

## **TTM4130 Suggested solution for regular Exam Spring 2007 (Sorry just in Nrowegian).**

### **TTM4130 Regulær eksamen vår 2007, forslag til løsning**

Under eksamen ble det opplyst at første oppgave ville telle ca 20 % og at de tre øvrige oppgavene ca like mye hver. (Ved karakterfastsetting brukte man følgende vekter: 27%, 27% og 26% på oppgave 2, 3 og 4).

#### **Oppgave 1 NGN**

##### **1.1 NGN: Hva forstår vi med det dette?**

**Omfatter det:**

- a. Emulering/samvirke med PSTN?**
- b. Funksjonalitet som beskrevet for IMS (som inngår i 3GPP)?**
- c. Aksessnettfunksjonalitet og terminalutstyrfunksjoner?**

Tolkningen av denne oppgaven ble kommentert under eksamen, det ble klart sagt at **både** a, b og c kunne inngå (man skulle ikke nødvendigvis velge bort 2 av dem).

Neste generasjons nett: En IP basert nettarkitektur. Denne arkitekturen utarbeides av ITU-T, ETSI (I TISPAN) og flere. Arkitekturen omfatter (beskriver blant annet):

- a. Emulering/samvirke med PSTN
- b. Funksjonalitet som beskrevet for IMS (som inngår i 3GPP), - man arbeider aktivt med å "harmonisere" eller inkludere IMS inn i NGN (TISPAN- 3GPP samarbeid)
- c. Aksessnettfunksjonalitet og terminalutstyrfunksjoner (nettfunksjonelle grupper i TISPAN dekker også disse).

Jeg synes godt man kan henviser til internasjonalt standardiseringsarbeid i besvarelsen, ikke bare til et "generisk begrep".

##### **1.2 TISPAN/TIPHON referansemodell for applikasjonsplan for IP telefoni har 5 nivå, som illustrert i figur 14.2 (gjengitt bakerst i oppgavesettet). Beskriv hvilke funksjoner som inngår i**

###### **a. Tjenestestyringslaget henholdsvis**

Tjenestestyringslag (Funksjonslag for tjenestestyring).

Dette laget sørger for to klasser av funksjonalitet:

- administrasjon av registreringer og
- sesjonstøtte

For å administrere registreringene trengs mulighet for å realisere følgende funksjonalitet:

- mottak av informasjon fra terminal om bruker etterfulgt av generert forespørsel om autentisering fra eget eller et fjerntliggende tjenestefunksjonslag.
- behandling av svar fra tjenestefunksjonslaget og generering av autorisasjonssertifikater eller - tillatelser som lagres i brukerens terminal. Slike tillatelser blir brukt sammen med sesjonsforespørsler. På engelsk kalles dette

en "ticket", dvs billett. en foreslår innført billett som norsk oversetting (billett: et "bevis" for en rettighet, f.eks. flybillett, teaterbillett osv.). og så eventuelt en beskrivelse av hva som må til for sesjonsstøtte

## **b. Lag for sesjonsstyring**

Disse funksjoner skal vedlikeholde betingelsene rundt en sesjon (sesjonens eller oppsetningens kontekst). Sesjonens kontekst gjør det mulig for bærerstyringslaget å opprette forbindelser med den tjenestekvalitet som brukeren spør etter (i følge regler gitt av tjenesteleverandør). For å kunne utføre disse oppgavene, kan laget komme til å behøve hjelp fra tjenestestyringslaget.

Laget har følgende funksjon:

<b>Funksjon for sesjonsstyring (CC= Call Control)</b>	Denne funksjon finnes i enhver nettfunksjonell gruppe. Den vedlikeholder sesjonstilstanden (oppsetningstilstanden).
---	---

### **1.3 Diskuter essensielle problemstillinger som inngår ved telefoni samtrafikk mellom et IP basert telenett og et linjesvitsjet (tradisjonelt nett). Illustrer diskusjonen med en skisse, som viser nødvendige funksjoner.**

Ved samtrafikk mellom disse nettene må man for de medieformene som overføres (f.eks. tale eller lyd) oversette kodingsform og overføringsformat (kodningen av tale **kan** være den samme, f.eks. PCM i begge nett, men i NGN forutsettes i alle fall IP (internett) pakksvitsjet overføringsformat, mens man i PST/ISDN benytter linjesvitsjing). I tillegg må man oversette mellom signaleringssystemene (f.eks. SIP og SS7), og samt avgjøre passende overgangspunkt mellom nettene.

