Jimmy Bergman

Ansvarig för utveckling och roliga skämt vid kaffemaskinen

Lärdomar från vår IPv6-lansering

LOOPIA

Bakgrund

- Vi såg det som en marknadsföringsmöjlighet
- Vi ville börja innan många slutanvändare använde IPv6, för att få tid på oss att stabilisera lösningen innan många påverkades av potentiella problem
- Långsiktigt ser vi det som en nödvändighet
- Det är kul

LOOPIA

Delprojekt

- Vi valde att dela in projektet i tre faser:
    1. Inför IPv6 i vårt nätverk, samt i servrar som hanterar vår hemsida samt våra administrationsverktyg
    2. Inför IPv6 i våra namnservrar
    3. Inför IPv6 för våra kunders webbsidor samt i vårt e-postsystem

LOOPIA

Steg 1: Nätverk + få servrar

- Förberedande arbete:
  - Ansökte om medlemskap i RIPE
  - Ansökte om en IPv6-allokering
- Gick snabbt och smärtfritt, nästa steg var att få ISP:er att sälja transit åt oss
  - Inte lika enkelt, ett par ISP:er verkade inte förstå varför vi ville köpa IPv6-trafik – Vi sade *vi vill bli kund*, de svarade *ni vet väl att ingen använder IPv6*
  - ISP:er behöver förstå att de kanske inte kommer tjäna pengar på att erbjuda detta direkt, men de kommer förlora pengar på att inte erbjuda det i längden

LOOPIA

Inkoppling av ISP

- Köpte av Tele2
  - Deras attityd är uppfriskande hjälpsam och utan byråkrati
  - De erbjöd oss att köra BGP via en tunnel direkt och att ansluta våra routers direkt via IPv6 så fort deras nät var helt utbyggt
  - De har varit enormt kunniga samt trevliga att ha att göra med
- Vi bestämde oss för att köra på detta för steg 1 samt att vänta med delprojekt 2 och 3 tills vi har kopplat in flera Internetleverantörer samt fått bort tunneln

LOOPIA

Border-routers

- Vi använder OpenBSD med OpenBGPD
  - Stödde redan IPv6, ingen uppgradering nödvändig
  - Vi uppgraderade till senaste versionen på samma gång ändå, fördelen med redundans i alla steg är att uppgraderingar är enkla
  - Konfiguration var enkel men omfattande:
    - I princip all konfiguration för IPv4 fick motsvarighet
    - CARP-adresser, BGP-konfiguration, brandväggsregler, routing-regler
    - Många enkla ändringar ➔ Stort krav på testning

LOOPIA

Brandväggar

- Även här använder vi OpenBSD med OpenBGPD
- Regelverket var specifierat för IPv4 och med *block all inet6*
- Man måste tänka på att IPv4-regler inte per automatik gäller för IPv6, så man inte går från att ha ett väl fungerande regelverk till att ha ett väl fungerande IPv4-regelverk och öppen gata in på IPv6
- I vårt fall valde vi att lägga in ett fåtal regler för att släppa igenom enbart tjänsterna i steg 1 när anslutningarna kom via IPv6
- Man måste tänka på att det är ännu viktigare att tillåta ICMP6 än ICMP, IPv6 utan fungerande ICMP Neighbor Discovery är inte en trevlig upplevelse (även ICMP bör vara självklart att tillåta, men så ser ju inte världen riktigt ut)

LOOPIA

Ändringen med andra ord

- Ett pakets väg före införandet:
  - IPv4-användare →
  - Någon av våra ISP:er →
  - En av våra border-routers →
  - En virtuell IP (CARP) som hanteras av någon av våra brandväggar →
  - Någon server hos oss →
  - En virtuell IP (CARP) som hanteras av någon av våra brandväggar →
  - En virtuell IP (CARP) som hanteras av någon av våra border-routers →
  - Någon av våra ISP:er → IPv4-användare

