Petteri Papunen

Ciscon autentikointiratkaisuja
Cisco Secure ACS ja NAC Profiler

Opinnäytetyö
Tietotekniikan koulutusohjelma

Joulukuu 2010

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

KUVAILULEHTI

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Opinnäytetyön päivämäärä** 3.12.2010
Tekijä(t) Petteri Papunen	**Koulutusohjelma ja suuntautuminen** **Tietotekniikan koulutusohjelma**
Nimeke Ciscon Autentikointiratkaisuja: Cisco Secure ACS ja NAC Profiler	

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli tutkia 802.1X-autentikointia verkon reunalla käyttäen kahta Cisco Systems Inc.:n valmistamaa autentikointijärjestelmää. Nämä järjestelmät olivat Cisco Secure Access Control System 5.1, lyhyesti ACS, joka toimi AAA-palvelimena, ja Cisco NAC Profiler, joka profiloi verkon päätelaitteita ja toimi ulkoisena identiteettivarastona.

Työ toteutettiin kahdessa osassa. Ensin tutkittiin ACS:iä autentikointipalvelimena sekä normaalissa 802.1X-autentikoinnissa että MAB-autentikoinnissa, jonka jälkeen keskityttiin NAC Profilerin toimintaan. Profilerista tutkittiin laiteprofiilien tekoa, laitteiden tunnistamista sekä profilointia, ja lopuksi miten Profiler suhtautuu MAC-osoitteen väärentämiseen.

ACS todettiin melko hyväksi AAA-palvelimeksi, sillä sen sääntöpohjainen toimintaperiaate sallii joustavan erilaisten autentikointitapahtumien käsittelyn, ja sen raportointityökalut osoittautuivat erinomaisiksi. NAC Profilerin rooli 802.1X-autentikoinnissa osoittautui odotettua pienemmäksi, sillä se toimii MAB-autentikoinnissa vain ulkoisena identiteettivarastona.

802.1X-autentikointi on hyvä vaihtoehto mille tahansa yritykselle, joka haluaa turvata verkkoympäristönsä, sillä oikein käytettynä se estää luvattomien laitteiden ja käyttäjien liittymisen verkkoon.

Asiasanat (avainsanat) Autentikointi, RADIUS, IEEE 802.1X, MAB, AAA		
Sivumäärä 41+18	**Kieli** suomi	**URN** URN:NBN:fi:amk-2010121518272
Huomautus (huomautukset liitteistä) liitteenä kaksi kytkinkonfiguraatiota		
Ohjaavan opettajan nimi Matti Koivisto	**Opinnäytetyön toimeksiantaja** Saimaan Talous ja Tieto Oy	

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

Date of the bachelor's thesis

December 3th, 2010

Author(s)
Petteri Papunen

Degree programme and option
Degree Program of Information Technology

Name of the bachelor's thesis

Authentication Solutions from Cisco: Cisco Secure ACS and NAC Profiler

Abstract

The main goal of this bachelor's thesis was to examine 802.1X authentication in the fringe of a network using two authentication systems made by Cisco Systems Inc. These two systems were Cisco Secure Access Control System 5.1, shortly ACS, which operated as an AAA server, and Cisco NAC Profiler, which profiled endpoints of a network and worked as an external identity store for ACS.

The thesis was executed in two parts. The first part was to study the functionality of ACS as an authentication server in both 802.1X and MAB authentication. The second part concentrated on the functionality of NAC Profiler. Things that were examined were making of endpoint profiles, recognition and profiling of endpoints and finally how NAC Profiler reacts on MAC spoofing.

ACS turned out to be quite good as an AAA server, because it's rule-based operating principle allowed flexible handling of different types of authentication events, and it's monitoring and reporting tools proved to be excellent. NAC Profiler's role in 802.1X turned out to be less than expected, for it worked only as an external identity store in this authentication.

802.1X is a great alternative for companies who want their network environment to be secure, because when used correctly, it denies access for unauthorized users and endpoint devices.

Subject headings, (keywords)

authentication, RADIUS, IEEE 802.1X, MAB, AAA

Pages	**Language**	**URN**
41+18	Finnish	URN:NBN:fi:amk-2010121518272

Remarks, notes on appendices

two switch configurations as appendices

Tutor	**Bachelor's thesis assigned by**
Matti Koivisto	Saimaan Talous ja Tieto Oy

SANASTOA

ACS	Cisco Systems Secure Access Control System, Ciscon valmistama autentikointijärjestelmä
NAC	Network Access Control, myös Network Admission Control (Cisco)
AAA	Authentication, Authorization and Accounting
RADIUS	Remote Authentication Dial In User Service
EAP	Extensible Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network, virtuaalinen lähiverkko
MAC	Media Access Control
AD	Active Directory, Microsoftin hakemistopalvelu
AD-ryhmä	Active Directoryn sisältämä ryhmä, joka sisältää käyttäjä- tai konetunnuksia
OUI	Organizationally Unique Identifier, MAC-osoitteen kolme ensimmäistä tavua, jotka ovat laitevalmistajakohtaisia
MAB	MAC Authentication Bypass, keino laitteille, jotka eivät voi käyttää 802.1X-todennusta, autentikoida itsensä
ACL	Access Control List, pääsylista, jolla voidaan kontrolloida verkon liikennettä
SNMP	Simple Network Management Protocol, verkkojen hallinnassa käytetty protokolla
PORT MIRRORING	Portin liikenteen kahdentaminen toiseen porttiin valvontatarkoituksessa, myös SPAN eli Switched Port Analyzer (Cisco)
LDAP	Lightweight Directory Access Protocol, hakemistopalveluihin suuntautuvissa kyselyissä käytetty protokolla, käytössä mm. AD:ssa

SISÄLTÖ

1 JOHDANTO 1

2 AAA JA SIIHEN LIITTYVÄT PROTOKOLLAT 2

2.1 AAA:n osat 2

2.2 RADIUS 3

2.3 802.1X 3

2.4 Extensible Authentication Protocol 5

2.4.1 EAP Over LAN 5

2.4.2 PEAP 6

2.4.3 EAP-MSCHAPv2 6

2.4.4 EAP-TLS 7

3 MAC-OSOITE JA SEN KÄYTTÖ AUTENTIKOINNISSA 7

4 HAKEMISTOPALVELUT 8

4.1 Active Directory 8

4.2 LDAP 9

5 CISCON AUTENTIKOINTIRATKAISUJA 9

5.1 Cisco Secure Access Control System 9

5.1.1 Toimintaperiaate 10

5.1.2 Asetukset 10

5.1.3 ACS:n edut 12

5.2 Cisco NAC Profiler 13

5.2.1 Toimintaperiaate 14

5.2.2 Asetukset 15

6 TOIMEKSIANNON TOTEUTUS 16

6.1 Kytkimen asetukset 18

6.2 ACS:iin tehdyt asetukset 20

6.3 Autentikoinnin testaus 25

6.4 NAC Profileriin tehdyt asetukset 30

6.4.1 Autentikointitestaus ACS:n kanssa 34

6.4.2 Laiteprofiilien teko ja testaus 35

6.4.3 Tunkeutuminen väärennetyllä MAC-osoitteella 38

6.5 Verkon toiminta 40

7 POHDINTA 40

LIITE/LIITTEET

1 Cisco Catalyst 2960-S -kytkimen autentikointitestissä käytetty konfiguraatio
2 Cisco Catalyst 2960-S -kytkimen Profiler-testissä käytetty konfiguraatio

1 JOHDANTO

Nykyaikana tietoverkot ovat niin laajoja ja niihin kohdistuva rikollisuus niin taidokasta, että verkkoyhteyksien salaus on lähes välttämätöntä. On helppoa kaapata täysin suojaamaton yhteys ja käyttää sitä joko tietovarkauksissa tai sotkea verkon toiminta täysin. Tästä syystä on kehitetty erilaisia salaus- ja tunnistusprotokollia, joilla pidetään huolta siitä, että vain sallitut käyttäjäryhmät voivat käyttää eri verkkoja ja heille niihin henkilökohtaisesti määritettyjä palveluita.

Protokollista huolimatta tunkeutumiseen on löydetty keinoja. Yksi niistä on laitteen MAC-osoitteen väärentäminen ohjelmallisesti, jolloin verkkoon fyysisesti liittyvä tietokone voidaan naamioida vaikka toisenlaiseksi laitteeksi, jolla on lupa liittyä verkkoon. Ratkaisuksi edellä mainittuun ongelmaan Cisco Systems on valmistanut NAC Profiler -laitteen, jolla jokaisen tiettyyn verkkoon kytkeytyvän päätelaitteen toimintaa pystytään sekä seuraamaan monipuolisesti että tutkimaan, sopiiko se kyseisenlaisen laitteen käyttäytymisprofiiliin. NAC Profiler toimii yhteistyössä IEEE 802.1X -standardin kanssa, joten se tarjoaa turvallisen verkkoympäristön oikein käytettynä.

Tämä opinnäytetyö on tehty Saimaan Talous ja Tieto Oy:lle, ja sen tarkoituksena on tutkia 802.1X-tunnistautumista verkon reunalla Cisco Systemsin NAC Profiler-laitteella, erityisesti kun verkkoon liitetään sellaisia laitteita, esimerkiksi IP-puhelimia tai tulostimia, jotka eivät voi käyttää 802.1X-standardin mukaista autentikointia. Lisäksi selvitetään Ciscon Secure Access Control System -ohjelmiston toimintaa ja raportointia osana lähiverkon todennusprosessia.

Aluksi käyn läpi työssä tarvittavaa teoriaa ja esittelen AAA:n periaatteen ja RADIUS-protokollan, IEEE:n 802.1X-autentikointistandardin ja sen tämän työn kannalta oleellisimmat protokollat ja selitän samalla, miten todennusprosessi käytännössä toimii. Sitten esittelen lyhyesti MAC-osoitteen ja sen käyttöä, minkä jälkeen kerron hakemistopalveluista Active Directoryn ja LDAP:n perusperiaatteen. Seuraavaksi esitellään työssä käytetyt laitteet ja ohjelmistot, niiden tärkeimmät ominaisuudet ja niiden toimintaperiaatteen. Lopuksi kerron toimeksiannossa määritetyn autentikointiratkaisun toteutuksesta käyttäen Secure ACS:ää sekä NAC Profileria ja miten toteutus toimi. Osa konfiguraatioista, jotka laitteille tein, ovat luottamuksellisia, ja tästä johtuen mm. IP-osoitteet, salasanat, MAC-osoitteet ja VLAN-numeroinnit on muutettu tai peitetty.

2 AAA JA SIIHEN LIITTYVÄT PROTOKOLLAT

Käsitteellä autentikointi tarkoitetaan verkkotekniikassa käyttäjän tai laitteen identiteetin tunnistamista verkkoon liittyessään. Autentikointi terminä pitää sisällään paljon asiaa, osa tämän opinnäytetyön kannalta hyvinkin olennaista ja osa taas ei. Pyrin seuraavissa luvuissa antamaan kuvan siitä, mitä autentikointi käytännössä tarkoittaa ja mitä se pitää sisällään. AAA on terminä ehkä se oleellisin, ja koko järjestelmä pohjautuu siihen.

2.1 AAA:n osat

AAA eli Authentication, Authorization and Accounting on menetelmä, jota käytetään eri osapuolten tunnistamiseen tietoverkoissa. Se koostuu kolmesta osiosta, jotka muodostavat sen nimen. Authentication, eli autentikointi, viittaa prosessiin, jossa kohteen henkilöllisyys tunnistetaan ja varmistetaan, että kohteella on käyttöoikeus tietoverkkoon ja sen resursseihin. Tunnistus voidaan tehdä mm. käyttäjätunnus-salasana-yhdistemän, digitaalisen sertifikaatin tai kertakäyttöisen avaimen perusteella. /3; 11./

Authorization, eli valtuutus, taas määrittelee käyttäjäprofiilin perusteella onko kohteella oikeus sen hakemaan palveluun, esimerkiksi liittymään tietoverkkoon tai käyttämään sen palveluita. Oikeutta voidaan rajoittaa monien eri ominaisuuksien, esimerkiksi päivänajan tai kohteen sijainnin perusteella. /3; 11./

Accounting, eli tilastointi, on kolmikon viimeinen, ja sen tehtävä on seurata käyttäjien verkkoresurssien kulutusta ja kerätä tietoa siitä. Tyypillistä tietoa, jota kerätään, on mm. käyttäjän identiteetti, IP-osoite, käytetyn palvelun laatu ja sekä käytön alkamis- että loppumisaika. /3; 11./

AAA toimii tietoverkoissa autentikointipalvelimen ja sen verkkolaitteen, johon autentikoitava laite kytketään, välillä. AAA-protokollia ovat RADIUS, Diameter, TACACS ja TACACS+, mutta tässä työssä keskitytään vain sen kannalta oleellisimpaan eli RADIUS-protokollaan. /3; 6; 11./

2.2 RADIUS

RADIUS eli Remote Authentication Dial In User Service on AAA-protokolla, joka toimii asiakas-palvelin – periaatteella (client-server). Sillä on kolme päätehtävää: autentikoida käyttäjät, valtuuttaa nämä käyttäjät palveluja varten ja pitää kirjaa näiden palveluiden käytöstä. Asiakkaalla tarkoitetaan jotain verkkolaitetta, esimerkiksi kytkintä tai tukiasemaa, jonka fyysiseen tai loogiseen porttiin liitetään päätelaite, esimerkiksi tietokone. Palvelin on esimerkiksi ACS tai muu autentikointia tarjoava palvelin. RADIUS on siis lyhyesti sanottuna liikennöintiprotokolla näiden kahden laitteen välillä. /11; 17./

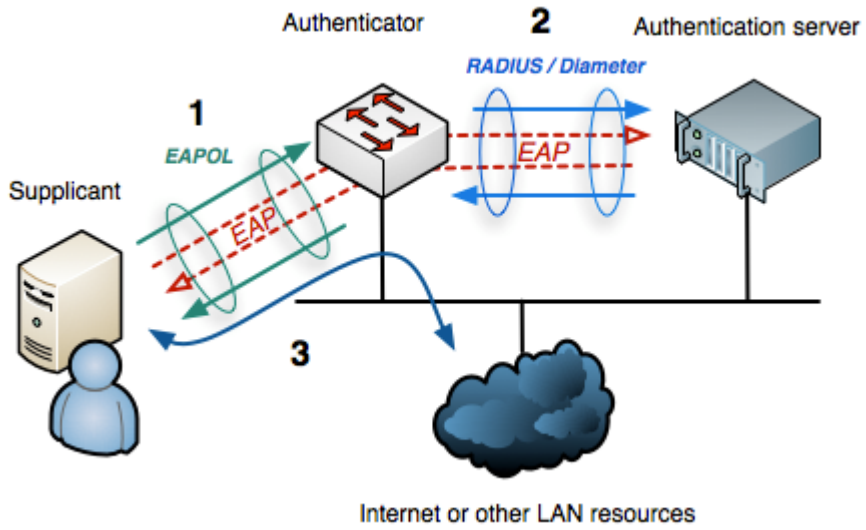
RADIUS toimii siten, että asiakas lähettää EAP Request – viestin, johon päätelaite vastaa EAP Response – viestillä. Asiakas lähettää tämän viestin eteenpäin palvelimelle käyttäen RADIUS-protokollaa, joka kapseloi EAP-viestin RADIUS Access Request – viestiksi. Kun palvelin vastaanottaa RADIUS-viestin, se hakee siitä alkuperäisen EAP-viestin ja luo sen perusteella uuden, päätelaitteelle lähetettävän EAP Request – viestin, jonka se kapseloi RADIUS Access-Challenge –viestiin. Tämä viesti menee asiakkaalle, joka purkaa sen ja lähettää EAP-viestin asiakkaalle. Tällaista epäsuoraa EAP-viestien vaihtoa käydään päätelaitteen ja palvelimen välillä autentikointiin käytetystä EAP-protokollasta riippuen enemmän tai vähemmän. Näiden viestien mukana lähetetään se data, jota tarvitaan autentikoinnissa. Kun palvelin on vastaanottanut tarpeeksi dataa päättääkseen autentikoinnin lopputuloksen, se lähettää EAP Success – tai EAP Failure –viestin kapseloituna RADIUS Access-Accept – tai RADIUS Access-Reject –viestiin. Näiden viestien mukana siirtyvät ne tiedot, joita asiakas käyttää joko hylkäämään yhteyspyynnön tai hyväksymään sen ja tekemään tarvittavat porttiasetukset. /6./

2.3 802.1X

IEEE eli Institute of Electrical and Electronics Engineers on kansainvälinen tekniikan alan järjestö, jonka toimintaan kuuluu mm. koulutuksen ja konferenssien järjestämisen ohella alan keskeisten standardien määrittely. Verkkoliikenteen kannalta keskeisimpiä ovat 802.-alkuiset standardit, joilla määritetään pakettipohjaisten lähiverkkojen toimintaa.

