes.

Et nytt og voksende forskningsområde er **eVitenskap**. eVitenskap har fått betegnelsen den tredje vei, eller det tredje alternativet, der de to andre er teoretiske vurderinger og fysiske eksperimenter. Eksperimenter vil i fremtiden bli stadig mindre brukt, enten fordi det er farlig, kontroversielt, upraktisk, forurensende eller kostbart. Innen eVitenskap brukes avansert vitenskaplig utstyr, herunder regneressurser knyttet sammen i det globale nettet for å søke innsikt i kompliserte naturvitenskapelige, teknologiske og medisinske fenomener. Potensialet som de internasjonale forskningsnettene her representerer er på langt nær utnyttet.

Et langsiktig og helhetlig program for **eVitenskap** i Norge, **eVITA**, er foreslått. Programmet fokuserer på beregninger i vitenskaplige og industrielle anvendelser og beregningsorientert matematikk, statistikk og informatikk. For å underbygge dette foreslås en betydelig satsing på infrastruktur som nettverk og maskinvare, herunder tungregning, tunglagring og **Grid-løsninger**.

Grid-løsninger er programvare bygget over Internett som skal gi brukere effektiv og sømløs tilgang til data, regneressurser og systemer for å utføre ulike oppgaver. Det forventes at Grid vil ha like stor industriell og forskningsmessig betydning de neste 10 årene som innføring av web-løsninger har hatt de siste 10 årene.

GigaCampus sitt infrastrukturinitiativ med gigabit-kapasitet til den enkelte forsker bygger direkte opp under «Vilje til forskning» og eVITA. Et nasjonalt løft på IKT-infrastrukturen er en nødvendig premisse for å nå «Vilje til forskning» sin ambisjon om å gjøre Norge til en ledende forskningsnasjon.

**Bologna-avtalen ble undertegnet i Bologna, Italia, av 29 land, inkludert Norge. Deklarasjonen har som målsetting å etablere et europeisk rom for høyere utdanning, slik at høyere utdanning i Europa skal kunne måle seg med utdanning i USA og den øvrige verden. Det er et mål å utvikle en bedre samordning av studieplaner, samarbeid mellom institusjoner, planer for mobilitet og integrerte programmer for studier, praksis og forskning. Midlene for å nå dette målet er identifikasjon og fjerning av formelle og strukturelle hindringer for mobilitet for studenter og forskere, innføring av transparente og sammenlignbare grader og karakterer, samt samarbeid om kvalitetssikring gjennom utvikling av sammenlignbare kriterier og metoder.**

## 2.2 BRUKSOMRÅDER I VEKST

Utover de formidable krav forskningen stiller, vil vi i programperioden se en generell og betydelig tilvekst av nye bruksområder. Sannsynlige utviklingstrekk er:

- **Mer kringkasting av undervisning**

Stadig flere forelesninger vil i fremtiden bli filmet og gjort tilgjengelig for studentene over nett, enten ved kringkasting i sanntid eller ved at videoarkiv benyttes. Vi må forvente en stor vekst i nedlasting av slikt tungt innhold.

- **Person-til-person kommunikasjon over nett**

Dette gjelder en rekke sanntidsapplikasjoner som IP-telefoni, videokonferanser, lynmeldinger og tilstedemarkering. For fremtidens studenter, forskere og andre ansatte vil bruk av multimedie-samtaler være like naturlig som dagens telefonsamtaler. Vi vil se et omfangsrikt løft i hvordan vi kommuniserer og samarbeider over avstand.

- **Nomadiske tjenester i mobile nett**

Studenter og ansatte ønsker nettilgang fra alle tenkelige steder. Fullt utbygde trådløse nett på alle campus blir et folkekrav. I neste instans vil dette bli utvidet til større sammenhengende dekningsområder, slik det bl.a. skisseres i «Trådløse Trondheim», der målet er å gjøre store deler av byen trådløs. En rekke stedbaserte tjenester vil komme. Et eksempel kan være forelesningsplan til det auditoriet du er ved eller informasjon om nærmeste kantine eller bokhandel. Utover bærbare PC-er vil bruk av små, håndholdte enheter eksplodere. Særlig utfordrende kan WLAN-telefoni bli. Krav til mobilitet og sømløshet vil bli satt på en helt ny prøve. Allerede nå har mobiltelefoner som støtter både GSM og WLAN/SIP begynt å komme. Å sørge for sømløshet mellom tradisjonelle mobilnett og trådløse nett blir en viktig utfordring.

- **Sentralisering av tjenester**

Dersom man ser sektoren under ett, er det ikke rasjonelt at drift av alle tjenester spres utover for

mange institusjoner eller avdelinger. Sentralisering og rasjonalisering av tjenestedrift har allerede tvunget seg frem, og for mange institusjoner har en sentralisert fil-, skriver- og/eller sikkerhetskopieringstjeneste vist seg formålstjenlig. Sentraliserte tjenester stiller krav til kapasitet og kvalitet på det mellomliggende nett. Tilgjengelighet blir bare viktigere, og vi må bygge robuste, feiltolerante løsninger. Vi må også vurdere lagring på flere adskilte steder.

- **Mer tungregning, nasjonale og internasjonale Grid**

Vi har store tungregnesenter ved de fire største universitetene, og disse vil rustes opp ytterligere i programmerperioden. Grid vil få sine utspring fra tungregnemiljøene. De vil utgjøre fundamentalt viktige, kapasitetshungrige overbygninger over det nettet GigaCampus skal sørge for. **Lambdanett** vil komplettere bildet og gi mulighet for dedikerte forbindelser til særlig krevende brukergrupper. Lambdanett forutsetter kontroll på fiberinfrastrukturen, også langdistanse. Med kontroll menes her enten eierskap til fiber eller avtalemessig leie av mørk fiber, ev. leie av et sett med bølgelengder/optiske kanaler. Ved å benytte **optiske bølgelengdemultipleksere** kan vi utnytte flere kanaler i hver enkelt fiberkabel, og på denne måten mangedoble den totale kapasiteten.

- **Nasjonale deponi av rådata**

Vi vil se stadig større deponi av rådata som tilgjengeliggjøres over nett. Et eksempel er klimadata, som minimum må lagres i 10 år. Andre eksempler er blant annet petroleumsforskning, nanoteknologi, medisinsk og bioteknologisk forskning. Der vi for tungregning snakker om beregningsgrid, vil vi her se nasjonale lagringsgrid.

- **Fjerninstrumentering, telemedisin og romforskning**

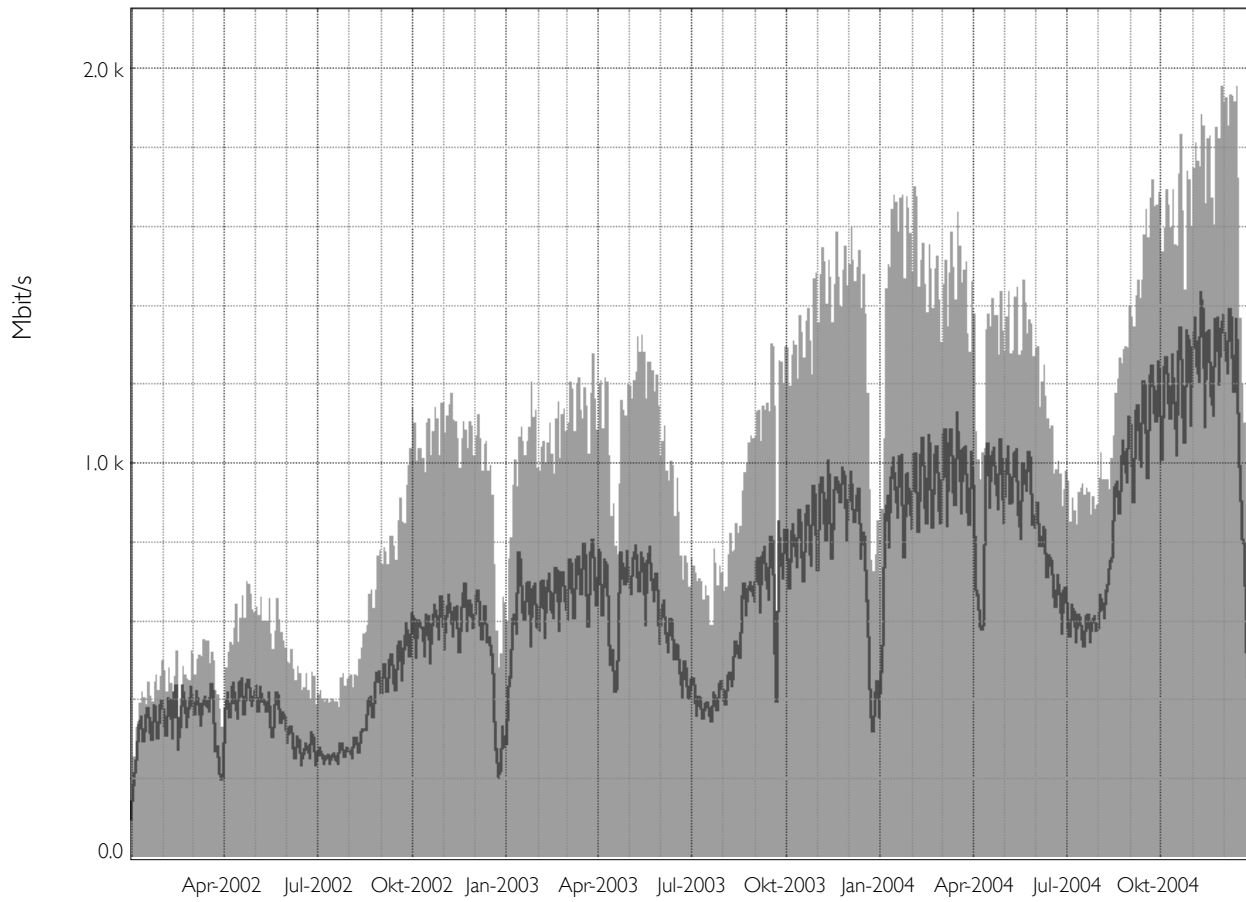
Når man har tilgang til nett fra alle steder, vil mulighetene for fjerninstrumentering øke betraktelig. Pålitelig høykapasitetsnett vil utvide omfanget av anvendt telemedisin. Med nytt høykapasitet-

nett til Svalbard har UNINETT åpnet helt nye muligheter for arktisk forskning. Blant annet har romforskning med sine **VLBI**-antennene i Ny-Ålesund ekstreme overføringsbehov.

## 2.3 MOORE'S LOV

Moore's lov av 1965 anslår en eksponensiell vekstrate for den teknologiske utviklingen, forklart ut fra prosessorteknologi. Loven har vist seg å slå til og den har gitt en analog trend hva angår vekst i Internett-trafikk. Trafikken i forskningsnettet har doblet seg hvert år de siste 10 årene. Den senere tids trafikkvekst er ikke like dramatisk, men det er ingen tegn til markant utflating. Figur 1 på neste side illustrerer veksten.

De statistiske dataene gir oss prognoser om fortsatt betydelig vekst. Dette i seg selv underbygger behovet for kontinuerlig opprusting av det nasjonale forskningsnettet og de tilknyttede campusnett.



Figur 1: Samlet trafikkrate UNINETT hadde mot sine kunder i perioden januar 2002 – desember 2004.

## 2.4 EUROPEISK SATSING

GigaCampus-programmet er helt i tråd med med EUs satsing:

- EU vil gjennom GÉANT2-prosjektet investere omlag 200 millioner Euro over fire år for å bygge et 10-40 Gbit/s stamnett med mulighet for dedikerte lambdanett i tillegg. Nettet vil binde sammen 3900 universiteter i 43 land. GÉANT2 har prosjekter verden over og jobber for en global e-infrastruktur, en gigantisk arena for alle verdens studenter og forskere.
- EU konkluderer gjennom SERENATE-rapporten fra desember 2003 at forskningsnettene er viktige, nasjonale goder:

### *Research networks are a national asset*

«National governments should be aware that research and education networking in their country, and in particular their National Research and Education Network organisation (NREN), is an asset for economic growth and prosperity. It is a source of innovation and provides fast and widespread technology transfer to society and industry. Promoting such technology transfer should be an explicit goal of NRENs. NRENs and industry should ensure that collaboration between research teams in industry and teams in universities and publicly funded research centres can be supported effectively.»

- EUs SERENATE-rapport påpeker videre at svakeste ledd i nettverksskjeden er campusnettverkene. Dette er også tilfelle i Norge og det er nettopp her GigaCampus har fått sitt mandat:

### *The campus is often the weakest link in the network chain*

«In Europe, campus networks are now often the weakest link in the chain of the end-to-end services needed for research and education.

Therefore, universities and research institutes and their supervisory and funding authorities need to ensure that their campus networks are appropriately resourced. In general, expenditure for ongoing technical upgrade in campus networks is best treated as a budget expense on an annual basis.»

## 2.5 ETABLERT SAMARBEIDSKULTUR

UNINETT-konsernet har lang tradisjon for å invite-re til samarbeid i sektoren. Det ligger i UNINETTs mandat å påta seg nasjonale koordineringsroller på vegne av Kunnskapsdepartementet. UNINETT AS driver og videreutvikler det nasjonale forsknings-nettet. UNINETT FAS sørger for felles innføring av administrative systemer, UNINETT Sigma koordinerer nasjonal tungregning, UNINETT ABC gir IKT-veiledning til skolesektoren og UNINETT Norid er den nasjonale instansen som nøytralt forvalter det nasjonale topp-domenet no. UNINETT koordinerer også FEIDE som skal sørge for felles elektronisk identitet for alle landets studenter og forskere.

Mest relevant for GigaCampus, er UNINETTs etablerte samarbeidsarenaer innen nettverks-området. Vi peker her på to sentrale fora:

- UNINETTs nasjonale forskningsnett har siden oppstarten vært drevet i tett samarbeid med universitetene. Universitetene har en regional driftsoppgave, ettersom de huser sentrale UNINETT-rutere og er vår forlengede arm med lokale driftsoppgaver. De inngår som en strategisk partner i et felles nettfaglig kompetanseforum, organisert gjennom UNINETTs nasjonale nettmøte, der videreutvikling av forskningsnettet diskuteres.
- **KOMPAKT**-satsingen startet i 1994 i forbindelse med omorganiseringen av høgskolesektoren. Den er senere utvidet til også å omfatte de seks vitenskapelige høgskolene og de to kunsthøgskolene, i alt 34 høgskoler på rundt 130 studiesteder. Hensikten var å få etablert en standardisert telefoni- og



nettinfrastruktur med god kommunikasjon mellom de ulike studiestedene. Prosjektet har satt i drift rasjonelle løsninger som har gitt store besparelser for sektoren. KOMPAKT har også mye av æren for en konstruktiv og faglig god samarbeidskultur. KOMPAKT-prosjektet ble avsluttet i 2003.

I GigaCampus vil vi bygge videre på den godt etablerte samarbeidskulturen. Vi vil i en samlet satsing forene de gode kreftene fra både universiteter og høyskoler om et felles løft for landets campusnett.

## 2.6 ØKONOMISKE BESPARELSER

Slik **KOMPAKT**-prosjektet kan dokumentere, ligger det en signifikant økonomisk begrunnelse for å samordne utbyggingen av den nettverksmessige infrastrukturen ved landets universiteter og høyskoler. GigaCampus er en utvidet satsing, både i nedslagsfelt og fagområder, noe som vil gi enda større besparelser. Noen sentrale virkemidler vil være:

- Felles innkjøpsavtaler for nettverkselektronikk og telefoni
- Felles kompetansebygging om forente teknologi-plattformen
- Utveksling av egenutviklede verktøy og løsninger
- Implementasjon av gode, langsiktige løsninger basert på høy kompetanse og årelang kollektiv erfaring
- Implementasjons- og driftsstøtte organisert innen sektoren, fremfor bruk av kostbare konsulent-honorar
- Samordnet reservedelslager, koordinert drifts- og beredskapsapparat

Tilsammen skal GigaCampus tilrettelegge for standardiserte løsninger. Lik markedstilgang for leverandører er en viktig premisse. Gjennom godt samarbeid og rasjonell kompetansefordeling vil GigaCampus ta ut betydelige gevinster.

Det er viktig å poengtere at GigaCampus ikke vil virke hemmende på ønsket konkurranse mellom

de ulike universitetene og høyskolene. Konkurransen om studenter og forskningsmidler foregår på faglig plan, ikke på grunnleggende infrastruktur. Den nettverksmessige infrastrukturen GigaCampus foreslår, inngår i det felles fundament alle landets læresteder må stå på. Dette er et nasjonalt anliggende, ikke et lokalt konkurranseelement.



# VISION



## VISJON

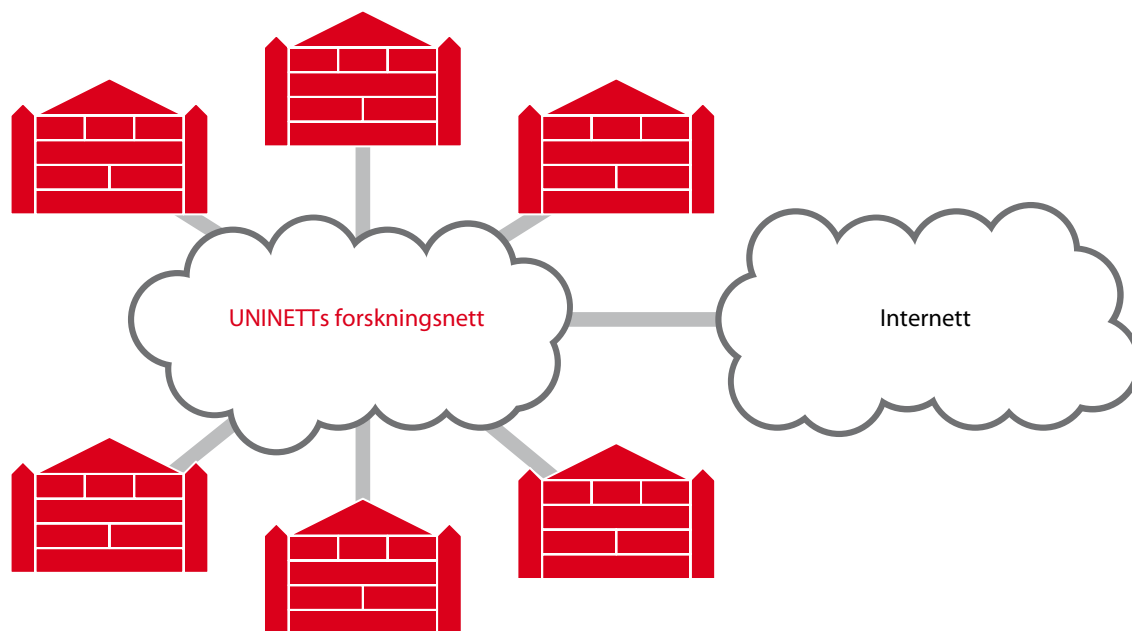
Vår visjon er en koordinert IKT-infrastruktur på campus i internasjonal toppklasse, som inviterer til innovasjon, samarbeid og effektiv forskning og utdanning.

Vi fokuserer på campus og tar initiativ til et omfattende, kapasitetsmessig løft ved landets universitets- og høyskolenett. Hver enkelt arbeidsplass skal innen programperiodens utløp tilbys gigabitkapasitet. Dette vil stille fundamentale krav til de respektive campusnett og til UNINETTs nasjonale transportnett. Oppgradering av UNINETTs nasjonale transportnett er utenfor GigaCampus sitt fokusområde, men må gjennomføres i tett samarbeid med GigaCampus-initiativet. Den totale infrastrukturen må til enhver tid være riktig avstemt, fornuftig skalert og dimensjonert.

GigaCampus skal også sørge for godt utbygde, fleksible og sikre trådløse nett. En operativ SIP-infrastruktur skal tilby gode IP-baserte løsninger for person til person-kommunikasjon (tale og video).

Campusnettene og UNINETTs forskningsnett utgjør en virksomhetskritisk infrastruktur. Stadig flere produksjonskritiske tjenester blir nettverksbaserte. GigaCampus tar til orde for et forsterket fokus på pålitelighet, sikkerhet, kvalitet og profesjonell drift.

GigaCampus skal være resultatorientert og kosteffektiv, ved både å være en pådriver for gode nasjonale tiltak og sørge for gjenbruk av verktøy og løsninger. GigaCampus vil gjennom et kollektivt kompetanseløft tilby opplæring, implementasjons- og driftsstøtte.



Figur 2: UNINETTs forskningsnett og campusnettene må sees i sammenheng.

