



RIIGI INFOSÜSTEEMI AMET

## **IPv6 kasutuselevõtt – hetkeseis ja soovitused**

2023



## Sisukord

<b>Sissejuhatus.....</b>	<b>3</b>
<b>Levinumad hirmud ja eelarvamused.....</b>	<b>4</b>
<b>Miks tuleb IPv6 kasutusele võtta?.....</b>	<b>8</b>
<b>Riigi Infosüsteemi Ameti soovitus.....</b>	<b>10</b>
<b>Kuidas alustada IPv6-ga? .....</b>	<b>11</b>
<b>Loe lisaks .....</b>	<b>12</b>



## Sissejuhatus

IPv6 on kõige hiljutisem versioon internetiprotokollist<sup>1</sup>, mille roll on asendada juba 1980. aastate algusest kasutatud IPv4 internetiprotokoll. IPv6 loodi, sest unikaalseid IPv4-aadresse ei oleks enam pikas perspektiivis jätkunud. Kuigi IPv6 loomisest on samuti möödas juba mitukümmend aastat (esialgsed kavandid mõeldi välja 1990. aastatel), ei ole selle rakendamine olnud väga kiire, sest hakati kasutama IPv4 võrguaadresside teisendamist ehk NAT-imist, mis IP-aadresside puudujääki ajutiselt kompenseeris. Eestis on viimase kümne aastaga tehtud IPv6 rakendamisel küll edusamme, kuid töö selle kasutuselevõtmisel peab kiirenema, kuna see on konkurentsivõimelise digiriigi säilitamise vaatepunktist oluline. Maailma juhtivad majandusriigid nagu Ameerika Ühendriigid, Hiina ja India tahavad näiteks nii kiiresti kui võimalik ainult IPv6-põhiseid IT-lahendusi kasutama hakata. Valge Maja plaani kohaselt, mis avaldati 19. novembril 2020, peavad 2023. aasta lõpuks töötama vähemalt 20% USA föderaalvõrgus internetiprotokoll kasutavatest varadest ainult IPv6-ga, 2025. aasta keskpaigaks peab sama näitaja olema juba vähemalt 80%<sup>2</sup>. Hiina eesmärk on liikuda täielikult IPv6-põhiste lahenduste peale aastaks 2030<sup>3</sup>. 2022. aasta lõpuks ületas Hiinas IPv6 kasutajate hulk juba 700 miljoni piiri<sup>4</sup>. Indias aga peavad alates eelmisest aastast toetama kõik valitsusasutused IPv6-põhiseid lahendusi, samuti tuleb alates sellest aastast India kohalikel telekommunikatsiooniettevõtetel pakkuda klientidele võrguseadmeid, millel on IPv6 võimekus<sup>5</sup>. Need on ainult mõned näited, kuidas teised riigid sellele teemale keskenduvad. Euroopa Liit on hakanud samuti üha laialdasemalt IPv6 rakendamise vajalikkusele tähelepanu juhtima. IPv6 on välja toodud ühena viiest interneti arenguga seotud kategooriast, millele on EL enda fookuse seadnud<sup>6</sup>. Ühes Euroopa Komisjoni strateegias, mis üritab lahendada majanduse digitaliseerimisega seotud probleeme, mainitakse ainukese standardina nimeliselt vaid IPv6<sup>4</sup>. Samuti rõhutatakse IPv6 olulisust 2020. aastal avaldatud Euroopa Liidu küberturvalisuse strateegias<sup>7</sup>.

Arvestades kõike eelnevat on õigustatud ootus, et ka Eestis kiireneb IPv6 rakendamine, kuigi mõned võrgud ja pärandrakendused võivad jääda tõenäoliselt veel aastateks IPv4 sõltuvaks<sup>8</sup>. Käesoleva dokumendi eesmärgiks on ümber lükata IPv6 rakendamisega seotud

---

<sup>1</sup> Internetiprotokoll teeb võimalikuks võrkudevahelise andmevahetuse IP-aadresside põhjal.

<sup>2</sup> <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf>

<sup>3</sup> [https://www.theregister.com/2021/07/26/china\\_single\\_stack\\_ipv6\\_notice/](https://www.theregister.com/2021/07/26/china_single_stack_ipv6_notice/)

<sup>4</sup> <https://news.cgtn.com/news/2023-04-03/China-s-IPv6-active-users-exceed-700-mln-1iHtU8Jscmc/index.html>

<sup>5</sup> <https://www.sidn.nl/en/news-and-blogs/governments-everywhere-make-ipv6-mandatory>

<sup>6</sup> <https://ec.europa.eu/internet-standards/>

<sup>7</sup> <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>

<sup>8</sup> <https://www.rfc-editor.org/rfc/rfc6180>



hirmud ja eelarvamused, selgitada, miks IPv6 kasutamine on mõttekas ja anda soovitusi, mida tuleks selle rakendamisel arvestada.

