

TU:s internetspecifikation

Inledning

Syftet med den här specifikationen är att beskriva en internetinfrastruktur för Sverige som är utformad enligt internets grundläggande principer. Den viktigaste aspekten för en framtidssäker internetinfrastruktur är **end-to-end-principen** som innebär att ett nätverks 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. Trots detta finns det inget som förhindrar en användare att själv införa ytterligare funktioner som begränsar trafik och funktionalitet, exempelvis brandväggar eller adressöversättningsfunktioner.

Arbetet med att fastställa internets arkitekturprinciper och standarder sker inom ramen för **The Internet Engineering Task Force (IETF)**. Resultaten av IETF:s arbete publiceras i en dokumentserie känd som **Request for Comments (RFC)**. För att ett nätverk som utgör en del av internet ska vara fungerande och framtidssäkert är det en förutsättning att det är designat på det sätt som beskrivs av gällande RFC:er.

Utgångspunkten i designen av en internetinfrastruktur för Sverige har varit att den ska tillhandahålla förmedling av IPv6-paket i enlighet med IETF:s designprinciper.

Utveckling av specifikationen

Utvecklingen av den här specifikationen är pågående. Aktuell version av specifikationen finns alltid tillgänglig på projektets Github-sida: <https://github.com/tu-stiftelsen/femsmahus2>. Bidrag i form av ändringsförslag och "issues" välkomnas.

OSI-modellen

Den så kallade OSI-modellen definierar data överföring i 7 olika lager. I den här specifikationen benämns de fyra nedersta lagren enligt nedan.

Lager 1 Fysiska lagret

Lager 2 Datalänklagret

Lager 3 Nätverkslagret (adressering, routing etc)

Lager 4 Transportlagret (uppdelning i datapaket med omsändningar etc)

Lager 3: Förmedling av IPv6

Grunden för all kommunikation enligt den här specifikationen är förmedling av IPv6-paket. Lager 3 i den levererade internetanslutningen ska därför alltid utgöras av IPv6 enligt RFC 8200.

Tilldelning av IP-adresser

I IPv6 tilldelas adresser i block. Storleken på ett block uttrycks normalt som ett snedstreck följt av antalet fasta bitar i början av blockets adresser. Exempelvis innebär tilldelning av ett /48-block att kunden tilldelas en mängd adresser där de första 48 bitarna i adressen är desamma. Kunden är fri att fördela de återstående 80 bitarna inom sitt nät. Det minsta block som tilldelas en enskild broadcastdomän är normalt /64.

Samtliga tilldelade adresser ska vara globalt adresserbara.

Tilldelning av adressblock till användare sker genom Dynamic Host Configuration Protocol version 6 (DHCPv6) prefix delegation (PD).

Standardtilldelningen av IP-adresser till en kund ska vara ett /56-block, vilket motsvarar 256 /64-block. Minsta tillåtna tilldelning för en fast anslutning är ett /60-block.

Det block som ansluter användare till leverantör (avlämningsnätet) tilldelas normalt det första eller sista /64-blocket ur användarens allokering. Det är även tillåtet att tilldela ett annat globalt adresserbart adressblock till avlämningsnätet. Avlämningsnätet annonseras mot användaren genom ICMPv6 router advertisement (RA). I de fall ett adressblock ur användarens allokering används för avlämningsnätet ska det indikeras för användaren genom DHCPv6 PD exclude. Det ska vara möjligt för kunden att ansluta minst 16 enheter direkt till avlämningsnätet.

Ändring av de tilldelade adresserna för en anslutning ska undvikas så långt som möjligt. I de fall ändring sker ska trafik till och från de tidigare tilldelade adresserna fortsätta förmedlas under lägst tre månader.

Rekommendation för kundansluten utrustning

Eftersom adresser är semistatiska, dvs. förändras relativt sällan, är det lämpligt att ansluten utrustning sparar sina tilldelade adresser och adressblock vid omstarter och kraftavbrott. I händelse av felfall där paketförmedling fungerar men stödfunktioner, exempelvis DHCPv6, är otillgängliga blir det då fortfarande möjligt att förmedla paket.

Krav

Förmedling Operatören ska vidarebefordra IPv6-paket adresserade till adresser inom användarens tilldelade adressrymd till minst en enhet ansluten till avlämningsnätet.

Transparens Ett korrekt formaterat IPv6-paket adresserat till användarens tilldelade adressrymd ska vidarebefordras till användarens utrustning oförvanskat, oaktat innehåll eller avsändare. Detsamma gäller paket från användarens utrustning till alla globalt adresserbara IPv6-adresser. I sammanhanget är det viktigt att notera att korrekt och oförvanskad förmedling av Internet Control Message Protocol version 6 (ICMPv6)-paket en förutsättning för full funktion i IPv6, vilket inte är fallet för IPv4.