IEEE 802.1X määrittelee porttikohtaisen autentikoinnin, jota käytetään 802-lähiverkoissa eli Ethernetissä (IEEE 802.3) ja langattomissa lähiverkoissa eli WLAN:eissa (IEEE 802.11). Sen tarkoitus on estää luvattoman laitteen kytkeytyminen lähiverkkoon liityntäpisteen kautta. Liityntäpisteellä tarkoitetaan esimerkiksi lähiverkossa olevan kytkimen porttia tai langattoman verkon tukiaseman (Access Point) loogista porttia. IEEE 802.1X yhdistää EAP:n ja AAA:n toimivaksi kokonaisuudeksi. /5./

802.1X:ssä on kolme eri osapuolta: asiakas (Supplicant), autentikoija (Authenticator) ja autentikointipalvelin (Authentication Server). Asiakas on päätelaite, esimerkiksi tietokone, IP-puhelin tai tulostin, jonka tehtävänä on vastata autentikoijan lähettämiin pyyntöihin. Autentikoija on verkkolaite, jossa on fyysisiä tai loogisia liityntäpisteitä ja se voi olla esimerkiksi kytkin. Sen tehtävä on vastata asiakkaan ja autentikoijan välisestä keskustelusta ja lähettää autentikointitietoa autentikointipalvelimelle. Autentikointipalvelin taas on laite tai virtuaalisessa koneessa ajettava ohjelmisto, esimerkiksi ACS, jonka tehtävänä on autentikoida asiakas ja lähettää autentikoijalle tieto lopputuloksesta ja tarvittavat asetukset. Kuvassa 1 näkyy 802.1X:n mukainen rakenne, jossa ovat kaikki kolme osapuolta ja niiden välinen liikenne. /5./



KUVA 1. 802.1X:n osapuolet ja niiden välinen liikennöinti /13/

2.4 Extensible Authentication Protocol

Extensible Authentication Protocol eli EAP on autentikointiin tarkoitettu kehysrakenne, joka tukee useita eri autentikointimetodeja, ja jota käytetään PPP- ja 802-yhteyksissä. Se toimii OSI-mallin toisessa eli data link –kerroksessa, eikä tarvitse IP-osoitetta toimiakseen. EAP:ia voidaan käyttää sekä langallisissa että langattomissa yhteyksissä. Langallisissa verkoissa EAP-kapselointi on määritetty IEEE 802.1X-standardissa ja langattomissa IEEE 802.11i-standardissa./1./

Alun perin EAP suunniteltiin langallisiin yhteyksiin, joiden oletettiin olevan fyysisesti suojattuja. Esimerkiksi PPP:n yhteydessä käytettävä EAP liikennöi leased line- (jonkun tahon palveluntarjoajalta tilaama yksityinen symmetrinen datayhteys) tai modeemiyhteyksillä, jolloin verkkoon hyökkäävä osapuoli joutuisi ensin tunkeutumaan puhelinverkkoon päästäkseen vakoilemaan verkkoliikennettä. Tästä johtuen EAP:n liikennöintiä ei salattu. Taulukossa 1 on erilaisten EAP-metodien eri ominaisuuksia. /1; 6./

TAULUKKO 1. EAP-protokollia ja niiden ominaisuuksia /18/

EAP/Feature	General	Server Authentication	Supplicant Authorization	Dynamic Key Delivery	Security Risks
EAP Message Digest (EAP-MD5)	• Username/ password • Base-level EAP support	None	Password Hash	No	Man-in-the-middle (MitM) attack, Session hijacking
Lightweight EAP (LEAP)	• Server Certificate • Mutual Authentication	Password Hash	Password Hash	Yes	Identity exposed, Dictionary attack.
EAP Transport Layer Security (EAP-TLS)	• Client/server Certificates • Mutual Authentication	Public Key (Certificate)	Public Key (Certificate or SMART Card)	Yes	Identity exposed
EAP with Tunneled TLS (EAP-TTLS)	• Server Certificate • Client/server certificates	Public Key (Certificate)	CHAP, PAP, MS-CHAP (v2), EAP	Yes	MitM attack
PEAP	• Server certificate • Tunneled EAP Authentication	Public Key (Certificate)	Any EAP such as EAP-MS-CHAPv2 or Public Key	Yes	MitM attack; identity hidden in phase 2 but potential exposure in Phase 1

2.4.1 EAP Over LAN

EAP over LAN eli EAPoL on 802.1X:ssä määritelty viitekehys, joka on tarkoitettu autentikointiin ja käyttäjän liikenteen ohjaamiseen suojattuun verkkoon. Sitä käyte-

tään sekä langallisissa että langattomissa lähiverkoissa. EAP-viestit asiakkaan ja autentikoijan välillä kuljetetaan koteloituna EAPoL-viesteihin. /4./

2.4.2 PEAP

PEAP eli Protected Extensible Authentication Protocol on autentikointiprotokolla, joka koteloi EAP:n TLS-tunneliin, joka on salattu. Tämä tunneli tarjoaa turvallisen keskusteluväylän asiakkaan ja palvelimen välille. PEAP korjaakin yhden EAP:n suurista vioista: EAP olettaa, että yhteyteen käytetään turvallista linjaa, esimerkiksi fyysistä johtoa ja ei suojaa linjalla tapahtuvaa liikennettä. /6; 15./

PEAP-autentikoinnissa palvelin tunnistetaan digitaalisen sertifikaatin perusteella, mutta asiakkaan tunnistaminen tehdään käyttäjä- tai konetilin tietojen perusteella, mihin käytetään sisempää EAP-metodia, tässä tapauksessa EAP-MSCHAPV2:ta. Protokollan ulompi metodi siis tunnistaa palvelimen ja sisempi asiakkaan. /6; 15./

2.4.3 EAP-MSCHAPv2

CHAP eli Challenge Handshake Authentication Protocol on autentikointiprotokolla, joka todentaa käyttäjän jollekin sen autentikoivalle taholle. Itse autentikointi tapahtuu niin, että kun linkki näiden kahden tahon välille on muodostettu, autentikoiva taho lähettää haasteviestin autentikoituvalle, johon viimeksi mainittu vastaa MD5- tarkistusluvulla, jonka se laskee tietyllä tavalla. Kun autentikoiva taho saa luvun, se tarkistaa täsmääkö luku sen omaan samalla tavalla tehtyyn laskelmaan. Jos arvot täsmäävät, autentikointi katsotaan onnistuneeksi. Autentikoiva taho tekee kuitenkin sattumanvaraisin aikavälein uusia haasteita, joissa se käy prosessin uudestaan läpi ja tarkistaa autentikoinnin. MSCHAPv2 on Microsoftin versio CHAP:sta. Sen suurin ero perus-CHAP:iin on mahdollisuus vaihtaa salasana. /6./

EAP-MSCHAPv2, joka on muunnelma MSCHAPv2:sta, toimii PEAP-autentikoinnissa ns. ”sisempänä EAP-metodina” kun taas PEAP on tässä yhteydessä ”ulompi EAP-metodi”. Tämä tarkoittaa siis sitä, että sisempi metodi tarjoaa lisäautentikointia ulomman viitekehyksessä. /6./

2.4.4 EAP-TLS

EAP-TLS eli Extensible Authentication Protocol – Transport Layer Security on autentikointiprotokolla, joka on erittäin turvallinen versio EAP:sta. EAP-TLS vaatii sertifikaattiautentikoinnin sekä asiakkaalta että serveriltä. Yhteyttä ei avata, jos jompikumpi epäonnistuu autentikoinnissa. /2; 6./

EAP-TLS luottaa molemminpuoleisessa autentikoinnissa digitaalisiin sertifikaatteihin ja niiden täytyy täyttää tietyt vaatimukset sekä serverissä että asiakkaassa, jotta autentikointi voi onnistua. Tämä autentikointimekanismi on nimeltään Public Key Infrastructure (PKI) ja pohjautuu X509-sertifikaattitunnistukseen. /2; 6./

EAP-TLS:n EAP-osio sisältää alustavat autentikointitiedot, erityisesti 802.1X:n mukaisen EAPoL-kapsuloinnin, kun taas TLS-osio käyttää sertifikaatteja kirjautumiseen./2; 6/

3 MAC-OSOITE JA SEN KÄYTTÖ AUTENTIKOINNISSA

Media Access Control - eli MAC-osoite on uniikki laitekohtainen tunnus, joka annetaan verkkolaitteille ja varastoidaan laitteen ROM-muistiin. MAC-osoitteet luotiin alun perin auttamaan lähiverkkojen lähettäjä- ja vastaanottajalaitteiden osoitteiden tunnistamisessa, ja ne ovat suoraa seurausta IEEE:n laitevalmistajille suunnatuista säännöistä varmistaa jokaiselle verkkolaitteelle maailmanlaajuisesti ainutlaatuinen osoitetieto. Itse osoite koostuu 48 bitistä, toisin sanoen kuudesta tavusta tai kuudesta kaksinumeroisesta heksadesimaalisesta luvusta. Jokaisen osoitteen kolme ensimmäistä tavua kertovat laitevalmistajan, sillä jokaisella valmistajalla on oma OUI eli Organizationally Unique Identifier, joka tulee aina MAC-osoitteen alkuun. Kolme viimeistä taas muodostavat jokaiselle laitteelle ainutlaatuisen tunnisteen.

MAC-osoitteet toimivat OSI-mallin toisella kerroksella (Data Link), ja ne käytännössä muodostavat perustan koko tietoverkon toiminnalle.

MAC-osoitetta käytetään autentikoinnissa päätelaitteiden tunnistamiseen niiden verkkosovittimen osoitteen perusteella. Nykyään osoitteen voi muuttaa ohjelmallisesti,

joten pelkän MAC-autentikoinnin käyttö ei ole turvallista. MAC-osoitteen väärentämisestä puhutaan termillä MAC Spoofing, ja internetistä löytyy lukuisia ohjelmia tähän tarkoitukseen. Joidenkin verkkokorttien osoitteen voi myös vaihtaa suoraan laitteen asetuksista.

MAC Authentication Bypass eli MAB on kuitenkin oleellinen osa 802.1X-autentikointia, sillä se sallii verkkoon liittymisen laitteille, jotka eivät voi käyttää varsinaista 802.1X-autentikointia. Tällaisia laitteita ovat esimerkiksi IP-puhelimet ja verkkotulostimet. MAB:n käyttö edellyttää sitä, että se on mahdollistettu sekä autentikoijassa että autentikointiserverissä. MAB-autentikointi vaatii AAA-palvelimelta jonkinlaisen tietokannan laiteprofiileista, joihin asiakkaan tietoja voidaan verrata. Tämän opinnäytetyön kohdalla sen tarjoaa NAC Profiler, joka keskustelee ACS:n kanssa LDAP-protokollan kautta. /8./

4 HAKEMISTOPALVELUT

Sanalla hakemistopalvelu tarkoitetaan verkkopalvelua, joka tarjoaa käytöstä riippuen erilaista tietoa tai verkkoresursseja. Monet valmistajat ovat tehneet erilaisia hakemistopalveluja, mutta tässä työssä keskityn Microsoftin Active Directoryyn ja LDAP-protokollaan.

4.1 Active Directory

Active Directory eli AD on Microsoftin valmistama järjestelmä, jonka päätehtävä on varastoida tietoa verkossa olevista kohteista ja mahdollistaa tämän tiedon helppo löytäminen ja käyttäminen sekä verkon valvojille että käyttäjille. AD käyttää jäsentynyttä datavarastoa loogisen ja hierarkisen hakemistoinformaation rakenteeseen. Tämä datavarasto sisältää informaatiota Active Directoryn kohteista, jotka yleensä sisältävät jaettuja resursseja, esimerkiksi verkon käyttäjä- ja konetunnuksia, palvelimia, tulostimia ja kansioita. Active Directory on siis toisin sanoen käyttäjätietokanta ja hakemistopalvelu. /16./

Käsite domain eli toimialue on joukko tietokoneita, joissa on Microsoft Windows -käyttöjärjestelmä ja joita voidaan hallita keskitetysti Windows-palvelimilta. Jokaisella toimialueen käyttäjällä on oma käyttäjätunnus ja salasana, joilla hän voi kirjautua sisään miltä tahansa toimialueen tietokoneelta ja päästä käsiksi omiin tiedostoihinsa. /16./

4.2 LDAP

Lightweight Directory Access Protocol eli LDAP on protokolla, jonka avulla voidaan tehdä kyselyjä hakemistopalveluihin ja muokata niiden sisältöä. LDAP kehitettiin korvaamaan DAP eli Directory Access Protocol, joka oli raskas protokolla. Muun muassa Active Directory käyttää LDAP-protokollaa yhteyksissään. /14./

LDAP on suunnattu hallinta- sekä selainohjelmakäyttöön ja se tarjoaa interaktiivista kirjoitus- ja lukuoikeutta hakemistoihin /14/.

5 CISCON AUTENTIKOINTIRATKAISUJA

Cisco Systems Inc. on yhdysvaltalainen johtava verkkolaitteiden valmistaja, joka on valmistanut monia erilaisia ratkaisuja verkkojen turvaamiseksi. Tässä työssä keskityn kuitenkin niistä kahteen, jotka ovat Secure Access Control System ja NAC Profiler.

5.1 Cisco Secure Access Control System

Cisco Secure Access Control System eli ACS on Cisco Systemsin valmistama autentikointiratkaisu, jota saa sekä erillisenä laitteena että virtuaalikoneelle asennettavana järjestelmänä. ACS:n perustarkoitus on toimia AAA-palvelimena ja keskittää autentikointi yhteen pisteeseen, jossa tehdään autentikointipäätöksiä sekä siihen säädettyjen sääntöjen ja käytäntöjen että ulkoisten identiteettivarastojen, esimerkiksi Active Directoryn, perusteella. Vaikka se on täysverinen RADIUS-palvelin, niin sen voi myös säätää toimimaan proxy-asiakkaana toiselle RADIUS-palvelimelle, jolloin se välittää autentikointipyynnöt viimeksi mainitulle. ACS:n voi linkittää erilaisiin ulkoisiin iden-

titeettivarastoihin, mm. Microsoft Active Directoryyn tai NAC Profileriin, jolloin autentikoinnin yhteydessä käyttäjätietoja voidaan sääntömääritysten perusteella hakea niistä. /6; 10./

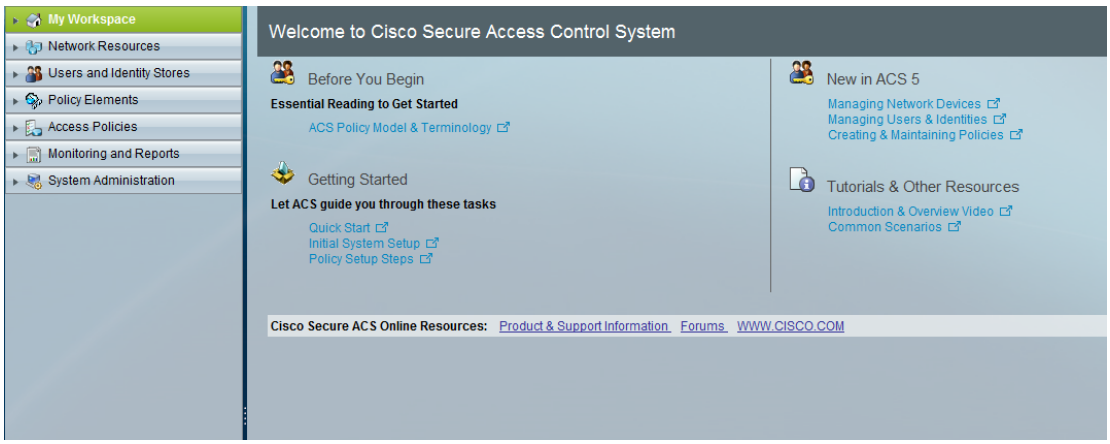
5.1.1 Toimintaperiaate

ACS:n toiminnan perusperiaatteena on ottaa vastaan AAA-protokollaan koteloituja autentikointipyyntöjä asiakaslaitteilta, kuten kytkimiltä tai tukiasemilta, verrata yhteyspyynnön tietoja siihen säädettyjen sääntöjen ja käytäntöjen perusteella, joko hyväksyä tai hylätä pyyntö ja ilmoittaa asiakkaalle toimintaohjeet joko portin avaamiseksi ja siirtämiseksi oikeaan VLAN:iin tai sulkemiseksi. Sääntöpohjainen joustava toimintamalli mahdollistaa sen, että eri tilanteissa voidaan käyttää eri sääntöjä, jolloin autentikointikäytännöt ovat yhteydestä riippuvaisia eivätkä sidonnaisia esimerkiksi yhteen AD-ryhmään. /6; 10./

5.1.2 Asetukset

Cisco Secure ACS:ssä on paljon erilaisia asetuksia, joista suurin osa on toiminnan kannalta kriittisiä ja loput lähinnä kosmeettisia. Asetukset löytyvät web-hallinnan vasemmasta laidasta, kuten kuvasta 2 näkyy. Asetukset on jaettu aihepiireittäin pääryhmiin, jotka ovat

- My Workspace
- Network Resources
- Users and Identity Stores
- Policy Elements
- Access Policies
- Monitoring and Reports
- System Administration



KUVA 2. ACS:n etusivu, vasemmalla asetusvalikot

Network Resources määrittelee eri elementtejä siitä verkosta, josta lähetetään autentikointipyyntöjä ACS:lle. Täältä voi mm. liittää kytkimiä ACS:n RADIUS-palvelimen alaisuuteen (**Network Device Groups > Network Devices and AAA Clients**) ja säätää ACS:n toimimaan jonkun toisen RADIUS-palvelimen proxy-asiakkaana (**Network Device Groups > External RADIUS Servers**). Tämän lisäksi verkkolaitteita voidaan ryhmitellä eri kriteerien mukaan ja käyttää eri käytäntöjen määrittelemiseen. /6./