## **Oppgave 2 SIP og H323**

**2.1 SIP: Hva er det og hva er det ikke?** SIP (Session Initiation Protocol) er primært et signaleringssystem for å sette opp, modifisere og terminere sesjoner (dvs. "samtaler") i et IP nett. SIP er **IKKE** en medieoverføringsprotokoll. Informasjon mellom brukerne "under samtale" benytter ikke SIP, men f.eks. RTP.

### **2.2 Hvilken forskjell er det på en SIP redirect server og en SIP proxy.**

En SIP server er en datamaskin (eller tjenerfunksjon på en datamaskin). En SIP redirect server svarer kun på henvendelser ved å sende ny informasjon (i form av en ny nett-adresse tilbake): Eks. Sende en INVITE melding til en SIP redirect server. Vil få et svar tilbake med "Ikke her, men prøv istedenfor adresse YYY som vil bringe deg nærmere målet". En redirect server trenger ikke mye "tilstandslogikk"- En SIP proxy er en SIP server, som behandler forespørselen "på vegne av" den som spør. Den kan eventuelt spørre videre i systemet og sender svar tilbake når den har kommet så langt det lar seg gjøre. Den må derfor ha noe mere tilstandslogikk (for å kunne koble sammen svar den får fra nettet, med de forespørsler som er sendt ut, og for selv å kunne svar tilbake til den som

spurte). Sammenhengen mellom ”redirect” og ”proxy” er omtrent som mellom iterativ og rekursive virkemåte i DNS.

- 2.3 En ren SIP proxy: Kjenner den til pågående samtaler?** Nei, den husker bare signaleringsinformasjon lenge nok til den har fått sendt endelig svar.
- 2.4 Hvilke SIP baserte servere i IMS kjenner pågående samtaler: P-CSCF (Proxy – Call Session Control Function), I-CSCF (Interrogation – CSCF) og/eller S-CSCF (Serving-CSCF)?** Ideelt sett er det kun S-CSCF som kjenner pågående samtaler: Tjenestestyring og avregningsfunksjoner er lagt til S-CSCF, som ligger i abonnentens hjemmenett. De andre serverne trenger ikke ha noe ”tilstandsbilde” av en pågående samtale. (Men for nødsamtaler kan P-CSCF eller i alle fall en proxy i det nettet der man oppholder seg være ”serving” dvs. betjenende node.) I spesifikasjonen sies det også at P-CSCF skal kunne generere CDRer. Skal dette gjelde noe annet et registrering av ”start” så må P-CSCF også kjenne en pågående samtale-
- 2.5 Hva er en (H323) Gatekeeper?** Det er en ”server” i H323 arkitekturen. Den representerer signaleringsfunksjonene i IP telefonsentralen inklusive registreringsfunksjoner, AAA funksjonalitet, ruting etc. (I SIP arkitekturen blir tilsvarende funksjoner delt på flere ”servere”)
- 2.6 Hva slags metodikk/teknikk/oppskrift brukes for å strukturere innholdet i henholdsvis:**  
**SIP meldinger og H323 meldinger?**  
**Karakteriser/diskuter fordeler og ulemper med SIP måten og H323 måten å gjøre ting på.** Meldingsinnholdet i SIP meldinger beskrives (normalt) som angitt i SDP (Session Description Protocol), dette er en teksbasert metode. Parametrene er ”leselige”/tolkbare for en programmerer. Men metoden er ikke effektiv med hensyn på overføringskapasitet, og meldingene kan være uøkonomisk utformet med hensyn på maskinell tolkning. Meldingsinnholdet i H323 er strukturert og kodet i følge ASN.1. Dette gir en effektiv koding med hensyn på overføringskapasitet og maskinell tolkning. Innholdet blir imidlertid lite ”tilgjengelig” underveis, det blir nærmest ”kryptert”.

### **Oppgave 3 Nummer, adresser, identiteter, navn**

- 3.1 Forklar følgende begreper og hvordan de eventuelt henger sammen.: Nummer, adresser, identiteter, navn.**

**Forklar følgende begreper:**

<b>TMSI:</b>	<b>Temporary Mobile Subscriber Identity og</b>
<b>TLLI:</b>	<b>Temporary Logical Link Identity</b>
<b>MSISDN:</b>	<b>Mobile Station International PSTN/ISDN Number</b>
<b>MSRN:</b>	<b>Mobile Station Roaming Number</b>
<b>IMEI:</b>	<b>International Mobile Equipment Identity</b>

