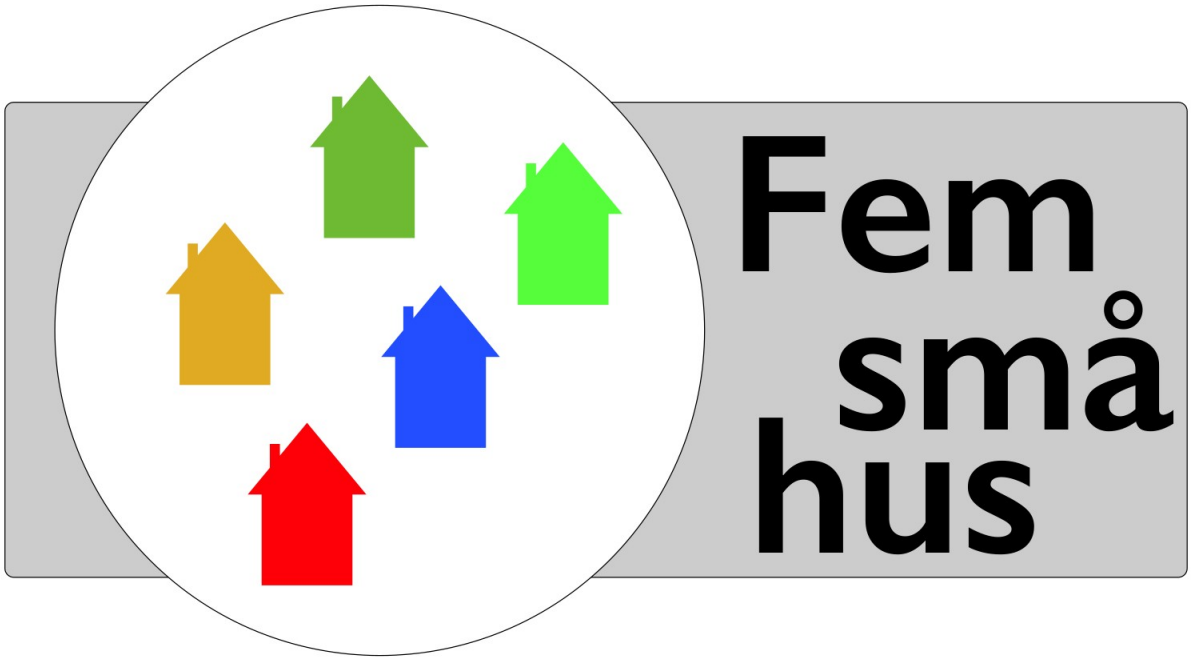
TU
STIFTELSEN



Kommunikationsarkitektur för samhället

Del 2: Målbild, översikt, grundläggande krav och principer, organisation

Version 2.0

Fem små hus presenteras i tre dokument:

- Del 1. Sammanfattning
- Del 2. Målbild, översikt, grundläggande krav och principer, organisation
- Del 3. Teknisk specifikation

Innehåll

Inledning

De senaste decennierna har internet utvecklats till en infrastruktur av samma dignitet som elektricitet, vatten, avlopp, telefoni, järnväg och vägnät. Den gemensamma svenska nationella IT-infrastrukturen används inte bara för konsumentorienterade tjänster, utan även för tjänster som är kritiska för företag, myndigheter och samhället i övrigt. Internet och internetteknologi är med andra ord en förutsättning för att vårt moderna samhälle ska fungera. Mobiltelefoninät har utvecklats från rena telefonnät till att huvudsakligen utgöra accessnät till internet. Med undantag för de radiobaserade delarna mellan antennmast och mobilterminal använder mobilnäten i hög grad samma fiberinfrastruktur som resterande delar av internet i Sverige. I vissa fall delas, utöver den fysiska fiberförbindelsen, även den trafikförmedlande utrustningen mellan internet, mobilnät och ”privata nät”.

Sverige har sett en snabb utbyggnad av mer eller mindre genomtänkta lösningar. De som byggde de nuvarande lösningarna saknade i vissa fall erforderlig erfarenhet eller drevs och begränsades i vad som kunde byggas av faktorer utanför de rent tekniska. Resultatet är ett nät som inte uppfyller dagens krav på transparens, neutralitet, robusthet, uthållighet och redundans.

Målet med Fem små hus är att inom ramen för internetarkitekturen skapa en infrastruktur i Sverige som ska ge maximal uthållighet kombinerad med en neutral och öppen decentraliserad fysisk infrastruktur (de fem husen). Infrastrukturen ska säkerställa att den så kallade ändpunktsprincipen följs för alla användare. Den nya infrastrukturen kommer också stödja utveckling och etablering av distribuerade och redundanta tjänster och funktioner med fokus på ett modernt IP-lager med IPv6.