Users and Identity Stores sisältää identiteettivarastojen, sekä sisäisten että ulkoisten, tiedot ja niiden käyttöön tarkoitetut käytännöt. Autentikoinnin kannalta tärkeimpiä kohteita ovat Active Directoryn yhteysasetukset ja ryhmät (**External Identity Stores > Active Directory**), NAC Profilerin yhteysasetukset (**External Identity Stores > LDAP**) ja identiteettivarastojen käyttämisjaksot (**External Identity Stores > Identity Store Sequences**), jolla määritetään erilaiset käytettävät identiteetin tunnistustavat, joita ovat salasana- ja sertifikaattikirjautuminen ja joista voi olla käytössä joko vain toinen tai molemmat. /6./

Policy Elements on ryhmä, jossa päässään määrittelemään erilaisia käytäntöjen elementtejä. Nämä elementit ovat niitä palasia, joita tarvitaan sääntöjen tekemiseen. Ehkä tärkein kaikista on valtuutusprofiilit (**Authorization and Permissions > Authorization Profiles**), joilla pystytään määräämään tapauskohtaisesti mihin virtuaaliseen lähiverkkoon eli VLAN:iin mikäkin hyväksytty tai hylätty yhteyspyyntö ohjataan. VLAN-numeroinnin voi säätää joko dynaamiseksi tai staattiseksi. /6./

Access Policies on se kriittisin ryhmä, jossa määritetään tarkasti autentikoinnissa käytetyt säännöt ja käytänteet. Kohdassa Access Services voidaan luoda uusi Access Ser-

vice Policy. Näillä käytännöillä ja niiden sisältämillä valtuutus- ja identiteettikäytännöillä suodatetaan tarkasti tulevia autentikointipyyntöjä. /6./

Monitoring and Repots on myös erittäin tärkeä ryhmä, sillä se sisältää ACS:n sisäiset valvontatyökalut, jotka ovat korvaamattoman arvokkaita työkaluja vikojen etsimisessä. Tästä ryhmästä löytyy mm. autentikointiloki ja graafista statistiikkaa autentikoinnista. Ensimmäiseksi mainittu oli kovassa käytössä tehdessäni ACS:n käytäntöjä, sillä siitä näin suoraan, toimivatko ne, ja jos eivät, näin myös, missä vika on. Lokissa on valtavasti erilaista tietoa jokaisesta autentikointitapahtumasta ja jokainen merkintä näkyy joko vihreänä tai punaisena osoittaen, hyväksyttiinkö vai hylättiinkö se. /6./

System Administration sisältää ACS:n huoltotyökalut, mukaan lukien lisenssien ylläpidon, päivitysmahdollisuudet ja järjestelmän asetusten varmuuskopioinnin. ACS:ssä on myös monipuolinen varmuuskopiointijärjestelmä, jonka kautta pystytään määrittämään järjestelmän säännöllinen varmuuskopiointi. Tätä varten on tehtävä säilö (engl. repository) valitsemalla **System Administration > Operations > Software Repositories**. Tänne määritetään säilön nimi, varmuuskopioinnissa käytettävä protokolla, esim. TFTP tai FTP, ja vastaanottavan serverin asetukset. Kun säilö on valmis, se voidaan linkittää varmuuskopiointitapahtumaan. /6./

Säännöllinen varmuuskopiointi saadaan toteutettua kohdasta **System Administration > Operations > Scheduled Backups**, jossa määritetään varmuuskopiotiedostolle etuliite, säilö, johon varmuuskopio tehdään ja kopioiden ottotiheys, esimerkiksi päivittäin /6/.

5.1.3 ACS:n edut

Ciscon ACS on monipuolinen autentikointijärjestelmä, jonka etuna on helppo käytettävyys, kaksi käytettävää AAA-protokollaa, usean samanaikaisen tietokannan käyttömahdollisuus autentikoinnissa, joustavat suodatussäännöt, joita sovelletaan erilaisten pyyntöjen käsittelyyn ja erittäin hyvät sisäiset valvonta- ja diagnostiikkatyökalut. ACS tarjoaa verkon ylläpitäjille mahdollisuuden löytää vikoja autentikoinnissa nopeasti ja helposti, lisäksi jos sitä käytetään yhdessä Ciscon kytkinten kanssa, se tarjoaa tietoa niistä ja niiden porteista. Autentikointilokista näkee helposti jokaisen autentikointita-

pahtuman vaiheet ja tunnuskohtaista kirjautumisstatistiikkaa aina autentikointimääristä kirjautumislaitteiden MAC-osoitteisiin asti. /6; 10./

ACS pystyy lähettämään virheilmoituksia sekä ulkoiseen Syslog-palvelimeen että määritettyyn sähköpostiosoitteeseen. Nämä ominaisuudet auttavat verkon toiminnan valvonnassa, sillä laitteen omaa lokia ei välttämättä muista aina tarkkailla. Kun verkon valvoja saa omaan sähköpostiinsa ilmoitukset toiminnan vaarantavista virheistä, hän pystyy reagoimaan niihin nopeasti ja turvaamaan verkon jatkuvan toiminnan. /6./

Järjestelmä pystyy joustavaan autentikointiin, joka ei ole sidottuna vain yhteen protokollaan tai identiteettivarastoon. Sääntöpohjainen toimintamalli mahdollistaa tarkan ja tehokkaan autentikointipyyntöjen käsittelyn jokaiselle verkkoon liitettävälle päätelaitteelle riippumatta siitä, onko se 802.1X-yhteensopiva vai ei. Tämä kuitenkin edellyttää myös NAC Profiler -järjestelmän käyttöä, sillä ACS vaatii ulkoisen tietokannan MAB-autentikoituvista laitteista. /6./

Säännöllinen järjestelmän asetusten varmuuskopiointi mahdollistaa sen, että vikatilanteissa pystytään nopeasti palauttamaan ACS toimivaan tilaan /6/.

5.2 Cisco NAC Profiler

Cisco Systemsin Network Access Control Profiler, eli lyhyesti NAC Profiler, on järjestelmä, jolla pystytään tehostamaan tietoverkkojen turvallisuutta. Sen avulla nekin laitteet, jotka eivät voi käyttää IEEE 802.1X-tunnistautumista, voivat autentikoitua ja ohjautua oikeisiin VLAN:eihin. NAC Profiler koostuu kahdesta osasta, jotka ovat NAC Profiler Server ja NAC Profiler Collector. Collectoreja voi olla verkossa joko yksi tai useampia, ja ne toimivat Profiler-järjestelmän antureina, joiden keräämä tieto lähetetään Profiler Serverille käsiteltäväksi. NAC Profiler Server toimii Secure ACS:n kanssa ulkoisena identiteettivarastona, ja yhteys näiden kahden välillä tapahtuu LDAP- eli Lightweight Directory Access Protocol -protokollan avulla. /7./

5.2.1 Toimintaperiaate

Kuten jo aiemmin mainitsin, NAC Profiler Collectorit keräävät tietoa verkon toiminnasta ja toimittavat nämä tiedot Profiler Serverille. Tieto kerätään viidellä moduulilla, joista jokaisella on oma tehtävänsä:

- **NetMap**, kyselee SNMP-protokollalla verkkolaitteilta tietoja, mm. porteista, 802.1X:stä, reitityksestä, IP:stä ja järjestelmätiedoista
- **NetTrap**, ilmoittaa linkkien tilavaihteluista ja uusista MAC-osoitteista, kerää SNMP trap -tietoja verkkolaitteilta
- **NetWatch**, passiivinen verkon liikenteen analysoija
- **NetInquiry**, aktiivinen päätelaitteiden profilointimoduuli
- **NetRelay**, kerää tietoa muilta datankeräysjärjestelmiltä.

Näiden lisäksi on vielä yksi moduuli, Forwarder, joka toimii väliohjelmistona Serverin ja Collectorien välillä ja tarjoaa niille turvallisen keskusteluväylän /7/.

NAC Profiler –järjestelmä vaatii Cisco-verkkolaitteista rakennetun tietoverkon, jotta sen kaikki ominaisuudet saataisiin hyödynnettyä, sillä moduulit eivät osaa kerätä tietoa esim. Hewlett-Packardin Procurve-kytkimistä tai -reitittimistä. Kun koko verkko koostuu Cisco-laitteista, pystytään päätelaitteiden paikka määrittämään kytkimen ja sen portin tarkkuudella. /7./

NAC Profiler tekee päätelaitteiden tunnistamisen laiteprofiilien perusteella. Nämä profiilit sisältävät seuraavat asiat:

- profiilin nimi
- määritelmä
- onko 802.1X-autentikointi aktiivinen vai ei, oletusasetuksena ei
- onko profiili aktiivinen vai ei, oletusasetuksena aktiivinen
- onko aikakatkaisu aktiivinen, oletusasetuksena ei
- onko LDAP-autentikointi aktiivinen, oletusasetuksena ei.

Jos LDAP-autentikointi mahdollistetaan, niin silloin NAC Profiler voi profiilien perusteella tunnistaa verkkoon kytkettäviä laitteita jos autentikointipalvelin lähettää sille

pyynnön. Tällöin Profiler toimii Active Directoryn tapaan ulkoisena identiteettivarastona. /7./

Profiileissa pystytään määrittämään myös sääntöjä, joiden perusteella päätelaitteita jaotellaan. Sääntöjä tehdään mm. MAC-osoitteiden, AD-ryhmien, IP-osoitteiden, verkkoliikenteen, avointen TCP-porttien sekä liikennöivien sovellusten perusteella ja jokaiselle säännölle määritetään varmuusprosentti. Tämä varmuusprosentti kuvaa sitä, kuinka luotettavasti laite voidaan säännön perusteella tunnistaa, esimerkiksi MAC-osoitteeseen perustuva sääntö ei voi olla sataprosenttisen luotettava. Jokaiselle profiilille kannattaakin tehdä useita eri sääntöjä, jotta oikeat laitteet ryhmittyvät oikeisiin profiileihin. /7./

Jos NAC Profiler liitetään Ciscon NAC Appliance -järjestelmään, joka on vaihtoehto 802.1X:lle, se voi toimia reaaliaikaisesti osana verkon pääsynvalvontaa. Tällöin se lähettää laitekohtaisia tilapäivitystietoja NAC Appliance Manager –laitteelle, joka tekee päätöksiä niiden perusteella. /7./

5.2.2 Asetukset

NAC Profiler Serverissä on melko vähän erilaista säädettävää. Lähes kaikki asetukset löytyvät Configuration-välilehdeltä, josta pääsee seuraaviin asetusryhmiin:

- **My Network**, verkon asetukset
- **Modules**, serverin ja collectorin moduulien asetukset
- **Network Devices**, verkon kytkinten yms. tiedot
- **Profiles**, päätelaiteprofiilien teko
- **Events**, ilmoitustapahtumien luominen
- **Accounts**, käyttäjätilien hallinta
- **Apply Changes**, tallentaa tehdyt asetukset ja käynnistää haluttaessa collectorin moduulit uudestaan.

My Network – ryhmässä määritetään tutkittavan verkon asetuksia, mukaan lukien IP-osoitealue CIDR-muodossa, eli esim. 192.168.1.0/24. Modules keskittyy Profiler Serverin ja Collectorin asetuksiin ja on Profiler-järjestelmän toiminnan kannalta kriitti-

nen. Kolmanteen eli Network Devices –ryhmään määritetään ne verkkolaitteet, joiden kautta kulkevaa liikennettä Collectoreilla halutaan seurata. Profiles sisältää päätelaite-profiiliasetukset ja Events-ryhmään voidaan määrittää eritasoisia ilmoituksia, joita voidaan lähettää mm. ulkoiselle Syslog-palvelimelle. Accounts sisältää käyttäjätilien hallinnan. /7./

Kun asetuksia tehdään, moduulit on yleensä käynnistettävä uudelleen. Tämä tapahtuu Apply Changes –kohdassa Update Modules –painikkeella. Tässä ryhmässä voidaan valita edellä mainitun toimintamallin lisäksi kaksi vaihtoehtoa: Re-Map, jolloin Profiler pakotetaan mallintamaan verkko uudelleen ilman moduulien uudelleenkäynnistystä ja Re-Model, jolloin Profiler pakotetaan tarkastamaan päätelaitteiden sijoitusprofiilit juuri luodut profiilit huomioon ottaen. /7./

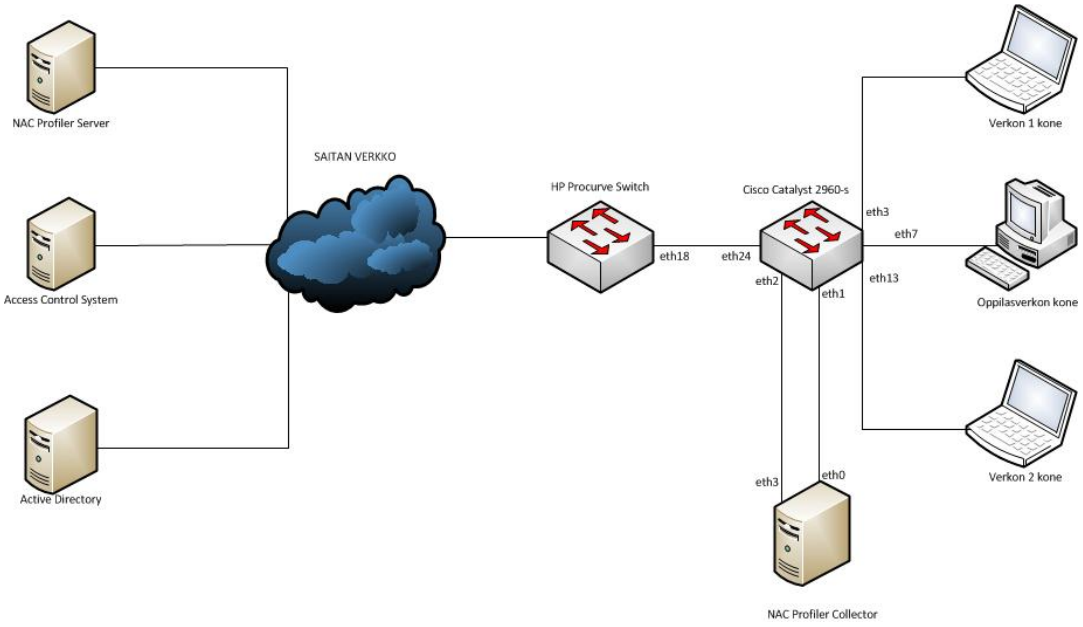
6 TOIMEKSIANNON TOTEUTUS

Tämä opinnäytetyö tehtiin Saimaan Talous ja Tieto Oy:n, lyhyesti Saita, toimeksiannosta, ja sen päätavoite oli kaksiosainen: ensiksi tutkia Cisco Systemsin valmistamaa NAC Profiler –laitetta 802.1X-autentikoinnissa verkon laidalla ja toiseksi selvittää Cisco Systemsin Secure Access Control System –ohjelmiston käyttöä osana verkon autentikointia ja raportointia. Apunani toteutuksessa oli Saitan verkkotekniikan asentaja, joka auttoi vianetsinnässä ja kytkinten liittämisessä ACS:n alaisuuteen.

Saimaan Talous ja Tieto oy on 1.8.2009 perustettu Lappeenrannan kaupungin ja Etelä-Karjalan sosiaali- ja terveyspiirin omistama yritys, jonka toimialana on tarjota talous-hallinto- ja tietotekniikkapalvelujen ns. standardipalveluja osakkeenomistajilleen.

Saita vastaa Lappeenrannan kaupungin sekä Etelä-Karjalan sosiaali- ja terveyshuollon tietoteknisistä palveluista, ja tästä johtuen sen verkko koostuu useista eri VLAN:eista, jokainen suunnattu tietylle organisaatiolle. Huomionarvoista on se, että useimmat päätelaitteet kirjautuvat sertifikaateilla autentikointipalvelimelle EAP-TLS-protokollan mukaisesti, jonka jälkeen käyttäjä voi kirjautua omilla AD-ryhmän mukaisilla tunnuksillaan. Osa koneista, pääasiassa koulujen oppilaskoneet, ovat sellaisia, jotka eivät tunnistaudu sertifikaateilla vaan pelkästään käyttäjätunnuksella ja salasanalla, joiden on täsmättävä AD:sta tietystä ryhmästä löytyvien kanssa. Päätelaite kirjautuu ensin

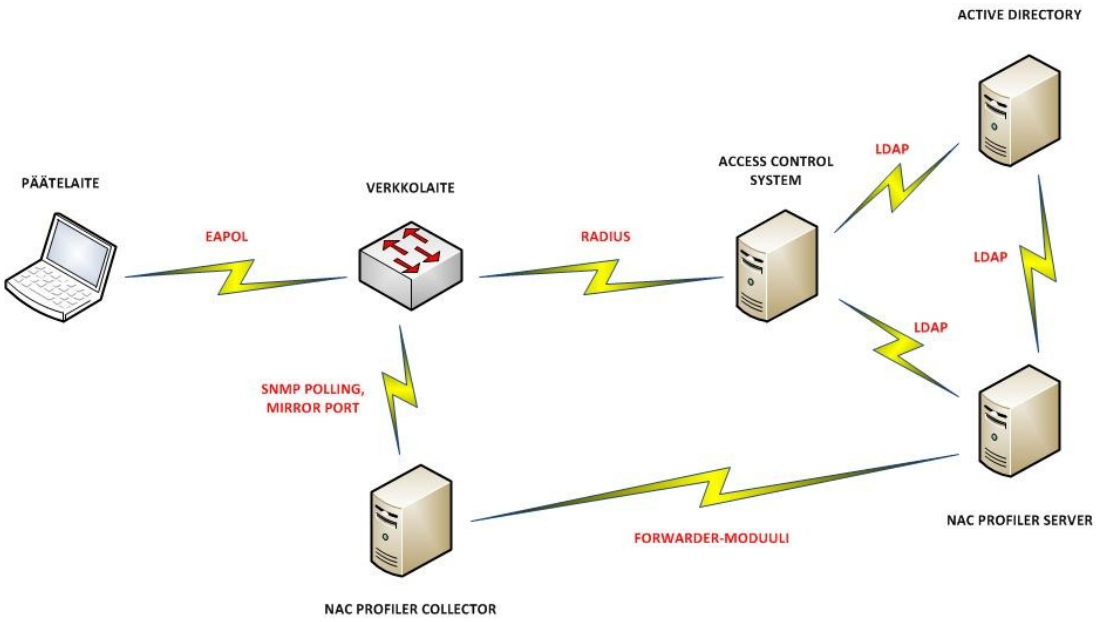
käynnistyessään konetilin perusteella ja käyttäjä kirjautuu Windowsin Winlogon/GINA-kirjautumisessa (Graphical Identification and Authentication) omilla tunnuksillaan. Tämä kirjautumistapa noudattaa PEAP- protokollaa. Alla olevasta kuvasta 3 nähdään verkon toteutus.



