STADIA
HELSINGIN AMMATTIKORKEAKOULU

TEKNIIKAN JA LIIKENTEEN TOIMIALA

Tietotekniikka

Tietoliikennetekniikka

INSINÖÖRITYÖ

802.1X-AUTENTIKOINNIN KÄYTTÖÖNOTTO TOIMISTOVERKOSSA

Työn tekijä: Lehmonen Harri
Työn valvoja: Kasurinen Timo
Työn ohjaaja: Salainen

Työ hyväksytty: 28.3.2007

INSINÖÖRITYÖN TIIVISTELMÄ

Tekijä: Harri Lehmonen

Työn nimi: 802.1x-autentikoinnin käyttöönotto toimistoverkossa

Päivämäärä: 10.4.2007 Sivumäärä: 64 s. + 4 liitettä

Koulutusohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoliikennetekniikka

Työn valvoja: lehtori, Timo Kasurinen, Tietotekniikka, Helsingin ammattikorkeakoulu

Työn ohjaaja: Salainen

Tämän insinöörityön tarkoituksena on tutkia, mitä 802.1x-autentikoinnin käyttöönotto toimistoverkossa vaatii.

Aluksi tutkitaan autentikoinnissa tarvittavat komponentit ja niiden toiminta teorian kannalta. Kun teorian puolesta kaikki on selvää, on aika viedä teoria käytäntöön ja muodostaa olemassa olevien komponenttien avulla toimiva 802.1x-autentikointi. Autentikointiin tarvittavat asetukset esitetään yksityiskohtaisesti, jotta autentikointi olisi mahdollista toteuttaa myös muissa ympäristöissä.

Muodostuksen jälkeen tutkitaan autentikoinnista saatavia lokeja ja selvitetään niiden tarkoitus. Jos saavutettu lopputulos on halutun kaltainen, otetaan 802.1x-autentikointi käyttöön koko toimistoverkossa.

Avainsanat: 802.1x, RADIUS, AAA, AD, LDAP, CISCO IOS, CISCO ACS, EAP, PEAP

STADIA
HELSINGIN AMMATTIKORKEAKOULU

ABSTRACT

Name: Harri Lehmonen

Title: Implementing 802.1x on wired network

Date: 10 Apr. 08 Number of pages: 64 + 4

Department: Information Technology

Study Programme: Telecommunication

Instructor: Lecturer, Timo Kasurinen, Helsinki Polytechnic / Technology

Supervisor: Salainen

The purpose of this graduation study is to determine what the deployment of the 802.1x authentication on wired network requires.

This study is based on the theory of authentication and wired networks as well as identifying what components must be used.

In the practical part of this study the authentication feature was added to the wired network with the existing components. Detailed setup instructions have been presented, which makes it possible to deploy the authentication in other environments, as well.

After deployment the logs created by the authentication can be studied and explained. If the achieved goal is the one desired, the authentication will be implemented throughout.

Keywords: 802.1x, RADIUS, AAA, AD, LDAP, CISCO IOS, CISCO ACS, EAP, PEAP

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

LYHENTEET

LYHENTEET

AAA	Authentication Authorization Accounting
ACS	Cisco Secure Access Control Server
AD	Active Directory
ADSL	Asymmetric Digital Subscriber line
ARA	AppleTalk Remote Access
CHAP	Challenge-handshake authentication protocol
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol overLAN
EAP-MD5	Extensible Authentication Protocol-Message Digest 5
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
ISDN	Integrated Services Digital Network
IEEE	Institute of Electrical and Electronics Engineers
IOS	Internetwork Operating System
IP	Internet Protocol address
IPX	Internetwork Packet Exchange
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MMC	Microsoft Management Console
MSCHAP	Microsoft CHAP
NAS	Network Access Server
ODBC	Open Database Connectivity
PAP	Password Authentication Protocol

PEAP	Protected EAP
PKI	Public Key Infrastructure
PPP	Point-To-Point Protocol
RADIUS	Remote Authentication Dial In User Service
SHA	Secure Hash Algorithm
SLIP	Serial Line Internet Protocol
SNMS	CiscoWorks Small Network Management Solutionin
SSH	Secure Shell
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual LAN
VPN	Virtual Private Network

