Tampereen ammattikorkeakoulu, insinööritutkinto
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Kalle Koivumäki

Opinnäytetyö

Modularisoitu lähiverkostointijärjestelmä

Tampereen ammattikorkeakoulu, insinööritutkinto
Tietotekniikan koulutusohjelma, Tietoliikennetekniikka
Tekijä Kalle Koivumäki

Työn nimi Modularisoitu lähiverkostointijärjestelmä
Sivumäärä 18 sivua, 2 liitettä
Valmistumisaika Joulukuu 2010
Työn valvoja Mauri Inha
Työn tilaaja Tampereen Ammattikorkeakoulu/ Ari Rantala

TIIVISTELMÄ

Työn tarkoituksena on toteuttaa järjestelmä, jolla voidaan helposti jakaa lähiverkko hajautettuna Tampereen ammattikorkeakoulun campuksella pidettävillä messuilla ja muissa vastaavissa tapahtumissa, joissa tarvitaan väliaikaisia verkkoja Internet-jakeluun. Tämän työn kuvaama järjestelmä on ideaalinen etenkin väliaikaisiin lähiverkkojakeluihin, esimerkiksi LAN-party tapahtumissa sekä messuilla, joissa lähiverkkoa tulee jakaa useille asiakaskoneille eri pöytäryhmissä. Järjestelmä on erittäin mukautuskykyinen ja sisältää lukitut lasiovelliset pöytäryhmäräkkikaapit, joihin voidaan ripustaa 3 U:n edestä standardeja 19” räkkilaitteita. Kuljetuksen ajaksi kaapit voidaan pinota päällekkäin ja kiinnittää toisiinsa asianmukaisin soljin. Järjestelmän syöttöjännite kulkee UPS:in kautta, joten verkkolaitteille täten taataan puhdas syöttöjännite ja täten vähennetään mahdollisia laiterikkoja.

Tässä työssä tarkastellaan järjestelmän peruskoostumusta sekä esitellään järjestelmää käyttäville huomattavia asioita turvallisuuden ja järjestelmän konfiguroinnin tärkeimpiin kysymyksiin, joiden vastauksilla voi käytännöllisesti täydentää CCNA Academy -kurssin tietoja verkonylläpidossa ja tietoturvallisuuden parantamisessa. Tässä työssä ei käsitellä reititysprotokollia, koska lähtökohtana on käyttää staattista reititystä väärinkäytösten välttämiseksi. Tämän työn liitteissä on harjoitustyö, jossa on esitetty TiTeLAN 1/09 -verkkopelitapahtuman lähiverkon suunnittelu ja toteutus komentoineen dokumentoituna, joten näitä asioita ei käsitellä varsinaisessa työssä.

Kalle Koivumäki
Modularized LAN delivery system
Engineering Thesis
18 pages, 2 appendices
Thesis supervisor
Mauri Inha
Commissioning Company
Tampere University of Applied Sciences
December 2010
Keywords
networking, information security, switch, router

ABSTRACT

The modularized LAN delivery system introduced in this thesis was designed to help LAN delivery in events hosted on the Tampere University of Applied Sciences Campus (TAMK). The necessity for this system was high, as the previous network housing racks were not capable to be transported outside and this was one criterion which had to be filled in the events. This system has been deployed twice at TiTeLAN events up to the point of writing. The first time it was deployed the cases were beta tested and the second time the whole system was finished and in working order. It was then noted that the system works exactly as needed. There have been ideas about updating the design and upgrading some equipment housed in the system. These upgrades and updates are only mentioned in this thesis, as they are not essential information regarding the introduction of the system which is the main focus for this thesis.

SISÄLLYS

1 Johdanto

Tämän työn tarkoitus on selittää yksinkertaisen Internet-yhteydellisen lähiverkkototeutuksen laatimisen perusteita sekä toimia oppaana yksinkertaisen verkon rakentamisessa, kun alustana on siirrettävä moduulipohjainen hajautettu järjestelmä. Järjestelmän kehittämisessä päätavoite oli toteuttaa helposti hajautettava rakenne, jonka vuoksi järjestelmä koostuu useasta pienestä 19” räkkikaapista, jotka ovat kiinnitettyinä pikalukoin toisiinsa kuljetuksen aikana. Pikalukituksella on erittäin helppo tarpeen mukaan säädellä tarvittavien laitekaappien lukumäärää, jottei kuljeta ylimääräisiä laitteita eikä laitekaappeja silloin kun niitä ei tarvita. Näin järjestelmä saavuttaa hyvin sille asetetut fyysiset skaalautuvuustavoitteet. Pienikokoiset lukittavat kaapit helpottavat hajauttamista antamalla kytkimille suojaisan sijoituspaikan, jonka lisäksi ne vähentävät ilkivallan tekomahdollisuutta rajoittaen pääsyä laitteelle.

Lähiverkkojen toteuttamista hallittavin laittein suositellaan, kun verkossa liikkuvaa liikennettä tulee tavalla tai toisella ohjata, suodattaa tai rajoittaa. Liikenteen tarkastelu on aina suhteellisen raskasta verkon aktiivilaitteille. Tarkastelevat laitteet joutuvat avaamaan kunkin määritetyntyyppisen paketin todetakseen, täsmääkö paketti rajoitetuntyyppiseksi liikenteeksi, jonka pääsyä sisään tai ulos tulee rajoittaa tai estää. Tämä on resursseja kuluttavaa, joten rajoituksia ja suodatuksia on optimoitava mahdollisuuksien mukaan. Liikenteen suodattamisessa on huomioitava, onko kyseessä turvallisuuden vai kannattavuuden vuoksi suodatettu liikennettä, sillä jotkin julkiverkon palveluista ovat suoranaisia kaistantuhlaajia, jolloin varsinainen hyötyliikenne kärsii, jos pääsyä näihin palveluihin ei rajoiteta tai estetä.

