Koppla upp till internet med framtidssäkra IPv6-adresser

Praktisk vägledning för it-personal

www.pts.se

Innehållsförteckning

Inledning	3
Varför en praktisk vägledning?	4
Att införa IPv6	5
Planera	9
Genomföra	15
Avslutande ord	21
Användbara länkar	22
Begrepp och förkortningar	23

Inledning

Det har varit känt sedan länge. Det begränsade antalet IPv4-adresser kommer att ta slut. Hittills har nödlösningar räddat situationen, men det är inte en hållbar väg. Varje ny enhet – datorer och teknisk utrustning – som kopplas upp mot internet, måste ha en IP-adress för att fungera. När det inte finns fler adresser kan vi inte använda internet som vi vill. Lösningen är att införa IPv6.

Varför en praktisk vägledning?

Den här praktiska vägledningen vänder sig till er som har fattat beslut om att införa IPv6 och nu ska påbörja införandet. Med digitala tjänster avses i den här vägledningen främst sådana tjänster som kommunicerar externt med användare/kunder, det vill säga webbplats, e-post och DNS.

Den riktar sig till dig som har grundläggande förståelse för IP-adressering, nätverksdrift och förvaltning. Du förutsätts ha grundläggande kännedom om de begrepp och förkortningar som används. På sidan 23 finns en sammanställning över använda begrepp och förkortningar.

Vägledningen ger stöd genom hela införandeprocessen och underlättar för er att planera, genomföra och förvalta införandet på ett kostnadseffektivt och långsiktigt sätt. Vi vill också stödja ert arbete genom att bidra med argument, idéer och inspiration i arbetet med IPv6.

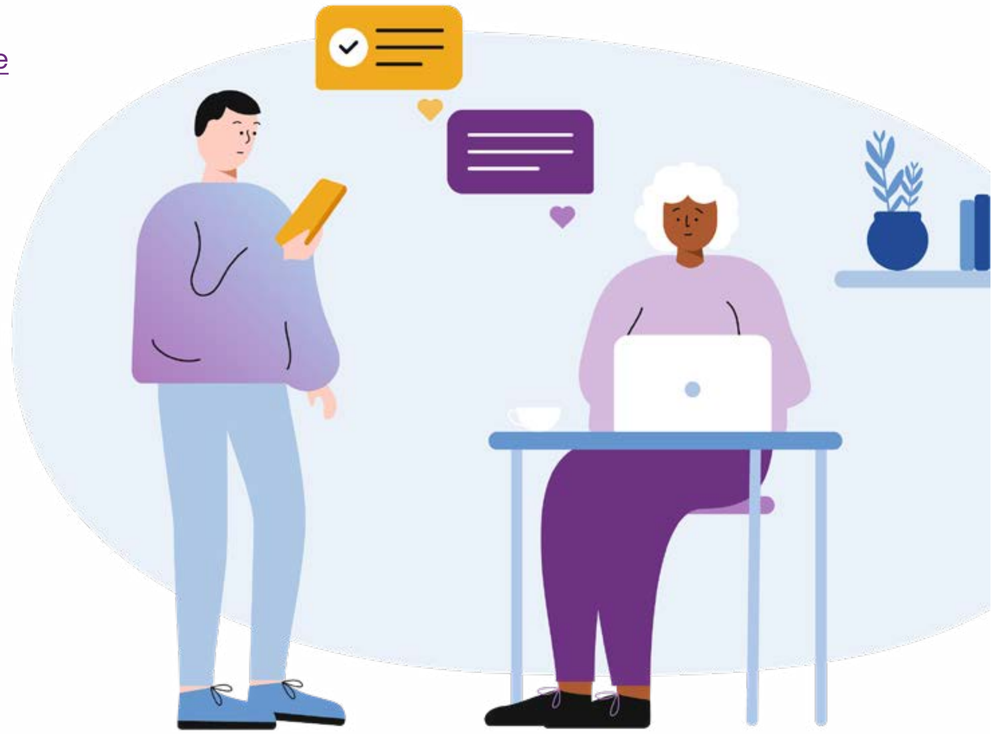
Vägledningen har tagits fram av PTS, med stöd av konsultbolaget Interlan Gefle AB, som en del i ett regeringsuppdrag om att främja och följa införandet av IPv6.

Införandet i offentlig sektor kommer också att följas genom webbtjänsten ”IPv6 i offentlig sektor” som tagits fram inom ramen för samma regeringsuppdrag.

Kontakta gärna PTS om du har frågor, via pts@pts.se

Läs mer om PTS arbete för att främja införandet av IPv6 i offentlig sektor på pts.se/ipv6

Läs mer om regeringsuppdraget på regeringens webbplats, regeringen.se/regeringsuppdrag



Att införa IPv6

Införande av IPv6 bör integreras i samtliga interna it-utvecklingsprojekt och processer istället för att bli ett eget separat projekt som riskerar att tynga organisationen. I allt arbete avseende nät, adressering, säkerhet och arkitektur ska både IPv6 och det äldre IPv4 tas med.

Arbeta i två faser

Många organisationer inom offentlig sektor som redan infört IPv6 har uppgett att införandet varken varit särskilt kostsamt eller tidsödande. Det framkommer en samstämmig bild om att det sällan eller aldrig har behövts köpas in ny hårdvara, då befintlig hårdvara redan har stöd för IPv6.

Arbetet med att införa IPv6 vid sidan av IPv4 för externa digitala tjänster, har ofta kunnat utföras i det dagliga arbetet, antingen helt utan konsultstöd, eller med ett fåtal konsulttimmar.