UNINETT fagstyrke vil utgjøre en viktig del av Giga-Campus. Fagstyrken skal bestå av aktive arbeidsgrupper med bred deltagelse fra universiteter, høyskoler og UNINETT selv. UNINETT fagstyrke vil jobbe med våre felles faglige utfordringer, både i et kort- og lang-siktig perspektiv. Tuftet på sektorens beste praksis vil konkrete anbefalinger og veiledninger bli utarbeidet. Disse vil være viktige redskap i det standardiseringsarbeidet GigaCampus skal ha ansvar for. Med internasjonal kontaktflate, og som brobygger mellom operative miljø og FoU, vil UNINETT fagstyrke bane vei for de beste løsninger.

**GIGACAMPUS – SAMORDNET NETTBYGGING PÅ NORSKE UNIVERSITETER OG HØGSKOLER.**





# HOVEDMÅL

## HOVEDMÅL

I 2009 skal:

- norsk UH-sektor ha et høykvalitets og feiltolerant datanett med gigabitkapasitet til de fleste arbeidsplasser. Særlige brukergrupper skal tilbys høyere kapasitet.
  - landets studenter, forskere og øvrige ansatte sømløst kunne bevege seg på campus med trådløs nettilgang fra PC-er og håndholdte enheter som PDA-er og dets like. Integrasjon med trådløse bynett skal være adressert der det er relevant.
  - IP-basert person til person-kommunikasjon være tilgjengeliggjort. Det skal være enkelt å etablere sanntids tale- og videosamtaler over nett.
  - UH-sektorens sikkerhetsarbeid være godt koordinert. Lokale sikkerhetsteam (IRT, Incident Response Teams) skal være etablert og felles rammeverk for sikkerhetspolicy tatt i bruk.
  - proaktiv drift ha et sterkere fokus. Felles standarder og anbefalinger skal være implementert og verktøy og løsninger skal være bredt anvendt i sektoren.
  - gode virkemidler fange opp og utbedre kvalitetsmessig forringelse av tjenester. Vi skal ha et særlig fokus på å ivareta sanntidskrav.
  - et bredt anlagt og omfattende kompetanseløft være gjennomført. Sektorens samarbeidsvilje og -evne skal stå sterkt. Kostnadseffektive drifts- og utviklingsmodeller skal fungere og et formålstjenlig innkjøpssamarbeid skal være på plass.
- GigaCampus setter seg også organisatoriske og økonomiske mål. Disse er naturlige premissgivere for vår suksess:
- **Organisatoriske mål**  
GigaCampus skal skape grobunn for et tettere IKT-samarbeid i UH-sektoren og på denne måten sørge for bedre nasjonal utnyttelse av eksisterende kompetanse. GigaCampus skal i sterkere grad tilgjengeliggjøre UNINETTs og universitetenes spisskompetanse for sektoren. Dette skal skje blant annet gjennom konkrete prosjektaktiviteter og faglige seminarer. GigaCampus skal sikre et permanent distribuert samarbeid mellom UNINETT og UH-institusjonene.
  - **Økonomiske mål**  
GigaCampus kan begrunnes ut fra et betydelig økonomisk rasjonale. Målsettingen er at vår innsats skal være fire til fem ganger så lønnsom sammenlignet med markedets konsulentløsninger.





# SATSINGSOMRÅDER

## SATSINGSOMRÅDER

GigaCampus er inndelt i sju satsingsområder::

1. Fysisk infrastruktur
2. Høykapasitetsnett
3. Mobilitet
4. Person til person-kommunikasjon
5. Sikkerhet
6. Drift og overvåking
7. Ende til ende-kvalitet

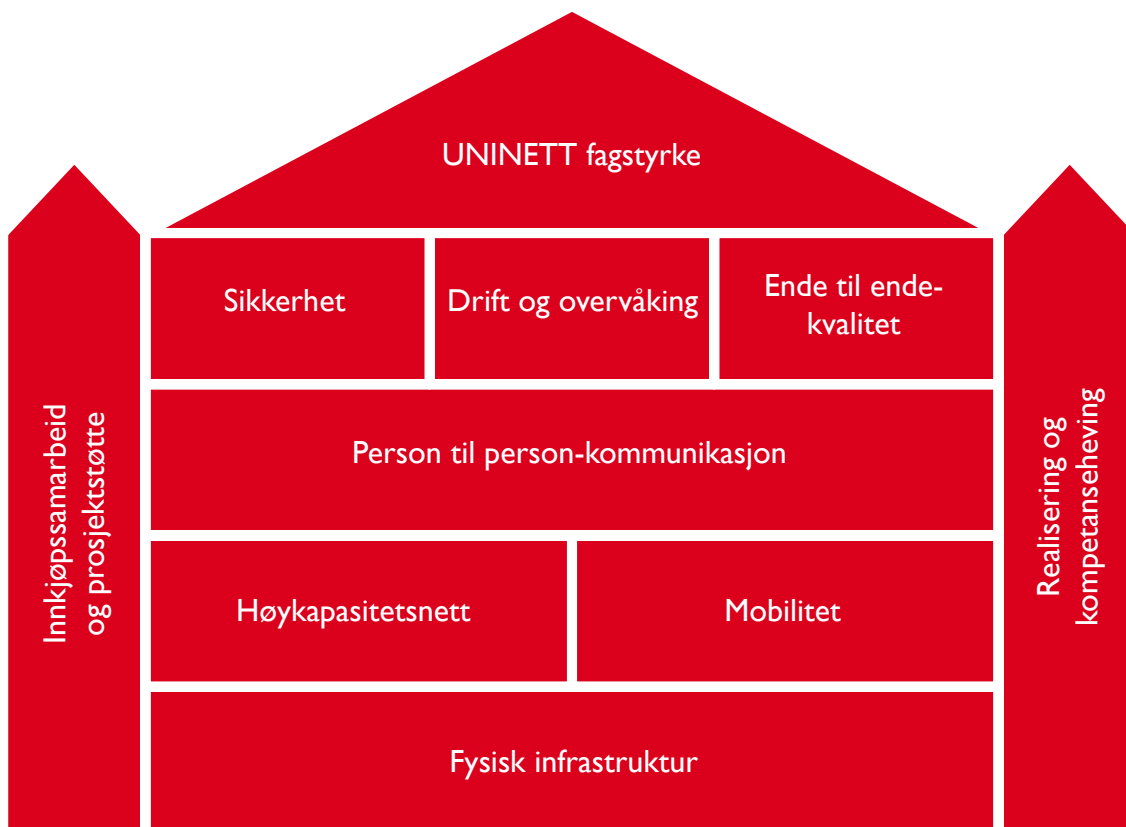
GigaCampus er et dynamisk program og nye områder kan komme til underveis i programperioden.

På tvers av alle satsingsområdene vil GigaCampus sørge for hensiktsmessig samordning av både kompetanse og felles løsninger for sektoren gjennom fem sentrale prosesser:

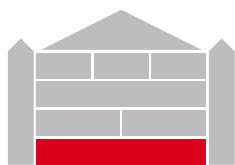
- a) UNINETT fagstyrke – bredt sammensatte arbeidsgrupper som arbeider for utarbeidelse av standardiserte løsninger i sektoren (6.1).
- b) Innkjøpssamarbeid, herunder felles innkjøpsavtaler (6.2)
- c) Prosjektstøtte for felles verktøy og løsninger (6.3)
- d) Realisering av implementasjons- og driftsstøtte, utrulling av tjenester og løsninger (6.4)
- e) Kompetanseheving (6.5)

Figur 3 viser GigaCampus-programmets referansemodell. Her inngår de syv satsingsområdene og de fem sentrale prosessene.

Vi beskriver i dette kapitlet hvert satsingsområde med referanse til dagens situasjon og peker på de utfordringer og målsettinger vi har for programperioden. I neste kapittel omtales prosessene.



Figur 3 viser GigaCampus-programmets referansemodell. Her inngår de syv satsingsområdene og de fem sentrale prosessene.



## 5.1 FYSISK INFRASTRUKTUR

Området fysisk infrastruktur omfatter **strukturert sprednett**, fiberstruktur og bygningsmessige forhold relatert til telematikkrom på campus, herunder strøm og kjøling. Fiberanlegg i bysentra omfattes også.

Erfaringsfall viser at nedetid i altfor mange tilfeller skyldes problemer relatert til fysiske forhold som strømstans, svikt i kjøling eller graveskade med dertil kabelbrudd. Dårlig utført installasjonsarbeid introduserer sporadiske eller permanente feil i transmisjonsnett.

### STATUS

Alle universitetene har siden tidlig 90-tall jobbet planmessig med overgang fra koaksialkabling til **strukturert kabling**. Tilsvarende prosess har pågått i høgskolesektoren i regi av **KOMPAKT**. I tillegg er mange byggeprosjekter gjennomført, der universitetene/KOMPAKT har hatt det faglige ansvaret for oppfølging av strukturert kabling. Det er også gjennomført en rekke fiberprosjekter i de større byene, der samarbeid mellom UNINETT og universitetene/høgskolene og andre aktører har gitt kosteffektive løsninger. For konkrete eksempler, se vedlegg A.

Universitetene, høgskolene og UNINETT sitter på en betydelig erfaringsbakgrunn. Vi ser en rekke områder der den fysiske infrastrukturen må forsterkes ytterligere. Dette omfatter alt fra utskifting av førstegenerasjons kabling<sup>1</sup> til styrking av bygningsmessige forhold. I programperioden settes stadig høyere krav til ytelse med gigabit- og 10 gigabitkapasitet, og dessuten strengere krav til oppetid.

<sup>1</sup> Typisk strukturert sprednett av kategori 3-typen standard. Maksimal hastighet for slik kabling er 10 Mbit/s.

<sup>2</sup> Det er to hovedtyper fiberkabel; multimodus (MM) og singlemodus (SM). MM-kabel opererer på bølgelengdene 850 nm og 1300 nm, mens SM-kabel opererer på bølgelengdene 1310 nm og 1550 nm. SM-kabel har lengre rekkevidde (pga. lavere signaldemping) og har derfor vært den mest hensiktsmessige kabeltypen utendørs. Med 10 Gbit/s hastigheter er rekkevidden til MM-kabel svært kort og SM-kabel bør derfor benyttes innendørs også.

## UTFORDRINGER

Vi ønsker i programperioden å gjennomgå alle installasjoner og peke på svakheter og nødvendige forbedringer. Dette er et omfattende arbeid der vi går i detalj innen hvert delområde. En rekke krav skal møtes, og en detaljert kravspesifikasjon vil bli brukt som underlag. Foruten fysiske krav, settes krav til dokumentasjon og generell ryddighet. Overordnet ser vi følgende utfordringer:

- **Strukturert sprednett:** All **horisontal kabling** må minimum tilfredsstillende kravene til kategori 5 (5e for ny kabling), som tillater datarater opptil 1 Gbit/s. Multimodusfiber på høye hastigheter over lang avstand er et problem<sup>2</sup>. Det må gradvis gjennomføres en migrering til singlemodusfiber, og all ny kabling skal baseres på dette. Ved innføring av 10 Gbit/s-hastigheter settes det svært strenge krav til terminering. Vi må anta at reterminering av et stort antall fiberkabler blir nødvendig.
- **Strøm:** Vi må se på utlegg av kurser; bruk av **UPS** og dieselaggregat. Særlig viktig er hensiktsmessig disponering av strømkilder, samt gode rutiner relatert til vedlikehold av **UPS** og aggregat<sup>3</sup>. Dårlig eller manglende jording kan medføre problemer vedrørende personsikkerhet, **EMC** og/eller overspenninger som igjen medfører nettutfall. Tradisjonelt blir jording viet liten oppmerksomhet, og dette er noe vi vil rette på i programperioden.
- **Ventilasjon/kjøling:** Det er svært viktig at datarom er utrustet med tilstrekkelig kjøling, og at det også er redundant. Dette betyr at ved svikt i et kjølesystem, skal resterende kjølesystem ha tilstrekkelig kapasitet.

<sup>3</sup> Et klassisk problem er at for mye utstyr blir hengt på samme kurs pga. gradvise utvidelser. I normal drift går dette bra, men etter en strømstans der alt utstyret startes samtidig blir kursen overbelastet og sikring løses ut, med dertil forlenget nedetid. Tilsvarende kan en manglende vedlikeholdt UPS ha flate batterier når du endelig trenger den, eller dieselaggregatet slår ikke inn som det skal.

- Branneteksjon/slukking: Alle data-/telematikkrom skal være utrustet med detektorer for branneteksjon og tilkoblet automatisk brannvarslingsentral som igjen er tilknyttet lokalt brannvesen. I forbindelse med viktige datarom bør man vurderes å installere **aspirasjonsdetektorer**.

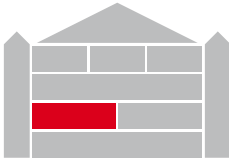
Videre bør viktige datarom utrustes med brannslukningsanlegg. Generelt skal alle retningslinjer/pålegg gitt av sentral og lokal brannmyndighet følges.

- Bygningsmessige forhold må gjennomgås: Mange institusjoner preges av manglende planlegging ved etablering av datainstallasjoner. Dette medfører lite hensiktsmessige rom som igjen kan medføre manglende ryddighet og redusert oppetid. GigaCampus vil utarbeide generelle krav til data-/telematikkrom.
- Fysisk sikring: Alle data-/kommunikasjonsrom må sikres slik at kun autorisert personell har tilgang. Sabotasje eller guttestreker kan i verste fall medføre utfall av sentrale datakomponenter, som igjen kan medføre manglende produksjon eller undervisning. Alle data-/telematikkrom må ha tilstrekkelig skallsikring, herunder være utrustet med blant annet adgangskontroll og videoovervåking.
- Overvåking: Proaktiv drift krever overvåking av ulike typer miljøalarmer. Med miljøalarmer menes blant annet temperatur, ventilasjon, strøm, vanninntrenging, brann og adgang. I utgangspunktet er det ønskelig å hente alle miljøalarmer fra institusjonens sentrale driftskontroll (SD)-anlegg. Erfaring tilsier at svært få institusjoner har **SD-anlegg** med tilstrekkelig funksjonalitet. Inntil slike blir etablert, er det ønskelig å installere miljøovervåkingssensorer med **SNMP**-støtte. Disse kan da overvåkes av institusjonens generelle nettadministrasjonssystem, gjerne **NAV**. Les mer om dette i kapittel 5.6.

- Fiberanlegg: I de senere år finnes det mange eksempler på at samarbeid mellom offentlige og private fiberutbyggere har gitt topp moderne fiberanlegg til en svært lav pris, sammenlignet med om de ulike aktørene skulle ha etablert egne separate anlegg. I årene som kommer ønsker GigaCampus å være en pådriver til at slike felles fiberprosjekter blir etablert der dette er nødvendig og forholdene ellers ligger til rette for samarbeid.

## DELMÅL

- I løpet av 2006 skal felles kravspesifikasjoner for fysisk infrastruktur utarbeides. Institusjonsvise befaringer skal initieres med 20 besøk i 2006 og 20 besøk i 2007. Alle avvik fra vedtatte krav og standarder skal rapporteres til de aktuelle institusjonene for lokal utbedring.
- Innen 2009 skal alle installasjoner være befart. Innen utgangen av året skal alle installasjoner være i tråd med de vedtatte standarder for fysisk infrastruktur.
- Innen 2009 skal viktige fiberprosjekter i de større byene ha gitt sektoren kostnadseffektiv tilgang på mørk fiber. Dette muliggjør høykapasitetsforbindelser mellom campus innenfor bysentra. Tilsvarende gir det gunstig aksesskostnad mot lokalt termineringssted av UNINETT's nasjonale forskningsnett. Det legger også til rette for implementasjon av **lambdanett**, der dette er formålstjenlig.



## 5.2 HØYKAPASITETSNETT

Satsingsområdet nett omhandler selve nettverksinfrastrukturen på campus. Kapasitet og funksjonalitet må kontinuerlig tilpasses lokale behov, men må også sees i sammenheng med UNINETT's nasjonale forskningsnett. På denne måten kan behovet for reelle høykvalitets maskin til maskin-forbindelser realiseres, både nasjonalt og internasjonalt.

Campusnettet består i essens av en sammenkobling av rutere og svitsjer<sup>4</sup>. Vi deler svitsjer inn i tre kategorier: **kjernesvitsjer**, **distribusjonssvitsjer** og **kant-svitsjer**<sup>5</sup>. Figur 4 viser et typisk design, slik det er i dag. Kjernesvitsj og rutere er typisk sammensmeltet i en enhet som håndterer både lag-2 og lag-3.

### STATUS

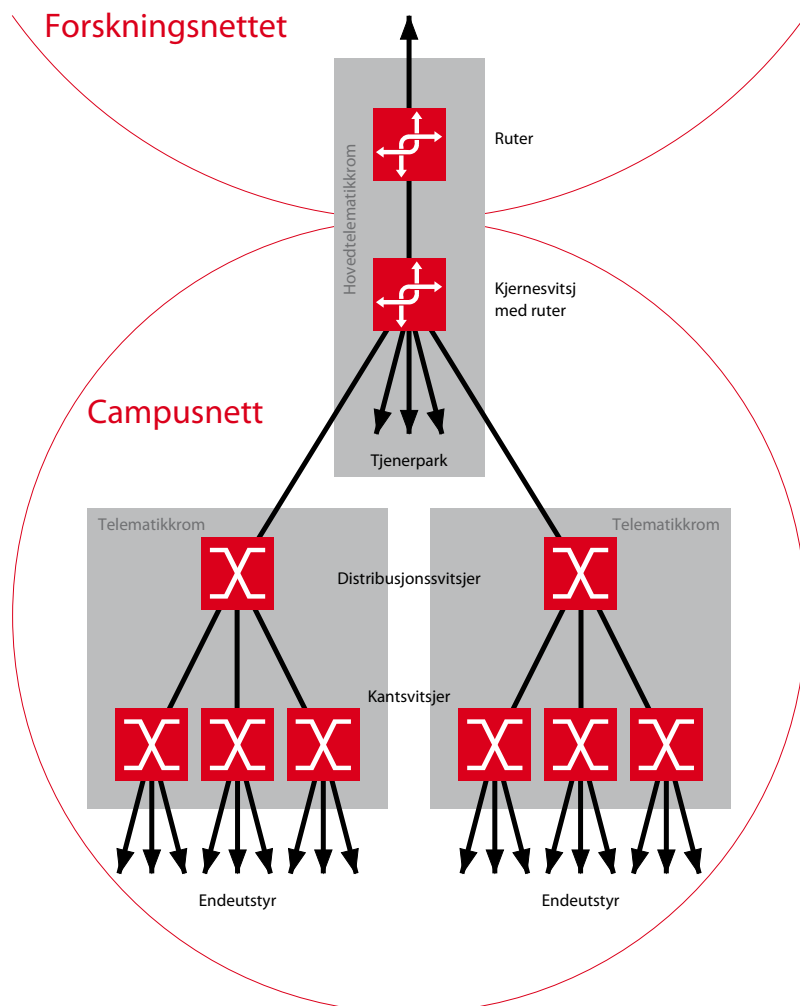
Det investeres kontinuerlig i campusnettene og som **SERENATE**-rapporten også påpeker, gjøres opprusting av campusnettene best gjennom faste, årlige budsjettposter (jfr. kp. 2.4). Utstyr må jevnt og trutt skiftes ut og kortsiktige investeringer bør unngås. Typisk levetid for kjerneutstyr er 3-4 år, for kantutstyr rundt 5-6 år.

En trend er innfasing av kjernesvitsjer som håndterer både lag-2 og 3. Alle universiteter og flere og flere høyskoler benytter dette. En slik løsning gjør at lokalnettruting kan gjøres lokalt og ikke via tilstedeværende UNINETT-rutere, noe som gir et mer effektivt trafikkmønster, samt et ryddigere administrativt skille. Det stiller samtidig nye krav til høyskolens IKT-personell i forhold til mer kompleks nettmessig drift, herunder rutingoppsett og vedlikehold av pakkefiltre.

## UTFORDRINGER

Vi står overfor mange utfordringer i programperioden. Dette er de mest sentrale utfordringene:

- **Kapasitet:** Vi må gradvis oppgradere til 1 Gbit/s støtte for de aller fleste klientmaskiner i nettverket, og spesielle behov kan kreve enda høyere kapasitet. Dette stiller formidable krav til kjernenettet og det nasjonale forskningsnettet. Nytt kjerneutstyr må ha støtte for 10 Gbit/s og etterhvert høyere datarater. For de større universitetene vil 10 gigabitaksess



Figur 4: Typisk campusnettdesign anno 2005.

