TRAFICOM
Liikenne- ja viestintävirasto

Suositus IPv6:n käyttöönotosta kuluttajalaajakaistaliittymissä

Klaus Nieminen

Traficomin julkaisuja

230/2020

Sisällysluettelo

1 Johdanto

Liikenne- ja viestintävirasto Traficomin IPv6-työryhmä on laatinut nämä suositukset IPv6:n käyttöönotosta kuluttajalaajakaistaliittymissä. Suositukset on laadittu kuluttajien käyttöön tuotteistettuihin liittymiin riippumatta siitä, onko yksittäisen liittymän käyttäjä kuluttaja tai yritys. Suosituksia voidaan soveltaa myös yritysliittymien ja tukkutuotteiden tuotteistuksessa ottaen huomioon näiden erityispiirteet kuten yritysliittymien manuaalinen konfigurointi, suurempi osoiteavaruuden koko sekä dynaaminen reititys.

Traficom suosittelee, että laajakaistapalveluntarjoajat alkavat tarjota IPv6-yhteyksiä oletusarvoisesti myös kuluttajien käyttöön tuotteistetuissa liittymissä. Tämä on tärkeää, sillä IPv6:n käyttöönotto ei tapahdu antamalla osoitteita niitä pyytäville vaan IPv6 on kytkettävä kytketä automaattisesti päälle. Suositukset on laadittu luomaan hyviä käytäntöjä sekä auttamaan tätä tuotteistusta.

Suositukset on laadittu mahdollisimman yhteneviksi eri verkkotekniikoille. Matkapuhelinverkkojen ja kiinteiden verkkojen välillä on kuitenkin eroja, joiden takia kummallekin on jouduttu laatimaan omia suosituksiaan.

Valitettavasti osa vanhemmista verkkolaitteista, esimerkiksi DSLAM-laitteista ja Ethernet-kytkimistä eivät tue natiivin IPv6:n tarjoamista (mm. DHCP optio 37 leimaaminen, IPv6 ryhmälähetykset ja tietoturva). Tällöin IPv6 on mahdollista ottaa käyttöön näiden laitteiden takana olevissa liittymissä vain erilaisilla tilapäisratkaisuilla. Mikäli teleyritys haluaa tarjota IPv6-yhteyden myös näille käyttäjille, Traficom suosittelee 6rd-mekanismin käyttöä. Asiaa on käsitelty tarkemmin luvussa 5.4.

2 Operaattorin verkon IPv6-tuki (verkko ja nimipalvelu)

On tärkeää, että teleyritys tarjoaa käyttäjille samat palvelut riippumatta käyttääkö käyttäjä IPv4- tai IPv6-yhteyttä. Asiaa on käsitelty tarkemmin luvussa 6 Operaattorin kuluttajille tarjottavat tietoturva- ja muut oheispalvelut.

Tässä luvussa on kuvattu suositukset liittymän tunnistamisesta ja käänteisnimipalvelun tarjoamisesta. Tietoturvaa käsitellään luvussa 3 ja muuhun liittymien tuotteistukseen kuten osoitteiden jakoon liittyviä suosituksia luvussa 5.

Laitehankintojen yhteydessä Traficom suosittelee tutustumaan Broadband Forumin laatimiin IPv6-suosituksiin verkkoelementtien yhteentoimivuudesta ja tietoturvasta (TR-177) [1] sekä RIPE:n IPv6-työryhmän laatimiin IPv6-laitevaatimuksiin (ripe-554) [2].

Lisäksi teleyrityksen on hyvä tutustua IPv6 Forumin IPv6 Ready -sertifiointiin ja hyväksynnän saamiin tuotteisiin. Lisätietoa näistä löytyy osoitteesta: https://www.ipv6ready.org/

2.1 Liittymän tunnistaminen

Teleyrityksellä voi olla tarpeen tunnistaa loppukäyttäjän käyttämä liittymä ja/tai liittymäsopimuksen haltija esimerkiksi palvelun ja sen laskutuksen toteutuksen, vika- ja häiriötilanteiden selvittämistä varten sekä mahdollisten väärinkäytösten selvittämistä varten. Erilaista jälkikäteistä selvitystyötä varten riittää, että liittymän haltija pystytään tunnistamaan tilaajalle jaetun IPv6-verkkoalueen perusteella.

IPv6-liittymien tunnistamiseen pätevät samat periaatteet kuin IPv4-liittymiin, mutta tarkempi mekanismi riippuu käytettävästä tekniikasta. Esimerkiksi käytettäessä liittymäryhmäkohtaista VLANia palveluoperaattori ei pysty

yhdistämään liikennettä mihinkään tiettyyn liittymään ilman liikenteeseen lisättävää erillistä tunnistetta.