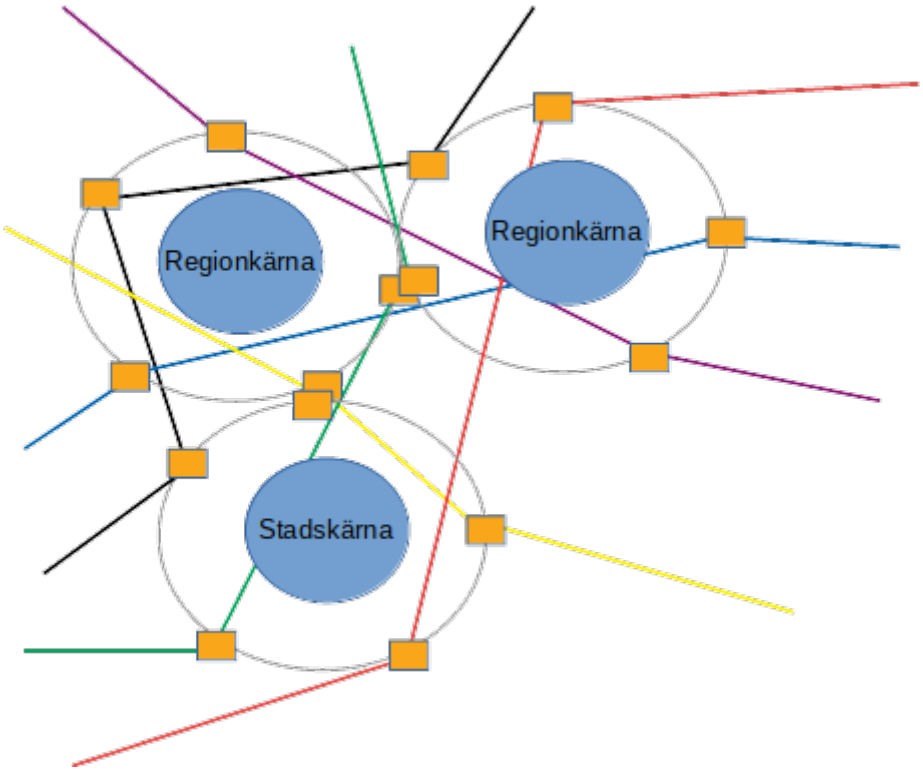
Fem små hus tar ett samlat grepp om existerande behov ur ett samhällsperspektiv och drar nytta av många av de välbeprövade funktioner som utvecklats inom internetarkitekturen sedan dess visionära början.

Data för de flesta tjänster som mobilanvändare använder transporteras via det fasta publika internet. Finansiella tjänster, livs- och drivmedelsförsörjning, sjukvård, larmsystem, elnät och andra kritiska samhällstjänster drabbas snabbt av störningar när internet slutar att fungera. Det är därför viktigt att Sverige har en IT-infrastruktur som är decentraliserad på alla nivåer och som är både robust och säker – även vad gäller drift och underhåll. Oavsett var man befinner sig i landet ska det finnas tillgång till stabil funktionalitet och tillräcklig bandbredd för alla behov, även när samhället och infrastrukturen är påfrestade.

Modellen kan ses som ett sätt att skapa och vidmakthålla ”beredskapslager” av elektronisk kommunikation. Som med alla färskvaror kommer lagren att behöva ”uppdateras” med jämna mellanrum. Kommunikationsberedskapen måste vara färsk, fungerande och redo att tas i bruk helt automatiskt alla dagar på året under alla tider.

Projektets byggstenar är enkla. Fem små hus placeras inom en region definierad som 60 000 – 120 000 användare och andra ändpunkter. Husen förbinds med varandra inom en husregion med redundanta svartfiberförbindelser. Regionens brukare kopplas till husen. Varje hus kopplas till en annan region med geografiskt skilda förbindelser. Figur 1 visar en bild av detta med tre förbundna husregioner. Förbindelser inom en husregion utgörs av redundant neutral svartfiber som tillhandahålls till de som har utrustning placerad i husen. Förbindelser mellan regioner organiseras på IPv6-nivå.

Funktionalitet och kapacitet upphandlas på IPv6-nivå, inklusive dynamisk routing och drift av de fem olika vägarna. Upphandlingen sker från fem eller fler olika operatörer. Reservkapacitet upphandlas på alla förbindelser så att en ensam fungerande väg kan ge fullgoda tjänster och prestanda till samtliga brukare inom en husregion.