Även om det kan variera, bland annat på grund av organisationens storlek och hur många tjänster det handlar om, så har den tid som den egna it-avdelningen bedömts ha lagt ner på införande av IPv6 för externa digitala tjänster i de flesta fall uppgetts handla om cirka en arbetsvecka.

Planera och genomföra

Det är viktigt att införandet av IPv6, precis som annan it-utveckling, sker med ett systematiskt och planerat tillvägagångssätt för att behålla en fortsatt hög säkerhet och tillgänglighet. För att uppnå detta är det viktigt att starta i god tid och erhålla den kunskap som behövs.

Ett införande kan förenklat delas in i två faser – planera och genomföra. De två faserna innehåller i sin tur ett antal viktiga delmoment.

1. Planera
- Inventera it-miljön med sikte på framtiden.
- Planera och ta fram en adressplan.
- Beställ internetanslutning med IPv6.

2. Genomföra
- Aktivera internetanslutningen med IPv6.
- Fördela adresser enligt adressplanen.
- Konfigurera brandväggen.
- Aktivera IPv6 för serverplattformar.
- Kontrollera och förvalta.

Aktiviteter och råd inom respektive fas beskrivs närmare från sidan 9 (planera) och från sidan 15 (genomföra).

Inför planeringsstart

Tillsätt resurser för att underlätta och effektivisera införandet av IPv6 i organisationen. Målbild och tidplan kan variera utifrån organisationens storlek, behov och krav.

Om ni bedömer att ni behöver ta in externa konsulter för stöd i vissa delar av arbetet, finns hjälp att få via de ramavtal som finns för offentlig sektor (se sidan 12).

IPv6-arbetet bör dock inte i sin helhet läggas ut på externa konsulter. För att säkerställa att det finns kompetens internt behöver arbetet med att införa IPv6 integreras i den egna verksamheten.

Finns det behov av kompetensutveckling räcker det ofta med en generell utbildning om IPv6 för berörd it-personal.

Råd inför planeringsstart

Råd vid upphandling

Förenkla adressplanen

Börja i liten skala, inför IPv6 utifrån och in

Håll koll på att IPv6 fungerar

Råd inför planeringsstart

Råd vid upphandling

Ställ alltid krav på IPv6-stöd vid upphandling och anskaffning av all it-utrustning och alla tjänster. Om ni på regelbunden basis ser över era upphandlingsunderlag för it-utrustning och tjänster, säkerställ att kravet för IPv6-stöd alltid finns med. Beakta även krav på säkerhet och tillgänglighet. Då medför införandet av IPv6 inga direkta merkostnader i form av att ytterligare upphandling behöver genomföras.

Förenkla adressplanen

En plan över användningen av de egna IPv6-adresserna bör påbörjas tidigt i planeringsfasen. Det är givetvis ett levande dokument, men det viktiga är att man redan från början tänker på annat sätt än för det äldre interna IPv4-nätet som har mycket begränsade resurser.

Ta fram en adressplan och tänk på att adressplanen för IPv6 inte nödvändigtvis behöver följa IPv4-planen. Med den stora tillgången till subnät och IP-adresser som IPv6 möjliggör kan adressplanen ofta förenklas. Det gör också säkerhetsarbetet enklare.

Börja i liten skala, inför IPv6 utifrån och in

Ett grundläggande råd är att börja i liten skala. Dra nytta av att IPv4 och IPv6 kan samexistera, och inför IPv6 stegvis. Prioritera digitala tjänster som ni använder för extern kommunikation och som vänder sig till allmänheten, så att ni kan vara tillgängliga över både IPv6 och IPv4.

Inför IPv6 med perspektivet ”utifrån och in” och rådet är att prioritera de digitala tjänsterna i följande ordning:

1. Internetanslutning
2. Brandvägg med säkerhetsfunktioner
3. Extern auktoritativ DNS, webbplatser, e-post
4. L3-switchar
5. Aktivera IPv6 på interna resurser och datorer

Kom ihåg att all prioritering ska utgå från organisationens egna behov och resurser.

Håll koll på att IPv6 fungerar

Vid införande av ett nytt internetprotokoll är övervakning av tjänster som använder det nya protokollet av stor betydelse. När ni tagit steget till IPv6 på en extern tjänst är det viktigt att den upprätthålls och övervakas. En tjänst som är felaktig eller instabil över IPv6 leder till samma problem som för IPv4.

Planera

Planeringsfasen innehåller följande steg för ett genomtänkt införande:

– Inventera it-miljön med sikte på framtiden.
– Upphandla vid behov ny hårdvara, mjukvara eller tjänster.
– Planera och ta fram en adressplan.
– Beställ internetanslutning med IPv6.

Inventera it-miljön med sikte på framtiden

Innan IPv6 kan aktiveras på digitala tjänster och i ert interna nät är det viktigt att inventera nuläget i organisationens it-miljö och analysera det framtida behovet.

Om inventering inte nyligen har gjorts, är det dags att identifiera behov av åtgärder för att tjänster ska ha stöd för både IPv4 och IPv6, det vill säga dual stack.

Inventeringen ska omfatta såväl hårdvara (utrustning) som mjukvara såsom operativsystem och applikationer. Även om operativsystemet har dual stack så innebär det inte att alla programvaror har det.

Vid kommunikation på det interna nätet där både server och klientprogram har dual stack kan utvecklarna använda olika principer för vilket IP-protokoll som prioriteras och hur programmet agerar om ett av protokollen (IPv4 eller IPv6) inte kan anslutas. Det kan vara en fördel att titta specifikt på de verksamhetsspecifika eller egenutvecklade tillämpningarna, som inte finns tillgängliga på den allmänna it-marknaden, och identifiera eventuella brister i förhållande till dual stack-stödet.