Tätä varten käytettäessä DHCPv6 prefix delegation (PD) -mekanismia esimerkiksi DHCPv6-välityspalvelimena toimivien laitteiden tulee lisätä esimerkiksi Interface-ID (optio 18, RFC 3315) [3], remote-id (option 37, RFC4649) [4] tai subscriber-id (optio 38, RFC4580) [5] tieto välittämiinsä asiakkaalta palvelimelle lähetettäviin DHCPv6-paketteihin. Yhteentoimivuuden takaamiseksi Traficom suosittelee, että teleyritykset käyttävät tähän tarkoitukseen option 37:aa (remote-id, RFC4649) [4].

Lisäksi älykkään L3-terminointilaitteen avulla on mahdollista sitoa liittymän IPv6-verkkoalueet jaettuun IPv4-osoitteeseen ja sen tunnistetietoihin, jolloin riittävä tunnistustaso saavutetaan vaikka liityntäverkkolaitteet eivät tukisi DHCPv6-liikenteen rikastamista liittymän tunnistetiedoilla. Ominaisuus edellyttää, että liittymälle on jaettu myös IPv4-osoite.

Käytettäessä RADIUS-palvelinta jakamaan IPv6 osoitteita tarvittava tieto on saatavissa sen lokeista yhdistämällä Framed-IPv6-Address, Framed-IPv6-Prefix ja Framed-Interface-Id -tiedot (RFC6911) [6].

2.2 Käänteisnimipalvelu

Käänteisnimipalvelun avulla on mahdollista hakea IP-osoitetta vastaava verkkotunnus. Palvelulla on merkitystä, sillä esimerkiksi osa sähköpostipalvelimista (esim. gmail.com) kieltäytyy ottamasta vastaan viestejä palvelimelta, jolla ei ole käänteisnimipalvelua.

Traficom suosittelee, että teleyritys tarjoaa käänteisnimipalvelun automaattisesti kaikille asiakkaille jaettaville IPv6-verkkoalueille ja -osoitteille.

On oleellista, että käänteisnimipalvelu tarjotaan nimenomaan automaattisesti ilman asiakkaalta vaadittavia toimenpiteitä. Käytännössä verkkoalue voidaan delegoida dynaamisesti luotuihin tietueisiin. Dynaaminen käänteisnimipalvelu voidaan toteuttaa monella eri tavalla [7] kuten [8] ja [9] ja teleyrityksen kannattaakin valita itselleen sopivin toteutus.

Lisäksi Traficom suosittelee, että teleyritys tarjoaa asiakkailleen lisäpalveluna mahdollisuuden linkittää käänteisnimipalvelu esimerkiksi asiakkaan käytössä olevaan verkkotunnukseen.

3 Liityntäverkon tietoturva

Liikenne- ja viestintäviraston määräyksen 67 A/2015 M teletoiminnan tietoturvasta [10] mukaan teleyrityksen on suojattava oma verkkonsa yhteenliittämis- ja asiakasrajapinnoista tulevalta haitalliselta liikenteeltä toteuttamalla verkossaan tarvittavat suojausmekanismit.

Määräyksen mukaan teleyrityksen on pidettävä huolta, että sen asiakas- ja yhteenliittämisrajapinnassa olevissa viestintäverkon tai -palvelun komponenteissa tai näiden porteissa ei ole päällä tarjotun palvelun kannalta tarpeettomia palveluita tai protokollia.

Esimerkiksi tarpeelliset reititys- ja hallintaprotokollat on syytä sallia vain ennalta määritellyistä osoitteista. Ping- ja traceroute -palvelut on syytä sallia, mutta teleyrityksen on syytä rajoittaa niissäkin sallitun liikenteen määrää.

Teleyrityksen on lisäksi estettävä yhteenliittämisrajapinnoissa sellainen sen viestintäverkkoon suuntautuva IP-liikenne, jossa vastaanotetun IP-paketin lähdeosoite on virheellinen sekä myös oletusarvoisesti hylättävä vastaanotetut virheelliset reittimainostukset.

Teleyrityksen on myös suodatettava sellainen asiakasliittymästä viestintäverkkoon suuntautuva liikenne, jonka lähdeosoite ei ole kyseiselle asiakasliittymälle osoitettu (verkkoalue tai yksittäinen IP-osoite).

