Ref Fi2023/01693

fi.registrator@regeringskansliet.se
david.troeng@regeringskansliet.se

Synpunkter från Peter Löthberg

Jag har arbetat med Internet från 1983, varit med och byggt upp IP-nätverk för bland annat Sunet, Nordunet, Ebone, Tele2, Försvarsmakten samt det amerikanska telefonbolaget Sprint. Medverkade till etablerandet av den internationella knutpunkten MAE-East på 90-talet, det RIPE och var aktivt drivande i bildandet av de svenska stiftelserna IIS och TU-stiftelsen samt Netnod AB. Jag var den som övertygade Jon Postel om att en root-name-server skulle placeras i Sverige.

Utöver detta var jag arkitekt för den internationella delen av NSFnet. Jag var även teknisk arkitekt åt Cisco Systems Inc (1998-2010) och designade två generationers stamnätsroutrar åt dem.

Internet Engineering Task Force (IETF) är standardiseringsorganet för de kommunikations-protokoll som används på Internet. Där har jag varit aktiv sedan tidigt 90-tal. Särskilt kan nämnas routing-protokollet BGP4, där jag var aktivt drivande i utveckling och test.

2022 tilldelade Kungl Ingenjörsvetenskapsakademien (IVA) mig guldmedalj för mitt arbete med Internet.

För att framtidssäkra den svenska infrastrukturen gäller det att manövrera genom det kompakta minfältet av företag, organisationer och personer med olika egenintressen inom detta område. Det är helt klart att ingen representerar användarna och av förklarliga skäl saknar nästan alla i användarkategorin de detaljkunskaper som krävs för att kunna förutse olika åtgärders inverkan på framtiden. Ingen på ansvarigt håll verkar heller på allvar ha insett att mer och mer av samhällets funktioner, av alla kategorier från sjukvård till kommersiella företag, är helt beroende av en fungerande infrastruktur för elektronisk kommunikation.

I Sverige har vi lagar och regler för elsäkerhet, avloppshantering, sopsortering, etc., men när det gäller den elektroniska infrastrukturen så finner man att det är ett eftersatt område trots att det är så mycket som skulle sluta fungera om det blir allvarliga störningar.

Mina synpunkter är helt baserade på de tekniska förutsättningar som dikterar funktioner etc., utan hänsyn tagen till någon aktörs egenintresse. Fysikens lagar kan vi inte ändra på, bara anpassa oss efter.

Internet är ett symmetriskt nät där man kan representera alla ändpunkter med vad som kallas för en nivå-3 nät-adress. Fram till cirka 1995 kunde man göra detta med IPv4 och detta var basen för all utveckling av nya protokoll ovanpå IP och applikationer i dessa protokoll. World Wide Web (WWW) med kommunikationsprotokollen HTTP och HTTPS är inget annat än en applikation bland många andra, om än väldigt populär *just nu*. När det hade varit klokt att uppgradera hela Internet från IPv4 till IPv6 så att Internets generella funktion kunde bibehållas så valde marknaden att installera vad som kallas NAT (network address translation). Operatörerna gjorde det valet för att klara den då explosiva utökningen av antalet

användare i sina nät. Resultatet av deras val är att Internets grundläggande princip av änd-till-änd-kommunikation har gått helt förlorad för de allra flesta användare.

En liten historia: När Tim Berners-Lee designade den första versionen av HTTP protokollet för WWW var det existerande Internet (IPv4) byggt enligt Internets grundprincip (änd-till-änd) så det enda han behövde göra, för att alla skulle kunna såväl komma åt den webserver han satte upp som att sätta upp en egen, var att be Internet Assigned Numbers Authority (IANA) om ett protokollnummer för HTTP inom TCP. Hade han behövt övertyga all världens operatörer "att bygga ut för HTTP" hade det aldrig blivit något.

Under den tidsperioden skapades många av de grundfunktioner vi fortfarande är beroende av i baren under IETF-möten, många gånger skrevs det först på pappersservetter. T.ex den första versionen av BGP, som håller ihop världens Internet-routing, skapades av Kirk Logheed och Yakov Rekhter på 3 pappers-servetter. Paul Triana, Andrew Partan och jag förverkligade BGP version 4 i UUnet och Ebone och var världens första transkontinentala BGP4 routing-session.

Slutsats: Bygg en infrastruktur som inte bryr sig om vad som transporteras. Eftersom alla ändpunkter då måste ha en unik adress är det idag bara IPv6 som kan komma i fråga. Att utgå från hur de applikationer som tas fram i vår tid är designade är det största misstag man kan göra!