KUVA 3. Verkon rakenne

Pyrin toteutuksen tavoitteeseen seuraavalla tavalla: aluksi säädin kytkimen toimimaan osana Saitan verkkoa, sitten säädin ACS:n toimimaan autentikointipalvelimena ja liitin säätämäni kytkimen sen alaisuuteen. Testattuani kytkimeltä tulevat autentikoinnit toimiviksi liitin lisää laitteita ACS:n alaisuuteen. Kun olin varmistunut ratkaisun toiminnasta, liitin NAC Profiler –järjestelmän kytkentään mukaan, säädin sen toimimaan LDAP-protokollalla ulkoisena identiteettivarastona ACS:lle ja annoin verkkosegmenttejä Collectorin moduuleille tutkittavaksi. Seuraavaksi testasin Hewlett-Packardin valmistaman tulostimen MAB-autentikointia ja Profilerin päätelaitteiden profilointia.

Kun kaikki edellä mainittu oli testattu, eristin kytkimen Saitan verkosta ja ACS:stä ja keskityin tutkimaan Profileria. Asiat, joita tutkin, olivat päätelaiteprofiilien teko, päätelaitteiden sijoittuminen profiileihin ja se, miten Profiler suhtautuu laitteeseen, joka liitetään tutkittavaan verkkoon väärällä MAC-osoitteella varustettuna. Kuvasta 4 ilmenee työn kannalta oleelliset osapuolet ja niiden yhteydet toisiinsa.



KUVA 4. Eri laitteiden yhteydet toisiinsa ja yhteysmetodit.

6.1 Kytkimen asetukset

Työ aloitettiin kytkimen konfiguroinnilla. Testikytkimeksi saatiin Cisco Catalyst 2960-s -24ps-l -kytkin, jossa on 24 gigabit ethernet-porttia, 1 fast ethernet-portti ja 4 kuituporttia. Kytkimessä käytetty ohjelmistoversio oli 12.2.

Konfiguraation pohjaksi saatiin Saitalla käytössä olleen vanhan Cisco-kytkimen konfiguraatio tekstitiedostona, jota lähdettiin muuttamaan. Tarkoitus oli muokata konfiguraatio ensin sopivaksi ja sitten ajaa se kerralla kytkimeen. Muutosprosessi aloitettiin lisäämällä porttien määrää, sillä niitä oli konfiguraatiossa aluksi vain kahdeksan. Kun ne oli saatu kuntoon, muokattiin VLAN-listan ajan tasalle. Lisäksi muutettiin kytkimen nimi, käyttäjätunnukset ja salasanat.

Kun perusmuutokset oli saatu valmiiksi, keskitettiin huomio kytkimen AAA-asetuksiin, erityisesti seuraaviin riveihin:

aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

dot1x system-auth-control

Aaa new-model mahdollistaa AAA:n käytön. Seuraava rivi taas luo 802.1X porttikohtaisen autentikointimetodilistan. Kolmas rivi mahdollistaa VLAN:ien ja ACL:ien (Access Control List) käytön. Toiseksi viimeinen rivi mahdollistaa 802.1X-tilastoinnin sekä MAB:n käytön ja viimeinen mahdollistaa 802-1X –porttikohtaisen autentikoinnin. Seuraavaksi RADIUS-serverin asetukset /9; 12./

radius-server host xxx.xxx.xxx.xxx auth-port 1645 acct-port 1646
radius-server key (RADIUS SHARED SECRET)

Näillä asetuksilla määritetään, mihin RADIUS-palvelimeen kytkin ottaa yhteyden ja mikä on yhteydessä käytetty salasana. Palvelimen IP-osoitteeksi laitettiin ACS:n osoite, sillä kytkimen haluttiin autentikoivan siihen liitettävät päätelaitteet ACS:n kautta. Seuraavaksi määritettiin porttien asetukset, joista esimerkki löytyy seuraavasta /9; 12./

interface GigabitEthernet1/0/3
switchport mode access
authentication event fail action authorize vlan A
authentication event no-response action authorize vlan A
authentication port-control auto
mab
snmp trap mac-notification change added
dot1x pae authenticator
dot1x timeout quiet-period 5
dot1x timeout tx-period 1
dot1x max-reauth-req 1

Switchport mode access –rivi pakottaa portin päätelaitekäyttöön eikä sitä silloin voi käyttää trunk-porttina. Seuraavalla rivillä määritetään se VLAN, johon yhteys ohjataan, ellei autentikointi onnistu. Kolmas rivi tekee saman siinä tapauksessa jos RADIUS-palvelin ei vastaa. Authentication port-control auto mahdollistaa porttikohtaisen autentikoinnin tässä portissa. Mab taas mahdollistaa MAC Authentication Bypass:n käytön. SNMP-trap –rivillä mahdollistetaan portin kautta tapahtuvien MAC-osoitteiden muuttumisen ilmoittaminen eteenpäin. Neljä alinta riviä liittyvät 802.1X-

autentikointiin: ylimmässä mahdollistetaan 802.1X-autentikointi portissa ja seuraavassa määritetään sekunneissa, kuinka kauan kytkin pysyy hiljaisessa tilassa epäonnistuneen autentikoinnin seurauksena. Toiseksi alimmassa määritetään, kuinka kauan kytkin odottaa vastausta EAP-pyyntöön ennen pyynnön uudelleenlähetystä. Alimmassa määritetään autentikointiyritysten määrä, ennen kuin kytkin määrittää portin ei-autentikoituun tilaan. /9; 12./

Kun porttien asetukset oli määritetty, säädettiin SPAN/PORT MIRRORING-asetukset, jotta Collector saisi analysoitavaa liikennettä. Määritykset tapahtuivat seuraavalla tavalla.

monitor session 1 source interface Gi1/0/1 , Gi1/0/3 - 24
monitor session 1 destination interface Gi1/0/2

Ylemmällä rivillä määritetään ne portit, joiden liikennettä peilataan ja toisella rivillä se portti, johon kerätty tieto ohjataan. Viimeinen työn kannalta oleellinen rivi oli: /9; 12/

snmp-server host (collectorin IP-osoite) (COMMUNITY STRING) mac-notification snmp

Tällä rivillä määritetään se palvelin, tässä tapauksessa NAC Profiler Collector, johon SNMP Trap –tiedot lähetetään. Community string-kohdan täytyy täsmätä NetTrap-moduuliin säädetyn kanssa. /9; 12./

6.2 ACS:iin tehdyt asetukset

Autentikointiratkaisuista tutustuin ensin ACS:iin ja sen moniin ominaisuuksiin. Käytin Cisco Systemsin kotisivulta saamaani ohjekirjaa hyödyksi ja kokeilin suodatusasetusten tekoa ensin laboratorio-olosuhteissa. Testi koostui Saitan verkosta, johon ACS oli kytketty, kytkimestä, joka oli liitetty Saitan verkkoon ja kolmesta eri VLAN:eihin kirjautuvasta tietokoneesta. Kytkin oli konfiguroitu niin, että portit 1-23 käyttivät 802.1X-tunnistusta ja portti 24 toimi trunk-porttina seuraavaan kytkimeen. Jotta ACS olisi toiminut AAA-palvelimena, liitin edellä mainitun kytkimen nimen, IP-

osoitteen ja shared secret-salasanan ACS:n verkkolaitelistaan. Kytkimeen piti lisäksi määrittää radius-palvelimen asetuksiin ACS:n IP-osoite ja sama shared secret-salasana. Liitin kytkimeen aluksi kolme eri toimialueiden sertifikaateilla varustettua tietokonetta, joista kaksi käytti EAP-TLS –kirjautumista ja yksi PEAP:ia MS-CHAPv2:lla. Koska käytettäviä protokollia oli kaksi, jouduin tekemään moneen asetuskohtaan niille molemmille merkinnät. Kytkimen konfiguraatio löytyy liitteestä 2.

ACS oli osittain jo valmiiksi säädetty, siihen oli mm. tuotu valmiiksi kaksi sertifikaattia, juurisertifikaatti ja asiakassertifikaatti, joita autentikoinnissa tarvitaan ja joitain suodatusasetuksia. Tästä johtuen siirryttiin seuraavaan vaiheeseen ja tuotiin ACS:lle niitä AD-ryhmiä, joilla on tarvittavien VLAN:ien käyttäjien tunnuksia. Näitä siis tarvitaan siihen, että kirjautuvan käyttäjän päätelaite osataan AD-ryhmän tietojen perusteella ohjata kytkimellä oikeaan VLAN:iin. Lisäksi säädettiin LDAP:n palvelinasetukset, jotta MAB–autentikointi toimisi. Koska LDAP-servereitä (tässä tapauksessa NAC Profiler Server) oli vain yksi, vain ensisijaiseen serveriin säädettiin seuraavat asetukset:

- **Hostname: (Profiler serverin IP-osoite)**
- **Port: 389 (oletusarvo)**
- **Anonymous/Authenticated access: Authenticated**

Viimeisimmässä kohdassa valitaan, käytetäänkö yhteyteen autentikointia. Jos autentikointi valitaan, silloin syötetään käyttäjätunnus ja salasana:

- **Admin DN: cn=root,o=beacon**
- **Password: GBSbeacon**

Admin DN eli Distingueshed Name tulisi aina olla yllä oleva ja salasana on tehdasmäärityksenä GBSbeacon. Jos yhteyden muodostamiseen halutaan käyttää sertifikaattia, sen saa tehtyä valitsemalla Use Secure Authentication ja tämän jälkeen valitsemalla sertifikaatti liukuvalikosta. Näiden jälkeen painetaan Test Bind to Server, joka kertoo, onnistuuko yhteys. Autentikointiin käytettäviä laiteprofiileja saa lisättyä samalla tavalla, kuten AD-ryhmiä Active Directoryn asetuksissa.

Seuraava vaihe oli määritellä Identity Store Sequencet, joita tehtiin kaksi: 802.1X ja 802.1X with certificates. Ensimmäisen tarkoituksena on toimia käyttäjätunnuksien hakusääntönä PEAP-autentikointipyynnöille ja toisen EAP-TLS:lle. 802.1X:n asetuksiin säädin nimen, autentikointimetodiksi salasanapohjaisen ja autentikointi- sekä attribuuttien hakemislistaan AD1:n, jolloin tunnuksia haetaan ensisijaisesti Active Directorylta. 802.1X with certificatesin asetuksiin taas laitettiin nimi, autentikointimetodiksi sertifikaattipohjaisen ja lisäksi kohtaan Additional Attribute Retrieval Search List valinnan AD1, jolloin onnistuneen sertifikaattikirjauksen jälkeen käyttäjätunnuksia haetaan AD:lta. LDAP:ta varten ei tehty profiilia, sillä NAC Profilerilla se on oletusarvoisesti olemassa valmiiksi.

Seuraavaksi määriteltiin auktorisointiprofiilit jokaiselle AD-ryhmälle. Tämä on tärkeää, sillä näillä profiileilla määrätään mihin VLAN:iin kukin autentikointipyyntö ohjataan jos pyyntö läpäisee suodatussäännöt. Vain nimi ja staattinen VLAN-numero määriteltiin jokaiseen profiiliin, joita tuli käytännössä yksi yhtä AD-ryhmää kohti. Niille laitteille, jotka halutaan autentikoida, luodaan tänne omat profiilit, esim. tulostimet.

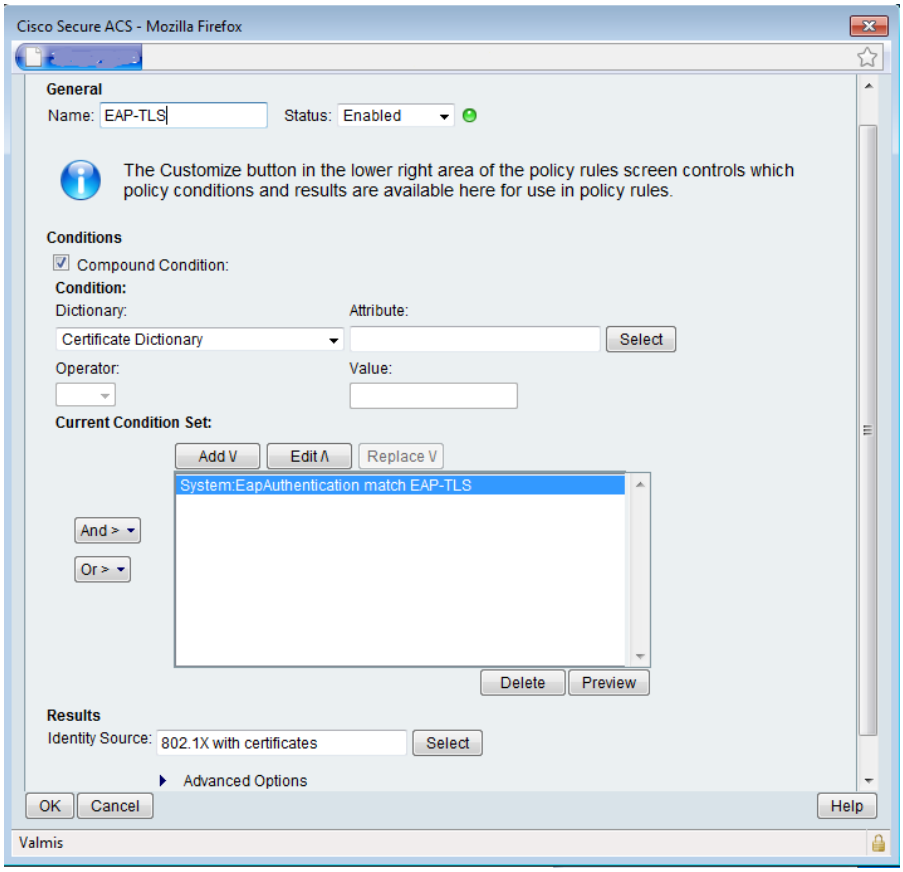
Tämän jälkeen siirryttiin tärkeimpään kohtaan eli Access Service –käytäntöjen tekemiseen. Ensimmäinen askel oli tehdä Service Selection –käytännöt, jotka ovat suodatuksen ensimmäinen vaihe. Käytäntöjä oli kaksi: RADIUS ja TACACS. Radiukselle säädin säännöiksi seuraavat:

- **Protocol match Radius**
- **RADIUS-IETF:Service-Type match framed or RADIUS-IETF:Service-Type match call-check**
- **RADIUS-IETF:NAS-Port-Type match Wireless-IEEE-802.11**

Jälkimmäisen säännön toinen osio tarkistaa, onko kyseessä MAB-autentikointi, ja kolmas sallii langattoman verkon tukiaseman kautta tulevat pyynnöt. Result-kohtaan laitettiin seuraavaksi säädettävän Access Service-käytäntö. TACACS-käytännölle laitettiin säännöksi vain Protocol match Tacacs.