Määräyksessä teleyrityksille on annettu lisäksi internetyhteyspalveluja koskevia erityisiä vaatimuksia kuten velvoitteita haitallisen liikenteen havaitsemisesta ja suodattamisesta sekä internetyhteyspalvelujen liikennöinnin eriyttämisestä.

Tarkempaa ohjeistusta aiheesta löytyy määräyksen perustelut ja soveltaminen (MPS 67) -dokumentista.

Suositus

Traficom suosittelee lisäksi, että liityntä ja runkoverkon linkkiosoitteisiin sallitaan yhteydet vain palveluntarjoajan omasta verkonhallintaverkosta.

4 Asiakaspäätelaitteen IPv6-tuki

Teleyrityksen tuotteistus kuten teleyrityksen käyttämät IPv6-verkkoalueen delegointitavat asettavat vaatimuksia palvelussa käytettäville päätelaitteille. Teleyrityksen on kuvattava tarjoamansa palvelun asiakasrajapinta ja sitä kautta palvelun tukemat päätelaitteet.

IPv6 Forumin lista IPv6-sertifioiduista päätelaitteista löytyy osoitteesta: https://www.ipv6ready.org/.

Yleisiä kiinteän verkon CPE-reitittimen vaatimuksia on käsitelty RFC:ssä 7084 Basic Requirement for IPv6 Customer Edge Routers [11].

Lisäksi suosituksia kuluttajaliittymässä käytettävän asiakaspäätelaitteen tietoturvasta löytyy RFC:stä 6092 Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service [12].

5 IPv6-tuotteistus kuluttajalaajakaistaliittymissä

5.1 Yleiset suositukset

On tärkeää, että teleyritys tarjoaa käyttäjille samat palvelut riippumatta käyttääkö käyttäjä IPv4- tai IPv6-yhteyttä. Asiaa on käsitelty tarkemmin luvussa 6.

Traficom haluaa lisäksi muistuttaa, että säänneltyjen tukkutuotteiden tulee tukea samoja palveluita kuin verkko-operaattori tarjoaa itse omille asiakkailleen. Eli kun IPv6 otettaan käyttöön, myös verkossa toimiville kilpailijoille tulee tarjota sama mahdollisuus IPv6:n käyttöön.

5.2 Kiinteät verkot

Valitettavasti osa vanhemmista verkkolaitteista, kuten DSLAM-laitteista ja Ethernet-kytkimistä eivät tue natiivin IPv6:n tarjoamista (mm. DHCP optio 37 -leimaaminen, IPv6-ryhmälähetykset ja tietoturva). Tässä luvussa esitetyt suositukset soveltuvat siten vain kaapelimodeemi-, ethernet- ja WLAN-tekniikoilla toteutettuihin verkkoihin sekä xDSL-liittymiin, joiden tarjonnassa käytetty DSLAM tukee natiivin IPv6:n tarjoamista.

5.2.1 IPv6-verkkoalueen pituus

Traficom suosittelee, että asiakkaalle jaettavan verkkoalueen pituus on neljällä jaollinen. Tällöin verkkoalueen raja osuu IPv6-osoitteessa heksadesimaalimerkkien väliin.

Traficom suosittelee, että yhdelle liittymälle jaetaan vähintään /56:n pituinen verkkoalue, jolloin asiakkaalla on käytettävissään ainakin 256 aliverkkoa. Tähän vähimmäissuositukseen päädyttiin siksi, että asiakaspäätelaitteen tulee jakaa jokaiseen porttiin oma /64-aliverkko [12] ja sama koskee käytännössä myös muita kotona olevia reitittimiä. Siksi esimerkiksi /60-osoiteavaruus tulee loppumaan helposti kesken jo tavallisissa kuluttajaliittymissä. Lisäksi pieninkin teleyrityksille jaettava verkkoalue mahdollistaa 16 miljoonaa tällaista /56-liittymää, eli osoitteet eivät tule loppumaan kesken. Myös RIPE NCC [13] ja Broadband Forum [1] ovat antaneet saman suuntaiset suositukset. Käytännössä teleyritys voi esimerkiksi jakaa kuluttajaliittymiinsä /56:n pituisen verkkoalueen ja yritysliittymiin /48:n pituisen verkkoalueen tai kaikille voidaan antaa /48, mikä on yksinkertaisin ratkaisu [13].

Mikäli teleyritys tarjoaa osalle käyttäjistä IPv6-palvelua 6rd:n avulla, tällöin myös /60 voi olla perusteltu vaihtoehto (katso luku 5.4).

Kuten luvusta 5.2.3 käy ilmi, SLAACin avulla jaetaan /64 -pituisia verkkoalueita, joista asiakaspäätelaite voi luoda yhden tai useamman IPv6-osoitteen.