Kommentar: Dagens "IPv4 bredbands surf" blir en applikation över framtidens IPv6 infrastruktur. En fördel med en sådan modell är att man då kan välja godtycklig ”gateway” från användaren och därmed ha valfrihet i funktionalitet.

För framtiden behöver Sverige till att börja med en fungerande befordran av IPv6 paket till och från alla inom landet, oavsett paketens innehåll vad gäller protokoll och tjänst. Denna funktion måste vara "stateless" och symmetrisk och alltid på.

Redundans är en annan viktig faktor, det är ohållbart att olika organisationer skall bygga stuprör och andra "reservsystem" eller särskilda system för viss användargrupp, ur ett samhällsperspektiv får vi mycket bättre funktion och tillgänglighet genom att alla de resurser som idag spenderas kombineras på bästa sätt.

Blåljus, försvar, sjukvård, betalningar etc., kan ges tillräckligt god säkerhet genom kryptering. 100% tillgänglighet kan de få om det finns ett logiskt gemensamt IPv6-paket förmedlingsnät med aktiv dynamisk routing.

Vi bör vara beredda på att öar av användare kan bli isolerade och då gäller att vi på förväg placerat och strukturerat resurser så att de faktiskt kan leverera de grundfunktioner som behövs för att det ska fungera med betalningar, SOS-alarm, telefoni, information till medborgare, VMA etc.

En rimlig modell kan vara att dela in Sverige i t.ex. 100 områden (ca 60000 ändpunkter) med redundans inom området och lokala "front end tjänster" mot flera oberoende "back end tjänster" som kan agera oberoende av varandra för funktioner som betalningar, elektronisk identifiering etc., med minst en placerad i varje "försvarsområde".

En ”viktig tjänst” definieras helt på om de har fler än 5000 oberoende användare, detta innefattar även de undertjänster som en tjänst kan begära att användaren anropar.

För att säkra den svenska infrastrukturens funktionalitet och uthållighet måste man dela upp problemet i olika delmoment, där var och ett löser sin nivå i Internet-arkitekturen. Det är av största vikt att man *inte* blandar ihop nivåerna. Lösningarna måste fungera för alla som använder Internet, enligt dess specifikationer, *utan* att den gemensamma infrastrukturen har kännedom om enskilda användarfall.

- Elkraft (det måste någon annan ordna)
- Redundanta och diversifierad fysisk infrastruktur för nivåerna L1/L2
- Flera byggnader inom ett område som kan agera backup för varandra
- Befordran av alla sorters IPv6-paket
- Tillräcklig redundans med automatisk omkoppling på IPv6 L3-nivå med hjälp av IP-routing. ("Fem hus" från TU-stiftelsen är en bra start och en absolut miniminivå.)
- Redundanta stödsystem, DNS-server, DNS-resolver, DHCP för de som förlorat sin etc.
- Regler för hur tjänster skall utformas som har mer än 5000 användare, (exempel, ID-tjänster, banker, polis, regioner, kommuninfo, dvs. allt som behövs för att samhället skall fungera "som vanligt")
- Geografisk redundans för ovanstående tjänster samt att dessa skall kunna betjäna användarna även om de olika instanserna inte kan nå varandra
- Rekommendation och information till användarna
- Entydigt utpekade ansvariga för de olika delsystemen som ingår i svensk infrastruktur.
- Fortlöpande uppföljning och verifiering att uppsatta krav och funktioner fungerar.

Sist ett ord om "routing-säkerhet" eller RPKI (Resource Public Key Infrastructure).
Om RPKI används krävs att det finns en "PKI-validerare" mer eller mindre vid varje router och kontrollen över vad som finns i denna validerare och därmed är "godkända routes" ligger helt utanför svensk kontroll.

Man bör ha ett svenskt vägvalsregister "routing registry", som kan användas för att bygga routrarnas konfigurationer för destinationer inom landet och i första hand förlita sig på den informationen.

Svar på era frågor

Användning av konnektivitet och delaktighet?

En förutsättning är en bas-infrastruktur som stödjer en etablerad kommunikationsarkitektur på ISO-Nivå3, dvs. IPv6 paketförmedling.

Denna infrastruktur måste även vara redundant och uthållig mot såväl naturkatastrofer som aktivt sabotage. Att det är viktigt har såväl rysk aggression som översvämningar visat under det här året.

