

TU:s internetspecifikation

Inledning

Det här dokumentet beskriver en del av designen i en internetinfrastruktur för Sverige. Infrastrukturen är baserad på förmedling av IPv6-paket i enlighet med IETF:s designprinciper. Den viktigaste av detta 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 dokumentserien **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.

Användning och målgrupp

Det här dokumentet är tänkt att användas av internetoperatörer (ISP:er) vid design av deras tjänster. Det kan även användas av slutanvändare för att verifiera att ISP:er lever upp till de krav som ställs på dem.

Terminologi

I det här dokumentet avser begreppet **IP** enbart **IPv6**.

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.

Nätverksmodell

I den här specifikationen används en nätverksmodell där de fyra nedersta lagren benämns 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.

– **Krav:**

- En internetanslutning **ska** baseras på förmedling av IPv6-paket

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) (RFC 8415). Detta bör ske enligt DHCPv6 option 18, 37 eller motsvarande beständig¹ tilldelning.

Standardtilldelningen av IP-adresser till en kund ska vara ett /56-block, vilket motsvarar 256 /64-block.

Det block som ansluter användare till operatör (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 IPv6 Stateless Address Autoconfiguration (SLAAC) (RFC 4862). SLAAC använder ICMPv6 router advertisement (RA) (RFC 4861). I de fall ett adressblock ur användarens allokering används för avlämningsnätet ska det indikeras för användaren genom DHCPv6 PD exclude (RFC 6603). Det ska vara möjligt för kunden att ansluta minst 16 enheter direkt till avlämningsnätet.

Föredragen livstid (preferred lifetime) för DHCPv6-lease är 604 800 sekunder (7 dagar). Giltig livstid (valid lifetime) är 2 592 000 sekunder (30 dagar).

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.

– **Krav:**

- Adresser tilldelade av operatör till användare **ska** vara globalt adresserbara.
- Tilldelning av adresser **ska** ske genom DHCPv6 PD (RFC 8415).
- Tilldelning av adresser **ska** ske med minst ett /56-block.
- DHCPv6 PD exclude **ska** användas för att indikera de adresser som avlämningsnätet använder.
- Avlämningsnätet **ska** klara av *minst* 16 direktanslutna enheter.
- Ändring av tilldelade adresser **ska** informeras om tre månader innan ändring.

¹Med *beständig* avser vi den engelska tekniska termen *persistent*.

– **Rekommendation:**

- Tilldelade adresser **bör** inte ändras.
- Tilldelning av adresser **bör** ske genom DHCPv6 option 18, 37 eller motsvarande beständig tilldelning² (RFC 8415).

Rekommendation för kundansluten utrustning vid anslutningspunkt

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:**

- Tilldelade adresser **ska** fungera under hela DHCPv6-lease tiden, även om DHCPv6-funktionen går ner.

Rekommendation för kundansluten utrustning bakom anslutningspunkt

Enheter bakom anslutningspunkt ska hantera både DHCPv6 och SLAAC för adresstilldelningen.

– **Krav:**

- Enskilda enheter bakom anslutningspunkt **ska** ska stödja DHCPv6 (RFC 8415) och SLAAC (RFC 4862).
- Adresser tilldelade till enheter bakom anslutningspunkt **ska** vara globalt adresserbara.

– **Rekommendationer:**

- IPv6-noder **bör** fungera enligt RFC 8504.

Paketförmedling

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 (RFC 4443) 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.

Neighbor Discovery Protocol (NDP) Operatörens avlämningsutrustning ska kunna hantera minst 16 simultana NDP-frågor för utrustning ansluten direkt till avlämningsnätet (RFC 4861).

²Med *beständig* avser vi den engelska tekniska termen *persistent*.

Reverse-path forwarding (RPF)-kontroll Internetoperatören ska genomföra RPF-kontroll av paket förmedlade från användaren (RFC 2827). Endast paket med avsändaradresser från användarens tilldelade adressområde ska vidarebefordras.

DiffServ I det fall olika trafikmärkning används för olika tilläggstjänster ska taggning med DiffServ, eller så kallad färgning eller colors, ske (RFC 2474). Märkningen 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 skall ingå i avtalet.