**Kommenter også hvorfor noe heter ”Number” og andre ting ”Identity” her.**

**Prøv også å illustrere strukturen (oppbygningen) for hvert begrep (vis hvilke datafelt som inngår).**

I denne sammenheng oppfattet vanligvis "nummer" (i betydning telefonnummer) som en adresse. Eks. 73 59 50 00 er adressen eller telefonnummeret til NTNUs sentralbord. Slike nummer- eller adressesystemer er som regel hierarkisk bygd opp. En adresse er en informasjon for å kunne finne fram til noe. En identitet er en betegnelse gitt til en forekomst av "noe". Man tilstreber ofte at identiteten skal være "entydig" i den sammenhengen den blir brukt. Et personnummer kan sees på som eksempel på en identitet. Et navn kan generelt sett ikke brukes til adressering. Det har også vanligvis en litt mer uformell bruk (flere ting eller personer kan hete det samme). Men i Internett har man etablert et hierarkis **navnesystem**, DNS dette er strukturert. Et fullstendig oppgitt DNS navn representerer en (IP) adresse. For TMSI osv. Se kompendiet side xxx

**3.2 Forklar og illustrer med skisse/meldingssekvensdiagram hvordan et utstyr kan skaffe etablere en gyldig IPv6 adresse ved å benytte "Stateless Autoconfiguration".** Hint (har ikke tegnet diagrammet): Først lytte på nettet etter "ruter annonsering" (eller etterspørre en slik selv). Da får man vite MAC adresse til (en) ruter samt kan lese seg til "network prefix". Ut fra av network prefix og egen MAC adresse kan man så utlede sin egen gyldige IP adresse for det nettet man oppholder seg i. For sikkerhets skyld sjekkes det om noen andre enheter kan ha fått den samme adressene (f.eks. satt manuelt). Dette gjøres ved å sende ut forespørsel til "til alle lokalt" om noen har denne adressen. Hvis adressen er unik, er den gyldig og kan brukes.

**3.3 Hva er grunnen til at man for Ipv6 gjennomgående snakker om adresser for grensesnitt ("interfaces") og ikke vertsmaskiner (hosts)?** I IPv6 regner man med at hver vertsmaskin kan ha mange nett-grensesnitt (dette blir en etter hvert en realistisk modell).

**3.4 Prøv å forklare følgende begrep:**

- **Unikast adresse** En adresse som peker på en bestemt mottaker
- **Loop-back adresse** En adresse som peker tilbake på det samme utstyret (en melding med en slik adresse vil ikke synes på det lokale nettet, men vil internt bli "loopet" fra en prosess til en annen prosess på den samme datamaskinen.
- **Alle noder linklokalt adresse.** En adresse som alle noder på samme link (i samme lokalnett) skal kunne reagere på. Alle lokale noder skal lese/motta disse meldingene.
- **Anykast adresse.** En adresse som vanligvis benyttes for å "adressere" en funksjon. Samme format som en unikast adresse. Anykast adressene tolkes lokalt innen sitt definisjonsområde. Eks. Man kan etterspørre en HA i et gitt domene, men

dette domenet kan (av lasthensyn eller for å lage et sikrere nett) ha flere HAer. Det er da "Boarder Router" mot dette domenet som må (om)tolke en anykast adresse til en spesiell (velegnet) unikast adresse, for å rute meldingen til et fornuftig sted. (Avsender og nettet forøvrig trenger ikke vite at dette er en anykast adresse). Omtolkningen medfører imidlertid en del løpende administrasjon (finne ut hvilke serverer som er aktive nå, osv.). Anykast i følge WIKIPEDIA: Anycast is a network addressing and routing scheme whereby data is routed to the "nearest" or "best" destination as viewed by the routing topology.

Forklar også hvorfor de er definert (hva de kan brukes til).

**4 Prøv å liste opp hvilke destinasjonsadresser en (Ipv6) ruter skal kunne gjenkjenne (en komplett liste består av 9 punkter, du får full score om du greier 6 av disse).**

- 1 Foreskrevne linklokale adresser (for alle grensesnitt)
- 2 Enhver unikast- eller anykastadresse som har blitt konfigurert for nodens grensesnitt (manuelt eller automatisk)
- 3 Loopbackadressen,
- 4 "Alle (lokale-)noder" multikastadresser som definert foran
- 5 Resulterende "Etterspurt nodes multikastadresse" for alle slike adresser som kan dannes ut fra nodens tilordnede uni- og anykastadresser
- 6 Multikastadresser for alle andre grupper som noden tilhører

En **ruter** må kunne gjenkjenne alle de adresser som en vertsmaskin skal kunne gjenkjenne, pluss følgende typer:

- 7 Subnet-ruter anykastadressene for alle grensesnitt hvor den virker som en ruter.
- 8 Alle andre anykastadresser som ruterens har blitt konfigurert for
- 9 "Alle-(lokale-)rutere" multikastadresser, som definert foran.