Figur 1 Tre husregioner i en tänkt Fem små hus-infrastruktur. Varje region har fem hus som vart och ett har en oberoende koppling till ett hus i en annan husregion.

Infrastruktur byggd av kommersiella aktörer på deras villkor är nästan undantagslöst byggd för att ge acceptabel kundnöjdhet. Då kunderna i de flesta fall inte ställer några definierade och mätbara krav på funktion, prestanda eller tillgänglighet blir infrastrukturen bräcklig. Det är i allmänhet billigare för en kommersiell aktör att i efterhand be om ursäkt och ersätta drabbade kunder än att tillse att prestanda och hög tillgänglighet finns. Kommersiella aktörer

har dessutom ekonomiska incitament att centralisera många av sina nätfunktioner eller dela dem med andra operatörer. Det bidrar ytterligare till dålig redundans. Ur ett ekonomiskt perspektiv är sådana åtgärder rimliga. Ur ett samhällssäkerhetsperspektiv är de däremot mindre önskvärda, eller direkt skadliga.

Marknaden agerar snabbt och effektivt för att möta kundernas önskemål i syfte att exempelvis ta marknadsandelar och öka lönsamheten. Den är betydligt sämre på att lösa uppgifter som handlar om att ta helhetsansvar och värna kollektiva intressen, såsom en god krisberedskap. I vissa fall arbetar stora internationella aktörer aktivt för att montera ner den aktivitet som syftar till att vidmakthålla hela internets funktion i Sverige. Hela infrastrukturen för elektronisk kommunikation, inklusive samordningsfunktioner, är viktig och prioriterad. Den behöver därför adekvat skydd.

För att tillgodose hela samhällets krav på tillgängliga internettjänster skyddar Fem små hus-modellen mot både avsiktlig och oavsiktlig påverkan på infrastrukturen. Skydd mot påverkan från naturkatastrofer och annan oavsiktlig påverkan (exempelvis avgrävningar) sker genom tillräcklig mångfald och diversitet i infrastrukturens alla nivåer. Infrastrukturens utformning tillgodoser även skyddet mot avsiktlig påverkan. I det fallet är utformningen sådan att en motståndare eller angripare inte kan påverka funktionen i nätet nämnvärt utan en ansträngning som är uppenbart överflödig i förhållande till den skadeeffekt som erhålls.

Kommunikationsarkitektur

En kommunikationsarkitektur är ett sammanhållet system av funktioner som behövs för att etablera kommunikation mellan två ändsystem och stödja deras applikationer. En vanlig modell för att beskriva kommunikationsarkitektur är den så kallade OSI-modellen. Den beskriver sju lager av funktioner sammanlänkade för att åstadkomma kommunikation mellan två ändpunkters applikationer.

Kommunikationsarkitekturen OSI blev ej implementerad i verkligheten. Istället blev internetarkitekturen, även känd som TCP/IP, den globala infrastrukturen för elektronisk kommunikation. TCP/IP har bara fem definierade lager (se figur 2). System som inte är byggda på kompletta, korrekta och öppna arkitekturer är en återvändsgränd och måste undvikas för samhällsviktiga funktioner.

En viktig aspekt av internetarkitekturens utveckling till dagens möjligheter och applikationer är ändpunktsprincipen. Den innebär att nätet är symmetriskt: Vilket ändsystem som helst kan vara server och vilket ändsystem som helst kan vara klient. Det gjorde att Tim Berners-Lee inte behövde övertala alla internetoperatörer i världen att bygga ut sina tjänster och system för att kunna köra HTTP-protokollet, vilket är det som gör att webben fungerar.

Internetarkitekturen innehåller även de stödfunktioner som behövs för att applikationer ska kunna utvecklas utan att varje applikation eller användningsområde behöver skapa egna

lösningar för gemensamma problem. En sådan stödfunktion är domännamnssystemet DNS som är en distribuerad katalog för översättning av namn till IP-adresser och vice versa. DNS används även för andra funktioner som att lokalisera webb- och e-postserver för en viss domänadress eller översättning av telefonnummer till de parametrar som behövs för att etablera ett samtal över internet med protokollet SIP.

Övervakning, styrning och konfigurering av nätfunktioner sker med protokoll som exempelvis SNMP (simple network management protocol) och Netconf (network configuration protocol). Datamodeller beskrivs med modelleringsspråket Yang.

För krypterade förbindelser med TCP används vanligen TLS (transport layer security).

