JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ:

Extreme Networksin L2-tietoturvaominaisuudet

Juha Piispanen

Opinnäytetyö
Toukokuu 2012

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTi

Tekijä(t) PIISPANEN, Juha	Julkaisun laji Opinnäytetyö	Päivämäärä 11.05.2012
	Sivumäärä 110	Julkaisun kieli Suomi
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty (X)

Työn nimi
EXTREME NETWORKSIN L2-TIETOTURVAOMINAISUUDET

Koulutusohjelma
Tietotekniikan koulutusohjelma

Työn ohjaaja(t)
NARIKKA, JORMA

Toimeksiantaja(t)
Jyväskylän ammattikorkeakoulu Oy
VATANEN, MARKO

Tiivistelmä

Opinnäytetyö toteutettiin Jyväskylän ammattikorkeakoulun SpiderNet-laboratorioympäristössä. SpiderNet-laboratorio ympäristöä käytetään Jyväskylän ammattikorkeakoulun tietotekniikka-koulutusohjelman opetuksessa, sekä tutkimus- ja kehityshankkeissa.

Opinnäytetyön tavoitteena oli toteuttaa SpiderNet-laboratorioympäristöön L2-kytkinympäristö Extreme Networksin laitteilla, jossa testattiin ja todennettiin Extreme Networksin kytkinten tukemia L2-tason tietoturvatekniikoita. Työssä käytössä oli Extreme Networksin BlackDiamond 12802 ja Summit X250 -kytkimiä.

Työssä rakennettu verkko jaettiin neljään kokonaisuuteen, jossa testattiin ja todennettiin eri tietoturvatekniikoita. Kokonaisuudet keskittyivät Private VLAN:n (PVLAN), 802.1X-autenttikoinin, MAC- ja IP-securityn sekä CLEAR-Flow'n testaamiseen.

Työn tuloksena saatiin testattua ja todennettu käytettyjen tietoturvaominaisuuksien toiminta. Tämän lisäksi Jyväskylän ammattikorkeakoulun tietotekniikka-koulutusohjelmalle toteutettiin kaksi laboratorioharjoitusta, jotka käsittelivät tutkittuja tietoturvaominaisuuksia.

PVLAN, 802.1X, MAC, IP, Security, SpiderNet, L2, LLDP, ARP

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
PIISPANEN, JUHA	Bachelor´s Thesis	11052012
	Pages 110	Language Finnish
	Confidential ( ) Until	Permission for web publication (X)

Title
L2-SECURITY OF EXTREME NETWORKS

Degree Programme
Data Network Technology

Tutor(s)
NARIKKA, Jorma

Assigned by
JAMK University of Applied Sciences
VATANEN, Marko

Abstract

This bachelor's thesis was carried out in SpiderNet. SpiderNet is a laboratory at JAMK University of Applied Sciences. SpiderNet is mainly used in data network technology degree program, it is, however, also used in several research and development projects such as bachelor's theses.

The main goal of this thesis was to building a layer 2 network topology using Extreme Networks switches. The topology was used to implement, test and study L2-security techniques. BlackDiamond and Summit X250 switches from Extreme Networks were used in this thesis.

Topology that was built in this thesis were divided into four sections. Each section was tested with different security techniques. The techniques were Private VLAN (PVLAN), 802.1X, MAC & IP Security and CLEAR-Flow.

As a result of the thesis the security techniques were configured and tested in the SpiderNet laboratory. Additionally two laboratory exercises were completed for the use of JAMK University of Applied Sciences.

Keywords

PVLAN, 802.1X, MAC, IP, Security, SpiderNet, L2, LLDP, ARP

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

LYHENTEET

ACL	Access Control List
ARP	Address Resolution Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
FDB	Forwarding Database
FIB	Forwarding Information Base
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
LLDP	Link Local Discovery Protocol
MAC	Media Access Control
POE	Power Over Ethernet
PVLAN	Private Virtual Local Area Network
QoS	Quality of Service
SNMP	Simple Network Management Protocol
TDM	Time-division multiplexing
TLV	Type, Length and Value
TPMR	Two port MAC Relay
VLAN	Virtual Local Area Network

1 TYÖN LÄHTÖKOHDAT

1.1 Toimeksiantaja

Työn toimeksiantajana on Jyväskylän ammattikorkeakoulun (JAMK) tietotekniikan koulutusohjelma. JAMK tarjoaa koulutusta ammattikorkeakoulututkintoihin ja ylempiin ammattikorkeakoulututkintoihin sekä opetuksesta kiinnostuville myös opettajakoulutusta.

Jyväskylän ammattikorkeakoulu on vetovoimainen ja kansainvälinen korkeakoulu. Toimipisteet sijaitsevat Jyväskylässä ja Saarijärven Tarvaalassa. Opiskelijoita Jyväskylän ammattikorkeakoulussa on yli 8000. JAMK tarjoaa korkeakoulututkintoon johtavaa koulutusta, ammatillista opettajakoulutusta, avoimia ammattikorkeakouluopintoja, täydennyskoulutusta ja myös oppisopimustyyppistä täydennyskoulutusta nuorille ja aikuisille. (Jyväskylän ammattikorkeakoulu 2012a.)

Tietotekniikan koulutusohjelma

Tietotekniikan koulutusohjelma keskittyy pääsääntöisesti tietoverkkotekniikan osaalueelle. Koulutusohjelman opintojen kokonaislaajuus on 240 opintopistettä. Opetuksen painopistealueina korostuvat laajakaista, langattomat ja langalliset operaattoritason teknologiat, verkkojen ylläpito ja suunnittelu sekä tietoturvallisuuden hallinta. Koulutusohjelman kolmantena vuotena opiskelijat voivat valita neljästä eri ammatillisesta osaamisalueista kaksi, joihin he erikoistuvat. Valittavana ovat Cisco Network Academyn CCNP, langattomat tietoliikennejärjestelmät, tietoturva ja palveluiden hallinta sekä verkkopalveluiden laadun hallinta -opintojaksot. Cisco Network Academyn Cisco Certified Network Professional (CCNP) on Cisco Systemsin laatima kansainvälinen opintokokonaisuus, joka tarjoaa valmiudet verkkotekniikoiden ammatilliseen soveltamiseen sekä valmiudet suorittaa CCNP-sertifikaatti. Langattomat tietoliikennejärjestelmät - opintojakson jälkeen opiskelija kykenee soveltamaan tietojaan lisensoimattomien lyhyen kantaman ja lisensoitujen laajan kantaman langattomien tietoliikennejärjestelmien suunnittelussa ja toteutuksessa. Tietoturva ja palveluiden hallinta -opintojakson avulla opiskelija kykenee vastaamaan yrityksen verkkojen ja palve-

luiden tietoturvasta, hallinnasta sekä ylläpidosta. Verkkopalveluiden laadun hallinta tuttavallisemmin QoS (Quality of Services)-opintojakso keskittyy IP-QoS mekanismien ja runkoverkkojen palvelunlaatuun vaikuttavien tekniikoiden opettamiseen ja soveltamiseen. (Jyväskylän ammattikorkeakoulu 2012b).

1.2 Tavoitteet

Opinnäytetyön tavoitteena oli toteuttaa Jyväskylän ammattikorkeakoulun SpiderNet-laboratorioympäristöön Extreme Networksin laitteilla Layer2 (L2) -kytkinympäristö, jossa testataan ja todennetaan L2-tietoturvatekniikoita. Ympäristö jaettiin neljään osaan käytettävien tietoturvatekniikoiden mukaisesti. Sillä kaikkia käytettäviä tekniikoita ei ole mahdollista käyttää samanaikaisesti. Yksi osa keskittyy PrivateVLANiin (PVLAN), toinen IP-security -tekniikoihin, kolmas IEEE 802.1X sekä Radiukseen ja viimeinen ACL ja CLEARFlow -tekniikoihin.

Tavoitteena oli myös testata tekniikoiden toimivuus multivendor-ympäristössä, jossa Extreme Networksin ohella käytetään Cisco Systemsin laitteita. Opinnäytetyön lopputuotteena toteutetaan Jyväskylän ammattikorkeakoulun tietotekniikka-koulutusohjelmalle kaksi laboratorioharjoitusta.

2 EXTREME NETWORKS

2.1 Yleistä

Extreme Networks on perustettu vuonna 1996 Californian Santa Clarassa. Extreme Networks suunnittelee, rakentaa ja asentaa Ethernet-ratkaisuja, jotka vastaavat haasteisiin, joita IP-pohjaiset verkot tuovat. Yritys on toimittanut yli 25 miljoonaa Ethernet-porttia ja vaikuttaa yli 50 maassa. Extreme Networks palvelee asiakkaitaan sekä langallisissa että langattomissa verkkotekniikoissa. Extreme Networks tarjoaa näiden tekniikoiden lisäksi asiakkailleen täydentäviä palveluita esimerkiksi suunnittelupalvelut sekä turvallisuuskartoitukset. (Extreme Networks 2011a.)

2.2 Laitteet

2.2.1 Yleistä

Extreme Networksin laitetarjonta on keskittynyt kytkimiin. Kytkimet Extreme Networks on jakanut Summit- sekä BlackDiamond-sarjoihin. Kytkinten lisäksi Extreme Networksin tarjonnassa on langattomiin verkkoihin tarkoitettuja ratkaisua, kuten WLAN-tukiasemat sekä 2G- ja 3G-verkkojen päätepisteenä toimivien reitittimien tarjoaminen, jotka muuntavat matkapuhelinverkoissa käytettävät TDM T1/E1 yhteydet Ethernet yhteyksiksi. (Extreme Networks 2011b.)

2.2.2 Summit-sarja

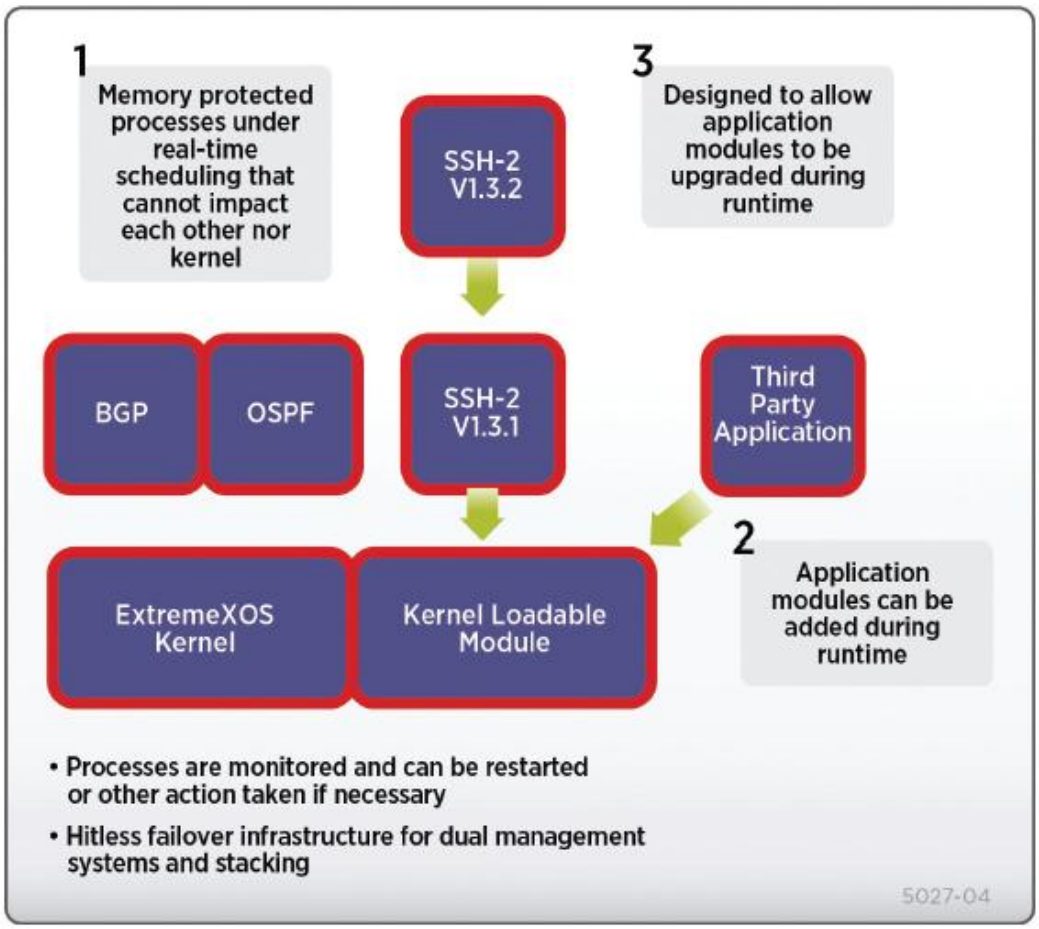
Summit-sarjan kytkimien ominaisuudet kattavat Access-tason kytkimestä aina Core-tason kytkimiin. Summit-sarjan ominaisuuksiin kuuluvat muun muassa palvelunlaatu (QoS), Power over Ethernet (PoE). Lisäksi sarja tarjoaa verkkoon joustavuutta ja alhaisen viiveen. Suurin ero Summit-sarjan ja BlackDiamond-sarjan välillä on Summit-sarjan käyttämä SummitStack-tekniikka. SummitStack-tekniikka mahdollistaa useamman kytkimen liittämisen yhdeksi loogiseksi kytkimeksi. SummitStack-tekniikkaa käyttäviä kytkimiä oli kirjoitushetkellä kahdeksan mallia. (Extreme Networks 2011b.)

2.2.3 BlackDiamond-sarja

BlackDiamond-sarjan kytkimet on tarkoitettu datacentereihin, metro Ethernetin runkoon ja kaikkiin muihin korkeaa suorituskykyä vaativiin verkkoihin. BlackDiamond-sarja soveltuu erinomaisesti verkkoihin, joissa käsitellään reaaliaikaista puhetta ja videota, koska kytkimet pystyvät välittämään liikennettä minimaalisella viiveellä sekä viiveen vaihtelulla (Jitter). Kirjoittamishetkellä BlackDiamond-sarja jaotellaan X-sarjaan ja 8800-sarjaan. Näistä X-sarja on tarkoitettu DataCentereihin. X-sarjan kytkimet tarjoavat 20 Tbps kokonaiskytkinkapasiteettiä ja jopa 40 GbE porttinopeuden. 8800-sarja on suunniteltu datacenttereiden ohella myös runkokytkimiksi. 8800-sarjan ominaisuuksiin kuuluvat korkea PoE-kapasiteetti, 10Gbe porttinopeus ja korkea saatavuus. (Extreme Networks 2011b.)

2.3 ExtremeXOS

ExtremeXOS on Extreme Networksin kehittämä käyttöjärjestelmä, jota kaikki Extreme Networksin kytkimet käyttävät. ExtremeXOS on ollut käytössä yli kahdeksan vuotta ja se on saanut CommonCriterian EAL 3+ sertifikaatin. ExtremeXOS on kehitetty verkkoihin, joilta vaaditaan korkeaa suorituskykyä sekä saatavuutta. Tämä saavutetaan ExtremeXOS korkeaan saatavuuteen perustuvalla arkkitehtuurilla sekä käyttämällä käyttöjärjestelmän tukemia saatavuutta parantavia tekniikoita kuten Extremen kehittämää Ethernet Automatic Protection Switching (EAPS). ExtremeXOS on CLI-pohjainen käyttöjärjestelmä, joka tukee myös CLI-skriptausta, jolla voidaan automatisoida monimutkaisia tehtäviä ja näin vähentää inhimillisiä virheitä. ExtremeXOS on tehty modulaariseksi käyttöjärjestelmäksi, joka mahdollistaa samanaikaisesti useamman ohjelman tai protokollan ajamisen vaikuttamatta muihin prosesseihin (Ks. kuvio 1).



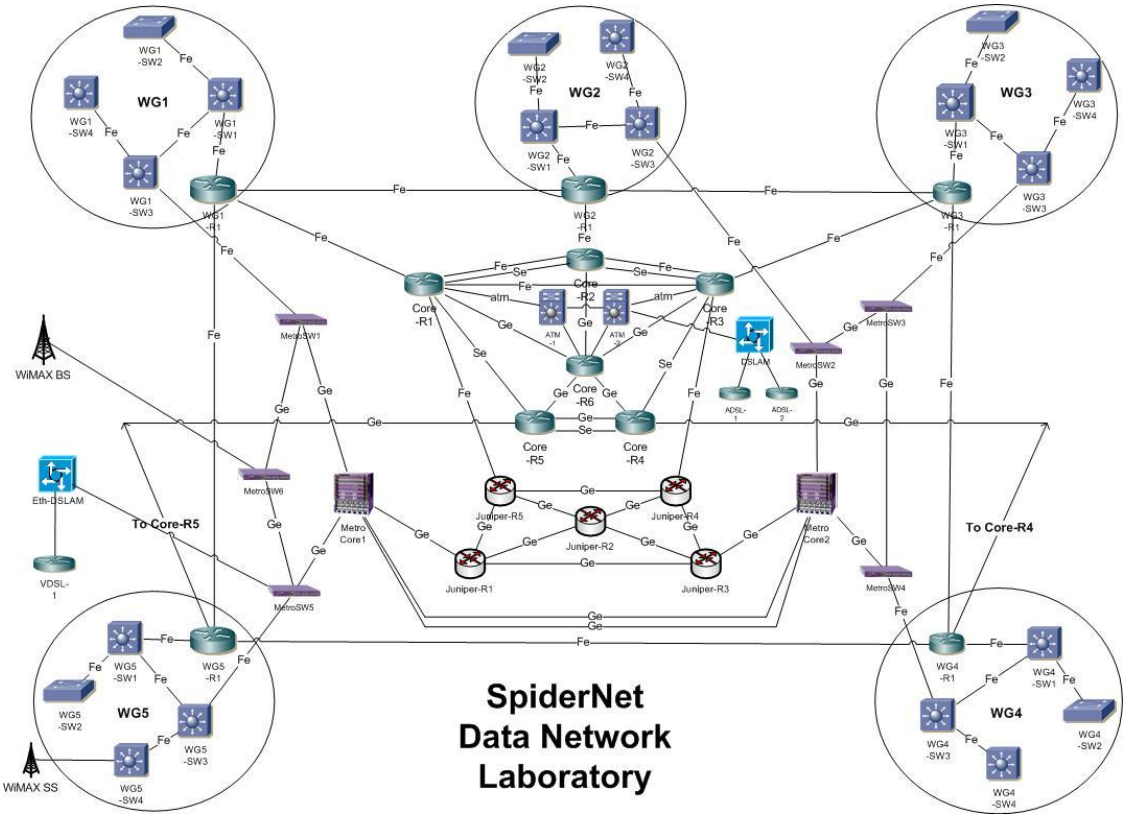
KUVIO 1. ExtremeXOS-käyttöjärjestelmä (Extreme Networks 2011c)

3 SPIDERNET

3.1 Yleistä

SpiderNet on JAMK:n tietoverkkolaboratorioympäristö. SpiderNetiä on kehitetty yli kymmenen vuotta. Kehitys jatkuu edelleen, jotta uudet tekniikat, joita operaattorit ja palveluntarjoajat käyttävät, tulisi katetuiksi. SpiderNetiä käytetään pääasiallisesti tietoverkkokursseilla, mutta myös tutkimus- ja kehityshankkeissa. (Labranet 2011.)

SpiderNet tarjoaa realistisen tietoverkkoympäristön, jossa on usean valmistajan laitteita. Tällä hetkellä SpiderNetistä löytyy laitteita seuraavilta laitevalmistajilta: Airspan Networks, Cisco Systems, Extreme Networks, Juniper Networks ja Zhones. SpiderNet rakentuu Cisco Coresta, Metro Ethernetistä, Juniper Coresta sekä viidestä työryhmästä (ks. kuvio 2), (Labranet 2011.)

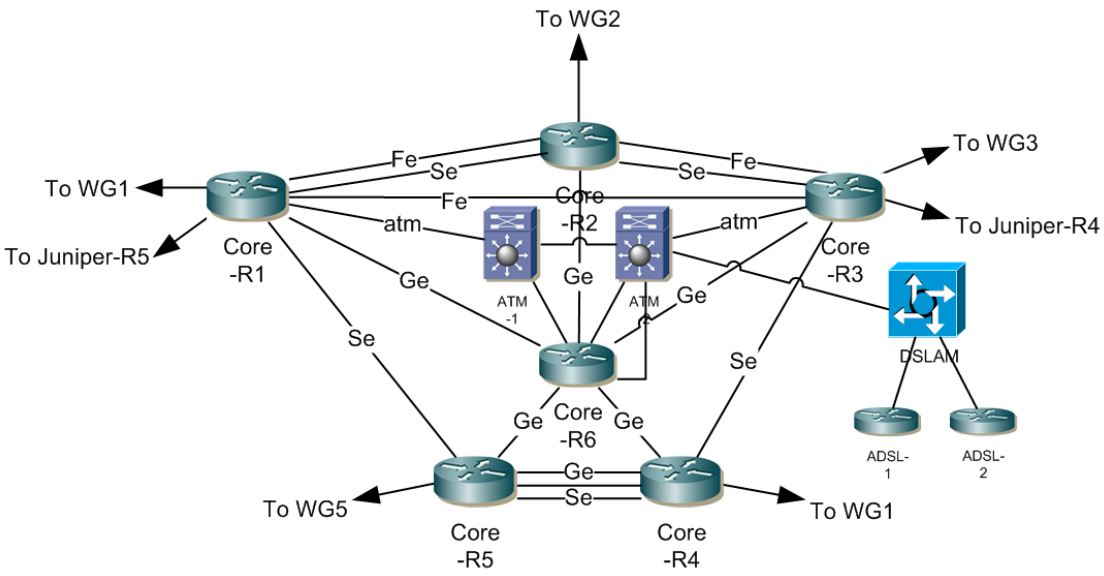


KUVIO 2. SpiderNet Topologia (Labranet 2011)

SpiderNet-ympäristö tarjoaa tuen useisiin verkkoprotokolliin lähtien peruslähiverkkotekniikoista, kuten VLAN-reititys ja IGP-reititysprotokollat (EIGRP, OSPF) aina monimutkaisempiin runkoverkon tekniikoihin, kuten Mac-in-Mac(802.1AH) ja MPLS-VPN. SpiderNet on eristetty kokonaan Jyväskylän ammattikorkeakoulun tuotantoverkoista. SpiderNetin laitteiden hallinta on toteutettu Ciscon terminal-palvelimen avulla, joka muuntaa lähiverkkoyhteyden konsoliyhteydeksi. SpiderNetiin on myös yhdistetty VmWare ESX-virtuaalipalvelin, joka tarjoaa työryhmille 3 virtuaalikonetta (yksi Linux-palvelin ja kaksi Windows-työasemaa.) Virtuaalikoneiden avulla voidaan testata konfiguraatioiden toimivuus sekä tarjota erinäisiä palveluita verkkoon. (Labranet 2011.)

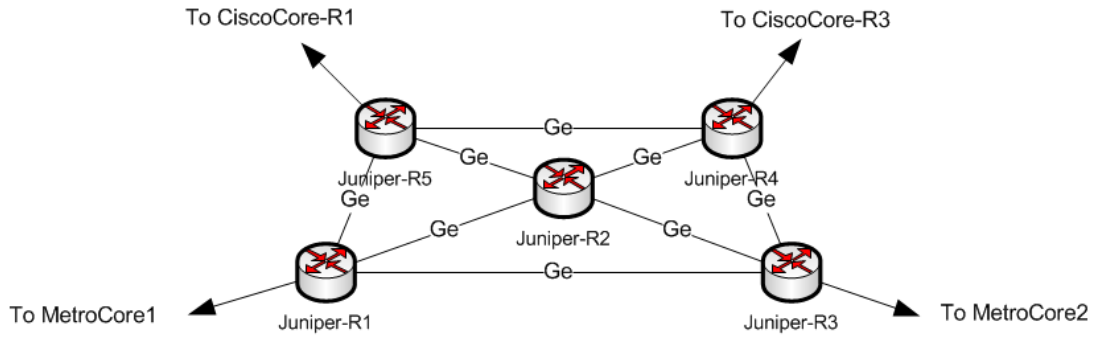
3.2 Laitteisto

Cisco Coressa on kolme Cisco Systemsin 3640-sarjan reititintä (Core-R1,Core-R2 ja Core-R3) sekä kolme 7200-sarjan reititintä (Core-R4, Core-R5 ja Core-R6). Näiden lisäksi Cisco Coressa on kaksi ATM-reititintä ja DSLAM, johon on kytketty ADSL-modeemeja. Jokainen Cisco Core -reititin on kytketty myös omaan työryhmään (WG1 – Core-R1), lisäksi Core-R1- ja Core-R2-reitittimistä on yhteys Juniper Coreen. (Ks. kuvio 3.)



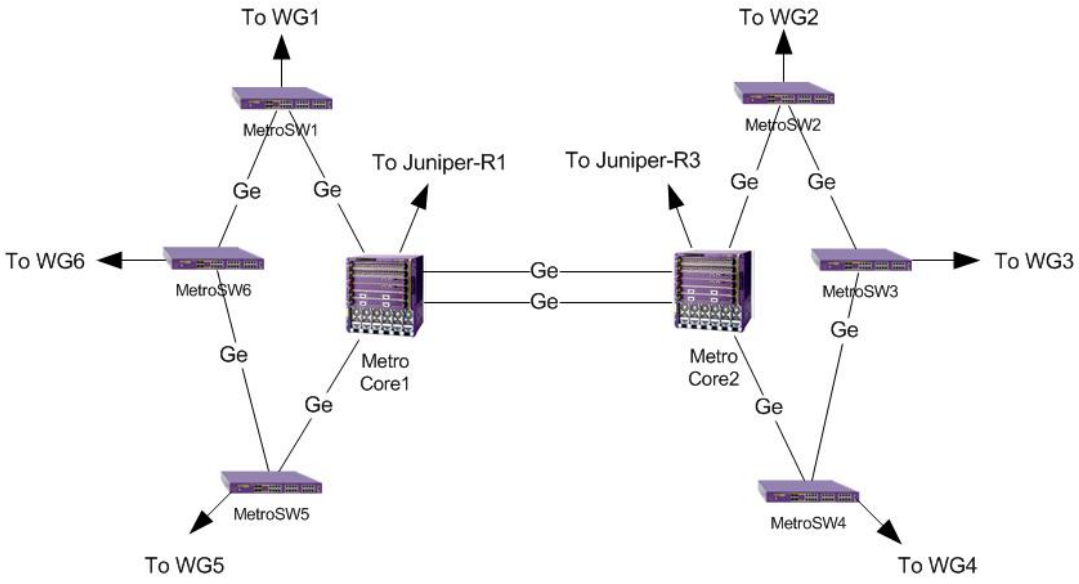
KUVIO 3. Cisco Core

Juniper Core muodostuu viidestä Juniperin J2320-reitittimestä. Kahdesta näistä reitittimistä on yhteys Cisco Coreen ja kahdesta on yhteys Metro Ethernetin MetroCore kytkimiin. (Ks. kuvio 4.)



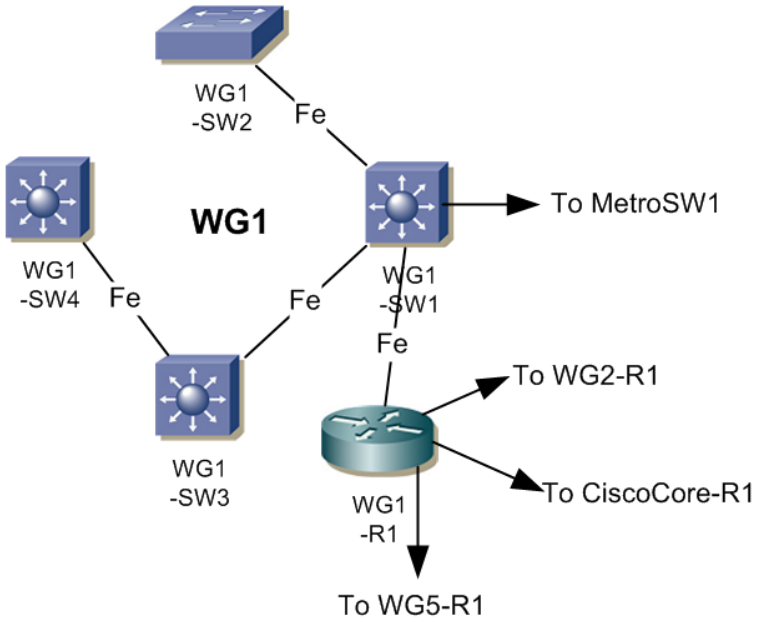
KUVIO 4. Juniper Core

Metro Ethernet koostuu kahdesta Extreme Networksin Black Diamond 12802-kytkimestä (MetroCore 1-2) sekä kuudesta Summit X250 -kytkimestä (MetroSW 1-6). Metro Ethernet on kytketty niin, että se muodostaa kaksi erillistä rengasta, joiden välillä voidaan testata ja todentaa esimerkiksi MACinMAC (802.1AH) tekniikkaa. MetroCore-kytkimistä on yhteys Juniper Coreen, ja jokainen MetroSW-kytkin on yhdistetty työryhmään. (Ks. kuvio 5.)