Inventeringens omfattning påverkas av storleken på befintlig it-miljö och kvaliteten på befintlig dokumentation.

Inventera och dokumentera följande:

- Berörda serverplattformar avseende stöd för IPv6.
- Nätverksutrustning, nätverksstruktur och adressering på övergripande nivå med stöd för IPv6.
- Operativsystem samt programvaror med stöd för IPv6.
- Tjänster och funktioner som ansvaras för internt respektive funktioner som extern leverantör ansvarar för.

Utifrån denna inventering påbörjas arbetet med att införa IPv6. Om brister uppmärksammats kan det dock bli aktuellt att upphandla nya tjänster eller ny utrustning inför IPv6-införandet.

Upphandling av nya tjänster eller ny utrustning

Se över befintliga avtal

Diskutera med er leverantör om befintliga avtal omfattar anpassning till IPv6. Generella skrivningar i avtalet kan ibland möjliggöra detta. Om så inte är fallet, kan det vara möjligt att göra ett tillägg.

Förläng inte avtal som inte medger IPv6

Säkerställ att befintliga avtal omfattar den utrustning och de tjänster som ni behöver i framtiden, innan ni beslutar er för att förlänga avtalen.

Råd för kravställning vid upphandling

Här har vi sammanställt ett antal råd om vilka krav ni bör ställa vid en upphandling för att säkerställa stöd för IPv6.

Generella råd

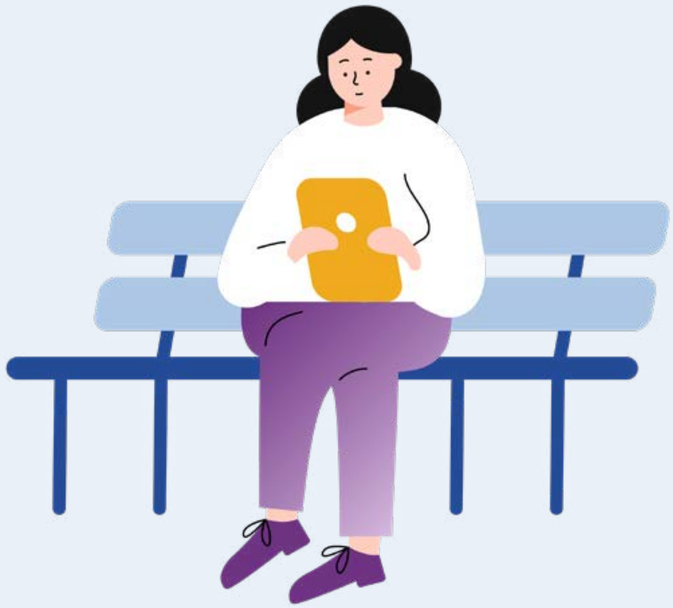
- Ny utrustning bör ha stöd för både IPv4 och IPv6 samtidigt, så kallad dual stack.
- Utrustning för IPv6 bör ha samma funktionalitet och prestanda som för IPv4.
- Programvaror som hanterar IP-adresser bör kunna hantera både IPv4- och IPv6-adresser.
- Ställ samma krav på tillgänglighet (upp- och nertid, inställelse- och åtgärdstid) på en tjänst som har dual stack, som för en med endast IPv4.

Specifika råd

- Om er e-post sköts av extern leverantör, ställ krav på att den har stöd för IPv6.
- Om e-postfiltrering sker externt, se till att leverantören stödjer IPv6 för både in- och utgående e-post.
- Om auktoritativ DNS sköts av extern leverantör, ställ krav på IPv6 för auktoritativ DNS.
- Brandväggen och dess inbyggda säkerhetsfunktioner ska ha stöd för IPv6. Brandväggen bör även ha ett skalskydd baserat på så kallad UTM-funktion.

UTM-funktionen innebär att brandväggen kan förses med till exempel spam- och antivirusskydd, IPS, IDS, VPN, filtrering av innehåll och domäner samt förhindra dataläckage.

När det gäller de krav som ställs vid upphandlingen ska de utgå från organisationens krav på funktion, tillgänglighet och säkerhet. Som regel gäller att ju fler säkerhetsfunktioner (krav) som kravställs, desto dyrare blir det. Se till att innebörden av kraven är kända, innan kravställning görs.



Använd inköpscentralernas ramavtal

Statens inköpscentral – avropa.se

Statens inköpscentral har ett flertal ramavtal inom it- och telekomområdet som statliga myndigheter, samt anslutna kommuner och regioner kan använda. Syftet är att samordna inköp för att åstadkomma besparingar. Ramavtalen finns på avropa.se. De är grupperade i flera områden, till exempel följande:

- Kommunikationstjänster inom tele- och datakom
- It-drift
- It-konsulttjänster
- Klienter
- Programvaror och tjänster
- Datacenter
- Telefoniprodukter

Avtalen är utformade på olika sätt och har olika detaljeringsgrad, vilket gör att varje organisation måste se till sina behov och inrikta sina krav utifrån dessa behov. I dagsläget finns möjligheter för beställare att införa krav om IPv6 i sin egen beställning. Avtalen ger möjlighet att erhålla både tjänster och utrustning, exempelvis följande:

- It-utbildning avseende IPv6
- Konsulttjänster för genomförandeplan för IPv6
- Internetanslutning

Kommuner och regioner som inte är anslutna till Statens inköpscentral kan använda SKL Kommentus ramavtal.

SKL Kommentus ramavtal

SKL Kommentus har ramavtal inom it-och telekomområdet som kan nyttjas av kommuner och regioner. Det finns flera ramavtal som kan vara till nytta och anpassas efter era behov vid IPv6-införandet.