OSI-lager	**Namn**	**Internetmodellen**
(8)	Tjänst: BankID, Facebook, Webb	Ej del av internetspecifikation
7	Applikation	Applikation (HTTP)
6	Presentation	
5	Session	(TLS) System till system (TCP/UDP)
4	Transport	
3	Nätverk	Internet (IP)
2	Datalänk	Nätverksaccess[1] (Ethernet)
1	Fysiskt	

Figur 2 Jämförelse mellan OSI- och internetmodellerna. Lager 8 är ett tänkt tjänstelager som inte finns specificerat i modellerna.

I en förenklad beskrivning av hur internetarkitekturen byggs upp är grundfunktionen ett IP-paket som överförs från sändare till mottagare. Ett IP-paket kan vara endera version 4 (IPv4) eller version 6 (IPv6). Den största skillnaden mellan dessa är storleken på adressfältet. IPv4 använder 32-bitarsadresser och IPv6 128-bitarsadresser för avsändare och mottagare. IP-paket är fristående datagram och all information om vad det används till, inklusive funktioner som omsändning, feldetektering, felrättning och sekvensering görs av protokoll på högre lager.

Internets arkitektur förutsätter bara att lagren under IP-lagret förmedlar paket från avsändare till mottagare. Ingen information förutom själva IP paketet överförs till eller från de underliggande lagren. En implementation kan ha olika former av statistik tillgänglig för de

1Ej del av TCP/IP-arkitekturen, men det finns dokument från IETF som beskriver hur IP-paket kan transporteras med hjälp av en mängd olika media och metoder.

andra lagren, men hur den överförs till t.ex. SNMP är ospecificerat.

Målsättning

Fem små hus skapar en robust svensk infrastruktur för elektronisk kommunikation. Infrastrukturen är baserad på internet och ger stabil funktionalitet även om den utsätts för större avsiktlig eller oavsiktlig påverkan. Därigenom ger den möjlighet för användare (och deras applikationer) att alltid nå såväl andra användare som andra nätverksbaserade tjänster i Sverige. Samtidigt möjliggörs maximering av tillgången till kommunikation utanför landet.

Fem små hus-projektet möter behoven hos alla användare som följer internetarkitekturen korrekt. Användarna inkluderar statliga och kommunala myndigheter, operatörer, företag, föreningar och privatpersoner. Ett styrande krav i design och implementation är att normal funktionalitet för alla användare i så stor utsträckning som möjligt bibehålls vid störningar utan att t.ex. trafikprioriteringar sker. Trafikprioritering ökar risken för felaktiga konfigurationer och gör dessutom den prioriterade trafiktypen till ett attraktivt mål för, bland annat, olika former av överbelastningsattacker. Bastjänsten i Fem små hus är IPv6. Metoder för att överföra exempelvis IPv4 eller Ethernet över IPv6 finns redan idag standardiserade av IETF.

För användare med krav på enbart robust transport erbjuds redundant och säker funktion genom krypterad transport av lager 2-ramar över den beskrivna infrastrukturen. Den kan exempelvis användas för uppbyggnad av privata nät. Funktionen innefattar även stöd för, bland annat, hantering eller eliminering av överbelastningsattacker. Fördjupad information om denna funktion finns i del 3.

Målen realiseras genom en nätarkitektur avsedd att bibehålla avsedd funktion även vid flera samtidiga skador orsakade av exempelvis naturkatastrofer eller antagonistiska hot[2]. Den fysiska fiberinfrastrukturen anläggs på ett sätt som maximerar geografisk diversitet. I möjligaste mån undviks samförläggning med annan kritisk infrastruktur såsom elnät, vägar, järnvägar, broar och liknande. Minst två av de fem fiberdragningarna mellan regioner ska inte vara samförlagda med annan infrastruktur. Inom en husregion ska minst en av förbindelserna måste vara skild från annan infrastruktur.

Infrastrukturen delas in i husregioner där varje region betjänar 60 000 – 120 000 användare, d.v.s. hushåll, företag, mobilbasstationer eller andra anslutningar. Den valda storleken är en avvägning mellan önskad diversitet, det totala antalet hus, antal användare per region och förekomsten av samhällsviktiga funktioner som polis, brandkår m.m. I varje husregion finns fem hus som utgör ändpunkterna i den fysiska fiberinfrastrukturen. Ett hus omfattar byggnad med fysiskt skydd, kraftförsörjning, reservkraftförsörjning, klimat och EMP-skydd. I huset tillhandahålls plats för inplacering av den utrustning som krävs för att skapa robusthet. Varje

2Detta innefattar alla avsiktliga fysiska eller logiska angrepp på nätet – från enskilda brottsliga angrepp till krigshandlingar.

hus har två kanalisationsvägar för fiber till de fyra övriga husen i regionen samt en kanalisationsväg för förbindelse till en annan region. Husens placering i en region är sådan att fiberlängden från ett hus till ett annat hus typiskt ej överstiger 80 km. Det medger direkta fiberförbindelser utan förstärkning. Förbindelser med förstärkning skulle medföra att även förstärkningsutrustningen behöver förses med skydd och reservkraft – i praktiken ytterligare ett hus.