Kun teleyritys toimittaa asiakaspäätelaitteen, Traficom suosittelee, että jokaisen aliverkon kooksi määritellään /64.

5.2.2 Verkkoalueen elinikä

Asiakkaalle jaettavan verkkoalueen tulisi olla pitkäikäinen, sillä kotiverkossa voi ilmetä ongelmia aliverkkojen kanssa käytetyn verkkoalueen vaihtuessa. Traficom suosittelee, että teleyritys jakaa asiakkaalle uudelleen aina saman verkkoalueen. Tarkoituksena on, että asiakkaan saama verkkoalue ei vaihdu tarpeettomasti. Perusteita tälle suositukselle on avattu tarkemmin dokumentissa ripe-690:n luvussa 5 [13].

IPv6-osoitteiden elinikää säätelee kaksi parametria. "Preferred" ja "Valid". Preferred-elinikä kertoo, että kyseistä osoitetta voi käyttää ongelmitta. Näitä osoitteita tulee käyttää ensisijaisesti verrattuna osoitteisiin, jotka eivät ole Preferred-tilassa. Valid-elinikä kertoo, että osoitetta saa vielä käyttää, mutta uusien yhteyksien luomista kyseisellä osoitteella tulee välttää, mikäli käytettävissä on vaihtoehtoisia Preferred-osoitteita. Kun Valid-elinikä on umpeutunut, osoitetta ei voi enää käyttää lähde- tai kohdeosoitteena.

Käytettäessä DHCPv6-protokollaa osoitteiden jakoon joko suoraan tai DHCPv6-PD-mekanismilla, asiakasreitittimelle voidaan protokollan renew-viestien lähetysparametri asettaa huomattavasti lyhyemmäksi, esimerkiksi tunniksi. Silloin osoitteiden Preferred ja Valid -arvoja voidaan tarvittaessa muuttaa esimerkiksi valmistauduttaessa osoitteiden muutokseen.

Traficom suosittelee, että osoitteet ovat voimassa pitkään. Suositus Preferred-eliniäksi on 604 800 s eli 7 vuorokautta ja Valid-eliniäksi 2 592 000 s eli 30 vuorokautta. Suositus pitkästä Valid-eliniästä annettiin varmistamaan asiakkaan sisäverkon toiminta myös tilanteissa, joissa yhteys teleyrityksen verkkoon katkeaa esim. vikatilanteen vuoksi.

Asiakkaan sisäverkon koneet saavat osoitteensa sisäverkon reitittimiltä asiakkaalle jaetusta IPv6-verkkoalueesta. Sisäverkon reitittimet jatkavat toimintaa, vaikka verkkoyhteys ulkomaailmaan katkeisi ja IPv6-verkon osoitetta ei saataisi uusittua teleyrityksen DHCPv6-palvelimelta. Mikäli Valid-elinikä on liian

lyhyt ja se ehtii vanhentua ennen verkkoyhteyden palautumista, katoavat IP-osoitteet myös sisäverkosta. Tämä saattaa aiheuttaa sen, että sisäverkossa ei voi enää kommunikoida edes toisten sisäverkossa olevien koneiden kanssa. Tilanne poikkeaa IPv4:sta, jossa sisäverkon reititin yleensä jakaa edelleen DHCP:llä IPv4-osoitteita verkkoyhteyden katkeamisesta teleyrityksen verkkoon huolimatta. Pitkä Valid-elinikä varmistaa, että IPv6-osoitteet toimivat samantapaisella tavalla kuin IPv4-osoitteet.

Mikäli IPv6-verkon osoitteistusta joudutaan muuttamaan, tulisi noudattaa "make-before-break" periaatetta. Käyttämällä tarpeeksi aikaa ja tekemällä muutokset suunnitellusti voidaan muutokset tehdä aiheuttamatta asiakkaille mitään katkoja. Tarvittavat toimenpiteet ja niiden järjestys on dokumentissa RFC 4192 [14]. Ongelmakenttää on tarkasteltu laajemmin dokumentissa RFC 7010 [15]. Parhaita käytäntöjä osoitteiden vaihtumisesta aiheutuvien ongelmien välttämiseksi on kuvattu dokumenteissa [16] ja [17].