Yksi Access Service -käytäntö riittää oikein hyvin, sillä erilaiset autentikointipyynnöt voidaan käsitellä erikseen luomalla sääntöjä Authorization-kohtaan. Ensimmäinen pykälä on siis käytännön luominen ja niitä luotiin yksi, nimeltään 802.1X-

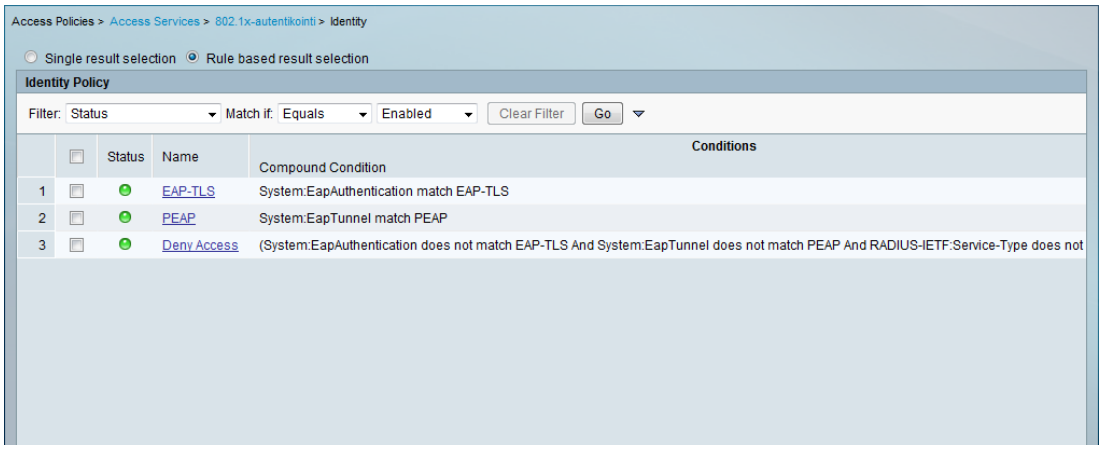
autentikointi. Autentikointiprotokollista sallittiin EAP-TLS:n ja PEAP:in, sillä kuten aiemmin jo mainittiin, ne ovat ne kaksi autentikointiprotokollaa jota tässä työssä käytettiin. Lisäksi sallittiin Process Host Lookup, joka hoitaa MAB-autentikoinnin. PEAP-protokollan alta sallittiin lisäksi MS-CHAPv2. Tämän jälkeen luotiin neljä identiteettikäytäntöä: EAP-TLS:n, PEAP:n, Deny Access:n ja Mac Auth:n. EAP-TLS:ään laitettiin seuraavanlainen yhdistesääntö eli Compound Condition: **System:EapAuthentication match EAP-TLS**, mikä tarkoittaa sitä, että ainoa autentikointitapa, jonka tämä käytäntö hyväksyy, on EAP-TLS. Lisäksi laitettiin sen identiteettilähteeksi aiemmin luotu 802.1x with certificates, kuten kuvasta 5 näkyy.



KUVA 5. Access Servicen EAP-TLS –Identity Policy

PEAP-käytännölle annettiin seuraavanlainen yhdistesääntö: **System:EapTunnel match PEAP**. Tämä sääntö sallii ainoastaan PEAP-autentikoinnin. Lisäksi laitettiin identiteettilähteeksi 802.1X-profiili. Kolmas käytäntö on Deny Access, joka estää pääsyn eteenpäin. Tämä tapahtuu yhdistesäännöllä **System:EapAuthentication does not match EAP-TLS And System:EapTunnel does not match PEAP And RADIUS-**

IETF: Service-Type does not match Framed. Sääntö siis tutkii, täsmääkö autentikointipyyntö kumpaankaan protokollaan, ja tutkii lisäksi, onko autentikointipyyntö 802.1X:n EAP-protokollien mukainen. Viimeiselle käytännölle, eli Mac Auth:lle, annettiin yhdistesäännöksi **RADIUS-IETF:Service-Type match call-check**, joka jo aiemmin selitettiin. Valmiit policyt ja niiden säännöt, poislukien Mac Auth, näkyvät kuvassa 6.



KUVA 6. Access Serviceen määritetyt Identity Policyt

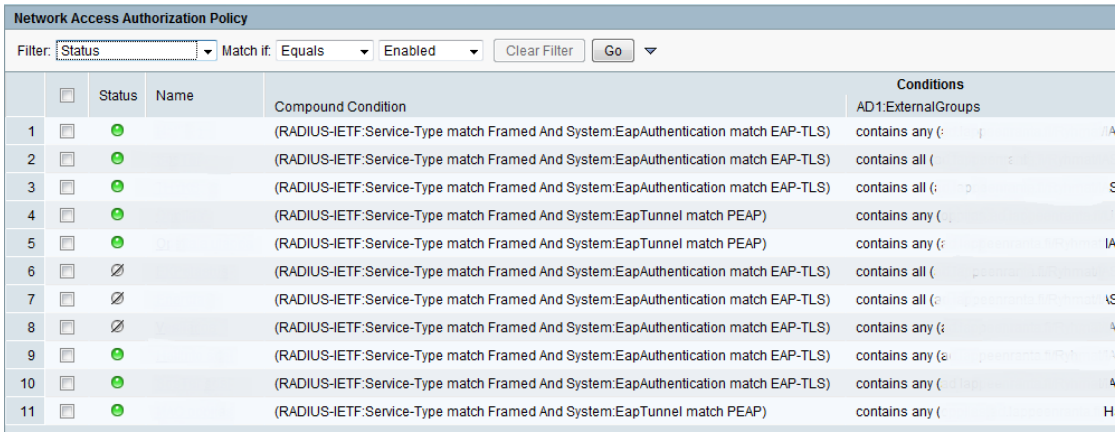
Seuraava askel oli tehdä verkkoon liittymisen valtuutuskäytännöt (Network Access Authorization Policy), joilla varsinainen suodatus tapahtui. Jotta kaikkien eri AD-ryhmien suodatus olisi onnistunut oikeisiin VLAN:eihin, niitä tehtiin useita, kuten kuvasta 7 näkyy. Käytännöt kannattaa nimetä tapauskohtaisesti ja yhteyttä kuvaavasti, jolloin mahdollisten asetusongelmien ratkaiseminen helpottuu. Jokaiselle käytännölle määritetään nimi, yhdistesäännöt, joita voi olla yksi tai useampia, AD-ryhmät, johon 802.1X:n mukaisen asiakkaan on kuuluttava ja valtuutusprofiili, jonka mukaisesti hyväksytty autentikointi yhdistetään. MAB-autentikointia varten kannattaa lisätä customize-painikkeella Use Case – ja NAC Profiler:ExternalGroups -valinnat, jolloin näille käytännöille päästään määrittämään tarvittavat asetukset, eli **Use Case match Host Lookup** ja halutut laiteprofiilit. AD-ryhmiä lisätessä kannattaa olla tarkkana, sillä jos ryhmäkentän yläpuolella olevasta liukuvalikosta valitsee Contains All -vaihtoehdon ja valittuja ryhmiä on useita, silloin asiakkaan on löydyttävä niistä jokaisesta. Contains Any -vaihtoehdolla riittää, että se löytyy vain yhdestä. Lisäksi yhdistesääntöjä luodessa kannattaa miettiä ensin mitä haluaa kunkin käytännön tekevän, sillä erilaisia sään-

tövaihtoehtoja on valtavasti ja niistä riippuu koko ACS:n toiminta. Työssä käytettiin lähinnä kahta erilaista yhdistesääntöä:

- **RADIUS-IETF:Service-Type match Framed And System:EapAuthentication match EAP-TLS**

- **RADIUS-IETF:Service-Type match Framed And System:EapTunnel match PEAP**

Näillä säännöillä ainoat hyväksyttävät autentikointipyynnöt määritellään tuleviksi RADIUS-kapseloituina EAP-TLS- ja PEAP-autentikointiviesteinä. Sääntöjä tehdessä suosittelen tutustumaan ensin RADIUS-kirjastoihin, joita yhdistesäännöissä on tarjolla, ja niiden ominaisuuksiin. Myös ACS 5.1 käyttäjän ohjekirjasta on valtavasti apua. Kuvassa 7 on valmiit suodatussäännöt, pois lukien tulostus, joita Saitan verkon autentikoinnissa käytettiin.



KUVA 7. Access Serviceen määritetyt suodatussäännöt, nimet ja AD-ruhmät peitettynä

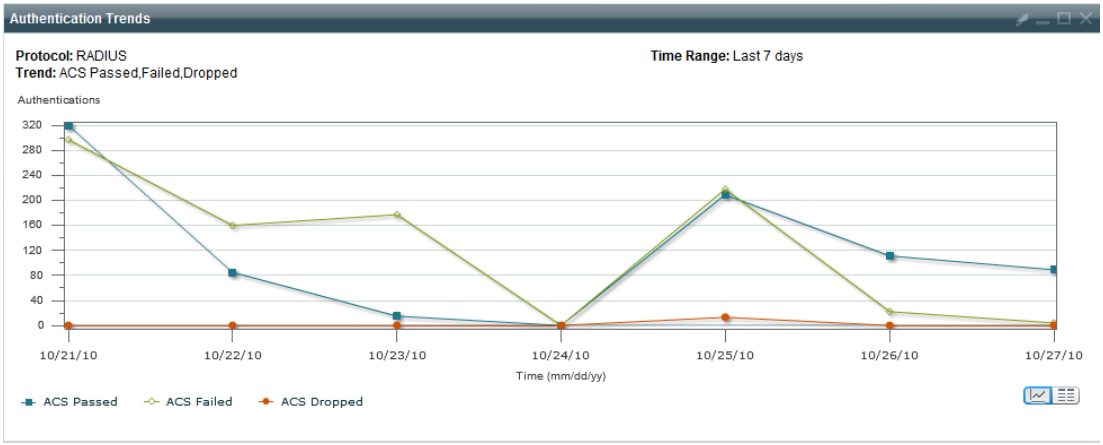
6.3 Autentikoinnin testaus

ACS:n asetusten testaaminen aloitettiin laboratorioympäristössä, jossa Cisco Catalyst 2960-S –kytkin oli liitetty trunk-portiksi säädetystä gigabit ethernet –portti 24:stä Hewlett-Packard Procurve –kytkimeen, joka oli osa Saitan verkkoa. Catalyst-kytkin oli siis nyt yhteydessä ACS:iin. Ciscon kytkimeen liitettiin kolme tietokonetta, joista

kaksi oli kannettavia sertifikaateilla autentikoituvia ja yksi oli työasema, joka autentikoitui aluksi konetunnuksen perusteella ja sitten käyttäjätunnus-salasana –yhdistelmällä. Kytkimen fyysiset portit 1-23 oli säädetty 802.1X-tunnistusta käyttäviksi, joten ei ollut väliä, mihin portteihin nämä kolme konetta liitettiin. MAB-autentikointitestauksesta kerrotaan myöhemmin NAC Profilerin osiossa.

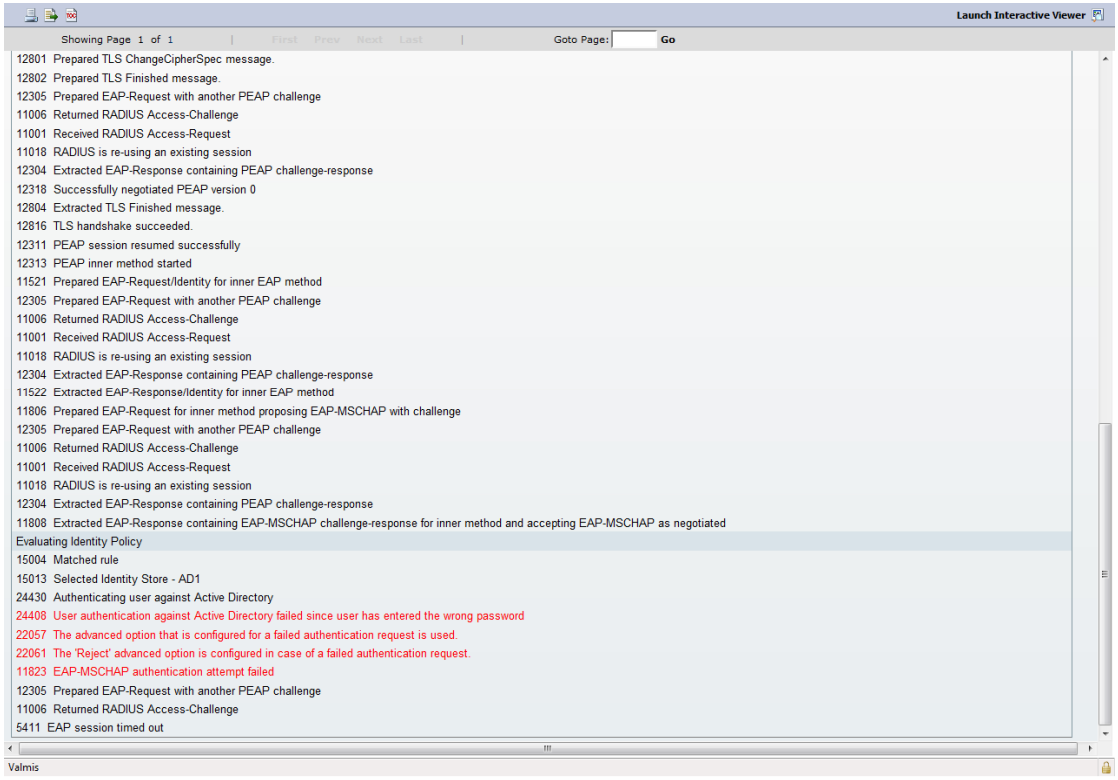
Testauksessa käytettiin apuna ACS:n omia valvontatyökaluja ja kytkimen komentorivikäyttöliittymää. ACS:n autentikointilokista näkyi tapauskohtaisesti, onnistuiko autentikointi, ja jos ei onnistunut, syyn sai melko helposti selville. Yleisin syy epäonnistumiseen oli liian epämääräisesti määritetyt säännöt, jolloin yhteyspyyntö, jonka olisi pitänyt siirtyä VLAN:iin A, siirtyikin, VLAN:iin B. Lisäksi useita autentikointipyyntöjä hylättiin siksi, että oli valittu väärä AD-ryhmä, josta identiteetti tarkistetaan. Myöhemmin huomattiin, että ACS:n lokista näkee ne ryhmät, joihin kukin tietokone tai käyttäjä kuuluu. Kun testikoneiden autentikointi oli saatu toimimaan, siirryttiin käyttämään ACS:ää laajemmin Saitan verkossa ja ACS:n RADIUS-asiakkaiksi liitettiin aluksi sellaisia kytkimiä, joissa oli vain muutamia tietokoneita kiinni ja joiden toiminta ei ollut niin kriittistä. Yksi näistä oli Saitan asennuspisteen kytkin, joka tuotti autentikointilokiin valtavasti epäonnistuneita autentikointeja johtuen lähinnä siitä, että koneet, joita siihen liitettiin, olivat joko uusia ja niitä ei ollut vielä liitetty mihinkään AD-ryhmään tai sitten niissä oli vanhentuneet sertifikaatit. Joitain muitakin epäonnistuneita pyyntöjä tuli, mutta ne saatiin loppumaan muokkaamalla sääntöjä ja käytäntöjä. Tässä vaiheessa autentikointipyyntöjä tuli päivässä n. 30 kappaletta poislukien asennuspisteeltä tulleet epäonnistuneet autentikoinnit. Näistä kolmestakymmenestä keskimäärin 20-25 oli onnistuneita autentikointeja, loput epäonnistuneita joko viallisten sääntöjen tai sitten ACS:lle ilmeisesti tyypillisen EAP timeout-vian takia. Tukifoorumeilta ilmeni, että tämä vika on melko yleinen. Se saattaa johtua liian hitaasta tunnusten syöttämisestä eikä haittaa autentikoinnin varsinaista toimintaa. Jostain syystä ACS vain kirjaa näitä virheilmoituksia.

Kun ACS:n toiminta näiden kytkimien kanssa oli varmistettu, ACS:n autentikoinnin piiriin liitettiin kolmen eri Lappeenrannan seudulla olevan pienehkön koulun kytkimet. Tästä seurasi päivittäisten autentikointipyyntöjen moninkertaistuminen, sillä nyt näiden koulujen oppilaat ja henkilökunta käyttivät ACS:ää autentikointiin. Pyyntöjen määrä liikkui päivästä riippuen n. 100 - 300 välillä. Joitain ongelmia ilmeni taas, mutta ne korjautuivat tarkastamalla AD-ryhmät ja viilaamalla sääntöjä.



KUVA 8. Autentikointitrendikäyrä ajalta 21.10. – 27.10.2010

Kuvassa 8 näkyy autentikointitapahtumamäärät seitsemän päivän ajalta. Estettyjen yhteyksien määrä johtuu suurimmaksi osaksi asennuspisteen koneasennuksista, mutta 23. päivän, joka oli lauantai, on poikkeus. Silloin lokiin kerääntyi valtavasti epäonnistuneita autentikointeja, joiden syyksi ACS ilmoitti väärän salasanan PEAP-autentikoinnissa. Kyseiset tapahtumat löytyivät lokista, mutta ne eivät sisältäneet mitään tietoa autentikointia pyytävästä päätelaitteesta eivätkä myöskään siitä verkkolaitteesta, joka pyynnön oli välittänyt. Tämän vuoksi epäiltiin, että ACS:ssä oli tapahtunut virhe, jonka takia se toisti samaa virheilmoitusta. On kuitenkin mahdollista, vaikkakin epätodennäköistä, että joku on yrittänyt tunkeutua verkkoon, sillä kuvassa 9 näkyvistä autentikoinnin vaiheista ilmenee, että autentikointi on läpäissyt PEAP-pyynnöt, eli sillä on asiakassertifikaatti kunnossa, mutta AD-tilin salasana on ollut väärä. Yhteyspyyntöjä tuli n. 1,5 minuutin välein, joten voisi olla mahdollista, että joku ohjelma oppilaskoneella yrittää autentikoida itseään.