Alla tjänster och funktioner ska levereras via denna grundläggande infrastruktur.

Tillgång till digital infrastruktur

Man är inte "uppkopplad" i infrastrukturens nätelement, internet-arkitekturen bygger på "förbindelselös" förmedling av oberoende paket. Om man skall hålla reda på något, utöver den aggregerade mottagar-adressen, går det åt ytterligare resurser och extra onödig komplexitet.
I en korrekt konstruerad adressplan kan en post representera alla användare inom ett geografiskt område.
Mellan avsändare och mottagare i internet-arkitekturen kan t.ex. en "felrättande förbindelse" åstadkommas med protokollet TCP mellan två godtyckliga ändpunkter var som helst i infrastrukturen och initieras från godtycklig sida.

För att kunna använda infrastrukturen krävs sedan terminalutrustning samt applikationer för de protokoll som etableras.

Eftersom vi här avser framtidsäker så är det helt förkastligt att titta på dagens protokoll och applikationer för de kommer att förändras. Fokus måste ligga på nätets fullständiga transparens och uthållighet.

När jag läser era frågor blir jag lite alarmerad, det verkar som ni råkat blanda infrastruktur med applikationer etc., något som man till varje pris måste undvika för att vara framtidssäker.

Man måste titta på det som en komplett kommunikationsarkitektur, t.ex. OSI:s 7 lager även om IP bara har 5 lager, IVA har beskrivit det som "lasagne-princip". Man får inte göra saker som går mellan lagren, utan varje lager ska kunna bytas ut mot ett likvärdigt. Vertikalt integrerade tjänster är det sista vi behöver för framtiden.

Tyvärr så pratar och tänker ofta de traditionella tele-operatörerna och kanske främst deras leverantörer som t.ex. Ericsson i "tjänster", men det betyder bara att de vill ha större lönsamhet för sitt eget företag. Dessa intressen är ofta diametralt motsatta mot samhällets intressen.

Ett lysande exempel på att försöka radera ut Internet-arkitekturens flexibilitet är det som leverantörerna tog fram det som kallas IMS (integrated multimedia system). IMS innebär att

inför nätelementet SBC (session boarder controller), vilket stoppar all trafik som man inte hade ”prenumererat” på. Detta görs helt i strid med Internet-arkitekturen.

Under 2014-2017 studerade vi vid Deutsche Telekom hur man kunde bygga ett komplett nät på modernt sätt. Vi kom fram till att kostnaden för uppbyggnad, drift och underhåll var 4-7 gånger lägre för samma kapacitet, om man bara levererade paket i ett helt redundant nät. Dokumentationen tillhandahålls vid förfrågan.

Varje generation av mobilnäts-teknik (x-G) har hittills innehållit någon eller några få nya ”tjänster”, historien visar att de bara fördyrar systemen. Marknaden är bra på marknadsföring, främst från utrustnings-leverantör till tjänste-operatören vilka oftast lever i villfarelsen att de skall kunna skapa ”tjänster” för att få större inkomster samt dess personal vars jobb är att hantera den specifika utrustningskomponenten. Men vem vill egentligen ha en terminal som bara kan ett fåtal saker och inte går att uppgradera eller installera nya saker i (kommer ni ihåg Minitel)? I verkligheten så används ju mobilnäten med all sin (oftast helt onödiga) komplexitet som världens mest komplicerade Internetanslutning.

Kommentar: Kommer ni ihåg mobilutrustnings-leverantörernas försök i början att trasa sönder Internet med WAP. Allt det tog en ända med förskräckelse när Apple stoppade in ett Unix-operativsystem med en standard IP-protokollstack samt en browser i en telefon. Google gjorde sen likadant med Android.

Förutsättningar för utbyggnad av digital infrastruktur

Den extrema redundans och de lokala resurser som erfordras för att undvika ett större sammanbrott i samhället måste på något sätt dels finansieras och dels att dess funktion vidmakthålls med kontinuerlig uppföljning från samhållsresurser.

I det långa loppet blir det billigare för alla om man inte bygger privata strukturer för varje användare, myndighet eller applikation.

De flesta myndigheter pratar sällan med andra myndigheter utan nästan alltid med medborgare och andra funktioner i samhället. Myndigheternas huvuduppgift är normalt sett ge service till medborgarna. Detta kom Stattel-delegationen fram till i början av 1990-talet då man på Statskontoret utredde huruvida staten skulle ha ett eget telefon-nät.