Liikenteen rajoittaminen avaa QOS (Quality Of Service), eli palvelunlaatunäkökohdat, joissa karsitaan hukkakaistaa pienemmäksi asettamalla rajoitettavalle liikenteelle paljon pienempi prioriteetti kuin tärkeälle hyötyliikenteelle. QOS:n lisäksi on huomioitava tarve loogiselle skaalautuvuudelle, joka helposti saavutetaan agrekoimalla linkkejä runkoyhteyksissä. Tällöin voidaan avartaa helposti kehittyviä pullonkauloja lisäämällä datavirralle käytettävissä olevaa kaistaa ja oikein suunnitellulla kuormantasausmetodilla järjestelmä kykenee helposti jakamaan käytössä olevan kaistan sitä tarvitseville yhteyksille oikeudenmukaisesti. Täydellinen tasapaino kuormantasauksessa on erittäin vaikea tehtävä, koska tällöin koko verkon kokoonpanoa pitäisi olla mahdollista mukauttaa kaistojen tasaamiseksi yksinkertaisilla säännöillä. Tehdasasetuksilla kuormantasaus agrekoidulla linkillä tapahtuu vastaanottajan laiteosoitteen perusteella. Liikenteen kohdistuessa lähinnä yksittäiseen palvelimeen tämä osoittautuu ongelmaksi, koska tällöin kuorma kulkee vain tiettyä reittiä kyseiseen palvelimeen. Agrekoidusta linkistä ei tällöin saavuteta sen muutoin tuomaa hyötyä ja se osoittautuu siten ainakin osittain hyödyttömäksi, koska suurin hyöty saavutetaan vasta kuorman jakautuessa tasan agrekoidun linkin komponenteille. Pahimmillaan linkin kuorma kulkee vain yhdellä agrekoidun linkin osista, jolloin agrekoinnista saavutetaan vain kahdennus linkille. Reitittimien konfiguraatioita laadittaessa on oppaina käytetty lähteiden /1/ ja /2/ teoksia sekä Ville Haapakankaan/TAMK neuvoja.

2 Verkkotopologian suunnitteleminen

Järjestelmässä käytetyn topologian suhteen on tiettyjä rajoituksia, koska järjestelmä on suunniteltu hajautetuksi. Hajauttaminen on toteutettu agrekoimalla yhdyslinkit vikasietoisuuden ja suuremman käyttökaistan saavuttamiseksi. Laskennallisesti käyttökaista asiakkaalta runkokytkimeen saakka on noin 100 Mb/s, josta palvelimelle tulisi olla 1 Gb/s kaista, mikäli käytössä on lähiverkkoa palvelevia palvelimia. Runkokytkimen kautta luonnollisesti on linkki reitittimelle, jonka tehtäväksi jää siirtää ulkoverkkoon sopivaksi rajoitettuna ulos suuntaava liikenne.

Verkkotopologiaa suunniteltaessa tulee huomioida verkossa kulkevan liikenteen laatu. Jos verkossa kulkee lähinnä http-liikenne internetiin, niin on pakettien lukumäärä/koko –suhde yleisesti kohdallaan. Sen sijaan, jos liikenne on pakettien lukumäärällisesti huomattavasti suurempi kuin näiden pakettien koko, tulee valita käytettävät aktiivilaitteet kytkentänopeudeltaan riittäväksi välittämään paketteja viiveettömästi. Täten looginen yhteys ei kärsi eivätkä asiakassovellukset oleta yhteyden katkenneen. Liikenteen optimoinnissa on hyvä suunnitella erityyppisten verkkoliikenteiden jonotusasetukset, jotka ovat tehdasasetuksilla FIFO-moodissa (First-In, First-Out), jolloin ensimmäisenä saapunut paketti lähetetään ensimmäisenä ulos. Tämän tyyppinen toiminta ei ole kuormaa tasaavaa eikä varsinkaan QOS-pohjaista ajattelua, koska viimeisimpänä saapunut korkeanprioriteetin paketti joutuu tällöin odottamaan jonossa ennen pääsyä eteenpäin. Jonojen käsittelemiseksi on olemassa useita eri toimintoja, joista tehdasasetuksena oleva FIFO-moodi on yleispätevin, mutta aiheuttaa usein ongelmia liian pieneksi käyneen ulkoverkkolinkin kanssa. Jotkin sovellukset käyttävät reilusti kaistaa eivätkä välttämättä ole verkkosovellusten joukossa niitä kaikkein tarvituimpia. Näiden sovellusten tarpeellisuuteen en ota kantaa, mutta kerta toisensa jälkeen tietyt sovellukset tuntuvat olevan estolistoilla syistä tai toisista, joten kutsutaan niitä tarpeettomiksi verkkosovelluksiksi. FIFO-moodin lisäksi on mahdollista asettaa jonojen käsittely malliksi: tasapainotettu jonotus (Weighted Fair Queuing eli WFQ), priorisoitu jonotus (Priority Queuing) tai mukautettu jonotus (Custom Queuing). Tasapainotetun jonotuksen (WFQ) pääpainotus on interaktiivisten sovellusten kuten terminaali sessioiden parannettu suorituskyky, koska kyseinen liikennetyyppi aktiivisesti keskustelee päätteen ja palvelimen välillä, täytyy kyseisen liikenteen päästä mahdollisimman vaivatta kulkemaan. WFQ soveltuu hyvin myös tiettyjen verkkopelien käyttäytymiseen, vaikkakin WFQ täytyy konfiguroida erikseen parantamaan juuri tiettyä palvelua. WFQ –jonotusmalli on mahdollista asettaa parantamaan palvelun laatua käsin määritetylle liikenne tyypille, viitaten lähteeseen /3/.

” *Under WFQ, elastic traffic can only interfere with the interactive traffic by the fact that a data packet is in service at the instant a real-time packet becomes eligible. It can be justified to assume that this queuing delay due to the residual service of the data is statistically independent from the queuing delay due to competition in the queue dedicated to the interactive services [19]. Moreover, on links of moderate to high rate the delay associated with this kind of interference is negligible, while on links with a very small link rate (e.g., the DSL upstream link) it can be assumed that there is some form of pre-emption to interrupt a long data packet in service that would introduce too much delay on the interactive traffic. We conclude that in such a situation one can study the real-time queue in isolation.*
The network provider will tune its (WFQ) schedulers such that the interactive traffic gets just the treatment that it needs to meet the delay (and packet loss) bound. So, although the link rates in the current and future IP-based networks are huge compared to the bit rate of one interactive flow, or even compared to the aggregate bit rate of all interactive flows, still queuing delay can occur, as the actual capacity provisioned for the interactive services will be just modestly higher than the (average) offered traffic.”