KUVIO 5. Metro Ethernet

Työryhmät (WG1-5) ovat kaikki identtisiä. Nämä työryhmät koostuvat yhdestä Cisco Systemsin 2821-reitittimestä (WGx-R1) sekä 3550 L2/L3-kytkimestä (WGx-SW1) sekä 2950-L2 kytkimestä(WGx-SW2). Näiden lisäksi työryhmissä on kaksi Extreme Networksin Summit e48 kytkintä (WGx-SW3-4). 2821-reitittimet on kytketty vastaaviin CiscoCore-reitittimiin (WG1-R1 – CiscoCore-R1). Tämän lisäksi reitittimet on kytketty naapurityöryhmien reitittimiin. Toinen Summit e48-kytkimistä (WGx-SW3) on kytketty MetroCoren vastaaviin kytkimiin (WG1-SW3 – MetroSW1). (Ks. kuvio 6.)



KUVIO 6. WG1

4 PRIVATE VLAN

4.1 Yleistä

Private VLAN (PVLAN) on tekniikka, jonka avulla voidaan samassa aliverkossa olevat päätelaitteet eristää toisistaan L2-tasolla eli OSI-mallin toisella kerroksella (siirtokerros). Tekniikan avulla voidaan luoda isompia aliverkkoja ja näin ollen säästää IP-osoitteita. PVLAN on Cisco Systemsin kehittämä tekniikka, ja Cisco Systems on julkaisut tekniikasta RFC 5517 -muistion. (Foschiano & HomChaudhuri 2010, 1.)

Ethernet-verkossa jokainen Virtual LAN (VLAN) on erillinen Broadcast-alue, jossa päätelaitteet ovat yhteydessä toisiinsa suoraan L2-tasolla. Tämän takia jokaisen VLANissa olevan päätelaitteen tulee olla luotettava, muuten verkkoon voi syntyä tietoturvariski. Perinteisesti tämä ongelma ratkaistaan luomalla uusi VLAN ja samalla uusi aliverkko, jolloin uudet päätelaitteet ovat toisessa Broadcast-alueessa. Tämä ratkaisu toimii pienissä verkoissa, joissa skaalautuvuus ja VLANeille IEEE 802.1Q standardin asettama 4094 maksimi määrä ei ole ongelma. Mutta suurissa verkoissa, kuten palvelinhotelleissa, joissa laite ja asiakasmäärä kasvavat suureksi, 802.1Q:n asettama 4094 VLANin maksimimäärä voi tuottaa ongelmia. Mitä tehdä, kun asiakasmäärä kasvaa 4095:een? (Foschiano & HomChaudhuri 2010, 2.)

Kuten aiemmin todettiin, VLAN on yksi Broadcast-alue. Private VLAN -tekniikan avulla voidaan normaalin VLANin broadcast-alue jakaa pienempiin sub-domaineihin. PVLANissa on määritelty kahdenlaisia sub-domaineita: Isolated ja Community. Extreme Networks kutsuu sub-domaineita Subscriber-VLANeiksi eli tilaajaVLANeiksi. Lisäksi Extreme Networks käyttää Community sub-domainista nimitystä Non-Isolated. Sub-domainit ovat VLANeja, jotka on liitetty Private VLANiin. (Foschiano & HomChaudhuri 2010, 3.)

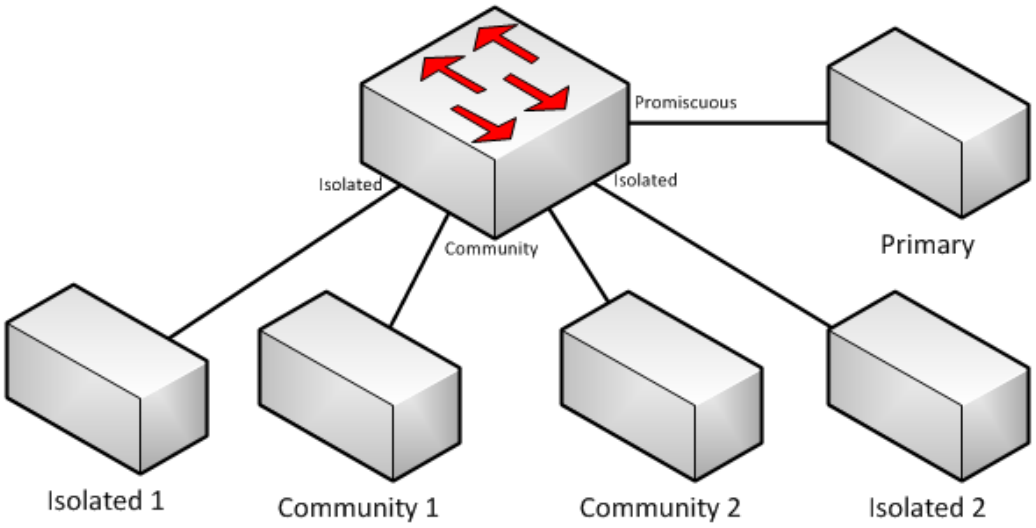
PVLANin sisällä kytkimen portit voidaan konfiguroida kuuluvaksi yhteen kolmesta määritellystä tilasta. Nämä tilat ovat Promiscuous, Community ja Isolated. Jokaisella näistä tiloista on omat sääntönsä, joilla kontrolloidaan porttiin liitetyn päätelaitteen

kommunikointi toisten samassa Private VLANissa olevien päätelaitteiden kanssa. (Foschiano & HomChaudhuri 2010, 3.)

Promiscuos-porttiin liitetty päätelaite pystyy keskustelemaan kaikkien PVLANiin liitettyjen päätelaitteiden kanssa. Tämän takia Promiscuous-portteihin kytketään yleensä L3-tason laite, esimerkiksi DHCP-palvelin tai verkon oletusyhdyskäytävä. Community tilan avulla voidaan Private VLANin sisälle muodostaa ryhmiä. Näihin ryhmiin liitetyt portit voivat keskustella samassa ryhmässä olevien porttien kanssa sekä Promiscuous porttien kanssa, mutteivät toisissa ryhmissä olevien eivätkä Isolated-porttien kanssa. Isolated portit pystyvät keskustelemaan ainoastaan Promiscuous porttien kanssa. Isolated portit on nimensä mukaisesti eristetty L2-tasolla toisista porteista. (Foschiano & HomChaudhuri 2010, 3-4.)

Porttien asettaminen haluttuun tilaan tapahtuu liittämällä ne VLANeihin, joita on myös kolmea eri tyyppiä. Isolated-porttia vastaa Isolated VLAN, Community-porttia vastaa Community VLAN ja Promiscuous-porttia vastaa Primary VLAN. Extreme Networks käyttää Primary VLANin tilalla Network VLAN -nimitystä. (Foschiano & HomChaudhuri 2010, 4.)

Kuviossa 7 on esitetty esimerkkikonfiguraatio PVLANista. Konfiguraatiossa on yksi PVLAN, johon on luotu yksi primary-VLAN sekä neljä sub-domainia. Sub-domaineista kaksi on konfiguroitu Isolated-tilaan ja kaksi Community-tilaan. Taulukossa 1 on esitetty VLANien kommunikointi PVLANissa. Taulukosta 1 nähdään, etteivät isolated VLANit voi keskustella muun kuin Primary-VLANin kanssa. Community VLANit voivat keskustella Primary VLANin lisäksi samassa Community VLANissa olevien laitteiden kanssa. Jos PVLANissa ei käytetä VLAN traslationia, Community VLAN vastaa normaalia VLANia. (Foschiano & HomChaudhuri 2010, 5.)



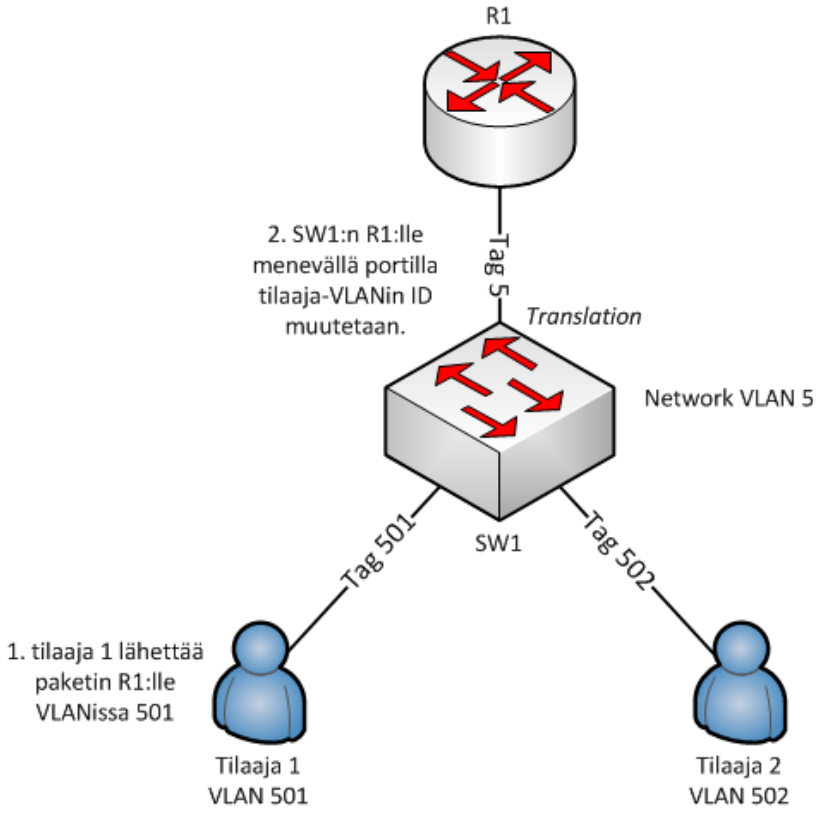
KUVIO 7. PVLAN esimerkki

TAULUKKO 1. PVLAN kommunikointi

	Isolated 1	Community 1	Community 2	Isolated 2	Primary
Isolated 1	EI	EI	EI	EI	KYLLÄ
Community 1	EI	KYLLÄ	EI	EI	KYLLÄ
Community 2	EI	EI	KYLLÄ	EI	KYLLÄ
Isolated 2	EI	EI	EI	EI	KYLLÄ
Primary	KYLLÄ	KYLLÄ	KYLLÄ	KYLLÄ	KYLLÄ

4.2 PVLAN Translation

PVLANia voidaan käyttää ilman translationia, joka on PVLAN valinnainen ominaisuus, mutta tällöin PVLANin tarjoama hyöty vähenee. Tämän takia myös translation kannattaa ottaa käyttöön. Translationissa PVLANista lähtevän liikenteen ID vaihdetaan tilaajaVLANin ID:sta Network-VLANin ID:een (Ks. kuvio 8). Tällöin verkon hallinnointi paranee ja verkko skaalautuu paremmin. (Extreme Networks 2011d, 493 - 494.)

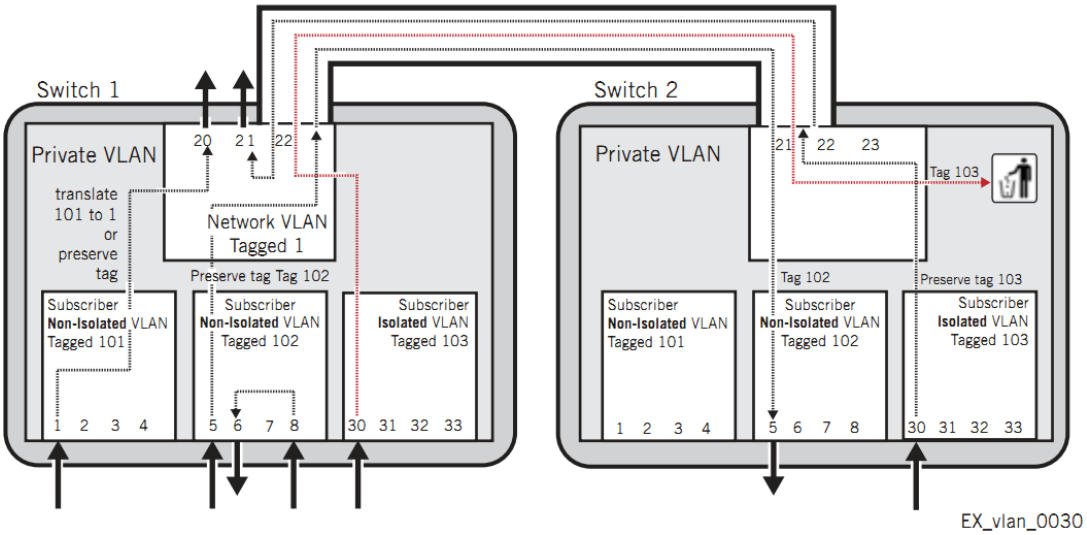


KUVIO 8. PVLAN translation

4.3 PVLAN multiswitch

PVLANia voidaan myös käyttää useammalla kytkimellä. Kuviossa 9 on PVLAN konfiguroitu kahdelle kytkimelle. Kytkinten väliset portit tulee konfiguroida Tagged-tilaan. Kun PVLAN konfiguroidaan useammalle kytkimelle, kytkimet käyttäytyvät kuin yhtenä PVLAN kytkimenä. Tilaaja VLANit (isolated ja community) toimimat samalla tavalla

kuin jos PVLAN olisi konfiguroitu yhdelle kytkimelle. Tällöin samassa community VLA-Nissa olevat päätelaitteet voivat keskustella toistensa kanssa, vaikka olisivat kytketty fyysisesti eri kytkimiin ja isolated-VLANiin kytketty päätelaite on edelleen eristetty L2-tasolla muista päätelaitteista. (Extreme Networks 2011d, 496 - 498.)



KUVIO 9. PVLAN multiswitch (Extreme Networks 2011d)

PVLAN voidaan laajentaa myös kytkimelle, joka ei tue PVLANia, mutta silloin kytkimeltä joka ei tue PVLANia jää uupumaan joitakin PVLANin toiminnallisuuksia, kuten PVLAN translation. Isolated VLANissa olevat laitteet voivat keskustella toistensa kanssa. (Extreme Networks 2011d, 498.)

4.4 PVLAN FDB-kirjaukset

Jokaisella PVLANiin liitetyllä laitteella täytyy olla uniikki MAC-osoite PVLANin sisällä. PVLANissa yhtä MAC-osoitetta kohtaan tarvitaan useampi FDB-kirjaus. Esimerkiksi Isolated-tilaajaVLANista opittu MAC-osoite merkitään kahteen FDB-kirjaukseen; yksi tilaajaVLANia varten ja yksi Network-VLANia varten. Extreme Networksin kytkimillä PVLANia varten tehdyt FDB-kirjaukset merkitään P-lipulla ja ne nähdään *show fdb*-komennolla. (Extreme Networks 2011d, 498 - 499.)

FDB-kirjausten kokonaismäärä voidaan arvioida seuraavalla kaavalla:

$$FDBtotal = [(MACnon-iso + MACiso) * 2 + (MACnetwork * (VLANnon-iso + VLANiso + 1))]$$

Kaavan muuttajat:

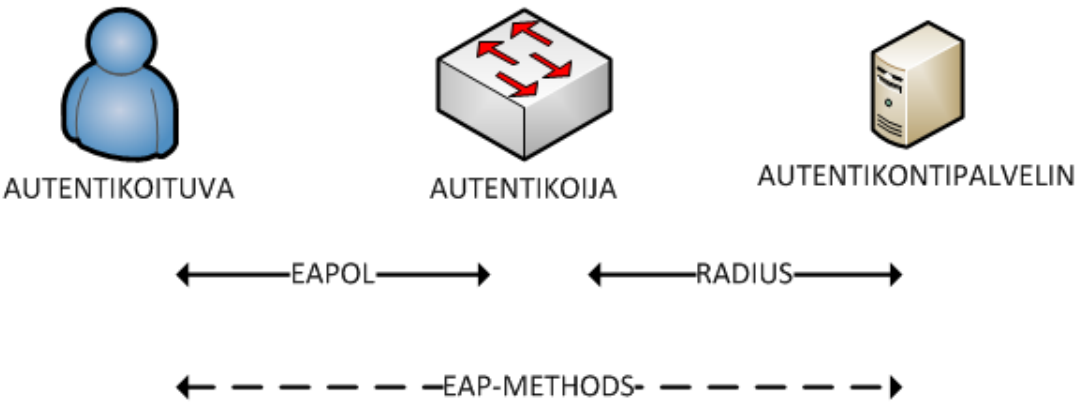
- MACnon-iso =Non-isolated tilaajaVLANista opittujen MAC-osoitteiden määrä
- MACiso = Isolated tilaajaVLANista opittujen MAC-osoitteiden määrä
- MACnetwork = NetworkVLANista opittujen MAC-osoitteiden määrä
- VLANnon-iso = Non-isolated VLANien määrä
- VLANiso = Isolated VLANien määrä

5 802.1X PORT BASED AUTHENTICATION

5.1 Yleistä

IEEE julkaisi 802.1X-standardin vuonna 2001. Standardilla haluttiin parantaa lähiverkkojen fyysistä tietoturvaa. Ennen 802.1X-standaria ei ollut tekniikkaa, jolla käyttäjä/laite pystyttiin autentikoimaan verkkoon kytkettäessä ja näin varmistamaan, ettei verkkoon pääse käyttäjiä tai laitteita, joilla ei ole verkkoon oikeuksia. 802.1X-standardi koostuu useista komponenteista, jotka ovat 802.1X, EAP, EAP-methods sekä valinnaisena Radius. (Brown 2008, 9 - 10.)

Autentikointiprosessi 802.1X-standarsissa pitää sisällään kolme osapuolta. Osapuolet ovat autentikoituva, autentikoija sekä autentikointipalvelin. Autentikoituvana autentikointiprosessissa on yleensä verkon päätelaite, esimerkiksi työasema. Autentikoijana verkossa toimii kytkin ja autentikointipalvelimena Radius-palvelin. Viestintä autentikoituvan ja autentikoijan välillä tapahtuu EAPOL-tekniikan avulla. Autentikointipalvelimen ja autentikoijan välisestä viestinnästä vastaa Radius-protokolla. Näiden lisäksi EAP-Methods muodostaa loogisen yhteyden autentikoituvan ja autentikontipalvelimen välille (Ks. kuvio 10). (Brown 2008, 20.)



KUVIO 10. 802.1X Kommunikointi

5.2 EAP

Extensible Authentication Protocol (EAP) julkaistiin IETF:n toimesta RFC 2284:ssa ja se on yksi 802.1X-standardin pääprotokollista. EAP suunniteltiin alun perin käytettäväksi Point-to-Point (PPP) protokollassa eikä sitä suunniteltu käytettäväksi IEEE 802 lähiverkoissa (Ethernet, Token Ring).

EAP-Kehysrakenne

EAP-paketti pitää sisällään Code, Identifier, Length ja Data -kentät (Ks. kuvio 11).

Code (1 tavu)	Identifier (1 tavu)	Length (2 tavu)	Data (Variable)

KUVIO 11. EAP-kehysrakenne

Yhden tavun kokoinen **Code**-kenttä identifoi EAP-pakettiluokan. EAP-pakettiluokkia on neljä: Reques (1), Response (2), Success (3) ja Failure (4).

Identifier-kenttällä voidaan yhdistää EAP-response paketti EAP-request pakettiin. Jos esimerkiksi autentikoituva vastaanottaa EAP-request paketin autentikointipalvelimelta identifier-kentän arvolla 1, niin autentikoituva vastaa tähän pakettiin EAP-response paketilla, jonka identifier-kentän arvo on myös 1.

Length-kenttä on kahden tavun kokoinen ja se ilmaisee EAP-paketin koon tavuina. Se sisällyttää arvoon koko EAP-paketin. Jos vastaanotettu EAP-paketin koko on pienempi kuin Length-kentän arvo, niin paketti hylätään.

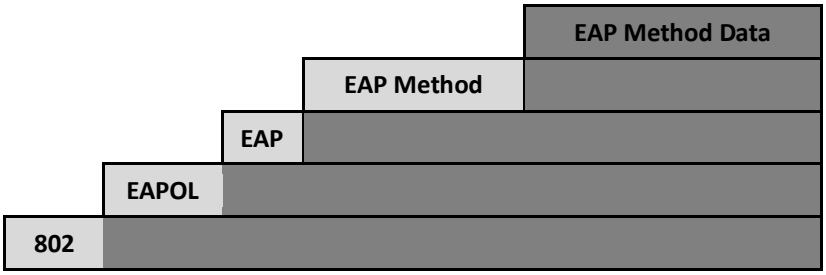
Data-kenttä pitää sisältää EAP-paketin hyötykuorman, joka on usein EAP-method paketti.

5.3 EAPoL

EAPOL-protokolla mahdollistaa EAP-protokollan käytön lähiverkoissa 802.1X-standardissa. EAPOL lisää otsikko-kentän EAP-pakettiin sekä tarjoaa uusia EAP-paketti tyyppejä. (Geier. 2008, 55.)

5.3.1 EAPOL-kapsulointi

Kuviosta 12 nähdään, että EAPOL kapsuloi sisälleen EAP-paketin ja EAP-Method paketin. Autentikoituvan ja autentikoijan välisessä liikenteessä EAPOL-paketti kapsuloidaan 802.3-pakettin. (Geier. 2008, 56.)



KUVIO 12. EAPOL-kapsulointi

5.3.2 EAPOL-kehysrakenne

EAPOL lisää kolme uutta kenttää EAP-pakettiin. EAPOL-paketti koostuu Version, Type, Length ja Body -kentistä (Ks. kuvio 13).

Version(1 tavu)	Type (1 tavu)	Length (2 tavu)	Packet Body (Variable)

Kuvio 13. EAPOL-kehysrakenne

Version-kenttä on yhden tavun kokoinen kenttä. Kenttä identifoi EAPOL-protokollan version, jota paketin lähettäjä käyttää. 802.1X-standardissa tämä kenttä saa aina arvon 0000 0002. (Geier. 2008, 57.)

Type-kenttä kertoo EAPOL-paketin luokan. Type-kenttä on yhden tavun suuruinen. EAPOL-paketin luokaksi on määritelty viisi eri luokkaa. (Geier. 2008, 58.)

Length-kenttä ilmaisee EAPOL-paketin body-kentän koon. Esimerkiksi EAPOL-Start ja EAPOL-Logoff paketeilla tämän kentän arvo on 0, koska näillä paketeilla ei ole body-kenttää. (Geier. 2008, 58.)

Body-kenttä pitää sisällään EAPOL-paketin hyötykuorman. Kenttää käytetään EAP-packet, EAPOL-key ja EAPOL-encapsulated-ASF-Alert EAPOL-paketeilla. (Geier. 2008, 59.)

5.3.3 EAPOL-pakettiluokat

EAP-Packet Type 00

EAP-Packet-luokka kuljettaa nimensä mukaisesti EAP-pakettia. Linkin muodostumisen jälkeen nämä ovat yleisimpiä EAPOL-paketteja. (Geier. 2008, 59.)

EAPOL-Start Type 01

Autentikointiprosessin aloittaa yleensä autentikoija, joka huomaan autentikoijan ja autentikoituvan välisen linkin aktivoituvan. Mutta jos linkki on esimerkiksi valmiiksi aktiivinen ja autentikoitava haluaa aloittaa autentikointiprosessiin, niin tällöin autentikoituva lähettää autentikoijalle EAPOL-start paketin. Paketin saatuaan autentikoija käynnistää autentikointiprosessin. (Geier. 2008, 59 – 60.)

EAPOL-Logoff Type 02

EAPOL-logoff paketilla autentikoituva kertoo autentikoijalle, että autentikoitu rajapinta voidaan palauttaa takaisin autentikoitumattomaan tilaan. (Geier. 2008, 60.)

EAPOL-Key Type 03

EAPOL-Key pakettiluokka on valinnainen. Sitä käytetään, kun 802.1X toteutus vaatii avaintenvaihtoa autentikoijan ja autentikoituvan välillä. (Geier Jim. 2008, 60 – 62.)

EAPOL-Encapsulated-ASF-Alert Type 04

Tätä pakettiluokkaa käytetään silloin, kun autentikoituvan täytyy lähettää tietoa suojeltuun verkkoon ennen autentikointia. Esimerkkinä SNMP-trap, jolla laite kertoo ylläpidolle hälytyksestä. (Geier Jim. 2008, 62.)

5.4 RADIUS

Radius on yleisin käytetty protokolla autentikoijan ja autentikointipalvelimen välillä 802.1X-standardissa ja siitä onkin tullut DEFACTO-standardi. Radius-protokolla esiteltiin IETF:n toimesta vuonna 2000 RFC 2865:ssä. (Geier Jim. 2008, 72.)

5.4.1 Radius-kehysrakenne

Radius-paketti koostuu Code, Identifier, Length, Autenticator ja Attributes kentistä (ks. kuvio 14). Näistä neljä ensimmäistä kenttää ovat Radius-paketin otsikkotietoja ja näiden koko on 20 tavua. Radiuspaketin maksimi koko on 4096 tavua. (Geier Jim. 2008, 72.)

Code (1 tavu)	Identifier (1 tavu)	Length (2 tavua)	Authenticator (16 tavua)	Attributes (variable)

KUVIO 14. Radius kehysrakenne

Code

Code-kenttä on yhden-tavun suuruinen. Kenttä kertoo Radius-paketin tyypin. Määritetyt tyypit näkyvät taulukossa 2.

TAULUKKO 2. Radius-pakettityypit

CODE (Decimal)	**Tyyppi**
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Identifier kenttä

Identifier-kentällä varmistetaan, että autentikoija ja autentikointipalvelin käsittelevät samaa autentikointiprosessia. Esimerkiksi jos autentikoija lähettää autentikointipalvelimelle RADIUS access-request paketin Identifier-kentän arvolla 0000 1111, niin paketissa, jolla autentikointipalvelin vastaa, on myös samaa arvo Identifier-kentässä. Myös uudelleen lähetetyissä paketeissa Identifier-kentän arvo pysyy samaa, jottei esimerkiksi autentikointipalvelin käsittele samaa pyyntöä kahdesti. (Geier. 2008, 73.)

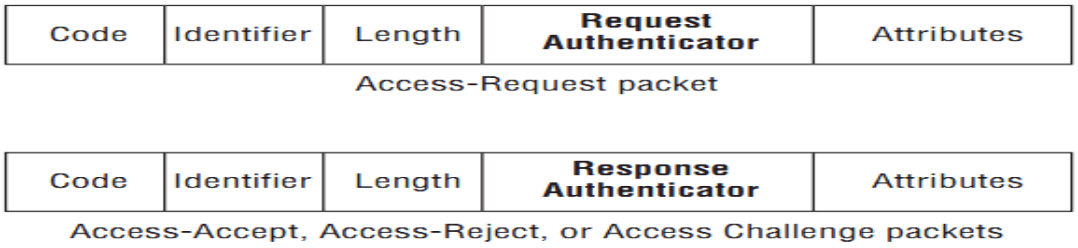
Length-Kenttä

Length-kenttä on kaksi oktettia pitkä. Kenttä kertoo Radius-paketin koon tavuina. Kentän arvo voi olla 20 – 4096. 20-tavun on Radius-paketin minimi koko ja sen vie

paketin pakolliset otsikkotiedot ja 4096 tavua on paketin maksimi koko. Length-kentän arvosta voidaan päätellä attributes-kentän koko. Esimerkiksi jos Lenght-kentän arvo on desimaaleina 1182 tavua, niin silloin saadaan tästä vähentämällä 20 tavua Attributes-kentän arvoksi 1162 tavua. Jos autentikoija tai autentikointipalvelin vastaanottaa Radius-paketin, jonka koko on pienempi kuin Length-kentän arvo, niin paketti hylätään. Jos taas paketin koko on suurempi kuin Length-kentän arvo, niin vastaanottaja hylkää ainoastaan arvoa ylittävät tavut. (Geier. 2008, 74.)