#### **Oppgave 4 Mobilitetshåndtering**

**Innen mobilitetshåndtering har man (blant annet) følgende essensielle problemstillinger som må løses:**

1. **Hvordan finne adressen/ruten til en mobil bruker.**
2. **Hvordan gi en mobil bruker adgang til nettressurser på et nytt sted.**
3. **Hvordan sikre kontinuitet/avbruddsfrihet under bevegelse.**

**4.1 Forutsett at vi anvender SIP direkte (i IETF eller ”Internet” utgaven),  
a. Hvilke 2 problemstillingene (nevnt ovenfor) lar seg (enkelt) løse, og  
hvordan (skisser og forklar)?**

Legg merke til at det står SIP i IETF utgave (man skal altså IKKE løse denne oppgaven ved hjelp av mobil IP eller ved hjelp av enheter forskrevet i 3GPP (f.eks. er referanser til IMSI, HSS osv. helt irrelevante).

**Problemstilling 1** lar seg enkelt løse. Man bruker domenenavnet i brukers adresse for å finne fram til mottakers ”hjemme-SIP server”. Denne serveren slår opp i ”Location server”, for å finne ut IP adressen til den maskin brukeren er logget på nå. Når brukeren flytter seg foretas det en ”location update” i Location server.

**Problemstilling 2** lar seg vel egentlig **IKKE** så enkelt løse i SIP alene (Men dette hadde faglærer tenkt, dessverre er **påstand i 4.1 feil! – Det skulle ha stått .... adgang til tjenesten på et nytt sted (ikke nettressurser)**). For å gi brukeren adgang til nettresseruser på nytt sted, må brukeren autentiseres og autoriseres og dette er funksjoner som ligger på lavere lag (ikke på applikasjonslaget hvor SIP hører hjemme). SIP sikrer heller ikke avbruddsfrihet (uten tilleggsfunksjoner). Men SIP håndterer diskret (nomadisk) mobilitet bra. Brukeren vil imidlertid få umiddelbart tilgang til ”tjenesten” SIP hvis hun på et nytt sted finner et ”åpent” internett. Hun kan da bruke sin egen hjemmeserver.

**b. Utarbeid et forslag et system som også tar vare på den siste problemstillingen, og formuler forutsetninger for at dette skal virke.**

Kontinuitet under bevegelse kan sikres ved å lage et ”make before break” system. Mottaker må da være i stand til å kaste eventuell dublerede pakker med nytteinformasjon. En annen måte er at den ruter man forlater ”ettersender” trafikken som ankommer etter at brukeren har flyttet på seg. Denne ruter må da få vite den nye adressen. Slike ettersendelseskjema kan ”time” ut nokså snart etter en flytting. Slike skjema kan virke bra hvis tidsforsinkelsen ikke er for store. Og er relativt enkelt å administrerer lokalt hvis man har legger opp til en hierarkisk (2 nivå) administrasjon av mobilitet, der lokale flyttinger kan ”skjules” for korrespondenten.

**På grunn av faglæres feilantagelse har man også honorert svar som angir at Problemstilling 1 og 3 lar seg løse, og som angir løsning på problemstilling nr 2 under b – hvis diskusjonen, argumenteringen er fornuftig og god! Imidlertid gir man ikke særlig kreditt til løsninger som anvender mobil IP (det står SIP!).**

4.2 SIP i 3GPP utgave benytter en type SIP serverfunksjon kalt ”Call Session Control Function” (CSCF). Denne serverfunksjonen finnes i 3 utgaver kalt henholdsvis P-CSCF, I-CSCF og S-CSCF. Beskriv egenskapene til /hensikten med hver av disse.

4.3 Hvilke forskjeller ser du mellom følgende begreper (ta hvert punkt for seg)

- a. ”brukermobilitet” henholdsvis ”terminalmobilitet”
- b. ”horisontal handover” og ”vertikal handover”(den siste kalles også ofte for ”heterogen handover”).
- c. ”nomadisk mobilitet” og ”kontinuerlig mobilitet”.

4.4 Diskuter hvordan realisering av sikkerhetsaspektene kan forårsake problemer ved samtidig realisering av løsning på nr. 2 og 3 av de essensielle problemstillingene