Sitaatissa kuvataan epäinteraktiiviselle liikenteelle interaktiivisesta liikenteestä muodostuvaa ylimääräistä viivettä WFQ:n alaisuudessa. Sitaatin perusteella käytettäessä WFQ:ta ylimääräinen viive muodostuu silloin, kun epäinteraktiivinen (pelien dataliikenne) paketti on käsiteltävänä jonossa ja interaktiivinen eli korkeamman prioriteetin omaava liikennetyyppi saapuu käsiteltäväksi. Tällaisessa tilanteessa häviön kokee aina pienemmän prioriteetin liikenne tyyppi, mutta on mahdollista muokata prioriteettijärjestystä erikoistuneisiin tarpeisiin, jolloin voidaan itse määrittää millainen liikenne vaatii parhaan mahdollisen yhteyden. Näin tekemällä esimerkiksi LAN-party ympäristössä voidaan määrittää tarpeettomiksi nähdyt verkkoliikennetyypit niin suurelle viiveelle, ettei kyseistä liikennettä tarvitse suodattaa pois, sillä kyseistä liikennettä tekevälle asiakasohjelmalle (client) tulee ilmoitus aikakatkaisusta. Olisi tietenkin parempi mikäli kyseinen virheilmoitus sisältäisi tiedon, jonka mukaan liikennetyyppi on verkossa kielletty, mutta tämä vaatisi jo huomattavasti suuremman määrän konfigurointia ja verkkolaitteiden ohjelmistojen uudelleen ohjelmointia, koska kyseistä toiminnallisuutta ei ole olemassa. Aiemmassa sitaatissa käsitellään myös palveluntarjoajien asettamaa prioriteetti politiikkaa, jossa interaktiivisellekin liikenteelle annetaan vain juuri sen tarvitsema viiveettömyys, mikä sinällään luo osittaisesti jonoja sekä aiheuttaa uudelleen lähetyksiä, kun jokaisessa tilanteessa ei päästä edes minimivaatimustasolle viiveettömyydessä. Tällä tarkoitetaan että mikäli pelien data liikenne menee pääsääntöisesti oman verkon ulkopuolelle, WFQ:n käytöstä ei tällöin muodostu erityisen suurta hyötyä, sillä varsinainen pullonkaula on vasta oman verkon ulkopuolella erityisesti ahtaammilla kaistoilla.

3 DHCP-palvelu

DHCP-palvelu (Dynamic Host Configuration Protocol) mahdollistaa verkkoasetusten jakamisen asiakaslaitteille automaattisesti, jolloin ei ole tarvetta asettaa jokaiselle asiakaslaitteelle manuaalisesti esim. IP-osoitetta, verkkomaskia, oletus reititintä, sekä muita tarpeellisia tai hyödyllisiä verkkoparametreja.

DHCP-palvelun käyttöön tarvitaan DHCP-palvelin ja asiakaskoneiden täytyy käyttää DHCP-asiakas-palvelua. Asiakaskone aloittaa verkkoparametrien määrityksen lähettämällä kyselyn yleislähetysosoitteeseen (Broadcast address, 255.255.255.255 IPv4-verkoissa), jota kutsutaan DISCOVERY-paketiksi, se sisältää tiedot NIC:stä (Network Interface Controller, esim. verkkokortti tietokoneessa), mikäli verkossa on käytössä DHCP-relay – välityspalvelin se ohjaa DISCOVERY-paketit oikealle palvelimelle myös tapauksissa, joissa varsinainen DHCP-palvelin on kyseisen lähiverkon ulkopuolella. Yleisimmin kuitenkin paketti ohjautuu samassa verkossa tai pikemmin samassa broadcast-alueessa olevalle DHCP-palvelimelle, koska mikään muu verkkolaite ei siihen vastaa, mikäli vastaus palvelimelta, nimeltään OFFER-paketti ei saavu ajoissa takaisin, lähettää osoitteeton NIC uuden DISCOVERY-paketin, niin monesti kun sille on määrätty, useimmiten tämä määrä on 4 yritystä ja luovutus. Tällöin monet nykyiset niin Windows kuin Linux työasemat käyttävät zeroconf-palvelua /4/, josta Microsoft käyttää nimeä APIPA-palvelu /5/, joka asettaa laitteelle uniikin ns. huuhaa-osoitteen, joille on varattu käyttöön 169.254.0.0/16 -verkko-osoite IPv4:ssä tarjoten mahdollisuuden 65534 laiteosoitteelle, jolloin todennäköisimmin laite löytää vapaan osoitteen viimeistään toisella yrityksellä. Zeroconf ja APIPA-osoitteita ei reititetä ulkopuolisiin verkkoihin, joten tämä osoitteen jako tapa ei ole kovin hyödyllinen tapa perustaa lähiverkkoja, ja koska koneet arpovat osoitteensa itse niin laitteet saattavat saada osoitteet aivan eripuolilta verkko-osoitteistoa, joka edelleen syö hieman käytettävyyttä.

DHCP-palvelin vastaanottaessaan DISCOVERY:n tarkistaa lokistaan onko kyseinen laite saanut aiemmin jonkin osoitteen ja tarjoaa tätä OFFER-paketilla asiakkaalle, mikäli asiakaslaitetta ei listalta löydy palvelin määritystensä nojalla tarjoaa vapaana olevaa osoitetta asiakkaalle. Saatuaan OFFER-paketin tai uusiessaan edellistä osoitettaan DHCP-asiakas lähettää REQUEST-paketin, jolla siis pyydetään osoitetta palvelimelta, mikäli kyseessä on edellinen osoite pyytää asiakas saada edelleen käyttää sitä ja jos kyseinen osoite on vapaa tilassa palvelimella saa asiakas luvan ACT-paketilla käyttää samaa osoitetta, jos kyseessä on uutta osoitetta pyytävä laite se pyytää tällöin REQUEST-paketilla osoitetta, jota palvelin tälle tarjosi OFFER-paketilla ja palvelin kuittaa luvan osoitteelle ACT-paketilla. Jos asiakas pyytää osoitetta, jota palvelin ei voi myöntää lähettää palvelin asiakkaalle uuden OFFER-paketin ja jää odottamaan pyyntöä eli REQUEST-pakettia.

DHCP-palvelun myötä on mahdollista jakaa paljon oleellista ja joissain tapauksissa tarpeetonta tietoa verkon asiakaslaitteille. On mahdollista jakaa tiedot verkon sisäisistä palvelimista suoraan DHCP-tietueilla, mutta harva ohjelmisto osaa suoraan hyödyntää laitteille jaettuja tietoja, koska monissa verkoissa joitain näistä tiedoista ei ole tarpeen jakaa. Käytettävyyden kannalta on kuitenkin hyvä, että näitä tietoja voidaan jakaa asiakkaiden koneille. Tällöin asiakkaat voivat esimerkiksi Windows-alustalla ajaa komennon ”ipconfig /all” komentoriville ja saada tulosteen käytössä olevan verkon käytössä olevista palveluista ja palvelimista, mikäli nämä on määritelty jaettavaksi DHCP-palvelun myötä.

