Datavetenskap

Opponenter:

William Hemmingsson, Emil Vieweg

Respondent:

David Andersson

Teoretisk och praktisk genomgång av IPv6 och dess säkerhetsaspekter

---

Oppositionsrapport, C-nivå

2012-06-07

1 Sammanfattning

Överlag är detta en mycket välskriven uppsats som tar upp ett intressant ämne och flera viktiga frågeställningar kring säkerhet. Språket är klanderfritt och texten lättläst. Uppsatsen ger utförlig och relevant information som krävs för implementation av IPv6. Den stora negativa aspekten är att uppsatsen stundom är väldig teknisk och saknar viktiga referenser och mer utförliga beskrivningar. Det som vi också känner saknas är en beskrivning hur säkerheten i implementationen testades, då det uppges att fokus har legat på säkerhetsaspekter,

2 Generella synpunkter

2.1 Titel

Uppsatsens titel är bra och summerar vad arbetet har handlat om. De teoretiska och praktiska delarna av projektet nämns i titeln. Att arbetet fokuserat mycket på säkerhetsaspekter avspeglas också i titeln.

2.2 Begreppsapparat

Uppsatsen innehåller många begrepp, där några förklaras men andra inte. Vissa begrepp kan man kanske anta att läsare kan sedan tidigare, men andra borde förklaras eller förklaras bättre. Detta gäller även hantering av akronymer som ibland blir förvirrande. Önskvärt vore en begreppslista som bilaga eller kanske i uppsatsens inledning.

2.3 Argumentering och slutsats

Uppsatsen innehåller få argument, då uppsatsen mer beskriver en teknik och inte val av olika tekniker för en implementation. Vissa argument som förkommer är inte refererade, som till exempel i Sammanfattning:

”behovet av kunskap kring IPv6 växer lavinartat”.

Även argument för vissa val saknas, som till exempel val av mjuk och hårdvara för implementationen. Varför gjordes just de valen, och finns det alternativ?

2.4 Disposition

Uppsatsen har en bra sammanhållning och kapitlen är ordnade på ett logiskt sätt. De inledande kapitlen ger en bra inblick i teorin bakom IPv6 samt olika säkerhetsaspekter. Ibland nämns begrepp som förklaras senare, de bör kunna förklaras tidigare för att få en ännu bättre röd tråd. Även inledningar till varje kapitel skulle förbättra sammanhållningen och hjälpa läsaren att få en överblick över varje kapitel utan att behöva läsa hela kapitlet. Även om detta är lite vad sektionen Disposition i Inledning är till för, gör det inget att upprepa sig och beskriva kapitlet mer utförligt.

2.5 Referat

Bra referenser och god struktur på referenslistan. ISBN-nummer saknas på böcker. Tyvärr saknas också referenser till begrepp som är centrala för förståelsen, de borde refereras antingen till extern källa eller till en beskrivning längre fram i uppsatsen (om en sådan existerar). Referens till bilder saknas i många fall också i texten, även bilden förklaras.

2.6 Sammanfattning och abstract

Sammanfattningen saknar en summering av resultaten, vad som i slutändan blev implementerat. Sammanfattningen bör återspegla hela uppsatsen, med fokus på bakgrund, problem samt resultat.

2.7 Språkhantering

Språket i uppsatsen är mycket bra i sin uppbyggnad. Meningarna är korta, koncisa och lättbegripliga. Uppsatsen innehåller inga anmärkningsvärda fel med avseende på stavning och meningsuppbyggnad. Ibland används tyvärr vissa ovanliga och främmande ord som kan bytas ut till mer vardagliga termer, utan att det ger ett mindre proffsigt intryck.

3 Kapitel för kapitel

3.1 Kapitel 1 - Inledning

Det inledande kapitlet är kort och sammanfattar bra vad uppsatsen handlar om. Utöver detta har inte något anmärkningsvärt hittats.

3.2 Kapitel 2 – Bakgrund

Bakgrunden ger en kort men bra översikt av Internetprotokollets historia.