<sup>4</sup> Rutere og svitsjer danner veikryss i nettet. Rutere er mest intelligente, ettersom de er i stand til å rute trafikk basert på IP-adresser (lag-3 i OSI-modellen). Svitsjer befinner seg på lokalnettet (de opererer på lag-2 i OSI-modellen) og har til hensikt å skille trafikk fra hverandre, slik at en stor total kapasitet kan tillates.

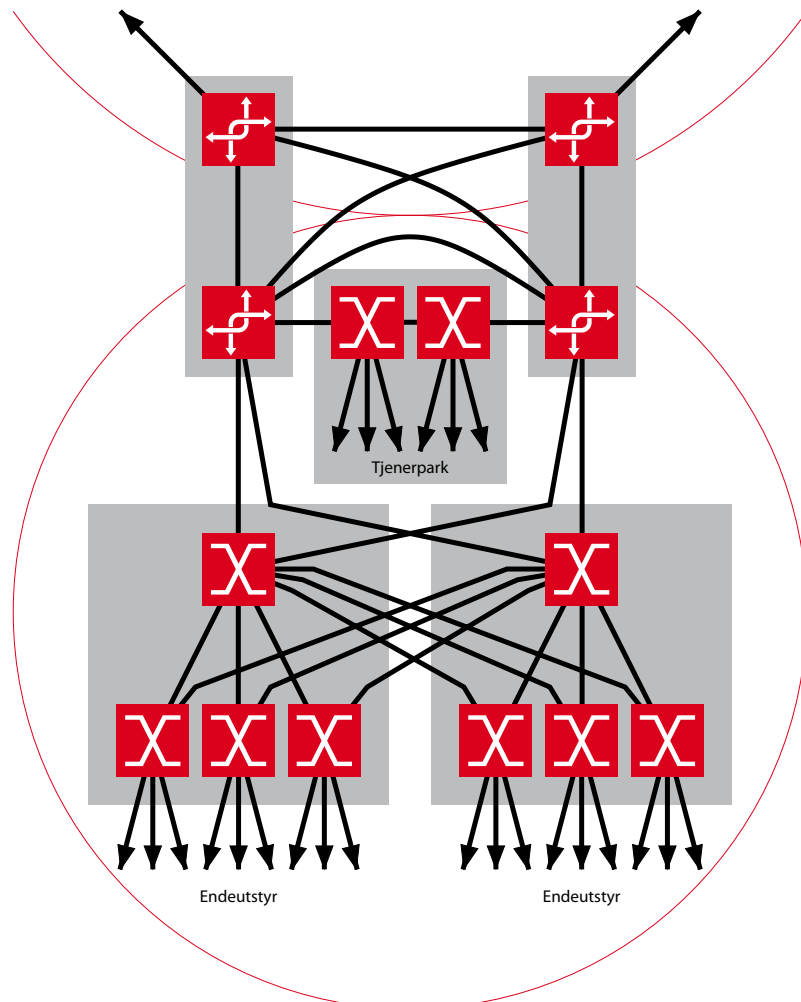
<sup>5</sup> For mindre steder brukes ikke distribusjonssvitsjer.

mot UNINETT være aktuelt. Dette gir betydelige kostnadmessige ringvirkninger.<sup>6</sup>

- **Tjenestekvalitet:** Det er ikke nok å oppgradere nettverket i gigabitrate. Vi må fokusere på opplevd kapasitet fra maskin til maskin. Sentraliserte fil-, skriver- og sikkerhetskopi-løsninger aktualiserer problemstillingen. **Jumboframes**-støtte i alle relevante ledd blir viktig, samt gode mekanismer for bufring og prioritering. Fornuftig konfigurasjon av TCP-parametre i endemaskinene er også svært viktig. Feil innstilling kan redusere ytelsen betraktelig når rundreisetidene er høye.
- **Tilgjengelighet:** Avhengigheten til den datamesige infrastrukturen blir bare større og større. Ikke-planlagte driftstanser må reduseres til et minimum. Sunn, proaktiv drift med gode rutiner og verktøy er viktig, og dette er et eget satsingsområde, se kapittel 5.6. Det er også viktig å bygge inn feiltoleranse i infrastrukturen. Det blir en kost-nytte vurdering hvor langt man skal gå, men viktige stikkord er:
  - o redundant strømforsyning
  - o redundant lag-2 struktur med lav konvergenstid (**RSTP** e.l.)
  - o redundant aksessruter med **VRRP/HSRP**
  - o redundant lag-3 design på/mellom campus med **OSFP/IS-IS**
  - o redundant UNINETT-aksess med **BGP**
  - o fysisk adskilte hovedtelematikkrom i hver sin ende av campus
  - o fysisk adskilte aksessfiber/fiberføringsveier
  - o redundant tjenesteløsning, f.eks. basert på **anycast**
- **Lambdanett/ekstrembehov:** Vi vil i programperioden se nye bruksområder som har ekstreme kapasitetsbehov. En god fiberinfrastruktur muliggjør innføring av bølglengdemultipleksere. Da

kan vi utnytte ulike kanaler (bølglengder) i fiberkabelen til ulike formål. Det ordinære nettet kan gå på en kanal, mens spesialnett, såkalte lambdanett kan benytte andre kanaler. De utskilte brukergruppene får sine behov dekket, samtidig som det ordinære nettet blir avlastet.

- **Multicast** Vi forventer en markant vekst i kringkasting av forelesninger og konferanser. Det fordrer at multicast virker i alle deler av nettet. Multicast har også andre bruksområder, som f.eks. spredning av programvare. Det er viktig å forene behovene



Figur 5 skisserer et fullredundant campusnettdesign.

<sup>6</sup> Med 1 Gbit/s kapasitet for endeutstyr kan 10 Gbit/s aksess mot UNINETT virke lavt, rent intuitivt. Vi må her bemerke at en stor andel av trafikken holdes lokalt, mot lokale tjenester. Erfaringstall tilsier at vårt forslag gir en fornuftig skalering. Vi må likevel følge trafikktviklingen nøye og oppgradere ytterligere ved behov.

for lokale så vel som globale multicast-behov. Giga-Campus vil jobbe for fullgod multicast-støtte i alle campusnett. Dette inkluderer også støtte for nye multicast-arkitekturer, som **SSM** og IPv6 multicast.

- **IPv6**: Neste generasjons Internett-protokoll heter IPv6. Den vil løse flere problemer med dagens IPv4, der den viktigste er den globale knappheten på IP-adresser, som igjen har gitt suboptimale designløsninger basert på **NAT**. Vi må forfekte ekte ende til ende-design<sup>7</sup>, og det er mange argumenter for dette.

I norsk UH-sektor er knapphet av IP-adresser foreløpig ikke akutt, men vi nærmer oss. Forventet vekst av teknologiløsninger som blant annet **PDA**-er, telefoner, instrumenter og sensorer som trenger IP-adresser vil inntreffe i programperioden. Vi vil også se flere tjenester som støtter, og kanskje bare støtter IPv6.

Godt utbygde trådløse nett med innføring av **SIP**-baserte mobiltelefoner (se 5.3) vil sette nye krav til mobil IP. Mobil IP vil si at man beholder samme IP-adresse, selv om man beveger seg utenfor IP-adressens naturlige tilholdsted (subnett). Å beholde samme adresse er nødvendig for ikke å bryte en pågående sesjon, som f.eks. en telefonsamtale. IPv6 har her en foretrukket og mer skalerbar modell sammenlignet med IPv4<sup>8</sup>.

UNINETT har jobbet med IPv6 siden 1998 og kjører i dag IPv6 i hele forskningsnettene side om side med IPv4 med noen unntak. Flere universiteter har pilotert IPv6, men bruken har enda ikke tatt av.

Vi vil i programperioden jobbe for en fullgod utbygging av IPv6, med de krav og utfordringer dette medfører. Vi må forberede en gradvis overgang, der første steg vil være å gi fullgod dekning.

## DELMÅL

- I 2006 skal institusjonsvise befaringer initieres med det for øye å kvalitetssikre og ev. utbedre design og konfigurasjon av de respektive campusnett. 20 befaringer gjennomføres i 2006 og 20 befaringer i 2007.
- I 2009 skal ende til ende-gigabitkapasitet være en realitet for de aller fleste.
  - o Særlige brukermiljø skal ha høyere kapasitet, gjerne basert på lambda-nett. Pilotering skal være gjennomført.
  - o Vi skal ha 10 gigabitaksess mot de største universitetene.
- I 2009 skal vi med fullgod kvalitet kunne anvende nettverket til sanntidsapplikasjoner som tale og video.
- I 2009 skal feiltoleransen i campusnettene være signifikant styrket.
  - o Det skal være redundans for sentrale komponenter i nettarkitekturen.
  - o Det skal være feiltolerant vei ut av de største studiesteder
- I 2009 skal multicast støttes ende til ende, herunder også **SSM** og IPv6 multicast.
- I 2009 skal alle campusnett tilby IPv6 side om side med IPv4. Plan om fullverdig migrasjon til IPv6 skal foreligge.

<sup>7</sup> Med ende til ende menes at en maskin på Internett kommuniserer direkte med en annen, uten at adresser oversettes underveis. Alle har sin globalt unike adresse. **NAT**-løsninger, samt mange typer brannmurer, forringer ende til ende-forbindelsen, bl.a. med den bieffekt at det kompliserer oppsett av tjenester og gjør sikkerhetsarbeid vanskelig. Vi har sett flere eksempler der utskyldig tredjepart har mistet sin nettaksess, siden den tilfeldigvis deler forbindelsen med en maskin som har begått sikkerhetsbrudd.

<sup>8</sup> IPv4 introduserer konseptet med en hjemmeagent som all trafikk til og fra den mobile IP-adressen må gå innom. Dette gir et suboptimalt trafikkmønster som IPv6 løser mer elegant. Hjemmeagent er også involvert med IPv6, men bare initielt under oppsett av en sesjon. Partene vil i neste instans enes om å kommunisere direkte.



### 5.3 MOBILITET

Satsingsområdet mobilitet fokuserer på trådløse nett. Vårt overordnede mål er å sørge for godt utbygde trådløse nett på alle campus, der krav til ytelse, sikkerhet og pålitelighet er ivaretatt. Trådløse nett gir rom for mobile, fleksible tjenester. Her inngår bruk av bærbare PC-er, PDA-er og andre håndholdte WLAN-enheter. Vi forventer en markant vekst i bruk av WLAN IP-telefoner i programperioden. Stedbaserte tjenester vil også komme, herunder WLAN-baserte RFID-brikker .

Det er viktig å poengtere at det trådløse nettet er et supplement til det regulære fastnettet. Trådløst nett har begrenset kapasitet og kan ikke dekke alle de bruksområdene som fastnettet skal dekke. Til tross for en positiv kapasitetsmessig utvikling, ligger trådløst en størrelsesorden under fastnettet.

#### STATUS

Utbygging av trådløse campusnett har pågått i en årrekke. Alle universiteter og høyskoler har i dag et trådløst tilbud, i større eller mindre grad. De største løsningene finner vi på universitetene. Både UiO og NTNU har 200-300 basestasjoner i drift. Dette gir en god dekning i blant annet vrimeleareal, kantiner, biblioteker og grupperom. En fullverdig dekning er imidlertid langt unna, eksempelvis har NTNU estimert at de da trenger omlag 1800 basestasjoner.

For mindre høyskoler er full dekning lettere å realisere på grunn av den mer beskjedne bygningsmassen. Noen høyskoler rapporterer om bortimot full dekning, mens andre har en lengre vei å gå. Merk at full dekning er et relativt begrep ettersom lav tetthet av basestasjoner kanskje gir trådløst signal de fleste steder, men til lav ytelse.

Når det gjelder bruk, er denne i markant vekst. NTNU har de senere år sett en dobling i trafikkmengden per

år. I 2005 registrerte de hele 7000 unike trådløse enheter. I all hovedsak utgjør bruksmassen bærbare PC-er, og vekstraten kan derfor sees i sammenheng med veksten i bærbare PC-er blant studenter.

Primært støttes IEEE 802.11b i dag, men basestasjoner som støtter alle tre WiFi-standardene (a/b/g) blir mer og mer vanlig. Mens IEEE 802.11b er en 11 Mbit/s-løsning, har de to etterkommerne overlegen kapasitet med 54 Mbit/s.

Når det gjelder sikkerhet er bildet nokså sammensatt. På svært mange høyskoler har man lav eller ingen sikkerhet. Høgskolen i Østfold tok steget når de i 2005 gjennomførte en større utbygging på sitt nybygg i Halden. De har implementert sin sikkerhetsløsning basert på IEEE 802.1X-standard. UiO har også gjort dette, mens NTNU, UiT og UiB baserer seg på VPN-løsninger, NTNU i en kombinasjon med web-portal.

UNINETT har lenge hatt en drivende rolle innen trådløst med koordinert aktivitet mot TERENA og IETF. Foruten teknologien som sådan, har vi fokusert på sikkerhet og sømløshet (roaming). Vi deltar også i det europeiske eduroam-initiativet, som har til hensikt å gi gjensidig trådløs nettilgang til studenter og forskere på alle tilknyttede studiesteder i Europa. Vi er også involvert i GÉANT2-prosjektet JRA5 som jobber med neste generasjon eduroam, kalt eduGAIN. eduGAIN tilbyr en sterkere integrasjon mot etablerte AA-infrastrukturer som FEIDE og Shibboleth.

UNINETT bistår som teknisk rådgiver i NTNUs prosjekt «Trådløse Trondheim» som startet våren 2005. «Trådløse Trondheim» har tegnet intensjonsavtale med Trondheim kommune, Næringsforeningen i Trondheim og Sør-Trøndelag fylkeskommune og flere bedrifter er aktivt med i prosjektet. Første fase skal ferdigstilles i 2006 basert på WiFi-standard. Alle NTNUs campus, samt traseér imellom skal dekkes, i tillegg til store deler av Trondheim sentrum. Fase

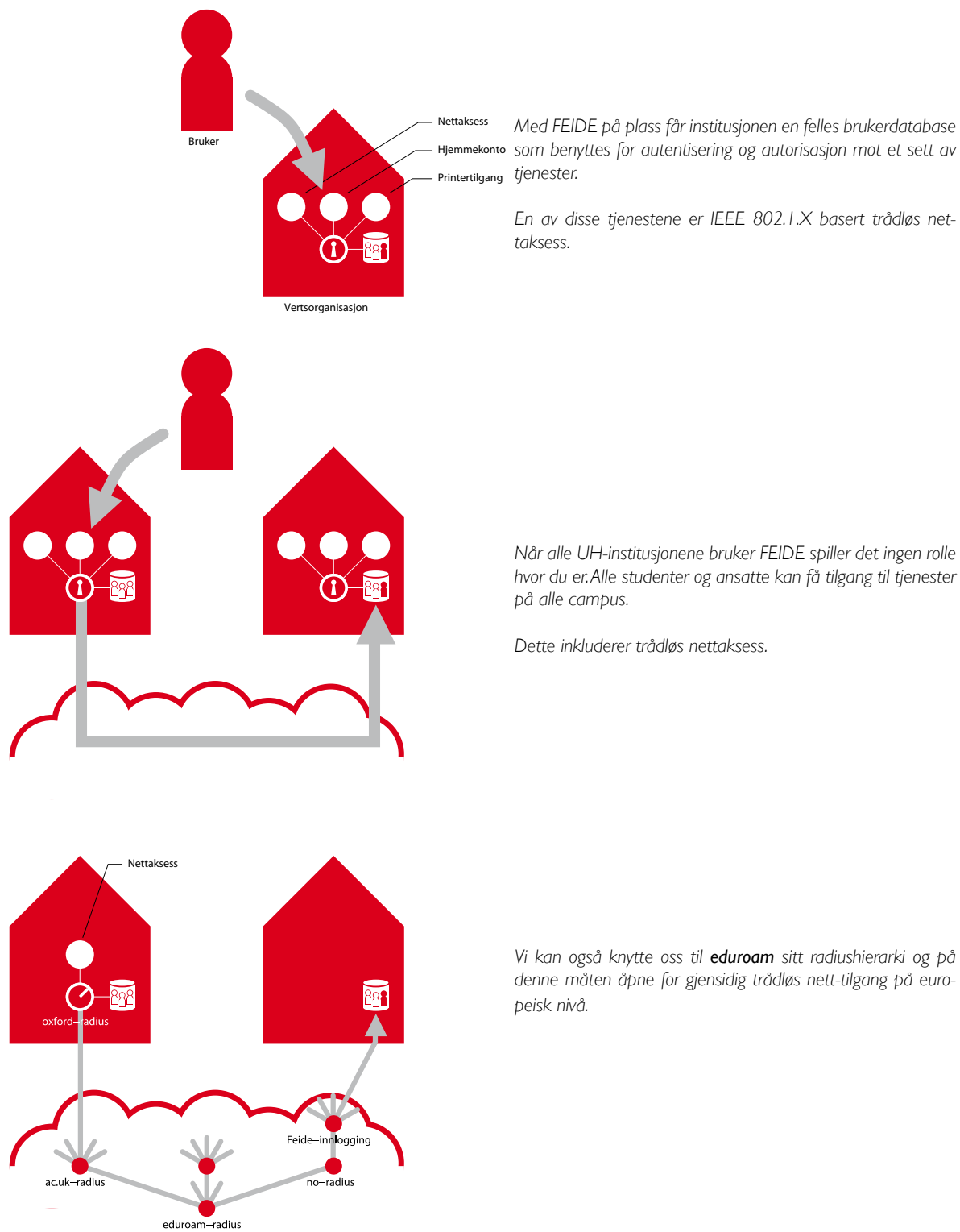


2 skal dekke hele Trondheim basert på WiMax eller nyere teknologi. «Trådløse Trondheim» har som mål å skape et utviklingslaboratorium i verdensklasse. Utforskning av nye bruksområder står sentralt, og likeså forretningsmodeller for storskala bynettdrift.

## UTFORDRINGER

Trådløsområdet er utvilsomt i en rivende utvikling. GigaCampus ønsker å bidra aktivt i den videre utbyggingen av trådløse nett ved landets studiesteder. Vi skal ligge i forkant og teste ut ny teknologi, samtidig som vi skal medvirke til gode, pålitelige og ikke minst sikre produksjonsløsninger.

Det er i dag vedtatt enighet om at IEEE 802.1X er fremtidens løsning for aksess- og innholdssikring. Standarden er nå moden for storskala bruk. Den innfører imidlertid økt kompleksitet, både på nett- og klientsiden. De største utfordringene kan relateres til sertifikathåndtering og klientkonfigurasjon, særlig under Windows XP. Løsningen fordrer også et brukeradministrativt system i bakkant. Separat brukerdatabase for trådløst bør unngås, og med FEIDE på plass blir dette en naturlig kilde. I tillegg trengs løsninger for å gi nettdgang til besøkende. FEIDE kan gi adgang på nasjonal basis, mens eduroam utvider rekkevidden til å gjelde Europa. I begge tilfeller avgrenser vi oss til utdanningssektoren. Et fleksibelt system som kan håndtere andre besøkende, må også komme på plass. UiB og UiO har allerede adressert problemstillingen, og deres løsningsvalg bør ses nærmere på. Figur 6 på neste side illustrerer ulike scenarier for nettaksess.



Figur 6: IEEE 802.1X basert trådløs nettaksess vist i ulike scenarier.

En annen viktig utfordring blir sømløshet. Vi forventer en markant vekst i håndholdte enheter, herunder **WLAN/SIP**-telefoner. Behovet for mobilitet blir da mer reellt enn hva tilfelle er for dagens bærbare PC-er. Ved forflytning innen et område, må sømløshet (roaming) fungere fra basestasjon til basestasjon. **IAPP** er en standard som har til hensikt å løse dette, men da innen et subnett. Ved lengre forflytninger, eller forflytning i grenseland mellom to trådløse subnett, må man i utgangspunktet fornye sin IP-adresse, med dertil tap av pågående sesjoner. Mobil IP er en standard<sup>9</sup> som søker å løse dette problemet, men implementerte løsninger er imidlertid få. En rekke utstyrsleverandører tilbyr ulike proprietære tilnærminger, da med det til felles at de ikke fungerer med basestasjoner fra tredjeparts leverandører. GigaCampus må i programperioden gå dypere inn i problemområdet. Så langt råd er, bør vi tilstrebe åpne løsninger. Som nevnt i kapittel 5.2, så har IPv6 et interessant potensial her.

Et annet viktig aspekt blir sømløshet mellom tradisjonell mobiltelefoni (**GSM/GPRS/UMTS**) og **SIP**-telefoni. Teknologier som adresserer problemstillingen begynner å komme, et initiativ er **UMA**, Unlicensed Mobile Access.