4 Tietoturvallisuus

Verkon tietoturvallisuus on suunniteltu siten, etteivät verkon asiakkaat voi tietäen aiheuttaa harmia verkon aktiivilaitteille eivätkä tietämättään aiheuttaa haittaa verkon suorituskyvylle käyttämällä tiettyjä ulkoverkon sivustoja tai palveluja, joista saattaisi koitua harmia verkon internet-yhteydelle. Verkkoon on suunniteltu ja implementoitu tiettyjä palveluja sekä sivustoja karsiva tutkiva pääsylista sekä ulkoverkosta sisään suuntaavaa liikennettä estävä palomuuri. Edellä mainittujen suodattimien oikeaoppisen toiminnan kannalta, tulisi verkon ulkoreuna reititin kytkeä julkiseen internet-yhteyteen, muutoin verkosta sallitut yhteystyypit eivät välttämättä toimi ja moninkertainen liikenteen suodatus hidastaisi yhteyttä kohtuuttomasti.

4.1 Yhteyden salaus

Yhteyden salaus ulkoverkkoon voisi tuoda parempaa tietoturvaa ja mikäli verkon sisällä käytettäisiin sovelluksia joiden tietoihin muilla ei ole oikeutta, olisi yhteyksien salaaminen yksi tärkeimmistä verkon tavoitteista. Verkko on rakennettu koostumaan kytkimistä ja reitittimestä, sekä verkossa on estetty ”väärien DHCP-palvelinten” toiminta, joten tällä verkko topologialla olisi lähes mahdotonta urkkia tietoja vahingossa. On tapoja kiertää myös tämä laitteistollinen suojaus, esimerkiksi ”tulvaamalla” kytkimeen MAC-osoitteita, tämän estimme TiTeLAN 109 tapahtumassa asettamalla portteihin riittävän tiukat MAC-osoite-rajoitustaulut, jonka vuoksi jouduimme tapahtumassa korjaamaan verkkoa käytönaikaisesti, kun muutamilla asiakkailla oli käytössä eräänlainen VPN-ohjelmisto nimeltä Hamachi, jolla luodaan virtuaalinen aliverkko mm. internetin yli. Kyseinen ohjelmisto teki juuri niin kuin MAC-Flood-hyökkäyksessä toimitaan, eli loi tietokoneelle virtuaalisia MAC-osoitteita, joilla se keskusteli muiden saman verkon Hamachi asiakasohjelmien kanssa ja aiheutti niiden linkkien alasajon, joissa Hamachi oli käynnissä. Ongelma ratkesi, kun saimme tietoomme mikä sovellus ongelman aiheuttaa ja kieltämällä kyseisen ohjelmiston käyttämisen. Ciscon kytkinten toiminta osoitti, ettei kyseistä verkkoa voida

urkkia virtuaalisten MAC-osoitteiden avulla, kun porttiturva (Port Security; Cisco IOS - AdvancedIP) on kytkettynä.

Varsinkin suurikuormaisen verkon liikenteen salaaminen on itsessään jo huono idea, mutta etenkin, kun verkolta odotetaan suurta datavirtaa sekä pieniä viiveitä on tällöin yhteyden salaaminen käsittämättömän huono idea. Mikäli mahdollista tulee ns. peliverkon aina olla mahdollisimman nopea ja tällöin salaaminen tulee jättää yritysverkkojen ominaisuudeksi.

Kukin käyttäjä voi tahtoessaan salata oman ulkoliikenteensä asianmukaisilla ohjelmistoilla, mutta tällöinkin edellä mainitussa peliverkossa tarvittavan portin avaamista täytyy anoa verkon ylläpitäjiltä, koska tietoturva syistä on useimmat pelaamiseen ja surffaamiseen ei tarvitut portit suljettu, jottei verkossa oleville koneille olisi niin paljon riskiä ulkomaailmasta tuleviin hyökkäyksiin.

4.2 Palomuuri

Verkon palomuuri on kaksiosainen, sisään- ja ulossuuntaavaa liikennettä käsitellään eri tavoin. Koska TiTeLAN verkkoon, eikä todennäköisesti moneen muuhunkaan tällä järjestelmällä luotavaan verkkoon ole tarkoitus päästä verkon ulkopuolelta käsiksi, voidaan tällöin ulkomuurille antaa yksirivinen suodatuslista [deny any], joka kieltää kaiken liikenteen, joka on aloitettu verkon tai tarkemmin ottaen reitittimen ulkoliitännän puolelta, tällöin ulkopuoliset voivat korkeintaan ajaa verkolle Dos-hyökkäyksen tai houkutella verkon sisällä oleva asiakas pahantahtoiselle sivustolle tai palvelimelle päästäkseen verkon sisälle kiinni. Dos-hyökkäyksellä tarkoitetaan palvelunestohyökkäystä, joka on useimmiten kiusantekoa, mutta yritysmaailmassa kyseessä voi olla kilpailijoille etua luova tapa häiritä yrityksen tietoliikennettä ja täten yrityksen toimintaa.

Sisäliitännälle suunnittelimme asianmukaisen pääsylistan (access list), jolla sallimme olennaiset palvelut, kielsimme ei-halutut sivustot ja palvelut sekä rajoitimme tiettyjen palveluiden käyttöastetta. Näin saimme luotua internet-yhteydellisen peliverkon, josta pääsi katsomaan sähköpostin ja hakemaan peleihin vaaditut päivitykset, muttei aiheuttamaan tarpeetonta kuormaa verkon muiden käyttäjien vastaaviin internet tarpeisiin. Esimerkiksi