## Levinumad hirmud ja eelarvamused

**IPv6 rakendamine on kulukas.** Organisatsioonid võivad IPv6 rakendamises näha kulutust millessegi, mis neil juba on ehk interneti kasutamise võimalusse. Seetõttu ei pruugi nad sageli mõista IPv6 kasutuselevõtmiseks tehtava investeeringu mõttekust. IPv6 rakendamine ei pruugi olla aga ületamatult kulukas. Üldjuhul on selle rakendamisega võimalik arvestada juba erinevates planeerimisprotsessides, mis organisatsiooni IT-lahendusi puudutavad, näiteks uute seadmete ja tarkvarade soetamisel või tarkvara arendamisel IPv6-ga ühildumist varakult silmas pidades. Organisatsioonidele on tehtud IPv6 rakendamine juba ka lihtsamaks, sest näiteks kõikides kaasaegsetes operatsioonisüsteemides (sh mobiiliseadmetes) on IPv6 tugi tegelikult olemas<sup>9</sup>.

**Kui kõik töötab, miks midagi muuta.** Paratamatult võib organisatsioonide juhtidel tekkida küsimus, et kui praegu toimivad IT-lahendused väga edukalt, siis miks peaks midagi muutma. Paraku ei jää tehnoloogia arengus seisma, vaid sammub alati edasi. Kuigi täna võivad lahendused IPv4 peal toimida, on kasulik siiski muutustega kaasas käia. Uute tehnoloogiate kasutuselevõtt aitab muuhulgas ka konkurentsivõimele kaasa<sup>10</sup>.

**NAT-ist loobumine teeb IPv6 ebaturvalise lahenduse.** Aeg-ajalt arvatakse ka seda, et kuna IPv6 puhul ei pea NAT-imist kasutama, on tegu ebaturvalise standardiga. Siiski on selline mõtteviis veidi ekslik. NAT-imine ei takista otseselt sissetulevaid ühendusi või küberründeid, vaid selleks on muud tehnilised lahendused (nt tule müüri tasemel). NAT-imise eesmärk on tekitada unikaalsete IPv4-aadresside piiratuse tõttu lihtsalt rohkem aadressiruumi. NAT-imise kasutamise lõpetamine võib parandada läbipaistvust, mis võib omakorda suurendada ka turvalisust – logisid võib olla lihtsam lugeda ja nendest vajalik teave kätte saada, kui seadme ja välisvõrgu vahel ei ole mitut NAT-imisega seotud lahendust.

**IPv6 võimekusega kasutajaid ei ole veel piisavalt.** Viimase kümnendi jooksul on selliste kasutajate arv, kes IPv6 saaksid kasutada, kasvanud märkimisväärselt. Kasv on seotud mitme teguriga. Esiteks pakuvad maailma sideettevõtted klientidele üha enam IPv6 kasutamise võimalust, teiseks töötavad mitmed populaarsed teenused juba IPv6 peal (nt Google, Facebook) ning kolmandaks on vastav tugi olemas ka paljudel veebimajutuse ja pilveteenuste pakkujatel. Lisaks toetavad seda kaasaegsed operatsioonisüsteemid.

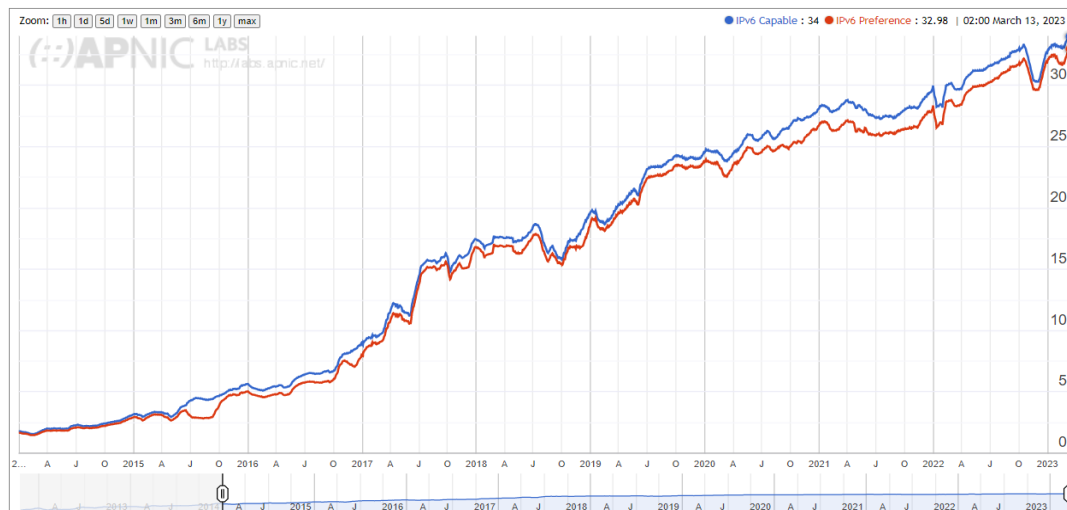
<sup>9</sup> <https://joinup.ec.europa.eu/sites/default/files/document/2019-12/Plum-EC-IPv6-Guidelines.pdf>