Med IP-telefoni vil krav til opprinnelsesmarkering komme. Stedsbestemmelse blir uansett en viktig tjeneste. Dersom man vet hvor brukeren befinner seg, blir det mulig å sende ut sted- og tidsriktig informasjon (såkalte push-tjenester). Sted danner også basis for bruk av trådløse **RFID**-brikker. Ved å feste slike brikker på ulikt utstyr får man mulighet til å overvåke dets bevegelser. Eksempelvis kan de brukes som tyverialarm.

GigaCampus må se på administrasjonsløsninger som kan angi sted og bruksmønster. Muligens kan egne verktøy utvikles, og da gjerne i integrasjon med **NAV**. Administrasjonsverktøy er et viktig område i seg selv og med mange hundre basestasjoner, er et sentralt

system å foretrekke. Manuell konfigurering og oppgradering av hver enkelt basestasjon blir en uoverkommelig oppgave. Vi trenger også trafikkstatistikk, herunder bruksmønster per basestasjon. Videre ønsker vi å kartlegge radiobildet rundt hver enkelt basestasjon bl.a. for å avdekke uønskede stasjoner/ ad hoc-løsninger.

Nok et viktig område blir radioplanlegging. Sektoren har her opparbeidet mye praktisk erfaring, og denne bør utnyttes. Utfordringene står i kø, det er et puslespill å legge et godt trådløst lappeteppes med støtte på ulike frekvenser. Dette er heller ikke en engangsjobb, det trådløse nettet må kontinuerlig bygges ut etter behov. Selv om utstyrsleverandører lokker med programpakker som gjør dette for deg ser vi ingen vei utenom manuell radioplanlegging. Programsystemer kan avhjelpe, ettersom de hensiktsmessig kan velge kanal og effekt, men overordnet plan må man selv stå for.<sup>10</sup>

På klientsiden må vi studere ulike initiativ, herunder Microsoft sin **WPS**, Wireless Provision Service. Idéen er god, og brukeren skal med WPS enklere kunne konfigurere seg opp mot nye nett og mot ulike IP-soner den møter på sin vei.

<sup>9</sup> Mobil IP er definert i RFC2002 og RFC2977.

<sup>10</sup> Når det gjelder radioplanlegging, er det særlig 2,4 GHz-standardene som volder bry, gitt en praktisk begrensning på tre

basestasjoner i samme område. IEEE 802.11a (og trolig også den kommende IEEE802.11n) tillater langt flere overlappende basestasjoner.



## DELMÅL

- I 2006 skal fokus på **IEEE 802.1X** intensiveres med kurs, workshops og pilottester. Flere trådløse nett skal implementere støtte. Det blir særlig viktig å adressere sertifikat- og klientproblematikk. Det skal legges til rette for **FEIDE** og **eduroam**.
- I 2006 skal det gjennomføres felles workshop i radioplanlegging. Det skal deretter utarbeides retningslinjer for god radioplanlegging.
- I 2006 skal ulike trådløse pakkelsesløsninger vurderes. Stadig flere leverandører satser på lettvekts basestasjoner som styres av sentrale komponenter.
- I 2006 skal verktøystøtten rundt trådløs overvåking og administrasjon styrkes. Egenutvikling skal vurderes opp imot proprietære administrasjonssystemer.
- I 2006 skal mobiltelefoner som støtter **SIP/WLAN** testes ut. Tjenestekvalitet og lag-3 roaming skal adresseres, likeså sømløs roaming mellom **WLAN** og GSM. Arbeidet vil fortsette utover i programperioden, stabile produksjonstjenester kommer tvisomt før 2008.
- I 2008 skal alle trådløse nett bruke **FEIDE** som autentiseringskilde (det fordrer naturligvis at institusjonen har innført FEIDE). De skal også tilby **eduroam**- (ev. **eduGAIN**) aksess for sine tilreisende studenter og forskere.
- I 2009 skal utbygging av trådløse nett ha kommet så langt at alle campus har fullgod dekning. Sikkerhet, tjenestekvalitet, sømløshet og storskala drift skal være godt ivaretatt. Der det er naturlig skal integrasjon med trådløse bynett være adressert.

## 5.4 PERSON TIL PERSON-KOMMUNIKASJON

Satsingsområdet person til person-kommunikasjon har fokus på multimediesamtaler. Dette omfatter i prioritert rekkefølge: telefoni, videokonferanser, lynmeldinger og tilstedemarkering. Området kan også omfatte applikasjoner for delt arbeidsflate, kalenderløsninger, i tillegg til LMS (Learning Management Systems). GigaCampus beveger seg her opp i applikasjonslaget, der vi vil legge til rette for gode løsninger. Vi vil tilstrebe bruk av åpne standarder og her står **SIP** sentralt. Vår ambisjon er å utforme og implementere en skalerbar SIP-arkitektur for sektorens person til person-tjenester. Interoperabilitet med dagens tradisjonelle telefoniløsninger er essensielt i vårt arbeid.

**SIP (Session Initiation Protocol)** er en åpen standard laget for oppsett av multimediesamtaler. Den registrerer og formidler hvor en person er tilgjengelig, og formidler forhandling av protokoller og formater for en samtale. Det er viktig å poengtere at SIP er mer enn telefoni, fokuset er bredere. SIP tar nå mer og mer over for konkurrenten fra televerdenen, ITU-T sin H.323. Der H.323 er monolittisk og kompleks, har SIP en enklere og mer modulær arkitektur. SIP er enklere å ta i bruk, den er mer skalerbar og derfor anvendbar på flere områder

## STATUS

Sektoren har i dag en moderne ISDN-basert telefoniplattform med **PABX**-løsninger fra Alcatel, Ericsson og Nortel. For høgskolene, koordinert med universitetene er det i **KOMPAKT**-regi forhandlet frem gode løsninger for anskaffelse, drift og administrasjon av telefonisystemene. Det er inngått konsernavtaler for alle tre sentraltyper. Det er også fremforhandlet trafikkavtaler for både fasttelefoni og mobil. Totalt 60 000 fasttelefoner og 4 600 mobiltelefoner er omfattet av avtalene. **KOMPAKT**-prosjektet har her oppnådd betydelige besparelser.

GigaCampus vil videreføre det arbeidet **KOMPAKT** har gjort på tradisjonell telefoni. Selv med en gradvis overgang til IP-telefoni, har dagens telefonsentraler og apparater lang levetid. Vi må sørge for fortsatt god drift og vedlikehold. På avtalesiden er det fortsatt besparelser å hente, særlig gjelder dette mobiltelefoni som nå utgjør omlag 70 % av de totale trafikkkostnadene. Mobiltelefoner som støtter **SIP** over **WLAN** har begynt å komme (nevnt i kap 5.3), og dette er en utvikling GigaCampus vil følge nøye med på. En stor andel av mobiltrafikken foregår fra campus, og med godt utbygde trådløse nett kan vi potensielt oppnå store besparelser.

IP-telefoner har vært gjenstand for pilotering i en årrekke, og de er også i mindre skala brukt som produksjonsløsninger, typisk for utskutte enheter og hjemmekontor. Som besparende transportkanal mellom høgskolenes studiesteder, har **KOMPAKT**-prosjektet med hell konvertert fra interne 2 Mbit/s-samband til IP-baserte forbindelser.

I hjemmemarkedet ser vi nå en tydelig overgang til IP-telefoni, muliggjort av stadig bedre bredbåndsnett og motivert ut fra et privatøkonomisk rasjonale. Det er også stadig flere eksempler på overgang til IP-te-

lefoni i bedriftsmarkedet verden over. Det er ikke lenger et spørsmål om IP-telefoni tar over, men når og hvor fort det vil skje.

Videokonferanseløsninger har vært på markedet lenge og også her har vi sett en overgang fra tradisjonelle, ISDN-baserte systemer, til IP-løsninger, initialt H.323, senere **SIP**. Når **SIP** er anvendt har det oftest vært avgrenset til proprietært videokonferanseutstyr, ikke som et ledd i en skalerbar arkitektur. Vi har til gode å se en allmenn, massiv bruk av videokonferanse som verktøy. Det er mange barrierer, foruten fundamental mangel på skalerbar arkitektur nevnes uholdbar brukerterskel og manglende tilgjengeligjøring. Å sette opp en videosamtale må bli like enkelt som å løfte av røret på telefonen. GigaCampus må adressere disse problemstillingene. Her blir det blant annet viktig å se til pågående **IETF**-arbeid relatert til **SIP**-basert konferansebruk.

Når det gjelder lynmeldinger og tilstedemerkning, som også favnes av **SIP**-arkitekturen gjennom **SIMPLE**, er løsningene mange og broget. Der **MSN**, **ICQ** og dets like har en stor brukerskare i hjemmemarkedet, er åpne løsninger som **Jabber/XMPP** til en viss grad anvendt i vår sektor. **SIPs SIMPLE** seiler nå opp som et lovende alternativ, men dette området er ferskt. En premiss for våre veivalg er uansett åpne løsninger, og vi kan ikke anbefale lynmeldingstjenester som baserer seg på proprietære, kommersielle servere. Det er uholdbart, både fra et drifts- og sikkerhetsperspektiv.

En spennende forlengelse av tilstedemerkning, er kalenderfunksjonalitet. Det er en aktivitet i **IETF**-regi<sup>11</sup>, og vi bør undersøke hvorvidt åpne løsninger lar seg integrere med en **SIP**-arkitektur.

<sup>11</sup> Kalenderstandarder er definert i RFC 2445, 2446 og 2447 fra november 1998. Det er pågående arbeid med å forenkle standarden og adressere reelle interoperabilitetsproblemer

mellom dagens løsninger. **IETF** arbeidsgruppen som jobber med dette heter «calsify» – Calender and Scheduling Standards Simplification.

## UTFORDRINGER

GigaCampus arbeidsgrupper har i 2005 fordypet seg i SIP-baserte arkitekturer. Et rammeverk er utarbeidet, se figur 7. Dette er et godt utgangspunkt til den arkitektur vi skal lage. Et tungtveiende hensyn har vært interoperabilitet med dagens PABX-løsninger. En SIP-arkitektur må naturligvis gi «global summetone», og vi må ha transparent samtrafikk mellom gammel og ny telefoni-infrastruktur. Et vel så viktig designkriterie er det at SIP-arkitekturen blir åpen og frittstående fra de lukkede PABX-systemene. Det er mange argumenter for dette, blant annet det faktum at SIP er mer enn telefoni. Å bevege leverandørledet i retning åpne løsninger er i seg selv viktig.

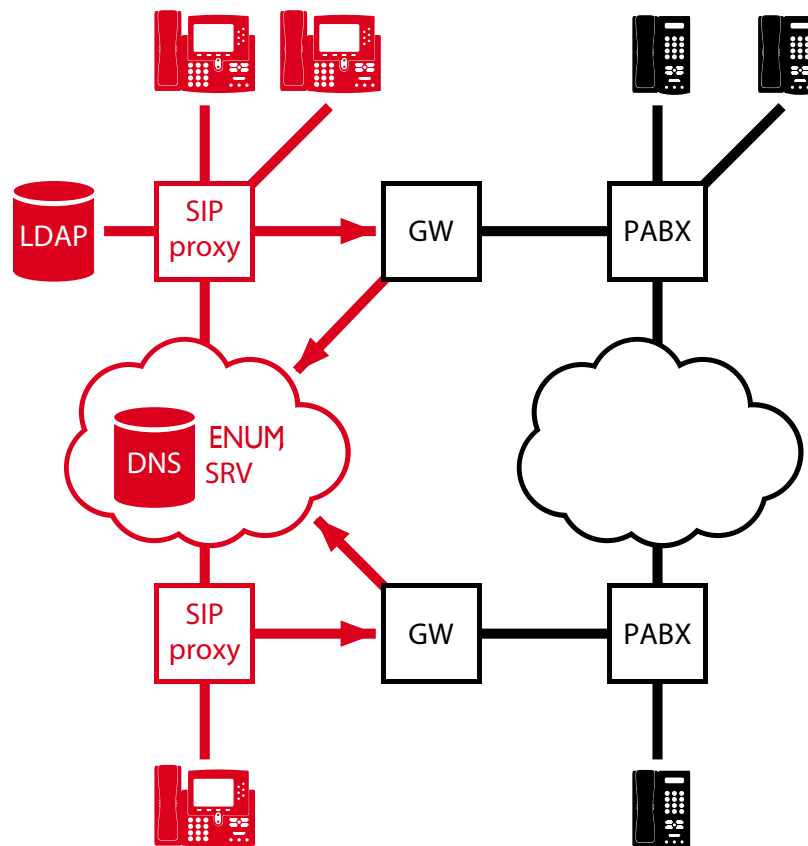
En rekke pilottester er gjennomført i 2005. Arbeidet må fortsette og allerede i 2006 utvider vi med flere piloter. Det endelige målet er en nasjonal infrastruktur med SIP-registrarer, proxyer og portnere ved hvert universitet og høyskole. Med dette på plass, kan tradisjonell telefoni gradvis og naturlig migrere.

Det ligger imidlertid mange utfordringer på vår vei. Vi må være trygge på at SIP-infrastrukturen skalerer, og at den er stabil og sikker. Dagens telefonsentraler har en svært god driftsstabilitet og en pålitelig talekvalitet. En IP-basert løsning kan ikke forringe dette. Vi må tilstrebe redundant design og vi må adressere tjenestekvalitet i IP-nettet. Merk her at tale har relativt små båndbreddebehov, og kapasitetsmessig kan vi uten problem tillate økt talekvalitet per samtale sammenlignet med tradisjonell telefoni.

Et nødvendig telefonitjenestesett må også ivaretas, herunder blant annet sentralbord/kundesenterløsninger, svartjenester og viderekobling. Vi må adressere felles administrasjon og drift, herunder integrert støttesystem. CTI-løsninger som ser på integrasjon mellom telefon og arbeidsstasjon, har et uforløst potensial. IP-basert talekommunikasjon vil gjøre det enklere å lage gode løsninger her.

Et annet spennende aspekt er transport av tale mot omverden over IP-nett. Dette er naturlig når mottaker er SIP-bruker, men det kan også være kostnadsbesparende mot tradisjonelle telefoner. Jo lenger transporten går over IP-nett, jo bedre, gitt dagens debiteringsordninger. Allerede i 2006 vil vi starte overgang av trafikk mot sektorens telefonioperatør, fra ISDN-linjer til IP.

Det blir et mylder av aktivitet innen satsingsområdet. Særlig viktig er det å få koordinert aktivitet med våre tradisjonelle telefonimiljøer. Å bygge opp kompetanse og forståelse av SIP blir viktig. Universitetene er tunge aktører og ønskes sentralt i arbeidet. Parallelt må vi jobbe frem løsninger rundt videokonferanser og lynmeldinger.



Figur 7: Åpen SIP-arkitektur (rød farge) som interopererer med tradisjonell telefoni (sort).

SIP introduserer en overgang fra telefonnummer til SIP-adresser på formen navn@domene. Et viktig lim mellom gammel og ny verden er ENUM. ENUM er en mekanisme for å lagre telefonnummer i domenenavnesystemet (DNS) slik at man kan slå opp en tilknyttet tjeneste som SIP. Tradisjonelle telefonisentraler kan da gjennom portnere, som igjen bruker ENUM, etablere samtaler mot SIP-brukere. ENUM er relativt ferskt og UNINETT Norid startet i november 2005 et nasjonalt testprosjekt. På sikt kan vi forvente en ENUM produksjonstjeneste i Norge.

Sentralt i SIP-infrastrukturen er SIP-tjenere eller proxyer. En SIP-proxy betjener alle brukere i et domene. Når en SIP-telefon ringer en annen SIP-telefon, bruker SIP-proxyene ENUM og **SRV-poster** i DNS for å lokalisere mottagers tilhørende SIP-proxy.

Et siste basalt element i arkitekturen er katalog. Her er det nærliggende å benytte LDAP og se dette i sammenheng med FEIDE. Merk at katalogen har to funksjoner; den brukes for å autentisere en SIP-klient mot sin SIP-proxy og den danner basis for en telefonkatalogtjeneste for brukeren. Integrert katalog mellom gammel og ny arkitektur blir viktig.

I pilottester i 2005 har en linux-maskin med programvaren «SIP Express Router» fungert som SIP-proxy. Videre har en annen linux-maskin med Asterisk programvare fungert som portner mot hussentral. Det er også eksperimentert med **PABX**-enes egne portnerløsninger.



## DELMÅL

- I 2006 skal en pilot SIP-infrastruktur bygges der flere institusjoner; herunder minst to universiteter inngår. Her skal det høstes erfaring med særlig fokus på interoperabilitet mellom gammel og ny arkitektur. Utfordringer relatert til felles administrasjon blir viktig. Vi skal ha fokus på sentrale tjenester som blant annet kundesenter og svartjenester.
- I 2006 skal en andel av eksternt fasttelefontrafikk kanaliseres over IP mot en eller flere leverandører; I 2007 leverer vi mesteparten av trafikken over IP.
- I 2007 vil en nasjonal SIP-infrastruktur ta form. GigaCampus skal med utgangspunkt i forberedt SIP proxy-pakke initiere utrulling av SIP-tjenere i hele sektoren. SIP- produksjonstjenester kan da settes i drift.
- I 2007 vil videokonferanser basert på SIP få utbredelse i sektoren. Det skal jobbes aktivt med tilgjengeliggjøring av gode verktøy på den nye infrastrukturen.
- I 2007 skal en fortrinnsvis SIP-basert infrastruktur for lynmeldinger realiseres.
- I 2008 skal blant annet kalender og delt arbeidsflate innarbeides i SIP-arkitekturen.
- I løpet av 2009 skal utfasing av en rekke tradisjonelle telefonsentraler være iverksatt.

## 5.5 SIKKERHET

Sikkerhet blir et stadig viktigere tema. Trusselbildet er økende, og kompleksitet og kreativitet i ondsinnert aktivitet kjenner få, om noen grenser. Vi ser nå en skremmende utvikling fra rampestreker til organisert kriminalitet. Det kan ligge betydelige økonomiske motiver bak.

*«No country is immune from cybercrime, which includes corporate espionage, child pornography, stock manipulation, extortion and piracy.»*

*«Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over \$105 billion.»*

*«Cybercrime is moving at such a high speed that law enforcement cannot catch up with it.»*

Valerie McNiven,  
rådgiver, internettkriminalitet,  
Det amerikanske Finansdepartementet  
til Reuters 28. november 2005

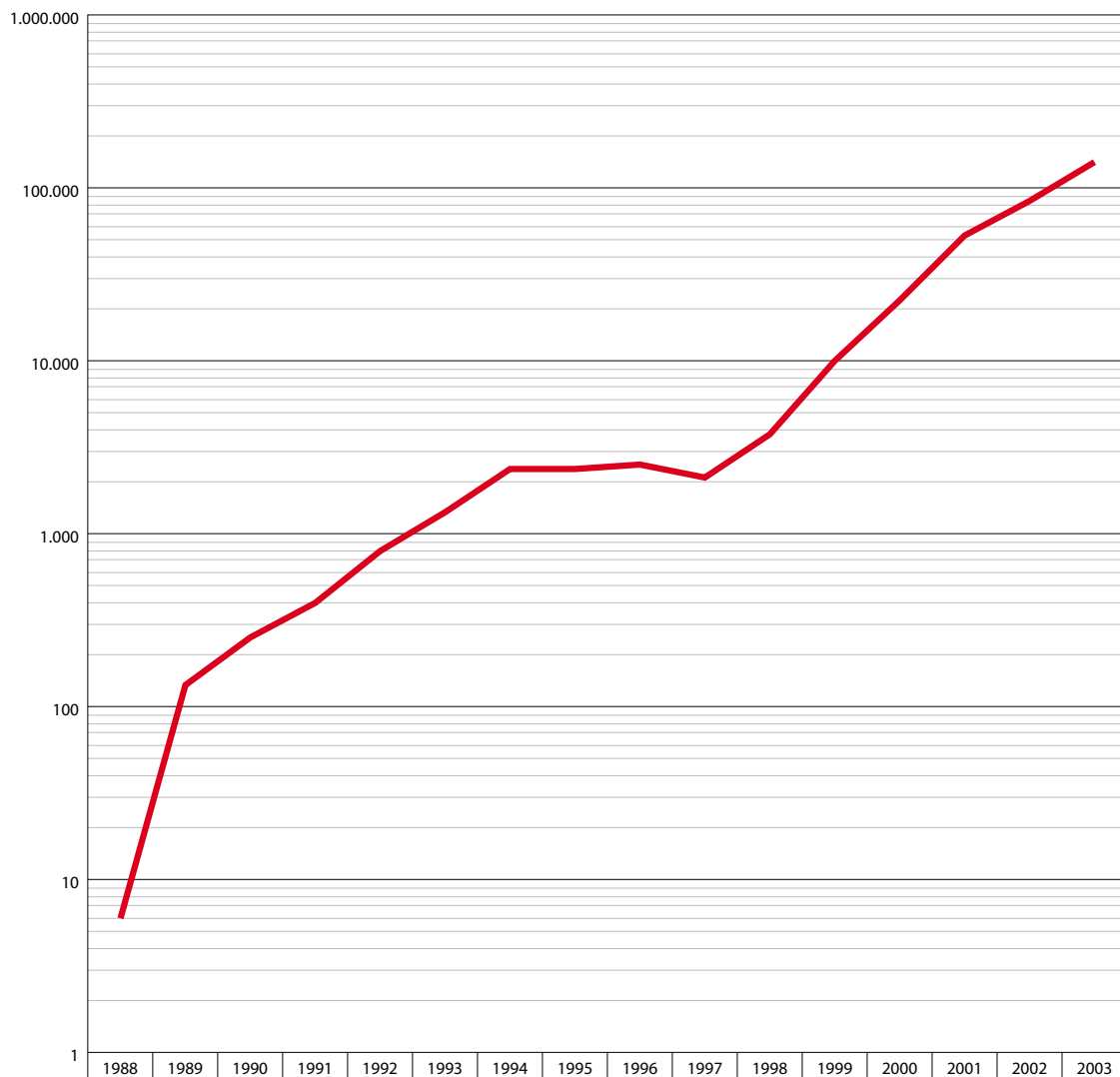
Vi blir med andre ord satt på store prøvelser. Bekjempelse fordrer stadig mer kompetanse og teknisk innsikt. Det krever et velorganisert forsvarsverk med innarbeidet sikkerhet i alle ledd. Det krever gode verktøy, gode rutiner og ikke minst et godt kontaktnett mot andre sikkerhetsmiljø. Et velfungerende samarbeid i sektoren er her særdeles viktig.