tiedostonjako/lataus torrent-palvelu oli täysin estetty ja muun muassa yhteisösivustot facebook ja irc-galleria sekä videoportaali youtube olivat poissa käytöstä niiden aiheuttaman verkkokuorman sekä mahdollisten tietoturva uhkien vuoksi. Tietoturvallisuutta vaalien on helppo asettaa verkon aktiivilaitteille kohtuuton kuorma asettamalla liian monimutkaisia liikennettä suodattavia sääntöjä, siksi tuleekin jo suunnittelu vaiheessa harkita tarkoin millä tavalla kukin estettävä palvelu on kevyimmin estettävissä. Esimerkiksi torrent-palvelun esto on mahdollista monella eri tavalla, mutta näistä kätevin on protokollaa tutkiva ja estävä NBAR (Network Based Application Recognition) -sovellus, joka tunnistaa liikennevirrasta tiettyjen esimääritettyjen vertauskuvien perusteella liikennettä muodostavan ohjelmiston käyttämän protokollan ja tekee reitittimelle asetetun ohjeen mukaisen toimen. Nämä toimet voivat vaihdella kaiken vastaavan liikenteen pudottamisesta aina täsmäävän liikenteen prioriteetin nostoon saakka. Tällä sovelluksella voidaan siis erittäin helposti määrätä mitä liikennettä ulkoverkkoon suuntaa ja kuinka laajalla kaistalla kukin liikenne saa ja voi kulkea. Tämä sovellus on kohtuullisen raskas ajaa etenkin, jos se on määritetty tutkimaan montaa erilaista liikennetyyppiä, joilla on erilaisia pääsyrajoituksia. Tämä johtuu lähinnä siitä että kyseinen sovellus ei ole moni ajava, vaan järjestyksessä liikennetyyppejä tutkiva, kuten tavallinen pääsylista. Siksi tätä sovellusta käytettäessä palvelutason korottamiseen tietyllä liikennetyypillä on sallivat tunnistukset tehtävä ensimmäisinä ja estävät aina viimeiseksi, kun ensimmäinen osuma listassa on se johon tunnistus päättyy ja toimet toteutetaan.

NBAR-sovellusta huomattavasti nopeampi ja kevyempi ratkaisu on yksinkertainen- tai laajennettupääsylista, jollaista tulisi käyttää, mikäli liikenne on porttikohtaista. Tällöin voidaan avata ulossuuntaavat portit liikennetyypeille jotka sallitaan ja estää muut, koska näin tekemällä vain sallittu liikenne pääsee NBAR-sovelluksen tutkittavaksi. jolloin kaikkea liikennettä ei edes ajeta NBAR-sovelluksen läpi, joka keventää huomattavasti reitittimen taakkaa, kun osa kielletystä liikenteestä voidaan karsia jo ennen liikenteen yksityiskohtaisempaa tutkimista sekä suodatusta.

Sisäverkon sisäistä liikennettä ei tässä toteutusmallissa suodateta millään tavalla, mutta mikäli on tarpeellista estää sisäverkossa olevia laitteita keskustelemasta keskenään, sekin voidaan toteuttaa kohtuullisen vaivattomasti jakamalla verkko niin moneen VLAN (Virtual Local Area Network) -alueeseen kuin on tarpeen. VLAN-alueita asettamalla voidaan vaikka koko verkko jakaa yksilöllisiin alueisiin, joissa verkon käyttäjät eivät voi keskustella keskenään käymättä julkisessa verkossa, mikäli näin rajataan, toki on mahdollista tehdä tikunnokka-reititys, jolloin edellä mainittu keskustelu on mahdollista sekä rajoitettavissa tiettyihin palveluihin, mutta kyseinen toteutusmalli aiheuttaa huomattavan pullonkaulan käyttäjien väliselle keskustelulle, koska kaikki eri VLAN-alueissa olevien käyttäjien liikenne kuljetetaan reitittimen läpi ja

mahdollisesti tarkistetaan. Tietenkin samassa VLAN-alueessa olevat käyttäjät voivat asioida keskenään Layer2-liikenteenä käymättä reitittimessä ollenkaan.

VLAN-alueiden kautta voidaan fyysisesti eri kytkimelle kytketyt laitteet asettaa samaan aliverkkoon ja eristää ne muusta verkosta reitittimellä pääsylistoin, tällöin laitteet näkevät toisensa samassa lähiverkossa, mutta eivät näe heidän verkkoon kuulumattomia, mutta samassa IP-verkossa olevia laitteita, mikäli tätä ei ole erikseen sallittu. Esimerkiksi pääsy verkon aktiivilaitteille kielletään verkon käyttäjiltä, mutta sallitaan ylläpitäjiltä, voidaan toteuttaa asettamalla verkon aktiivilaitteet hallinnan VLAN-alueeseen 2 ja käyttäjät käyttäjien VLAN-alueeseen 3. Mikäli käyttäjiä pitää jakaa omiin ryhmiinsä, voidaan esimerkiksi osasto yhden käyttäjät asettaa VLAN-alueeseen 10 ja osasto kahden käyttäjät VLAN-alueeseen 20 ja asettaa kuitenkin yhteistyölle oleelliset palvelut reititettäviksi VLAN-alueiden 10 ja 20 välillä reitittimen kautta, kukin käyttäjä voidaan laittaa kumpaan tahansa ryhmään. VLAN tekniikasta lisää lähteen /6/ linkistä.

5 Verkkohyökkäykset

Ensimmäisenä on kysyttävä: ”Miksi joku haluaisi tunkeutua tietokoneeseen, jossa ei ole arkaluontoista tai muuten kriittistä tietoa?”

Vastaus kysymykseen on monimutkaisimpia asioita, jota käsitellään tässä työssä, kun kyseessä ei ole puhtaasti tekninen vastaus. Syy hyökkäykseen voi vaihdella kiusanteosta liiallisen uteliaisuuden kautta aina bottiverkkojen pystyttämiseen saakka, mutta nykyisin listan jälkimmäinen vaihtoehto on huomattavasti todennäköisempää kuin ”mikään muu syy”. On huomioitava puhuttaessa bottiverkoista, että siihen haluttavimmat jäsenet ovat hyvin usein tehokkaita, suuri prosessorisia tietokoneita, kuten raskaansarjan palvelimet tai pelitietokoneet. Tässä työssä keskitytään pelitietokoneisiin, kun verkonjakelu järjestelmän ensimmäinen käyttöönottokohde on LAN-tapahtuma, jossa parhaimmillaan jaetaan lähiverkkoa yli 100 pelitietokoneelle.

Pelitietokone on haluttava alusta osaksi bottiverkkoa, koska useimmiten kyseisessä konetyypissä on suorituskykyinen prosessori, ajureilla laskentakäyttöön konfiguroitu tehokas tai erittäin tehokas näytönohjain, keskivertoa heikompi tietoturva (jotta pelien ajaminen ja järjestelmän hallinta olisi helpompaa) sekä ikävän usein kyseisissä koneissa käytetään piraattiohjelmistoja, jotka ovat hyökkääjille kuin palkollisia namusetiä. moniin piraattiohjelmistoihin on ujutettu sisään troijalaisia sekä palomuuria muokkaavia ominaisuuksia, joista useimmat esiintyvät pelkkinä päivitys apuohjelmina. Pahaa aavistamattomat ohjelmistojen

laittomien kopioiden käyttäjät altistavat järjestelmänsä usein lähes täysin suojatta etähallittaviksi laskentakoneiksi hyökkääjien tarpeisiin.