Authenticator kenttä

Authenticator kenttä on 16 tavun kokoinen ja sen sisältö riippuu Radius-paketin tyypistä (Ks. kuvio 15). Radius Access-Request paketilla tämä arvo on nimeltään Request Authenticator ja Access-Accept. Access-Reject ja Access-Challenge paketeilla Authenticator kentässä on Response Authenticator-arvo. (Geier. 2008, 74-75.)



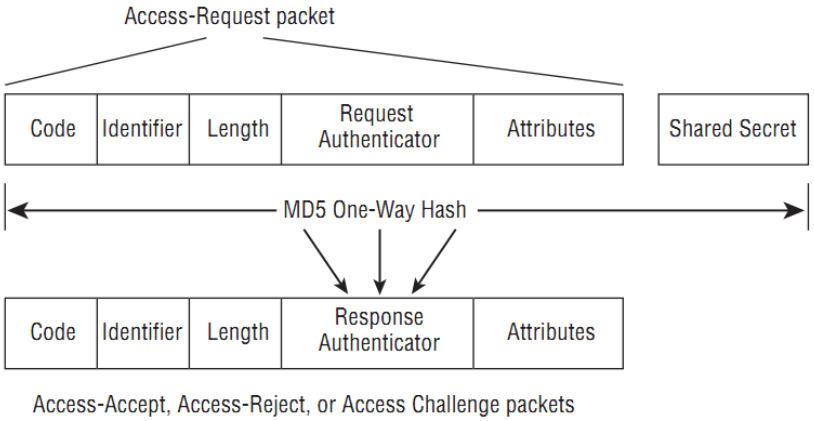
KUVIO 15. Authenticator-kenttä (Geier. 2008)

Request Authenticator

Request Authenticator -arvo tulee olla satunnainen ja uniikki. Arvo muuttuu aina silloin kun Identifier-kentän arvo muuttuu. Autentikoijan ja autentikointipalvelimen tietämällä salasanalla ja Request Authenticator -arvon avulla muodostetaan yhdensuuntainen MD5-hashi, joka on 16 tavun kokoinen. Tälle luvulle sekä käyttäjän salasanalle suoritetaan XOR-operaatio ja tämä arvo sijoitetaan User-Password attribuutiin Radius Access-Request paketissa. Näin saadaan käyttäjän salasana suojattua. (Geier. 2008, 74-75; Joshua. 2001)

Response Authenticator

Response Authenticator arvo on autentikointipalvelimen lähettämissä paketeissa. Response Authenticator arvo muodostuu saadusta Access-Request –paketista sekä autentikoijan ja autentikointipalvelimen yhteisestä salasanasta. Näille luvuille suoritetaan yhdensuuntainen MD5 ja tämä hashi sijoitetaan Authenticator-kenttään (Ks. kuvio 16) (Geier 2008, 74 – 75.)



KUVIO 16. Response Authenticator –kenttä (Geier. 2008)

Attributes-kenttä

Attributes-kenttä pitää sisällään tietoja joita tarvitaan autentikoinnissa, auktorisoinnissa autentikoijan ja autentikointipalvelimen välillä. Kuviosta 17 nähdään, että Attributes-kenttä kostuu Type, Length ja Value –kentistä. (Geier. 2008, 76.)

Type (1 tavu)	Length (1 tavu)	Value (Variable)

KUVIO 17. Attributes-kenttä

Type ja Length kentät ovat yhden tavun suuruisia. Value-kentän arvo on muuttava. Type-kenttä identivoi käytettävän attribuutin. Käytettävät attribuutit ovat arvoltaan 1- 191. Arvot 192-223 ovat koekäyttöön, 224-240 ovat varattu implementation-specific use ja 241-255 ovat varattuja eikä niitä pidä käyttää. Radius-palvelimet ovat suunniteltu niin, etteivät ne hyväksy vääriä arvoja, vaan hylkäävät paketit, joilla on tuntematon arvo Attributes-kentän type-kohdassa. Length-kenttä on kooltaan yhden tavun ja se kertoo Radius-paketin Attributes-kentän koon. Value-kenttä on kooltaan 0

tavua tai enemmän. Sen sisältö voi olla tekstiä, merkkijono, osoite, kokonaisluku tai aika. (Geier. 2008, 79 - 80.)

5.4.2 RFC 2865 määrittelemät RADIUS-pakettiluokat

Access-Request Code 1

Access-Request –paketti lähetetään Radius-palvelimelle, jonka sisältämän tiedon perusteella Radius-palvelin tekee päätöksen, onko pyytäjällä oikeutta palveluun, jota tämä pyytää, esimerkiksi verkkoon pääsyä. Access-Request –paketti pitää yleensä sisällään Autentikoijan IP-osoitteen tai identikaattorin. (RFC 2865, 16.)

Access-Accept Code 2

Jos autentikoituvalla käyttäjällä on oikeus palveluun, niin Radius-palvelin lähettää vastauksena Access-Request –pakettiin autentikoijalle Access-Accept –paketin, joka pitää sisällään tarvittavat tiedot autentikoituvan palveluun pääsemiseksi. Tämä tieto voi olla esimerkiksi VLAN, johon autentikoituva liitetään. (RFC 2865, 17 – 18.)

Access-Reject Code 3

Mikäli jokin Access-Request-paketin sisältämistä attribuuteista on virheellinen, niin silloin Radius-palvelin vastaa autentikoijalle Access-Reject-paketilla. (RFC 2865, 19.)

Access-Challenge Code 11

Access-Challenge –pakettia käytetään silloin, kun Radius-palvelin haluaa lisätietoja autentikoituvalta Access-Request-paketin jälkeen. Jos autentikoija ei tue Access-Challenge pakettia, niin silloin autentikoija käsittelee paketin Access-Reject –pakettina. (RFC 2865, 20 – 21.)

5.5 EAP-METHODS

EAP-Methods on tekniikka, jolla luodaan looginen yhteys autentikointipalvelimen ja autentikoituvan välille. 802.1X-standardissa EAP-Methods vastaa autentikointiproses-

sista, kun taas EAPOL ja Radius vastaavat EAP-Methods datan kuljettamisesta autentikointi osapuolien välillä. (Geier. 2008, 93.)

Kehysrakenne

EAP-Methods paketeilla kehysrakenne koostuu Type ja EAP-Method-Data kentistä (Ks. kuvio 18).

Type (1 tavu)	EAP Method Data (Variable)

KUVIO 18. EAP-Methods kehysrakenne

Type-kenttä on yhden tavun kokoinen. Type-kentän arvo kertoo EAP-paketin luokan. Alun perin rfc3748 määritti taulukon 3 EAP-Method luokat. (Geier. 2008, 95 - 96.)

TAULUKKO 3. EAP-Method luokat

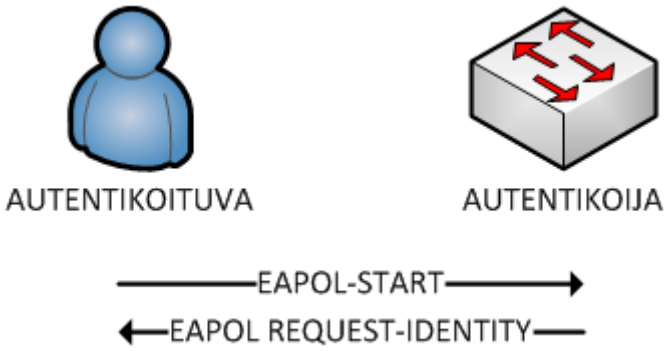
Identity	Type 1
Notification	Type 2
Legacy NAK	Type 3
MD5-Challenge	Type 4
One-Time Password	Type 5
Generic Token Card	Type 6
Expanded Types	Type 254
Experimental Use	Type 255

EAP-Method-Data-kenttä sisältää tietoa, jota kyseinen pakettiluokka tarvitsee. Kenttä voi sisältää esimerkiksi autentikoituvan tietoja, jotka ovat menossa autentikointipalvelimelle. (Geier. 2008, 96.)

5.6 802.1X TOIMINTA

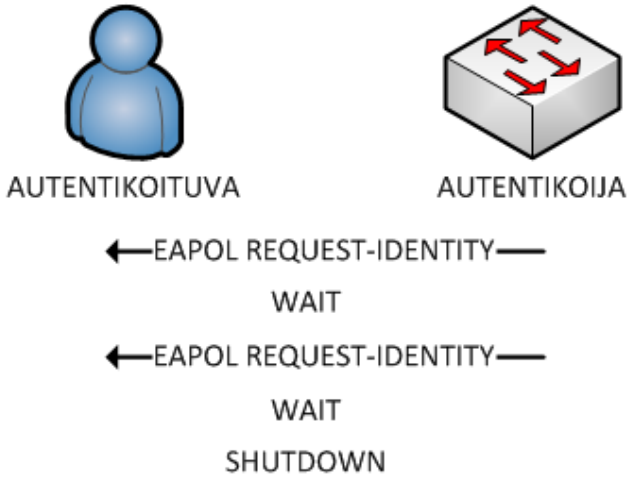
802.1X prosessi käynnistyy, kun autentikoijan ja autentikoituvan välinen linkki aktivoituu. Linkin aktivoituessa autentikoija aloittaa keskustelun autentikoituvan kanssa lä-

hettämällä tälle EAPOL Request Identity-paketin, jonka jälkeen autentikoituva jää odottamaan vastausta. Jos jostain syystä autentikoija ei lähetä EAPOL Request-Identity-pakettia autentikoituvalle, voi autentikoituva käynnistää prosessin lähettämällä autentikoijalle EAPOL-Start-paketin (Ks. Kuvio 19). (Brown. 2008, 22 - 23.)



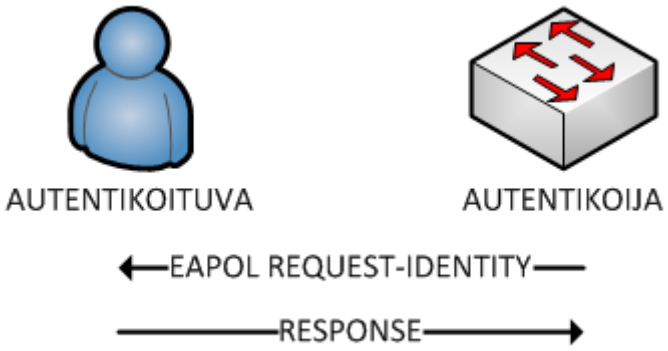
KUVIO 19. 802.1X käynnistys

Kun autentikoija on lähettänyt autentikoituvalle EAPOL request-identity –paketin, jää se odottamaan vastausta. Jos autentikoija ei saa vastausta autentikoituvalta, lähettää se paketin uudelleen määritetyn X kertaa, jonka jälkeen se sulkeen portin (Ks. Kuvio 20). Tähän syynä voi olla esimerkiksi se, että autentikoituva ei tue 802.1X –standardia tai esimerkiksi verkkokaapeli on rikki. (Brown. 2008, 23.)



KUVIO 20. EAPOL request-identity

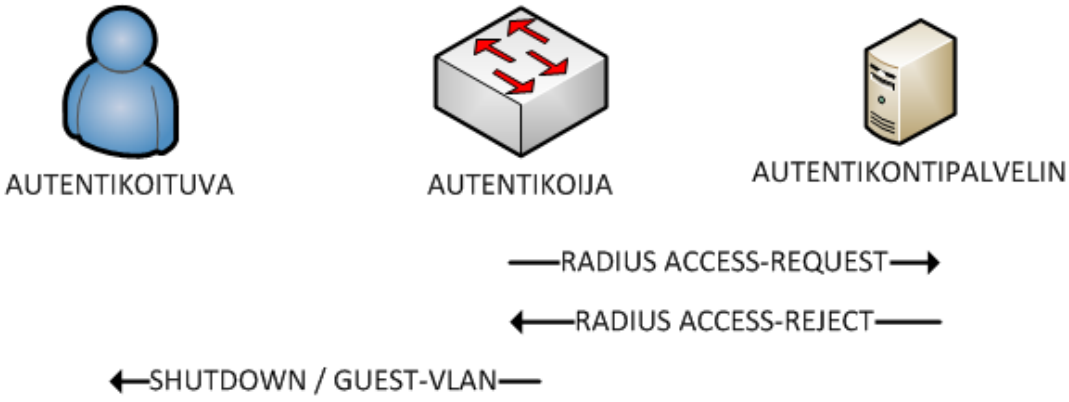
Jos 802.1X toimii linkkivälillä oikein, niin autentikoituva saa autentikoijan lähettämän paketin ja tällöin vastaa siihen. Autentikoituva lähettää tiedot identiteetistään EAPOL-paketin data-osassa. Tässä vaiheessa autentikoituva ei lähetä salasanaansa (Ks. Kuvio 21). (Brown. 2008, 24.)



KUVIO 21. Vastaus

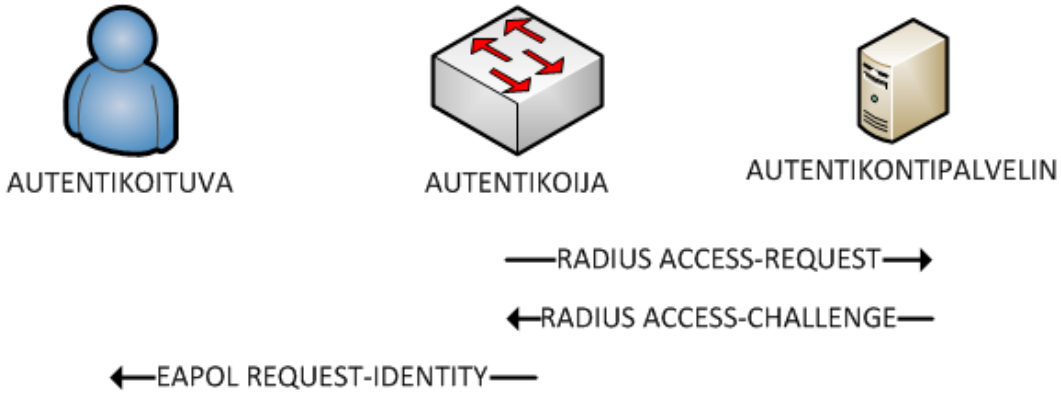
Kun autentikoija on saanut autentikoituvalta vastauksen, lähettää autentikoija Radius access-request –paketin autentikointipalvelimelle. Jotta autentikoija voi lähettää autentikointipalvelimelle viestin, on siihen konfiguroitava autentikointipalvelimen osoite sekä autentikointipalvelimen kanssa yhteinen salasana. Access-request-paketti pitää sisällään autentikoijan tiedot, joiden perusteella autentikointipalvelin päättää hyväksyykö se yhteyden.. Kieltäytyessä autentikointipalvelin lähettää Access-Reject-paketin autentikoijalle. Tällöin autentikoija voi yrittää yhteyttä toiseen autentikointipalveli-

meen, jos sellainen on määritetty. Muutoin sen täytyy olettaa, ettei autentikoituvaa ole autentikoitu ja estää autentikoituvan pääsyn verkkoon tai antaa sille pääsy Guest-VLANiin (Ks. kuvio 22). (Brown. 2008, 28.)



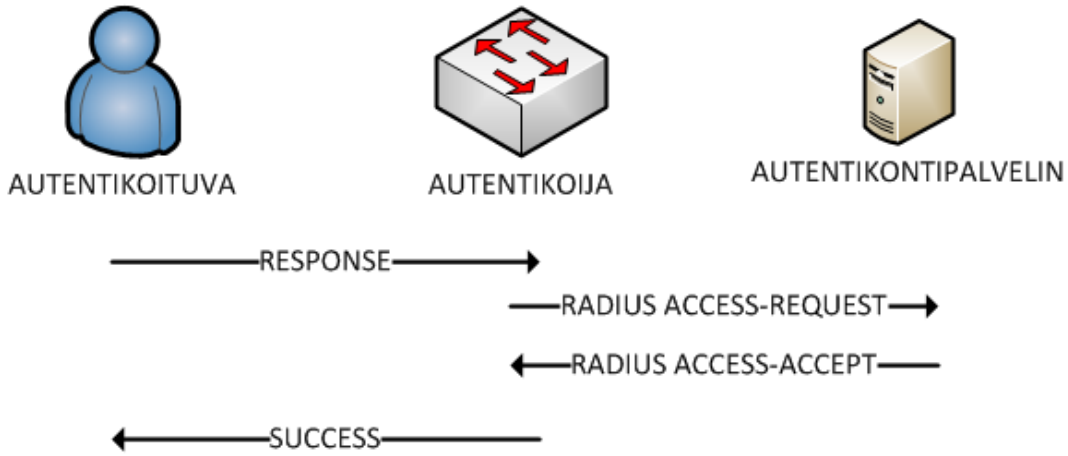
KUVIO 22. Access-Reject

Autentikointipalvelimen hyväksyessä autentikoijan lähettämän pyynnön, vastaa autentikointipalvelin Access-challenge-paketilla, joka on tarkoitettu autentikoituvalle (Ks. Kuvio 23). Tässä vaiheessa autentikoija toimii välikätenä ja välittää autentikointipalvelimen lähettämän viestin autentikoituvalle. (Brown. 2008, 31 - 32.)



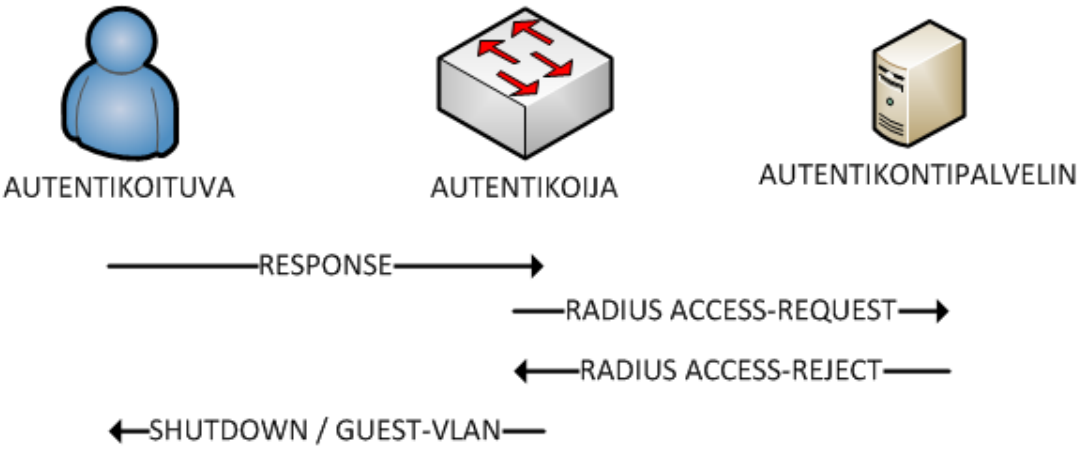
KUVIO 23. Access-Challenge

Autentikointipalvelimen pyynnön saatuaan autentikoituva lähettää vastauksen, jonka autentikoija välittää autentikointipalvelimelle. Vastaus sisältää autentikoituvan tiedot mukaan lukien autentikoituvan salasanan. Näiden tietojen perusteella autentikointipalvelin tekee päätöksen, onko autentikoituvalla oikeudet verkkoon. Jos autentikoituvalla on oikeudet verkkoon, vastaa autentikointipalvelin Access-Accept-paketilla ja autentikoituva saa pääsyn verkkoon (Ks. kuvio 24). Vastaus voi myös sisältää esimerkiksi VLANin, johon autentikoitava liitetään. (Brown 2008, 33 - 34.)



KUVIO 24. Access-Accept

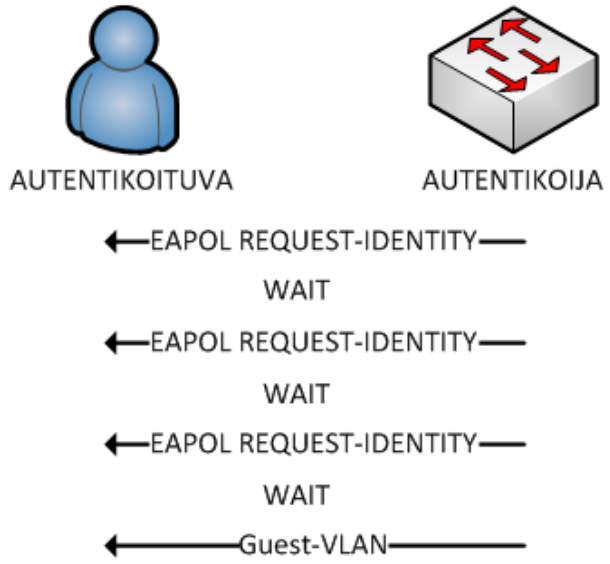
Jos autentikoituvalla ei ole oikeuksia, autentikointipalvelin lähettää Access-reject –paketin. Tällöin autentikoituva ei pääse verkkoon ja linkki joko suljetaan tai autentikoituva siirretään Guest-VLANiin (Ks. kuvio 25). (Brown 2008, 33.)



KUVIO 25. Access-Reject

5.7 GUEST-VLAN

Guest-VLAN on kehitetty tarjoamaan verkkoon pääsyn asiakkaille, jotka eivät tue 802.1X autentikointia tai ovat vierailijoita verkossa, sekä joissakin tapauksissa niille joiden 802.1X autentikointi epäonnistuu. Guest-VLANille annetaan rajoitettu pääsy verkkoon (yleensä internetiin pääsy), jolloin siitä ei ole haittaa muulle verkolle. Oletuksena Extreme Networksin kytkimillä autentikoituva sijoitetaan Guest-VLANiin kolmen autentikointipyynnön jälkeen (Ks. Kuvio 26).



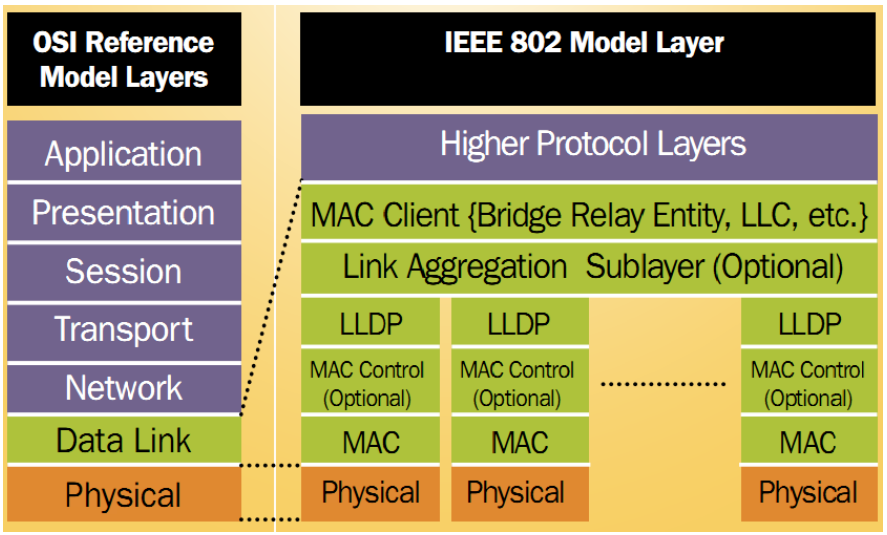
KUVIO 26. Guest-VLAN

6 LINK LAYER DISCOVERY PROTOCOL (LLDP)

6.1 Yleistä

LLDP on määritetty IEEE:n 802.1ab-standardissa. LLDP on avoin protokolla laitteiden ja niiden ominaisuuksien löytämiseen ja mainostamiseen IEEE:n 802 lähiverkossa. LLDP mahdollistaa IEEE 802 lähiverkkolaitteen mainostaa sen ominaisuuksia ja tilaansa naapurilaitteille. LLDP on riippumaton mediasta ja se on tarkoitettu toimimaan kaikissa IEEE 802 laitteissa, kuten WLAN-tukiasemissa, IP-puhelimissa, kytkimissä ja reitittimissä.

LLDP on L2-tason protokolla, joten se toimii OSI-mallin siirtokerroksella. L2-kerroksen sisällä LLDP toimii MAC-kerroksen päällä (Ks. Kuvio 27). LLDP on yhdensuuntainen protokolla. Se pystyy lähettämään ja vastaanottamaan tietoja naapurilaitteilta, mutta se ei pysty hakemaan tietoja naapurilaitteilta eikä protokolla mahdollista varmistusta tiedon vastaanottamisesta. (Extreme Networks, 2006)



KUVIO 27. LLDP

LLDP:n avulla vian selvitystä voidaan parantaa muun muassa verkoissa joissa on useamman valmistajan laitteita, koska LLDP-protokollan avulla verkonhallintatyökalut pystyvät luomaan tarkan kuvan verkosta ja sen tilasta.

6.2 Kehysrakenne

LLDP:n kehysrakenne koostuu Destination Multicast-osoitteesta, Source MAC-osoitteesta, Ethertypestä, LLDPDU datasta sekä Frame Check Sequencestä (FCS).

LLDP Multicast Address (6 tavua)	Source MAC Address (6 tavua)	Ethertype 88-CC (2 tavua)	LLDPDU (1500 tavua)	FCS (4 tavua)

KUVIO 28. LLDP kehysrakenne

LLDP Multicast Address –kentässä käytetään ryhmä MAC-osoitteita, jotka ovat 01-80-C2-00-00-0E, 01-80-C1-00-00-03 ja 01-80-C2-00-00-00.

Source MAC Address –kenttään tulee lähtevän portin MAC-osoite.

Ethertype-kenttä saa aina arvon 88-CC.

Link Layer Discovery Protocol Data Unit (LLDPDU) –kenttä pitää sisällään aina neljä pakollista TLV-kenttää (Type, Length and value fields). TLV:t koostuu kolmesta kentästä, jotka ovat Type, Length ja Value. TLV-kentissä Type-kenttä identivoi lähetettävän tiedon, Length-kenttä ilmoittaa paketin koon tavuina ja Value-kenttä pitää sisällään tiedon, joka lähetetään. Tämä voi olla esimerkiksi laitteen nimi. LLDPDU-kentän neljä pakollista TLV:tä on:

- Chassis ID TLV
- Port ID TLV
- Time To Live TLV
- End of LLDPDU TLV

6.3 TLV:t

TLV:t määrittävät mitä tietoja LLDP mainostaa naapurilaitteille. Pakollisten TLV:eiden lisäksi on IEEE määrittänyt 802.1AB-standardissa kolme valinnaista TLV-ryhmää. Ryhmät ovat Basic management TLV-ryhmä, IEEE 802.1 Organizationally Specific TLV-ryhmä ja IEEE 802.3 Organizationally Specific TLV-ryhmä. Näiden ryhmien lisäksi Telecommunication Industry Association (TIA) on kehittänyt ja standardisoinnut LLDP-MED TLV-ryhmän. LLDP-MED on kehitetty tuomaan parannusta päätelaitteiden konfiguroimiseen kuten VoIP-puhelinten liittämiseen verkkoon. Nämä neljä ryhmää pitää sisällään seuraavat TLV:t. (IEEE 802.1AB, 2009.)

- Basic Management TLV -ryhmä
    - Port Description TLV
    - System Name TLV
    - System Description TLV
    - System Capabilities TLV
    - Management Address TLV
- IEEE 802.1 Organizationally Specific TLV -ryhmä
    - Port VLAN ID TLV
    - Port And Protocol VLAN ID TLV
    - VLAN Name TLV
    - Protocol Identity TLV
    - VID Usage Digest TLV
    - Management VID TLV
    - Link Aggregation TLV
- IEEE 802.3 Organizationally Specific TLV –ryhmä
    - MAC/PHY Configuration/Status TLV
    - Power Via MDI TLV
    - Link Aggregation TLV
    - Maximum Frame Size TLV
- LLDP-MED TLV-ryhmä
    - LLDP-MED capabilities TLV

- Network policy TLV
- Power management TLV
- Inventory management TLV
- Location TLV

7 TIETOTURVAOMINAISUUDET

7.1 MAC Security

Kytkin tallentaa kaikki oppimansa MAC-osoitteet FIB-tauluun (Forwarding Database), jonka perusteella se kytkee tai tiputtaa paketin. MAC-Securityllä voidaan hallita osoitteiden oppimista FIB-tauluun. Tällä tavoin voidaan parantaa tietoturvaa ja vähentää esimerkiksi MAC-flood hyökkäyksen vaaraa, jossa hyökkääjä lähettää satunnaisia MAC-osoitteita kytkimelle ja täyttää FIB-taulun. Kun FIB-taulu tulee täyteen, kytkin ei voi oppia enää uusia MAC-osoitteita. Tällöin kytkin alkaa toimia hubina, jolloin kaikki verkossa kulkeva liikenne ohjataan kytkimen kaikkiin rajapintoihin ja näin hyökkääjä pääsee näkemään verkon liikenteen. Extreme Networksin kytkimillä MAC-Securityllä voidaan hallita seuraavia asioita (Extreme Networks, 2011d, 821 – 824.):

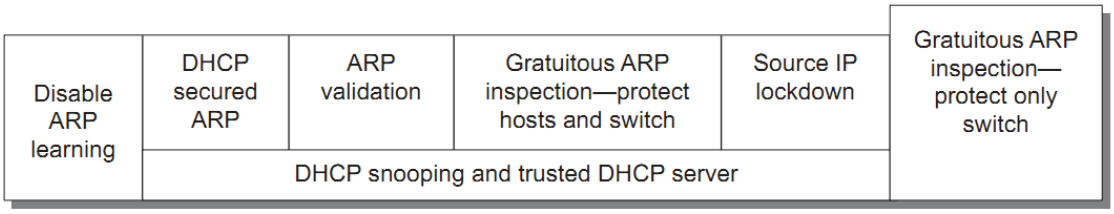
- Dynaamisesti opittujen MAC-osoitteiden määrä per rajapinta,
- Lukita MAC-osoite rajapintaan, jonka jälkeen uusia MAC-osoitteita ei opita,
- Asettaa aika kuinka kauan opittuja MAC-osoitteita säilytettään FIB-taulussa.