<sup>10</sup> [https://www.hm.ee/sites/default/files/documents/2022-10/haridus-ja\\_teadusstrat\\_2035\\_konkurentsivoime\\_visioon.pdf](https://www.hm.ee/sites/default/files/documents/2022-10/haridus-ja_teadusstrat_2035_konkurentsivoime_visioon.pdf)



Kasvutrendi iseloomustab ka alumine graafik (Graafik 1). Sinine joon näitab protsentuaalselt kasutajate hulka, kes saaksid külastada veebilehti, mis kasutaksid ainult IPv6 ning punane joon protsentuaalselt kasutajate hulka, kes IPv6 ja IPv4 kasutava veebiserveri puhul eelistaksid IPv6. 13. märtsi 2023. aasta seisuga oli “siniseid” kasutajaid kokku 34 protsenti kogu kasutajate hulgast ning “punaseid” kasutajaid 32,98 protsenti kogu kasutajate hulgast. Eestis olid 13. märtsil 2023. aastal vastavad näitajad 38,17 ning 37,9 (Graafik 4).

### Use of IPv6 for World (XA)



**Graafik 1.** IPv6-e kasutamise võimekus maailmas 2014 – 2023

**Allikas:** APNIC<sup>11</sup>

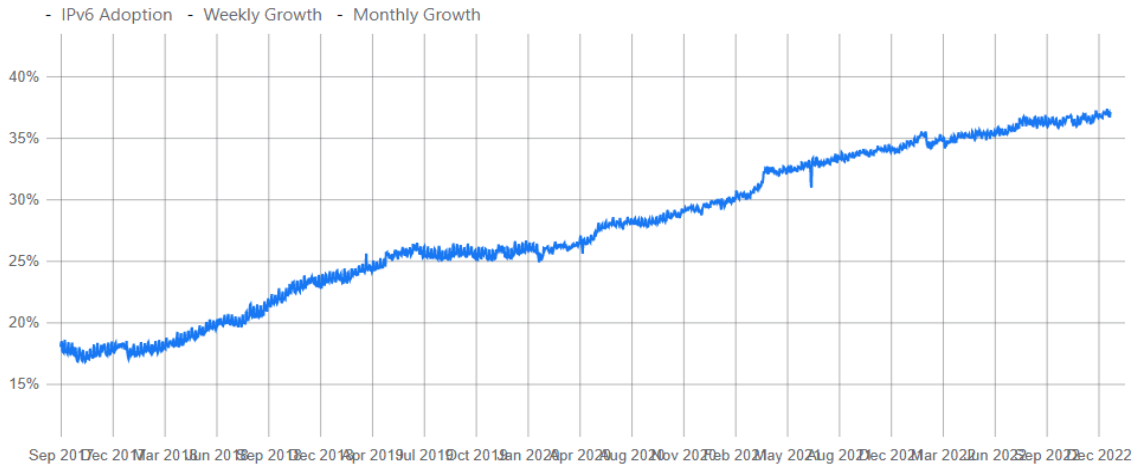
Google'i ja Facebooki andmed (Graafik 2 ja 3) näitavad samuti selget kasvu IPv6 kasutuselevõtus. Kui 2014. aasta lõpus oli vaid 5,5% Google'i kasutajatest IPv6 kasutamise võimalus olemas, siis 2023. aasta märtsiks oli see kasvanud 40% peale (Graafik 3). Facebooki kasutajatel on samuti IPv6 kasutamise võimalus paranenud – kui 2017. aasta lõpus sai seda teha 18% kõikidest Facebooki kasutajatest, siis 2023. aasta märtsiks oli vastav protsent tõusnud 37% peale (Graafik 2). Eestis saavad märtsi seisuga 36,8% Facebooki kasutajatest vajadusel IPv6 kasutada (Graafik 5).