LOOPIA

Ändringen med andra ord

- Ett pakets väg efter införandet:
  - Användare på IPv4 eller IPv6 →
  - Någon av våra ISP:er →
  - En av våra border-routers →
  - En av två virtuella IPs (CARP) som hanteras av någon av våra brandväggar (en för IPv4 och en för IPv6) →
  - Någon server hos oss →
  - En av två virtuella IPs (CARP) som hanteras av någon av våra brandväggar →
  - En av två virtuella IPs (CARP) som hanteras av någon av våra border-routers →
    - Någon av våra ISP:er →
    - Användare på IPv4 eller IPv6

LOOPIA

Ändringen med andra ord

- Vi gör exakt samma sak på IPv6 som på IPv4
- Men vi gör det en gång till. Man får inse att man måste konfigurera alla punkter i sitt nätverk till att stödja IPv6 om man vill stödja samma saker som på IPv4

LOOPIA

Anslutning av servrar

- Nästa steg var att tillgängliggöra vår hemsida och våra kontrollpaneler via IPv6
- Men först ordnade vi så att vårt kontorsnät hade IPv6-stöd, så att våra support-tekniker kunde se samma sak som IPv6-anslutande kunder
- På vårt kontorsnät så kör vi nu:
  - IPv4: Användare → NAT-gateway → Internet
  - IPv6: Användare med publik adress → Gateway utan NAT → Internet
- Detta exemplifierar en av fördelarna med att ha sjukt många adresser, man slipper vederstyggelser som NAT

Anslutning av servrar

- Ändra så att lagring av IP-adresser i våra system stödjer adresser längre än 15 tecken
- Konfiguration av servrar som ska finnas på IPv6:
  - Tilldela en adress
    Vi gör det manuellt för servrar, på kontorsnätet använder vi autoconfiguration
  - Några få rader konfigurationsändring:
    - Sätta upp interface
    - Sätta default-route
    - Verifiera att demonen som kör tjänsten lyssnar på både IPv4 och IPv6
  - DNS-ändringar
- Allt verkade fungera bra

LOOPIA

Fel som man bara upptäcker efteråt

- Allt fungerade bra utifrån
- Allt fungerade oftast bra från vårt kontorsnät
- Då och då gick det inte att ansluta via IPv6 från kontorsnätet till berörda servrar
- När vi tcpdump:ade på servrarna för att se om trafik kom in började det fungera
- Även om man har bra koll på IPv6 så tar det längre tid att felsöka ju kortare erfarenhet man har
  - För IPv4 har många tekniker 10+ års erfarenhet
  - Detsamma gäller oftast inte för IPv6

LOOPIA

Vad var det då?

- Vi hade konfigurerat servrarna korrekt i konfigurationsfiler
- Men vi hade tilldelat IPv6-adresser manuellt via ifconfig för att slippa ta ned/upp hela nätverksinterfacet
- Därför saknades auto-tilldelade link-local-adresser, vilket gjorde att Neighbour Discovery inte fungerade korrekt, eftersom maskinen inte var medlem i ff02::1

LOOPIA

Fel som man kunde ha upptäckt före

- Kunder som anslöt via IPv6 rapporterade in problem med att administrera sin epost
- Problemet:
  - Vår e-postadministration ligger på en annan server än vår vanliga kontrollpanel
  - E-postadministrationen verifierar att den inloggade kunden använder samma IP-adress som när denne loggade in
  - Vi hade inte lagt till IPv6-stöd för e-postadministrationen, så kundens IP-adress var annorlunda i kontrollpanelen och e-postadministrationen
- Enkel fix: Gör det då.