7.2 IP Security

Extreme Networksin kytkimillä IP Security käsittää seuraavat ominaisuudet:

- DHCP Snooping and Trusted DHCP Server
- Source IP Lockdown
- ARP Learning
- Gratuitous ARP Protection
- ARP Validation

Kuviosta 29 nähdään ominaisuuksien keskinäiset riippuvuudet. Kuvassa ylempänä olevaa ominaisuutta varten on konfiguroitava alempi ominaisuus. IP Securityä konfiguroitaessa on myös muistettava, että Extreme Networksin kytkimissä ei samalle portille voi konfiguroida Network Loginia ja IP Securityä. (Extreme Networks, 2011d, 831 – 832.)



KUVIO 29: IP Securityn ominaisuuksien riippuvuudet

7.2.1 DHCP Snooping and Trusted DHCP Server

Suurin osa verkkoon kytketyistä päätelaitteista saa IP-osoitteensa DHCP-palvelimelta. Kun päätelaite liittyy verkkoon, lähettää se DHCP-pyynnön, jolla se pyytää itselleen IP-osoitetta. Tämä pyyntö lähetetään verkkoon yleislähetyksenä, jolloin se näkyy kaikille verkossa oleville laitteille. Normaalisti tähän pyyntöön vastaa ainoastaan verkon DHCP-palvelin, joka lähettää päätelaitteelle DHCP-vastauksen, joka pitää sisällään IP-osoitteen, aliverkonpeitteen ja oletusyhdyskäytävän päätelaitteelle. Mikään ei kuitenkaan estä sitä, että jokin muu laite vastaisi tähän pyyntöön DHCP-palvelimen lisäksi. Tämä laite voi kuulua esimerkiksi hyökkääjälle, joka haluaa tarkkailla verkon liikennettä. Lähettämällä päätelaitteelle DHCP-vastauksen, jossa oletusyhdyskäytävä on esimerkiksi hyökkääjän IP-osoite, saa hyökkääjä kaiken päätelaitteelta tulevan liikenteen kulkemaan hyökkääjän kautta. DHCP Snooping ja luotettu DHCP-palvelin (Trusted DCHP Server) –ominaisuudet Extreme Networksin kytkimissä minimoi tämänkaltaisen hyökkäyksen mahdollisuuden.

DHCP Snoopingilla voidaan suodattaa epäluotettavasta lähteestä tulevia DHCP-paketteja. Tämä tapahtuu asettamalla kytkimen rajapinta joko luotettavaksi tai epäluotettavaksi. Jos kytkin vastaanottaa DHCP-vastauksen portilla, joka on määritetty epäluotettavaksi, kytkin hylkää paketin. Tämä rajapinta voidaan myös sulkea määritetyksi ajaksi tai DHCP-vastauksen lähettäjän MAC-osoite voidaan estää. DHCP-vastaukset, jotka tulevat luotetulle portille, välitetään normaalista. Extreme Networksin kytkimille voidaan määrittää myös luotettu DHCP-palvelin, jolloin luotettuja rajapintoja ei tarvitse määrittää. Kun luotettu DHCP-palvelin on määritetty kytkimelle, niin kytkin sallii ainoastaan DHCP-vastaukset luotetuilta DHCP-palvelimilta. Kytkimiin voidaan määrittää enintään kahdeksan luotettua DHCP-palvelinta. Jos DHCP-

palvelimen lisäksi määritetään luotettu rajapinta, hyväksyy kytkin kaikki DHCP-vastaukset myös luotetulta portilta. (Extreme Networks, 2011d, 832 – 835.)

7.2.2 DHCP Secured ARP

Ethernet-verkoissa IP-osoitetta vastaava MAC-osoite selvitetään ARP-protokollalla. Kun kytkin haluaa kommunikoida toisen lähiverkossa olevan laitteen kanssa, täytyy kytkimen tietää vastapuolen IP-osoitetta vastaava MAC-osoite. Selvittääkseen MAC-osoitteen lähettää kytkin ARP-kyselyn yleislähetyksenä, johon kyseisen IP-osoitteen omaava laite vastaa omalla MAC-osoitteellaan. Vastauksen saatuaan kytkin tallentaa IP-osoitteen ja MAC-osoitteen ARP-taulukkoon.

DHCP Secured ARP –ominaisuus käyttää DHCP Snooping –ominaisuuden kytkimelle rakentamaa DHCP-bindings –tietokantaa, joka pitää sisällään IP-osoitteen, MAC-osoitteen, VLAN ID:n ja portin. ARP-tauluun lisätään MAC-osoite ainoastaan silloin kun DHCP-palvelin jakaa päätelaitteelle IP-osoitteen ja tämä lisäys säilyy niin kauan kunnes DHCP-palvelin jakaa uuden osoitteen tai päätelaite lähettää DHCP RELEASE, NAK tai DECLINE viestin. (Extreme Networks, 2011d, 840 - 842.)

7.2.3 Source IP lockdown

Source IP lockdown –ominaisuus sallii ainoastaan portista liikenteen, joka on lähtöisin luotetulta DHCP-palvelimelta saadusta osoitteesta. Source IP Lockdown –ominaisuus käyttää DHCP Snoopingin luomaa DHCP-bindings –tietokantaa luodakseen portille pääsylistan, joka sallii ainoastaan DHCP-bindings –tietokannassa portille liitetyn osoitteen. Kaikki muu liikenne hylätään. Source IP Lockdown –ominaisuudella voidaan puolustautua hyökkäyksiltä, joissa hyökkääjä käyttää staattista IP-osoitetta tai joissa käytettään satunnaisia IP-osoitteita. (Extreme Networks, 2011d, 839 - 840.)

Kun Source IP lockdown –ominaisuus otetaan portille käyttöön, kytkin luo portille kaksi pääsylistaa, joista ensimmäinen estää kaiken ja toinen sallii DHCP-liikenteen portilla. Kun rajapintaan liitetty päätelaite saa IP-osoitteen luotetulta DHCP-palvelimelta, niin tällöin kytkin luo uuden pääsylista DHCP-bindings –tietokannan perustella, jossa se sallii liikenteen tästä ks. IP-osoitteesta. Kuviosta 30 nähdään Source IP lockdownin luomat pääsylistat. (Extreme Networks, 2011d, 839.)

ACL Name	Match Condition	Action	When Applied	Comments
esSrcIpLockdown_<portIfIndex>_<source IP in hex>	Source IP	Permit	Runtime	Multiple ACLs of this type can be applied, one for each permitted client.
esSrcIpLockdown_<portIfIndex>_1	Proto UDP, Dest Port 67	Permit	Configuration time	
esSrcIpLockdown_<portIfIndex>_2	Proto UDP, Dest Port 68	Permit	Configuration time	
esSrcIpLockdown_<portIfIndex>_3	Ethertype ARP	Permit	Configuration time	
esSrcIpLockdown_<portIfIndex>_4	All	Deny + count	Configuration time	

KUVIO 30. Source IP Lockdown ACLs (Extreme Networks, 2011d.)

7.2.4 Gratuitous ARP

Extreme Networksin kytkimien Gratuitous ARP –ominaisuudella voidaan turvata, ettei-vät verkonpäätelaitteet liitä väärää MAC-osoitetta kytkimen IP-osoitteelle. Tavallisesti Gratuitous ARPia käytetään ilmoittautumaan, että IP-osoite on siirtynyt toiseen rajapintaan tai sillä voidaan etsiä verkosta duplikaatti IP-osoite. Gratuitous ARPia voidaan käyttää myös man-in-the-middle –hyökkäyksiin, jolloin hyökkääjä lähettää verkkoon gratuitous ARP-paketin, jossa se kertoo esimerkiksi olevansa verkon oletusyhdyskäytävä. Tällöin verkon päätelaite poistaa vanhan oletusyhdyskäytävän IP-osoitteeseen liitetyn MAC-osoitteen ARP-taulustaan ja korvaa tämän hyökkääjän MAC-osoitteella. Tämän jälkeen oletusyhdyskäytävään kulkeva liikenne kulkee hyökkääjän kautta. (Extreme Networks, 2011d, 842 - 843.)

Kun kytkimelle on konfiguroitu Gratuitous ARP-ominaisuus päälle ja kytkin vastaanottaa gratuitous ARP-paketin, jossa on kytkimen oma IP-osoite, kytkin lähettää oman gratuitous ARP-paketin verkkoon ja kumoaa hyökkääjän gratuitous ARP-paketin. (Extreme Networks, 2011d, 844.)

8 ACCESS CONTROL LISTS & CLEAR-FLOW

8.1 Access Control Lists (ACLs)

Pääsylistoja (ACL) käytetään yksinkertaiseen pakettisuodatukseen kytkimissä ja reitittimissä. Pääsylistoilla voidaan esimerkiksi estää sisääntuleva liikenne sen kohde MAC-osoitteen perusteella. Tämän lisäksi pääsylistalla voidaan suorittaa valinnaisia toimintoja kuten pakettilaskentaa ja liikenteen peilausta. Pääsylista voidaan asettaa joko rajapinnalle tai tietylle VLANille. Extreme Networksin kytkimillä ainoastaan osa sisääntulevan liikenteen suodatusehdoista on käytössä lähtevälle liikenteelle. Esimerkiksi kohde MAC-osoitteen voi asentaa ehdoksi ainoastaan sisääntulevalle liikenteelle. ExtremeXOS eroaa monista muista valmistamien käyttöjärjestelmistä siten, että ExtremeXOS:ssa kaiken estävä sääntö estää sananmukaisesti kaiken liikenteen eikä salli esimerkiksi OSPF-päivityksiä, kuten esimerkiksi Cisco Systemsin IOS-laitteilla. (Extreme Networks, 2011d, 617 - 618.)

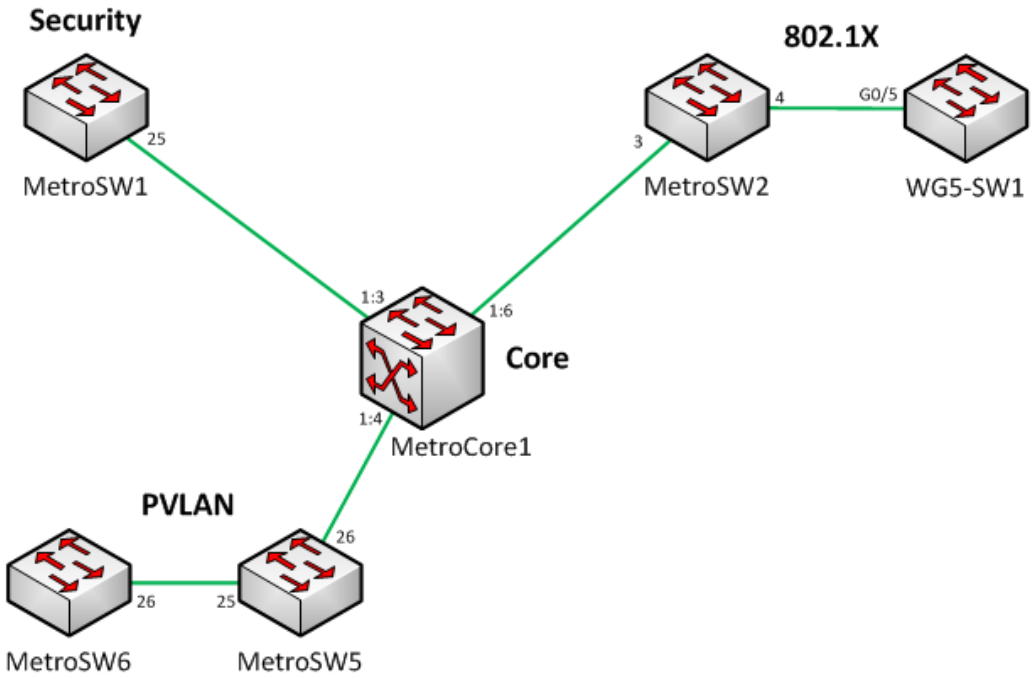
8.2 CLEAR-Flow

Extreme Networksin CLEAR-Flow on laajennus pääsylistoihin. CLEAR-Flow:lla voidaan pääsylistan ehtoihin sopiva liikenne ottaa tarkempaan tarkasteluun. CLEAR-Flow:n avulla voidaan verkon liikennettä monitoroida ja analysoida sekä siihen pystytään reagoimaan. CLEAR-Flow tarkkailee pääsylistaan tehtyä laskuria ja tekee tämän laskurin pohjalta konfiguroidut toiminnot, joita voi olla esimerkiksi liikenteen tiputtaminen alempaan QoS-luokkaan tai CLI-komennon suorittaminen. CLEAR-Flow:lla voidaan tarkkailla yhtä aikaa myös useampaan laskuria ja tehdä päätökset esimerkiksi näiden laskurien suhteiden perusteella. (Extreme Networks, 2011d, 903 - 906.)

9 TOTEUTUS

9.1 Topologia

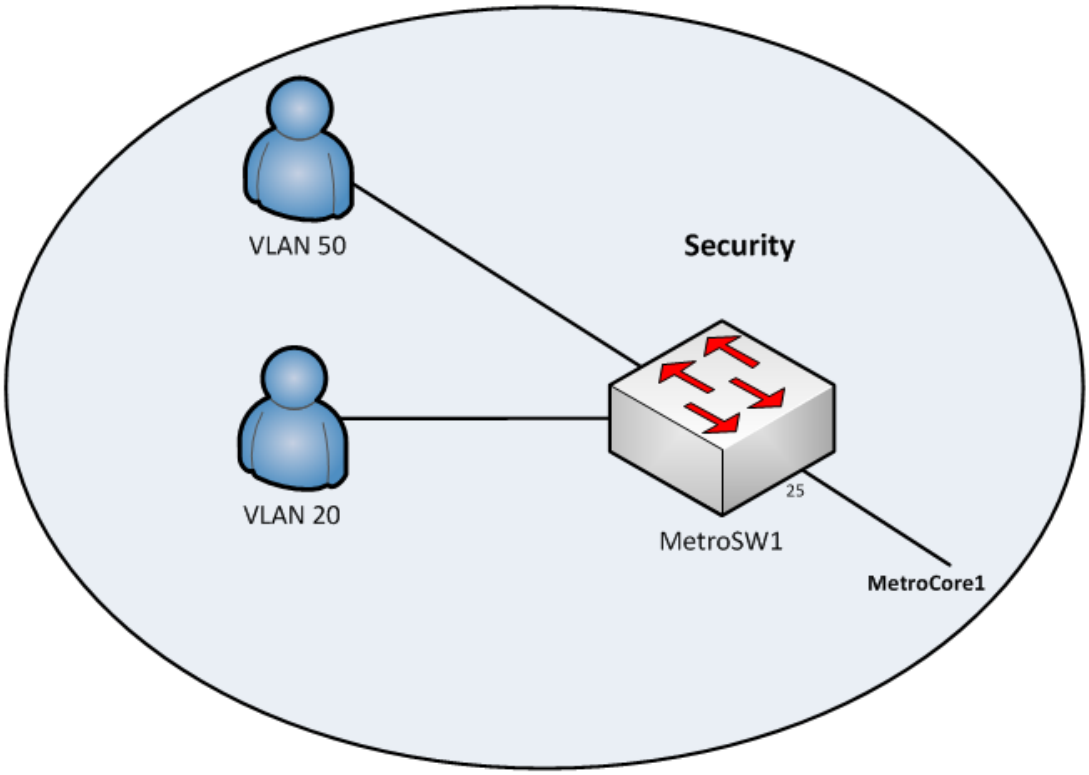
Työssä käytettävä topologia koostuu SpiderNetin Metro Coren kytkimistä sekä yhdestä WG5-työryhmän kytkimestä (Ks. kuvio 31). Työn suunnitelman mukaisesti eri tietoturvatekniikoille annettiin oma osa verkosta, koska kaikkia tekniikoita ei voida käyttää samanaikaisesti käytettävissä kytkimissä. Verkon osat nimettiin käytettävien tekniikoiden mukaisesti: Security, 802.1X, PVLAN ja Core.



KUVIO 31. Topologia

9.1.1 Security-osa

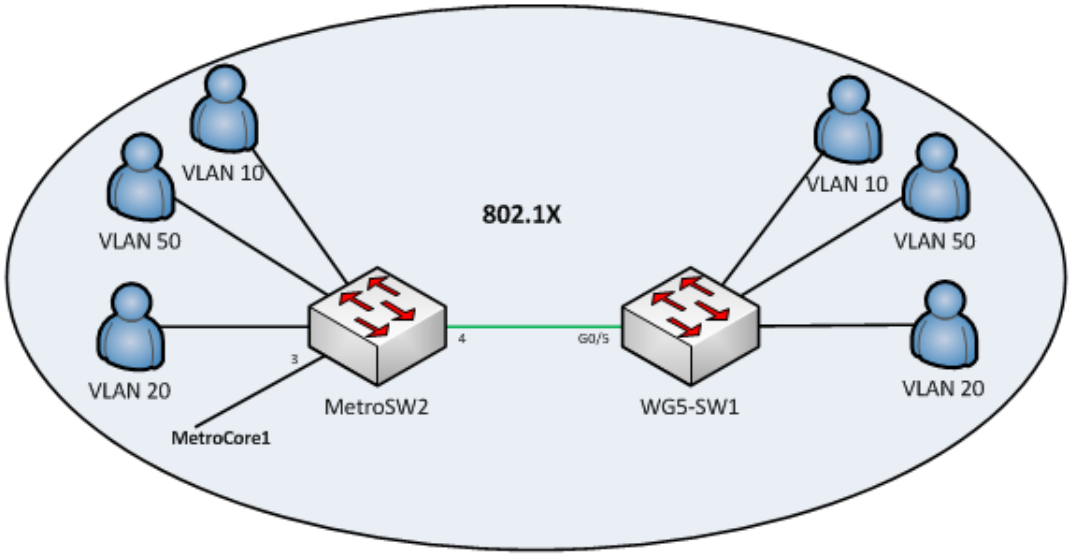
Security osassa todennettiin IP-security sekä Mac-security ominaisuuksia. Security osan MetroSW1-kytkin liitettiin muuhun verkkoon MetroCore1-kytkimen kautta. Tämän lisäksi MetroSW1-kytkimeen liitettiin kaksi tietokonetta, jotka mallinsivat loppukäyttäjien tietokoneita (Ks. kuvio 32).



KUVIO 32. Security-osa

9.1.2 802.1X-osa

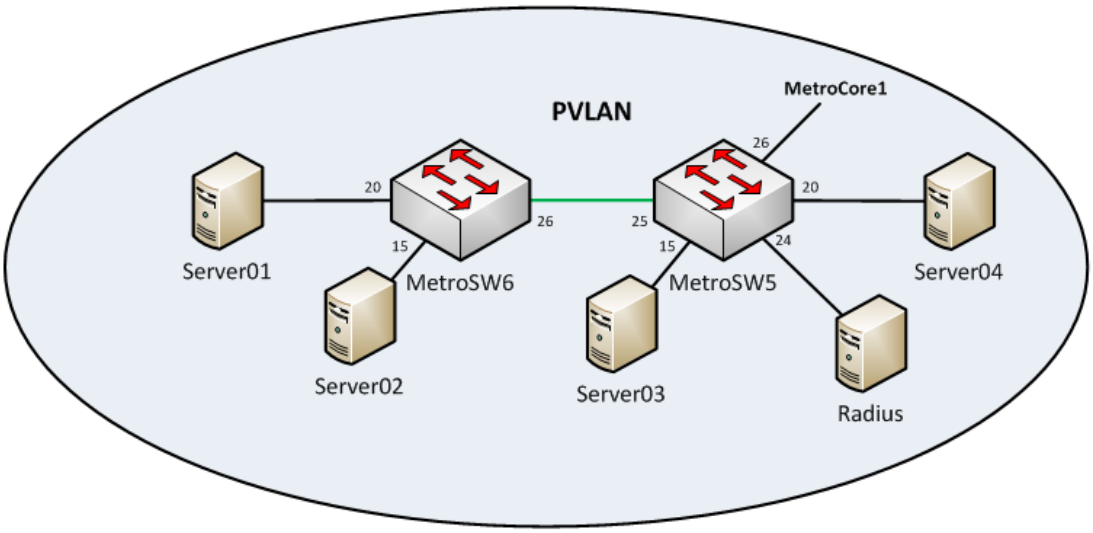
Kuviosta 33 nähdään, että 802.1X-osa koostuu MetroSW2 ja WG5-SW1 kytkimistä. Näillä kytkimille testattiin 802.1X toimintaa. MetroSW2 on liitetty MetroCore1-kytkimeen. 802.1X-osan kytkimillä on kolme VLANia, jotka määräytyvät päätelaitteille Radius-palvelimelta saatujen oikeuksien perusteella.



KUVIO 33. 802.1X-osa

9.1.3 PVLAN-osa

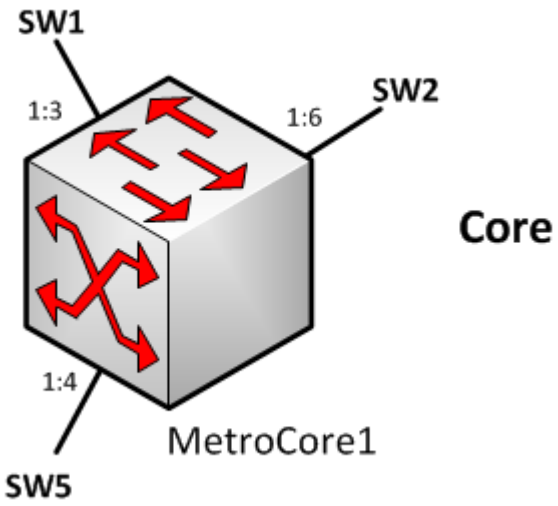
PVLAN-osassa sijaitsi verkon palvelimet ja tässä osassa käytettiin PVLANia tietoturvan parantamiseksi. PVLAN-osaan kuuluu MetroSW5 ja MetroSW6 kytkimet, joihin molempiin liitettiin kaksi palvelinta (Ks. kuvio34). Näiden palvelimien lisäksi MetroSW5-kytkimeen liitettiin myös Radius-palvelin. Yhteys muuhun verkkoon tapahtuu MetroSW5 ja MetroCore1 välisellä linkillä.



KUVIO 34. PVLAN-osa

9.1.4 Core

Core-osan muodostaa MetroCore1-kytkin, joka yhdistää muut verkon osat toisiinsa. Tässä osassa todennettiin ACL sekä ClearFlow-tekniikoita. MetroCore1:llä sijaitsee myös verkon DHCP-palvelin, jolla jaetaan IP-osoitteet 802.1X ja Security osissa sijaitseville päätelaitteille.



KUVIO 35. Core-osa

9.2 IP-Osoitteet ja VLANit

Työssä jokaiselle kytkimelle luotiin ”hallinta”-niminen VLAN jonka ID:ksi annettiin 99. Tämän lisäksi ”hallinta”-VLANille konfiguroitiin IP-osoitteet. IP-osoitteet annettiin 192.168.99.0/24 aliverkosta. Kytkimille luotiin myös tilaajaVLANit, joihin verkon päätelaitteet sijoittuvat. MetroCore1-kytkimelle konfiguroitiin myös näille VLANeille IP-osoitteet, jotka toimivat tilaajaVLANeille oletusyhdyskäytävinä (Ks. Taulukko 4).