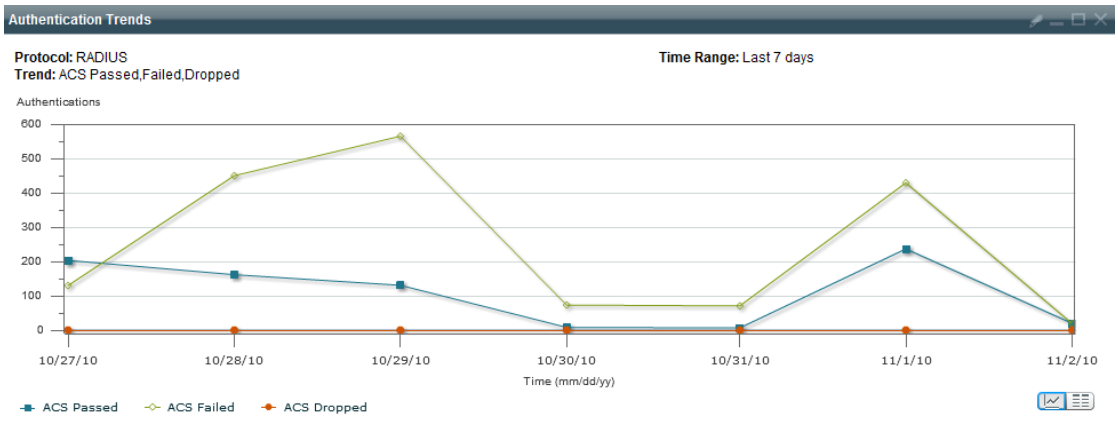


KUVA 9. Lauantaina 23.10. tapahtuneen hylätyn yhteyspyynnön autentikoinnin vaiheita

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instanc
Oct 23,10 8:43:25.150 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:41:59.923 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:40:24.920 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:38:54.906 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:37:24.886 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:35:54.876 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:34:24.846 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:32:54.856 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:31:24.806 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:29:54.916 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:28:24.796 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:26:54.776 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:25:24.726 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:23:54.726 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:22:24.726 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:20:55.533 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:19:24.656 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:17:54.693 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:16:24.653 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:14:54.643 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:13:24.603 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:11:54.606 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:10:24.583 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:08:54.583 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:07:24.546 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:05:54.653 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:04:24.516 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:02:54.483 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 8:01:24.463 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 7:59:59.453 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 7:58:24.420 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 7:56:54.436 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs
Oct 23,10 7:55:24.623 AM	✖					802.1x-autentikointi	PEAP (EAP-MSCHAPv2)					ciscoacs

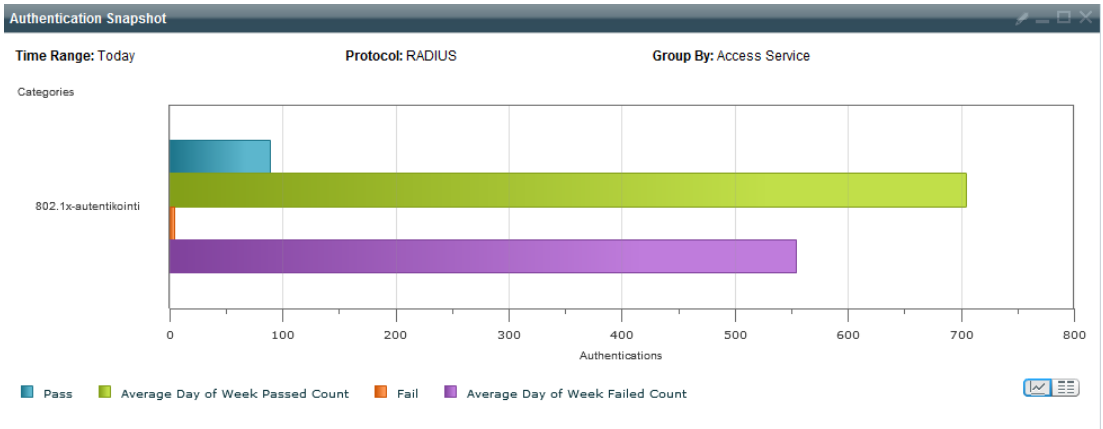
KUVA 10. Ote lauantain 23.10. autentikointilokista

Edellisellä sivulla kuvassa 10 näkyy, miten näitä omituisia autentikointipyyntöjä tuli melko tarkasti 1,5 minuutin välein. Mystisintä on se, ettei ACS ole saanut autentikointia yrittävän laitteen MAC-osoitetta eikä myöskään tietoja siitä kytkimestä, jonka kautta pyynnöt tulivat. Kuvassa 8 näkyy maanantain 25.10 kohdalla myös 12 kappaletta hylättyjä (dropped) autentikointipyyntöjä, jotka johtuivat siitä, että erään kytkimen IP-osoite oli kirjoitettu väärin, eikä ACS täten tunnistanut kyseiseltä laitteelta tulevia pyyntöjä.



KUVA 11. Autentikointitrendikäyrä ajalta 27.10. – 2.11.2010

Kuvassa 11 näkyy autentikointimäärät viikon ajalta. Korkeat epäonnistumismäärät johtuvat taas asennuspajan koneasennuksista. Ajankohta, jolloin määrät laskevat vähiin on lauantai – sunnuntai ja sen epäonnistumiset johtuvat myös asennuspajasta, sillä sinne oli jätetty viikonlopun ajaksi tietokoneita asentumaan. Kuvakaappaus on otettu aamulla n. klo. 9:00, joten 2.10. tapahtuneita tunnistautumisia ei ole vielä monta.



KUVA 12. Ruutukaappaus autentikoinnista 27.10.2010

Kuvassa 12 näkyy yhden päivän autentikoinnit Access Service-käytännöittäin lajiteltuna. Kuten asetuksissa mainittiin, tehtiin vain yksi käytäntö. Kuva on klo. 9:45 olleesta tilanteesta, joten tulleita autentikointeja ei ole vielä kovin paljon. Kuten kuvasta voi huomata, sallittuja yhteyksiä on suhteessa hylättyihin valtavasti. Tämä on melko todenmukainen kuva ACS:n autentikoinnin toimimisesta, sillä tässä ei ole vielä mukana asennuspisteen aiheuttamia hylättyjä yhteyksiä. Päivän päätteeksi hyväksyttyjen yhteyksien määrä oli n. 200 ja hylättyjen n. 130.

6.4 NAC Profileriin tehdyt asetukset

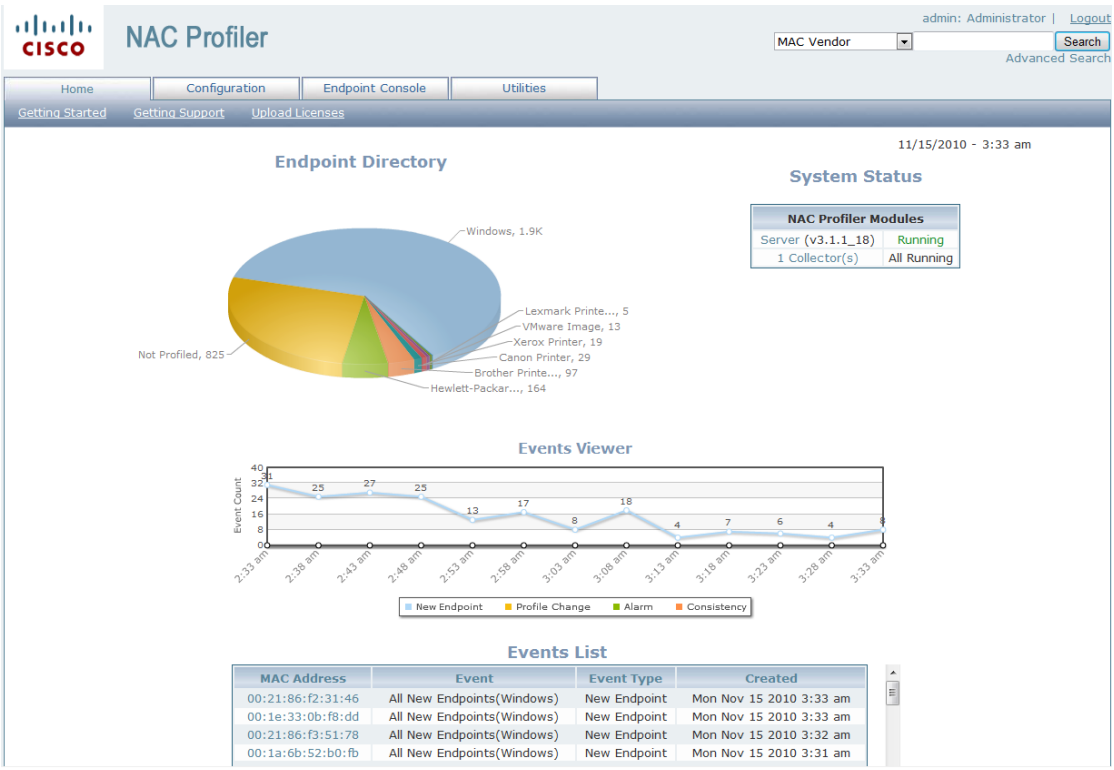
Työssä käytetty NAC Profiler -järjestelmä koostui kahdesta Cisco NAC Appliance 3350 –laitteesta, jotka olivat kumpikin kooltaan 1 RU eli yhden Rack Unitin. Toinen piti sisällään NAC Profiler Serverin ja toinen Collectorin. Alun perin laitteissa oli Profiler-ohjelmiston versio 2.1, mutta molempiin ladattiin uudempi ohjelmisto, joka oli versioltaan 3.1.1_18.

NAC Profilerin toiminnot sijoittuvat kahteen eri laitteeseen: Collectoriin (yhteen tai useampaan) ja Serveriin. Aloitetaan Collectorista. Se sijaitsee NAC Appliance Clean Access Serverissä (CAS) ajettavana moduulina ja on säädettävä laitteen komentokehotteessa, joka on unix-pohjainen. Sekä Serverissä että Collectorissa säädetään aluksi perusasetukset, jotka sisältävät mm. ethernet-porttien IP-osoitteet, aliverkon peitteet ja oletusyhdyskäytävät, laitteen nimen sekä eritasoiset käyttäjätunnukset ja niiden nimet. Eth0 on oletuksena molemmissa laitteissa se portti, jonka kautta liikennöidään. Kun asetukset on tehty ohjeiden mukaisesti /5, chapter 4/, päästään säätämään Collectorin asetuksia. Collectoriin liittyvät komentokehotekäskyt ovat

- **service collector config** asetukset
- **service collector start** collectorin käynnistys
- **service collector stop** collectorin sammutus
- **service collector verify** näyttää collectorin asetukset
- **service collector status** näyttää moduulien tilan
- **service collector restart** uudelleenkäynnistää collectorin

Listan ensimmäisellä komennolla päästään asetuksiin. Alussa kysytään, haluaako käyttäjä mahdollistaa collectorin käytön ja halutaanko sen asetuksia muuttaa. Kun näihin on vastattu kyllä, päästään säätämään varsinaiset collector-asetukset eli laitteen nimi, toimiiko Collector palvelimena vai asiakkaana, IP-osoite johon Collector on yhteydessä (Profiler Serverin eth0:n osoite), porttinumero (oletuksena 31416), salaustapa (AES, Blowfish tai ei mikään) ja shared secret –salasana. Seuraavaksi Profiler Serverin asetukset.

Profiler Serverin perusasetukset tehdään jo ensimmäisellä käynnistyskerralla, tosin niitä pääsee muuttamaan myöhemminkin komentokehotekäskyllä **service profiler config**. Laitteen perusasetukset saa helposti määritettyä verkkokohtaiseksi ruudussa näkyviä ohjeita seuraamalla /5, chapter 4/. Kun perusasetukset on määritetty, päästään selainhallinnalla käsiksi Profiler Serverin asetuksiin. Selainhallintaan pääsee käsiksi kirjoittamalla selaimen osoitekenttään **https://(profilerin ip-osoite)**, käyttäjätunnukseksi admin ja salasanaksi perusasetuksissa säädetty verkkohallinnan salasana. Näkyviin tulee kuvan 13 mukainen sivu.



KUVA 13. NAC Profilerin etusivu

Kuvasta 13 näkyy eri profiilien osuus koko verkon laitemäärästä piirasdiagrammina, Profiler serverin ja collectorien tila ja profilerin tapahtumat viiden minuutin välein, sekä käyränä että taulukkona esitettynä. Kuvankaappauksen aikaan profiler-järjestelmä oli kytkettynä Saitan verkkoon ja järjestelmä profiloi n. 3100 päätelaitetta, joista 825 oli kyseisellä hetkellä vielä tuntemattomia.

Profileria säädettäessä työnkulku on seuraava: lisenssien asennus, verkkoasetusten teko, palvelinasetukset, Collectorien lisääminen, verkkolaitteiden lisääminen, päätelaiteprofiilien teko, raportointitapahtumien määritteleminen, integrointi muiden verkkolaitteiden, esimerkiksi ACS:n, kanssa ja käyttäjätilien muokkaaminen.

Ensin ladataan lisenssitiedosto, joka mahdollistaa Serverin kaikki toiminnot. Kyseinen lisenssitiedosto on aina laitekohtainen, ja sen saa Ciscon edustajalta. Kun tiedosto on saatu, se ajetaan Serveriin valitsemalla etusivulta **Home > Upload Licenses**. Aukeavassa ikkunassa päästään etsimään tietokoneelta kyseinen lisenssitiedosto, joka sitten hyväksytään Import License –painikkeella. Kun lisenssi on hyväksytty, pitäisi etusivulla näkyä Serverin tilana **Running** (kuva 13). Käyttämäni lisenssitiedosto oli demolisenssi, joka oli voimassa vain rajoitetun ajan.

Seuraavaksi säädettiin verkkoasetukset kohdasta **Configuration > My Network**. Aluksi syötetään nimi sille verkolle, joka halutaan liittää tutkittavaksi. Seuraavaksi verkon IP-segmentti, jota halutaan tutkia, esimerkiksi 192.168.100.0/24. Kolmannessa kentässä voidaan määritellä ne tutkittavan verkon osiot, joita ei haluta mukaan. Sitten tulostuspalvelimien IP-osoitteet ja lopuksi Voice gatewayt. Näistä kentistä syötin tietoa vain kahteen ylimpään ja toiseksi alimpaan. Alla olevassa kuvassa 14 näkyy säätömahdollisuudet. Lisää verkkoja voi määritellä tarpeen mukaan.

KUVA 14. Tutkittavan verkon määrittäminen

Seuraava vaihe oli palvelinasetusten säätäminen kohdasta **Configuration > Modules > server**. Näitä asetuksia ei tarvitse välttämättä muokata kovinkaan paljon, tärkeintä tämän opinnäytetyön kannalta oli aktivoida LDAP ja säätää verkkoyhteydet. Jälkimmäisen tarkoitus on määritellä se yhteystapa, jolla Collectorit ovat yhteydessä serveriin. Add Connection –painikkeesta pääsin säätämään seuraavanlaisen yhteyden: **Server: xxx.xxx.xxx.xxx[31416] using AES**. Aukeavaan asetusikkunaan laitettiin siis yhteystavaksi palvelin, sillä haluan, että collectorit toimivat asiakkaina. IP-osoitekenttään määritettiin serverin osoite ja porttinumero annettiin olla oletusarvossaan. Salaustyypiksi valittiin AES, sillä Serverin ja Collectorin välinen yhteys haluttiin salata. Kun salaustapa oli valittu, päästiin säätämään shared secret –salasanan, jonka oli täsmättävä Collectorissa olevan kanssa. Yhteys hyväksyttiin Add Connection-painikkeella. Muut palvelimen asetukset käsittelivät lähinnä profiilien vanhenemisaikoja ja Profilerin linkittämistä NAC-järjestelmään ja olivat tämän työn kannalta toissijaisia.

Kun palvelin oli säädetty, oli aika lisätä Collector-moduuli konfiguraatioon. Tämä tapahtui valitsemalla **Configuration > Modules > Add Collector**. Ensimmäiset asiat, jotka määritetään, ovat Collectorin nimi ja sen sisältävän NAC-laitteen eth0-portin IP-osoite. Näiden jälkeen päästään muokkaamaan Collectorin moduulien asetuksia. Tärkein näistä on Forwarder, sillä se hoitaa liikennöinnin Profiler-järjestelmässä. IP-osoitekentässä pitäisi nyt olla Collectorin osoite ja Connection-kohtaan valitaan edellisessä kappaleessa määritetty yhteys, jonka pitäisi olla muodossa **Connect to: Server (xxx.xxx.xxx.xxx:31416)**. Kun tämä on määritetty, voidaan Collector tallentaa ja päivittää moduulit. Niiden uudelleenkäynnistyksessä kestää hetki, mutta jos yhteys Serverin ja Collectorin välillä toimii, moduulien tilan pitäisi vaihtua oranssista No Contact –tilasta Running-tilaksi, joka on kirjoitettu vihreällä.

Muita tärkeitä asetuskohtia ovat NetTrapin Community String, jonka tulee vastata valvottavan verkkolaitteen SNMP-asetuksiin määritetyn kanssa ja NetWatch, johon määritetään se Collector-laitteen ethernet-portti. Vähemmän kriittisiä ovat loput moduulit, eli NetInquiry ja NetRelay. NetMapissa ei oikeastaan ole edes juuri säädettävää ja sen voikin antaa olla sellaisenaan ellei erityistä muutostarvetta esiinny. Tässä vaiheessa kun asetukset on tehty, kannattaa taas uudelleenkäynnistää moduulit, jotta uudet asetukset tulisivat voimaan.