5.2.3 IPv6-verkkoalueen jakaminen asiakkaalle

Jotta IPv6-verkoista saada kaikki hyöty irti ja yli /64-kokoisista verkkoalueista on hyötyä, IPv6-verkkoalueet tulisi jakaa asiakkaalle pääasiassa reititettynä. Asiakkaalle voidaan tarjota myös suoraan kytkettyä tapaa, jossa operaattorin reititin jakaa asiakkaalle IPv6 osoitteita yhdestä erillisestä /64-verkkoalueesta. Tällä kytketyllä tavalla ei ole mahdollista käyttää muuta kuin yhtä /64 IPv6 verkkoa. Reititetty IPv6-verkkoalue tarkoittaa sitä, että operaattori reitittää asiakkaalle jaetun verkkoalueen asiakkaan reitittimelle, joka voi käyttää hyväkseen koko saamansa verkkoalueen ja jakaa siitä IPv6-verkkoja eteenpäin haluamallaan tavalla.

Asiakaslaitteet voivat muodostaa IPv6-osoitteet automaattisesti kahdella mekanismilla, joita ovat tilaton osoitteenmuodostus (SLAAC, Stateless Address Auto-Configuration) [18] ja tilallinen osoitteenmuodostus (DHCPv6) [19].

Tilaton osoitteenmuodostus hyödyntää reitittimen lähettämiä Router Advertisement (RA) -viestejä, joista käy ilmi asiakaslaitteen käytettävissä olevat /64-verkkoalueet. Asiakaslaite luo itselleen osoitteen ja tarkistaa, ettei se ole käytössä. Käyttäessään tilatonta osoitteenmuodostusta, teleyrityksen on suositeltavaa jakaa jokaiselle liittymälle oma /64-verkkoalue, jotta tilaajan tunnistaminen käytetyn IPv6-verkkoalueen perusteella on jälkikäteen mahdollista.

Tilallisessa osoitteenmuodostuksessa osoite anotaan DHCPv6 palvelimelta. RA-viestissä on tällöin "Managed Config" -lippu, joka viittaa DHCPv6:n käyttöön. DHCPv6-palvelimet tallettavat tyypillisesti tiedot jaetuista osoiteavaruuksista ja yksittäisistä osoitteista palvelimen lokitiedostoon.

DHCPv6:n mukana voidaan jakaa muutakin konfiguraatiotietoa, kuten DNS- ja NTP-palvelinten osoite ja asiakkaalle reititettävä verkkoalue (Prefix Delegation, DHCPv6-PD) [20]. Nämä tiedot voidaan jakaa myös DHCPv6:n tilattomalla toiminnolla, vaikka osoitteiden muodostus tapahtuisi SLAAC-mekanismilla. Tämä mahdollisuus kerrotaan RA-viestin ”Other Config” lipulla.

Reititetty IPv6-verkkoalue jaetaan asiakkaalle joko DHCPv6-PD:llä tai manuaalisesti konfiguroituna:

- DHCPv6-PD:ssä asiakkaan reititin lähettää DHCPv6-PD pyynnön operaattorin reitittimelle. Pyynnössä asiakkaan reititin voi esittää haluamaansa verkkoaluetta, esimerkiksi sille aiemmin delegoitua osoiteavaruutta. Operaattorin reitittimessä voi olla DHCPv6 palvelin, jolloin se voi tehdä delegoinnin itsenäisesti tai se välittää pyynnön keskitetylle DHCPv6 palvelimelle. DHCPv6 palvelin delegoi joko pyydetyn tai muun IPv6-verkkoalueen omien asetustensa mukaisesti. Välittäessään

vastauksen asiakkaan reitittimelle operaattorin reititin asettaa reititintaulun niin, että kyseinen verkkoalue reitite tään asiakkaan reitittimelle.

- Manuaalisessa konfiguraatiossa operaattori konfiguroi reitit valmiiksi ja kertoo asiakkaalle IPv6-osoitteen johon reitit on konfiguroitu. Tyypillisesti tämä vaatii erillisen reititysverkon, jos koko asiakkaalle varattu verkkoalue halutaan antaa asiakkaan käyttöön.

Suositukset

Traficom suosittelee, että teleyritys jakaa IPv6-verkkoalueen automaattisesti ilman asiakkaalta vaadittavia toimenpiteitä ja tukee ainakin DHCPv6-PD:n käyttöä IPv6-verkkoalueen jakamiseen.

Vaihtoehtoisesti teleyritys voi hoitaa osoitteiden automaattisen jakamisen myös etähallinnalla tai tekemällä asiakkaan päätelaitteen määritykset asiakkaan puolesta.