Varje hus har minst en fjärroperatör. Den är upphandlad för att driva infrastrukturen och installerar ändutrustning i form av en router med tillbehör för fjärrkommunikation med IPv6 över fiber till en annan husregion. Alla fem husoperatörers routrar i en husregion är kopplade i en alla-till-alla-konfiguration med två förläggningsvägar för varje par av husroutrar. Brukare i en region är kopplade till den operatör de är kunder hos. Lämpligen sker anslutningen via en router i ett eller flera av husen där deras operatör deltar i Fem små hus-arkitekturen. Därigenom får brukarna maximal redundans och tillgänglighet.

Ett hus är en operatörsneutral plats. De som uppfyller krav och riktlinjer för inplacering i ett hus skall kunna ställa in utrustning med enhetliga villkor för alla hus. Riktlinjer och villkor för inplacering i ett hus fastställs av kansliet och dess arbetsgrupper. Normalfallet är att man vid inplacering i ett hus erhåller ett tredjedels rack och får tillgång till två svartfiberpar via två skilda förläggningsvägar till de andra fyra husen i husregionen. Kraftförsörjningen utgörs av en trefasanslutning till den avbrottsfria kraften. Tillgänglig effekt beror på vilken effektklass aktuellt hus är dimensionerat för.

Varje hus förses med tjänster som tillser att lokal funktionalitet bibehålls om det skulle bli isolerat. Exempel på sådana tjänster är DNS, DNS-resolvrar, DHCP, gateway för IPv4 över IPv6, generell datorkapacitet (moln) och tid/takt.

Målsättningarna med Fem små hus begränsas till projektets egna infrastruktur. Tjänster som har externa komponenter omfattas inte av några tillgänglighetsgarantier. Infrastrukturen kan inte heller garantera funktion vid felaktig användning av internetarkitekturen.

Målsättningarna syftar till att alla resurser som behövs för att vidmakthålla funktion enligt de standarder som utgör grunden för internet skall finnas med redundans inom varje region. Under senare tid har det svenska publika internet drabbats av avbrott som tyder på att vissa funktioner centraliseras och sedan drabbats av driftavbrott. Detta är en oacceptabel konfiguration om man eftersträvar maximal uthållighet och funktion inom ett fåtal hopkopplade öar, vilket kan bli möjligt vid en större samhällspåfrestning.

IPv6

IPv6 kommer på lång sikt att till stor del ersätta IPv4 för det globala internet. Eftersom IPv6 använder 128-bitarsadresser kan alla slutanvändare och delar i infrastrukturen tilldelas egna globalt nåbara adresser. Detta är inte möjligt med IPv4 där adressutrymmet redan idag är fullt

allokerat. För att få IPv4 att fungera idag används adressöversättning (NAT), vilket innebär att flera ändsystem eller användare delar på en globalt adresserbar IPv4-adress. Denna teknik används både hos slutanvändare och i operatörsnät. Det omöjliggör individuell adressering av ändsystem och bryter därmed mot internetarkitekturens ändpunktsprincip.

För att hantera IPv4 i IPv6-nät finns flera standardiserade metoder för transport som kombinerar NAT med förpackning av IPv4 i IPv6. De kan med fördel användas av både fasta och mobila användare. En metod för att transportera IPv4 över IPv6 rekommenderas framför så kallad ”dual stack” för både fasta och mobila nät.

Sverige är idag ett av de sämsta länderna i Europa vad gäller att modernisera sin infrastruktur och införa IPv6. Fokus i det här förslaget ligger på IPv6 för att framtidssäkra infrastrukturen och fullt ut stödja internets ändpunktsprincip. Modellen kan användas för att fullt ut tillgodose dagens behov av IPv4-användning.

Ett modernt IPv6-nät ska kunna hantera paketstorlekar (IP MTU) upp till 9000 bytes mellan två ändpunkter.[3] Det ger möjlighet till högpresterande förbindelser såväl som goda möjligheter att förpacka andra protokoll och tjänster i IPv6-paket för transport över den gemensamma feltoleranta infrastrukturen.