<sup>11</sup> <https://stats.labs.apnic.net/ipv6/XA>



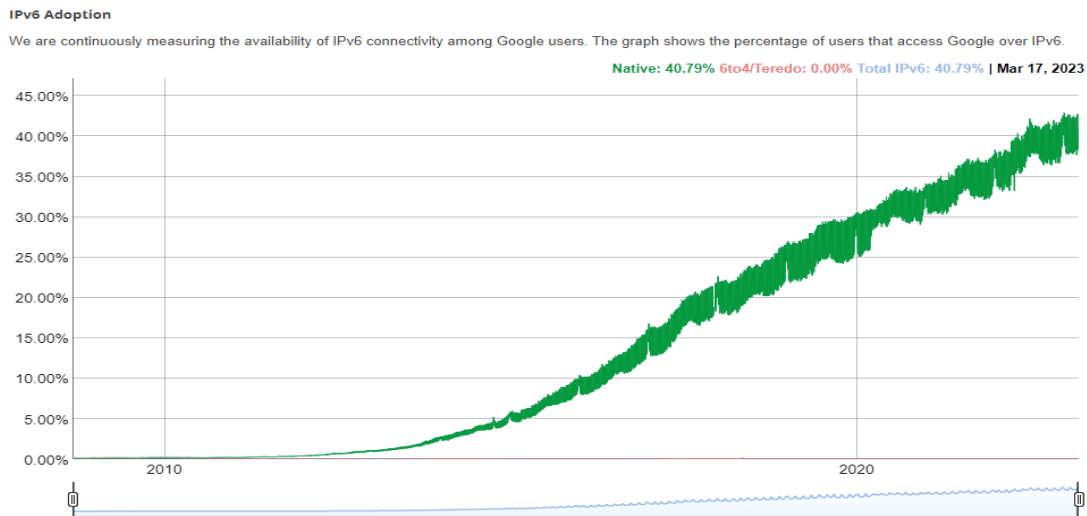
### IPv6 Adoption

Export All ▾



**Graafik 2.** IPv6 võimekusega Facebooki kasutajate osakaal kogu Facebooki kasutajate hulgast maailmas

**Allikas:** Facebook<sup>12</sup>



**Graafik 3.** IPv6 võimekusega Google'i kasutajate osakaal kogu Google'i kasutajate hulgast maailmas

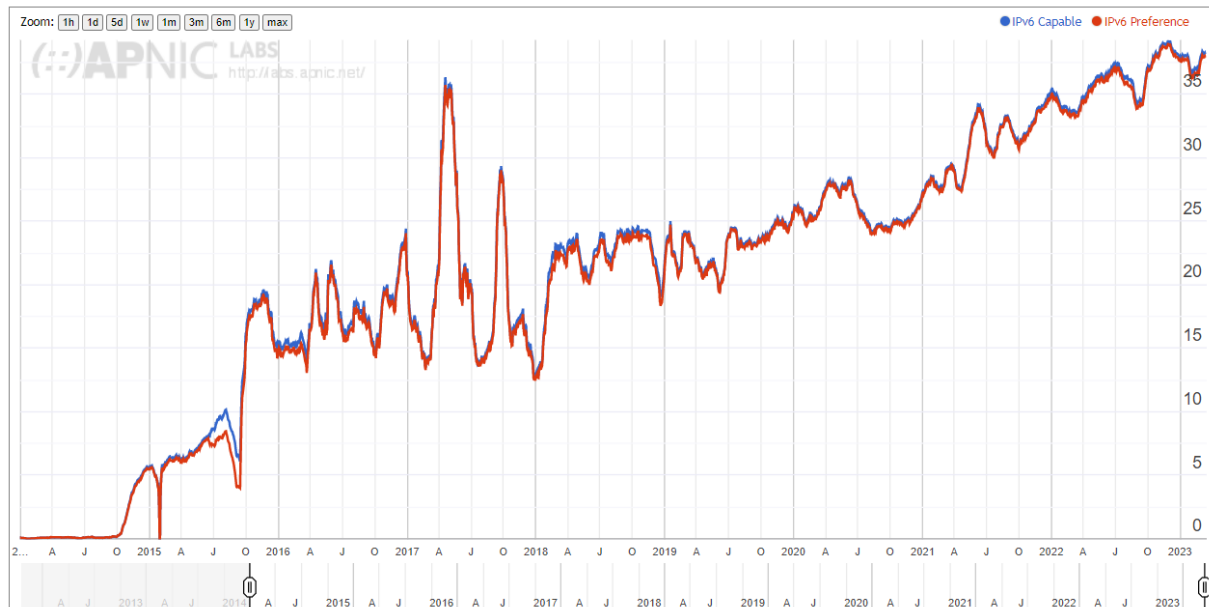
**Allikas:** Google<sup>13</sup>

<sup>12</sup> <https://www.facebook.com/ipv6/>

<sup>13</sup> <https://www.google.com/intl/en/ipv6/statistics.html>

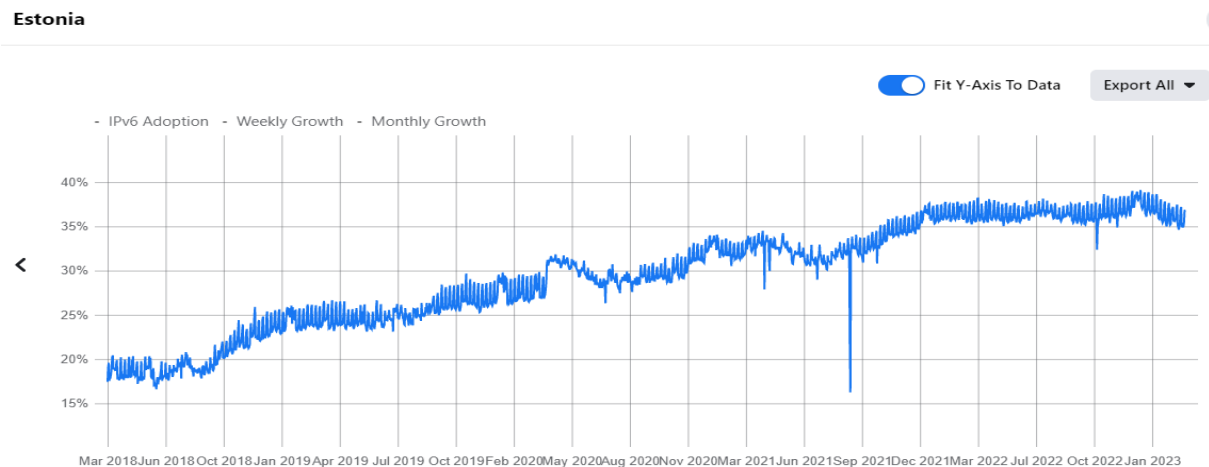


## Use of IPv6 for Estonia (EE)



**Graafik 4.** IPv6 kasutamise võimekus Eestis 2014 – 2023

**Allikas:** APNIC<sup>14</sup>



**Graafik 5.** IPv6 võimekusega Facebooki kasutajate osakaal Eestis

**Allikas:** Facebook<sup>15</sup>

IPv6 kasutamise võimekus on seega Eestis kui ka mujal maailmas 30-40 protsendi vahel. Eelnevalt viidatud numbrid kehtivad avalike võrkude puhul. Suure tõenäosusega on Eesti

<sup>14</sup> <https://stats.labs.apnic.net/ipv6/EE?o=cXEw30x1r1>

<sup>15</sup> [https://www.facebook.com/ipv6/?tab=ipv6\\_total\\_adoption](https://www.facebook.com/ipv6/?tab=ipv6_total_adoption)



organisatsioonide sisevõrkude IPv6 võimekuse tase mõneti madalam, kuid täpseid numbreid ei ole võimalik välja tuua. Eestis pakuvad sideettevõtted IPv6 varieeruvalt. Dokumendi kirjutamise hetkel saab Riigivõrgu ning Hariduse ja Teaduse andmesidevõrgu (EENet) klient IPv6 aadressid siis, kui ta neid teenusepakkujalt küsib, Telia toetab IPv6 vaid kaabluga interneti puhul, Elisa vaid mobiilse interneti puhul ning Tele2 ei toeta IPv6 ei kaabel- ega ka mobiilse interneti puhul.

## Miks tuleb IPv6 kasutusele võtta?

IPv6 kasutamiseks on veel teisigi argumente, mis on seotud eelkõige uute tehnoloogiate tuleku, turvalisuse, efektiivsuse, majanduslike tegurite ning rahvusvahelise olukorraga.