Mikäli teleyritys ei käytä verkkoalueen automaattista jakamista (DHCPv6-PD:llä tai etähallinnalla) ja tarjoaa verkkoa manuaalisesti konfiguroituna, niin on suositeltavaa käyttää seuraavia arvoja:

- Mikäli jaetaan manuaalisesti konfiguroitu reitetty verkko, on operaattoripään reititin reititysverkon ::1-osoite ja asiakkaan reititin on reititysverkon ::2-osoite. Reititysverkko voi olla joko asiakkaalle jaetusta verkosta yksi /64-verkko tai täysin erillinen reititysverkko.

- Mikäli käytetään manuaalisesti konfiguroitua kytkettyä verkkoa, jossa asiakkaan päätelaite on asetettu siltaavaksi ja teleyritys jakaa linkille yhden /64:sen SLAACilla, on suositeltavaa, että linkille jaetaan viimeinen /64 asiakkaalle varatusta verkkoalueesta. Suositus on annettu siksi, että näin verkkoalueen ensimmäinen /64 jää asiakkaan muuhun käyttöön.

Jos asiakkaan päätelaite ei tue IPv6:tta asiakkaan päätelaitteen voi vaihtaa tai päätelaitteen voi asettaa sillaksi, jolloin päätelaitteet saavat osoitteet suoraan operaattorin linkkiverkosta. Tällöin teleyrityksen verkon on määräyksen 13 mukaisesti estettävä suora liikennöinti eri asiakkaiden välillä.

5.2.4 ICMPv6

ICMPv6-pakettien suodatusta on tehtävä erittäin varovaisesti. Traficom suosittelee noudattamaan RFC:ssä 4890 [21] kuvattuja suosituksia.

IPv6:ssa ICMP:hen on lisätty mm. ARP:n ja IGMP:n toiminnallisuudet sekä yllä mainittu RA-toiminnallisuus. Lisäksi moni muukin asia IPv6-arkkitehtuurissa nojaa vahvasti ICMPv6:n tukeen. Jos teleyritys poistaa ICMPv6-viestit verkosta, IPv6 lakkaa toimimasta.

Reitittimet eivät pilko IPv6-paketteja ja liian suuret paketit tiputetaan. Tämän vuoksi Path MTU Discovery (PMTUD) on oleellinen osa IPv6 toiminnallisuutta. Jotta IPv6-yhteys toimii, teleyrityksen on varmistettava, että

- reitittimen lähettämän ICMPv6-viestin lähdeosoite on reitite ttävissä (muuten reverse-path-forwarding tarkistus pudottaa paketin)

- palveluntarjoajan oma verkko-infra suojataan ulkopuolelta ja asiakkailta tulevalta liikenteeltä, mutta ainakin ICMPv6-viestien lähdeosoitteet pitää mainostaa reitityksessä

Monet ICMPv6-viestit on tarkoitettu toimimaan vain lähiverkon sisällä, jolloin paketti on lähetetty :: tai fe80::/10 -osoitteella ja/tai hop limit -arvolla 255. Näitä ovat esimerkiksi MLD- ja NDP-viestit (tyypit 130–138, 141–143, 148–149, 151–153.). Mikäli näitä viestejä pyrkii sisään verkon ulkopuolelta, ne voidaan suodattaa.

Toiset ICMPv6-viestit on tarkoitettu toimimaan verkkojen välillä, jolloin niiden lähdeosoitteiden pitää olla julkisia globaalisti reitittyviä osoitteita. Usein nämä viestit ovat reititinten lähettämiä, jolloin teleyrityksen on pidettävä huolta, että reitittimet käyttävät globaalisti reitittyviä osoitteita näiden viestien lähettämiseen. Käytännössä kaikki ICMP-tyyppikoodit 1-99 kuuluvat tähän ryhmään.

5.2.5 IPv6-laajennusotsikkokentät

IPv6 mahdollistaa joustavan mekanismin laajentaa IP-paketin kenttiä (extension headers). Toisin kuin IPv4:ssa laajennusmekanismi on kiinteä osa IPv6-protokollan toimintaa ja laajennuskenttien summittainen poistaminen (filtering) rikkoo suurella todennäköisyydellä päästä-päähän IP-yhteyden ja johtaa huonoon loppukäyttäjän palvelukokemukseen.

IPv6 laajennusmekanismin joustavuutta voidaan myös helposti väärinkäyttää, esimerkiksi palvelunestohyökkäyksen toteuttamiseen.

Traficom suosittelee, että teleyrityksen on oltava varovainen IPv6-laajennusotsikkokenttiin perustuvassa liikenteen suodattamisessa [22] ja suodattamista saa tehdä vain kun se on välttämätöntä ja siinä laajuudessa kuin se on välttämätöntä tietoturvasta huolehtimiseksi. Tällä perusteella teleyrityksen on syytä suodattaa tunnetut IPv6-laajennusotsikko- kenttiin perustuvat hyökkäykset. Vastaavasti muu eteenpäin välitettäväksi tarkoitettu liikenne on syytä päästää läpi sellaisenaan.