Sektion 2.3 om RFC'er känns något överflödigt då själva RFC'erna inte är del av själva projektet utan används som referenser i uppsatsen. Mer intressant vore att veta hur RFC'er skrivs, av vilka, och hur en RFC blir till en standard, istället för en listning av de olika RFC'erna. Referenser till ICMP och ARP saknas då läsarna inte kanske har ingående kunskaper om IPv4. Referenserna kan antingen vara till extern källa eller beskrivas här eller i Kapitel 3.

3.3 Kapitel 3 – Uppbyggnad av IPv6

Kapitlet beskriver hur IPv6 är uppbyggt och hur det fungerar i teorin. Det jämför också aspekter med IPv4. Överlag är kapitlet bra strukturerat och innehållet är intressant och högt relevant för uppgiften. En del saker är otydliga och kan utvecklas och refereras.

I Sektion 3.1 saknas referens till IPsec och Link Local. Link Local beskrivs som APIPA, om denna term ska användas bör det nämnas att detta är en term använd av Microsoft och inte den ”officiella” benämningen. Argumentationen kring NAT kan styrkas,
”På gott och ont togs simultant specifikationen för NAT (Network Adress Translation) fram”.

Det framgår inte vad gott och ont är i detta sammanhang. Dessutom behöver påståendet att det är NAT som är orsaken till att övergången till IPv6 fördröjts, styrkas.

Antalet IP-adresser för IPv4 bör skrivas med standardform, exempelvis ”cirka $4 * 10^9$”. Engelska begreppen ”stateless” och ”stateful” kan ersättas med ”tillståndslös” och ”tillståndsbaserad”.

Ordvalet ”begär” är inte helt bra:

”Den stora skillnaden i detta fall mellan IPv4 och IPv6 är att i IPv4 måste en förfrågan efter en dynamiskt tilldelad IP-adress från en DHCP-server tagit för lång tid varpå protokollet sedan begär en APIPA-adress”

Bättre vore ”genererar” eller ”skapar” då ”begär” antyder att tilldelning sker från en extern källa.

I Sektion 3.2.1 har figur 3.3 något otydlig bildtext. Följande kan vara en bättre beskrivning: ”IPv6-paket med flera Extension Headers”

I Sektion 3.2.2 bör akronymen EH nämnas i samband med Extension Headers då EH används senare i tabell 3.1. Det är även otydligt hur Extension Headers fungerar.

I Sektion 3.3 finns en underlig referens ([15]) som stöder påståendet att IP-adresser i IPv4 använder 32-bitar. Kanske är denna felplacerad, men den kan tas bort. CIDR kräver dessutom referens.

I Sektion 3.3.3.1 är det otydligt hur tilldelning av Link Local-adresser sker i IPv4. Dessutom är det otydligt vad som menas med ”169.254.0.0/16-nätverket”. I sektionen finns en lista över olika Unicast-adresser, flera som inte beskrivs alls. Överväg att ej nämna dem (se listan i Sektion 3.3.1) då de inte verkar vara relevanta för uppgiften.

I Sektion 3.3.1.2 finns meningen

”*Dessa adresser befolkas dynamiskt genom medlemskap”.*

Det är otydligt vad detta innebär, en referens eller utförligare beskrivning är önskvärt.

3.4 Kapitel 4 – Säkerhet och säkerhetsmekanismer i IP

Kapitlet känns relevant för uppgiften och tar upp många intressanta aspekter rörande säkerhet. En del viktiga referenser saknas, som kan hjälpa läsare som inte har stora förkunskaper inom datasäkerhetsområdet.

I Sektion 4.1.1 nämns NAT i meningen

”... men då vi under lång tid har levt med den falska känslan av säkerhet i och med NAT och användande av privata ickeåtkomstbara adresser...”

och det är svårt att förstå vad som menas med ”falsk säkerhet”, vilka är ”vi” utveckla gärna. Förslag på förbättring, ha en egen Sektion för NAT och dess positiva och negativa aspekter.

I Sektion 4.1.2 saknas referenser till IDS och IPS. Hur fungrerar dessa?