Seuraavaksi siirryttiin määrittämään verkkolaitteita, joiden liikennettä tutkittaisiin. Tämän työn tapauksessa niitä oli vain yksi, eli Ciscon Catalyst 2960-s –kytkin. Tämä tapahtui valitsemalla **Configuration > Network Devices > Add Device**. Network Devices –kohdasta pystyy myös linkittämään Profilerin AD-palvelimeen, jolloin päätelaitteiden profilointiin tulee yksi mahdollisuus lisää. Mutta nyt palataksemme päätelaitteisiin, niitä lisätessä on paljon säätömahdollisuutta. Ne kohdat, joilla saavutettiin perustoiminnallisuus, olivat seuraavat:

- **Device Name** Laitteen nimi
- **IP Address** Laitteen IP-osoite
- **Setting Type: Layer 2** Layer 2, koska laite oli kytkin
- **Collector Mapping Module** Aiemmin lisätty collector
- **Trunk Ports: xx** Trunk-portit, numero xx
- **Access: Method : SNMP 1**
- **Read-Only Community String** aiemmin määritetty tekstijono

Näillä asetuksilla saatiin Collector keräämään melkoisen määrän tietoa päätelaitteista ja niiden liikennöinnistä.

Tässä vaiheessa oli oikeastaan saatu kaikki yhteyden kannalta oleellisimmat vaiheet valmiiksi. Kokonaisuudesta puuttui enää päätelaiteprofiilien ja ilmoitustapahtumien teko. Laiteprofiilien tekemistä selitän myöhemmin kohdassa 6.3.2.

Profileriin tehtiin kahdet erilaiset asetukset, joista ensimmäisessä linkitettiin se toimimaan ACS:n kanssa ulkoisena identiteettivarastona ja samalla tutkittiin miten se tunnistaa verkossa olevia päätelaitteita. Toisessa tehtiin testilähiverkko, joka oli täysin Saitan verkon ulkopuolella. Tässä tapauksessa lähiverkon keskipisteenä oli Ciscon Catalyst 2960-S –kytkin, jonka portteihin liitettiin kaikki laitteet.

6.4.1 Autentikointitestaus ACS:n kanssa

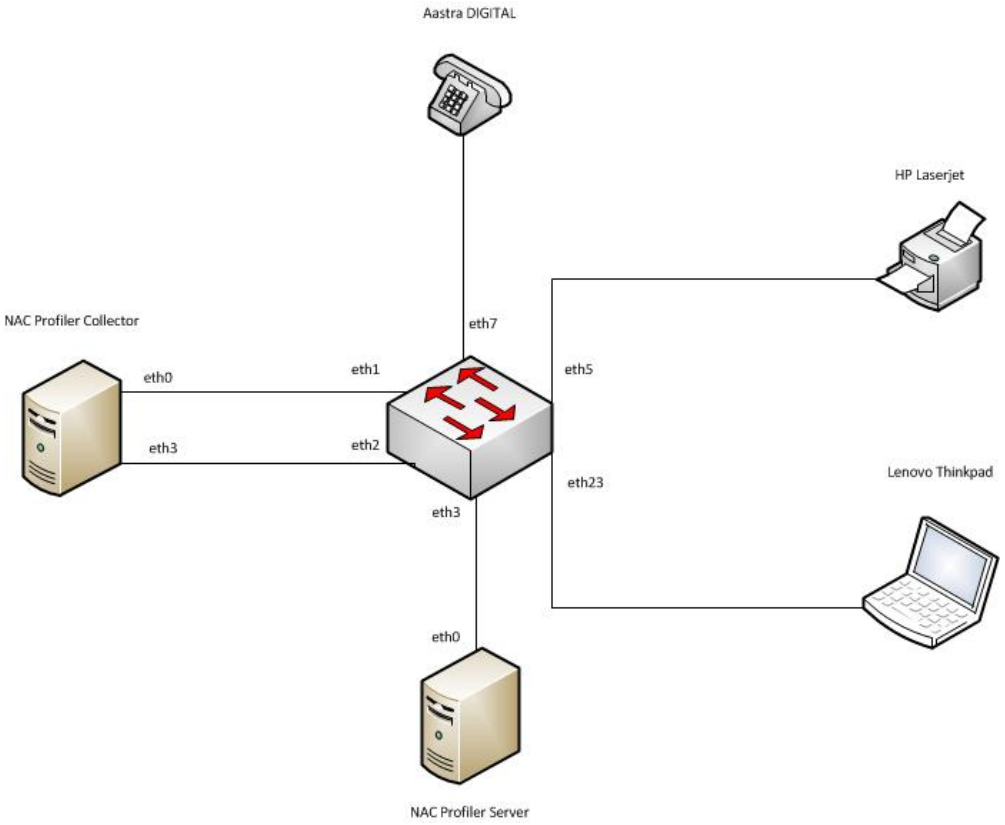
Tämän osion tarkoituksena oli NAC Profilerin linkittäminen ACS:n ulkoiseksi identiteettivarastoksi ja laitteen autentikointi käyttämällä Profiler Serverissä olevaa päätelaiteprofiilia. Laite, jonka valittiin testiin, oli Hewlett-Packardin valmistama LaserJet

P2015dn -verkkotulostin. Koska ACS:n LDAP-asetukset tehtiin jo aiemmin, päästiin nyt tekemään asetukset Profilerin päässä.

Autentikointi toimii tässä tapauksessa siten, että kytkin yrittää ensin välittää autentikointipyynnön 802.1X:n mukaisesti, mutta pyyntö epäonnistuu, sillä tulostin ei voi käyttää edellä mainittua autentikointia. Seuraavaksi kytkin yrittää MAC Authentication Bypass- eli MAB-autentikointia ja lähettää pyynnön tästä autentikoinnista RADIUS-palvelimelle, joka on tässä tapauksessa ACS. RADIUS-palvelin ottaa pyynnön vastaan, tosin Host Lookup –pyyntönä, jonka se käsittelee siihen määritettyjen sääntöjen ja käytäntöjen perusteella. Jos pyyntö täsmää jonkun säännön kanssa, palvelin lähettää pyynnön NAC Profilerille, joka vertaa sen tietoja olemassa oleviin päätelaiteprofiileihin. Jos laitteen tiedot täsmäävät jonkun profiilin kanssa, Profiler lähettää tiedon siitä RADIUS-palvelimelle, joka hyväksyy autentikoinnin ja ilmoittaa siitä kytkimelle.

6.4.2 Laiteprofiilien teko ja testaus

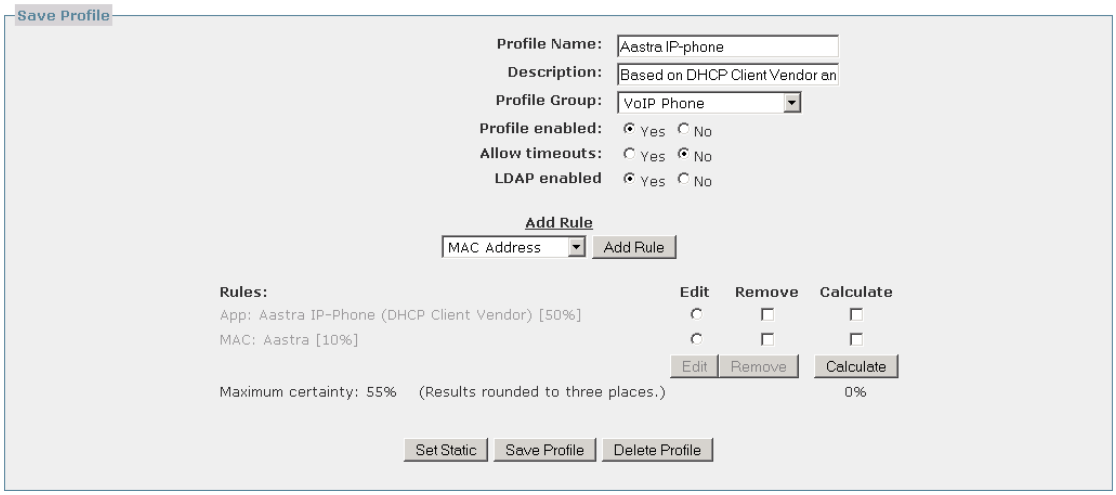
Tätä vaihetta varten tehtiin täysin uusi lähiverkko, jotta pystyttäisiin hahmottamaan miten päätelaiteprofiileja tehdään, miten ne toimivat ja kuinka luotettavia ne ovat. Lähiverkko on IP-osoiteavaruudeltaan 192.168.10.0/24, ja se on kuvan 15 mukainen. Tarkoituksena oli siis tutkia kolmella laitteella miten päätelaiteprofiileja tehdään, mitä tietoa Collectorin moduulit saavat niistä kerättyä ja miten laitteet osuvat oikeisiin profiileihin. Testiin valittiin kaksi erilaista laitetta: yksi Aastran valmistaman IP-puhelin ja yksi Hewlett-Packardin verkkotulostin. Testin kytkentä oli kuvan 15 mukainen.



KUVA 15. Päätelaiteprofiilien testiverkon rakenne

Lisäksi kytkimeen tehtiin täysin uusi konfiguraatio, josta otettiin kaikki ylimääräinen pois. Konfiguraatio löytyy liitteestä 3. Kytkimeen säädettiin DHCP-palvelimen, joka jakoi 192.168.10.0/24 –avaruuden osoitteita, pois lukien 192.168.10.1 - .30.

Aastra IP-puhelimelle tehtiin laitteistoprofiili, sillä sille sopivaa profiilia ei ollut valmiina Profilerissa. Profiilista tuli kuvan 16 mukainen.

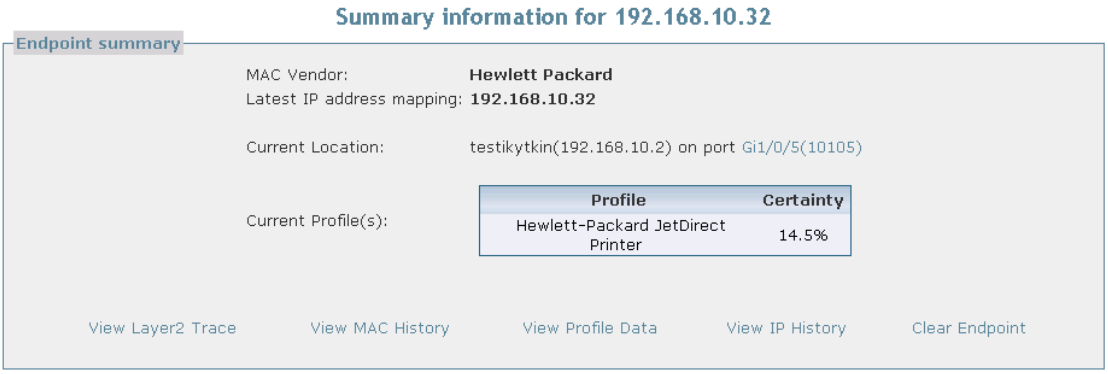


KUVA 16. Aastra IP-puhelimelle tehty profiili

Profiili nojaa kahden säännön varaan: valmistajan OUI-tunnuksen, jolle annettiin varmuudeksi 10 % ja DHCP Client Vendoriin, joka on luotettavampi ja jolle annettiin varmuudeksi 50 %. Kuvasta ilmenee myös maksimivarmuus, joka saavutetaan silloin jos päätelaite läpäisee molemmat säännöt. Tärkeää on se, että profiili on aktivoituna (Profile enabled: yes), sen sallitaan käyttävän vanhentumislaskureita jos halutaan (Allow timeouts: yes), ja LDAP sallitaan, jos puhelin aiotaan autentikoida MAB:n avulla (LDAP enabled: yes).

Kun profiili oli saatu valmiiksi, oli aika testata sitä. Kun puhelin kytkettiin kiinni kytkimeen, kesti hetken, ennen kuin Profiler tunnisti sen. Oli hienoa huomata, että laite päätyi oikeaan profiiliin maksimivarmuudella eli 55 %:lla. Tämä tarkoittaa sitä, että laite täsmäsi molempien sääntöjen kanssa.

Profilerissa oli valmiiksi Hewlett-Packard JetDirect Printer –profiili, johon verkkotulostimen oletettiin osuvan. Tulostin liitettiin kiinni ja katsottiin mitä tapahtui. Lopputulos oli kuvan 17 mukainen.

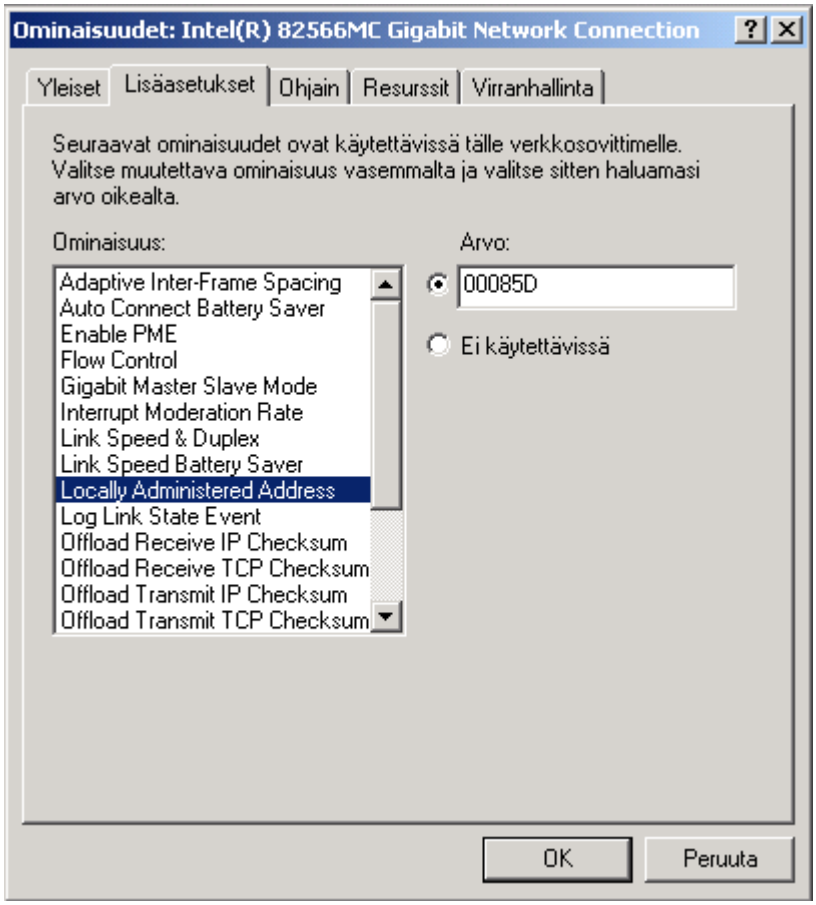


KUVA 17. Hewlett-Packard –tulostimen tunnistaminen Profilerilla

Maksimivarmuus, jolla laite olisi voinut profiiliin asettua, olisi ollut 57,25, mutta siitä ei saavutettu kuin 14,5 %. Tämä johtuu siitä, että Profiler ei jostain syystä saanut laitteen MAC Vendor –tietoa, jolle oli määritetty varmuudeksi 50 %. Ainoat säännöt, joihin laite osui, olivat avonainen TCP-portti 9100 ja MAC- osoitteen OUI.

6.4.3 Tunkeutuminen väärennetyllä MAC-osoitteella

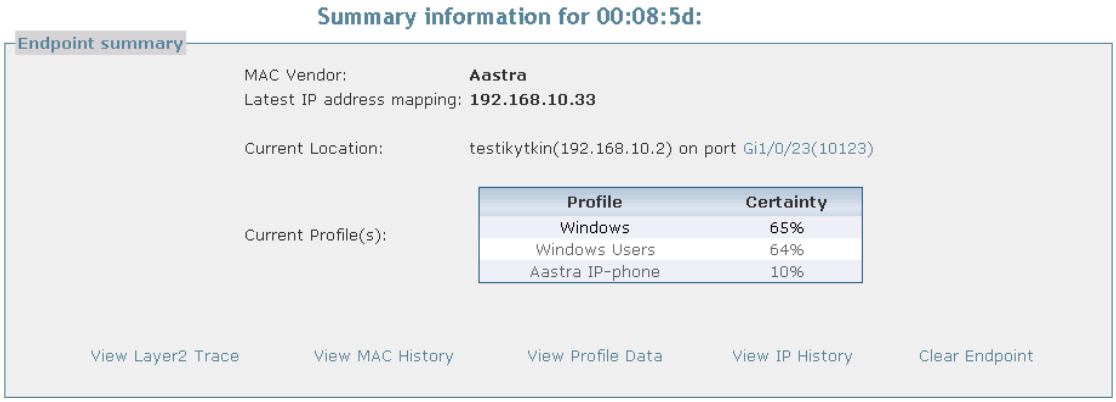
Tämän osion tarkoituksena on tutkia sitä, miten NAC Profiler suhtautuu MAC-osoitteen väärentämiseen (MAC Spoofing). Tätä tarkoitusta varten Lenovo Thinkpad –tietokoneen MAC-osoite vaihdettiin ensin vastaamaan Aastran IP-puhelimen ja sitten Hewlett-Packardin verkkotulostimen osoitetta. Jotta osoitepäällekkäisyyksiä ei tulisi, molemmilla kerroilla aito laite irrotettiin kytkimestä. Osoitteen vaihtaminen tapahtui verkkokortin asetuksista välilehdeltä lisäasetukset. Kuvasta 18 näkyy kohta, johon haluttu MAC-osoite laitetaan. Huomionarvoista tässä on se, että vaihtaminen tällä tavalla ei onnistu kaikilla verkkokorteilla.