5.1 Hyökkäystyypit

Verkoissa tapahtuvat hyökkäykset ovat yleisiä ja lähes mahdottomia estää. Tästä syystä verkon ylläpitäjien tuleekin osata ennalta varautua, että heidän verkkoonsa tullaan hyökkäämään, jonka vuoksi pyrkiä suojaamaan verkkonsa yleisimpiä hyökkäyksiä rajoittavaksi. Yksi yleisimmistä hyökkäyksistä nykyisin on DoS-hyökkäys (Denial of Service). Näissä palvelunesto hyökkäyksissä motiivina on useimmiten kiusanteko. Kyseistä hyökkäystä käyttämällä yhdistelmä hyökkäyksen osana voidaan aikaansaada hyökkääjän tarpeisiin olennainen toiminta kehittyneiltä verkkoprotokollilta, kuten liikenteen uudelleen ohjaus hyökkääjän hallinnoiman palvelimen kautta. Tätä kutsutaan MitM-hyökkäykseksi (Man in the Middle), eli suomalaisittain välimies hyökkäys.

Tämän välimies hyökkäyksen tarkoitus yleisimmin on tietojen urkinta ja toiseksi yleisimmin vastausten väärentäminen asiakkaalle. Välimies pystyy usein lähes huomaamattomasti välittämään todelliseen verkkopalvelimelta vastaanotettuun vastaukseen nähden identtisen vastauksen. Tällöin hyökkääjä voi usein lukea liikennevirrasta käyttäjätunnukset ja salasanat lähes vaivatta sekä tulkitsemaan lähetettyjä tietoja esimerkiksi henkilöllisyys varkauden parantamiseksi. Yksi yleisimmistä tavoista välimieshyökkäyksen aloittamiseen on yhdistelmä DoS-hyökkäystä ja väärennetyn DHCP-palvelimen tietojen mainostamalla yhteydettömäksi itseään luulevalle järjestelmälle.

Bottiverkot ovat yleistymässä maailmanlaajuisesti. Kuten aiemmin totesin, pelitietokoneet ovat heti raskaiden verkkopalvelimien jälkeen halutuimpia alustoja bottiverkkojen osaksi. Bottiverkoilla saavutetaan erittäin suuria laskentakapasiteettejä suuremman hyökkäyksen tai muun tietoturvarikoksen aikaansaamiseksi. On olemassa myös laillisia bottiverkkoja sekä käyttäjän suostumuksella tehtäviä bottiverkko tyyppisiä laskentoja, näistä yksi kuuluisimmista on osa SETI-projektia, jossa kotikäyttäjien tai suurempien koneiden hukkasuorituskykyä valjastetaan verkon yli Maapallon ulkopuolisen älyn etsintään sekä tähtien kartoitukseen. On olemassa myös muita laillisia bottiverkkoja, mutta useimmiten niistä käytetään nimitystä pilvilaskenta, ja nimitys bottiverkko yleisimmin viittaa tietokoneiden laskentakyvyn luvattomaan käyttöön.

Virukset, madot ja troijalaiset ovat yksi passiivisimmista hyökkäystavoista, joilla voidaan aikaansaada haittoja, etälaskentaa sekä tieto- ja henkilöllisyysvarkauksia. Näiltä on vaikeinta suojautua, sillä näiden riskien kohdalla kaikkein suurin vastuu on käyttäjällä itsellään. Suurimassa osassa tapauksista käyttäjä on tietämättään paremmin asettanut tai altistanut

tietojärjestelmänsä uhalle, jota hyödyntämällä hyökkääjän haittaohjelmisto ottaa järjestelmästä osia tai koko järjestelmän haltuunsa. Ajantasainen virusturva sekä hyvin päivitetty laittomia ohjelmistoja sisältämätön tietojärjestelmä ja valistunut internetin käyttö ovat ainoat tavat yrittää välttyä näiltä tietoturva riskeiltä.

5.2 Suojautuminen hyökkäyksiltä

Mikäli järjestelmässä käytettäisiin reititintä DHCP-palvelimena tai hierarkiassa olisi useampi reititin peräjälkeen, niin olisi hyödyllistä käyttää reititysprotokollia kertomaan verkon rakenteesta ulkorajalta verkon sisälle. Toki reititysprotokollien käyttö aiheuttaa mahdollisen tietoturva aukon, sillä Internetissä on saatavilla valmiita ohjelmia, joilla on mahdollista väärinkäyttää etenkin laajoihin verkkoihin suunniteltuja protokollia. Edellä mainittuja työkaluja jaellaan muun muassa muutamien Linux-jakeluiden mukana valmiina käyttöön, suurin osa kyseisistä jakeluista on peräti live-jakeluita, joilla siis käynnistetään tietokone ulkoiselta medialta, eikä täten käyttöjärjestelmiä saati ohjelmistoja tarvitse edes asentaa tietokoneisiin. Linux järjestelmissä on myös muita ominaisuuksia, jotka edesauttavat väärinkäytöksiä sekä heikentävät jäljitysmahdollisuuksia, kuten sisäänrakennettu MAC-osoitteen ohjelmistollinen muokkaus. Osittain tämän vuoksi on aina pyrittävä hyödyntämään DHCP-palvelun optiota 82, joka ei pahimmassa tapauksessa auta juurikaan, mutta mikäli hyökkääjä ei huomioi kyseisen palvelun käyttöä, niin kyseinen palvelu voi johtaa suoraan hyökkääjän jäljitettävyyteen. Toinen parempi vaihtoehto suojaamiselle tunnetussa verkkoarkkitehtuurissa on sallia verkkoon vain tietyt laitteisto-osoitteet (MAC-osoitteet), jolloin vain sallitut ”tiedossa olevat” laitteet voivat verkkoon liittyä, tämä tietenkään ei sovellu LAN-tapahtumaan, johon tämän työn järjestelmä alun perin on suunniteltu ja mitoitettu. Siksi tyydyimme optio82:n tuomaan jäljitettävyyden tasoon ja linkkien luotettavuus määrityksiä sekä kytkinten porttien MAC-osoitteiden määrärajoituksen aikaansaamaan lisäsuojaan. Kytkinten porttiturvallisuuden (Portsecurity) määrityksellä aikaansaadaan toiminta, jossa portti lukitsee itsensä automaattisesti, mikäli asetettua lukumäärää enemmän MAC-osoitteita yhdistyy porttiin ”yhtä aikaa” (kun käytössä ei ole muistava toiminto). Mikäli hyökkääjä asettaisi hänelle tarjottavaan asiakaslinkkiin hänen hallinnassaan olevan kytkimen, hyökkääjä voisi ”tulvata” esim. CDP-paketeilla (Cisco Discovery Protocol) verkon aktiivilaitteille väärää tietoa hierarkiasta tai MAC-osoitetaulun rajoituksen ylittävän määrän osoitteita. Täten DoS-hyökkäyksen avulla tunkeutua verkkoon, koska DoS-hyökkäyksen yhteydessä kytkimet käyttäytyisivät kuin hubit ja hyökkääjän olisi mahdollista nuuskia verkosta hänelle kuulumattomia tietoja. Porttiturvallisuus-toiminnon ollessa asetettuna esimerkiksi kolmeen laitteisto-osoitteeseen, portti lukitsee itsensä välittömästi, kun portissa on käytössä yli kolme laitteisto-osoitetta samanaikaisesti. DHCP-snooping asetuksen asiakasportille ollessa ei luotettu, tällöin portista hyväksytään vain DHCP-pyynnöt ja porttiin jaetut osoitteet voidaan ACT-viestin jälkeen raportoida DHCP-palvelimelle. Edellä mainitulla