LOOPIA

Fel som man kunde ha upptäckt före

- Kund rapporterade in problem med att hans traceroute till oss inte fungerade
- Vi hade bara öppnat för ICMP6-traceroutes i brandväggen
  - Ett par undermåliga operativsystem erbjuder inte traceroute6 –I utan bara UDP-traceroute
- Så vi tillät UDP-traceroutes för IPv6 för att Linux-användarna skulle bli glada (och vi får erkänna att det var en miss, vi har det självklart öppet på IPv4)

LOOPIA

Fel som man kunde ha upptäckt före *

- Kunder rapporterade in problem med att ansluta via IPv6
- Efter felsökning visade det sig att samtliga kunder använde 6to4
- Vidare felsökning visade att anycast-routern som Tele2 annonserade en route till åt oss inte fungerade
- Tele2 plockade bort routen omedelbart, lika hjälpsamma som vanligt och lät meddela att de snarast skulle införa en egen 6to4-gateway istället
- 6to4 ses av en del operatörer tyvärr lite som en oönskad plåga som man måste dras med
  - Leder till att det oftare är trasigt utan att det behagas fixas än för andra IPv6-prefix
- Tele2 höll sitt löfte och lanserade en egen 6to4-gateway
  - Tyvärr innebar detta att 6to4 slutade fungera igen för våra kunder, eftersom de glömde annonsera routen till 2002::/16 åt sina BGP-kunder
  - Sådana problem tar längre tid innan någon märker på IPv6, eftersom antalet användare är så få
  - Att få upplever problem är också något bra när man inför något nytt, så ta tillfället i akt att börja nu istället för om två år
  - Tele2 korrigerade problemet med den saknade utannonseringen minuter efter det att vi meddelade dem. Slutresultat: Vi är fortfarande en nöjd kund och rekommenderar alla som vill börja implementera IPv6-stöd att vända sig till dem.

** ja, ja – man kan göra som Wikipedia och testa felfrekvens före via magiska trix*

LOOPIA

Nästa steg

- Med IPv6 i nätet aktivt och ett par tjänster live som pilot är det dags för fas 2
- Första steget körde vi med raskare implementationstakt än vanligt eftersom vi kände att vi kunde få marknadsförings-payoff direkt med *Loopia lanserar IPv6* och så vidare. Det lyckades.
- Då våra namnservrar hanterar 25 % av alla .se-domäner är det dock viktigare med en mer försiktig lansering av IPv6 för våra namnservrar

LOOPIA

Namnservrar

- Vi väntar på att få redundans gällandes vår transit för IPv6 innan vi tar detta live. Minst en ISP till samt inga tunnlar.
- Att göra (i princip):
  - Konfigurera IPv6-adresser för maskinerna
  - Verifiera att Bind svarar korrekt sett utifrån på både IPv6 och IPv4
  - Uppdatera loopia.se-zonen samt lägg till glue i .se
- Total tidsåtgång: 25 minuter, att vi väntar är bara ett policy-beslut
- Klart sedan länge: Möjlighet att administrera AAAA-pekare i våra DNS-tjänster.

LOOPIA

Webb + epost

- När sedan namnservrarna finns på IPv6 kommer nästa steg:
  Resten av tjänsterna
- Detta är lite mer jobb, men av samma komplexitet (knappt någon alls)
- Att detta ännu ej är i produktion är även det policy snarare än implementationstid, med ett script görs arbetet på maximalt några timmar
- Dessa två steg kommer genomföras så fort vi känner att konnektivitet är tillräckligt god i vårt IPv6-nät
- Det vi då slutar på är en situation då relativt mycket svenskt innehåll finns tillgängligt på IPv6, inte minst 25% av .se-zonerna DNS-mässigt
  - Vi hoppas att det kan hjälpa till lite som motargument till de dåliga *ingen använder det ju ändå*-argumenten som ofta hörs från bakåtsträvare

LOOPIA

Kom ihåg-lista

- Gå igenom alla era publika tjänster
  - Tänk: Finns det någon vits med att erbjuda denna även på IPv6
- Var noggrann med att verifiera brandväggsregelverk även för IPv6
- Kontrollera att ert övervakningssystem även testar era tjänster via IPv6, samt IPv6-konnektivitet
- Tjata på era Internetleverantörer vid varje tillfälle
- Använd IPv6 på era arbetsstationer, så att ni ser eventuella fel före eller lika fort som era IPv6-kunder

LOOPIA

Frågor?

- Nej, inte om våra epost-problem (överbelastat lagringssystem, ja – det är löst).

LOOPIA


LOOPIA
Välkommen till ett riktigt webbhotell