Datakommunikation Sjunet 2018 som omfattar följande:
- Anslutningar till Sjunet
- Privata segment (lokala nät)
- Internetanslutningar

Programvaror och programvaror som molntjänst
Omfattar i princip alla typer av programvaror.

It-konsulttjänster 2016
Man kan avropa extern kompetens runt strategiframtagning, kravställning, implementering, förvaltning med mera.

Alla ramavtal för SKL Kommentus finns på sklkommentus.se

Tillgänglighet och säkerhet

Tillgänglighet och säkerhet i nät och tjänster ska fortsatt vara hög efter att ni har infört IPv6. Integrera därför befintligt säkerhets- och tillgänglighetsarbete vid införandet. Tänk på att införa IPv6 på ett kontrollerat sätt och se till att driften av IPv6 sker med samma kvalitet och säkerhet som IPv4. Om ni till exempel har DHCP-snooping och Dynamic ARP-inspection aktiverat bör ni aktivera DHCPv6-snooping och RA Guard också[1].

1 https://secureenduserconnection.se/wp-content/uploads/2010/06/SEC-Secure-End-user-Connection-2015-08-26.pdf

Planera och ta fram en adressplan

RIPE NCC tilldelar och administrerar IP-adresser i Europa och Mellanösternregionen. RIPE NCC har en policy för hur tilldelning av IPv6-adresser får ske (RIPE-738[1]) till sina medlemmar, så kallade LIR. En LIR kan exempelvis vara en operatör som tillhandahåller tjänster i form av internetanslutning, men även andra företag och myndigheter, kommuner eller regioner som själva ansökt om IP-adresser.

IPv6-adresser tilldelas på två olika sätt

- operatörsoberoende adresser – så kallade PI-adresser
- operatörstilldelade adresser – så kallade PA-adresser

Med PI-adresser kan ni behålla era IPv6-adresser i er nätverksstruktur, vilket kan vara av stor betydelse om ni exempelvis byter internetleverantör i framtiden. PI-adresser möjliggör också flera anslutningar till det egna nätet.

Statliga myndigheter, kommuner och regioner rekommenderas att använda PI-adresser. Tidigare fanns krav från RIPE NCC på multihoming (två eller flera internetleverantörer) för att få PI-adresser, men det kravet finns inte längre.

PI-adresser erhålls genom att ansöka om det via en valfri LIR, som i sin tur sköter kontakten med RIPE NCC[2]. Det är också möjligt att ansöka om PI-adresser direkt hos RIPE NCC, genom att bli medlem hos RIPE NCC och på så sätt själv agera som en LIR.

Kostnaden för att erhålla PI-adresser från en LIR uppgår till några tusen kronor per år. Att agera som eget LIR kräver mer tid och är mer kostsamt, men en fördel är att adresserna tilldelas direkt till er.

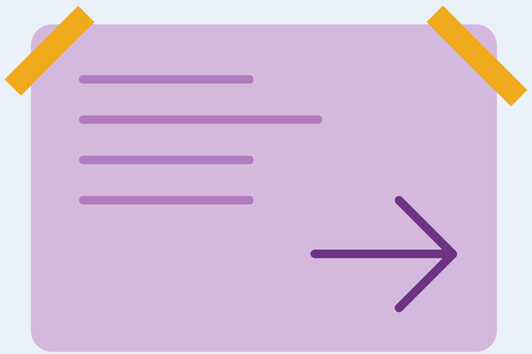
Ta fram en genomtänkt nätverksstruktur

En väl genomtänkt nätverksstruktur och adressplan är en förutsättning för fungerande IPv6-kommunikation. Det är viktigt att nätverksstrukturen blir bra från början eftersom den används under lång tid. För detta moment kan konsultstöd vara lämpligt om man ser ett sådant behov.

En rekommendation är att dela upp verksamheten i hela IP-nät som routas och hanteras som grupper i brandväggar. Den omfattande adressrymden i IPv6-tilldelningen ger möjlighet att tänka på nya sätt vad gäller adressering.
Till exempel kan skrivare med lätthet få ett eller flera subnät som kan dela säkerhetsregler i stället för att skrivarna hanteras enskilt.

På samma sätt kan grupper av applikationer/tjänster som till exempel interna webbsidor, biblioteksystem och skolsystem (inte nödvändigtvis servrar) sammanföras och hanteras i gemensamma nät.

Det som beskrivs ovan kan även med fördel användas på olika virtualiseringsplattformar och containersystem (som till exempel Kubernetes och Docker som är öppen källkod). IPv6 gör att mikrosegmentering med automatisk provisionering går att göra logiskt och överskådligt.



1 https://www.ripe.net/publications/docs/ripe-738

2 https://www.ripe.net/publications/docs/ripe-738#IPv6_PI_Assignments

Adressplan för IPv6

Det finns många olika sätt att skapa en adressplan för IPv6. Det går till exempel att skapa den efter IPv4-adressplanen, eller efter andra parametrar såsom VLAN ID, geografi, servergrupper, användargrupper, säkerhetszoner eller våningsplan i ett kontor. Det går även att strukturera planen på annat sätt, men det viktigaste är att den är strukturerad och alltid hålls uppdaterad.

Tidsåtgången för att ta fram en adressplan beror på de interna nätens storlek och komplexitet. Gäller det en liten organisation med få segment går det relativt fort. Gäller det en större organisation med flera hundra segment är det mer komplext och tar längre tid, men det rör sig i båda fallen om ett antal timmar och inte antal dagar.

Tips och idéer på adressplanering finns till exempel hos RIPE NCC.