Kommentar: Varför har vi ”SGSI” och inte ett krypto-VPN över gemensam infrastruktur och förstärkt lokal och regional koppling mot övriga samhället?

Robusthet och säkerhet

Aktiv alltid inkopplad full-kapacitets och geografiskt diversifierad redundans med dynamisk omkoppling baserad på IPv6-routing med kritiska resurser distribuerade så att eventuella attacker om möjligt kan hanteras och i värsta fall att en utslagning är högst lokal.

Vi behöver mer utbildning och spridd kunskap för att kunna hantera vår infrastruktur i händelse av någon form av kris. Delegerat ansvar är en förutsättning för att det ska fungera på tillräckligt bra sätt vid störningar. Åtgärder måste kunna sättas in på ett säkert sätt inom kort tid. Beslutsvägarna får inte vara för långa, en central ordergivning kan vara utslagen vid den kritiska tidpunkten.

Konkurrenskraft

Ett korrekt öppet nät som helt uppfyller Internet-specifikationerna och IETF:s ambitioner gör att de som vill utveckla applikationer, tjänster, etc. inte behöver ägna tid åt att hantera konstiga lokala avvikelser och "specialfixar". Genom att strikt förhålla sig till använd kommunikationsarkitektur är den adresserbara marknaden hela världen, istället för ett stadsnät i Götaland.

Exempel: Jag frågade ansvariga på Zoom, vilka gör ett videokonferenssystem, varför de inte stödjer IPv6 idag? Svaret var att för många leverantörer av internet-tjänster och ”hemma gateways” trasslat till det på för många sätt så det inte gick att operera en stabil tjänst. Zoom har hundratals olika ”trix” för att hantera IPv4-träsket.

Klimat, hållbarhet och resurseffektivitet

En gemensam *logisk* infrastruktur, inte ett SGSI, RAKEL, försvaret, regioner, Konsum etc. Alla har samma behov på IPv6-nivån. Det skall alltid fungera.

Om de sen vill använda sin förbindelse som VPN så placeras ett krypto i anslutningspunkten och sen har man en konfidentiell, robust och driftsäker förbindelse.

Statligt stöd

Lokala "datacenter" med distribuerade resurser, en ny fiber-väg som inte är samförlagd med järnväg, bilväg, kraftledning, etc.

Framtagning av lämpliga krypto-system för anslutning mot öppet nät med hantering av extern routing och överbelastnings attacker etc. Dessa krypto-system måste uppfylla respektive organisations krav.

Utbildning, forskning och backup-kapacitet.

Klara regler för vad som minst krävs av en anslutning, se bilaga 1.

Klara uppdelningar av vem som ansvar för vad bland de olika myndigheterna.

Tips: Läs TU-Stiftelsens "5-hus" förslag, vilket är en blandning av krav och implementationsförslag, bilaga 2-4.

Bilagor

Bilaga 1: Specifikation IPv6 tjänst
Bilaga 2: ”TU Fem Små Hus” Sammanfattning
Bilaga 3: ”TU Fem Små Hus” Huvuddokument
Bilaga 4: ”TU Fem Små Hus” Teknisk spec

Grundspecifikation IPv6 anslutning

Det här utkastet beskriver en framtidssäker internet-infrastruktur, utformad enligt internets grundläggande principer. Det bygger på den internetdefinition med nåbara ändpunkter som låg till grund för IETF:s skapande av IPv6.

Den viktigaste aspekten för en framtidssäker internet-infrastruktur är **end-to-end-principen**: nätverkets enda uppgift är att vidarebefordra paket mellan ändpunkter, utan att bearbeta eller förändra innehållet. End-to-end-principen gör nätverket symmetriskt, vilket innebär att alla ändpunkter är likvärdiga och kan utväxla vilken information som helst utan föregående koordinering, signalering eller tillstånd. Det finns inget som hindrar en användare av en anslutning att själv införa ytterligare funktioner som begränsar trafik och funktionalitet på det sätt användaren önskar, till exempel brandvägg eller NAT-funktion.

IPv4 bredbandsaccess

På grund av bristande tillgång till IPv4-adresser passerar majoriteten av internetanvändarnas trafik idag genom adressöversättare. Här beskrivs en infrastruktur där IPv6 används som bärare av all elektronisk kommunikation.