### Uute tehnoloogiate kasutuselevõtt eeldab IPv6 olemasolu

- IPv6-l on kandev roll juba müügis olevate seadmete teenindamisel. IoT ehk „asjade interneti“ seadmete üha kasvav populaarsus, nutikodud ja pilvepõhiste lahenduste kasv suurendavad nõudlust unikaalsete IP-aadresside järele. Samuti panustab IPv6 vajalikkusesse 5G ja Wi-Fi 6 kasutuselevõtt, mille abil on ettevõtetel võimalik kasutada üha rohkem seadmeid (nt tööstusautomaatikaseadmeid), mis kõik vajavad IP-aadresse<sup>16</sup>. Seadmed (nii virtuaalsed kui ka füüsilised) ja tarkvarad ei saa hakkama ilma IPv6 toeta.
- Arendatavad (ja juba arendatud) tehnoloogiad ei pruugi IPv4 enam toetada. Näiteks on IoT-lahenduste jaoks välja arendatud Matter-nimeline standard, mis on loodud IPv6 baasile<sup>17</sup>. Matter kasutab siiski ka BLE (Bluetooth Low Energy) tehnoloogiat, mis ei rakenda IP-d<sup>17</sup>. Google'i hinnangul teeb BLE tehnoloogia lihtsalt aga Matteri standardit kasutavate seadmete kasutuselevõtu hõlpsamaks<sup>17</sup>. IPv6 on oluline roll Matteri standardit kasutavate seadmete eesmärgipärase toimimise võimaldamiseks<sup>17</sup>. Selliseid asjade interneti seadmeid, mis Matteri standardit kasutavad, müüakse juba Eestis.

### Turvalisus

- Ründajatel on IPv6-aadresside skaneerimine võrreldes IPv4-aadressidega märgatavalt ebamugavam, sest unikaalseid IP-aadresse on IPv6 puhul lihtsalt palju rohkem.
- IPv6 puhul on igale teenusele võimalik anda unikaalne ja avalik IP-aadress ning selle aadressiga saab siduda täpselt teenuse jaoks sobiva tulemüürireeglistiku.

<sup>16</sup> <https://blogs.cisco.com/networking/transitioning-to-ipv6-for-simplicity-efficiency-and-modernization>

<sup>17</sup> <https://developers.home.google.com/matter/primer#prerequisites>



- IPv6 puhul on DDoS-rünnakute tõrjumine täpsem, sest igal rünnet teostaval seadmel (nii virtuaalsel kui ka füüsilisel) on unikaalne IP-aadress. Unikaalsed IP-aadressid teevad tõrjumise täpsemaks, kuna eemaldavad probleemi, mis tekib CGNATI (Carrier Grade NAT) kasutamisel. Nimelt jagavad CGNATI puhul paljud kliendid üht välist avalikku IP-aadressi. Sageli tõrjutakse aga DDoS-rünnakute puhul esmalt IP-aadressid, kust pahaloomulised päringud tulevad. Blokeeritud IP-aadresside hulka võib sattuda aga selline avalik aadress, mida kasutavad paljud erinevad kodused ühendused. Kuidas? Näiteks on ühe inimese kodune arvuti üle võetud ja sealt tehakse inimesele teadmata DDoS-rünnakutele viitavaid päringuid. Kuna see seade jagab välist IP-aadressi tuhandete teiste seadmetega (teiste telekommunikatsiooniettevõtete klientide seadmetega), blokeeritakse lisaks ründeliiklusele ka kõik seda sama välist IP-aadressi kasutavad legitiimsed internetikasutajad. IPv6 lahendaks selle probleemi, kuna igal seadmel on standardist tulenevalt ette nähtud unikaalne avalik IP-aadress.
- IPv6 on juba riistvara tasandil olemas täna enamikes seadmetes, mida poest saab osta. Isegi, kui IPv6 mingites lõikudes eemaldada, satuvad klientseadmed paratamatult võrkudesse, millel on IPv6 tugi olemas. See tähendab, et turvet tagavad süsteemid ning nendega töötavad inimesed peavad olema võimelised IPv6 seirama ning turvalisust tagama.

### **Efektiivsus**

- Võrguaadresside teisendamist ehk NAT-imist ei pea kasutama, mis teeb marsruutimise kiiremaks, lihtsamaks ja töökindlamaks.
- IPv6 on veebikasutaja vaatest kiirem (keskmiselt 10%-40% väiksem latentsusaeg ja APNICi andmetele tuginedes Eestis ligi 4ms kiirem<sup>18</sup>). Näiteks 2020. aastal ärgitas Apple rakenduste arendajaid kasutama IPv6, sest see on kuni 40% kiirem kui IPv4<sup>19</sup>.
- IPv6 on võimalik kasutada väiksemaid marsruutimistabeleid<sup>20</sup>, mis teeb marsruutimise efektiivsemaks.