## STATUS

Vår sektor har bittert erfart at sikkerhet, eller mangel på sikkerhet koster. Det har vært flere alvorlige episoder med innbrudd på sentrale maskiner/anlegg. Vi ser daglig angrep på infrastrukturen gjennom distribuerte tjenestenektingsangrep (DDoS). Noen av disse er så alvorlige at de kan lamme hele infrastrukturen til den angrepne institusjon i perioden,

og i tillegg gi ringvirkninger til andre institusjoner. Vi ser også mange andre brudd på IT-reglement og/eller norsk lov. Som figur 8 illustrerer, vokser antall sikkerhetshendelser eksponensielt fra år til år. Statistikken er tatt fra Carnegie Mellon University sin [CERT/CC](#), men tendensen er den samme i Norge.



Figur 8: Antall sikkerhetsinsider har vokst eksponensielt ved Carnegie Mellon universitetets CERT/CC

Vi må også huske at UH-sektoren har særlige utfordringer sammenlignet med øvrige Internett-tilknyttede virksomheter. Sikkerhetsbehovet er i prinsippet like høyt, men samtidig må nettverkene være åpne nok til at forskning, eksperimentering og utdanning kan gjennomføres. Vi vil ligge i forkant på trådløst, på bruk av blant annet **multicast**, IPv6 og **SIP**-telefoner. Dette setter igjen særlige krav til et bredt anlagt, proaktivt sikkerhetsarbeid. Når vi også ligger i forkant på kapasitet, blir det særlig forlokkende å bryte seg inn på våre maskiner. Det gir inntrengeren en mulighet til å utføre spesielt kraftige distribuerte tjenestenektingsangrep (**DDoS**).

For å bekjempe slike angrep er organisering og bemanning viktig. UNINETT var tidlig ute og etablerte i 1995 **UNINETT CERT**, landets første enhet for håndtering av sikkerhetshendelser. Over tid har vi knyttet et uvurderlig kontaktnett mot andre forskningsnett og Internett-tilbydere. I 2001 mottok UNINETT CERT akkreditering fra **Trusted Introducer**, som er organisert under **TERENA TF-CSIRT**. Akkrediteringen innebærer at vi fyller gitte krav til tilgjengelighet og kompetanse, og at vi er akseptert som fullverdig medlem blant tilsvarende sikkerhetsteam i Europa.

Fleire universiteter har også etablerte egne **CERT**, hvilket er svært positivt. Det vil i essens si at de følger krav og retningslinjer gitt av RFC 2350: «Expectations for Computer Security Incident Response».

Sikkerhetsarbeidet må forankres høyt i organisasjonen, og det er til syvende og sist ledelsens ansvar. Noen universiteter har tatt tak i dette og utarbeidet egen sikkerhetspolicy og de har også laget underliggende rutiner og prosedyrer. UNINETT FAS har gjennom sitt **TROST**-prosjekt utarbeidet en mal for hvordan policy og underliggende dokumenter kan og bør utarbeides ved en høyskole eller et universitet. Det er viktig at den konkrete policy-en utarbeides lokalt. Prosessen gir i seg selv lokal forankring og eierskap, og den gir dessuten rom for nødvendig lokal tilpasning.

Tilbake på det operative plan er det bred aktivitet i sektoren på sikkerhetsområdet. Det jobbes med sikkerhet på nettnivå gjennom pakkefiltrering og sikkerhetsfremmende nettdesign, herunder aksesikring og kryptering, primært for trådløse nett. Det arbeides med sikring av tjenester og med sikkerhet i endesystemene. Det er stor aktivitet på verktøysiden med en stadig voksende portefølje av avanserte hjelpemidler. Verktøyområdet har klare grensesnitt opp mot vårt satsingsområde drift- og overvåking. **FEIDE** inviterer til opprydning i brukeradminstrasjon. Her er gode rutiner og oppdaterte oversikter over egne brukere svært viktig.

For å samordne aktivitet, dele idéer og gode løsninger, har UNINETT i en årrekke arrangert sikkerhetsseminarer og samlinger, også knyttet opp mot UNINETT-konferansen.

## UTFORDRINGER

Til tross for mye aktivitet, er det mange uløste oppgaver. Jmfør trusselbildet, ser man at utfordringene står i kø. GigaCampus tar nå initiativ til et skikkelig krafttak og vår ambisjon er å ruste opp forsvarsverket ved hver enkelt institusjon. Hjelp til selvhjelp er vår modell, og de enkelte høgskoler og universiteter må selv være i stand til å adressere nødvendige proaktive og reaktive sikkerhetstiltak. I det operative, vil **UNINETT CERT** ha en sentral koordineringsfunksjon med sitt internasjonale kontaktnett og opparbeidede erfaring.

Oppsummert vil GigaCampus virke som katalysator i følgende viktige prosesser:

### Utarbeidet og implementert sikkerhetspolicy (i samarbeid med TROST)

- Utvikling og implementering av sikkerhetspolicy ved alle universiteter og høgskoler
- Utvikling av underliggende reglement, rutiner, prosedyrer og **beste praksis**.

### Operative sikkerhetsteam

- Etablering av lokale sikkerhetsteam, også kalt **IRT** (Incident Response Team)
- Styrke **UNINETT CERT**, herunder mer aktivt informere lokale **IRT** om aktuelle sikkerhetstrusler. Et viktig poeng er å avgrense informasjon til det som er relevant. Ofte kan vanlige sikkerhetskanaler gi en for overveldende informasjonsstrøm.

### Sikkerhet i alle ledd

- Arbeid med sikkerhetsfremmende nettdesign, herunder hensiktsmessig filtrering av trafikk.
- Aksess-sikring og adgangskontroll, kryptering (trådløse nett/**VPN**) og generell sikring av tjenester.
- Sikkerhet i endesystemer: Standardisering av klientparken vil forenkle problemområdet. Ikke-standardiserte klienter/operativsystem vil forekomme, og her må sikkerhet her særskilt adresseres.
- Samarbeid med **FEIDE** i forhold til brukeradministrasjon, autentisering, autorisasjon og aksesskontroll.

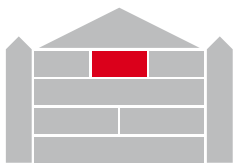
### Utvikling av gode verktøy

- Arbeid med verktøy til hjelp i proaktivt og reaktivt sikkerhetsarbeid, herunder videreutvikling og vedlikehold av eksisterende, samt utvikling av nye.

Ved at GigaCampus blir pådriver på dette feltet, kan sektoren i samarbeid oppnå mange konkrete resultater. Prosessen i seg selv vil gi uvurderlige gevinster. Det er viktig å ytterligere styrke relasjonene mellom sektorens mange sikkerhetsmiljøer.

## DELMÅL

- I 2006 skal flere kompetansehevende kurs arrangeres myntet på lokal sikkerhetsdrift. Kurs- og opplæringsvirksomhet skal gjennomføres regelmessig i hele programperioden.
- I 2006 skal det bygges lokale sikkerhetsteam (**IRT**) ved minst 10 universiteter/høgskoler. Det skal gjennomføres felles opplæring, dernest erfaringsutveksling mellom disse. Aktiviteten skal utvides til 10 nye per år. Innen 2009 skal alle ha etablert egne sikkerhetsteam.
- I 2006 skal åtte universiteter/høgskoler få en helhetlig sikkerhetsgjennomgang med konkrete anbefalinger til forbedring. Dette arbeidet skal fortsette utover i programperioden og sluttføres i løpet av 2009.
- I 2006 skal piloter velges for utarbeidelse av lokal sikkerhetspolicy. GigaCampus blir katalysator i prosessen, og **TROST**-prosjektet sin mal for arbeidet benyttes. Arbeidet gjøres lokalt og godkjent policy skal implementeres påfølgende år. I løpet av 2009 skal alle universiteter og høgskoler ha en godkjent sikkerhetspolicy.



## 5.6 DRIFT OG OVERVÅKING

Satsingsområdet drift og overvåking fokuserer på IKT-driftsprosessen. I ytterste forstand omfatter dette alle aspekter av ITIL-rammeverket. I GigaCampus kontekst vil vi fokusere de viktigste grepene norske universiteter og høyskoler bør ta for å snu eventuelle reaktive trender til sunn, proaktiv drift. I dette bildet vil vi utarbeide og vedlikeholde et konsentrat av den erfaringsbakgrunn som sektoren besitter, et UH-sektorens **beste praksis**. Dermed vil vi fokusere på gode åpen kildekode-verktøy som kan understøtte driftsprosessen.

Merk at vi på dette satsingsområdet i likhet med sikkerhetsområdet, har et bredere fokus enn nettverk.

### STATUS

Alle de store universitetene har tunge prosesser med fokus på å bedre egen IKT-drift:

- Ved NTNU har man siden 2003 arbeidet med **ITIL**. Man har fokusert særlig på områdene hendelses-håndtering, endringshåndtering, konfigurasjons-håndtering og tjenestenivåhåndtering. De kan vise til en særlig vellykket implementering av hendelses-håndtering, med et velfungerende opplegg for første- og andrelinje brukerstøtte.
- UiB har også tatt i bruk **ITIL** rammeverket og fokusert spesielt på førstelinje brukerstøtte og endringshåndtering. De erfarer at prosessen i seg selv er nyttig, fordi den bevisstgjør en rekke «selvfølgeligheter». Implementert med fornuft, uten at rutineverk og administrative forordninger tar helt overhånd, finner UiB ITIL nyttig.
- UiO gjennomførte i 2005 et større prosjekt, der de kartla de viktigste elementene i UiOs IT-infrastruktur som trenger overvåking og rapportering. De har videre gjennomført en detaljert analyse av USITs rutiner og metoder for overvåking og rapportering. Dette inkluderer hvilke verktøy, metoder

og rutiner som finnes og/eller brukes i dag. Prosjektet gir forslag til tiltak og videre arbeid.

- UiT gjennomførte også et kartleggingsprosjekt i 2005 der de evaluerte de behov IT-avdelingen har med hensyn til overvåking. Forslag til verktøy ble gitt.
- UiS sto i 2005 ved oppstarten av en ITIL-prosess med ønske om at den kan gi næring til forbedringer i eget driftsopplegg.

Når det gjelder bruk av verktøy, er det en klar overvekt i sektoren rundt åpen kildekode-løsninger. Det er få, om noen eksempler på vellykket innføring av store kommersielle rammeverk. De fleste universitetene har vært innom slike systemer, samt en del høyskoler. Nokså entydig og forenklet sagt, fungerer ikke slike systemer etter hensikten.

Mengden av egenutviklede løsninger i sektoren er stor med alt fra små, men nyttige perl script, til mer fullblods overvåkingssystemer som **NAV** og **Stager**. NAV, som er utviklet av NTNU siden 1999 er uten sidestykke den løsning som er mest utbredt i sektoren. Alle universiteter og 15-20 høyskoler har installert og mer eller mindre brukt NAV til egen nettovervåking.

## UTFORDRINGER

Å forbedre egen driftsprosess er en prosess som aldri tar slutt. Det er viktig at arbeidet forankres lokalt, og at man med eget utgangspunkt jobber med forbedringer, sortert ut fra det viktigste først. GigaCampus sin oppgave blir å veilede og bistå i denne prosessen. Referanserammen er UH sektorens **beste praksis**, som vi må utarbeide og vedlikeholde. Denne skal ikke være en absolutt fasit, men fungere som veiledende råd om hvor og hvordan man bør gripe an forbedringsprosessen.

På verktøysiden ser vi det som viktig å støtte gode utviklingsprosjekter og stimulere til videreutvikling i en åpen kildekode-kontekst. Vi ønsker åpne løsninger som kan være til nytte for hele sektoren, potensielt hele Internett-samfunnet. GigaCampus ønsker også å aktivt medvirke til bruk av disse verktøyene. Vi foreslår en GigaCampus overvåkingspakke til alle interesserte høyskoler og universiteter. Pakken vil inneholde en stadig voksende portefølje. Inisielt vil **NAV** og **Stager** vil være sentrale komponenter. NAV oppdager topologi, gir statusrapporter, samler inn trafikkstatistikk, varsler om utfall av komponenter og tjenester og kan foreta maskinsporing med mer. Stager kompletterer NAV med maskin til maskintrafikkanalyse på IP-adresse og portnivå basert på nettflytdata.<sup>12</sup>

Det er viktig av GigaCampus sin overvåkingsgruppe fungerer som et faglig aktivum, der man gjennom faste møter deler erfaringer, effektive løsninger, skript og verktøy. Infrastrukturen vi driver er i konstant bevegelse, der stadig nye og mer komplekse utfordringer møter oss. Vi trenger stadig nye verktøy, og svært ofte er det formålstjenlig med egenproduserte løsninger. Gjentatte ganger har sektoren vist at kombinasjonen høy kompetanse og effektfulle skript er en god oppskrift.

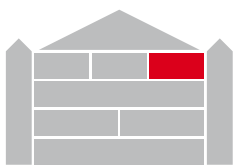
For å gi et bilde av spennet av verktøy GigaCampus sin overvåkingsgruppe vil arbeide med, se vedlegg B for klassifisering av overvåkingsverktøy. Som det fremkommer favner dette bredt med verktøy som har fokus på tilgjengelighet, målinger, inventar, sikkerhet, hendelser, varsling, konfigurering, samt prosessstøtte.

## DELMÅL

- En felles anbefaling skal utarbeides: «UH-sektorens beste praksis: proaktiv drift». Innen 2009 skal alle høyskoler og universiteter følge hovedprinsippene i denne.
- Innen 2006 skal et GigaCampus-apparat for å fange opp og støtte gode utviklingsprosjekter være på plass. Det skal stimuleres til deling av verktøy og løsninger. Brukerforum og referansegrupper rundt bredt anvendte løsninger skal dannes. Dette vil i første rekke gjelde **NAV**, her skal GigaCampus sikre finansiering av ønsket videreutvikling.
- Innen 2007 skal alle høyskoler og universiteter ha fått tilbud om installasjon og opplæring i GigaCampus sin overvåkingspakke. Som et minimum vil **NAV** og **Stager** inngå i denne porteføljen. Et sentralt driftsopplegg skal være på plass.
- Sentralisert drift av nett og tjenester kan organiseres som et tilbud i GigaCampus-regi, enten lagt til UNINETTs eget driftsenter eller i regi av et eller flere universiteter/høyskoler. Dette åpner for en større grad av sentralisering av driften og kan gjennomføres der det er formålstjenlig. GigaCampus skal innen 2007 anbefale et driftsopplegg med dette for øye.

<sup>12</sup> Nettflytdata (netflow) eksporteres fra Cisco-rutere og gir informasjon om hver eneste flyt i nettet, med kilde- og destinasjons IP-adresser og TCP/UDP portnummer (hvis relevant), antall pakker og byte, tidsangivelse m.m. En IETF-standard,

IPFIX, er under ferdigstilling og vil gi oss en åpen løsning tilsvarende nettflyt. Stager tar mål av seg å støtte IPFIX.



## 5.7 ENDE TIL ENDE-KVALITET

Der det foregående satsingsområde dekker de grunnleggende behov for overvåkning og proaktiv drift, går vi her lenger og fokuserer på måling av kvalitet. Nettverket og tjenestene skal ikke bare virke, de skal virke på et tilfredstillende nivå. I en tid der stadig flere sanntidstjenester settes i drift blir dette bare viktigere. Korte og pålitelige rundreisetider er avgjørende for slik trafikk. Selvfølgelig må vi sørge for at de nettverk vi bygger kan håndtere sanntidskrav, men det er ikke godt nok. Problemer vil inntreffe, og flaskehalsen vil oppstå. For effektiv feilsøking er gode målinger avgjørende.

Vårt perspektiv er globalt, fra ende til ende. Tjenestekvalitet kan ikke utelukkende analyseres og løses lokalt på campus. Mange tjenester krever transport over landegrensene gjennom mange nettverk. Vi må kunne måle interdomene; nasjonalt mellom våre campusnett, internasjonalt mot andre nettverk. Det er også viktig å gjøre måleverktøy, nettkart og statistikk tilgjengelig for brukerne. Mange problemer blir i dag underrapportert, fordi brukeren selv ikke vet hvordan hun skal angripe et opplevd problem. Her har GigaCampus en viktig utfordring.

### STATUS

I dag har vi en del grove redskaper og kombinert med god teft og årelang driftspraksis kommer vi ofte langt. Men tidvis kommer vi til kort, nevnte underreportering er nok også regjerende. Det vi har er data fra basis overvåkningsprogrammer. Disse kan gi indikasjoner på feil ved studie av feiltellere fra ruter- og svitsjereporter, samt overvåking av CPU-belastning og minneforbruk i rutere. Regulære rundreise- og pakketapsmålinger kompletterer datagrunnlaget. UNINETT har gode verktøy som dekker disse områdene (Nemo, Zino, GenPlot, Mping, *Stager*). Universitetene og en del høyskoler har også verktøy, da primært *NAV*.

<sup>13</sup> Web100, se <http://freshmeat.net/projects/web100/>

<sup>14</sup> I dag benyttes DAG-kort fra Endace, se <http://www.endace.com/products.htm>

For å effektivt feilsøke kvalitetsproblemer på et mikronivå, har vi imidlertid lite. Vi må i fremtiden være i stand til å feilsøke kvalitetsforringelse av en gitt IP-telefonisamtale. Vi må også ha en bedre forståelse av gjeldende trafikk sammensetning, herunder hvordan ulike tjenester oppfører seg. Vi må kunne studere intensitet for en gitt strøm og sammenstille dette med målinger fra andre observasjonspunkter. Vi må også kunne måle i en maskestruktur, ikke ut i fra et sentrisk punkt, som i dag.

Når vi i GigaCampus tar fatt på dette arbeidet, står vi heldigvis ikke på bar bakke. UNINETT har i flere år samarbeidet med *Q2S*-senteret på NTNU, et nasjonalt senter for fremragende forskning. Vi deltar også i flere internasjonale prosjekter som blant annet *LOBSTER*, som har fokus på passive målinger og *GÉANT2s JRA1* som tar mål av seg å bygge en ende til ende- måleinfrastruktur for europeiske forskningsnett, kalt *perfSONAR*. Vi samarbeider også med det amerikanske *Internet2*-miljøet.

### UTFORDRINGER

I 2005 som var GigaCampus sitt forprosjektår, startet vi vårt arbeid med utplassering av målemaskiner eller såkalte *målepåler* i nettet. Dette er et ambisiøst prosjekt som vil vare i hele programperioden. Vi ønsker å utplassere målepåler ved samtlige studiesteder i sektoren. Hittil er 14 maskiner utplassert.