Dynamiska eller statiska IP-adresser

Externa digitala tjänster såsom webbplats, e-post och DNS kräver statiska adresser. I övrigt är dynamiska IPv6-adresser att föredra framför statiskt tilldelade IPv6-adresser, även på servrar. Dynamiska adresser minskar komplexiteten och bör användas så långt det är möjligt både för IPv4 och för IPv6. I ett Windows Active Directory kan de flesta servrar använda dynamiskt tilldelade IPv6-adresser.

IPv6 har två sätt för dynamisk tilldelning av adresser: SLAAC och DHCPv6.

När det gäller interna nät är det en smaksak vilken man väljer. Med SLAAC genererar enheterna själva slumpmässiga adresser, medan DHCPv6 ger mer kontroll över vilka adresser en dator tilldelas och kan lämna över mer information som kan krävas för enhetens konfiguration. Ibland måste man i blandade miljöer använda båda för att mobila enheter med iOS- eller Android-operativsystem ska kunna använda både IPv4 och IPv6.

Trots att DHCPv6 har samma namn som DHCP för IPv4 så är grundfunktionerna inte desamma. Det viktigaste att tänka på i detta sammanhang är att DHCPv6 fokuserar, till skillnad från DHCP för IPv4, inte på MAC-adressen på en enhet utan använder DUID istället[1].

Vidare konfigurerar DHCPv6 i första hand inte den primära nätverkskonfigurationen (såsom default router och subnätmask), utan andra nödvändiga uppgifter för fungerande funktion (såsom HTTP-proxy, DNS-server och applikationsspecifika data som till exempel SIP-konfigurationsserver).

RIPE NCC:s motsvarighet i Nordamerika, ARIN, har tips om DHCPv6[2].

Beställ internetanslutning med IPv6

Statens inköpscentral (avropa.se) och SKL Kommentus inköpscentral (sklkommentus.se) har framtagna ramavtal, vilka kan användas för beställning av internetanslutning med IPv6, se sidan 12.

I rapporten ”Internetaccess – Definition” som är framtagen av Internetstiftelsen och Netnod finns ytterligare råd vid kravställning av olika krav på organisationens internetanslutning, se särskilt:

- IPv6 unicastförmedling (se beteckning 3.1 till 3.6)
- Adresstilldelning (se beteckning 4.2, 4.4 och 4.6)
- MTU (se beteckning 5.2).

1 https://tools.ietf.org/html/rfc8415#section-11
2 https://teamarin.net/2018/06/25/common-mistake-dhcpv6/

Genomföra

Genomförandet består av att införa IPv6 genom successiv och kontrollerad aktivering och driftsättning. Efter varje driftsättning krävs att övervakning sker för en bibehållen god funktion, säkerhet och tillgänglighet.

Genomförandet kan sammanfattningsvis delas upp i följande steg:
- Aktivera internetanslutningen med IPv6.
- Fördela adresser enligt adressplanen.
- Konfigurera brandväggen.
- Aktivera IPv6 för serverplattformar.
- Kontrollera och förvalta.

Aktivera internetanslutning med IPv6

Första steget är att er internetleverantör ska leverera internetanslutning med IPv6. Från beställning till leverans kan det ta allt från några timmar till flera veckor. Kontrollera leveranstiden med er leverantör.

Verifiera att internetanslutningen fungerar

Internetleverantören aktiverar IPv6 fram till brandväggen. Därefter är det viktigt att ni kontrollerar att IPv6-anslutningen är nåbar på insidan av brandväggen. Verifiera att IPv6 är korrekt routat, genom att till exempel ansluta en dator på insidan och testa genom brandväggen. Om det inte fungerar, se avsnitt ”Att tänka på vid användning av PI-adresser” och ”Konfigurera brandväggen för IPv6”.

Fördela IPv6-adresser utifrån adressplanen

När internetanslutningen är aktiverad och kontrollerad kan införandet av IPv6 fortsätta. Det adressblock som ni tilldelats ska nu fördelas på de segment där IPv6 ska aktiveras.

Tänk på att lägga upp en så kallad ”Null Route” för hela adressblocket någonstans i nätet så att routing-loopar undviks.

Att tänka på vid användning av PI-adresser

Vid införandet av PI-adresser krävs att ett så kallat route6-objekt finns skapad i RIPE NCC:s databas. Söker man på adressrymden i databasen ska ett route6-objekt finnas. Se ett exempel för PTS nedan:

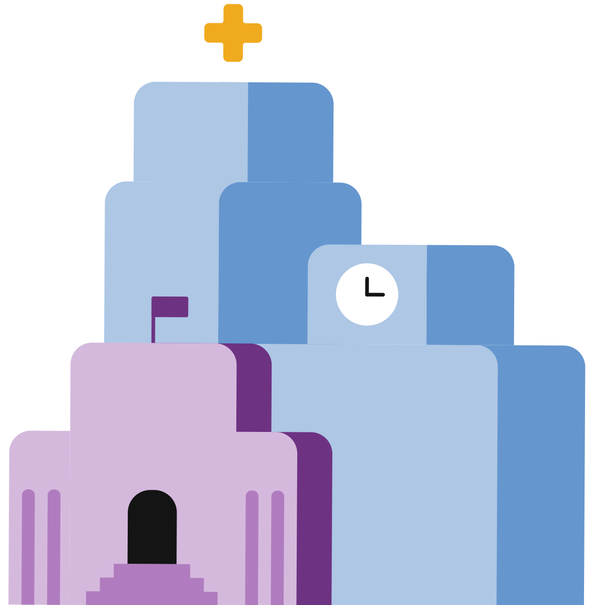
```
route6:          2001:67c:dc::/48
descr:           PTS
origin:          AS50273
mnt-by:          RESILANS-MNT
mnt-routes:      TDC-SE-MNT
created:         2011-02-24T14:00:40Z
last-modified:   2015-06-30T09:47:46Z
source:          RIPE
```

Om route6-objektet inte finns, kommer adresserna med största sannolikhet inte att routas överallt på internet. Om detta inträffar, kontrollera ert route6-objekt hos RIPE NCC:s databastjänst.