TAULUKKO 4. VLANit

Laite	VLAN	ID	IP-osoite
MetroCore1	Vieraat	10	192.168.10.1/24
	Tuotanto	20	192.168.20.1/24
	Henkilosto	50	192.168.50.1/24
	Servernetwork	60	192.168.60.1/24
	Hallinta	99	192.168.99.1/24
MetroSW1	Tuotanto	20	
	Henkilosto	50	
	Hallinta	99	192.168.99.11/24
MetroSW2	Vieraat	10	
	Tuotanto	20	
	Henkilosto	50	
	Hallinta	99	192.168.99.12/24
MetroSW5	Servernetwork	60	
	Servers	601	
	Tuotantopalvelimet	620	
	Hallinta	99	192.168.99.15/24
MetroSW6	Servernetwork	60	
	Servers	601	
	Tuotantopalvelimet	620	
	Hallinta	99	192.168.99.16/24
WG5-SW1	Vieraat	10	
	Tuotanto	20	
	Henkilosto	50	
	Hallinta	99	192.168.99.51/24

9.3 PVLAN

PVLANin konfigurointi aloitetaan luomalla halutut tilaajaVLANit sekä network-VLAN ja määrittämällä näille VLANeille ID:t. Kytkimille MetroSW5 ja MetroSW6 luotiin network-VLANiksi servernetwork ID:llä 60 ja tilaajaVLANeiksi isoservers ID:llä 601 ja tuotantoservers ID:llä 620. Alla esimerkkinä VLANien luomisesta MetroSW5-kytkimellä.

create vlan servernetwork
configure vlan servernetwork tag 60
create vlan isoservers
configure vlan isoservers tag 601
create vlan tuotantoServers

configure vlan tuotantoServers tag 620

Tämän jälkeen luodaan Private-VLAN instanssi, johon aiemmin luodut VLANit liitetään. Luotu Private-VLAN instanssi oli nimeltään palvelimet. TilaajaVLANeja liittäessä VLANin tyyppi määritetään *non-isolated* tai *isolated* –määreen avulla. Oletuksena ilman lisämäärettä, kytkin luo isolated tilaajaVLANin. Isoservers luodaan isolated-VLANiksi ja tuotantoservers luodaan non-isolated –VLANiksi. Servernetwork konfiguroidaan palvelimet private-VLANin network –VLANiksi. Alla esimerkkinä Private-VLANin luonti sekä tilaajaVLANien liittäminen MetroSW5 kytkimellä.

create private-vlan palvelimet
configure palvelimet add network servernetwork
configure palvelimet add subscriber isoservers
configure palvelimet add subscriber tuotantoservers non-isolated

Luotuihin VLANeihin täytyy vielä liittää portit. MetroCore1-kytkimelle menevä rajapinta MetroSW5:lla liitettiin servernetwork-VLANiin. Lisäksi tälle portille määriteltiin private-vlan translation, jolloin tilaajaVLANeista ulospäin menevä liikenne merkitään servernetwork-VLANin tagilla. Alla esimerkkinä translationin konfigurointi MetroSW5-kytkimellä:

configure servernetwork add port 26 private-vlan translated

Päätelaitteille menevät portit määritettiin tilaajaVLANehin untagged-tilassa. Alla esimerkkinä rajapintojen määrittäminen MetroSW5-kytkimellä:

configure isoservers add port 15 untagged
configure tuotantoservers add port 20 untagged
configure isoservers add port 25 untagged

Palvelimet Private-VLAN laajennettiin myös MetroSW6-kytkimelle, jolloin MetroSW5 ja MetroSW6 –kytkinten välinen rajapinta piti määritellä tilaajaVLANeihin tagged-tilaan. Jos tilaajaVLANeilla on käytössä samoja rajapintoja, tässä tapauksessa MetroSW5 ja MetroSW6 –kytkinten välinen rajapinta, niin Extreme Networksin Black-Diamond 8000 ja Summit-sarjan kytkimet vaativat loopback-portin jokaiselle tilaajaVLANille, joilla on käytössä sama rajapinta. Tämän takia tuotantoservers-VLANille täytyi tässä vaiheessa luoda oma loopback -rajapinta. Tämä tehdään samalla komennolla kuin aiemmin liittäessä tilaajaVLAN PVLANiin, mutta nyt lisätään määre *loopback-port*

X komennon perään. Alla esimerkkinä MetroSW5 ja MetroSW6 välisen linkin konfigurointi MetroSW5-kytkimeltä:

configure Isoservers add ports 25 tagged
configure Palvelimet add subscriber Tuotantoservers non-isolated loopbackport 1
configure Tuotantoservers add ports 25 tagged

9.4 802.1X

802.1X:n konfigurointi aloitetaan luomalla 802.1X:ää varten VLAN ja liittämällä tämä VLAN netloginiin. Tähän VLANiin sijoitetaan laitteet siksi aikaa, kunnes 802.1X autentikointiprosessi on suoritettu, jonka jälkeen laite sijoitetaan oikeaan VLANiin. Tämän jälkeen kytkimelle määritetään netlogin tyypiksi 802.1X komennolla *enable netlogin dot1x.* Kun netlogin on valittu 802.1X:ksi, määritetään mille kytkimen porteille netlogin tulee päälle. Tämän lisäksi kytkimille luotiin Tuotanto, Henkilosto ja Vieraat –VLANit ja määritettiin näille VLAN-ID:t. Esimerkki konfiguraatio MetroSW2-kytkimeltä:

create vlan temp
configure temp tag 5
configure netlogin vlan temp
enable netlogin dot1x
enable netlogin ports 10-24 dot1x

MetroSW2 –kytkimellä otettiin myös käyttöön 802.1X:n guest-VLAN. Guest-VLANin konfigurointi tapahtuu määrittämällä VLANin guest-VLANiksi ja portit joille tämä guest-VLAN tulee voimaan. Tämän lisäksi guest-VLAN toiminto tulee ottaa myös yleisesti päälle. Esimerkkikonfiguraatio MetroSW2:lta:

configure netlogin dot1x guest-vlan vieraat ports 10-15
enable netlogin dot1x guest-vlan ports 10-15

9.4.1 Radius

Jotta 802.1X autentikointi tapahtuisi Radius-palvelimelle, tulee kytkimelle määrittää yhteys Radius-palvelimeen. Yhteyden saamiseen tulee kytkimen tietää Radius-palvelimen osoite, portti sekä salasana. Extreme Networksin kytkimissä oletuksena Radius-palvelimen osoitetta määrittäessä kytkin käyttää kytkimen hallintaa tarkoitettua virtuaalikytkintä (vr-mgnt). Joten jos haluaa käyttää jotain toista virtuaalikytkintä, tulee se määrittää komennon perään. Kun nämä muuttujat on määritetty kytkimeen, tulee Radius-toiminto ottaa käyttöön kytkimeltä. Esimerkkikonfiguraatio MetroSW2:lta:

```
configure radius netlogin primary server 192.168.99.99 1812 client-ip
192.168.99.12 vr vr-default
configure radius netlogin primary shared-secret root66
enable radius
```

9.4.2 FreeRADIUS

Työssä Radius-palvelimena käytetään FreeRADIUS:ta. FreeRADIUS on opensource-tuote ja se on yksi käytetyimmistä Radius-palvelimista maailmassa. FreeRADIUS asennettiin CentOS-käyttöjärjestelmään. Radius-palvelimen IP-osoitteeksi konfiguroitiin 192.168.99.99. Jotta autentikointi toimisi FreeRADIUS-palvelimella, täytyi FreeRADIUS-palvelimeen lisätä käyttäjät sekä autentikoivat kytkimet ja näiden salasanat. Kytkimet lisätään clients.conf tiedostoon, joka löytyy /etc/raddb kansiosta. Tiedostoon täytyy määrittää kytkimen IP-osoite sekä salasana. Esimerkki konfiguraatio client.conf-tiedostosta:

```
client MetroSW2 {
        ipaddr = 192.168.99.12
        secret = root66
}
```

Autentikoituvat käyttäjät lisätään users-tiedostoon, joka löytyy samasta kansiosta kuin clients.conf-tiedosto. Käyttäjää varten tiedostoon täytyy määrittää nimi, salasana sekä VLAN, jos kytkimellä halutaan käyttää dynaamisesti määräytyvää VLANia. Esimerkkikonfiguraatio users-tiedostosta:

Steven *Auth-Type := EAP, Cleartext-Password := ”root66”*
Extreme-Netlogin-Vlan = tuotanto

9.4.3 802.1X konfigurointi WG5-SW1 -kytkimelle

Konfigurointi aloitetaan määrittämällä 802.1X:än oletus autentikointi tavaksi Radius-palvelin. Esimerkki konfiguraatio WG5-SW1-kytkimeltä:

aaa new-model
aaa authentication dot1x default group radius

Tämän jälkeen kytkimelle konfiguroidaan Radius-palvelimen IP-osoite sekä salasana. Esimerkki konfiguraatio WG5-SW1-kytkimeltä:

radius-server host 192.168.60.10
radius-server key root66

Rajapinnalle määritetään, että VLAN määräytyy dynaamisesti. Myös Guest-VLAN määritetään rajapinnalle IOS-käyttöjärjestelmässä. Esimerkki konfiguraatio WG5-SW1-kytkimeltä:

int range G0/6 - 12
description UserAccess
switchport mode access
spanning-tree portfast
dot1x port-control auto
dot1x guest-vlan 10

9.5 Tietoturvaominaisuudet

9.5.1 MAC Security

MAC Securityn konfigurointi tapahtuu Extreme Networksin kytkimissä rajapinta ja VLAN kohtaisesti. Mac Security konfiguroidaan kytkimiin seuraavanlaisella komennolla:

configure ports <portlist> vlan <vlan_name> [limit-learning <number> {action [black-hole | stop-learning]} | lock-learning | unlimited-learning | unlock-learning]

Mac Securityä konfiguroidessa määritetään portit sekä VLAN, jolle MAC Security tulee voimaan. Lisäksi komentoon täytyy määrittää portilta opittujen MAC-osoitteiden maksimi määrä sekä tämän arvon ylittäneille MAC-osoitteille tehtävä toimenpide. Esimerkki konfiguraatio MetroSW1-kytkimeltä:

configure ports 10-15 vlan tuotanto limit-learning 2 action blackhole
configure ports 16-21 vlan henkilosto limit-learning 1 action stop-learning

9.5.2 DHCP Snooping and Trusted DHCP Server

DHCP-Snoopingin konfiguroiti tapahtuu samoilla periaatteilla kuin MAC Securityn konfigurointi. DHCP-Snoopingissakin määritettään portit ja VLAN, jonka jälkeen asetetaan toimenpide mahdollisten rikkomusten varalta. DHCP-Snoopingin toimenpiteeksi voidaan asettaa none tai drop-packet, jolle voidaan lisäksi määrittää block-mac ja block-port toiminnot. Block-MAC toiminto tekee automaattisesti portille pääsylistan, joka estää DHCP-paketin lähteen MAC-osoitteen. Block-Port sulkee väliaikaisesti tai pysyvästi portin, joka on vastaanottanut DHCP-palvelimelta peräisin olevan paketin. None-toiminto sallii DHCP-palvelimelta peräisin olevien pakettien kulun ja ainoastaan kerää näistä tietoa DHCP bindings –tietokantaan. Esimerkkikonfiguraatiot MetroSW1:ltä.

enable ip-security dhcp-snooping tuotanto ports all violation-action drop-packet
enable ip-security dhcp-snooping henkilosto ports all violation-action drop-packet block-mac duration 60

Trusted DHCP-server toiminto konfiguroidaan jokaiselle VLANille erikseen. Komennossa määritetään VLAN sekä DHCP-palvelimen IP-osoite. Esimerkki konfiguraatiot MetroSW1:ltä:

configure trusted-servers tuotanto add server 192.168.20.1 trust-for dhcp-server
configure trusted-servers henkilosto add server 192.168.50.1 trust-for dhcp-server

9.5.3 DHCP Secured ARP

DHCP Secured ARP –ominaisuus konfiguroidaan myös rajapinta ja VLAN kohtaisesti. Oletuksena kytkin täyttää ARP-taulua seuraamalla ARP-pyyntöjä ja -vastauksia. Jotta

kytkin täyttäisi ARP-taulua DHCP-pakettien osoitteilla, täytyy kytkimeltä ensiksi ottaa VLANista MAC-learning pois käytöstä ja tämän jälkeen konfiguroida DHCP Secured ARP-learning päälle. Esimerkkikonfiguraatio MetroSW1:ltä:

disable ip-security arp learning learn-from-arp vlan tuotanto ports all

enable ip-security arp learning learn-from-dhcp vlan tuotanto ports all

9.5.4 Source IP lockdown

Source IP lockdown –ominaisuuden konfiguroiti tapahtuu yksinkertaisesti yhdellä komennolla, jossa määritetään rajapinnat, joille ominaisuus otetaan käyttöön. Esimerkkikonfiguraatio MetroSW1:ltä:

enable ip-security source-ip-lockdown ports 16-21

9.5.5 Gratuitous ARP

Gratuitous ARP –ominaisuus voidaan asettaa päälle tietyille tai kaikille VLANeille. Kun Gratuitous ARP –ominaisuus on kytkimellä päällä, lähettää silloin kytkin oman gratuitous ARP-paketin, jos vastaan otetussa gratuitous ARP-paketissa on:

- Lähettäjän IP-osoite sama kuin kytkimen VLANissa ja lähettäjän MAC-osoite on eri kuin kytkimen oma MAC-osoite.
- Lähettäjän IP-osoite on sama kuin staattisesti ARP-tauluun määritellyn ja MAC-osoite on eri kuin ARP-taulussa.

Esimerkkikonfiguraatio MetroCore1:ltä:

enable ip-security arp gratuitous-protection vlan vieraat
enable ip-security arp gratuitous-protection vlan tuotanto

9.6 LLDP

LLDP-konfigurointi Extreme Networksin kytkimillä aloitetaan ottamalla LLDP-protokolla käyttöön. LLDP otetaan käyttöön joko kaikille rajapinnoille tai ainoastaan osalle pinnoista. Jos halutaan, että kytkin ainoastaan lähettää LLDP-viestejä, niin *enable lldp* –komentoon lisätään *transmit-only* –määre. Jos taas halutaan, että kytkin

ainoastaan vastaanottaa LLDP-viestejä, komentoon lisätään receive-only –määre. Tämän jälkeen LLDP:lle määritetään valinnaiset TLV:t, joita kytkimen halutaan mainostavan. Esimerkkikonfiguraatiot MetroCore1:ltä:

```
enable lldp ports 1:3-4,1:6
configure lldp ports 1:3-4,1:6 advertise system-name
configure lldp ports 1:3-4,1:6 advertise vendor-specific dot1 vlan-name
```

9.7 ACL & CLEAR-Flow

Pääsylistan luominen Extreme Networksin kytkimissä tapahtuu joko luomalla policy-tiedosto tai dynaamisesti *create access-list* –komennolla. Työssä pääsylista luotiin policy-tiedostolla, joten seuraavat esimerkit ovat policy-tiedostosta. Extreme Networksin pääsylistojen syntaksi on seuraava:

```
entry <ACLrulename>{
if  {
<match-conditions>;
} then {
<action>;
<action-modifiers>;
}
}
```

Policy-tiedostossa ensiksi määritetään ACL-säännön nimi, jonka jälkeen tiedostoon määritetään halutun liikenteen ehdot ja tälle liikenteelle tehtävät toimenpiteet. Työssä ACL ja CLEAR-Flow –ominaisuudet testattiin yhdellä säännöllä, jossa tarkkailtiin liikennettä vieraat-VLANista Servernetwork-VLANiin. Toimenpiteeksi pääsylistaan määritettiin pääsylistan ehdot täyttävän liikenteen pakettimäärän laskeminen counter1-nimiseen laskuriin, jota CLEAR-flow tulee käyttämään. Esimerkki pääsylista MetroCore-kytkimeltä:

```
entry acl_rule_vieraat {
        if {
                source-address 192.168.10.0/24;
                destination-address 192.168.60.0/24;
        } then {
                count counter1
        }
        }
```

Kuten aiemmin todettiin, on CLEAR-Flow ACL:n lisäosa. Tämän takia CLEAR-Flow säännöt kirjoitetaan samaan policy-tiedostoon kuin aiemmin luotu pääsylista. CLEAR-Flow:n syntaksi on pääsylistan kaltainen:

```
entry <CLFrulename> {
        if <match-type> { <match-conditions>;
         }
        then {
                <actions>;
        } else {
                <actions>;
        }
        }
```

Työssä CLEAR-Flow konfiguroitiin tarkkailemaan pääsylistassa määritetyn counter1-laskurin delta-arvoa eli muutosta. Jos counter1-laskurin muutos on suurempi kuin 5000 pakettia kymmenessä sekunnissa, eli vieraat-VLANista servernetwork-VLANiin menevien pakettien määrä, CLEAR-Flow estää acl_rule_vieraat –pääsylistaan ehtoihin kuuluvan liikenteen. Jos laskurin arvo laskee alle 5000 paketin, CLEAR-Flow poistaa liikenteen eston.

```
entry cflow_vieraat {
 if { delta counter1 >= 5000 ;
        period 10 ;
} then {
        deny acl_rule_vieraat;
} else {
        permit acl_rule_vieraat;
}
```

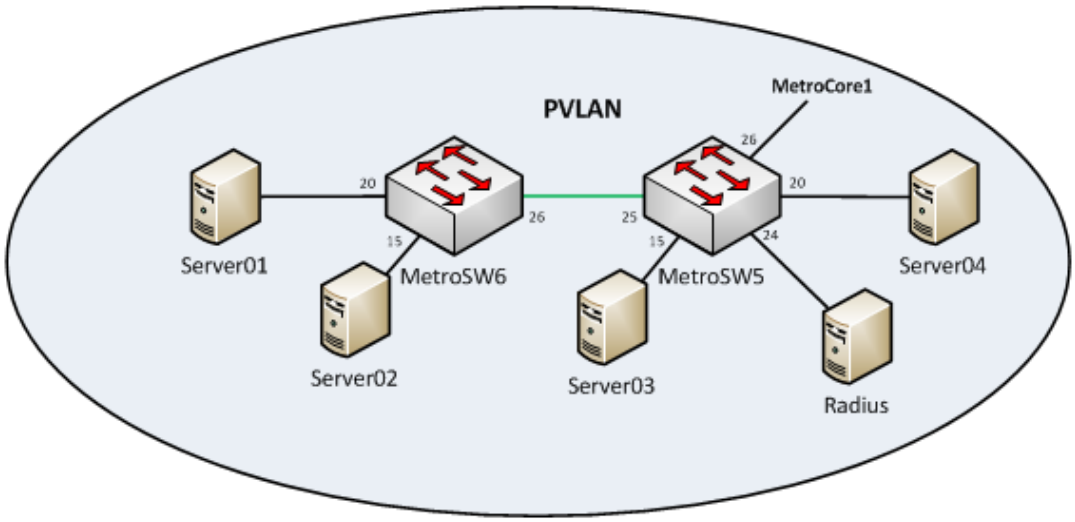
Kun policy-tiedosto on luotu, täytyy CLEAR-Flow ottaa kytkimellä käyttöön ja asettaa pääsylista rajapinnalle. Lisäksi komennossa täytyy määrittää tuleeko pääsylista voimaan sisään menevälle vai ulos tulevalle liikenteelle. Esimerkkikonfiguraatio Metro-Core1:ltä:

```
enable clear-flow
configure access-list acl_rule_vieraat  ports 1:1 ingress
```

10 TULOKSET

10.1 PVLAN

PVLANin toimintaa todennettiin topologian PVLAN-osassa. MetroSW5 ja MetroSW6 kytkimiin oli liitetty kumpaankin kaksi tietokonetta, joista toinen oli isolated VLANissa ja toinen non-isolated VLANissa. Näiden koneiden lisäksi SW5-kytkimeen oli kytketty Radius-palvelin (Ks. kuvio36). Tietokoneiden IP-osoiteet ovat taulukossa 6.



KUVIO 36. Topologia

TAULUKKO 5. PVLAN IP-osoitteistus

Kone	IP	VLAN	TYYPPI	KYTKIN
Server01	192.168.60.200	620	NON-ISOLATED	SW6 (PORT 20)
Server02	192.168.60.100	601	ISOLATED	SW6 (PORT 15)
Server03	192.168.60.101	601	ISOLATED	SW5 (PORT 15)
Server04	192.168.60.201	620	NON-ISOLATED	SW5 (PORT 20)

Todentaminen aloitettiin yksinkertaisella PING-testillä, jossa PING-komennolla testattiin laitteiden kommunikointi toistensa kanssa. PING-testi suoritettiin pingaamalla jokaiselta koneelta muita PVLANissa olevia tietokoneita sekä MetroCORE1:stä joka toimi oletusyhdyskäytävänä. Koska verkossa ei ollut käytössä proxyä, joka hoitaisi L3-liikennöintiä, eristyksessä L2-tasolla olevan tietokoneen ei pitäisi pystyä keskustelemaan kuin oletusyhdyskäytävän kanssa. Tällöin tietokoneilla Server02 ja Server03 PING kulkisi ainoastaan CORE1:lle, kun taas Server01 ja Server04 pystyvät MetroCORE1:n lisäksi pingaamaan toisiaan.

Aluksi MetroCore1:ltä pingattiin kaikkia PVLANissa olevia tietokoneita (Ks. kuvio 37). Näin varmistettiin, että verkko toimi oikein.

```
* MetroCore1.10 # ping 192.168.60.100
Ping(ICMP) 192.168.60.100: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 192.168.60.100: icmp_seq=0 ttl=128 time=4.967 ms
16 bytes from 192.168.60.100: icmp_seq=1 ttl=128 time=4.592 ms
16 bytes from 192.168.60.100: icmp_seq=2 ttl=128 time=4.582 ms
16 bytes from 192.168.60.100: icmp_seq=3 ttl=128 time=4.645 ms

--- 192.168.60.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 4/4/4 ms
* MetroCore1.11 # ping 192.168.60.101
Ping(ICMP) 192.168.60.101: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 192.168.60.101: icmp_seq=0 ttl=64 time=5.829 ms
16 bytes from 192.168.60.101: icmp_seq=1 ttl=64 time=4.517 ms
16 bytes from 192.168.60.101: icmp_seq=2 ttl=64 time=4.545 ms
16 bytes from 192.168.60.101: icmp_seq=3 ttl=64 time=7.926 ms

--- 192.168.60.101 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 4/5/7 ms
* MetroCore1.12 # ping 192.168.60.200
Ping(ICMP) 192.168.60.200: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 192.168.60.200: icmp_seq=0 ttl=128 time=6.059 ms
16 bytes from 192.168.60.200: icmp_seq=1 ttl=128 time=4.572 ms
16 bytes from 192.168.60.200: icmp_seq=2 ttl=128 time=1.182 ms
16 bytes from 192.168.60.200: icmp_seq=3 ttl=128 time=4.546 ms

--- 192.168.60.200 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 1/4/6 ms
* MetroCore1.13 # ping 192.168.60.201
Ping(ICMP) 192.168.60.201: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 192.168.60.201: icmp_seq=0 ttl=64 time=1.403 ms
16 bytes from 192.168.60.201: icmp_seq=1 ttl=64 time=4.746 ms
16 bytes from 192.168.60.201: icmp_seq=2 ttl=64 time=4.647 ms
16 bytes from 192.168.60.201: icmp_seq=3 ttl=64 time=4.712 ms

--- 192.168.60.201 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 1/3/4 ms
```

KUVIO 37. MetroCore1 PING

Kun verkon toimivuus oli varmistettu, niin testattiin PVLANissa olevin tietokoneiden kommunikointi keskenään (Ks. Kuviot 38 – 41).,

```
C:\Users\labranet>ping 192.168.60.1

Pinging 192.168.60.1 with 32 bytes of data:
Reply from 192.168.60.1: bytes=32 time=17ms TTL=64
Reply from 192.168.60.1: bytes=32 time<1ms TTL=64
Reply from 192.168.60.1: bytes=32 time=6ms TTL=64
Reply from 192.168.60.1: bytes=32 time=8ms TTL=64

Ping statistics for 192.168.60.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 7ms

C:\Users\labranet>ping 192.168.60.100

Pinging 192.168.60.100 with 32 bytes of data:
Reply from 192.168.60.200: Destination host unreachable.
Reply from 192.168.60.200: Destination host unreachable.
Reply from 192.168.60.200: Destination host unreachable.
Reply from 192.168.60.200: Destination host unreachable.

Ping statistics for 192.168.60.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\labranet>ping 192.168.60.101

Pinging 192.168.60.101 with 32 bytes of data:
Reply from 192.168.60.200: Destination host unreachable.
Reply from 192.168.60.200: Destination host unreachable.
Reply from 192.168.60.200: Destination host unreachable.
Reply from 192.168.60.200: Destination host unreachable.

Ping statistics for 192.168.60.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\labranet>ping 192.168.60.201

Pinging 192.168.60.201 with 32 bytes of data:
Reply from 192.168.60.201: bytes=32 time<1ms TTL=64
Reply from 192.168.60.201: bytes=32 time<1ms TTL=64
Reply from 192.168.60.201: bytes=32 time<1ms TTL=64
Reply from 192.168.60.201: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.60.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

KUVIO 38. Server 01 PING

```
C:\Documents and Settings\Administrator>ping 192.168.60.1

Pinging 192.168.60.1 with 32 bytes of data:

Reply from 192.168.60.1: bytes=32 time=17ms TTL=64
Reply from 192.168.60.1: bytes=32 time=7ms TTL=64
Reply from 192.168.60.1: bytes=32 time=7ms TTL=64
Reply from 192.168.60.1: bytes=32 time=7ms TTL=64

Ping statistics for 192.168.60.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 17ms, Average = 9ms

C:\Documents and Settings\Administrator>ping 192.168.60.101

Pinging 192.168.60.101 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.60.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>ping 192.168.60.200

Pinging 192.168.60.200 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.60.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>ping 192.168.60.201

Pinging 192.168.60.201 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

KUVIO 39. Server02 PING

```
administrator@administrator-desktop:~$ ping 192.168.60.1
PING 192.168.60.1 (192.168.60.1) 56(84) bytes of data.
64 bytes from 192.168.60.1: icmp_seq=1 ttl=64 time=1.89 ms
64 bytes from 192.168.60.1: icmp_seq=2 ttl=64 time=0.989 ms
64 bytes from 192.168.60.1: icmp_seq=3 ttl=64 time=0.982 ms

--- 192.168.60.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.982/1.288/1.893/0.427 ms
administrator@administrator-desktop:~$ ping 192.168.60.100
PING 192.168.60.100 (192.168.60.100) 56(84) bytes of data.
From 192.168.60.101 icmp_seq=1 Destination Host Unreachable
From 192.168.60.101 icmp_seq=2 Destination Host Unreachable
From 192.168.60.101 icmp_seq=3 Destination Host Unreachable

--- 192.168.60.100 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3009ms
, pipe 3
administrator@administrator-desktop:~$ ping 192.168.60.200
PING 192.168.60.200 (192.168.60.200) 56(84) bytes of data.
From 192.168.60.101 icmp_seq=1 Destination Host Unreachable
From 192.168.60.101 icmp_seq=2 Destination Host Unreachable
From 192.168.60.101 icmp_seq=3 Destination Host Unreachable

--- 192.168.60.200 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3008ms
, pipe 3
administrator@administrator-desktop:~$ ping 192.168.60.201
PING 192.168.60.201 (192.168.60.201) 56(84) bytes of data.
From 192.168.60.101 icmp_seq=1 Destination Host Unreachable
From 192.168.60.101 icmp_seq=2 Destination Host Unreachable
From 192.168.60.101 icmp_seq=3 Destination Host Unreachable

--- 192.168.60.201 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3008ms
, pipe 3
```

KUVIO 40. Server03 PING

```
C:\Documents and Settings\Admin>ping 192.168.60.1

Pinging 192.168.60.1 with 32 bytes of data:

Reply from 192.168.60.1: bytes=32 time=13ms TTL=64
Reply from 192.168.60.1: bytes=32 time=7ms TTL=64
Reply from 192.168.60.1: bytes=32 time=7ms TTL=64
Reply from 192.168.60.1: bytes=32 time=7ms TTL=64

Ping statistics for 192.168.60.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 13ms, Average = 8ms

C:\Documents and Settings\Admin>ping 192.168.60.100

Pinging 192.168.60.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.60.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Admin>ping 192.168.60.101

Pinging 192.168.60.101 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.60.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Admin>ping 192.168.60.200

Pinging 192.168.60.200 with 32 bytes of data:

Reply from 192.168.60.200: bytes=32 time<1ms TTL=128
Reply from 192.168.60.200: bytes=32 time<1ms TTL=128
Reply from 192.168.60.200: bytes=32 time<1ms TTL=128
Reply from 192.168.60.200: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.60.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

KUVIO 41. Server04 PING

Taulukosta 6 nähdään Ping-testauksen tulokset. Tulokset vastaavat ennalta arvioitua tulosta ja tästä voidaan päätellä, että tähän mennessä PVLAN konfigurointi on toiminut vaatimusten mukaisesti.

TAULUKKO 6. PING testaus

Kone	**CORE1**	**Server01**	**Server02**	**Server03**	**Server04**
Server01	Kyllä	-	EI	EI	Kyllä
Server02	Kyllä	EI	-	EI	EI
Server03	Kyllä	EI	EI	-	EI
Server04	Kyllä	Kyllä	EI	EI	-

L2-yhteydet pystyttiin tarkistamaan myös tietokoneiden ARP-taulusta. ARP-taulusta nähdään, ettei Isolated-Vlanissa olevilla tietokoneilla ole tiedossa muiden kuin oletusyhdyskäytävän ARP-merkintöjä (Ks. Kuvio 42) ja nonisolated-VLANissa olevilla tietokoneilla on oletusyhdyskäytävän lisäksi samassa nonisolated-VLANissa olevien tietokoneiden Mac-osoitteet (Ks. kuvio 43). ARP-taulut tarkistettiin Windowsin komentokehotteessa komennolla arp –a, sen jälkeen kun tietokoneilla oli suoritettu PING-testaus.

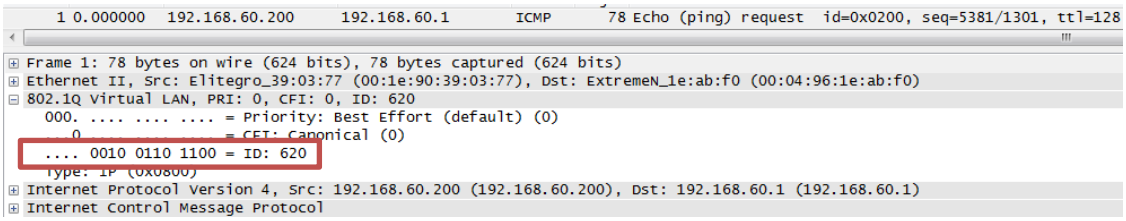
```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.60.100 --- 0x3
  Internet Address      Physical Address      Type
  192.168.60.1          00-04-96-1e-ab-f0     dynamic
```

KUVIO 42. Isolated ARP

```
C:\Documents and Settings\Admin>arp -a

Interface: 192.168.60.201 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.60.1          00-04-96-1e-ab-f0     dynamic
  192.168.60.200        18-a9-05-93-56-d9     dynamic

C:\Documents and Settings\Admin>_
```

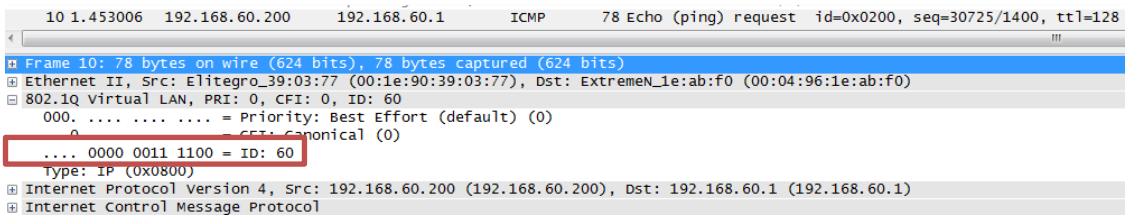
KUVIO 43. Non-Isolated ARP

PVLANin translation ominaisuutta varten liikenne peilattiin SW5 ja CORE1 kytkimiltä tietokoneelle, johon oli asennettu WireShark-ohjelma. WireSharkin avulla pystytään näkemään kytkinten välinen liikenne ja näin tarkastamaan translationin toimivuus. Translation testattiin pinggaamalla Server01:ltä MetroCore1-kytkintä. Ensimmäinen kaappaus on otettu SW5:n rajapintaan 25 tulevasta liikenteestä. Kuviosta 44 nähdään, että paketin VLAN ID on 620.



KUVIO 44. PING ennen Translationia

Toinen kaappaus on otettu MetroCORE1:n 1:4 rajapintaan tulevasta liikenteestä. Tästä kaappauksesta nähdään, että VLAN ID on vaihtunut 620:stä 60:een konfiguraation mukaisesti (Ks. kuvio 45).



KUVIO 45. PING Translationin jälkeen

10.2 802.1X

802.1X:n todentamiseen käytettiin Wireshark-ohjelmaa, jolla kaapattiin paketteja Windows XP-tietokoneen ja MetroSW2-kytkimen väliltä, sekä MetroSW2-kytkimen ja Radius-palvelimen väliltä. Näin 802.1X toiminta pystyttiin todentamaan pakettitasolla. Wireshark-ohjelman pakettikaappausten lisäksi todentamisessa hyödynnettiin ExtremeXOSin show-komentoja.

10.2.1 Onnistunut autentikointi

Onnistuneen autentikoinnin todentaminen aloitettiin liittämällä Windows XP-tietokone MetroSW2-kytkimeen ja asettamalla tietokoneelle 802.1X päälle. Radius-palvelimelle tehtiin käyttäjä nimeltä Steven, jolle annettiin salasanaksi root66. Lisäksi käyttäjälle määritettiin Radius-palvelimella VLANiksi tuotanto-VLAN.

Verkkoon kirjautuminen Windows XP-tietokoneessa tapahtuu Enter Credential-ikkunassa, joka ilmestyy ruutuun verkkoon liittyessä. Tähän ikkunaan syötetään tunnistautumistiedot, jonka jälkeen autentikoinnin onnistuttua käyttäjä saa pääsyn verkkoon. Kuten aiemmin todettiin, todentamisessa käytettiin apuna Wireshark-ohjelmaa, josta nähdään tietokoneen ja kytkimen välinen keskustelu (Ks. kuvio 46). Kuviossa 46 punaisella pohjalla olevat rivit ovat tietokoneen (autentikoituva) lähettämiä paketteja ja valkoisella pohjalla olevat rivit kytkimen (autentikoija) lähettämiä paketteja. Kuviosta huomataan, että Windows XP-tietokone aloitti autentikointiprosessin lähettämällä EAPOL-Start-paketin.