I Sektion 4.1.2 nämns NDPmon samt ARPWatch, utan referenser. Vore intressant att veta hur dessa fungerar.

I Sektion 4.3 saknas referens till ”protokoll 41”. Att detta har använts av virusmakare nämns också, utan referens. Bra källa vore en nyhetsartikel eller liknande som tar upp detta.

I Sektion 4.4, tabell 4.1 finns begreppen Spoofing och Återspeglingsattacker. Det är otydligt vad detta är, och referens till dessa skulle underlätta. Tabellen refereras inte heller från texten. Referenser till RSA och CGA saknas också. Akronymen CPA nämns inte tillsammans med utskrvningen av den, och SEND skrivs inte ut alls, och saknar referens.

I Sektion 4.5 finns en bakåtreferens till Figur 2.1. Bättre att referera till Figur 2.2 (TCP/IP-modellen, som är mer relevant), och även i texten nämna vilket lager som avses, besparar läsaren tiden att leta upp figuren igen.

I Sektion 4.6 saknas referens till Privacy Extensions.

3.5 Kapitel 5 – Design till implementation av IPv6-infrastruktur

Kapitlet ger en utförlig bild av designen för det nya nätverket. Argumentation skulle kunna vara bättre, argument som stöder de val som gjorts.

I Sektion 5.1 diskuteras några av de val (Buffalo Linkstation samt OpenWRT) som gjorts inför implementationen. Det framgår inte varför just dessa val gjorts och om det finns några alternativ. Termen ”internetdelare” är otydlig, kanske är router ett bättre och mer använt begrepp. Om en ”internetdelare” avser något annat bör det förklaras vad det är.

I Sektion 5.2, Figur 5.1, har vi flera synpunkter på. Tanken med bilden är mycket bra, den illustrerar komponenterna i nätverket. Legend saknas dock, och illustrationen över subnäten kan ge en falsk bild att trafik måste passera andra subnät. Vad DMZ är förklaras inte. Figuren refereras inte i texten.

I Sektion 5.4, Tabell 5.2 refereras inte i texten.

3.6 Kapitel 6 – Installation av IPv6-infrastruktur

Kapitlet är ganska tekniskt tungt, men mycket bra dokumenterat om man vill sätta sin egen IPv6-infrastruktur. Tillsammans med bilagan verkar detta ge en komplett beskrivning av hur en sådan implementation kan utföras. ”Installation” i titeln på kapitlet bör ändras till ”Implementation” då detta är den term som tidigare använts i uppsatsen. I kapitlet finns ett

antal figurer, där alla saknar referns från texten. Bra vore även om konfigureringarna i figurerna kommenteras ytterligare för att öka förståelsen.

I Sektion 6.2 används termen ”switch”, men denna switch har inte tidigare nämnts. Detta kanske avser ”Buffalo Linkstation” som nämndes i Kapitel 5. Tabell 6.1 är inte refererad från text.

I Sektion 6.3, vad en DHCP-relay är framgår inte.

I Sektion 6.4 saknas referens till ”Iptables”.

I Sektion 6.5.1 saknas refrens till vad FQDN är för något.

3.7 Kapitel 7 – Sammanfattning och resultat

Kapitlet speglar uppsatsen olika delar och sammanfattar resultatet. Dock tillkommer ny information som inte tidigare nämnts. Detta avser verifiering av implementationen av ”sårbarhetsgranskningar” och ”säkerhetsmekanismer”. Denna verifiering har inte tidigare diskuterats, men man kan göra antagandet att detta är säkerhetsbiten av implementationen som tidigare omnämnts som en viktig del.

I detta kapitel finns det enda faktafel vi har hittat. Det rör påståendet om att ingen svensk ISP levererar IPv6 till privatkunder. Detta är falskt. Som exempel på ISP som levererar IPv6 är CSBNET som leverer till Chalmers Studentbostäder[1].

Det vi tycker saknas i detta kapitel är slutsatser och kanske även personliga åsikter, en utvärdering av implementationen.

[1] http://www.chalmersstudentbostader.se/