### **Majanduslikud tegurid**

- IPv6 on odavam, eriti pikas perspektiivis. Näiteks küsivad avalikud pilveteenusepakkujad juba täna IPv4-aadresside eest lisatasu. Kui 2020. aastal müüdi IPv4-aadresse umbes 19 euro eest tükk, siis eelmisel aastal oli nende tükihind

<sup>18</sup> <https://stats.labs.apnic.net/v6perf/EE>

<sup>19</sup> <https://www.zdnet.com/article/apple-tells-app-devs-to-use-ipv6-as-its-1-4-times-faster-than-ipv4/>

<sup>20</sup> Marsruutimistabelid on nimekirjad IP-aadressidest koos juhistega, kuidas aadressideni jõuda.



tõusnud kohati juba 47 euroni<sup>21</sup>. Ressurss, mida on piiratud hulk, muutub aja kulgedes paratamatult kallimaks.

- IPv4 on muutumas ajas taakvaraliseks tehnoloogiaks<sup>22</sup>. Taakvara kasutamisega võivad kaasneda aga täiendavad kulud. Kulud võivad olla seotud näiteks IPv4 infrastruktuuri ülalpidamisega<sup>23</sup>.
- Kuna IPv6 ja IPv4 omavahel tehniliste eripärade tõttu otse ei ühildu, võib ainult IPv4 kasutamine organisatsioonile probleeme tekitada, sest erinevad teenused ei pruugi lihtsalt enam tulevikus toimida. Teenuste toimepidevus on aga ettevõtetele ja asutustele kriitiliselt oluline.

### Rahvusvaheline olukord

- Paljud riigid on juba kehtestanud nõude valitsusasutustele, et nad liiguks lähiaastatel ainult IPv6-põhiste lahenduste peale (kajastatud sissejuhatuses). Seetõttu ei ole Eestil mõistlik jääda selles osas pealtvaatajaks, sest konkurentsieelise ja teenuste käideldavuse tagamine nõuab lähitulevikus IPv6 rakendamist.

## Riigi Infosüsteemi Ameti soovitus

- Lähtudes eelnevast soovitab Riigi Infosüsteemi Amet IPv6 rakendada kõikide avalikult kättesaadavate teenuste puhul juba täna ehk võimalikult kiiresti.
- Lõpp-punktide (kontori- ja mobiiliseadmete) andmesideühenduse valikul veenduge, et teie sideteenuse pakkuja suudab pakkuda IPv6 tuge.
- Juhul, kui kasutate oma infrastruktuuri, siis veenduge, et teie sideteenuse pakkuja suudab pakkuda IPv6 alusühendust ning vajalikus suuruses IP aadressivahemikku. Aadressivahemiku suurus sõltub teie vajadustest. Vajaliku suuruse määratlemisel võite abi leida RFC6177-st.<sup>24</sup>
- Juhul, kui kasutate välise teenusepakkuja infrastruktuuri, siis veenduge, et teenusepakkuja suudaks tagada IPv6 toe nii baasinfstruktuuris kui ka alusühenduses.

<sup>21</sup> <https://www.akamai.com/blog/trends/10-years-since-world-ipv6-launch>

<sup>22</sup> <https://joinup.ec.europa.eu/sites/default/files/document/2019-12/Plum-EC-IPv6-Guidelines.pdf>

<sup>23</sup> <https://esynergy.co.uk/insights/blog/the-hidden-costs-of-legacy-tech/>