– **Krav:**

- Operatören **ska** förmedla IPv6-paket adresserade till adresser inom användarens adressrymd till minst en enhet ansluten till avlämningsnätet.
- Operatören **ska** stödja en MTU på 9000 byte och 1500 byte på avlämningsnätet.
- Operatören **ska** erbjuda en MTU på 9000 byte som standard och anpassa till 1500 byte om så krävs.
- Operatören **ska** kunna hantera *minst* 16 simultana NDP-frågor för användarutrustning ansluten direkt till avlämningsnätet.
- Operatören **ska** enbart förmedla vidare paket från användaren med avsändaradress inom den tilldelade adressrymden.
- Operatören **ska** följa etablerad paket-taggingsstandard.
- Operatören **ska** designa nät med redundans och erbjuda tjänster utan nedtid.
- Operatören **ska** kunna avhjälpa utrustningsfel i avlämningsnätet inom 8 timmar.

– **Rekommendation:**

- Operatören **bör** erbjuda en MTU på 9180 byte på avlämningsnätet på användarens begäran.

Lager 1 & 2: specifikation för överlämning

Denna specifikation gäller regler för överlämning. Denna överlämning sker mellan utrustning som pratar med operatörens nät, och kundens utrustning. Vanliga exempel på överlämningspunkter inkluderar mellan fiberkonverterare och kundutrustning, någonstans mellan radiochip och processor i användare enhet (e.g i telefon eller mot modem) för 3GPP baserat mobilnät, och mellan trådlös accesspunkt och användarenhet.

Anslutning

Följande standarder accepteras i avlämningspunkten:

- 1 Gbit Ethernet twisted pair (IEEE 802.3ab)
- 1 Gbit Ethernet optical duplex SM fiber, (IEEE 802.3ah ??)
- 10 Gbit Ethernet twisted pair (IEEE 802.3an)

- 10 Gbit Ethernet optical single fiber (IEEE 802.3ae ??)
- 10 Gbit Ethernet optical duplex SM fiber (IEEE 802.3ae ??)
- 100 Gbit Ethernet-avlämning specificeras under 2024
- 400 Gbit Ethernet-avlämning specificeras under 2025
- IEEE 802.11a/b/g/n/ac/ax/be
- IEEE 802.11ah

Förhandling av duplex och flödeskontroll ska ske automatiskt om inte annat har avtalats. Om trafikmärkning behövs, så skall denna ske med hjälp av DiffServ (RFC 2474).

Så kallad VLAN-tagging av virtuella nätverk (IEEE 802.1Q) *får* inte ske.

- **Krav:**
 - Operatören **ska** avlämna nät enligt någon av specifikationerna ovan.
 - **Om** trafikmärkning sker, **ska** detta göras med hjälp av DiffServ (RFC 2474).

Transport till avlämningspunkten

Bakom avlämningspunkten kan flera olika tekniker användas. Fibernät är att rekommendera. I de fall 3GPP-baserat nät används för transport sker avlämning på kundens sida av radiokretsen, detta innebär att avlämningen sker i exempelvis i en mobiltelefon eller i en router med 3GPP-baserad modem.

- **Rekommendation:**
 - Operatören **bör** avlämna med hjälp av fiberbaserat nät.
- **Möjlighet**
 - Operatören **kan** avlämna med hjälp av 3GPP-baserat nät bakom avlämningspunkten (RFC 7066).

Övriga kommentarer och rekommendationer

IPv4-tjänst

Utgångspunkten för den arkitektur som specificeras här är att IPv6 används som bärare för all elektronisk kommunikation. Tillgång till IPv4 ("IPv4 bredbandsaccess") ska därför levereras 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 "dual stack"-lösning bedöms denna arkitektur minska såväl systemkomplexitet som kostnader för utbyggnad och löpande drift av infrastrukturen.

- **Rekommendation:**
 - Operatören **bör** erbjuda en single-stack lösning baserat på IPv6.
 - Operatören **bör** erbjuda andra protokoll och adressrymder, såsom IPv4, över IPv6.

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.

Verifiering och trådlös anslutning

För verifiering av trådlös anslutning antas en fast enhet som mottagare. Presentandakrav nedan gäller ej för terminal i rörelse.

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.

Följande referensmottagare med stöd för olika MTU ska användas:

- 1280 byte
- 1500 byte
- 4470 byte
- 9000 byte

Detta för att ge en god testbredd.

- **Testkrav:**
 - 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 1280 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 paketen ska motsvara en MTU på 1500 byte.

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

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

– **Testkrav:**

- 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

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 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.

Dessa tester ska utvärderas mot testkraven.

– **Testkrav:**

- 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.