En *målepåle* er en kraftig linux-basert datamaskin med en spesialkjerne<sup>13</sup> som er særlig egnet til å studere detaljer i initierte trafikk målinger. Brorparten av målepålene utstyres med ekstern GPS-antenne for å få absolutt presisjon på tid. Dette er særlig viktig for å kunne gjennomføre enveis pakkeforsinkelsesmålinger. I tillegg vil en betydelig andel av målepålene ha spesiallagede, passive målekort som er i stand til å prosessere og analysere gigabitrate i hardware<sup>14</sup>. Passivt vil her si at forbigående trafikk speiles til kortet, enten i svitsj eller ved optiske splitters. Vi kan da analysere all trafikk som går inn og ut av et gitt

campusnett. Figur 9 illustrerer dette. Ved å benytte den svært avanserte MAPI-programvaren som videreutvikles i LOBSTER-prosjektet, kan analyse gjøres i hardware. I programperioden vil vi anskaffe 10 Gbit/s målekort som gjør oss i stand til å analysere ekstreme trafikkmengder i sanntid.

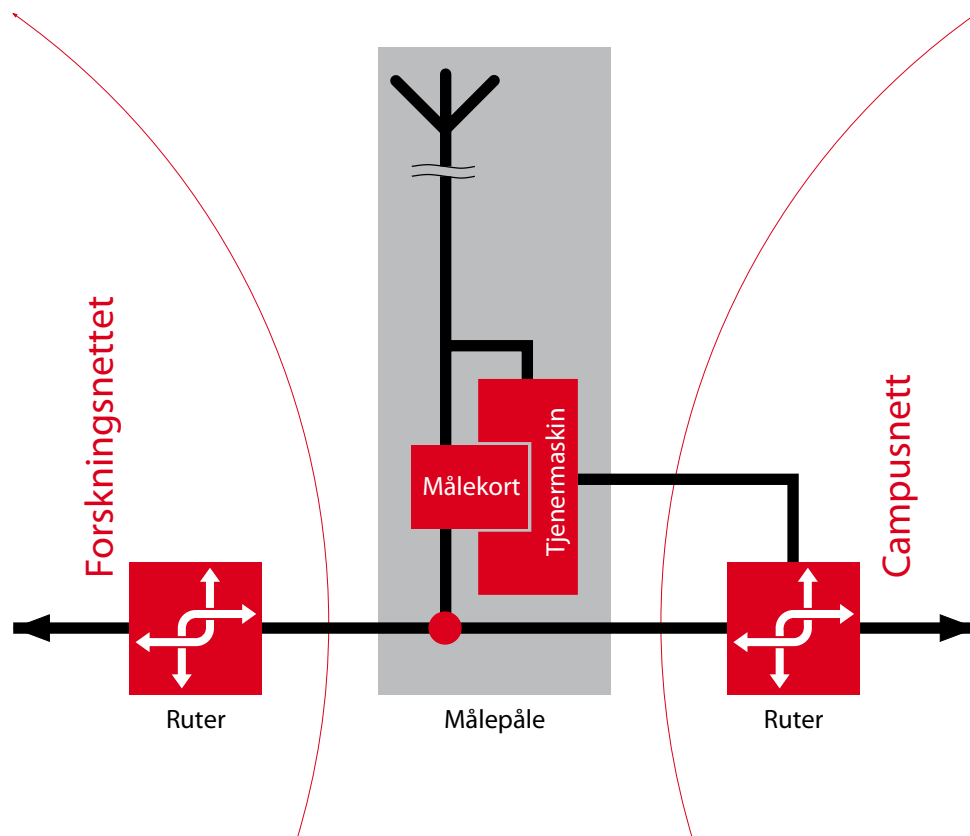
Initielt vil vi fokusere på målinger for:

- Toveis pakkeforsinkelse og tap mellom og forbi målepåler, også mot destinasjoner i Europa.
- Enveis pakkeforsinkelse og tap. Disse målingene setter krav til synkronisert klokke og er således tyngre å realisere. De er til gjengjeld svært verdifulle, da de er bedre i stand til å påpeke eksakt feilkilde.

- Måling av intensitet for hver sesjon, herunder pakkeavstand. Studie av RTP tidsmerker.
- Måling av tilgjengelig kapasitet
- Tjenestekarakterisering, blant annet hvordan web-trafikk og samtrafikk oppfører seg.

Regelmessige målinger skal suppleres med målinger gjennomført på forespørsel, gjennom et webgrensesnitt tilgjengelig for vilkårlig sluttbruker. Her er konseptet at alle skal kunne måle kvaliteten på sin egen forbindelse frem til en gitt målepåle.

Målepålene vil også inngå i JRAI-prosjektets europeiske måleinfrastruktur. En sluttbruker skal da kunne se karakteristika med sin forbindelse mot servere i Norge og utlandet.



Figur 9: Målepåle med passivt målekort og GPS-antenne

Det er i seg selv viktig å gjøre målepåle-infrastrukturen tilgjengelig for nasjonal og internasjonal nettforskning. Det arbeides med løsninger for anonymisering av data, slik at personvern krav ivaretas. Vi forventer en rekke prosjekter i programperioden som vil gjøre oss bedre i stand til å forstå og løse de utfordringene vi møter i trafikkbildet, ut fra et kvalitets- og sikkerhetsperspektiv.

Operativt vil vi forsterke vårt fokus på ende til ende-kvalitet betydelig. Inspirert av **GEANT2**, vil UNINETT opprette en nasjonal **PERT** (Performance Enhancement Response Team) som vil bli organisert sammen med vårt driftssenter og koordinert med vår døgn-kontinuerlige beredskapsvakt.

### DELMÅL

- I 2006 skal vi initiere regulære toveis og enveis forsinkelsesmålinger mellom og gjennom alle målepåler. Statistikk skal gjøres tilgjengelig og vi skal også tilby webgrensesnitt for sluttbruker for å interaktivt kunne initiere målinger ved behov.
- I løpet av 2007 skal de fleste studiesteder ha utplassert målepåler. Disse skal inngå i en europeisk måleinfrastuktur. UNINETT PERT skal etableres.
- I 2007 skal vi særskilt adressere utfordringer relatert til kvalitet i trådløse nett.
- Innen 2008 skal vi ha passive 10 Gbit/s målekort for alle av UNINETTs høyhastighetsaksesser. Forbindelsene til NORDUnet (d.v.s. Internett generelt), NIX (nasjonalt samtrafikkpunkt), UiO og NTNU, m.fl. vil inngå.
- Innen 2009 skal verktøyporteføljen på målepålene være omfattende og veletablert. De skal inngå som uvurderlige redskaper for UNINETT PERT og for sektorens øvrige driftspersonell, til hjelp i daglig drift og feilsøking.





# SENTRALE PROSESSER

## SENTRALE PROSESSER

I forrige kapittel presenterte vi de primære satsingsområdene for GigaCampus. Vi beskriver her de sentrale prosessene som skal sørge for aktivitet rundt satsingsområdene.

### 6.1 UNINETT FAGSTYRKE

Sektorens kollektive kompetanse er stor. Det er en utfordring å utnytte potensialet som ligger her på en felles formålstjenlig måte. Den enkelte fagmedarbeider har sitt lokale virke og vil primært være fokusert på å løse sine oppgaver der. Samtidig er det slik at faglig kontakt med andre både er stimulerende og givende. UNINETT ser det som sin oppgave å forme en felles arena. Konkret vil vi opprette arbeidsgrupper innen GigaCampus sine syv satsingsområder, på sikt kan flere områder komme til. Bred deltagelse fra sektoren er en premiss, primært fra universitetene, høyskolene og UNINETT selv, men også andre institusjoner kan delta. Hver arbeidsgruppe blir et faglig talerør for sitt område. De skal arbeide målrettet og utarbeide konkrete anbefalinger og veiledninger for sektoren, basert på sektorens **beste praksis**.

Arbeidsgruppene vil ha møter og arbeide mellom møter med diskusjoner på sin e-postliste. Hver arbeidsgruppe vil ha en leder som driver arbeidet frem. Arbeidsmåten vil være demokratisk, og her vil vi adoptere IETF sin modell med røff konsensus; vi kan synse, vi kan mene, vi kan saktens diskutere, men ved dagens slutt vil vi handle. Vi vil oppnå konkrete, målbare resultater. Arbeidsgruppene skal i essens:

- Være en pådriver for konkrete og matnyttige anbefalinger og veiledninger

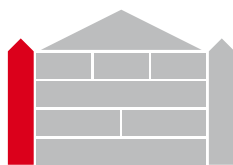
Anbefalingene vil så snart de er godkjent bli gitt et unikt nummer og gjort alment tilgjengelig. De vil i neste instans danne naturlige rettesnorer for løsningsvalg i sektorens campusnett.

Så langt det er praktisk mulig vil vi samle de ulike arbeidsgruppemøtene til felles samlinger. Deltagerne på disse samlingene utgjør en stor kollektiv, fag-

lig kraft, en kraft vi gir navnet *UNINETT fagstyrke*. UNINETT fagstyrke skal også diskutere faglige utfordringer i et lengre tidsperspektiv. Fagstyrkesamlingene blir et arnested for fagstrategi- og arkitekturarbeid på høyt nivå, og en viktig arena for synergi og erfaringsutveksling.

UNINETT's testnettgruppe vil være en sentral aktør i UNINETT fagstyrke. De har allerede etablerte samarbeidsprosjekter mot nasjonale og internasjonale forsknings- og piloteringsprosjekter. De er også aktivt deltagende i flere av IETFs standardiseringsprosesser. Vi ser gjerne en utvidet deltagelse på disse arenaene gjennom universitetene. Slike faglig tunge spillere vil tilføre UNINETT fagstyrke stimulerende impulser fra omverden. Således vil UNINETT fagstyrke bli en brobygger mellom det operasjonelle og FoU og et forum med internasjonal kontaktflate





## 6.2 INNKJØPSSAMARBEID

Universitetene har tradisjonelt forhandlet frem egne rammeavtaler for nettelektronikk og til dels telefoni. For høgskolesektoren har man sørget for samordning gjennom **KOMPAKT**. I noen tilfeller har man allerede gjort sektoromspennende avtaleverk, blant annet trafikkavtaler for mobil- og fasttelefoni og vedlikeholdsavtaler av telefonsentraler.

Samlet har UH-sektoren stor markedsrett og koordinerte innkjøpsavtaler og utstyrsanskaffelser vil ha mange fordeler. Her nevnes kort:

- Lavere kostnader på anskaffelse og vedlikehold
- Muligheter for anskaffelse av utstyr med høyere kvalitet
- Færre utstyrstyper gir sektoren en mer rasjonell teknisk drift og bedre teknisk kompetanse
- Enklere og billigere opplæring
- God kvalitetssikring av anskaffelsesprosessen
- God oppfølging av inngåtte kontrakter
- Enkeltinstitusjoner slipper å opprettholde anskaffelseskompetanse
- Alle UH-institusjoner kan gjøre avrop på avtalene

I perioden skal GigaCampus koordinere/tilrettelegge for flere innkjøpsavtaler for sektoren. Arbeidet er forutsatt gjennomført som et samarbeid mellom UNINETT, universiteter og høgskoler. Det forutsettes at sektoren synliggjør egne planer om forestående utstyrsanskaffelser. GigaCampus vil deretter lodde interessen for en koordinert utstyrsanskaffelse før eventuelt prosess igangsettes.

Følgende anskaffelser anses å være aktuelle:

- Nettverkselektronikk
- Trafikkavtale mobiltelefoni
- Trafikkavtale fasttelefoni
- Vedlikeholdsavtaler telefonsentraler

En viktig oppgave for GigaCampus er oppfølging av eksisterende avtaler/kontrakter.

UNINETT FAS og **TROFAST**-prosjektet fremforhandler også felles avtaler, beregnet for sektorens administrative systemer. GigaCampus vil samordne sin aktivitet med UNINETT FAS.

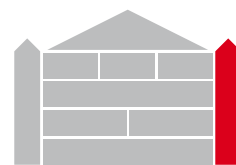
## 6.3 PROSJEKTSTØTTE FOR FELLES VERKTØY OG LØSNINGER

GigaCampus ser det som viktig å støtte gode utviklingsprosjekter ved universiteter og høgskoler. Dette er typisk prosjekter som er initiert lokalt, der man har grepet en utfordring og løst et konkret problem. Dersom verktøyene som lages utvikles generelt, vil de kunne bli til allmenn nytte ved flere universiteter og høgskoler. Det vil forandre et håndterbart apparat for drift av systemet, herunder dokumentasjon, brukerstøtte, feilretting og ønsket videreutvikling.

GigaCampus ønsker å støtte gode prosjekter slik at de kan overleve startfasen. UNINETT har allerede gjort dette i en årrekke for det NTNU-baserte overvåkingssystemet **NAV**, denne støtten vil fortsette med GigaCampus. Selv utvikler UNINETT **Stager**, initielt for eget behov, men en åpenbar kandidat for allmenn GigaCampus-nytte. Videreutvikling her må også sikres.

Et naturlig krav er at utviklet programvare blir lisensiert som åpen kildekode. Dette inviterer til tilbakemelding og potensielle bidrag fra det globale Internett-samfunnet. Som styringsinstans vil GigaCampus også sikre kvalitet, påse at produktet skalerer og at det har sektoromgripende potensiale. GigaCampus vil se til at støttede løsninger blir installert og brukt, jfr. kapittel 6.4 under.

GigaCampus sin arbeidsgruppe for overvåking i 2005 har utformet noen sentrale, generelle råd hva angår verktøyvalg. Prosjekter som vil være naturlige kandidater for prosjektstøtte fra GigaCampus bør arbeide innenfor denne referanserammen:



- Baser ikke overvåking av egen infrastruktur på ett verktøy, men et sett av verktøy som løser ulike oppgaver. Det er likevel viktig å tilstrebe et sentralisert alarmsystem.
- Gode verktøy har riktig fokus, og de viktigste problemene skal rapporteres på en tydelig måte.
- Samle inn masse data relatert til tilstand og trafikk i nettverket. Tilstreb gode løsninger for presentasjon av nåtids- og historiske data. Prioriter automatisk analyse og alarmering.
- Støtt opp under skripting som arbeidsform, og ikke undervurder betydningen av dette. Små skript gjør ofte stor nytte. Skripting er resultatorientert, det er også givende og utviklende for IKT-driftsmiljøet.
- Støtt opp under åpen kildekode, og bidra med åpen kildekode.

## 6.4 IMPLEMENTASJONS- OG DRIFTSSTØTTE

En sentral GigaCampus-aktivitet blir implementasjons- og driftsstøtte. Dette har fungert meget bra i **KOMPAKT**-regi, der jevnlig besøk ved landets høyskoler har vært gjennomført, da med innfasing av nye svitsjer, rutere og/eller telefonsentraler på agendaen. Svært mange høyskoler etterspør en slik tjeneste. Vi ser det som rasjonelt å sentralisere denne funksjonen. Det er ikke realistisk at hver enkelt høyskole selv kan ha tilstrekkelig dybdekompetanse for å gjennomføre slike større løft. Alternativet vil være kostbar konsulentbistand, og her har ikke erfaringene vært de beste.

En interessant GigaCampus-modell er å utvide gruppen som deltar i implementasjonsarbeidet. Kompetente bidrag fra universitetene/høyskolene er velkomne.

Merk at implementasjonsstøtte vil gjelde alle satsingsområdene i GigaCampus, ikke bare nettverksbygging. Sikkerhetsgjennomganger, trådløs utbygging, **SIP**-infrastrukturbygging er andre naturlige utrullingsaktiviteter.

Det er også etterspurt en felles verktøykasse (omtalt i kap. 5.6). Konkret tenker vi her på en utplassert maskin med egnet overvåkingsprogramvare. Inicialt vil dette være **NAV** og **Stager**, senere kan annen programvare komme til. GigaCampus ønsker å tilby sentralisert drift av løsningen, samt opplæring i hensiktsmessig bruk av verktøyene.

Innen kvalitetsområdet ønsker vi å utplassere målepåler (se kp. 5.7). De har til hensikt å gjøre regelmessige og målinger ved behov helt ned på et per-sesjonsnivå for å kunne avdekke potensielle kvalitetsmessige problemer i trafikkbildet. Problemkilden kan ligge i endesystem eller i mellomliggende transportnett.

Etter ønske kan UNINETT's sentrale driftssenter, ev. andre driftssenter, bistå med lokalnettdrift ved

høgskoler. Dette kan også inngå som en tjeneste i GigaCampus-regi. Det kan variere fra høgskole til høgskole hvorvidt og i hvilken grad dette er interessant. Noen vil ønske å i størst mulig grad håndtere drift lokalt, mens andre ønsker et sentralisert tilbud.

Vi tenker oss også en samordnet beredskapsordning med regional beredskap og rutiner for 24/7 feilretting. Samordnet reservedelslager med depot i hver region inngår i dette bildet. Likeså et distribuert sett av avanserte måleinstrumenter som for eksempel fiber analyseverktøy.

## 6.5 KOMPETANSEHEVING

Regelmessige kurs og opplæringsvirksomhet skal også inngå i GigaCampus. Dette kan skje sentralisert, i tilknytning til fagstyrkesamlinger eller i utrullingskontekst lokalt på et gitt studiested. Uansett er den overordnede målsettingen å løfte det allmenne kompetansenivået på nett- og sikkerhetsdrift.





# DOKUMENTASJON OG ERFARINGSSPREDNING

## DOKUMENTASJON OG ERFARINGSSPREDNING

Det er viktig at GigaCampus-programmet dokumenterer sin aktivitet og sine resultater. Det er ønskelig at de lærdommer og erfaringer som GigaCampus høster, kan komme andre til nytte.

Følgende tiltak vil bli gjort i programmet:

- GigaCampus sitt eksterne nettsted, [www.gigacampus.no](http://www.gigacampus.no), vil være et strukturert og oppdatert samlested for all offentlig informasjon som programmet produserer.
- Et nettsted med begrenset adgang vil supplere dette. Arbeidsdokumenter som er under utvikling vil bli lagt her; [wiki](#) vil bli brukt for formålet. Alle deltagere i UNINETT fagstyrke og/eller GigaCampus-prosjekter vil ha tilgang.
- E-postlister og webforum vil være viktige virkemidler for pågående aktivitet og diskusjon i UNINETT fagstyrke og pågående prosjekter. Tilgang vil være begrenset, som for wiki.

Følgende dokumenter gjøres tilgjengelig:

- UNINETT fagstyrke vil produsere skriftlige anbefalinger innen de ulike fagområdene. Disse vil bli understøttet med detaljerte oppskrifter og praktiske veiledninger.
- En rekke kurs, seminarer og konferanser vil bli holdt. Alle presentasjoner vil bli gjort tilgjengelig.
- De ulike GigaCampus-prosjektene vil ha prosjektplaner, milepælsrapporter og sluttrapper. Sluttrapper blir fritt tilgjengelig.





# ORGANISERING OG FORANKRING

## ORGANISERING OG FORANKRING

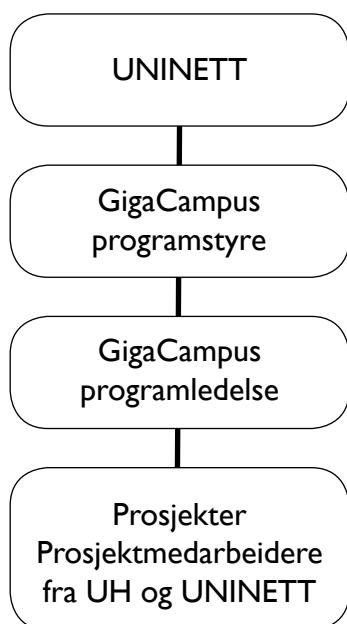
GigaCampus organiseres som et program med en programledelse. Programledelsen vil bestå av en programansvarlig, en fagsjef og en plansjef. Alle disse tre vil være UNINETT-ansatte.

Programledelsen organiserer aktiviteten i programmet med årlige planer, der en rekke prosjekter inngår. De enkelte prosjektene har selvstendige prosjektledere med underliggende prosjektmedarbeidere. Det er ønskelig med deltagelse fra hele sektoren. Prosjektlederne rapporterer til programledelsen på milepælsnivå.

Programledelsen rapporterer i sin tur til programstyret. Programstyret skal ha deltagere fra IKT-ledelsen ved flere universiteter og høyskoler, samt fra UNINETT selv.