tekniikalla voidaan DHCP-palvelimesta riippuen jakaa myös yksittäiset osoitteet kullekin portille, näin on erittäin helppoa aikaansaada jäljitettävyys sekä kiistämättömyys väärinkäytösten sattuessa.

Kiistämättömyys onkin yksi tietoturvallisuuden perusperiaatteesta, jonka mukaan kukin viesti tulee olla jäljitettävissä todelliselle lähettäjälle saakka, niin pätevästi että jäljityksellä saadut todisteet pätevät näytöksi oikeudessa. Muut pääperiaatteet ovat: saatavuus, luottamuksellisuus, eheys sekä tunnistus ja todennus. Saatavuudella tarkoitetaan, että tarvittu tieto on aina saatavilla, vain sitä tarvitseville käyttäjille ja/tai sovelluksille. Luottamuksellisuudella tarkoitetaan tiedon muokkauksen rajoittamista henkilöihin/sovelluksiin, joilla on siihen oikeus. Eheydellä tarkoitetaan tiedon koskemattomuutta sekä tiedon muokkaantumisen (korruptoitumisen) havaittavuutta, eheyttä voidaan käsitellä kahdella eri tasolla, joista sisäisellä eheydellä tarkoitetaan tiedon johdonmukaisuutta. Konkreettisesti tiedon johdonmukaisuus voi säilyä murretunkin eheyden jälkeen, mikäli hyökkäys on ollut riittävän edistynyt. Ulkoisella eheydellä tarkoitetaan tiedon paikkansapitävyyttä, joka onkin yleisimmin rikkoutunut, mikäli tiedon eheyteen kajotaan. On tärkeää huomioida, että vaikka tiedon ulkoinen eheys olisi kunnossa, tiedon sisältö voi muuttua täysin jos tiedon johdonmukaisuuteen kajotaan. Käytännössä esimerkiksi asiakirjan sisältöä siirrellään eri järjestykseen, tällöin ei asiakirjan koko, tarkistussumma eikä ascii-kartan käyttöaste muutu lainkaan, mutta sisältö on täysin eri alkuperäiseen verraten.

Ciscon laitteissa on oletuksena käytössä CDP (Cisco Discovery Protocol). CDP-protokollan käytöstä on hyötyä, mikäli laitteita ei pysyvästi manuaalisesti konfiguroida tiettyyn rooliin. CDP-protokolla kantaa mukanaan myös haittoja, koska se on luotu tuomaan yksikertaista Plug’n’Play -tyyppistä toiminnallisuutta välillä hieman monimutkaistenkin verkkolaitteiden käyttöönottoon. Tietoturvan kannalta tulisi CDP aina silloin kytkeä pois käytöstä, kun sitä ei erityisesti vaadita verkkototeutuksen toiminnallisuuden takaamiseksi. Tällöin CDP ei etsi portista kytkimiä eikä muita verkkolaitteita ellei niin ole erikseen asetettu, vaan olettaa portissa olevan asiakaskoneen tai muun ei-luotetun verkkolaitteen eikä täten tarjoa porttiin tietoja, joita ei asiakkaille kuulu. CDP:n kaltainen kehittyneempi versio on nimeltään smart port konfiguraatio, jota voi käyttää graafisen SDM-käyttöliittymän (Cisco Secure Device Management) kautta.

SDM-ohjelmisto onkin erittäin monipuolinen käyttöliittymä Ciscon laitteiden etähallintaan, mutta jälleen kerran tuo mukanaan kompastus kiven. SDM:n kautta konfiguroidut laitteet sisältävät usein moninkertaisen määrän asetuskomentorivejä, joista suurin osa on tarpeettomia halutun toiminnan aikaansaamiseksi. Tämä komentorivien määrä ei ole suoraan tietoturva riski, mutta voi aikaansaada sellaisen, jos verkkolaitteet voidaan ajaa DoS-tilaan näiden rivien vuoksi. Tästä syystä tuleekin aina tarkistaa, mitä rivejä SDM on kirjoittanut sekä epäselvissä tapauksissa ottaa selvää mitä kukin komento tekee, jotta voidaan taata vakaa ja mahdollisimman viiveetön verkkojakelu. SDM toki tuo mukanaan suuren määrän toimintoja sekä konfigurointia nopeuttavia ja helpottavia sovelluksia kuten esimerkiksi ’One step lockdown’, joka on erittäin hyödyllinen varsinkin hieman kokemattomille verkonhaltijoille. Edellä mainittua sovellusta voidaan käyttää

verkkolaitteen pikasuojaamiseen yleisimpiä tietoturva riskejä vastaan. Se sisältää listan komentoja, joka muun muassa poistaa CDP:n käytöstä. Lista komennoista ja niiden selitteistä on lueteltuna liitteessä 1. Lähteessä /7/ on lueteltu ja selitetty Cisco:n valmistamiin kytkimiin useimmiten käytettävät hyökkäystavat sekä ohjeistettu niiltä suojautumisessa.