Tillgång till IPv4 (“IPv4 bredbandsaccess”) levereras som en tjänst över IPv6-basfunktionen och presenteras mot kunden från abonnentplacerad utrustning. Det finns flera IETF-definierade metoder för detta, exempelvis med hjälp av CGNAT eller tunnling av globalt nåbara IPv4-adresser. Jämfört med så kallad ”dual stack” bedöms denna modell minska såväl systemkomplexitet som kostnader för utbyggnad och löpande drift av infrastrukturen.

OSI-modellen

Den så kallade OSI-modellen[1] definierar överföring av datatrafik i 7 olika lager. I detta dokument refererar vi till de grundläggande lagren L1-L4 enligt nedan.
Lager 1 fysiska lagret
Lager 2 datalänklagret
Lager 3 nätverkslagret (adressering, routing etc)
Lager 4 transportlagret (uppdelning i datapaket med omsändningar etc)

IPv6 internetanslutning

Lager 3 i den levererade internetanslutningen ska i samtliga fall utgöras av IPv6 enligt RFC 8200.

Fast anslutning

1https://sv.wikipedia.org/wiki/OSI-modellen

Lager 1 & 2

Följande standarder accepteras i avlämningspunkten:

- 100 Mbit Ethernet twisted pair, 802.3u
- 1 Gbit Ethernet twisted pair, 802.ab
- 1 Gbit Ethernet optical duplex SM fiber, 802.z el 802.3ah
- 10 Gbit Ethernet twisted pair, 802.an-2006
- 10 Gbit Ethernet optical single fiber, 802.?
- 10 Gbit Ethernet optical duplex SM fiber, 802.3ae-2002
- 100 Gbit Ethernet-avlämning specas under 2024
- 400 Gbit Ethernet-avlämning specas under 2025

Automatisk förhandling av duplex och flödeskontroll, alternativt statisk definition i kundprofil.

Inga vlan-taggar (IEEE 802.1Q).

Mobil anslutning

Lager 1 & 2 via mobilnät

Följande standarder accepteras i avlämningspunkten:

- 1 Gbit Ethernet twisted pair, 802.11(*)
- 10 Gbit Ethernet twisted pair, 802.11(*)

Lager 3 via mobilnät

I det fall Ipv6 avlämnas med en mobil terminal skall leverantören tillhandahålla en mobil terminal med ett API som tillåter access till att sända och ta emot kopletta Iv6 paket. API skall möjiggöra att man använder flera olika Ipv6 adresser inom terminalen t.ex för olika applikationer. API skall vara beskrivet i ett publikt IETF dokument. Format är valfritt IETF dokument; draft, informal eller induvidual submission.

MTU

IPv6 MTU ska vara 9000 byte över media med stöd för detta. Om den direktanslutna kundutrustningen endast klarar 1500 byte ska anpassning ske automatiskt (IETF BCP 39). Leverans av MTU på 9180 byte ska ske på begäran om avlämningsmediet har stöd för detta.

ICMP

Korrekt hantering av ICMP i alla nätelement mellan sändare och mottagare är en förutsättning för full funktion.

IP-adresser

Standardtilldelningen av IPv6-adresser är ett fast ett /56-block (256 /64-block) från

operatörens adressblock. Minsta tilldelade block för en fast anslutning är /60.

Till nätet som ansluter användaren (avlämningsnätet) används i första hand första eller sista /64-block ur kundens allokering. Detta signaleras i DHCP genom användandet av ”PD-exclude”. Avlämningsnätet kan också tilldelas ett annat globalt adresserbart prefix ur IPv6-operatörens adressblock. Oavsett hur adresserna i avlämningsnätet tilldelas ska det vara möjligt att adressera minst 16 direkt anslutna enheter. De ska kunna nå hela det globala internet.

Avlämningsnätet annonseras med ICMPv6 *router advertisement* (RA) mot abonnenten.

Operatören ska vidarebefordra paket som har destinationsadresser inom användarens tilldelade adressrymd till minst en enhet ansluten till avlämningsnätet.

Ändring av de tilldelade adresserna för en anslutning ska undvikas så långt som möjligt.

Vid en eventuell omnumrering av en anslutning skall man ge användaren minst 90 dagar att konvertera sina ändutrustningar och under denna tid skall både nya och gamla Pv6 adresser fungera.

IPv6 NDP

Operatörens avlämningsutrustning ska kunna hantera minst 16 samtidiga NDP-sessioner för utrustning ansluten direkt till avlämningsnätet. Tilldelade adresser ska kunna nå alla IPv6-destinationer i Sverige.