Anslutning av stadsnät och mobilnät

De aktörer som finns i en husregion, exempelvis stadsnät och kommunikationsoperatörer, förväntas ansluta sig till alla fem hus i regionen med individuella fibrer så långt som möjligt. Inledningsvis kan man tänka sig att de placerar utrustning i ett hus och ansluter sin egen fiber dit. Därefter nyttjar aktören den gemensamma fiberinfrastrukturen mellan husen för att förbinda utrustning placerad i de andra fyra husen. När möjlighet ges kan den lokala aktören ansluta egen fiber även till de andra husen för att på så sätt förbättra sin redundans och uthållighet. Lokala operatörer behöver ingen egen utrustning i de fall de har egen fiber till flera hus. Den kan då anslutas direkt till fjärroperatörens utrustning.

Stadsnät förväntas att via husen ansluta sig till en eller flera av de fjärr- eller transitoperatörer som deltar i Fem små hus-arkitekturen. Operatörer som idag transporterar sina användares trafik för hantering på ett fåtal centrala platser i landet bör uppmuntras att placera sin nya utrustning i husen i samband med att de inför IPv6. Om de önskar behålla sin centrala hantering av IPv4 kan de ansluta kunderna dit genom att tunnla IPv4-paket eller lager 2-ramar över IPv6 med lämpligt protokoll.

I det fall en basstation i mobilnäten förlorar kontakten med sina kontrollerande nätelement, d.v.s. när normal funktion inte längre är möjlig, kan man låta den acceptera alla mobilterminaler för IPv6-trafik. Adresser delas då ut till användarna i husregionen genom basstationer med hjälp av stödfunktioner i husen. Husregionens DNS/DHCP-tjänster går också att använda. Detta gör att all IPv6-trafik fungerar – inklusive webbsurfning och telefoni via en SIP-klient.

Det skulle underlätta om mobiloperatörerna hade IPv6 som enda pakettjänst i sina nät, d.v.s. ingen ”dual stack”. IPv6 blir då den grundläggande bärarfunktionen och IPv4 en tjänst ovanpå detta.

Att ha IPv6 som bärartjänst för IPv4 borde vara ett grundkrav i licenserna för tilldelning av 5G-frekvenser. Licenser för mobila och fasta nät bör också kräva att operatörerna stödjer ändpunktsprincipen i internetarkitekturen med sina tjänster och sin infrastruktur för IPv6.

Fem små hus-projektet fokuserar på det nationella nätet och tjänsterna som levereras i och i anslutning till husen. Senare projekt behöva hantera frågan om access inom regionerna, samt krav och profiler för tjänster till alla slutanvändare, såväl fasta som mobila.

Organisation

Ett kansli organiseras för att tillhandahålla teknisk referenslitteratur, dokumentation, mötesprotokoll med mera. All information hålls organiserad och publikt tillgänglig. Representanter från kansliet deltar i arbetsgrupper och möten för att ge stöd till genomförande, logistik och dokumentation. Genom kansliet anordnas regelbundna kurser och utbildningar. Det certifierar också personal som arbetar inom infrastrukturen. Slutligen administrerar kansliet återkommande funktionstester vid varje husregion.

TU-stiftelsen kan initialt tillhandahålla expertis för kansliet. Därigenom tillvaratas erfarenheter från framtagandet av detta dokument.

Kansliet organiserar till att börja med arbetsgrupper för följande områden:

- Fiberplanering, -utbyggnad, m.m.
- Routing mellan olika delar av Fem små hus.
- Autentiseringsmekanismer för utrustning, applikationer och personal.
- Driftrutiner mellan operatörer och andra ansvariga för infrastrukturens kritiska komponenter.
- Funktioner och tjänster i hus samt regler för husens användning.
- Verktyg och procedurer för konfigurering och övervakning.
- Drift av hus och husregioner: el, kyla, fastighet, säkerhet, fiberförbindelser etc.
- Användare av infrastrukturen för Ethernet-transport.
- Rutiner för felsökning och omstrukturering av nätelement i händelse av utslagning.
- Infrastrukturanvändare, referensgrupp.

En referensgrupp för användande av infrastrukturen bör organiseras med representanter från operatörer, stora användare, publika användare, andra aktörer samt relevanta myndigheter.

För projektet skapas en miljö för prov, försök och utbildning. Den är utrustad för att kunna testa olika trafikfall, utrustning och routingkonfigurationer. För underhåll av testmiljön finns driftpersonal knuten till kansliet. Det ska vara möjligt för alla som är inblandade i infrastrukturen att boka testmiljön för att genomföra egna prov och försök. Möjligheten att samordna testmiljön med högskoleresurser och -utbildning bör undersökas.

Den som önskar använda testmiljön ansöker om detta till kansliet med en beskrivning av önskade tester, utrustningsbehov, konfigurering och önskat resultat. Efter avslutade tester ska användaren skriva en utvärderingsrapport som tillsänds kansliet.