```
     6 22.553958  Elitegro_39:03:77   Nearest             EAPOL      60 Start
     7 22.555252  ExtremeN_28:35:c4   Elitegro_39:03:77   EAP        60 Request, Identity [RFC3748]
     9 32.812067  Elitegro_39:03:77   Nearest             EAP        60 Response, Identity [RFC3748]
    10 32.825077  ExtremeN_28:35:c4   Elitegro_39:03:77   EAP        60 Request, MD5-Challenge [RFC3748]
    11 32.825466  Elitegro_39:03:77   Nearest             EAP        60 Response, MD5-Challenge [RFC3748]
    12 32.845767  ExtremeN_28:35:c4   Elitegro_39:03:77   EAP        60 Success
```

KUVIO 46. Autentikoituva - Autentikoija

Tämän jälkeen autentikoituvan ja autentikoijan välinen keskustelu meni aiemman 802.1X toiminta –kohdan mukaisesti. Kuviosta 47 nähdään autentikoituvan lähettämän EAP-Response-paketin sisältämät tiedot, josta ilmenee, että tässä vaiheessa autentikoituva lähettää autentikoijalle ainoastaan käyttäjänimensä.

```
     9 32.812067  Elitegro_39:03:77   Nearest             EAP        60 Response, Identity [RFC3748]
⊞ Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: Elitegro_39:03:77 (00:1e:90:39:03:77), Dst: Nearest (01:80:c2:00:00:03)
⊟ 802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 11
  ⊟ Extensible Authentication Protocol
      Code: Response (2)
      Id: 219
      Length: 11
      Type: Identity [RFC3748] (1)
      Identity (6 bytes): Steven
```

KUVIO 47. EAP Response

Autentikoituva lähettää salasanansa vastauksena autentikoijan lähettämään MD5-Challenge Request-pyyntöön (Ks. kuvio 48).

```
    11 32.825466  Elitegro_39:03:77   Nearest             EAP       60 Response, MD5-Challenge [RFC3748]
⊞ Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: Elitegro_39:03:77 (00:1e:90:39:03:77), Dst: Nearest (01:80:c2:00:00:03)
⊟ 802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 28
  ⊟ Extensible Authentication Protocol
      Code: Response (2)
      Id: 220
      Length: 28
      Type: MD5-Challenge [RFC3748] (4)
      Value-Size: 16
      Value: cdd74c04e7e059cf8050c5d4b443b39b
      Extra data (6 bytes): 53746576656e
```

KUVIO 48. EAP MD5-Response

Autentikoinnin onnistuminen voidaan tarkistaa myös kytkimeltä komennolla *show netlogin dot1x*, josta nähdään, että rajapintaan 10 on autentikoitunut käyttäjä Steven ja käyttäjä kuuluu tuotanto-VLANiin (Ks. kuvio 49). Kuviossa 49 näkyy myös autentikoimaton rajapinta 11, joka on vielä temp-VLANissa.

```
* MetroSW2.5 # show netlogin dot1x

NetLogin Authentication Mode : web-based DISABLED;  802.1x ENABLED;  mac-based DISABLED
NetLogin VLAN                : "temp"
NetLogin move-fail-action    : Deny
NetLogin Client Aging Time   : 5 minutes
Dynamic VLAN Creation        : Disabled
Dynamic VLAN Uplink Ports    : None

-----------------------------------------------
        802.1x Mode Global Configuration
-----------------------------------------------
Quiet Period                    : 60
Supplicant Response Timeout     : 30
Re-authentication period        : 3600
Max Re-authentications          : 3
RADIUS server timeout           : 30
EAPOL MPDU version to transmit  : v1
Authentication Database         : Radius
-----------------------------------------------

Port: 10,  Vlan: tuotanto,  State: Enabled,  Authentication: 802.1x
Guest Vlan <Not Configured>: Disabled
Authentication Failure Vlan <Not Configured>: Disabled
Authentication Service-Unavailable Vlan <Not Configured>: Disabled

MAC               IP address       Authenticated     Type    ReAuth-Timer   User
00:1e:90:39:03:77  0.0.0.0          Yes, Radius       802.1x  3425           Steven
-----------------------------------------------
(B) - Client entry Blackholed in FDB

Port: 11,  Vlan: temp,  State: Enabled,  Authentication: 802.1x
Guest Vlan <Not Configured>: Disabled
Authentication Failure Vlan <Not Configured>: Disabled
Authentication Service-Unavailable Vlan <Not Configured>: Disabled

MAC               IP address       Authenticated     Type    ReAuth-Timer   User
-----------------------------------------------
(B) - Client entry Blackholed in FDB
```

KUVIO 49. Show netlogin dot1x

RADIUS

Autentikoijan ja Radius-palvelimen välinen keskustelu nähdään kuviosta 50. Tämäkin keskustelu menee 802.1X toiminta -kohdassa kuvatulla tavalla.

```
20 19.154930  192.168.99.12     192.168.99.99     RADIUS   152 Access-Request(1) (id=33, l=106)
23 19.162138  192.168.99.99     192.168.99.12     RADIUS   142 Access-challenge(11) (id=33, l=96)
24 19.166053  192.168.99.12     192.168.99.99     RADIUS   187 Access-Request(1) (id=34, l=141)
25 19.178150  192.168.99.99     192.168.99.12     RADIUS   114 Access-Accept(2) (id=34, l=68)
```

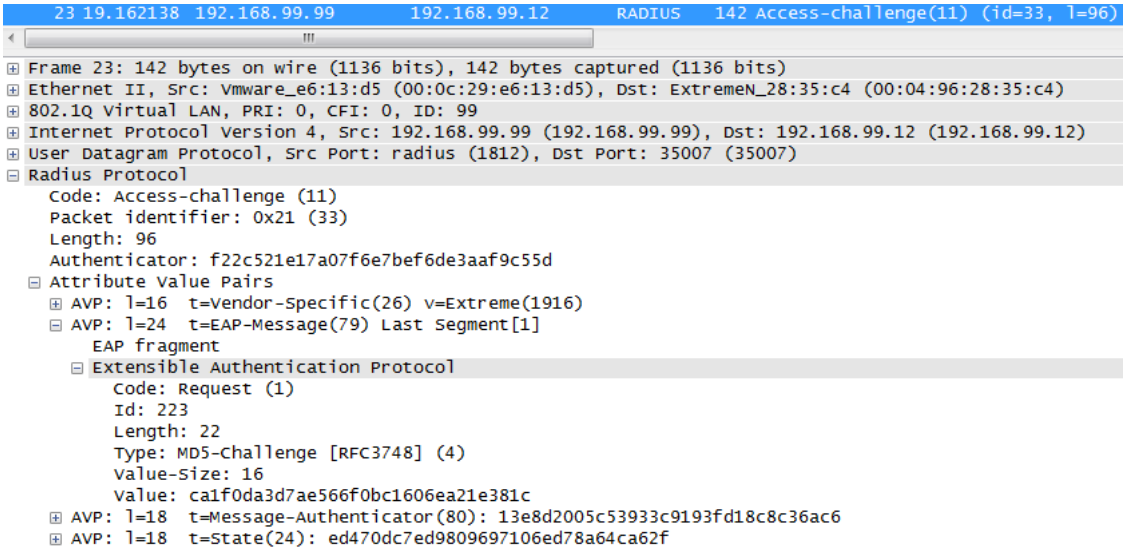
KUVIO 50. Autentikoija - Radius

Kuviosta 51 nähdään Autentikoijan lähettämän Access-Request-paketin sisältö. Paketti pitää sisällään autentikoituvan käyttäjän nimen sekä autentikoijan IP-osoiteen.

```
20 19.154930  192.168.99.12     192.168.99.99     RADIUS   152 Access-Request(1) (id=33, l=106)
⊞ Frame 20: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits)
⊞ Ethernet II, Src: ExtremeN_28:35:c4 (00:04:96:28:35:c4), Dst: Vmware_e6:13:d5 (00:0c:29:e6:13:d5)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 99
⊞ Internet Protocol Version 4, Src: 192.168.99.12 (192.168.99.12), Dst: 192.168.99.99 (192.168.99.99)
⊞ User Datagram Protocol, Src Port: 35007 (35007), Dst Port: radius (1812)
⊟ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x21 (33)
    Length: 106
    Authenticator: 74766f7c0115b3f9024e673379ced5f1
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=8  t=User-Name(1): Steven
    ⊟ AVP: l=13  t=EAP-Message(79) Last Segment[1]
        EAP fragment
      ⊟ Extensible Authentication Protocol
          Code: Response (2)
          Id: 222
          Length: 11
          Type: Identity [RFC3748] (1)
          Identity (6 bytes): Steven
    ⊟ AVP: l=6  t=NAS-IP-Address(4): 192.168.99.12
        NAS-IP-Address: 192.168.99.12 (192.168.99.12)
    ⊞ AVP: l=6  t=Service-Type(6): Login(1)
    ⊞ AVP: l=19  t=Calling-Station-Id(31): 00-1E-90-39-03-77
    ⊞ AVP: l=4  t=NAS-Port-Id(87): 10
    ⊞ AVP: l=6  t=NAS-Port(5): 1010
    ⊞ AVP: l=6  t=NAS-Port-Type(61): Ethernet(15)
    ⊞ AVP: l=18  t=Message-Authenticator(80): a6d6915239774d547600d248c344de58
```

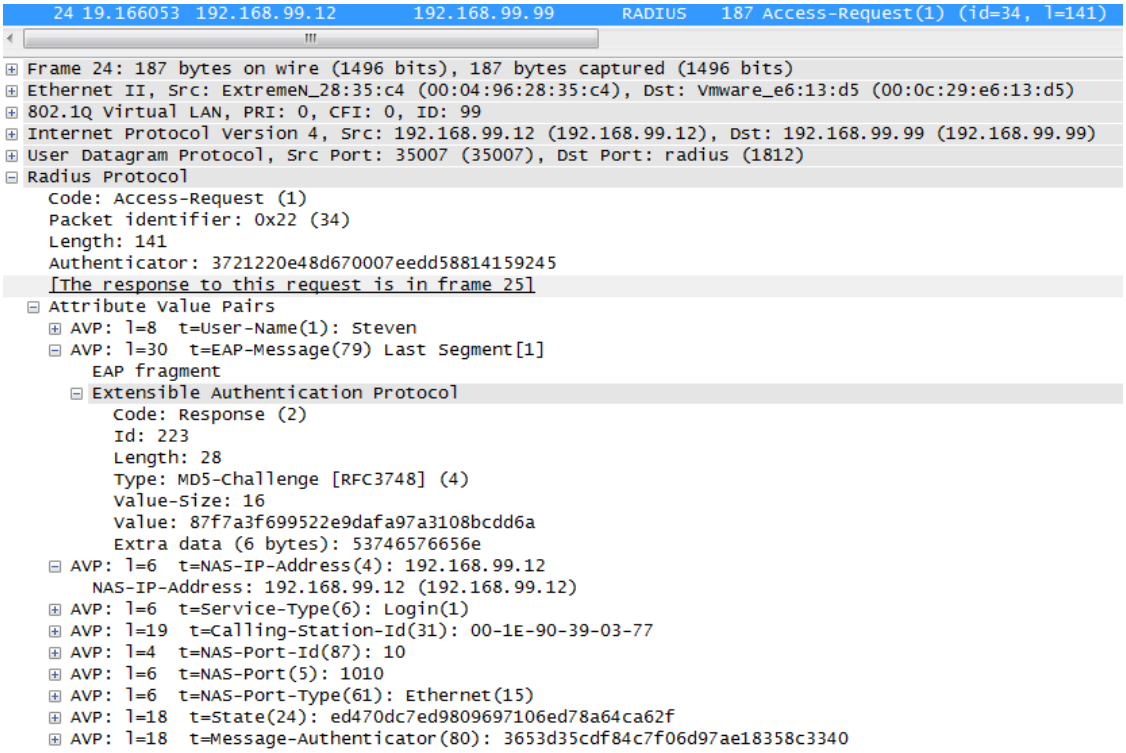
KUVIO 51. Radius Access-Request

Radius-palvelimen vastauksessa Attribute-kentän sisältämässä EAP-viestissä lähettää Radius-palvelin MD5-challenge-pyynnön autentikoituvalle(Ks. kuvio 52). Autentikoija välittää tämän pyynnön autentikoituvalle.



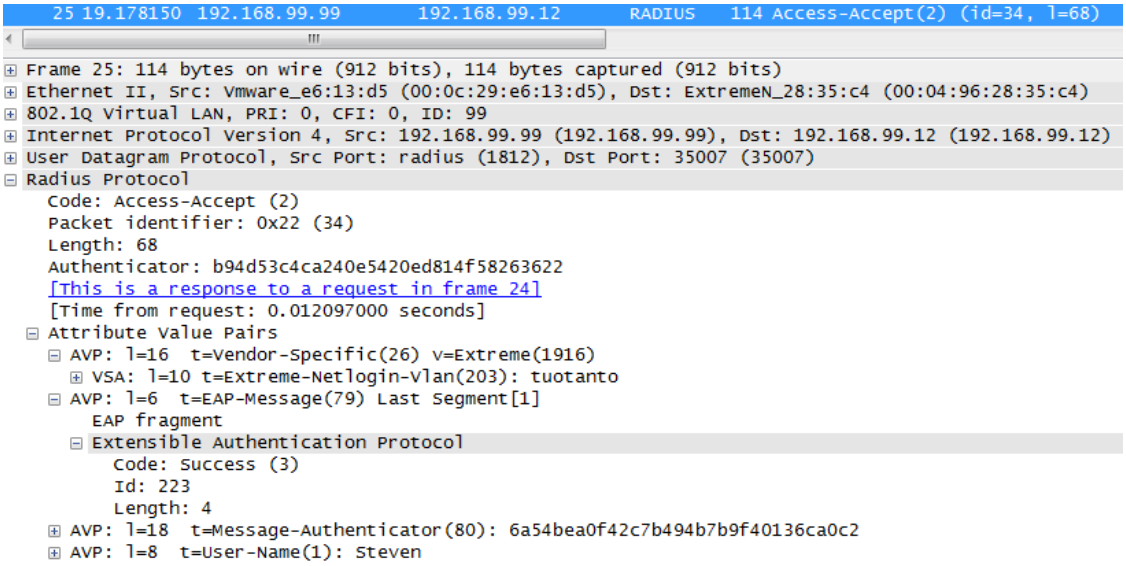
KUVIO 52. Radius Access-Challenge

Kuviosta 53 nähdään autentikoijan lähettämä toinen Access-Request-pyyntö, joka sisältää tällä kertaan myös autentikoituvan käyttäjän salasanan.



KUVIO 53. Radius Access-Reques 2

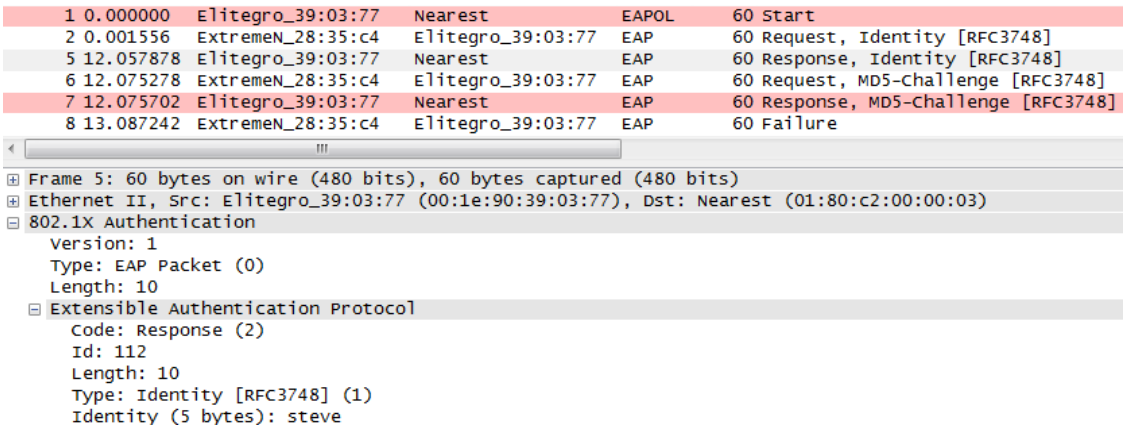
Radius-palvelimen lähettämä Access-Accept paketti sisältää EAP-success viestin lisäksi myös laitevalmistaja kohtaisen VLAN määrityksen, jolla Radius-palvelin käskee kytkimen sijoittaa autentikoituva päätelaite tuotanto VLANiin. (Ks. Kuvio 54)



KUVIO 54. Radius Access-Accept

10.2.2 Epäonnistunut autentikointi

Epäonnistunut autentikointi todennettiin syöttämällä Windows XP-tietokoneella väärä käyttäjänimi. Kuviosta 55 nähdään, että autentikointiprosessin kulku oli muuten samanlainen kuin onnistuneessa autentikoinnissa, mutta success-viestin tilalla oli failure-viesti, joka esti autentikoituvan pääsyn verkkoon.

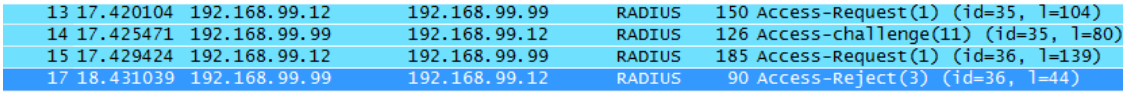


KUVIO 55. EAP Failure

Radius

Kuten 802.1X:n EAP osassa, niin myös Radius-prosessi meni kuten onnistuneessa autentikoinnissa, paitsi Access-Accept –viestin tilalla oli Access-Reject, jolla Radius-

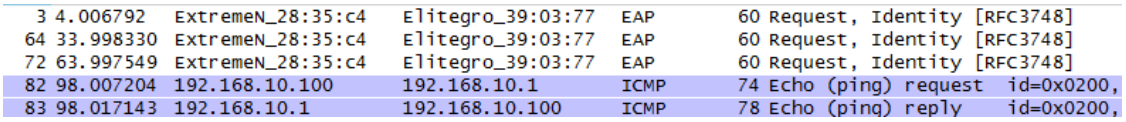
palvelin kertoo autentikoijalle, että autentikoituvalla ei ole oikeutta verkkoon (Ks. kuvio 56).



KUVIO 56. Radius Access-Reject

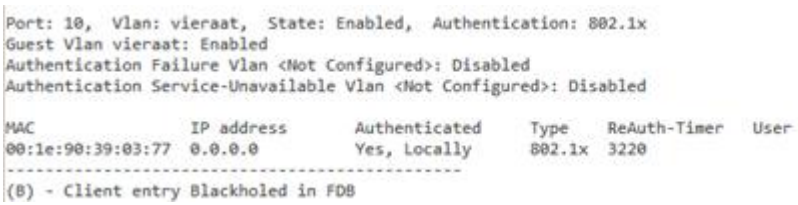
10.2.3 Guest-VLAN

Guest-VLANin toiminta testattiin 802.1X:ää tukemattomalle päätelaitteella sekä epäonnistuneella autentikoitumisella. Extreme Networksin kytkimillä 802.1X:ää tukematon päätelaite sijoitetaan oletuksena Guest-VLANiin kolmen autentikointipyynnön jälkeen. Tätä toimintaa testattiin laittamalla päätelaite pingaamaan oletusyhdyskäytävää samanaikaisesti kun päätelaite kytkettiin MetroSW2-kytkimeen. Näin pystyttiin todentamaan hetki jolloin kytkin sijoittaa päätelaitteen vieraat-VLANiin. Kuviosta 57 nähdään Wireshark-kaappaus, josta voidaan todeta, että Guest-VLAN –toiminto toimi kytkimellä oikein.



KUVIO 57. Guest-VLAN

Show netlogin dot1x –komennolla voidaan nähdä myös Guest-VLANiin liittynyt käyttäjä. Guest-VLANiin liittynyt vieras tunnistetaan siitä, ettei tällä ole käyttäjänimen kohdalle mitään ja rajanpinta kuuluu vieraat-VLANiin (Ks. kuvio 58).



KUVIO 58. Guest-VLAN - Show netlogin dot1x

Epäonnistunut autentikointi ja Guest-VLAN

MetroSW2-kytkimellä testattiin myös Extreme Networksin authentication failure VLAN-ominaisuutta, jossa epäonnistuneen autentikoinnin jälkeen päätelaite sijoitetaan rajoitettuun VLANiin, joka tässä tapauksessa on sama kuin Guest-VLAN. Todennuksessa käytettiin samaa tapaa kuin aiemmin Guest-VLANia todentaessa, eli päätelaite pingasi oletusyhdyskäytävää samanaikaisesti autentikointiprosessin kanssa. Kuviosta 59 nähdään, että kytkin sijoitti autentikoituvan päätelaitteen Guest-VLANiin, kun autentikointiprosessi epäonnistui, jolloin päätelaitteen lähettämä ping pääsi perille.

```
  3 10.081139  Elitegro_39:03:77   Nearest             EAPOL      60 Start
  4 10.082636  ExtremeN_28:35:c4   Elitegro_39:03:77   EAP        60 Request, Identity [RFC3748]
 48 34.060685  Elitegro_39:03:77   Nearest             EAP        60 Response, Identity [RFC3748]
 49 34.076513  ExtremeN_28:35:c4   Elitegro_39:03:77   EAP        60 Request, MD5-Challenge [RFC3748]
 50 34.076980  Elitegro_39:03:77   Nearest             EAP        60 Response, MD5-Challenge [RFC3748
 53 35.105144  ExtremeN_28:35:c4   Elitegro_39:03:77   EAP        60 Failure
 57 36.501718  192.168.10.100      192.168.10.1        ICMP       74 Echo (ping) request  id=0x0200,
 58 36.511661  192.168.10.1        192.168.10.100      ICMP       78 Echo (ping) reply    id=0x0200,
```

KUVIO 59. Guest-VLAN & epäonnistunut autentikointi

Autentication Failure Vlan –ominaisuus näkyy *show netlogin dot1x* –komennolla siten, että käyttäjänimen kohdalla on käyttäjän antama käyttäjänimi kuten onnistuneessa autentikoinnissa, mutta Authenticated –kohdassa nähdään että autentikaatio on tapahtunut paikallisesti. Komennolla nähdään myös, että Authentication Failure Vlan –ominaisuus on otettu käyttöön ja VLANiksi on määritelty vieraat-VLAN. (Ks. kuvio 60)

```
Port: 10,  Vlan: vieraat,  State: Enabled,  Authentication: 802.1x
Guest Vlan vieraat: Enabled
Authentication Failure Vlan vieraat: Enabled
Authentication Service-Unavailable Vlan <Not Configured>: Disabled

MAC               IP address       Authenticated     Type    ReAuth-Timer   User
00:1e:90:39:03:77 0.0.0.0          Yes, Locally      802.1x  3469           vaara
-----------------------------------------------
(B) - Client entry Blackholed in FDB
```

KUVIO 60. epäonnistunut autentikointi - show netlogin dot1x

10.3 Tietoturvaominaisuudet

10.3.1 MAC Security

Extreme Networksin kytkimistä MAC Securityn toiminta voidaan todentaan *show vlan-name security* –komennolla. Työssä tuotanto-VLANille konfigurointiin MAC-osoitteiden rajaksi kaksi osoitetta, jonka jälkeen opitut MAC-osoitteet sijoitetaan

Blackhole-tilaan, jolloin kaikki paketit, jotka ovat menossa tai tulossa näihin MAC-osoitteisiin hylätään. MetroSW1-kytkimen rajapintaan 10 kytkettiin kytkin sekä kaksi tietokonetta, jolloin MetroSW1-kytkimen pitäisi oppia kolme MAC-osoitetta rajapinnalta. Kuviosta 61 nähdään, että MetroSW1-kytkin on oppinut rajapinnalta kolme MAC-osoitetta, joista on viimeiseksi oppineen, kytkin on sijoittanut blackhole-tilaan.

```
* MetroSW1.47 # show "tuotanto" security
Port      Limit     State     Learned     Blackholed  Locked
3         Unlimited Unlocked  0           0           0
10        2         Unlocked  2           1           0
```

KUVIO 61. show tuotanto security

Myös MetroSW1-kytkimen rajapintaan 18 oli kytketty kytkin ja kaksi tietokonetta. Rajapinta kuuluu henkilosto-VLANille, jolle MAC Securityn raja-arvoksi oli konfiguroitu yksi MAC-osoite, jonka jälkeen kytkin lopettaa MAC-osoitteiden oppimisen rajapinnalta. Kuviosta 62 huomataan, että MetroSW1-kytkin on oppinut ainoastaan yhden MAC-osoiteen, jolloin MAC Security –ominaisuus toimii oikein.

```
* MetroSW1.48 # show "henkilosto" security
Port      Limit     State     Learned     Blackholed  Locked
3         Unlimited Unlocked  0           0           0
16        1         Unlocked  1           0           0
17        1         Unlocked  0           0           0
18        0         Unlocked  1           0           0
19        1         Unlocked  0           0           0
20        1         Unlocked  0           0           0
21        1         Unlocked  0           0           0
25        Unlimited Unlocked  0           0           0
```

KUVIO 62. show henkilosto security

10.3.2 DHCP Snooping and Trusted DHCP Server

DHCP Snooping ja Trusted DHCP Server –ominaisuudet testattiin liittämällä MetroSW1-kytkimeen toinen DHCP-palvelin, joka tässä tapauksessa kuvasi epäluotettavaa palvelinta. Luotetuksi DHCP-palvelimeksi oli konfiguroitu MetroCore1-kytkin. Jotta DHCP-snoopingin eri toiminnoille saatiin selvä ero, konfiguroitiin tuotanto ja henkilöstö VLANeille DHCP-snoopingiin eri toiminnot mahdollisten rikkomusten varalle.

Tuotanto-VLANille määritettiin DCHP-snoopingin toiminnoksi ainoastaan DHCP-paketin hylkäämisen, mikä tarkoittaa sitä, että jos kytkin huomaan DHCP-palvelimelta lähtöisin olevan paketin, joka ei ole lähtöisin luotetulta DHCP-palvelimelta, kytkin hylkää tämän paketin. Toiminnallisuus testattiin pyytämällä tuotanto-VLANiin kytketyllä

tietokoneella DHCP-palvelimelta IP-osoitetta ja samanaikaisesti toisella tuotanto-VLANiin liitetyllä tietokoneella pingattiin epäluotettavaa DHCP-palvelinta. Tällöin pystyttiin todentamaan, ettei DCHP-snooping toiminto tee muuta kuin DHCP-paketin hylkäämisen. DHCP-snoopingille määritetyt konfiguraatiot nähdään *show ip-security dhcp-snooping vlan "tuotanto"*-komennolla (Ks. kuvio 63).