5.2.6 Yhdysliikenteen järjestäminen

Traficom suosittelee, että teleyritys järjestää IPv4- ja IPv6-verkkojen yhdysliikenteen yhteneväisesti. Tämä yksinkertaistaa häiriönhallintaa palveluntarjoajien välillä sekä mahdollistaa loppukäyttäjän Internet-yhteyden viiveiden pysymisen samalla tasolla riippumatta käytetäänkö IPv4- vai IPv6-yhteyttä.

5.3 Matkaviestinverkot

Matkaviestinverkkoihin on suositeltavaa soveltaa samoja suosituksia kuin kiinteään verkkoon, aina kun se on mahdollista.

Traficom suosittelee, että yhdelle asiakkaalle jaetaan /56:n pituinen verkkoalue. Työryhmä on tunnistanut, että päätelaitteet tulevat rajoittamaan sitä, miten IPv6-osoitteita voidaan jakaa päätelaitteelle. Esimerkiksi suosituksen laatimishetkellä puhelimet tukivat useamman /64:n jakoa rinnakkaisilla verkkoyhteyksillä, mutta mokkulat käytännössä vain yhtä verkkoyhteyttä ja sen mukaisesti vain yhden /64:n jakoa päätelaitteelle.

Traficom suosittelee, että käyttäjä voi käyttää samaa APN-nimeä sekä IPv4- että IPv6-liikenteelle.

5.4 Kiinteät verkot kun natiivi IPv6 ei ole teknisesti mahdollinen

Valitettavasti osa vanhemmista verkkolaitteista, esimerkiksi DSLAM-laitteista ja Ethernet-kytkimistä eivät tue natiivin IPv6:n tarjoamista (mm. DHCP optio 37 leimaaminen, IPv6 ryhmälähetykset ja tietoturva). Tämän vuoksi IPv6 on

mahdollista ottaa käyttöön näiden laitteiden takana olevissa liittymissä vain erilaisilla tilapäisratkaisuilla.

Traficom suosittelee, että teleyritykset tarjoavat käyttäjilleen natiivin IPv6-yhteyden (katso luvut 5.2 ja 5.3). Mikäli tämä ei ole edellä mainituista syistä mahdollista, Traficom suosittelee siirtymäajan mekanismiksi 6rd:tä [23].

Työryhmän näkemyksen mukaan 6rd (RFC 5969) on muita parempi tilapäisratkaisu, sillä siinä käytetään operaattorin omaa IPv6-verkkoaluetta ja asiakkaan osoite voi pysyä samana siirryttäessä natiiviin IPv6-toteutukseen. 6rd-tunneliparametrit voidaan jakaa IPv4 DHCP:llä asiakkaan päätelaitteelle ja 6rd relay -reitittimenä voi toimia normaali PE-reititin.

Ratkaisu on standardoitu ja sitä tukevia laitteita on saatavilla. Suomessa yleisesti käytössä oleva liiketoimintamalli missä kuluttaja-asiakkaat ostavat itse päätelaitteensa asettaa haasteen tarvittavan tuen löytymisestä asiakkaan CPE-reittimestä. Lisäksi haasteena ovat siltaavat päätelaitteet, sillä työryhmän näkemyksen mukaan markkinoilla ei ole päätelaitteita, jotka osaisivat sillata IPv4-liikenteen ja tehdä IPv6-liikenteelle 6rd-tunneloinnin.

6 Operaattorin kuluttajille tarjottavat tietoturva- ja muut oheispalvelut

Traficom pitää tärkeänä, että teleyritys pyrkii tarjoamaan käyttäjille samat oheispalvelut riippumatta käyttääkö käyttäjä IPv4- tai IPv6-yhteyttä. Internetyhteyden mahdollistavan verkkopalvelun lisäksi teleyrityksen on syytä varmistaa, että sen yhteyden kanssa tarjoamat lisäpalvelut kuten esimerkiksi sähköposti-, kotisivu- ja tietoturvapalvelut tukevat IPv6-yhteyttä.

Traficomin näkemyksen mukaan huomiota on syytä kiinnittää erityisesti myös käyttäjälle tarjottaviin hallinta- ja monitorointipalveluiden kuten käyttäjille tarjottavien sähköisten itsepalvelukanavien IPv6-tukeen eli mahdollisuuteen käyttää näitä myös IPv6-yhteydellä.