För underhåll av hus avseende byggnad, elverk, kyla, vvs, passagekontrollsystem, bränsleförråd m.m. ordnas avtal med geografiskt skilda lokala leverantörer.

Operatörer

För att få effektiv och målmedveten produktion måste det gå att mäta och utvärdera det som produceras. Det måste också finnas alternativ att byta till i det fall man inte uppnår de uppsatta kraven i en ”produktionslina”. Eftersom ingen kan driva en perfekt infrastruktur måste det finnas redundans på alla nivåer, från kanalisationsförläggning till ledningen för respektive organisation. Det är också viktigt att ha viss diversitet i byggsätt, processer och metoder samt val av utrustning. Av dessa anledningar är det viktigt att flera operatörer gemensamt bidrar till att bygga upp infrastrukturen individuellt.

Från en operatör som sammanbinder husregioner upphandlas:

- Tillgänglighet för ”befordran av IPv6-paket”.
- Genomströmningsprestanda som motsvarar de fyra andra operatörernas trafik.
- Deltagande i gemensamma utbildnings- och utvärderingsprojekt.
- Leverans av drift- och trafikstatistik för den upphandlade reservfunktionen.
- Rapporter av backup- och trafikbehov från alla husregioner till kansliet var sjätte månad.
- Regelbundna uppdateringar av programvara och säkerhet.
- Representation i relevanta arbetsgrupper för t.ex routing och driftfrågor inom den gemensamma infrastrukturen.
- Sammankoppling och drift med övriga fjärroperatörers husroutrar inom en husregion.

Förläggning och tillhandahållande av svartfiber mellan hus i en region är en del av etableringen av husen. Förbindelserna mellan husregionerna är en del av den upphandlade IPv6-kapaciteten. Ytterligare utredning krävs rörande tillgång för andra aktörer till fiber som nyförläggs mellan regioner inom ramen för detta projekt.

Betalningsmodell

- Kostnaden för redundans utöver operatörens behov för ”normaldrift” täcks med samhällsmedel.
- Operatören förväntas bära sina egna kostnader för de nätresurser denne behöver för sin ”normaldrift”.
- Reservkapacitet, vilket kan innefatta uppdraget att bygga nya fiberstråk, upphandlas genom statens försorg.
- För trafik som använder reservvägar under en period av ”normaldrift” debiteras en kostnad, från ansvarig myndighet, som är satt så att kostnaden att föra trafiken i operatörens egna nät är lägre.

Infrastruktur med särskilda krav

Fem små hus-arkitekturen medger en samling av olika organisationers verksamhetskritiska nät. Det finns flera möjliga orsaker till att en organisation vill ha ett eget intranät. De vanligaste är tillgänglighet, skydd mot obehörig trafik, skydd mot avlyssning och skydd mot överbelastningsattacker. Ett exempel är det myndighetsgemensamma intranätet SGSI.

Existerande nät av denna typ är i dagsläget implementerade med en flora av olika tekniker, t.ex. hyrd fast anslutning, frame relay, ATM eller MPLS. Att bygga separata infrastrukturer för varje verksamhetskritiskt nät ökar den totala kostnaden för samhället eftersom vart och ett av dessa behöver, mer eller mindre, kopiera Fem små hus-modellen.

Fem små hus-infrastrukturen levererar Ethernet-transport via krypto för nät med särskilda krav där Ethernet är gemensam anslutningstyp. Alla typer av ramar och protokoll kan förmedlas upp till en maximal storlek (MTU) på 8192 bytes.

Tillgänglighet, uttrycks normalt som ett procenttal. En populär specifikation är ”five nines”, eller 99,999%. Det innebär att den sammanlagda avbrottstiden under ett år inte ska överstiga 315 sekunder, d.v.s. något mer än fem minuter. Vissa operatörer räknar endast tillgänglighet under kontorstid, vilket är viktigt att ta i beaktande när man jämför tillgänglighetsgarantier. Fem små hus tillgänglighet kommer att överstiga alla på marknaden förekommande alternativ. Avbrott, när paket inte befordras från sändare till mottagare, ska vara max tio stycken per 24-timmarsperiod. Inga avbrott får vara längre än 200 ms.

I Fem små hus-infrastrukturen åstadkoms skydd mot obehörig trafik, avlyssning och överbelastningsattacker med ett särskilt framtaget kryptosystem. Kraven på kryptoalgoritmer och nyckelhantering bestäms av respektive användarorganisation. Kryptosystemet åstadkommer skydd mot överbelastningsattacker med hjälp av dynamisk routing och av IETF specificerade metoder. Närmare tekniska krav på kryptoutrustningens funktionalitet finns i den tekniska bilagan.