6. Verkonjakelulaitteiden kuljetus ja käyttö

Verkonjakelujärjestelmän liikuteltavuus sekä koskemattomuus ovat olleet suunnittelun aloittamisesta lähtien ydinkriteerejä. Järjestelmästä suunniteltiin helposti siirrettävä ja helposti pystytettävä, jotta sitä voitaisiin käyttää mahdollisimman monessa tapahtumassa, joissa tarvitaan lähiverkon jakelua vaihtelevissa tiloissa TAMKin campuksella. Ensisijaisesti järjestelmä on ollut käytössä TiTeLAN -verkkopelitapahtuman sisäverkon jakelussa nykyisessä kokoonpanossaan jo kahdessa tapahtumassa tätä työtä kirjoitettaessa. Järjestelmän helppo siirrettävyys ja lukittavat lasioviset kaapit ovat osoittautuneet erittäin käyttökelpoisiksi tapahtuma käytössä. Olennainen osa järjestelmän liikuteltavuutta on sen pinottavuus kuljetuskuntoon, jolloin etäkytkimet pinotaan torniksi omissa pöytäkaapeissaan, jolloin koko jakelujärjestelmä voidaan siirtää kerralla jopa ulkona suurimman kaapin isojen pyörien ja hyvän maavaran ansiosta. Järjestelmän siirrettävyydessä voisi tehdä vielä hieman parannuksia ja päivityksiä, joilla korjattaisiin tähän mennessä havaittuja puutteita sekä heikkouksia. Suurimmaksi siirrettävyyden heikkoudeksi ovat osoittautuneet vääräntyyppiset pyörät ulkona liikkumisen kannalta. Nyt käytössä olevat muovirunkoiset kovakumipyörät ovat erinomaiset sisätiloissa, mutta esimerkiksi asvaltilla oleva hiekoitushiekka on haitaksi tasaisen etenemisen kannalta. Kehitysideana tämän ongelman poistamiseksi olisivat paineilmatäytteiset sisäkumilliset pyörät, jotka myös toisivat tasaisemman painojakauman järjestelmän kannatukseen. Kuviossa 1 on esitetty järjestelmä kuljetuskunnossa. Kuviossa 1 nähdään ovet avattuna kaapit, jotka on numeroitu pinoamisjärjestyksessä, näistä alin eli kaappi 0 on tarkoitettu reitittimille, runko kytkimille, UPS:lle sekä mahdollisesti pienelle verkkopalvelimelle, jolle ei tämän työn puitteissa hankittu räkkiin asennettavaa koteloa.

Kuvio 1. Verkonjakelujärjestelmä torniksi pinottuna.

Pöytäkaapeissa on tilaa läpi pujotettavien johtojen lisäksi enintään kahdelle kytkimelle kaappia kohden, jolloin Cisco C2960-24tx-kytkimiä käytettäessä voitaisiin jakaa 48 asiakkaalle lähiverkkoyhteyttä yhden pöytäkaapin sisältä. Cisco valmistaa Catalyst 2960 sarjassa myös 48 laiteportin 1 U:n kytkimiä, joita käyttämällä voisi tarjota yhdestä pöytäkaapista 96 asiakkaalle lähiverkkoyhteyden, mutta silloin alkaisi jo johdotus tila loppua pöytäkaapeista. Pöytäkaapit on kiinnitetty toisiinsa ja alakaappiin kuviossa 2 esitetyin lukoin. Kuten siitä voidaan havaita, lukoissa sisällä on pieni hammas, joka estää kaapin liukumisen, sekä salpa, joka kiristää kaappien välisen sauman tiiviiksi. Lukot ovat valmistettu ruostumattomasta teräksestä ja lukot on kiinnitetty ruostumattomin pop-niitein kaappien runkoihin. Näiden lukkojen ansiosta järjestelmä on helppo pinota kuljetuksen ajaksi ja purkaa osiin hajautettaessa. On myös helppoa mitoittaa tarvittava järjestelmän laajuus ennen siirtämistä ja tarvittaessa lisätä siihen moduuli, mikäli on tarve laajentaa järjestelmää. Pöytäkaapit on suunniteltu toimimaan moduuleina järjestelmässä eli ne sisältävät vain laitteen identifioimisessa ilmenevät erot konfiguraatioissaan, joten ylimääräisen moduulin lisääminen käynnissä olevaan verkkoon ei ole ongelma.

Kuvio 2. Kaapien kiinnitysmenetelmänä käytetty lukko

Isomman eli alakaapin kalustukseen kuuluu 1 kVA UPS, kaksi Hewlett Packard 24*1G 3400-sarjan hallittavaa kytkintä sekä kaksi Ciscon 2811-sarjan reititintä, joista toinen on varalla sekä laiterikon varalla olevat kaksi kytkintä, jotka ovat konfiguroitu valmiiksi geneerisiin asetuksiin. Järjestelmään on suunniteltu myös lisättäväksi automaattisen konfiguroinnin mahdollistavaa palvelinta, joka tunnistaisi verkkoon kytkettävän kytkimen sekä antaisi juuri siinä sijainnissa olevan kytkimen asetukset uudelle laitteelle, joka asennetaan korvaamaan esim. rikkoontunutta. Näin saavutettaisiin vielä suurempi plug-and-play, koska tällöin ei laitteita tarvitsisi konfiguroida geneerisiksi etukäteen. Järjestelmä huolehtisi, että tietyn alueen kytkimen korvaavalla olisi samat tunnistetiedot, jotta jäljitettävyys ei kärsi laitevaihdon yhteydessä. Toki on huomioitava, ettei käytetyillä laitteilla ilmene laiterikkoja kovin usein, joten kyseinen järjestelmä on edelleen idea-asteella.

LÄHTEET

Painetut lähteet

/1/ Gary A. Donahue, Network Warrior. O'Reilly 2007

/2/ Laura Chappel, Advanced Cisco Router Configuration. Macmillan Technical publishing / Cisco Press 1999

Sähköiset lähteet

/3/ - WFQ:n käyttö FPS-peleissä http://www.nas.ewi.tudelft.nl/publications/2006/conext06.pdf - 1.7.2009

/4/ - Zeroconf:in määrittelevä RFC-dokumentti - RFC 3927 - http://tools.ietf.org/html/rfc3927 - 1.7.2009

/5/ - APIPA-palvelu - http://msdn.microsoft.com/en-us/library/aa505918.aspx - 1.7.2009

/6/ - VLAN - http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml - 30.7.2009

/7/ - Cisco kytkimien useimmiten käytetyt hyökkäykset ja niiltä suojautuminen - http://www.bitmindframes.info/switch-security-common-attacks - (julkaistu 18.6.2009)