Idag kräver många internet- och innehållsleverantörer även att prefixen är signerade med RPKI. För detta krävs ett så kallat ROA-objekt för prefixet, vilket ni själva eller internetleverantören skapar.

- Kontrollera ROA på RIPE RPKI-validator.

Det finns mer information om ROA och RPKI på MANRS och RIPE NCC.



Konfigurera brandväggen för IPv6

Att aktivera IPv6 och sätta upp regler, interface, routes, hostar och nät påminner om tillvägagångssättet för IPv4. I en del brandväggar hanterar man IPv4 och IPv6 i samma regelverk, i andra använder man separata adresslistor och regelverk.

Gå igenom och dokumentera vilka hostar, nät, protokoll och portar som ska vara källa respektive destination i brandväggen. Det är en fördel att göra detta innan ni börjar med uppsättningen av regler. Det sparar tid och ni behöver skapa färre regler.

Att tänka på om ICMPv6 i brandväggen

I IPv4-kommunikation anses Ping och ICMP vara olämpliga protokoll och de filtreras därför ofta bort i brandväggen. För IPv6-trafik är däremot ICMPv6 fundamentalt och filtrering skadar normal trafik.

Neighbor Discovery Protocol, NDP, (RFC 4861) är grundläggande i IPv6 och använder ICMPv6. NDP motsvarar bland annat Address Resolution Protocol (ARP) i IPv4.

Var försiktig med filtrering av ICMPv6, det kan ge diffusa fel som gör att IPv6 förlorar funktionalitet.

För ytterligare rekommendationer om filtrering av ICMPv6, se APNIC:s blogg. APNIC är Asien och Stilla havsregionens motsvarighet till RIPE NCC.

Aktivera IPv6 för serverplattformar

Inför IPv6 i en server i taget. Testa att tjänsten fungerar som den ska innan ni aktiverar IPv6 i ytterligare tjänster. Tjänsten ska ha hög tillgänglighet och säkerhet och inte påverka andra tjänster på ett negativt sätt.

Aktivera inte IPv6 på en tjänst om den under tester visar sig vara instabil och inte fungerar som den ska. En bristfällig IPv6-funktion på en digital tjänst orsakar ofta problem för besökarna, även om webbläsare och många andra program idag stödjer så kallade Happy Eyeballs.

Aktivera IPv6 på DNS

Organisationens DNS-servrar ska både vara nåbara över IPv6 och ha uppgifter om IPv6-adresser i sina databaser. Alla DNS-servrar på marknaden har stöd för IPv6 och många har IPv6 aktiverat default och det är enkelt att aktivera IPv6, även i de DNS-servrar som inte har IPv6 default.

Det är viktigt att ni inte lägger upp resursposter för IPv6 (AAAA resource records) för era externa digitala tjänster innan samtliga steg i ”utifrån och in” är klara för berörda tjänster.

När DNS-servrarna har testats måste den registrar som hanterar er DNS-zon (till exempel ”kommunen.se”) uppdateras med de nya IPv6-adresserna så att .se-zonen, eller den toppdomän ni använder, har samtliga IPv6- och IPv4-adresser till era DNS-servrar. För full funktion och tillgänglighet är det viktigt att samtliga publika auktoritativa servrar för organisationens samtliga domäner har både A och AAAA-records.

Aktivera IPv6 för extern webbplats

Webbservrar (till exempel Apache/Nginx/IIS) inklusive operativsystem och CMS-system har IPv6-stöd sedan länge.

Om ansvaret för den externa webbplatsen finns inom den egna organisationen, aktivera IPv6 i operativsystemet. Om CMS-system används, kommer de oftast att fungera med IPv6 med automatik, eftersom de byggs som tillägg till webbservrar.

Om en extern leverantör ansvarar för den externa webbplatsen är det viktigt att kravställa IPv6-stöd vid upphandling av tjänsten. Kringfunktioner för webbplatsen behöver också ha stöd för IPv6-trafik, som till exempel statistikföring så att organisationens trafik och trafikmönster kan mätas (till exempel antal besök över IPv4 respektive IPv6).

Det är vanligt att lastdelare/proxys används för att säkerställa webbserverns kapacitet. I detta fall måste själva lastdelaren/proxyn ha stöd för IPv6, medan IPv6-stöd på webbservern inte är nödvändigt.

Tänk också på att det kan finnas underliggande tjänster som anropas av webbplatsen, antingen i användarens webbläsare eller servern (det kan till exempel vara externa tjänster som drivs av javascript). Alla dessa tjänster bör ha stöd för IPv6 och IPv4 parallellt så att användarens upplevelse inte försämras. Ett bra sätt att testa funktionaliteten är att inaktivera IPv4 och bara använda IPv6 och se vad som inte fungerar.

Genom att sätta upp ett specifikt testnät för surfning som bara har IPv6-stöd, till exempel ett begränsat Wifi-nät, är det enkelt för exempelvis system- eller webbansvarig att upptäcka om några externa tjänster slutar att fungera.

Aktivera IPv6 för serverplattformar

Aktivera IPv6 för e-post

Det finns flera lösningar för hur e-postkommunikation kan ske över IPv6 (till exempel MTA, e-postreläer och e-post-servrar).