7 Käyttäjätiedotus

Ottaessaan IPv6 käyttöön kuluttajalaajakaistaliittymissä, teleyrityksen on syytä tarkistaa myös käyttäjille antamansa ohjeistus mukaan lukien asiakaspalvelun kautta saatava neuvonta. Ohjeistus on syytä päivittää ja asiakaspalvelu kouluttaa kunnolla ennen käyttöönottopäivää.

Ohjeistuksen osalta teleyrityksen on syytä kiinnittää huomiota etenkin käyttäjän liittymän ja sisäverkon tietoturvaan, kuten tarpeeseen ottaa käyttöön palomuuri tai tarkistaa nykyisin käytössä oleva palomuuriratkaisun IPv6-asetukset. Lisäksi teleyrityksen on syytä määritellä, millä päätelaitteilla IPv6-yhteys on ainakin käytettävissä.

Teleyrityksen on syytä varmistaa, että vianselvitykseen käytettävät työkalut tukevat myös IPv6-vianselvitystä. Asiakaspalvelun koulutuksessa on syytä kiinnittää huomiota eri protokollaversioiden mahdollisiin eroihin vianselvityksen kannalta ja etenkin tilanteisiin, joissa vain toinen (IPv4 tai IPv6) yhteys toimii.

Vianselvityksen osalta Traficom suosittelee huomiomaan dokumentin ripe-631 IPv6 Troubleshooting for Residential ISP Helpdesks [24].

8 Lähdeluettelo

[1] Broadband Forum TR-177 IPv6 in the context of TR-101, http://www.broadband-forum.org/technical/download/TR-177.pdf

[2] ripe-554 Requirements for IPv6 in ICT Equipment, http://www.ripe.net/ripe/docs/ripe-554

[3] RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6), https://ietf.org/doc/rfc3315/

[4] RFC 4649 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option, https://ietf.org/doc/rfc4649/

[5] RFC 4580 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option, https://ietf.org/doc/rfc4580/

[6] RFC 6911 RADIUS Attributes for IPv6 Access Networks, https://ietf.org/doc/rfc6911/

[7] IPv6 Dynamic Reverse Mapping, http://users.on.net/~rmibus/pymds/IPv6-auto-rDNS.pdf

[8] Python Modular DNS Server (pymds), http://code.google.com/p/pymds/

[9] Kazunori Fujiwara (JPRS), One implementation of IPv6 reverse DNS server, http://member.wide.ad.jp/~fujiwara/v6rev.html

[10] Liikenne- ja viestintäviraston määräys 67 A/2015 M teletoiminnan tietoturvasta, https://finlex.fi/fi/viranomaiset/normi/480001/44046

[11] 7084 Basic Requirement for IPv6 Customer Edge Routers, https://ietf.org/doc/rfc7084/

[12] RFC 6092 Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service, http://tools.ietf.org/html/rfc6092/

[13] ripe-690 Best Current Operational Practice for Operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose, https://www.ripe.net/publications/docs/ripe-690

[14] RFC 4192 Procedures for Renumbering an IPv6 Network without a Flag Day, https://ietf.org/doc/rfc4192/

[15] RFC 7010 IPv6 Site Renumbering Gap Analysis, https://ietf.org/doc/rfc7010/

[16] ID Reaction of Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events, https://datatracker.ietf.org/doc/draft-ietf-v6ops-slaac-renum/

[17] ID Improving the Reaction of Customer Edge Routers to Renumbering Events, https://datatracker.ietf.org/doc/draft-ietf-v6ops-cpe-slaac-renum/

[18] RFC 4862 IPv6 Stateless Address Autoconfiguration, https://ietf.org/doc/rfc4862/

[19] RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6), https://ietf.org/doc/rfc3315/

[20] RFC 3633 IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6, https://ietf.org/doc/rfc3633/

[21] RFC 4890 Recommendations for Filtering ICMPv6 Messages in Firewalls, https://ietf.org/doc/rfc4890/

[22] RFC 7045 Transmission and Processing of IPv6 Extension Headers, https://ietf.org/doc/rfc7045/

[23] RFC 5969 IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification, https://ietf.org/doc/rfc5969/

[24] ripe-631 IPv6 Troubleshooting for Residential ISP Helpdesks, https://www.ripe.net/publications/docs/ripe-631

Liikenne- ja viestintävirasto Traficom

PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

ISBN 978-952-311-720-4
ISSN 2669-8757 (verkkojulkaisu)

TRAFICOM
Liikenne- ja viestintävirasto