Programstyret skal:

- fastsette rammene for programledelsen med hensyn til gjennomføring av GigaCampus-programmet, både faglig, økonomisk og framdriftsmessig.
- påse at bevilgede midler anvendes rettfærdig overfor sektorens institusjoner.
- rapportere kvartalsvis til UNINETTs styre om status relatert til aktivitet, økonomi og framdrift.



Figur 10 viser GigaCampus sin organisasjonsmodell.



# KOORDINERING MED ANDRE SATSINGER

## KOORDINERING MED ANDRE SATSINGER

GigaCampus er en stor satsing med mange kontaktflater. Internt i UNINETT AS vil GigaCampus initiere aktivitet i både nett-, testnett- og tjenestegruppen. Videre er tett koordinering med en rekke satsinger, nasjonale såvel som internasjonale viktig.

Vi nevner spesielt:

- **eVITA** (eVitenskap, Infrastruktur, Teori og Anvendelser) er et 10-årig program, initiert av Norges forskningsråd med oppstart i 2006. eVITA har som ambisjon å løfte norsk forskning innen **eVitenskap** til et høyt internasjonalt nivå. eInfrastruktur og operasjonell **Grid** inngår som viktige komponenter i eVITA. Disse blir koordinert av UNINETT Sigma. Tett samarbeid med GigaCampus er ønskelig.
- **GÉANT2**-prosjekter: GÉANT2 er drevet av **DANTE** og finansiert av EU og av de respektive europeiske forskningsnettene. GigaCampus vil gjennom sin måle-infrastruktur bli en aktiv utprøvningsarena i GÉANT2 sin ytelsesmonitorering og målesaktivitet (**JRA1**). UNINETT deltar også i GÉANT2 sitt **eduGAIN**-initiativ (**JRA5**) som kan gi viktige resultater til GigaCampus sin mobilitetssatsing, da relatert til nettaksess på tvers av læresteder i Europa (eduGAIN kalles populært «**eduroam2**»).
- **TERENA** er en organisasjon for samarbeid mellom europeiske forskningsnett. UNINETT er aktiv i flere TERENA arbeidsgrupper. I GigaCampus sin sikkerhetssatsing er koordinert aktivitet mot TERENAs **TF-CSIRT** viktig.
- **LOBSTER**-prosjektet er drevet av et konsortium med ni partnere, der bl.a. UNINETT og **TERENA** inngår. LOBSTER har fokus på nettmålinger basert på passive målekort. GigaCampus sine **målepåler** blir en arena for LOBSTER, og resultater blir viktige for GigaCampus. Videreutvikling av **Stager** inngår i LOBSTER og er et høyaktuelt verktøy for landets campusnett.
- UNINETTs **FEIDE**-prosjekt utvikler en strategi for hvordan elektronisk autentisering kan realiseres for alle ansatte og studenter/elever ved norske utdanningsinstitusjoner. I GigaCampus-regi vil FEIDE blant annet levere løsninger for trådløs nettaksess.
- UNINETT FAS sitt **TROST**-prosjekt jobber med IKT sikkerhetspolicy og vil i tett samarbeid med GigaCampus være pådriver for at alle universiteter og høyskoler implementer egen policy med underliggende reglement, rutiner og prosedyrer.
- UNINETTs **Samson-prosjekt** vil levere tjenermaskiner til GigaCampus for nettovervåking, måling av kvalitet (**målepåle**), **SIP**-tjenere, m.m.
- UNINETT ABC sitt **SOLID**-prosjekt driver en IKT-veiledningstjeneste myntet på skolesektoren (grunn- og videregående skoler). **SOLID**-delta-gerne er rekruttert fra IKT-avdelinger ved flere høyskoler. Kompetanseoppbygging, samt produksjon av anbefalinger og faktark står sentralt i deres arbeid. UNINETT fagstyrke og **SOLID** vil koordinere sin aktivitet tett.
- UNINETT FAS sitt **TROFAST**-program tilrettelegger for og utarbeider løsninger for felles tjenester og samspill mellom administrative systemer. Samarbeid med GigaCampus i forhold til avtaleverk, sikkerhet og driftsløsninger er viktig.
- UNINETT Norids **ENUM** pilotprosjekt er en viktig leverandør til satsingsområdet person til person-kommunikasjon. En **SIP**-infrastruktur betinger bruk av satsingsområdet i DNS.
- **NAV**-prosjektet besørger drift og videreutvikling av overvåkningssystemet NAV. Aktiviteten drives i samarbeid med NTNU og UNINETT. Flere andre universiteter vil bidra med komponenter til **NAV**, og Universitetet i Tromsø er allerede i gang. GigaCampus vil sørge for at NAV kommer til nytte ved landets campusnett.

- UNINETT har tett samarbeid med NTNUs **Q2S**-senter for fremragende forskning. Dette har grenseoppgang mot GigaCampus sin satsing på ende til ende-kvalitet.
- UNINETT deltar aktivt i flere **IETF**-arbeidsgrupper. Standardiseringsarbeid i IETF gir viktige føringer for UNINETT fagstyrke sine anbefalinger.





# FINANSIERING

## FINANSIERING

GigaCampus er finansiert over statsbudsjettet for 2006, der følgende formulering er gitt:

*«GigaCampus-programmet vil vere eit samarbeidsprosjekt mellom UNINETT og universitets- og høgskolesektoren. Regjeringa forslår å løyve 12,6 mill. kroner som eingongsløyving til GigaCampus-programmet. Vidare vil departementet øymerke til saman 15 mill. kroner av løyvinga til institusjonane i universitets- og høgskole-sektoren til dette prosjektet, slik at samla løyving til GigaCampus-programmet blir 27,6 mill. kroner i 2006. Utrekningane til UNINETT viser at ein årleg vil spare 60–100 mill. kroner i høve til om institusjonane skulle gjere tilsvarende oppgåver på eiga hand.»*

GigaCampus programstyre vil påse en fornuftig bruk og rettferdig fordeling av de bevilgede midlene. I tråd med universitets- og høgskolerådets anbefaling vil programmet hente inn og administrere de øremerkede midlene. Dette muliggjør en mest mulig rasjonell og hensiktsmessig fordeling i programperiodens fireårige løp.

Programledelsen vil gjennomføre aktivitet i henhold til de rammer programstyret gir. Det forutsettes en løpende regnskapsføring og god rapportering tilbake til programstyret. En reell kollektiv besparelse skal påvises.

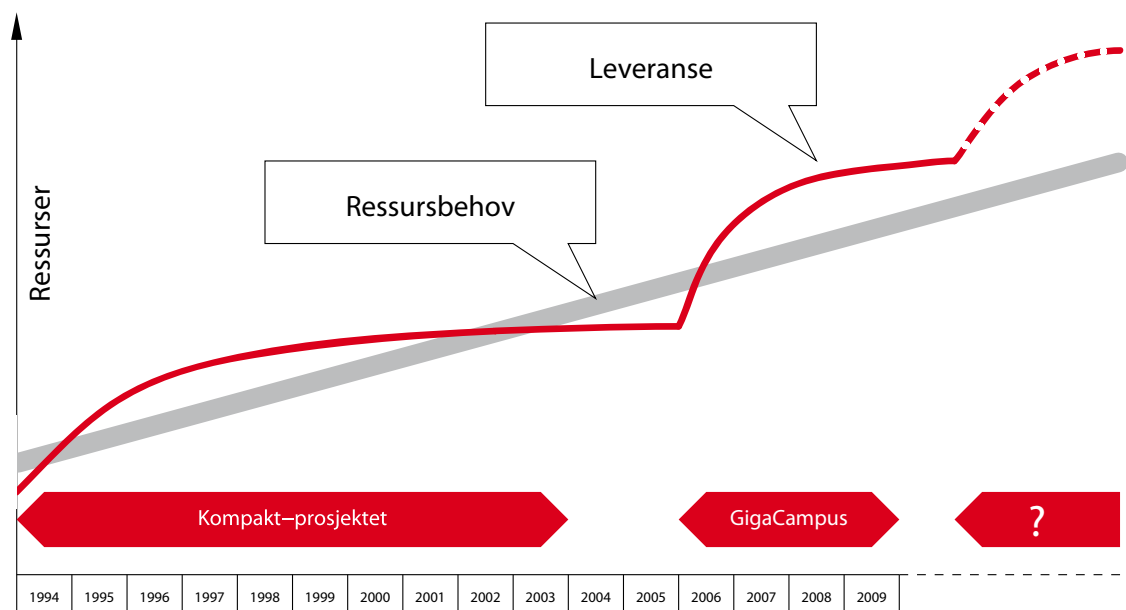
Statsbudsjettet for 2006 poengterer at UNINETTs direktebevilgning er en engangsbevilgning. Vi innser at alle programmets intensjoner og mål ikke kan nås uten ytterligere finansiering senere i programmet.



## BEHOV FOR NYE KRAFTTAK

Som **SERENATE**-rapporten understreker (jfr. 2.4), må vi kontinuerlig ruste opp vår felles nettverksmessige infrastruktur. **KOMPAKT**-prosjektet gjorde et løft for landets høyskoler i perioden 1994-2003. GigaCampus gjør nå et utvidet løft for perioden 2006-2009. Senere vil nye krafttak bli nødvendig, men fra når er det vanskelig å spå. Det vi med sikkerhet vet er at trenden vil fortsette, ettersom stadig flere tjenester og bruksområder vil se dagens lys. Behovet for en kraftig og pålitelig infrastruktur av høy kvalitet vil bare bli viktigere og viktigere.

Figur 11 illustrerer hittil erfart og videre stipulert vekst i ressursbehov. IKT-leveransen må stå i forhold til dette, både i programperioden og enda lenger frem i tid.







# VEDLEGG

## VEDLEGG

### A) GJENNOMFØRTE FELLES FIBERPROSJEKTER

- **Fibersameiet Tromsø:** Samarbeid om fiberutbygging i Tromsø. Deltakere: Høgskolen i Tromsø, Troms fylkeskommune, Tromsø kommune, Universitetet i Tromsø, Universitetssykehuset Nord-Norge, UNINETT. Prosjektkostnad: ca. kr 12,5 mill. delt mellom partene. Antatt levetid: 30 år. Lønnsomhet kontra leie hos operatør: 1-2 år.
- **Fiberanlegg mellom Trondheim og Stjørdal:** Deltakere er Trønder Energi, Malvik E-verk, BaneTele, Statens Vegvesen, Nord-Trøndelag E-verk og UNINETT. Prosjektkostnad: ca. kr 4 mill. Gir UNINETT bedre feiltoleranse i sitt landsdekkende stamnett og HiNT får gigabitforbindelse til sin nye avdeling i Stjørdal.
- **Fiberanlegg i Oslo, mellom sentrum og UiO:** Samarbeid med BaneTele og Oslo Sporveier. Kostnad for UNINETT og UiO var 300 000 kr. Innspart på få måneder.
- **Aksess- og internfiber i Mo, Bodø, Trondheim, Bergen m.fl.:** Disse var svært lønnsomme og ga samtidig mulighet for å iverksette konkurransen i telemarkedet fra åpningen i 1998.

### B) KLASSIFISERING AV OVERVÅKINGSVERKTØY

Overvåkingsverktøy kan klassifiseres langs mange akser; de kan være passive/aktive, de kan ha system-, nett- eller klientfokus og de kan blant annet være rammeverk eller nisjeprodukter. Vi forsøker oss her på en grov klassifisering som sier noe om funksjonsområde:

- A) Feilhåndtering
- B) Ytelseshåndtering
- C) Logistikkhåndtering
- D) Sikkerhetskategorier
- E) Hendelses- og varslingstjenester
- F) Konfigurasjonshåndtering
- G) Prosesshåndtering

NAV dekker kategoriene A,B,C og E, men ikke alle aspekter. **Stager** har fokus på kategori B. **Daily** og **Scanorama**, begge utviklet ved UiO, har fokus på område D.

En nærmere beskrivelse av kategoriene følger:

#### A) Feilhåndtering

- Har fokus på **tilgjengelighet**. Tilgjengelighet av bokser, tjenester og prosesser.
- Statusmonitorer (boks opp/ned, port/interface opp/ned), tjenesteovervåkere og prosessovervåkere inngår her.

#### B) Ytelseshåndtering

- Har fokus på **målinger**, typisk måling av kvalitet i en eller annen form. Vi er forbi virker/virker ikke-nivået og ser på måleparametre, statistiske data som beskriver virkeevne/ytelse/kvalitet.
- Dette er en stor sekkepost som igjen kan inndeles i:
  - o Datainnsamlere: f.eks. cricket/rtd, genplot, stager backend, andre netflow-innsamlere etc. Evnen til å lagre, herunder aggregere historiske data er sentralt.

- o Presentasjonsverktøy: rapportgeneratorer, grafisk visning (grafer, stolper, kakediagram etc.). Evnen til å fleksibelt sammenstille ulike datasett i en presentasjon er viktig, samt evnen til å sortere data og tydeliggjøre interessante trekk.
- o Auto-analyseverktøy: Dette er «datatygere» som gir alarmer. Fokuset er primært på proaktiv drift, ikke sikkerhet, men her er åpenbar overlapp. Eks.: terskelmonitører, anomalidetektorer.

### C) Logistikkhåndtering

- Kartlegger **inventaret**. Hva slags utstyr har vi, med hva slags innmat? Hvordan er utstyr sammenkoblet (topologi), hvor (og når) er endeutstyr og brukere tilkoblet (maskin/brukersporing). Hvilke tjenester har vi, og hva er relasjoner og avhengigheter mellom disse.

### D) Sikkerhetshåndtering

- Har fokus på **sikkerhet**, og skal understøtte proaktivt sikkerhetsarbeid. Omfatter scannere (nmap, nessus, scanorama, etc.), «sladrere» (daily m.fl), «snoop & analyze» (ids, nerd m.m.)

### E) Hendelses- og varslinghåndtering

- Dette er **hendelses- og varslingssystemene**.
  - o De er i stand til å varsle driftspersonell om alarmer, gjerne på ulike kanaler (e-post, sms, web, jabber etc).
  - o Mulighet for å motta alarmer fra eksterne systemer er essensielt (mottak kan være basert på snmp trap, e-post, syslogg, lytte på tcp-port m.m.).
  - o Evne til å klassifisere hendelser i alvorlighetsgrad, evne til å korrellere hendelser og tydeliggjøre «root cause», ev. undertrykke følgefeil/skyggefeil. Mulighet for å dempe blaff/forbigående feilsymptomer, etc.

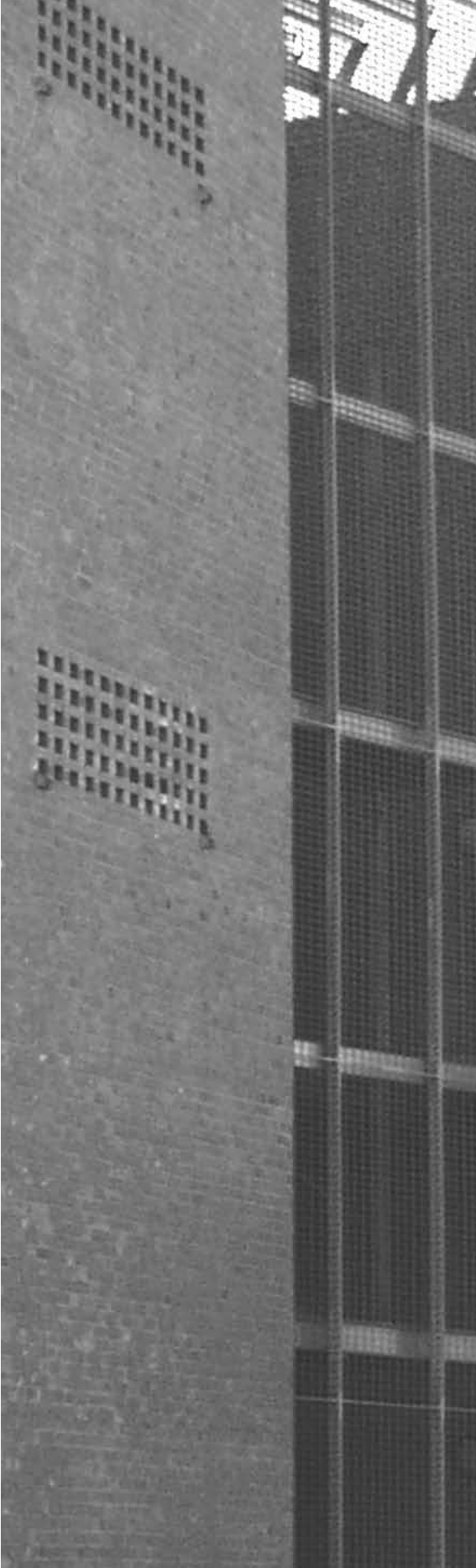
### F) Konfigurasjonshåndtering

- Har fokus på **konfigurasjon** av utstyr.

### G) Prosesshåndtering

- Understøtter de ulike IKT **driftsprosessene**. Eksempler på verktøy her kan være saksbehandlings(trouble ticket)-systemer og endringshåndteringssystemer.





# ORDLISTE

## ORDLISTE

**AA** (autentisering og autorisasjon) er en komplett mellomvarestruktur for håndtering av autentisering og autorisasjon av brukere mot ulike tjenester. **FEIDE** er et eksempel på dette.

**Anycast** er en mekanisme som gjør en IP-adresse tilgjengelig fra flere steder. Dersom de ulike instansene av IP-adressen tilbyr eksakt samme tjeneste og de har en fornuftig lastdeling mellom seg, oppnår man en skalerbar og robust løsning. Merk at ikke alle tjenester egner seg for anycast, p.g.a. ulike krav til synkronisering.

**ASP** (Active Server Pages) er en spesifikasjon for nettsider. En ASP-fil inneholder html-kode og annen kode, og filene har ofte endelsen .asp.

**Aspirasjonsdetektor** er en detektor som trekker til seg luften fra rommene, fjerner støv og fuktighet, for så å «lukte» om det er gasser i luften som indikerer brann.

**Beste praksis** – etter «best practice»-begrepet som kommer fra ITIL. Dette er anbefalinger som er basert på mange års konkrete erfaringer, gjerne fra flere ulike IKT-driftsmiljø.

**BGP** (Border Gateway Patrol) er en protokoll som bærer rutinginformasjon mellom ulike internettoperatører. Hele Internett er i dag basert på BGP-ruting. BGP gir et ryddig administrativt skille mellom ulike selvstendige nettverk. BGP brukes i dag mellom UNINETT og de største universitetene.

**CERT/CC** (Computer Emergency Response Team/Coordination Center) er et betydelig koordineringssenter som operativt håndterer Internett-sikkerhets hendelser. CERT/CC er organisert under Software Engineering Institute ved Carnegie Mellon University. CERT/CC ble operative i 1988, da som det første CERT i verden. Se også **UNINETT CERT**.

**CSIRT** (Computer Security Incident Response Teams) Begrepene CERT, CSIRT og IRT brukes om hverandre og uttrykker det samme.

**CTI** (Computer Telephony Integration) ser på integrasjon mellom telefoni og datamaskiner. Eksempler kan være programvare som viser relevant informasjon på skjermen knyttet til det telefonnummeret som ringer inn.

**Daily** er et overvåkingssystem utviklet ved Universitetet i Oslo. Daily har fokus på klientsikkerhet. En agent installeres på hver enkelt klientside i nettverket, disse rapporterer inn til en sentral tjener som strukturerer dataene og lager overordnede og detaljerte rapporter. Daily brukes aktivt ved Universitetet i Oslo og foreligger nå i sin andre versjon; Daily2.

**DANTE** (Delivery of Advanced Network Technology to Europe) er en ikke-kommersiell organisasjon som skal planlegge, bygge og drive sammenkoblinger mellom europeiske forskningsnett, les mer på: [www.dante.net](http://www.dante.net)

**DDoS** (Distributed Denial of Services) er distribuerte tjenestenektangsangrep. Tjenestenektangsangrep vil si at en maskin sender mengder med ondsinnet trafikk rettet mot en annen maskin, eller et sett med maskiner med den hensikt å sette målmaskinen, ev. hele målnettverk ut av spill. Tjenestenektangrep blir særlig kraftige når de opptrer som koordinerte angrep fra en rekke maskiner, og det er dette som kalles DDoS. Et DDoS-angrep fordrer at angriper på forhånd har brutt seg inn på en rekke maskiner slik at disse kan virke som fjernstyrte agenter i angrepet.

**Distribusjonssvitsjer** håndterer aggregert trafikk fra et sett av **kantsvitsjer** og har typisk en høykapasitets fiberforbindelse (gigabit eller 10 gigabit) mot **kjerne-svitsj**.