Det finns även flera olika hård och mjukvaror för att filtrera bort spam och virus.

Kontrollera status för IPv6 och hur IPv6 aktiveras i systemet. Tänk på att uppdatera er SPF för utgående e-post med motsvarande IPv6-adresser på e-post-servrarna.

När e-post ska skickas via IPv6 måste korrekt bak-längesuppslagning av IPv6-adresser i domänen ip6.arpa vara uppsatt för e-postservrarna .

IPv6 till organisationens anställda

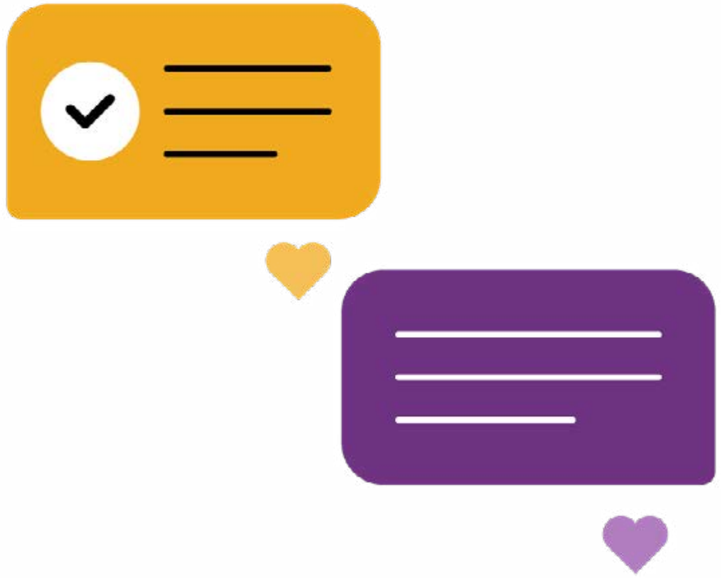
Alla moderna operativsystem i klientdatorer stödjer IPv6. Genom att aktivera IPv6 vid sidan av IPv4 på det interna nätet kan aktuella datorer snabbare nå externa datorer och andra resurser som har stöd för IPv6 eller IPv4.

Om en proxy används, kan aktivering av IPv6 i proxyservern ge alla datorer – även dem med enbart IPv4 – möjlighet att nå interna och externa tjänster med IPv6.

Förenkla specifika funktioner

När alla användares system har anslutning till båda protokollen kan man börja förenkla och låta vissa tjänster och utrustningar enbart ha IPv6-anslutning. Skrivare är ett exempel på sådan utrustning.

Detsamma gäller om ni använder IP-baserad telefoni via ett VLAN med alla IP-telefoner anslutna. Då kan ni snabbt gå över till IPv6 mellan abonnentväxel (PBX) och terminaler.



Kontrollera och förvalta

Allt eftersom ni har infört IPv6 tjänst efter tjänst, är det viktigt att kontrollera och övervaka att respektive tjänst fungerar med IPv6, precis som med IPv4. Det vill säga behandla IPv6 med samma noggrannhet och på samma sätt som IPv4 behandlas.

Ett fel i exempelvis IPv6 för en tjänst resulterar inte alltid i ett larm om tjänsten fortfarande är tillgänglig över IPv4. Av den anledningen är det viktigt att övervakningen larmar för fel i båda protokollen.

Det kan därför finnas behov att sätta upp separata system för övervakning, ett för IPv4 och ett för IPv6 för att minska risken av oupptäckta fel i något av protokollen för sina bevakade tjänster. Detta möjliggör upptäckt av onormala förhållanden, till exempel vad gäller trafikmängder, prestanda och svarstider. Övervakning med larm ger möjlighet att snabbt kunna vidta åtgärder vid behov.

Övervaka tjänster och era interna nät genom egen eller extern övervakning. Många externa övervakningsfunktioner kan övervaka IPv6. Om fel uppstår kan det medföra att det tar längre tid att nå en viss tjänst eller webbplats eller att det inte går att nå tjänsten eller webbplatsen alls.

De vanligaste felorsakerna är uppgraderingar av internetanslutningar, brandväggar med säkerhetsfunktioner samt extern auktoritativ DNS, webbplatser och e-post. Det förekommer att dessa fel inte upptäcks på grund av brist på automatiska övervakningssystem.

Det finns flera olika verktyg på internet[1] där det går att testa om webbserver, DNS och SMTP-server fungerar som de ska över IPv6. Om ni aktiverat IPv6 internt på arbetsstationer kan testverktyg[2] användas för att testa om HTTP/HTTPS och PMTU (Path MTU) fungerar.

1 https://www.hardenize.com/, https://internet.nl/, https://ipv6alizer.se/
2 http://test-ipv6.se/

Avslutande ord

För att bibehålla funktionalitet och tillgänglighet för era tjänster är det givetvis viktigt att överföra de kontroller och den övervakning som gjorts i samband med genomförandefasen till den långsiktiga förvaltningen.

Vi på PTS har valt att hålla vägledningen så kort som möjligt. Om ni vill fördjupa er ytterligare i olika aspekter och frågor rörande IPv6 har vi därför listat ett antal länkar nedan, som vi tror kan vara användbara för den som vill fördjupa sig.

Lycka till!