```
* MetroSW1.3 # show ip-security dhcp-snooping vlan "tuotanto"
DHCP Snooping enabled on ports: 3, 10, 11, 12, 13, 14,
                                15, 25
Trusted Ports: None
Trusted DHCP Servers: 192.168.20.1
Bindings Restoration     : Disabled
Bindings Filename        :
Bindings File Location   :
         Primary Server  : None
         Secondary Server: None
Bindings Write Interval  : 30 minutes
Bindings last uploaded at:
-----------------------------------
Port            Violation-action
-----------------------------------
3               drop-packet
10              drop-packet
11              drop-packet
12              drop-packet
13              drop-packet
14              drop-packet
15              drop-packet
25              drop-packet
```

KUVIO 63. show ip-security dhcp-snooping vlan tuotanto

Testauksen tuloksena oli, että tietokone sai IP-osoiteen luotetulta DHCP-palvelimelta ja ping kulki kokoajan epäluotettavalle DHCP-palvelimella. Jotta pystyttiin varmistamaan, että MetroSW1-kytkin oli oikeasti huomannut tämän, tarkistettiin DHCP-snoopingin huomaavat rikkomukset komennolla *show ip-security dhcp-snooping violation "tuotanto"*. Kuviosta 64 nähdään, että rajapinnalla 13, johon epäluotettu DHCP-palvelin kytkettiin, on huomattu rikkomus ja DHCP-snooping on kirjannut rikkomuksen aiheuttaneen palvelimen MAC-osoitteen.

```
* MetroSW1.19 # show ip-security dhcp-snooping violations "tuotanto"
-----------------------------------
Port              Violating MAC
-----------------------------------
13              00:04:96:28:36:ce
```

KUVIO 64. show ip-security dhcp-snooping violations tuotanto

DHCP-snoopingin luoma DHCP-bindings-taulu nähdään kytkimeltä *show ip-security dhcp-snooping entries "tuotanto"* –komennolla. Taulusta nähdään, että tuotanto-VLANissa kaksi tietokonetta on saanut IP-osoitteen ja nämä tietokoneet on kytketty rajapintoihin 10 ja 11 (Ks. kuvio 65).

```
* MetroSW1.20 # show ip-security dhcp-snooping entries "tuotanto"
------------------------------------------------------------------------
Vlan: tuotanto
------------------------------------------------------------------------
                                  Lease Time    Server    Client
IP Addr         MAC Addr          (hh:mm:ss)    Port      Port
-------         --------          ----------    ------    ------
192.168.20.10   00:16:e6:13:ff:03   02:00:00      25        11
192.168.20.100  00:1e:90:39:03:77   02:00:00      25        10

Total number of entries : 2
```

KUVIO 65. show ip-security dhcp-snooping entries tuotanto

Henkilosto-VLANiin DHCP-snoopping konfiguroitiin kuvion 66 mukaisesti. DHCP-snoopingin toiminnoksi rikkomusten varaksi oli konfiguroitu DHCP-palvelimen MAC-osoitteen blokkaaminen 60 sekunnin ajaksi, jolloin kaikki liikenne joka on lähtöisin tai menossa palvelimelle hylätään.

```
* MetroSW1.4 # show ip-security dhcp-snooping vlan "henkilosto"
DHCP Snooping enabled on ports: 3, 16, 17, 18, 19, 20,
                                21, 25
Trusted Ports: None
Trusted DHCP Servers: 192.168.50.1
Bindings Restoration     : Disabled
Bindings Filename        :
Bindings File Location   :
         Primary Server  : None
         Secondary Server: None
Bindings Write Interval  : 30 minutes
Bindings last uploaded at:
----------------------------------
Port            Violation-action
------------------------------------
3               drop-packet, block-mac for 60 seconds
16              drop-packet, block-mac for 60 seconds
17              drop-packet, block-mac for 60 seconds
18              drop-packet, block-mac for 60 seconds
19              drop-packet, block-mac for 60 seconds
20              drop-packet, block-mac for 60 seconds
21              drop-packet, block-mac for 60 seconds
25              drop-packet, block-mac for 60 seconds
```

KUVIO 66. show ip-security dhcp-snooping vlan henkilosto

Testaus suoritettiin samalla lailla kuin tuotanto-VLANissa. Tällä kertaa toisen tietokoneen pingin tulisi katketa 60 sekunniksi DHCP-pyynnöstä eteenpäin. Kun tietokoneelta pyydettiin IP-osoitetta DHCP-palvelimelta, tietokone sai IP-osoitteen jälleen luotetulta DHCP-palvelimelta. Mutta kuten aiemmin arvioitiin, katkesi toisen tietokoneen lähettämä ping epäluotettavalle DHCP-palvelimelle noin 60 sekunniksi. DHCP-Snoopingin huomaavat rikkomukset nähdään jälleen *ip-security dhcp-snooping violation "henkilosto"*-komennolla (Ks. kuvio 67).

```
* MetroSW1.15 # show ip-security dhcp-snooping violations "henkilosto"
-------------------------------------
Port               Violating MAC
-------------------------------------
18               00:04:96:28:36:ce

* MetroSW1.16 #
```

KUVIO 67. show ip-security dhcp-snooping violations henkilosto

Henkilosto-VLANin DHCP-bindings taulu näkyy kuviosta 68, jossa nähdään jälleen kaksi VLANiin liitettyä tietokonetta.

```
* MetroSW1.21 # show ip-security dhcp-snooping entries "henkilosto"
-----------------------------------------------------------------------
Vlan: henkilosto
-----------------------------------------------------------------------
                                    Lease Time    Server    Client
IP Addr         MAC Addr            (hh:mm:ss)    Port      Port
-------         --------            ----------    ------    ------
192.168.50.10   00:1e:90:39:03:77   02:00:00      25        16
192.168.50.11   00:16:e6:13:ff:03   02:00:00      25        17

Total number of entries : 2
```

KUVIO 68. show ip-security dhcp-snooping entries henkilosto

10.3.3 DHCP Secured ARP

DHCP Secured ARP konfiguroitiin tuotanto-VLANille. Konfigurointi voidaan todeta *show ip-security arp learning vlan* –komennolla. Kuviosta 69 nähdään tuotanto-VLANin ja henkilosto-VLANin ARP konfiguraatiot.

```
* MetroSW1.24 # show ip-security arp learning vlan "tuotanto"
Port               Learn from
----------------------------
3                  ARP
10                 DHCP
11                 DHCP
12                 DHCP
13                 DHCP
14                 DHCP
15                 DHCP
25                 ARP

* MetroSW1.25 # show ip-security arp learning vlan "henkilosto"
Port               Learn from
----------------------------
3                  ARP
16                 ARP
17                 ARP
18                 ARP
19                 ARP
20                 ARP
21                 ARP
25                 ARP
```

KUVIO 69. show ip-security arp learning vlan tuotanto | henkilosto

Extreme Networksin kytkimistä ARP-taulun saa näkyviin *show iparp*-komennolla. Kuviosta X nähdään MetroSW1-kytkimen ARP-taulu. ARP-taulussa nähdään kaksi staattista merkintää. DHCP Secured ARP on lisännyt nämä merkinnät Kuviossa 70 nähdyn

DCHP-bindings-taulun tietojen perusteella. Henkilosto-VLANille DHCP Secured ARP –toimintoa ei otettua käyttöön, jolloin henkilosto-VLANin ARP-taulussa ei ole staattisia lisäyksiä.

```
* MetroSW1.21 # show iparp "tuotanto"
VR            Destination      Mac                Age  Static  VLAN          VID   Port
VR-Default    192.168.20.10    00:16:e6:13:ff:03    0     YES  tuotanto      20
VR-Default    192.168.20.100   00:1e:90:39:03:77    0     YES  tuotanto      20

Dynamic Entries  :           0            Static Entries           :          2
Pending Entries  :           0
In Request       :         656            In Response              :         49
Out Request      :          49            Out Response             :        141
Failed Requests  :           2
Proxy Answered   :           0
Rx Error         :           0            Dup IP Addr              :      0.0.0.0
Rejected Count   :          48            Rejected IP              :  192.168.20.100
Rejected Port    :          11            Rejected I/F             : tuotanto

Max ARP entries  :        8192            Max ARP pending entries  :        256
ARP address check:     Enabled            ARP refresh              :    Enabled
Timeout          :          20 minutes     ARP Sender-Mac Learning  :   Disabled

* MetroSW1.22 # show iparp "henkilosto"
VR            Destination      Mac                Age  Static  VLAN          VID   Port

Dynamic Entries  :           0            Static Entries           :          2
Pending Entries  :           0
In Request       :         656            In Response              :         49
Out Request      :          49            Out Response             :        141
Failed Requests  :           2
Proxy Answered   :           0
Rx Error         :           0            Dup IP Addr              :      0.0.0.0
Rejected Count   :          48            Rejected IP              :  192.168.20.100
Rejected Port    :          11            Rejected I/F             : tuotanto

Max ARP entries  :        8192            Max ARP pending entries  :        256
ARP address check:     Enabled            ARP refresh              :    Enabled
Timeout          :          20 minutes     ARP Sender-Mac Learning  :   Disabled
```

KUVIO 70. show iparp tuotanto | henkilosto

10.3.4 Source IP Lockdown

Source IP Lockdown –ominaisuus testattiin hakemalla tietokoneelle ensiksi IP-osoite DHCP-palvelimelta, jonka jälkeen tietokoneen IP-osoite muutettiin staattiseksi. DHCP-palvelimelta saatu osoite näkyy MetroSW1-kytkimellä *show ip-security source-ip-lockdown* –komennolla. Kuviosta 71 nähdään, että tietokone, joka on kytketty raja-pintaan 16, on saanut IP-osoitteeksi 192.168.50.10.

```
* MetroSW1.2 # show ip-security source-ip-lockdown
Ports           Locked IP Address
16              192.168.50.10
17              None
18              192.168.50.11
19              None
20              None
21              None
```

KUVIO 71. show ip-security source-ip-lockdown

Kun tietokone oli saanut DHCP-palvelimelta IP-osoitteen, testattiin yhteyden toiminta pingaamalla oletusyhdyskäytävään, jonka jälkeen IP-osoite muutettiin staattiseksi ja oletusyhdyskäytävää pingattiin uudelleen (Ks. kuvio 72). Staattisella IP-osoitteella pingi ei kulje, koska MetroSW1-kytkin on sallinut ainoastaan 192.168.50.10 IP-osoitteen rajapinnalla 16.

```
C:\Documents and Settings\Admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.50.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.50.1

C:\Documents and Settings\Admin>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:

Reply from 192.168.50.1: bytes=32 time=14ms TTL=64
Reply from 192.168.50.1: bytes=32 time=10ms TTL=64
Reply from 192.168.50.1: bytes=32 time=9ms TTL=64
Reply from 192.168.50.1: bytes=32 time=9ms TTL=64

Ping statistics for 192.168.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 14ms, Average = 10ms

C:\Documents and Settings\Admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.50.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.50.1

C:\Documents and Settings\Admin>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.50.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

KUVIO 72. Source IP Lockdown testaus

10.3.5 Gratuitous ARP

Gratuitous ARP -toiminto konfiguroitiin MetroCore1-kytkimelle, joka toimi kaikille VLANeille oletusyhdyskäytävänä. Testauksessa MetroSW1-kytkimeen liitettiin tietokone, jolla verkkoon lähetettiin oma gratuitous ARP –paketti MetroSW1-kytkimen IP:llä.

Ensimmäisessä testissä käytettiin henkilosto-VLANia, jolle Gratuitous ARP –ominaisuutta ei otettu käyttöön. Kuviosta 73 nähdään WireShark-kaappaus, johon peilattiin liikennettä MetroSW1 ja MetroCore1 väliseltä linkiltä sekä MetroSW1 ja ”hyökkäävän” tietokoneen väliseltä linkiltä. Kuviosta nähdään, että kun tietokone lähettää MetroCore1-kytkimen IP:llä gratuitous ARP-paketin ei kytkin reagoi tähän. Tällöin VLANissa olevat tietokoneet lähettävät verkosta ulos suuntautuvan liikenteensä hyökkäävälle tietokoneelle.

```
304 141.042323 HewlettP_93:56:d9  Broadcast          ARP          64 Gratuitous ARP for 192.168.50.1 (Request)
307 142.044983 HewlettP_93:56:d9  Broadcast          ARP          64 Gratuitous ARP for 192.168.50.1 (Request)
```

KUVIO 73. Gratuitous ARP henkilosto

Toinen testi suoritettiin tuotanto-VLANissa, jolle Gratuitous ARP-ominaisuus otettiin käyttöön. WireShark-kaappauksesta nähdään, että kun ”hyökkäävä”-tietokone lähettää gratuitous ARP-paketin, reagoi MetroCore1 kytkin tähän välittömästi lähettämällä oman gratuitous ARP-paketin (Ks. kuvio 74).

```
Source                Destination  Protocol  Info
HewlettP_93:56:d9     Broadcast    ARP       Gratuitous ARP for 192.168.20.1 (Request)
ExtremeN_1e:ab:f0     Broadcast    ARP       Gratuitous ARP for 192.168.20.1 (Request) (duplicate use of 192.168.20.1 detected!)
```

KUVIO 74. Gratuitous ARP tuotanto

MetroCore1-kytkimeltä toiminta nähdään *show iparp security*-komennolla. Komennon tulosteesta nähdään, että tuotanto-VLANissa on tapahtunut rikkomus, joka on lähtöisin 18:a9:05:93:56:d9 MAC-osoitteesta (”hyökkäävä tietokone”) (Ks. kuvio 75).

```
* MetroCore1.8 # show iparp security

                                                    Most Recent Violation
                                                    =====================
Vlan              Security   Violations  Type   IP address        MAC                Port
=================================================================================================
Default           G---              0
hallinta          G---              0
vieraat           G---              0
palvelimet        G---              0
tuotanto          G---              2     g    192.168.20.1      18:a9:05:93:56:d9  1:3
henkilosto        ----

Security Setting: (G) Gratuitous ARP Protection
Violation Type  : (g) Gratuitous ARP Violation
```

KUVIO 75. show iparp security

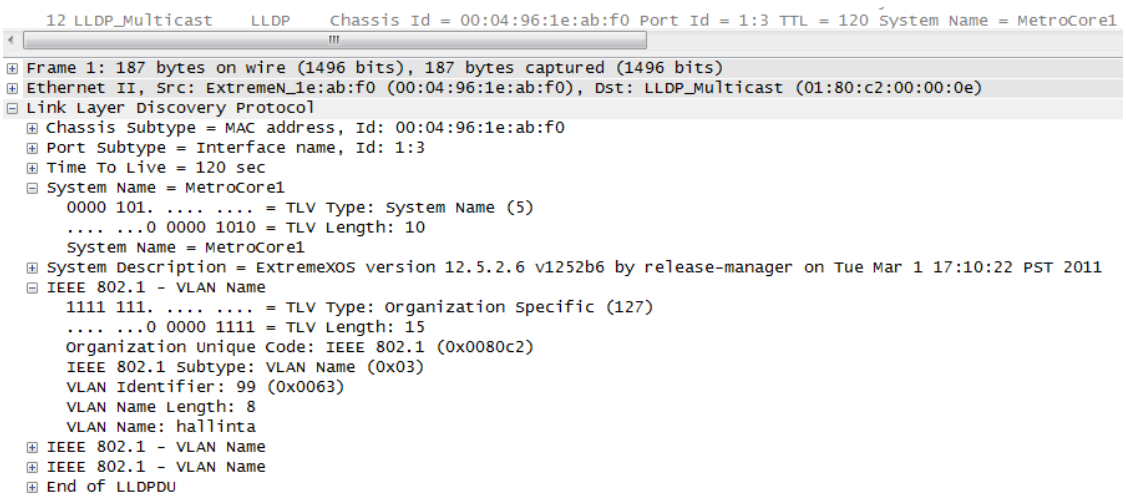
10.4 LLDP

LLDP konfiguroitiin kaikille Extreme Networksin kytkimille. Tarkoituksena oli konfiguroida LLDP myös WG5-SW1-kytkimellä, mutta kytkimen IOS-käyttöjärjestelmän versio ei tukenut LLDP:tä. LLDP määritettiin mainostamaan laitteen nimeä sekä laitteella sijaitsevia VLANeja. LLDP konfiguraatio pystytään näkemään kytkimeltä *show lldp*-komennolla (Ks. kuvio 76). Kuviosta nähdään, että konfiguroitujen TLV:eiden lisäksi Extreme Networksin kytkimet mainostavat oletuksena System Description TVL:ää.

```
* MetroCore1.2 # show lldp

LLDP transmit interval           : 30 seconds
LLDP transmit hold multiplier    : 4  (used TTL = 120 seconds)
LLDP transmit delay              : 2 seconds
LLDP SNMP notification interval  : 5 seconds
LLDP reinitialize delay          : 2 seconds
LLDP-MED fast start repeat count : 3

LLDP Port Configuration:

Port    Rx        Tx        SNMP          Optional enabled transmit TLVs
        Mode      Mode      Notification  LLDP   802.1  802.3  MED   AvEx
================================================================================
1:3     Enabled   Enabled   --            -ND--  --N    ----   ----  ----
1:4     Enabled   Enabled   --            -ND--  --N    ----   ----  ----
1:6     Enabled   Enabled   --            -ND--  --N    ----   ----  ----
================================================================================
Notification: (L) lldpRemTablesChange, (M) lldpXMedTopologyChangeDetected
LLDP Flags  : (P) Port Description, (N) System Name, (D) System Description
              (C) System Capabilities, (M) Mgmt Address
802.1 Flags : (P) Port VLAN ID, (p) Port & Protocol VLAN ID, (N) VLAN Name
802.3 Flags : (M) MAC/PHY Configuration/Status, (P) Power via MDI
              (+) Power via MDI with DLL Classification for PoE+,
              (L) Link Aggregation, (F) Frame Size
MED Flags   : (C) MED Capabilities, (P) Network Policy,
              (L) Location Identification, (p) Extended Power-via-MDI
AvEx Flags  : (P) PoE Conservation Request, (C) Call Server, (F) File Server
              (Q) 802.1Q Framing
```

KUVIO 76. show lldp

Kuviossa 77 nähdään WireShark-kaappaus MetroCore1-kytkimen lähettämästä LLDP-paketista. LLDP-paketti pitää sisällään aiemman kuvion osoittamien TLV:eiden lisäksi myös LLDP:n vaatimat pakolliset TLV:t. Nämä olivat Chassis ID TLV, Port ID TLV, Time To Live TLV ja End of LLDPDU TLV.



KUVIO 77. LLDP-paketti

LLDP naapureiden lähettämät tiedot nähdään Extreme Networksin kytkimillä *show lldp neighbors detail*-komennolla. Kuviossa 78 on kyseisen komennon tuloste Metro-Core1-kytkimeltä.

```
* MetroCore1.3 # show lldp neighbors detailed

--------------------------------------------------------------------------------
LLDP Port 1:3 detected 1 neighbor
  Neighbor: 00:04:96:28:35:C9/25, age 9 seconds
    - Chassis ID type: MAC address (4)
      Chassis ID     : 00:04:96:28:35:C9
    - Port ID type: ifName (5)
      Port ID     : "25"
    - Time To Live: 120 seconds
    - System Name: "MetroSW1"
    - System Description: "ExtremeXOS version 12.5.2.6 v1252b6 by release-ma\
                           nager on Tue Mar 1 17:38:45 PST 2011"
    - IEEE802.1 VLAN Name: "hallinta", VLAN ID: 99
    - IEEE802.1 VLAN Name: "tuotanto", VLAN ID: 20
    - IEEE802.1 VLAN Name: "henkilosto", VLAN ID: 50

--------------------------------------------------------------------------------
LLDP Port 1:4 detected 1 neighbor
  Neighbor: 00:04:96:28:36:FF/26, age 12 seconds
    - Chassis ID type: MAC address (4)
      Chassis ID     : 00:04:96:28:36:FF
    - Port ID type: ifName (5)
      Port ID     : "26"
    - Time To Live: 120 seconds
    - System Name: "MetroSW5"
    - System Description: "ExtremeXOS version 12.5.2.6 v1252b6 by release-ma\
                           nager on Tue Mar 1 17:38:45 PST 2011"
    - IEEE802.1 VLAN Name: "hallinta", VLAN ID: 99
    - IEEE802.1 VLAN Name: "servernetwork", VLAN ID: 60
    - IEEE802.1 VLAN Name: "isoservers", VLAN ID: 601
    - IEEE802.1 VLAN Name: "tuotantoservers", VLAN ID: 620

--------------------------------------------------------------------------------
LLDP Port 1:6 detected 1 neighbor
  Neighbor: 00:04:96:28:35:C4/3, age 22 seconds
    - Chassis ID type: MAC address (4)
      Chassis ID     : 00:04:96:28:35:C4
    - Port ID type: ifName (5)
      Port ID     : "3"
    - Time To Live: 120 seconds
    - System Name: "MetroSW2"
    - System Description: "ExtremeXOS version 12.5.2.6 v1252b6 by release-ma\
                           nager on Tue Mar 1 17:38:45 PST 2011"
    - IEEE802.1 VLAN Name: "hallinta", VLAN ID: 99
    - IEEE802.1 VLAN Name: "vieraat", VLAN ID: 10
    - IEEE802.1 VLAN Name: "tuotanto", VLAN ID: 20
    - IEEE802.1 VLAN Name: "henkilosto", VLAN ID: 50
```

KUVIO 78. show lldp neigbors detailed

10.5 ACL & CLEAR-Flow

CLEAR-Flow konfiguroitiin seuraamaan ja reagoimaan vieraat-VLANista servernet-work-VLANiin menevää liikennettä. CLEAR-FLOWn todentamiseen käytettiin JDSU-liikennegeneraattoria. JDSU asetettiin MetroSW2-kytkimeen vieraat-VLANiin ja JDSU:n päätepisteet sijoitettiin MetroSW5-kytkimelle. JDSU:lla lähetettiin 1 Mbps liikennevirtaa, jolloin paketteja liikkui reilut 2000 kappaletta kymmenessä sekunnissa (Ks. kuvio 79).

```
* MetroCore1.56 # show clear-flow port 1:6
Rule Name        Period   Type Last           Rel  Threshold      TCNT NumAction
                                Value          Oper                    If   Else
================================================================================
cflow_vieraat      10       DT 2259           >=   5000.000000    0    1    1
================================================================================
Total Entries: 1

Notation:
Threshold Type: CN - Count, DT - Delta, RT - Ratio, DR - DeltaRatio
TCNT - Number of times expression is continously evaluated to be true
```

KUVIO 79. show clear-flow port 1:6

Kun JDSU:lle lisättiin toinen yhtä suuri liikennevirta, ylittyi CLEAR-FLOW:hun määritetty raja-arvo ja CLEAR-Flow katkaisi vieras-VLANista servernetwork-VLANiin menevän liikenteen (Ks. kuvio 80).

```
* MetroCore1.56 # show clear-flow port 1:6
Rule Name        Period   Type Last           Rel  Threshold      TCNT NumAction
                                Value          Oper                    If   Else
================================================================================
cflow_vieraat      10       DT 6766           >=   5000.000000    5    1    1
================================================================================
Total Entries: 1

Notation:
Threshold Type: CN - Count, DT - Delta, RT - Ratio, DR - DeltaRatio
TCNT - Number of times expression is continously evaluated to be true
```

KUVIO 80. show clear-flow port 1:6 (2)

11 YHTEENVETO

11.1 Opinnäytetyön toteutus

Opinnäytetyön tekemisen aloitin tutustumalla Extreme Networksin ExtremeXOS-käyttöjärjestelmään sekä tutustumalla työssä tutkittaviin tekniikoihin. Ennen opinnäytetyötä oli käyttänyt Extreme Networksin laitteita opintoihini kuuluvissa WAN-tekniikat- ja QoS -opintojaksoilla. Kun olin saanut yleiskuvan tutkittavista tekniikoista, aloin suunnittelemaan opinnäytetyössä käytettävää topologiaa. Suunnitelman olisi voinut tehdä tarkemmin, koska alkuperäinen topologia muuttui useampaan otteeseen muun muassa tekniikoiden yhteensopimattomuuden takia.

Opinnäytetyön alussa oli tarkoitus myös testata tekniikoita enemmän Cisco Systemsin kytkimillä. Opinnäytetyön aikana kuitenkin huomasin, että Cisco Systemsin kytkimet eivät tukeneet suurintaosaa opinnäytetyössä tutkittavista tekniikoista. Tämän takia testasin ainoastaan 802.1X-tekniikan Extreme Networksin ja Cisco Systemsin kytkimillä.

Konfiguroinnin aloitin samanaikaisesti teorian kirjoittamisen kanssa. Näin jälkikäteen ajatellen olisi ollut parempi, jos olisin tehnyt teoriaosuuden ensin ja vasta sen jälkeen siirtynyt käytännönosuuteen. Tällöin minulle olisi tullut varmasti vähemmän virheitä konfiguroidessa ja työssä käytettyjen tekniikoiden yleiskuva olisi ollut parempi. Toisaalta tästä johtuneet virheet opettivat myös paljon ja auttoivat minua ymmärtämään tekniikoita paremmin.

11.2 Tulokset

Opinnäytetyössä käytetyt tietoturvaominaisuudet saatiin testattua ja todennettua alussa asetettujen tavoitteiden mukaisesti. Työntuloksena syntyi L2-tason verkon lisäksi kaksi laboratorioharjoitusta, jotka tulevat tukemaan seuraavien tietoverkkoinsinööri opiskelijoiden koulutusta. Laboratorioharjoitukset keskittyivät PVLAN, 802.1X ja MAC- & IP-security ominaisuuksiin.

Työssä tutkituista tekniikoista mielenkiintoisin minusta oli Private VLAN. PVLANin toiminta on hyvin yksinkertaista, mutta sillä voidaan parantaa paljon skaalautuvuutta verrattuna normaaleihin VLANeihin. Lisäksi PVLAN tuo lisää tietoturvallisuutta verkkoon erottamalla päätelaitteet toisistaan OSI-mallin siirtokerroksella. Uskonkin, että PVLAN tulee yleistymään tulevaisuudessa. LLDP ei ollut tietoturvaa lisäävä tekniikka kuten muut. LLDP:tä käytettäessä on varmistettava, että LLDP-viestit kulkevat suojatussa ja eristetyssä verkossa, ettei ulkopuoliset näe viestejä. Viestit ovat selkokielisiä, jolloin ulkopuolinen voi saada kriittistä tietoa verkosta. 802.1X-standardia käytetään nykyään pääsääntöisesti langattomissa verkoissa. Uskon kuitenkin sen tuovan myös langallisiin verkkoihin lisäarvoa nousevan turvallisuuden myöten.

LÄHTEET

Brown Edvin Lyle. 2008. 802.1X Port-Based Authentication. New York: Auerbach Publications

Extreme Networks. 2006. Extreme Networks Technical Brief: Link Layer Discovery Protocol.

Extreme Networks. 2011a. Extreme Networks yrityksenä. Viitattu 10.10.2011. http://www.extremenetworks.com/about-extreme/default.aspx

Extreme Networks. 2011b. Extreme Networksin laitteet. Viitattu 17.3.2012 http://extremenetworks.com/products/products-hub.aspx

Extreme Networks. 2011c. ExtremeXOS. Viitattu 17.3.2012 http://www.extremenetworks.com/products/extreme-xos.aspx

Extreme Networks. 2011d. ExtremeXOS Concepts Guide Software Version 12.5.3. Viitattu 19.3.2012

Foschiano, M. & HomChaudhuri, S. 2010. RFC 5517 Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment. IETF Tools.

Geier Jim. 2008. Implementing 802.1X Security Solutions for Wired and Wireless Networks. Indianapolis: Wiley Publishing.

Hill Joshua. 2001. An Analysis of the RADIUS Authentication Protocol. Viitattu 9.1.2012. http://www.untruth.org/~josh/security/radius/radius-auth.html

IEEE 802.1AB. 2009. Station and Media Access Control Connectivity Discovery. Viitattu 1.4.2012.