Rekommendation till ansluten utrustning

Eftersom adresser är “semistatiska” är det lämpligt att ansluten utrustning ”kommer ihåg” sin adressering i händelse av kraftavbrott och använder den initialt efter återstart. Därigenom erhålls tillgänglighet i driftfall där paketförmedling fungerar men stödfunktioner, som DHCPv6, är otillgängliga.

I fall när användaren har lokal DHCP-vidaredelegering är det lämpligt att även adressdelegeringar för de enheter som skall kunna nås globalt sparas så att de är nåbara direkt vid en återstart.

IP-transparens

Ett korrekt formaterat IPv6-paket avsänt från godtycklig avsändare inom Sverige med godtyckligt innehåll (IP-protokoll/port/etc) ska vidarebefordras till användaren oförvanskat.

RPF-kontroll

Internetoperatören skall bara vidarebefordra paket som har avsändaradresser inom det adressområde som tilldelats användaren.

Colours

I det fall olika IPv6-adressrymder används för olika tilläggstjänster skall dessa taggas med

"colours" (rfc) som är koordinerade i ett publikt tillgängligt nationellt register.

Tillgänglighet

Längsta tillåtna avbrott på utrustning sekundärt placerad i nätet är 60 sekunder, oberoende av felorsak.

Bilaga 3B – Verifiering av internetanslutning

Test av Protokolltransparens

Paket skickas med en hastighet av ett paket per sekund till referensmottagare. I det fall vald referensmottagare inte erhåller paket väljer avsändaren en annan mottagare. I fall ingen mottagare erhåller paket är förbindelsen trasig. Innehåll i paketen väljs slumpmässigt.

Referensmottagarna tar emot paket och skickar ICMP-svar till avsändaren. Det finns fyra typer av referensmottagare med stöd för olika MTU:

- 576 byte
- 1500 byte
- 4470 byte
- 9000 byte

Krav:

- För godkänt resultat ska avsändaren ha mottagit svar från referensmottagaren på 249 av 250 avsända paket (99,6%) med IPv6 MTU på 9000 byte, 4470 byte, 1500 byte och 576 byte.
- Paket som tar längre tid än 20 ms (en väg) att nå mottagaren räknas som förlorat.
- Kommer mer än 2% av paketen fram i oordning räknas det som avbrott på förbindelsen.

Test av adressering och routing

Korrekt formaterade IPv6-paket med slumpmässigt innehåll och en MTU på 1500 byte skickas till två slumpmässigt utvalda mottagaradresser på avlämningsnätet samt till en och samma adress på referensmottagaren skickas från en godtycklig avsändare inom Sverige.

Krav:

- För godkänt resultat ska mottagarna ha tagit emot 249 av 250 avsända paket (99,6%).

Korrekt formaterade IPv6-paket med slumpmässigt innehåll och en MTU på 1500 byte skickas till slumpmässigt utvalda mottagaradresser inom det adressblock som tilldelats användaren (exklusive avlämningsnätets adresser).

Krav:

- För godkänt resultat ska den enhet som tilldelats adresserna av internetoperatörens utrustning ha mottagit 249 av 250 avsända paket (99,6%).

Mätning av dynamiska prestanda

Här avses IPv6-genomströmning. Overhead på lägre läger, exempelvis Ethernet, är exkluderat.

Mätning av dynamiska prestanda sker genom att grupper av IPv6-paket med 128 byte nyttolast skickas utan tidsglapp mellan paketen. Varje grupp innehåller 4 paket per avtalad kilobit anslutningshastighet. Exempelvis innebär 1 Gbit/s kundanslutning 3800 paket om 128 byte per grupp.

Det ska finnas fler än tre referenssändarre/-mottagare i Sverige. Drivs av ansvarig myndighet.

Följande tester genomförs:

- Från en referenssändare till en adress i användarens anslutningsnät, i en takt motsvarande 100% av avtalad bandbredd
- Från en adress i användarens anslutningsnät till en referensmottagare, i en takt motsvarande 100% av avtalad bandbredd
- Från en referenssändare till en adress i användarens anslutningsnät, i en takt motsvarande 95% av avtalad bandbredd.
- Från en adress i användarens anslutningsnät till en referensmottagare, i en takt motsvarande 95% av avtalad bandbredd.

Krav:

- Max ett paket per sänd grupp får försvinna vid de två första testerna.
- Inga paket får försvinna vid de två sista testerna.
- Godkända prestanda ska uppnås mot samtliga referenssändare/-mottagare i Sverige.