KUVA 18. MAC-osoitteen väärentäminen eli MAC Spoofing. MAC-osoitteesta osa pyyhitty.

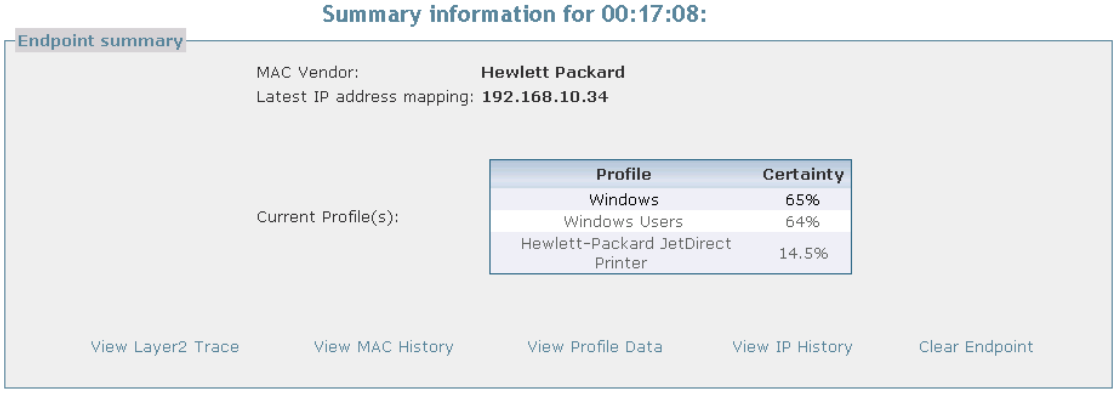
Tietokoneelle väärennettiin siis ensin IP-puhelimen MAC-osoite ja se liitettiin kytkimeen. Kesti hetken, ennen kuin Profiler huomasi muutoksen, mutta siitä huolimatta,

että MAC-osoite oli väärennetty, siirsi tietokoneen oikeaan profiiliin, joka oli tässä tapauksessa Windows. Tämä johtui siitä, että sen Windows-profiililla oli suurempi (65 %) varmuusprosentti kuin Aastra IP-Phone –profiililla (10 %), kuten kuvasta 19 ilmenee.



KUVA 19. Yhteenveto MAC-väärennyksen jälkeen, IP-puhelimen osoite

Seuraavaksi sama tehtiin HP:n verkkotulostimen MAC-osoitteella. Tälläkin kerralla Profiler osasi siirtää tietokoneen oikeaan profiiliin, sillä Windows-profiilin varmuusprosentti oli huomattavasti suurempi kuin tulostinprofiililla (kuva 20.). Molemmilla väärennyskerroilla kohdeprofiileissa on ollut muitakin sääntöjä kuin pelkkä OUI-tunnukseen perustuva MAC-osoitesääntö. Jos jossain profiilissa ei olisi muita kuin edellä mainittu sääntö ja Windows-profiilia ei olisi ollenkaan, silloin väärentämällä MAC-osoitteen päätelaitteena oleva tietokone voitaisiin naamioida toisenlaiseksi laitteeksi ja verkkoon voitaisiin päästä tunkeutumaan.



KUVA 20. Yhteenveto MAC-väärennyksen jälkeen, verkkotulostimen osoite

6.5 Verkon toiminta

Verkon autentikointi toimi suurimmaksi osaksi mallikkaasti, tosin 11.11. ACS jostain syystä alkoi dropata uudet, ennen kyseistä päivää kirjautumattomilta PEAP-protokollaa käyttäviltä käyttäjätileiltä tulleet autentikointipyynnöt. Droppauksella tarkoitetaan tilannetta, jossa autentikointipalvelin hylkää pyynnön suoraan eikä tee suodatuspäätöstä sääntöjen perusteella. Palvelin ei myöskään lähetä tässä tapauksessa mitään vastausta autentikoijalle. Tämä ilmeni aluksi vain yhden käyttäjätilin kohdalla, mutta seuraavana päivänä ilmiö alkoi levitä. Järjestelmän uudelleenkäynnistyksen jälkeen ACS alkoi dropata lähes kaikki autentikointipyynnöt, mikä johti siihen, että siirsin autentikointivastuun ACS:iä edeltäneelle järjestelmälle ja jätin ACS:n alaisuuteen pelkästään testikytkimen. Ilmeisesti jokin osa ohjelmasta oli korruptoitunut, sillä mitään muuta syytä tälle ilmiölle ei löytynyt. Palautin lähes kuukautta aiemmin otetun VMWare-snapshotin, joka sisälsi toimivan varmuuskopion ACS:stä ja muokkasin sen asetukset ajan tasalle. Ainut muutos, jonka asetuksiin tein, oli oma Access Service MAB-autentikoinnille. Tällä muutoksella pyrin selkeyteen erilaisissa säännöissä ja ongelmatilanteissa ongelman paikallistamisen helpottamiseen. Lisäksi päivitin ACS:n versioon 5.1.0.44.4, jonka pitäisi olla vakaampi.

Edellä mainittua ongelmaa lukuun ottamatta toteutusympäristö toimi hyvin sekä Saitan verkosta eristyksessä ollut NAC Profiler –testiverkkoni että Saitan verkko toteutuksen aikana. Pienet autentikointiongelmat, kuten puuttuva AD-ryhmä tai toimimaton sääntö, saatiin ratkaistua suuremmitta ongelmitta ACS:n valvontatyökalujen sekä kytkimen show-komentojen avulla.

7 POHDINTA

Opinnäytetyöni tarkoituksena oli siis tutkia NAC Profilerin ja ACS:n toimintaa autentikoinnissa verkon reunalla ja onnistuin mielestäni siinä melko hyvin. ACS osoittautui melko hyväksi autentikointipalvelinvaihtoehdoksi, tosin siitäkin löytyy joitain häiriöitä ja vikoja. Sen valvontatyökalut olivat erinomaiset ja auttoivat huomattavasti ongelmanetsinnässä.

NAC Profilerin osuus 802.1X-autentikointitapahtumissa oli odotettua pienempi. Toteutuksen aikaisen tutkimisen myötä selvisi, että Profiler toimii 802.1X-järjestelmässä vain ulkoisena identiteettivarastona, kun taas NAC-järjestelmässä sillä on aktiivisempi rooli. Jälkimmäisessä järjestelmässä se keskustelee jatkuvasti NAC Appliance Manager –laitteen, joka on kyseisessä tapauksessa verkon valvonnan keskus, kanssa ja lähettää jatkuvasti päätelaitteista tietoa, jonka perusteella Appliance Manager voi tehdä reaaliajassa laitekohtaisia autentikointi- ja valtuutuspäätöksiä. NAC ja 802.1X eivät kuitenkaan voi olla järkevästi käytössä samaan aikaan samassa verkossa, joten Profilerin toiminta jäi ehkä pieneksi pettymykseksi tässä suhteessa.

Päätelaitteiden valvonnassa se kuitenkin näyttää kyntensä, sillä se pystyy profiloimaan Collectorien määrästä riippuen laajojenkin verkkojen laitekannan, ja etsintätyökalun avulla mikä tahansa profiloitu laite voidaan etsiä kytkimen ja sen portin tarkkuudella. Lisäksi ulkoisiin lokipalveluihin, esimerkiksi Syslog-serverille, lähetetyt ilmoitukset auttavat verkon turvaamista, sillä niiden avulla voidaan paikallistaa mm. MAC-osoitteen väärentämisellä tapahtuvia tunkeutumisia verkkoon.

Autentikointi tuntuu olevan suuntaus, johon tietoliikenteessä pyritään nykyään. Koska eritasoiset tietomurrot ovat maailmanlaajuisesti lähes arkipäivää, monet organisaatiot haluavat suojata kaikki verkkoresurssinsa ulkopuolisilta tahoilta mahdollisimman tehokkaasti. Vaikka erilaisia autentikointimetodeja on useita, IEEE 802.1X pitää johtoasemansa, sillä monet eritasoiset EAP-protokollat tarjoavat joustavuutta erilaisiin tarpeisiin ja se on käytännössä yhteensopiva kaikkien verkkolaitevalmistajien tuotteiden kanssa.

LÄHTEET

1. Aboba, B. – Blunk, L. – Carlson, J. – Vollbrecht, J., Request for Comments: 3748: Extensible Authentication Protocol [verkkodokumentti]. The Internet Society 2004 [Viitattu 20.10.2010]. Saatavissa: http://tools.ietf.org/html/rfc3748

2. Aboba, B. – Hurst, R. – Simon, D., Request for Comments: 5216: The EAP-TLS Authentication Protocol [verkkodokumentti]. The IETF Trust 2008 [Viitattu 22.10.2010]. Saatavissa: http://tools.ietf.org/html/rfc5216

3. Barkley, S. – Mitton, D. – Nelson, D. – Patil, B. – St.Johns, M. – Stevens, M. – Wolff, B., Authentication, Authorization and Accounting: Protocol Evaluation [verkkodokumentti]. The Internet Society 2001 [Viitattu 13.10.2010]. Saatavissa: http://tools.ietf.org/html/rfc3127

4. Chu, Ellen, EAP over LAN [verkkodokumentti]. www.networkdictionary.com 2010 [Viitattu 19.10.2010] Saatavissa: http://wiki.networkdictionary.com/index.php/EAP_over_LAN

5. Cisco, Identity-Based Networking Services: IEEE 802.1X Deployment Guide [verkkodokumentti]. Cisco Systems Inc. 2010 [Viitattu 25.10.2010]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/guide_c07-627531.html

6. Cisco, User Guide for the Cisco Secure Access Control System 5.1 [verkkodokumentti]. Cisco Systems Inc. 2010 [Viitattu 15.10.2010]. Saatavissa: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/user/guide/acsuserguide.html

7. Cisco, Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 [verkkodokumentti]. Cisco Systems Inc. 2010 [Viitattu 5.11.2010] Saatavissa: http://www.cisco.com/en/US/docs/security/nac/profiler/configuration_guide/310/nacprofiler31.pdf

8. Cisco, MAC Authentication Bypass [verkkodokumentti]. Cisco Systems Inc. 2007 [Viitattu 10.11.2010]. Saatavissa: http://www.cisco.com/univercd/cc/td/doc/solution/macauthb.pdf

9. Cisco, Cisco IOS Quick Reference Guide for IBNS [verkkodokumentti]. Cisco Systems Inc. 2010 [Viitattu 15.10.2010]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/whitepaper_c27-574041.pdf

10. Cisco, Cisco Secure Access Control System 5.1 Data Sheet [verkkodokumentti]. Cisco Systems Inc. 2010 [Viitattu 15.10.2010]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps5698/ps6767/ps9911/ps9915/data_sheet_C78-577717.pdf

11. Cisco, Cisco IOS Security Configuration Guide, Release 12.2 [verkkodokumentti]. Cisco Systems Inc. 2006 [Viitattu 10.11.2010]. Saatavissa: http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfbook.pdf

12. Cisco, Configuring 802.1X Port-Based Authentication [verkkodokumentti]. Cisco Systems Inc. 2009 [Viitattu 20.11.2010]. Saatavissa: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/dot1x.html

13. Cudbard-Bell, Arran, 802.1X wired protocols.png [verkkodokumentti]. Arran Cudbard-Bell 2010 [Viitattu 13.10.2010]. Saatavissa: http://en.wikipedia.org/wiki/File:802.1X_wired_protocols.png

14. Howes, T. – Kille, S. – Wahl, M., Lightweight Directory Access Protocol (v3) [verkkodokumentti]. The Internet Society 1997 [Viitattu 10.11.2010]. Saatavissa: http://www.ietf.org/rfc/rfc2251.txt

15. Josefsson, S. – Palekar, Ashwin – Simon, Dan – Zorn, Glen, Protected EAP Protocol (PEAP) [verkkodokumentti]. The Internet Society 2002 [Viitattu 20.10.2010]. Saatavissa: http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-06

16. Merilinna, Juha, ACTIVE DIRECTORY [verkkodokumentti]. Juhani Merilinna 2005 [viitattu 11.11.2010].Saatavissa: http://myy.helia.fi/~merju/tie62d/ntRakenne7.pdf

17. Rigney, C. – Rubens, A. – Simpson, W. – Willens, S., Request for Comments: 2865: Remote Authentication Dial In User Service [verkkodokumentti]. The Internet Society 2000 [Viitattu 14.10.2010]. Saatavissa: http://tools.ietf.org/html/rfc2865

18. Techwriters Future, 802.1x Wireless Standard [verkkodokumentti]. IPv6.com Inc. 2008 [viitattu 25.11.2010]. Saatavissa: http://ipv6.com/articles/wireless/8021x-Wireless.htm

LIITE 1(1).

Cisco Catalyst 2960-s –kytkimen autentikointitestikonfiguraatio

```
Current configuration : 9931 bytes
!
! Last configuration change at 07:48:02 UTC Thu Nov 11 2010
! NVRAM config last updated at 07:49:01 UTC Thu Nov 11 2010
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname (KYTKIMEN NIMI)
!
boot-start-marker
boot-end-marker
!
enable secret 5 (HALLINTASALASANA)
!
username (LUKUTUNNUS) password 0 (LUKUSALASANA)
!
!
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
!
!
aaa session-id common
switch 1 provision ws-c2960s-24ps-l
authentication mac-move permit
```

```
ip subnet-zero
ip dhcp smart-relay
!
!
!
!
!
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
 switchport access vlan ABC
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/2
 switchport access vlan ABC
 switchport mode access
 snmp trap mac-notification change added
!
```

```
interface GigabitEthernet1/0/3
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/4
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/5
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
```

```
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/6
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/7
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/8
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
```

```
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/9
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/10
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/11
 switchport mode access
 authentication event fail action authorize vlan A
```

```
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/12
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/13
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
```

```
interface GigabitEthernet1/0/14
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/15
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/16
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
```

```
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/17
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/18
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/19
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
```

```
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/20
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/21
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/22
 switchport mode access
 authentication event fail action authorize vlan A
```

```
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/23
 switchport mode access
 authentication event fail action authorize vlan A
 authentication event no-response action authorize vlan A
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout quiet-period 5
 dot1x timeout tx-period 1
 dot1x max-reauth-req 1
!
interface GigabitEthernet1/0/24
 switchport mode trunk
 no cdp enable
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
```

```
interface Vlan 1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan A
 no ip address
 no ip route-cache
!
interface Vlan B
 no ip address
 no ip route-cache
!
interface Vlan C
 no ip address
 no ip route-cache
!
interface Vlan D
 no ip address
 no ip route-cache
!
interface Vlan E
 no ip address
 no ip route-cache
!
interface Vlan ABC
 ip address xxx.xxx.xxx.xxx 255.255.255.0
 no ip route-cache
!
interface Vlan DEF
 no ip address
 no ip route-cache
!
```

```
ip default-gateway xxx.xxx.xxx.xxx
ip http server
ip http secure-server
ip sla enable reaction-alerts
snmp-server community (COMMUNITY STRING) RO
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps syslog
snmp-server enable traps mac-notification change move threshold
snmp-server host (collectorin IP-osoite) (COMMUNITY STRING)  mac-notification
snmp
snmp-server host xxx.xxx.xxx.xxx (COMMUNITY STRING)  syslog snmp
radius-server host (ACS:n IP-osoite) auth-port 1645 acct-port 1646
radius-server key (RADIUS SHARED SECRET)
!
!
line con 0
 password (LUKUSALASANA)
line vty 0 4
 password (LUKUSALASANA)
line vty 5 15
 password (LUKUSALASANA)
!
!
monitor session 1 source interface Gi1/0/1 , Gi1/0/3 - 24
monitor session 1 destination interface Gi1/0/2
ntp clock-period 22518370
ntp server xxx.xxx.xxx.xxx
end
```

```
Current configuration : 4351 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname testikytkin
!
boot-start-marker
boot-end-marker
!
no aaa new-model
switch 1 provision ws-c2960s-24ps-l
authentication mac-move permit
ip subnet-zero
ip dhcp excluded-address 192.168.10.1 192.168.10.30
!
ip dhcp pool Pool1
   network 192.168.10.0 255.255.255.0
   domain-name mydomain
!
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0
 no ip address
 shutdown
```

```
!
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/3
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/4
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/5
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/6
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/7
 switchport access vlan 10
```

```
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/8
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/9
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/10
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/11
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/12
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/13
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
```

```
interface GigabitEthernet1/0/14
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/15
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/16
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/17
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/18
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/19
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/20
 switchport access vlan 10
 switchport mode access
```

```
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/21
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/22
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/23
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/24
 switchport access vlan 10
 switchport mode access
 snmp trap mac-notification change added
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface Vlan1
 no ip address
 shutdown
```

```
!
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
!
ip default-gateway 192.168.10.1
ip http server
ip http secure-server
ip sla enable reaction-alerts
snmp-server community public RO
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move threshold
snmp-server host 192.168.10.10 public  mac-notification snmp
!
!
line con 0
line vty 5 15
!
monitor session 1 source interface Gi1/0/1 , Gi1/0/3 - 24
monitor session 1 destination interface Gi1/0/2
end
```