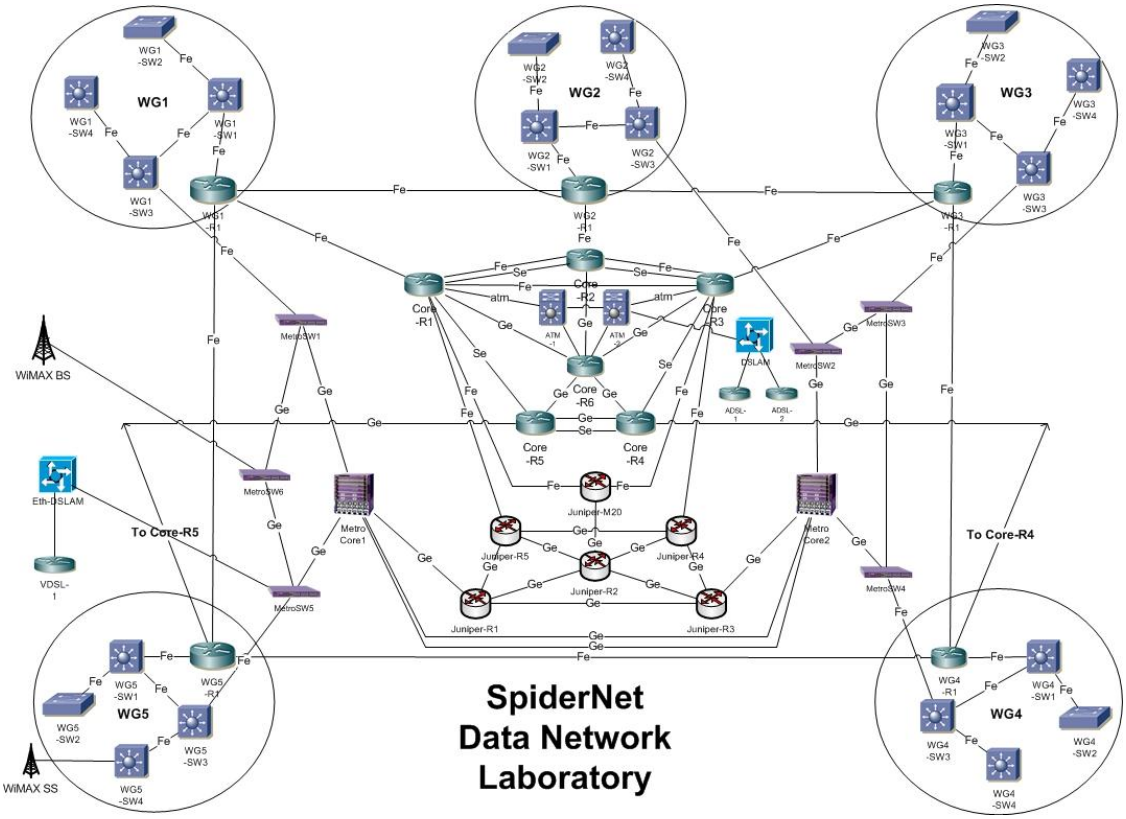
Jyväskylän ammattikorkeakoulu. 2012a. Tutustu JAMKiin. Viitattu 20.1.2012. Http://www.jamk.fi, tutustu.

Jyväskylän ammattikorkeakoulu. 2012b. Opiskelijalle. Viitattu 20.1.2012. Http://www.jamk.fi, Opinto-opas, AMK-tutkinto.

Labranet. 2011. SpiderNet. Viitattu 30.10.2011. http://student.labranet.jamk.fi/SpiderNet/

LIITTEET

Liite1: SpiderNet-topologia



Liite2: MetroCore1-kytkimen konfiguraatiot

```
#
# Module devmgr configuration.
#
configure snmp sysName "MetroCore1"
configure slot 1 module GM-20XTR
configure sys-recovery-level slot 1 reset
#
# Module vlan configuration.
#
configure vlan default delete ports all
configure vr VR-Default delete ports 1:1-20
configure vr VR-Default add ports 1:1-20
configure vlan default delete ports 1:1-20
create vlan "hallinta"
configure vlan hallinta tag 99
create vlan "henkilosto"
configure vlan henkilosto tag 50
create vlan "servernetwork"
configure vlan servernetwork tag 60
create vlan "tuotanto"
configure vlan tuotanto tag 20
enable iparp gratuitous inspection vlan tuotanto
create vlan "vieraat"
configure vlan vieraat tag 10
enable iparp gratuitous inspection vlan vieraat
disable port 1:1
disable port 1:2
configure ports 1:3 display-string TO-MetroSW1
configure ports 1:4 display-string TO-MetroSW5
disable port 1:5
configure ports 1:6 display-string TO-MetroSW2
disable port 1:7
disable port 1:8
disable port 1:9
configure ports 1:9 display-string MirrorPort
disable port 1:10
disable port 1:11
disable port 1:12
disable port 1:13
disable port 1:14
disable port 1:15
disable port 1:16
disable port 1:17
disable port 1:18
disable port 1:19
disable port 1:20
configure vlan hallinta add ports 1:3-4, 1:6 tagged
configure vlan henkilosto add ports 1:3, 1:6 tagged
configure vlan servernetwork add ports 1:4 tagged
configure vlan tuotanto add ports 1:3, 1:6 tagged
configure vlan vieraat add ports 1:6 tagged
configure vlan hallinta ipaddress 192.168.99.1 255.255.255.0
configure vlan vieraat ipaddress 192.168.10.1 255.255.255.0
```

```
configure vlan tuotanto ipaddress 192.168.20.1 255.255.255.0
configure vlan henkilosto ipaddress 192.168.50.1 255.255.255.0
configure vlan servernetwork ipaddress 192.168.60.1 255.255.255.0
#
# Module fdb configuration.
#
# Module rtmgr configuration.
#
# Module mcmgr configuration.
#
# Module aaa configuration.
#
# Module acl configuration.
#
# Module bfd configuration.
#
# Module bgp configuration.
#
# Module cfgmgr configuration.
#
# Module dosprotect configuration.
#
# Module dot1ag configuration.
#
# Module eaps configuration.
#
# Module edp configuration.
#
# Module elrp configuration.
#
# Module ems configuration.
#
# Module epm configuration.
#
# Module esrp configuration.
#
# Module etmon configuration.
#
# Module hal configuration.
#
# Module idMgr configuration.
#
# Module ipSecurity configuration.
#
enable ip-security arp gratuitous-protection vlan tuotanto
enable ip-security arp gratuitous-protection vlan vieraat
#
# Module isis configuration.
#
# Module lldp configuration.
#
enable lldp ports 1:3
configure lldp port 1:3 advertise system-name
configure lldp port 1:3 advertise vendor-specific dot1 vlan-name
enable lldp ports 1:4
configure lldp port 1:4 advertise system-name
configure lldp port 1:4 advertise vendor-specific dot1 vlan-name
```

```
enable lldp ports 1:6
configure lldp port 1:6 advertise system-name
configure lldp port 1:6 advertise vendor-specific dot1 vlan-name
#
# Module msdp configuration.
#
# Module netLogin configuration.
#
# Module netTools configuration.
#
configure vlan henkilosto dhcp-address-range 192.168.50.10 - 192.168.50.254
configure vlan henkilosto dhcp-options default-gateway 192.168.50.1
enable dhcp ports 1:3, 1:6 vlan henkilosto
configure vlan tuotanto dhcp-address-range 192.168.20.10 - 192.168.20.254
configure vlan tuotanto dhcp-options default-gateway 192.168.20.1
enable dhcp ports 1:3, 1:6 vlan tuotanto
configure vlan vieraat dhcp-address-range 192.168.10.10 - 192.168.10.254
configure vlan vieraat dhcp-options default-gateway 192.168.10.1
enable dhcp ports 1:6 vlan vieraat
#
# Module ospf configuration.
#
# Module ospfv3 configuration.
#
# Module pim configuration.
#
# Module rip configuration.
# Module ripng configuration.
#
# Module snmpMaster configuration.
#
# Module stp configuration.
#
configure mstp region 0004961eabf0
configure stpd s0 delete vlan default ports all
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan Default
#
# Module telnetd configuration.
#
# Module tftpd configuration.
#
# Module thttpd configuration.
#
# Module vmt configuration.
#
# Module vrrp configuration.
```

Liite3: MetroSW1-kytkimen konfiguraatiot

```
#
# Module devmgr configuration.
#
configure snmp sysName "MetroSW1"
configure sys-recovery-level switch reset
#
# Module vlan configuration.
#
configure vlan default delete ports all
configure vr VR-Default delete ports 1-26
configure vr VR-Default add ports 1-26
configure vlan default delete ports 1-26
enable mirroring to port 9
create vlan "hallinta"
configure vlan hallinta tag 99
create vlan "henkilosto"
configure vlan henkilosto tag 50
create vlan "tuotanto"
configure vlan tuotanto tag 20
disable port 1
disable port 2
disable port 3
disable port 4
disable port 5
disable port 6
disable port 7
disable port 8
disable port 10
disable port 11
disable port 12
disable port 13
disable port 14
disable port 15
disable port 16
disable port 17
disable port 18
disable port 19
disable port 20
disable port 21
disable port 22
disable port 23
disable port 24
disable port 26
configure vlan hallinta add ports 25 tagged
configure vlan henkilosto add ports 25 tagged
configure vlan henkilosto add ports 16-21 untagged
configure vlan tuotanto add ports 25 tagged
configure vlan tuotanto add ports 10-15 untagged
configure vlan hallinta ipaddress 192.168.99.11 255.255.255.0
configure port 10 vlan tuotanto limit-learning 2
disable iparp learning vlan tuotanto port 10
configure port 11 vlan tuotanto limit-learning 2
disable iparp learning vlan tuotanto port 11
```

```
configure port 12 vlan tuotanto limit-learning 2
disable iparp learning vlan tuotanto port 12
configure port 13 vlan tuotanto limit-learning 2
disable iparp learning vlan tuotanto port 13
configure port 14 vlan tuotanto limit-learning 2
disable iparp learning vlan tuotanto port 14
configure port 15 vlan tuotanto limit-learning 2
disable iparp learning vlan tuotanto port 15
configure port 16 vlan henkilosto limit-learning 1 action stop-learning
configure port 17 vlan henkilosto limit-learning 1 action stop-learning
configure port 18 vlan henkilosto limit-learning 1 action stop-learning
configure port 19 vlan henkilosto limit-learning 1 action stop-learning
configure port 20 vlan henkilosto limit-learning 1 action stop-learning
configure port 21 vlan henkilosto limit-learning 1 action stop-learning
configure mirroring add port 25 ingress-and-egress
#
# Module fdb configuration.
#
# Module rtmgr configuration.
#
# Module mcmgr configuration.
#
# Module aaa configuration.
#
# Module acl configuration.
#
# Module bfd configuration.
#
# Module cfgmgr configuration.
#
# Module dosprotect configuration.
#
# Module dot1ag configuration.
#
# Module eaps configuration.
#
# Module edp configuration.
#
# Module elrp configuration.
#
# Module ems configuration.
#
# Module epm configuration.
#
# Module esrp configuration.
#
# Module ethoam configuration.
#
# Module etmon configuration.
#
# Module hal configuration.
#
# Module idMgr configuration.
#
# Module ipSecurity configuration.
#
```

```
enable ip-security dhcp-snooping vlan henkilosto port 16 violation-action drop-packet block-mac dura-
tion 60
enable ip-security dhcp-snooping vlan henkilosto port 17 violation-action drop-packet block-mac dura-
tion 60
enable ip-security dhcp-snooping vlan henkilosto port 18 violation-action drop-packet block-mac dura-
tion 60
enable ip-security dhcp-snooping vlan henkilosto port 19 violation-action drop-packet block-mac dura-
tion 60
enable ip-security dhcp-snooping vlan henkilosto port 20 violation-action drop-packet block-mac dura-
tion 60
enable ip-security dhcp-snooping vlan henkilosto port 21 violation-action drop-packet block-mac dura-
tion 60
enable ip-security dhcp-snooping vlan henkilosto port 25 violation-action drop-packet block-mac dura-
tion 60
enable ip-security dhcp-snooping vlan tuotanto port 10 violation-action drop-packet
enable ip-security dhcp-snooping vlan tuotanto port 11 violation-action drop-packet
enable ip-security dhcp-snooping vlan tuotanto port 12 violation-action drop-packet
enable ip-security dhcp-snooping vlan tuotanto port 13 violation-action drop-packet
enable ip-security dhcp-snooping vlan tuotanto port 14 violation-action drop-packet
enable ip-security dhcp-snooping vlan tuotanto port 15 violation-action drop-packet
enable ip-security dhcp-snooping vlan tuotanto port 25 violation-action drop-packet
configure trusted-servers vlan tuotanto add server 192.168.20.1 trust-for dhcp-server
configure trusted-servers vlan tuotanto add server 192.168.50.1 trust-for dhcp-server
enable ip-security source-ip-lockdown ports 16-21
enable ip-security arp learning learn-from-dhcp vlan tuotanto ports 10
enable ip-security arp learning learn-from-dhcp vlan tuotanto ports 11
enable ip-security arp learning learn-from-dhcp vlan tuotanto ports 12
enable ip-security arp learning learn-from-dhcp vlan tuotanto ports 13
enable ip-security arp learning learn-from-dhcp vlan tuotanto ports 14
enable ip-security arp learning learn-from-dhcp vlan tuotanto ports 15
enable ip-security arp learning learn-from-arp vlan tuotanto ports 25
#
# Module ipfix configuration.
#
# Module lldp configuration.
#
enable lldp ports 25
configure lldp port 25 advertise system-name
configure lldp port 25 advertise vendor-specific dot1 vlan-name
# Module msdp configuration.
#
# Module netLogin configuration.
#
# Module netTools configuration.
#
# Module ospf configuration.
#
configure ospf vlan hallinta priority 0
#
# Module ospfv3 configuration.
#
# Module pim configuration.
#
# Module poe configuration.
#
# Module rip configuration.
#
```

```
# Module ripng configuration.
#

# Module snmpMaster configuration.
#
# Module stp configuration.
#
configure mstp region 0004962835c9
configure stpd s0 delete vlan default ports all
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan Default
#
# Module telnetd configuration.
#
# Module tftpd configuration.
#
# Module thttpd configuration.
#
# Module vmt configuration.
#
# Module vrrp configuration.
#
# Module vsm configuration.
#
```

Liite 4. MetroSW2-kytkimen konfiguraatiot

```
#
# Module devmgr configuration.
#
configure snmp sysName "MetroSW2"
configure sys-recovery-level switch reset
#
# Module vlan configuration.
#
configure vlan default delete ports all
configure vr VR-Default delete ports 1-26
configure vr VR-Default add ports 1-26
configure vlan default delete ports 1-26
create vlan "hallinta"
configure vlan hallinta tag 99
create vlan "henkilosto"
configure vlan henkilosto tag 50
create vlan "temp"
configure vlan temp tag 5
create vlan "tuotanto"
configure vlan tuotanto tag 20
create vlan "vieraat"
configure vlan vieraat tag 10
disable port 1
disable port 2
configure ports 3 display-string TO-MetroCore1
disable port 4
disable port 5
disable port 6
disable port 7
disable port 8
disable port 9
configure ports 9 display-string MirrorPort
disable port 10
configure ports 10 display-string UserAccess_Guest
disable port 11
configure ports 11 display-string UserAccess_Guest
disable port 12
configure ports 12 display-string UserAccess_Guest
disable port 13
configure ports 13 display-string UserAccess_Guest
disable port 14
configure ports 14 display-string UserAccess_Guest
disable port 15
configure ports 15 display-string UserAccess_Guest
disable port 16
configure ports 16 display-string UserAccess
disable port 17
configure ports 17 display-string UserAccess
disable port 18
configure ports 18 display-string UserAccess
disable port 19
configure ports 19 display-string UserAccess
```

```
disable port 20
configure ports 20 display-string UserAccess
disable port 21
configure ports 21 display-string UserAccess
disable port 22
configure ports 22 display-string UserAccess
disable port 23
configure ports 23 display-string UserAccess
disable port 24
configure ports 24 display-string UserAccess
disable port 25
disable port 26
configure vlan hallinta add ports 3-4 tagged
configure vlan henkilosto add ports 3-4 tagged
configure vlan tuotanto add ports 3-4 tagged
configure vlan vieraat add ports 3-4 tagged
configure vlan hallinta ipaddress 192.168.99.12 255.255.255.0
#
# Module fdb configuration.
#
# Module rtmgr configuration.
#
# Module mcmgr configuration.
#
# Module aaa configuration.
#
configure radius netlogin primary server 192.168.99.99 1812 client-ip 192.168.99.12 vr VR-Default
configure radius netlogin primary shared-secret encrypted "pcf~&lt;7"
enable radius mgmt-access
enable radius netlogin
# Module acl configuration.
#
# Module bfd configuration.
#
# Module cfgmgr configuration.
#
# Module dosprotect configuration.
#
# Module dot1ag configuration.
#
# Module eaps configuration.
#
# Module edp configuration.
#
# Module elrp configuration.
#
# Module ems configuration.
#
# Module epm configuration.
#
# Module esrp configuration.
#
# Module ethoam configuration.
#
# Module etmon configuration.
#
# Module hal configuration.
```

```
#
# Module idMgr configuration.
#
# Module ipSecurity configuration.
#
# Module ipfix configuration.
#
# Module lldp configuration.
#
enable lldp ports 3
configure lldp port 3 advertise system-name
configure lldp port 3 advertise vendor-specific dot1 vlan-name
#
# Module msdp configuration.
#
#
# Module netLogin configuration.
#
configure netlogin vlan temp
enable netlogin dot1x
enable netlogin ports 10-24 dot1x
configure netlogin ports 10 mode port-based-vlans
configure netlogin ports 10 no-restart
configure netlogin ports 11 mode port-based-vlans
configure netlogin ports 11 no-restart
configure netlogin ports 12 mode port-based-vlans
configure netlogin ports 12 no-restart
configure netlogin ports 13 mode port-based-vlans
configure netlogin ports 13 no-restart
configure netlogin ports 14 mode port-based-vlans
configure netlogin ports 14 no-restart
configure netlogin ports 15 mode port-based-vlans
configure netlogin ports 15 no-restart
configure netlogin ports 16 mode port-based-vlans
configure netlogin ports 16 no-restart
configure netlogin ports 17 mode port-based-vlans
configure netlogin ports 17 no-restart
configure netlogin ports 18 mode port-based-vlans
configure netlogin ports 18 no-restart
configure netlogin ports 19 mode port-based-vlans
configure netlogin ports 19 no-restart
configure netlogin ports 20 mode port-based-vlans
configure netlogin ports 20 no-restart
configure netlogin ports 21 mode port-based-vlans
configure netlogin ports 21 no-restart
configure netlogin ports 22 mode port-based-vlans
configure netlogin ports 22 no-restart
configure netlogin ports 23 mode port-based-vlans
configure netlogin ports 23 no-restart
configure netlogin ports 24 mode port-based-vlans
configure netlogin ports 24 no-restart
enable netlogin dot1x guest-vlan ports 10-15
enable netlogin authentication failure vlan ports 10-15
configure netlogin dot1x guest-vlan vieraat ports 10-15
configure netlogin authentication failure vlan vieraat ports 10-15
#
# Module netTools configuration.
```

```
#

#
# Module ospf configuration.
#
configure ospf vlan hallinta priority 0
#
# Module ospfv3 configuration.
#
# Module pim configuration.
#
# Module poe configuration.
#
# Module rip configuration.
#
# Module ripng configuration.
#
# Module snmpMaster configuration.
#
# Module stp configuration.
#
configure mstp region 0004962835c4
configure stpd s0 delete vlan default ports all
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan Default
#
# Module telnetd configuration.
#
# Module tftpd configuration.
#
# Module thttpd configuration.
#
# Module vmt configuration.
#
# Module vrrp configuration.
#
# Module vsm configuration.
#
```

Liite 4. MetroSW5-kytkimen konfiguraatiot

```
#
# Module devmgr configuration.
#
configure snmp sysName "MetroSW5"
configure sys-recovery-level switch reset
#
# Module vlan configuration.
#
configure vlan default delete ports all
configure vr VR-Default delete ports 1-26
configure vr VR-Default add ports 1-26
configure vlan default delete ports 1-26
create vlan "hallinta"
configure vlan hallinta tag 99
create vlan "isoservers"
configure vlan isoservers tag 601
create vlan "servernetwork"
configure vlan servernetwork tag 60
create vlan "tuotantoservers"
configure vlan tuotantoservers tag 620
disable port 1
disable learning port 1
disable port 2
disable port 3
disable port 4
disable port 5
disable port 6
disable port 7
disable port 8
disable port 9
configure ports 9 display-string MirrorPort
disable port 10
disable port 11
disable port 12
disable port 13
disable port 14
disable port 15
configure ports 15 display-string HenkilostoPalvelin
disable port 16
disable port 17
disable port 18
disable port 19
disable port 20
configure ports 20 display-string TuotantoPalvelin
disable port 21
disable port 22
disable port 23
disable port 24
configure ports 24 display-string Radius
configure ports 25 display-string To-MetroSW6
configure ports 26 display-string TO-MetroCore1
create private-vlan "palvelimet"
```

```
configure private-vlan palvelimet add network servernetwork
configure private-vlan palvelimet add subscriber tuotantoservers non-isolated loopback-port 1
configure private-vlan palvelimet add subscriber isoservers
configure vlan hallinta add ports 25-26 tagged
configure vlan hallinta add ports 24 untagged
configure vlan isoservers add ports 25 tagged
configure vlan isoservers add ports 15 untagged
configure vlan servernetwork add ports 26 private-vlan translated
configure vlan tuotantoservers add ports 1, 25 tagged
configure vlan tuotantoservers add ports 20 untagged
configure vlan hallinta ipaddress 192.168.99.15 255.255.255.0
#
# Module fdb configuration.
#
# Module rtmgr configuration.
#
# Module mcmgr configuration.
#
# Module aaa configuration.
#
# Module acl configuration.
#
# Module bfd configuration.
#
# Module cfgmgr configuration.
#
# Module dosprotect configuration.
#
# Module dot1ag configuration.
#
# Module eaps configuration.
#
# Module edp configuration.
#
disable edp ports 1
#
# Module elrp configuration.
#
# Module ems configuration.
#
# Module epm configuration.
#
# Module esrp configuration.
#
# Module ethoam configuration.
#
# Module etmon configuration.
#
# Module hal configuration.
#
# Module idMgr configuration.
#
# Module ipSecurity configuration.
#
# Module ipfix configuration.
#
# Module lldp configuration.
```

```
#
enable lldp ports 25
configure lldp port 25 advertise system-name
configure lldp port 25 advertise vendor-specific dot1 vlan-name
enable lldp ports 26
configure lldp port 26 advertise system-name
configure lldp port 26 advertise vendor-specific dot1 vlan-name
#
# Module msdp configuration.
#
# Module netLogin configuration.
#
# Module netTools configuration.
#
# Module ospf configuration.
#
configure ospf vlan hallinta priority 0
#
# Module ospfv3 configuration.
#
# Module pim configuration.
#
# Module poe configuration.
#
# Module rip configuration.
#
# Module ripng configuration.
#
# Module snmpMaster configuration.
#
# Module stp configuration.
#
configure mstp region 0004962836ff
configure stpd s0 delete vlan default ports all
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan Default
#
# Module telnetd configuration.
#
# Module tftpd configuration.
#
# Module thttpd configuration.
#
# Module vmt configuration.
#
# Module vrrp configuration.
#
# Module vsm configuration.
#
```

Liite 5. MetroSW6-kytkimen konfiguraatiot

```
#
# Module devmgr configuration.
#
configure snmp sysName "MetroSW6"
configure sys-recovery-level switch reset
#
# Module vlan configuration.
#
configure vlan default delete ports all
configure vr VR-Default delete ports 1-26
configure vr VR-Default add ports 1-26
configure vlan default delete ports 1-26
create vlan "hallinta"
configure vlan hallinta tag 99
create vlan "isoservers"
configure vlan isoservers tag 601
create vlan "servernetwork"
configure vlan servernetwork tag 60
create vlan "tuotantoservers"
configure vlan tuotantoservers tag 620
disable port 1
disable learning port 1
disable port 2
disable port 3
disable port 4
disable port 5
disable port 6
disable port 7
disable port 8
disable port 9
configure ports 9 display-string MirrorPort
disable port 10
disable port 11
disable port 12
disable port 13
disable port 14
disable port 15
configure ports 15 display-string HenkilostoPalvelin
disable port 16
disable port 17
disable port 18
disable port 19
disable port 20
configure ports 20 display-string TuotantoPalvelin
disable port 21
disable port 22
disable port 23
disable port 24
disable port 25
configure ports 26 display-string TO-MetroSW5
create private-vlan "palvelimet"
configure private-vlan palvelimet add network servernetwork
```

```
configure private-vlan palvelimet add subscriber tuotantoservers non-isolated loopback-port 1
configure private-vlan palvelimet add subscriber isoservers
configure vlan hallinta add ports 26 tagged
configure vlan isoservers add ports 26 tagged
configure vlan isoservers add ports 15 untagged
configure vlan tuotantoservers add ports 1, 26 tagged
configure vlan tuotantoservers add ports 20 untagged
configure vlan hallinta ipaddress 192.168.99.16 255.255.255.0
#
# Module fdb configuration.
#
# Module rtmgr configuration.
#
# Module mcmgr configuration.
#
# Module aaa configuration.
#
# Module acl configuration.
#
# Module bfd configuration.
#
# Module cfgmgr configuration.
#
# Module dosprotect configuration.
#
# Module dot1ag configuration.
#
# Module eaps configuration.
#
# Module edp configuration.
#
disable edp ports 1
#
# Module elrp configuration.
#
# Module ems configuration.
#
# Module epm configuration.
#
# Module esrp configuration.
#
# Module ethoam configuration.
#
# Module etmon configuration.
#
# Module hal configuration.
#
# Module idMgr configuration.
#
# Module ipSecurity configuration.
#

#
# Module ipfix configuration.
#
# Module lldp configuration.
#
```

```
enable lldp ports 26
configure lldp port 26 advertise system-name
configure lldp port 26 advertise vendor-specific dot1 vlan-name
#
# Module msdp configuration.
#
# Module netLogin configuration.
#
# Module netTools configuration.
#
# Module ospf configuration.
#
configure ospf vlan hallinta priority 0
#
# Module ospfv3 configuration.
#
# Module pim configuration.
#
# Module poe configuration.
#
# Module rip configuration.
#
# Module ripng configuration.
#
# Module snmpMaster configuration.
#
# Module stp configuration.
#
configure mstp region 0004963665b6
configure stpd s0 delete vlan default ports all
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan Default
#
# Module telnetd configuration.
#
# Module tftpd configuration.
#
# Module thttpd configuration.
#
# Module vmt configuration.
#
# Module vrrp configuration.
#
# Module vsm configuration.
#
```

Liite 6. WG5-SW1-kytkimen konfiguraatio

```
Building configuration...

Current configuration : 2195 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname wg5-SW1
!
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
dot1x system-auth-control
!
interface GigabitEthernet0/1
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/3
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/4
 switchport mode dynamic desirable
 shutdown
!
interface GigabitEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/6
 description useraccess
 switchport access vlan 20
 switchport mode access
 shutdown
 spanning-tree portfast
!
```

```
interface GigabitEthernet0/7
 description useraccess
 switchport mode access
 dot1x port-control auto
 dot1x guest-vlan 10
 spanning-tree portfast
!
interface GigabitEthernet0/8
 description useraccess
 switchport mode access
 shutdown
 dot1x port-control auto
 dot1x guest-vlan 10
 spanning-tree portfast
!
interface GigabitEthernet0/9
 description useraccess
 switchport mode access
 shutdown
 dot1x port-control auto
 dot1x guest-vlan 10
 spanning-tree portfast
!
interface GigabitEthernet0/10
 description useraccess
 switchport mode access
 shutdown
 dot1x port-control auto
 dot1x guest-vlan 10
 spanning-tree portfast
!
interface GigabitEthernet0/11
 description useraccess
 switchport mode access
 shutdown
 dot1x port-control auto
 dot1x guest-vlan 10
 spanning-tree portfast
!
interface GigabitEthernet0/12
 description useraccess
 switchport mode access
 shutdown
 dot1x port-control auto
 dot1x guest-vlan 10
 spanning-tree portfast
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 192.168.99.51 255.255.255.0
!
ip classless
ip http server
!
```

```
radius-server host 192.168.99.99 auth-port 1812 acct-port 1813
radius-server retransmit 3
radius-server key root66
!
line con 0
line vty 5 15
!
!
```