Användbara länkar

All about IPv6 – Governments

Basic IPv6 Troubleshooting Commands / IPv6 Rosetta Stone 2019

Deploy 360 Programme (ISOC)

Deploying IPv6 at IBM

Deploy IPv6 Now (RIPE NCC)

Enterprise IPv6 Deployment Guidelines RFC 7381 (IETF)

Guidelines and Process: IPv6 for Public Administrations in Europe

IPv6 Case Studies (ISOC)

IPv6 Deployment in the Enterprise GR IP6 001 (ETSI)

IPv6 Security for IPv4 Engineers

IPv6 Security – Frequently Asked Questions

ISOC – Introduction to IPv6

Why is /48 the recommended minimum prefix size for routing

World IPv6 Launch measurements

Begrepp och förkortningar

APNIC	Asia Pacific Network Information Centre	
ARIN	American Registry for Internet Numbers	
AS	Autonomous System Number	https://joinup.ec.europa.eu/sites/default/files/document/2019-12/Plum-EC-IPv6-Guidelines.pdf
CGN	Carrier Grade Nat – Adressöversättning (NAT) av Internetleverantören av slutkunders trafik Kallas även LSN – Large Scale NAT	https://www.apnic.net/community/ipv6-program/about-cgn/ https://tools.ietf.org/html/rfc6888
CMS	Content Management System	
Container-system	Ett sätt att paketera ett program med de funktioner som krävs för att programmet ska fungera. Programmet blir isolerat från det omgivande systemet och man uppnår på det sättet en isolerad virtuell miljö	https://www.docker.com/resources/what-container
DHCP Snooping	DHCP Snooping är en funktion för att förhindra att falska DHCP-servrar kan sättas upp.	https://packetpushers.net/five-things-to-know-about-dhcp-snooping/
DHCPv6	Dynamic Host Configuration Protocol version 6	
DHCPv6 snooping	Skydd mot oönskade DHCPv6-servrar	https://tools.ietf.org/html/rfc7610
DNS	Domain Name System	https://www.ietf.org/rfc/rfc1035.txt

Begrepp och förkortningar

DNS64	DNS64 används för att enheter ska få en fiktiv IPv6 adress som sedan översätts till IPv4. Se även NAT64	https://tools.ietf.org/html/rfc6147
Dual stack	När en nod har stöd för IPv4 och IPv6 samtidigt	
DUID	DHCP Unique Identifiers	
Dynamic ARP inspection	Funktion för att förhindra så kallad ARP-poisoning där attackeraren typiskt blir default gateway och på så sätt kan avlyssna och styra trafiken.	https://packetpushers.net/yes-we-really-need-dynamic-arp-inspection/
Happy Eyeballs	Standard som gör att enheter som har dual-stack använder det som ansluter snabbast av IPv6 och IPv4	https://tools.ietf.org/html/rfc6555 , https://tools.ietf.org/html/rfc8305
HTTP/HTTPS	Hyper Text Transfer Protocol / Hyper Text Transfer Protocol Secure	
ICMP	Internet Control Message Protocol för IPv4 – det protokoll som man använder i verktyget “ping”	
ICMPv6	Internet Control Message Protocol version 6 Tillämpning av ICMP för IPv6	
IDS	Intrusion Detection System	
IPS	Intrusion Protection/Prevention System	

Begrepp och förkortningar

L3-switch	Layer 3 switch	
LIR	Local Internet Registry, Organisation som är medlem i och representerar RIPE NCC och tilldelar slutkunder IP-adresser som de tilldelats från RIPE NCC	
MAC-adress	Media Access Control Adress	
MANRS	Mutually Agreed Norms for Routing Security	https://www.manrs.org/
MTA	Message Transfer Agent eller Mail Transfer Agent datorprogram som överför e-post från avsändarens e-postserver till mottagarens e-postserver.	
MTU	Maximum Transmission Unit	
Multi-homing	Att ha två eller flera samtidiga leverantörer av internetsanslutningstjänst	
NAT	Network Address Translation	
NAT444	Adressöversättning i två steg, så kallad dubbel NAT. CGN och LSG är också NAT444	
NAT64	NAT64 är adressöversättning från IPv6 till IPv4.	https://tools.ietf.org/html/rfc6146
NDP	Network discovery protocol	https://tools.ietf.org/html/rfc4861

Begrepp och förkortningar

Null Route	En så kallad “null route” dirigerar trafik till ett icke existerande gränssnitt, som innebär att trafiken försvinner i tomma intet.	https://www.inetdaemon.com/tutorials/internet/ip/routing/static/#null
PA-adresser	Provider Aggregatable	
PBX	Private Branch Exchange (Abonnentväxel)	
PI-adresser	Provider Independent	
Ping	Verktyg för att kontrollera till exempel en värddators nåbarhet i ett IP-nät	
PMTU	Path MTU	
RA Guard	Skydd mot oönskade IPv6-routrar	https://tools.ietf.org/html/rfc6105
RIPE NCC	RIPE NCC är det europeiska organet för fördelning av gemensamma nätresurser, som IP-adresser och nätidentifierare.	www.ripe.net
ROA	Route Origin Authorisation	https://www.ripe.net/manage-ips-and-asns/resource-management/certification/resource-certification-roa-management
Route6-object	Ett objekt som talar om vilket AS-nummer som routar adress-rymden	https://www.ripe.net/manage-ips-and-asns/db/support/documentation/ripe-database-documentation/rpsl-object-types/4-2-descriptions-of-primary-objects/4-2-6-description-of-the-route6-object

Begrepp och förkortningar

RPKI	Resource Public Key Infrastructure	https://www.ripe.net/manage-ips-and-asns/resource-management/certification
SIP	Session Initiation Protocol	
SLAAC	Stateless Address Autoconfiguration	https://tools.ietf.org/html/rfc4862
SMTP	Simple Mail Transfer Protocol	
SPF	Sender Policy Framework	
UTM	Unified Threat Management	
VLAN	Virtual LAN	
VPN	Virtuellt Privat Nätverk	

Oktober 2020
www.pts.se