**eduGAIN** er en felles protokoll som snakker mellom føderasjonene, og er en utvidelse av den standardiserte protokollen **SAML**. Viktige komponenter i eduGAIN arkitekturen vil være broelementer som oversetter protokoller brukt i de lokale føderasjonene til eduGAIN.

**eduroam** (Education Roaming) er en infrastruktur som gjør det mulig for studenter og ansatte å logge inn på trådløstnett på utdanningsinstitusjoner i eget land og i andre europeiske land. eduroam benytter 802.1X som aksessløsning. **RADIUS** benyttes for autentisering. Samarbeidet mellom de ulike utdanningsinstitusjonene er realisert gjennom et hierarki av RADIUS-tjenere.

**EMC** er en elektromagnetisk forstyrrelse som kan oppstå mellom elektriske komponenter dersom ikke gitte krav er overholdt.

**ENUM** er navnet på en protokoll som beskriver hvordan telefonnummer kan registreres som domenenavn i domenenavnsystemet (DNS). Protokollen knytter et telefonnummer til en vertsmaskin eller til ressurser på Internett som kan lage en forbindelse til det vanlige telefonnettet. Mer informasjon på [http://www.norid.no/enum/om\\_enum.html](http://www.norid.no/enum/om_enum.html)

**eVITA** (e-Vitenskap, infrastruktur, teori og anvendelser) er en nasjonal plan for koordinering og utvikling av **eVitenskap** i Norge. Planen er utarbeidet av en gruppe bestående av representanter fra alle universitetene, forskningsinstitutter, næringsliv og offentlige institusjoner. eVITA er et 10-årig program og initiell støtte for 2006 er gitt av Norges forskningsråd. UNINETT Sigma er satt til å koordinere infrastrukturkomponenten av eVITA, samt operasjonell **Grid**.

**eVitenskap** er bruk av datamaskiner for å gi forklaringer på kompliserte fenomener som ikke er mulig å studere teoretisk eller ved fysiske eksperimenter. eVitenskap gjør det mulig å analysere store mengder data på en rask og kostnadseffektiv måte.

**FEIDE** (Felles elektronisk identitet) er identitetsforvaltning for utdanning basert på et samarbeid mellom organisasjoner i utdanningssektoren og deres leverandører av IT-baserte tjenester. Mer informasjon på <http://www.feide.no/>

**FoU**: Forskning og utvikling

**Føderasjon** er en samling av vertsorganisasjoner og tjenesteleverandører som har felles policy og avtaleverk rundt identitetsforvaltning.

**GÉANT2** er et europeisk samarbeidsprosjekt i regi av DANTE og har et bredt perspektiv på nettbygging. Forskning, videreutvikling av teknologier, mellomvare og tjenester står også sentralt i prosjektet. UNINETT er aktiv deltager i flere GÉANT2-prosjekter; bl.a. innen områdene overvåking, mobilitet og identitetsforvaltning. Se <http://www.geant2.net/> for mer informasjon.

**GPRS** er en utvidelse av GSM-standarden som gir støtte for pakkesvitsjet datatransport. GPRS omtales ofte som 2,5G, altså en generasjon mellom andre generasjon (GSM) og tredje generasjon (f.eks. UMTS) mobiltelefoni.

**Grid** er en teknologi under utvikling som muliggjør fleksibel, sikker og koordinert deling av elektroniske ressurser mellom forskere og forskningsgrupper. Både på regionalt, europeisk og globalt nivå samles kreftene for å realisere det vitenskapelige potensialet som ligger i å samkjøre høyhastighets datanettverk, tungregneanlegg, lagringssystemer, måleutstyr og forskningsdatabaser ved bruk av Grid-teknologi.

**Horisontal kabling** er kablingen fra telematikkrom til kontor. Hvert enkelt datapunkt har en dedikert forbindelse til sitt tilhørende telematikkrom.

**HSRP** (Hot Standby Router Protocol) er en protokoll som sørger for dynamisk skifte mellom to eller flere default rutere ut av ett nettsegment. HSRP er en Cisco-proprietær variant av **VRRP**.

**IAPP** (Inter Access Point Protocol) er en del av **IEEE 802.11f** og er en protokoll som benyttes mellom trådløse basestasjoner for å gjøre «handover» mellom klienter.

**IEEE 802.11a** er en standard for trådløse nettverk som opererer på 5 GHz. IEEE 802.11a benytter **OFDM** og gir hastigheter opptil 54 Mbit/s.

**IEEE 802.11b** er en standard for trådløse nettverk som opererer på 2,4GHz båndet. IEEE 802.11b gir hastigheter opptil 11 Mbit/s.

**IEEE 802.11f** er en standardisering av **IAPP**.

**IEEE 802.11g**: opererer i likhet med IEEE 802.11b i 2,4 GHz-båndet, men har overlegne moduleringsteknikker basert på ortogonal frekvensdivisjon (OFDM) og gir hastigheter opp til 54 Mbit/s.

**IEEE 802.1X** er en standard for portbasert aksesskontroll, der en bruker må autentisere seg for å få tilgang til nettverket. Standarden kan benyttes som aksessikring i både fastnett og trådløse nett.

**IETF** (Internet Engineering Task Force) er en åpen organisasjon som utvikler standarder for Internett-samfunnet, såkalte, RFC-er. Arbeid i IETF er organisert i arbeidsgrupper og arbeid er basert på frivillighet.

**Internet2** er et konsortium av 207 amerikanske universiteter som jobber sammen med industri og regjering for å utvikle og ta i bruk morgendagens Internett. Les mer: <http://www.internet2.edu/>

**IRT** (Incident Response Team) er lokale sikkerhetsteam, begrepet brukes synonymt med CERT og **CSIRT**

**ITIL** (Information Technology Infrastructure Library) består av en omfattende samling av «best practices» for IKT-drift. ITIL har sin opprinnelse fra offentlig administrasjon i Storbritannia og er i dag et svært utbredt metodeverk som anvendes av mange bedrifter. Mer informasjon på <http://www.itsmf.no/bestpractice/>

**Jabber** er en åpen XML-basert protokoll for lynmeldinger og tilstedemarkering.

**Jumboframes** er vanlig pakkestørrelse på et lokalnett (ethernet) og er i utgangspunktet begrenset til 1500 byte. Ved gigabithastigheter gir dette et suboptimalt trafikkmønster som krever uforholdsmessig mange kvitteringspakker. Ved å tillate såkalte jumboframes,, kan svitsjer og rutere videresende pakker som er større enn 1500 byte, helt opptil 9000 byte.

**JRA1** (Joint Research Activity 1) er et delprosjekt innen **GÉANT2**. JRA1 jobber med arkitektur for uthenting av målinger på tvers av de europeiske forskningsnettene.

**JRA5** (Joint Research Activity 5) er et delprosjekt innen **GÉANT2** som både jobber med mobilitet på trådløse nett (**eduroam**) og innloggingsløsninger som virker sammen (**eduGAIN**).

**Kantsvitsjer** er ytterste nivå av svitsjer som står ut mot endeutstyret i nettverket.

**Kjernesvitsjer** er sentrale svitsjer i sentrum av campusnettet. En kjernesvitsj er en svært kraftig svitsj som håndterer aggregert trafikk fra en rekke **distri-busjonssvitsjer** og fra sentrale servere, m.m.

**KOMPAKT** er forløper til GigaCampus som jobbet med telefoni- og nettinfrastruktur på campus for høgskolesektoren. Opererte fra 1994-2003.

**Lambdanett** kommer av den greske bokstav lambda ( $\lambda$ ), som er tegnet for bølgelengde. Lambdanett er fysisk adskilte, bølgelengdeforbindelser som kan gi spesielle brukergrupper mulighet til dedikerte høykapasitets forbindelser. Lambdanett blir et supplement til det ordinære nettverket og kan i avlaste dette. Innføringen av fiber helt ut til tjenerparkene, samt bruk av bølgelengdemultiplesere i sentrale knutepunkter muliggjør bruk av lambdanett. Lambdanett blir også kalt hybride nett.

**LOBSTER** (Large-scale Monitoring of Broadband Internet Infrastructures) er en videreføring av EU-prosjektet SCAMPI, som skal utvikle maskin- og programvare for passiv overvåking av høyhastighetsnettverk.

**MAPI** (Messaging Application Programming Interface) er et programgrensesnitt.

**Multicast**: er kommunikasjon der en enkelt sender til en gruppe mottakere i ett nettverk. Multicast er egnet til bla. kringkasting av blant annet levende bilde og distribusjon av programvare.

**Målepåle** er målemaskiner som blir utplassert ved ulike universiteter og høyskoler som et ledd i Giga-Campus-programmet. Målepålene måler blant annet enveis pakkeforsinkelse og tap, tilgjengelig kapasitet, karakterisering av nett, kartlegging av kvalitet, ytelse per sesjon, intensitet i hver sesjon, avstandsvariasjon, multicast-målinger og regelmessige målinger/on-demand.

**NAT** (Network Address Translation) er en generell metode for å la flere maskiner i et nettverk dele en felles offisiell IP-adresse mot omverden. En NAT-ruter oversetter mellom den offisielle IP-adressen og IP-adresser på innsiden av NAT-ruteren. Det er vanlig å bruke adresser definert i RFC 1918-standarden på innsiden av en NAT-ruter.

**NAV** (Network Administration Visualized) er et nettovervåkingsverktøy utviklet ved NTNU siden 1999, fra 2001 i samarbeid med UNINETT. NAV oppdager automatisk topologien til nettverket, d.v.s. hvilke komponenter som er koblet sammen med hvilke andre. NAV er i stand til å spore maskiner i nettverket, både hvor de er tilkoblet og hvor de tidligere har vært tilkoblet. NAV samler trafikkstatistikk og gir alarmer ved utfall av enkeltkomponenter eller tjenester, eller dersom terskelverdier overskrides. NAV kan sende alarmer på e-post og SMS

**Optiske bølgelengdemultiplesere** er i stand til å utnytte kapasiteten i en fiberkabel langt bedre ved at ulike bølgelengder benyttes.

**Ortogonal frekvensdivisjon** (OFDM) splitter radio-signalet inn i flere samtidige subsignaler som igjen er sendt samtidig på forskjellige frekvenser. OFDM reduserer mengden krysstale i signaltransmisjon (krysstale er en forstyrrelse forårsaket av elektromagnetisk interferens).

**OSPF og IS-IS** er dynamiske rutingprotokoller som brukes mellom rutere internt på et campusnett. Alle de større universitetene benytter i dag OSPF og har til en viss grad bygget ringstrukturer som sikrer alternative veier i sitt campus ryggradsnett. UNINETT benytter IS-IS, primært fordi IS-IS også kan håndtere IPv6-ruting.

**PABX** (Private Automatic Branch Exchange) er en term for hussentral/telefonsentral. En ofte brukt synonym forkortelse er PBX.

**PDA** (Personal Digital Assistant) er en bærbar, håndholdt enhet som brukes for å holde orden på eksempelvis avtaler og gjøremål.

**perfSONAR** (Performance Service Oriented Network Monitoring Architecture) er en infrastruktur for overvåking av nettverksytelse som gjør det enklere å løse ende til ende- ytelsesproblemer på stier som krysser flere nettverk. perfSONAR er en sentral ingrediens i **GÉANT2**-prosjektet **JRAI** som også UNINETT er involvert i.

**PERT** (Performance Enhancement Response Team) er et driftssenter med særlig fokus på å adressere problemer relatert til ytelse og tjenestekvalitet. Et PERT er avhengig av avanserte verktøy. Målepåle-verktøyene vil være viktige redskap for et UNINETT PERT når denne enheten opprettes.

**Q2S** (Center for Quantifiable Quality of Service in Communication Systems) er et nasjonalt senter for fremragende forskning ved NTNU. UNINETT er partner i Q2S.

**RADIUS** (Remote Authentication Dial-in User Service) er definert i RFC 2865 og en protokoll for autentisering og autorisasjon av brukere. RADIUS legger til rette for sentralisert administrasjon av brukerdata.

**RFID** (Radio Frequency Identification) brukes til å registrere automatisk nærhet til sensor; men trenger ikke fysisk kontakt som bl.a. kredittkort o.l. Ved å feste en RFID-brikke på utstyr har man muligheten til å kartlegge hvor utstyret befinner seg.

**RSTP** (Rapid Spanning Tree Protocol) er en forbedring av den opprinnelige Spanning Tree Protocol (STP). STP bryter eventuelle løkker i lokalnettet, slik at ikke trafikk går i ring. Problemet med STP er at man ved utfall av primærvei bruker opptil 30 sekunder på å konvertere til alternativ vei. RSTP reduserer denne tiden betraktelig.

**RTP** (Real-time Transport Protocol) definerer et standard pakkeformat for leveranse av lyd og bilde over internett. RTP kjører over UDP og benyttes ofte ved streaming, IP-telefoni, videokonferanser m.m.

**SAML** (The Security Assertions Markup Language) er et XML-basert rammeverk for web-tjenester som muliggjør veksling av autentisering og autoriseringsinformasjon mellom ulike parter.

**Samson** er en tjenermaskinløsning UNINETT tilbyr sine nettkunder. Tilbyr DNS, e-post, basis fil- og web-tjenester.

**Scanorama** er et proaktivt overvåkingssystem utviklet og brukt ved Universitetet i Oslo. Scanorama scanner alle maskinene i nettverket på jakt etter sårbarheter og åpne porter.

**SD-anlegg** er et sentralt driftsanlegg. SD-anlegg har fokus på overvåking av bygningsmessige forhold som strøm, temperatur, fuktighet m.m. SD-anlegg er lukkede systemer som ikke er integrert av det generelle nettverket. Som regel er det teknisk avdeling eller Statsbygg som er brukere SD-anlegg.

**SERENATE** (Study into European Research and Education Networking As Targeted by eEurope) var en strategisk undersøkelse finansiert av EU-kommisjonen og administrert av den transeuropeiske forskningsorganisasjonen **TERENA**. Undersøkelsen ble avsluttet desember 2003 og konkluderte bl.a. med at de nasjonale forskningsnettene med tilhørende campusnett er et viktig nasjonalt gode. Se <http://www.serenate.org/> for mer informasjon.

**Shibboleth** er en arkitektur og programvareløsning for føderert innlogging tilsvarende **FEIDE**. Utviklet i USA og brukes i mange land, blant annet Storbritannia og Finland.

**SIMPLE** (SIP for Instant Messaging and Presence Leveraging Extensions) er en utvidelse av SIP som støtter lynmeldinger og tilstedeværelse. SIMPLE er definert i RFC 3428.

**SIP** (Session Initiation Protocol) er en åpen standard laget for oppsett av multimediesamtaler. Den registrerer og formidler hvor en person er tilgjengelig, og formidler forhandling av protokoller og formater for en samtale. SIP er definert i RFC 2543 og RFC 3261.

**SNMP** (Simple Network Management Protocol) er en standardprotokoll for overvåking og administrasjon av komponenter over et IP-nett.

**SRV-poster** (Service poster) er innslag i DNS (Domain Name System), definert i RFC 2782. Knytter en tjeneste ved et domene mot en eller flere spesifikke servere. Brukes blant annet i SIP for å opplyse om servernavn for SIP-proxy.

**SSM** (Single Source Multicast) er et alternativ til ASM, Any Source **Multicast**, som er mest utbredt i dag. ASM tillater alle deltagere av en multicast-gruppe å være sendere. I en del tilfeller, som f.eks. kringkasting av TV-program, er det ønskelig å effektivt avgrense kilden til en part (d.v.s. beskytte kilden mot «støy»).

**Stager**: er et verktøy for lagring, aggregering og presentasjon av nettverksstatistikk. Stager er utviklet av UNINETT og består av en webapplikasjon for presentasjon av data, og en back-end for datalagring og aggregering. Initielt hadde Stager fokus på analyse av nettflyt (netflow)-data, men har vokst til å bli et mer generelt statistikkverktøy.

**Strukturert sprednett** er kabling som bruker standardiserte komponenter og som følger nasjonal (NS-EN 50173) og internasjonal (EIA/TIA-568-A) standard. Dette gjør at nettet kan brukes til en rekke formål, som blant annet data, tele, video og diverse styringssystemer.

**TF-CSIRT** (Terena Task Force for Collaboration of Security Incident Response Teams) legger til rette for samarbeid mellom Computer Security Incident Response Teams (**CSIRTs**) i Europa. Hovedmålet er å sørge for et felles forum for deling av erfaringer og kunnskap, etablering av pilotjenester i det europeiske CSIRT og assistere ved opprettelse av nye CSIRT.

**TROST** (Trygg organisering av sikkerhet for tjenester) er et prosjekt i regi av UNINETT FAS som skal bidra til å bygge en sikkerhetskultur i universitets- og høyskolesektoren. Dette skal skje gjennom utvikling og tilpassing av et rammeverk for de enkelte institusjoners sikkerhetspolitikk innen informasjons- og kommunikasjonsteknologi. Les mer på: <http://www.uninett.no/fas/trost/>. TROST samordner nå sin aktivitet med GigaCampus.

**Trusted Introducer** er et felles, europeisk initiativ som skal sørge for samordning av sikkerhetsteam. Les mer på: <http://www.ti.terena.nl/>

**TERENA** (the Trans-European Research and Education Networking Association) er en samling av organisasjoner som jobber med å tilby infrastruktur for datanett og tjenester til utdanning og forskning i Europa. TERENAs hovedmedlemmer er de nasjonale utdannings- og forskningsnettene i mange europeiske land og i tillegg noen land rundt Europa (eks. Nord-Afrika).

**UMA** (Unlicensed Mobile Access) er en standard for å transportere GSM-samtaler over IP-nett. UMA gir sømløs roaming av samtaler mellom IP og GSM. UMA er utviklet av UMAC (Unlicensed Mobile Access Consortium).

**Unicast** er sending fra en sender til en og bare en mottaker. Motstykket er broadcast som sender trafikk fra en sender til alle maskiner på et lokalnett. Nok en variant er **multicast** der mottaker er en gruppe maskiner.

**UNINETT CERT** (The Norwegian Network for Research Education Computer Emergency Response Team) er UNINETT's lokale **CERT** og ble etablert som tjeneste i 1995. Hovedtjenesten er å assistere UNINETT's kundeinstitusjoner i hvordan håndtere og undersøke hendelser som involverer en eller flere av våre kunder. Eksempel på hendelser er uønsket e-post, mistenkelig port-scanning, tjenestenektingsangrep (DoS), innbrudd etc.

**UPS** (Uninterruptable Power Supply) gir strøm forsynt fra batteribank. Selv om strøm fra e-verk forsvinner vil UPS-en opprettholde strøm inntil batteriene er utladet. «Online» UPS jevner også ut spenningsforskjeller.

**VLBI** (Very Long Baseline Interferometry) er en teknikk der større matriser av enkeltstående antenner samler inn data. Ved analyse av alle de enkeltstående målinger dannes et sammensatt bilde som blir større enn det som kan fanges med tradisjonelle teleskop. VLBI genererer enorme datamengder.

**VRRP** (Virtual Router Redundancy Protocol) er en standard som tillater en alternativ ruter å betjene et lokalnett dersom den primære svikter. HSRP er en mye brukt Cisco-proprietær variant av VRRP.


**Wi-Fi** (Wireless Fidelity) er en sertifisering som sikrer at produkter overholder **IEEE 802.11**-standardene (a/b/g) for trådløse nett.

**Wiki** er et nettsted som tillater alle brukere å legge til og editere innhold og struktur. Wiki er egnet som et medium for samarbeid rundt produksjon av dokumenter. Wikipedia er et stortilt bevis på at wiki fungerer.

**WiMax**: er en sertifisering som sikrer at produkter overholder IEEE 802.16-standarden for trådløse bredbåndsnett. Tiltent bruksområde var initielt bredbånd til distriktene, men man ser også at løsningen kan være interessant i byområder.

**WLAN** (Wireless Local Area Network) er trådløse nett.

**XMPP** (eXtensible Messaging and Presence Protocol) er en protokoll for å streame XML-elementer (RFC3921). Utgangspunkt i systemer for lynmeldinger



UNINETT AS  
NO-7465 Trondheim

Telefon: 73 55 79 00  
Faks: 73 55 79 01  
Besøksadresse: Abels gate 5  
Teknobyen  
Trondheim

E-post: [info@uninett.no](mailto:info@uninett.no)

[www.uninett.no](http://www.uninett.no)

Design: Tor Gjerde og Grete Duna  
Figurer: Tor Gjerde  
Layout og foto: Grete Duna  
Trykk: Tapir Uttrykk  
Opplag: 500

03/2006



UNINETT  
NO-7465 Trondheim  
[gigacampus@uninett.no](mailto:gigacampus@uninett.no)