<sup>24</sup> <https://www.rfc-editor.org/rfc/rfc6177.html>



## Kuidas alustada IPv6-ga?

- 1) Koostage plaan, mis kaardistab IPv6 kasutamise võimalikkust – millised seadmed ja tarkvarad sellega juba ühilduvad ja millised mitte, kui palju IPv6 aadresse läheb vaja, kas kriitilised võrguteenused (nt DNS) toetaksid IPv6 jne. Ülevaatliku plaani abil on hiljem lihtsam edasi liikuda. RIPE on kirjeldanud enda kodulehel, kuidas näiteks plaani loomisega alustada. Samuti võib abi leida [siit](#).
- 2) Enamik pilve- ja virtuaalsete privaatserverite (VPS) teenusepakkujaid peaksid juba täna toetama IPv6 rakendamist. Mõnel juhul tuleb see aktiveerida manuaalselt. Juhul, kui teenusepakkujal ühtegi vastavat juhendit ei ole, võtke temaga ühendust ning uurige, milliseid samme on vaja teha, et tugi sisse lülitada. Juhul, kui teenusepakkuja ei toeta IPv6, kaaluge teenusepakkuja vahetust.
- 3) IPv6 rakendamine võib organisatsiooni IT-töötajatelt nõuda uusi teadmisi, mille tõttu on vaja neid koolitada.
- 4) Enda infrastruktuuri kasutamise puhul koostage IPv6 aadresside haldamiseks aadressiplaan. RIPE on võrguarhitektidele loonud juhendi, kuidas aadressiplaani koostada. Juhendi leiata [siit](#).
- 5) Reserveerige vajalikus mahus IPv6 aadresse ja arvestage sealjuures, et IPv6 aadresse vajavad lähitulevikus ka sellised füüsilised seadmed, mis ei ole traditsiooniliselt seda nõudnud (külmikud, kohvimasinad jne). Seega reserveerige neid pigem suure varuga, sest unikaalseid aadresse pakutakse piisavalt.
- 6) Kontrollige üle kõik rakendatud turbemeetmed ja veenduge, et need toimiksid ka IPv6 puhul. Näiteks, kui te kasutate pääsuõiguseid reguleerivaid reegleid (*Access Control List* ehk ACL), veenduge, et need toimiksid soovitud kujul ka IPv6 aadressidega.
- 7) Kasutage IP-aadresside haldamise jaoks mõeldud lahendust (*IP address management* ehk IPAM), mis aitab IPv4 aadressiruumi ära kaardistada. IPAM-i kasutamine teeb samuti IPv6 ülemineku lihtsamaks.
- 8) Otsustage, millist üleminekulahendust kasutada ja konfigureerige sellest tulenevalt võrk. Võimalik on liikuda ka ainult IPv6 põhiste lahenduste peale, kuid see ei ole 2023. aastal veel mõistlik, sest mõned teenused vajavad töötamiseks veel IPv4.
- 9) Arvestage rakenduste arendamisel juba IPv6. Näiteks veenduge, et API-d toetaksid sellega, samuti peavad rakendused hakkama saama IPv6 aadresside formaadiga, mis erineb IPv4 aadressidest tunduvalt.
- 10) Testige IPv6 lahendusi testkeskkondades, enne kui need päriselt rakendate. Testimiseks on taas erinevaid võimalusi, mis sõltub vajadusest. Näiteks serverite puhul võite pingida testitava serveri IPv6 aadressi teiselt võrgus olevalt IPv6 kasutavalt virtuaalselt või füüsiliselt seadmelt. Nii näete, kas testitavat serverit on võimalik IPv6 kaudu kätte saada või mitte. Samuti on mitmeid avalikke veebilehti, mille abil saate IPv6 ühendusi testida.



- 11) Teenuste kokkupanekul tuleks vaadata IPv6 tuge võimalikult horisontaalselt, st et kui organisatsiooni kodulehel on juturobot, kuid see ei toeta IPv6, siis seda funktsionaalsust ei pea IPv6 peal pakkuma, vaid võite seda teha ajutiselt IPv4 baasil.

## Loe lisaks

1. NSA<sup>25</sup> nõuanded IPv6 turvaliseks rakendamiseks (2023) - <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3270451/nsa-publishes-internet-protocol-version-6-ipv6-security-guidance/>
2. Head turvapraktikad IPv6 rakendamisel (2020) - <https://theinternetprotocolblog.wordpress.com/2020/11/28/ipv6-security-best-practices/>
3. Kõik RIPE IPv6 dokumendid - <https://www.ripe.net/publications/docs/ripe-documents/ipv6-documents>
4. RIPE IPv6 koostamismaterjalid - <https://www.ripe.net/support/training/material/ripe-ncc-training-material#IPV6>
5. IPv6 rakendamise suunised Euroopa avalikele asutustele (2018) - <https://joinup.ec.europa.eu/collection/egovernment/document/guidelines-and-process-ipv6-public-administrations-europe>
6. Juhised IPv6 konfigureerimiseks Windowsis kogenud kasutajatele - <https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/configure-ipv6-in-windows> (2022)
7. Ülevaade IPv6 seotud korduma kippuvatest küsimustest - <https://www.sidn.nl/en/modern-internet-standards/ipv6>
8. ARINi<sup>26</sup> ülevaade, kuidas ühildada rakendusi IPv6 - [https://www.arin.net/resources/guide/ipv6/preparing\\_apps\\_for\\_v6.pdf](https://www.arin.net/resources/guide/ipv6/preparing_apps_for_v6.pdf)

---

<sup>25</sup> USA riiklik julgeolekuagentuur

<sup>26</sup> Ameerika regionaalne internetiregister