Maximum transmission unit (MTU) MTU i anslutningen ska vara 9000 byte. I de fall kundens anslutna utrustning inte har stöd för detta ska anpassning av MTU till 1500 byte ske automatiskt. Om avlämningsmediet har stöd för MTU på 9180 byte ska det användas på begäran av kunden.

NDP Operatörens avlämningsutrustning ska kunna hantera minst 16 simultana NDP-sessioner för utrustning ansluten direkt till avlämningsnätet.

Reverse-path forwarding (RPF)-kontroll Internetoperatören ska genomföra RPF-kontroll av paket förmedlade från användaren. Endast paket med avsändaradresser från användarens tilldelade adressområde ska vidarebefordras.

Colours I det fall olika adressrymder används för olika tilläggstjänster ska taggning med colours ske (RFC xxxx). Taggningen ska vara densamma för alla operatörer i Sverige.

Tillgänglighet Längsta tillåtna avbrott på utrustning i operatörens nät som inte är avlämningsutrustning är 60 sekunder. Det här kravet innebär att all operatörens utrustning, utom avlämningsutrustningen, måste vara redundant. Längsta tillåtna avbrott på operatörens avlämningsutrustning är 8 timmar.

Lager 1 & 2

Fast anslutning

Följande standarder accepteras i avlämningspunkten:

- 1 Gbit Ethernet twisted pair (IEEE 802.3ab)
- 1 Gbit Ethernet optical duplex SM fiber, (IEEE 802.xx)
- 10 Gbit Ethernet twisted pair (IEEE 802.3an)
- 10 Gbit Ethernet optical single fiber (IEEE 802.xx)
- 10 Gbit Ethernet optical duplex SM fiber (IEEE 802.xx)
- 100 Gbit Ethernet-avlämning specificeras under 2024
- 400 Gbit Ethernet-avlämning specificeras under 2025

Förhandling av duplex och flödeskontroll ska ske automatiskt om inte annat har avtalats. Så kallad VLAN-taggning av virtuella nätverk (IEEE 802.1Q) ska inte ske.

Trådlös anslutning

Leverans av trådlös internetanslutning ska ske genom Wi-Fi (IEEE 802.11a/b/g/n/ac/ax/be).

IPv4-tjänst

Eftersom det råder stor brist på IPv4-adresser passerar majoriteten av internetanvändarnas trafik idag genom adressöversättare. Utgångspunkten för den arkitektur som specificeras här är att IPv6 används som bärare för all elektronisk kommunikation. Tillgång till IPv4 ("IPv4 broadbandaccess") levereras därför som en tjänst över IPv6 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"-lösning bedöms denna arkitektur minska såväl systemkomplexitet som kostnader för utbyggnad och löpande drift av infrastrukturen.

Verifiering av internetanslutning

Referenssändare och -mottagare

För verifiering av att en internetanslutning uppfyller kraven i den här specifikationen ska det finnas ett antal referenssändare- och mottagare placerade fysiskt på olika platser i Sverige och logiskt på olika platser i nätverket. Det ska finnas minst tre referenssändare- och mottagare i Sverige som drivs på uppdrag av ansvarig myndighet.

Test av transparens

Vid test av transparens skickas paket med slumpmässig nyttolast och lager 4-protokoll till en referensmottagare med en hastighet av ett paket per sekund. Referensmottagarna tar emot paket och skickar ICMP-svar till avsändaren. I det fall referensmottagaren inte erhåller paket väljs en annan mottagare. I fall ingen mottagare erhåller paket är testet underkänt.

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 fler än fem (2%) av paketen fram i ordning räknas det som avbrott på förbindelsen.

Test av adressering och routing

Korrekt formaterade IPv6-paket med slumpmässig nyttolast och lager 4-protokoll skickas till två slumpmässigt utvalda mottagaradresser på avlämningsnätet samt till en och samma adress på referensmottagaren skickas från en godtycklig avsändare inom Sverige. Storleken på pake-ten ska motsvara en MTU på 1500 byte.

Krav:

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

Korrekt formaterade IPv6-paket med slumpmässignyttolast och lager 4-protokoll skickas till slumpmässigt utvalda mottagaradresser inom det adressblock som tilldelats användaren (ex-klusive avlämningsnätets adresser). Storleken på paketen ska motsvara en MTU på 1500 byte.

Krav:

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

Mätning av dynamiska prestanda

Vid mätning av dynamiska data mäts genomströmning av lager 3, dvs. IPv6. Overhead på lägre lager, exempelvis Ethernet, är exkluderat. Mätningen 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.

Följande tester genomförs:

- Från en referenssändare till en adress i användarens anslutningsnät, i en takt motsvaran-de 100% av avtalad bandbredd
- Från en adress i användarens anslutningsnät till en referensmottagare, i en takt motsva-rande 100% av avtalad bandbredd
- Från en referenssändare till en adress i användarens anslutningsnät, i en takt motsvaran-de 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.