Telefoni och nödsamtal

Det nuvarande telefonisystemet kommer att behöva omstruktureras så att det använder internetarkitekturen som bas. Katalogsystemet DNS används då för att översätta telefonnummer till ändpunkter på internet. I och med denna övergång uppstår nya möjligheter. I normal drift går det att låta husregionernas DNS-resolverinfrastruktur peka på ordinarie ändpunkter för samhällstjänster som exempelvis 112. Om en region förlorar all kontakt med SOS Alarm kan trafiken dirigeras om automatiskt till lokal brandkår, polis eller liknande. Den nya mottagaren kan sedan vidarebefordra hjälpbehoven till lokal insatsorganisation eller använda egna resurser.

Vidmakthållande av kunskap och övning

- Grundutbildning av användare av infrastrukturen och de som producerar infrastrukturen.
- Nyutveckling. Revidera specifikationen för hela systemet var tredje år. Revideringen föregås av studie och test. Samla in önskemål från operatörer och användare om vad de ser behov av i nästa period.
- Upparbetade relationer med leverantörer som gör att vi har vägar för felrapportering och uppdatering.

Generell metod för autentisering

En generell metod för autentisering av alla komponenter i infrastrukturen behöver utvecklas. Den måste vara utformad så att funktionen kan upprätthållas på ett säkert sätt ner till ett fristående ensamt hus. Kraven skiljer sig väsentligt från dagens populära kommersiella produkter som förutsätter fungerande realtidskommunikation.

Övervakning

- Operatörernas användning av reservkapaciteten under normalförhållanden övervakas och debiteras.
- Nätets styrinformation, både statisk och dynamisk, rimlighetskontrolleras och valideras mot en dokumenterad referensmodell.
- Felaktig trafik till olika kritiska nättjänster och användare utvärderas för att identifiera eventuell spår av attacker etc.
- Svårt att få en komplett bild utan att få routingen från operatörerna, vilket inte är önskvärt.
- Larm, skalskydd, kraft, kyla, miljö, tillträde.

Förkortningslista

Förkortning	**Förklaring**	**Standard**
ATM	Asynchronous Transfer Mode	
BCP	Best Current Practice	
DEC	Digital Equipment Corporation	
DHCP	Dynamic Host Configuration Protocol	RFC 2131
DNS	Domain Name System	RFC 1034
DOCSIS	Data Over Cable Service Interface Specification	
DSL	Digital Subscriber Line	
E.164	Internationell standard för telefonnummer	
Ethernet		
HDLC	High-Level Data Link Control	ISO/IEC 13239:2002
HTTP	Hypertext Transfer Protocol	RFC 7230
IBM	International Business Machines	
IETF	Internet Engineering Task Force	
IP	Internet Protocol	
IPv4	Internet Protocol version 4	RFC 791
IPv6	Internet Protocol version 6	RFC 8200
IT	Informationsteknik	
MPLS	Multiprotocol Label Switching	RFC 3031
MTU	Maximum Transmission Unit	
NAT	Network Address Translation	RFC 2663
NetConf	Network Configuration Protocol	RFC 6241
NTP	Network Time Protocol	RFC 5905
OSI	Open Systems Interconnection	ISO 7498
Förkortning	**Förklaring**	**Standard**

PPP	Point-to-Point Protocol	RFC 1661
SGSI	Swedish Government Secure Intranet	
SIP	Session Initiation Protocol	RFC 3261
SNA	Systems Network Architecture	
SNMP	Simple Network Management Protocol	RFC 3411
TCP	Transmission Control Protocol	RFC 793
TLS	Transport Layer Security	RFC 8446
UDP	User Datagram Protocol	RFC 768

Referenser

BCP 39
RFC 1958 Architectural Principles of the Internet

Om TU-stiftelsen

Stiftelsen för telematikens utveckling, förkortat TU-stiftelsen, bildades 1996 och har som mål att arbeta för ett gemensamt internet i Sverige som klarar alla påfrestningar och tjänar som samhällets huvudsakliga kommunikationsinfrastruktur.

TU-stiftelsen äger Netnod som driver flera kritiska infrastrukturtjänster i den nordiska grenen av internet och delar ut stipendier till relevant forskning och utveckling inom dessa områden.

Författare

Dokumentet är framtaget av TU-stiftelsens arbetsgrupp för infrastruktur med deltagare från nätoperatörer, leverantörer och myndigheter. Deltagarna har inte representerat sina respektive organisation utan deltagit som experter. TU-stiftelsen tackar alla deltagare för sin medverkan och för dom resurser som ställts till gruppens förfogande i form av möteslokaler, databaser och andra typer av verktyg.

Upphovsrätt