1 JOHDANTO

Tämän insinöörityön tavoitteena on ottaa käyttöön 802.1X-autentikointi työasemaverkossa. Tarkoituksena on helpottaa työasemaverkon ylläpitäjien työmäärää poistamalla käytöstä paljon työtä vaativat MAC-lukot. Tällä tarkoitetaan sitä että kytkimen päästä on laitettu päälle MAC-tunnistus, jolloin ensimmäisen koneen MAC-osoite, joka kyseiseen porttiin laitetaan jää kytkimen muistiin. Jos samaan porttiin halutaan vaihtaa toinen kone, MAC-lukko on poistettava. Tämä on ollut hyvä tapa poistaa mahdollisuus liittää vieras kone verkkoon.

Toinen asia johon halutaan parannusta, on verkonylläpitäjien ainainen tarve vaihtaa kytkimen portti oikeaan aliverkkoon eli vlan:iin. Toisaalta tämä on ollut hyvä tapa hankaloittaa vieraiden laitteiden pääsemistä verkkoon, koska silloin on aina tiedettävä missä vlan:ssa kytkimen portti on. Jos portti on väärässä vlan:ssa, kone ei saa IP osoitetta DHCPltä, joka jakaa sen MAC-osoitteen perusteella.

Vaikka kummatkin systeemit ovat palvelleet tarkoitustaan hyvin, konekannan lisääntyessä ja verkkotopologian kehittyessä näistä on tullut liian vanhanaikaisia tapoja. Tilalle halutaan helppokäyttöisempi systeemi, joka ei vaadi kovin paljoa ylläpitoa. Lisäksi käytössä voi olla monia etäpisteitä, joista tarkoituksena olisi päästä mahdollisimman helposti verkkoon ja yhteys välttämättömiin palveluihin. Näihin kaikkiin ongelmiin ratkaisuna olisi 802.1X-autentikointi.

Työ alkaa 802.1X-protokollan esittelyllä ja läpi käydään työn kannalta tärkeitä termejä. Lisäksi tutustutaan mikä autentikoinnin perusidea on, miten se toimii ja mitä hyötyjä sen käyttöönotolla on. Tämän jälkeen tutustutaan EAP-protokollan toimintaan ja esitetään sen erilaisia variaatioita. EAP-protokollan esittelyn jälkeen tutustutaan AAA-palveluihin ja niissä käytettäviin RADIUS- ja TACACS+-protokolliin. Näiden lisäksi katsotaan hieman miten Ciscon kytkimissä käyttämä IOS-käyttöjärjestelmä toimii. Lisäksi perehdytään Ciscon ACS:ään ja sen toimintaan. Näiden ohessa luodaan nopea vilkaisu Microsoftin AD-palveluun ja LDAP:iin.

Teorian jälkeen muodostetaan työasemaverkkoon toimiva 802.1X-autentikointi. Työssä kuvataan autentikointiin tarvittavien laitteiden asetusten yksityiskohtainen asettaminen. Näiden ohjeiden perusteella ympäristön voi tarvittaessa asentaa uudestaan.

2 TEORIA OSUUS

Tässä osiossa käydään läpi mitä, 802.1x-autentikaatio tarvitsee teoriassa toimiakseen. Eri vaiheet käydään yksityiskohtaisesti läpi ja samalla kerrotaan erilaisista vaihtoehdoista.

2.1 802.1X

Lähiverkoissa yleensä käytetyllä käyttäjätunnus/salasana -ratkaisulla pystytään estämään asiaton pääsy palvelimille ja työasemille. Normaalisti näillä tunnuksilla pystytään joko sallimaan tai estämään pääsy tiedostoihin ja ohjelmiin sekä verkkoresursseihin, jotka ovat saman toimialueen sisällä. Vaikka käyttäjällä on pääsy tietylle koneelle tai tiettyihin ohjelmiin, se ei tarkoita että käyttäjä voisi käyttää tiettyjä verkkopalveluita. Verkkopalvelumääritykset joudutaan tekemään käsin verkon liityntäpisteessä. Vaikka koneelle kirjaudutaan millä tahansa tunnuksilla, verkkopalvelut pysyvät samoina. [1]

Tähän yritetään saada helpotusta ottamalla käyttöön 802.1x-standardi. Tämä on IEEEn määrittelemä standardi portti- ja käyttäjäkohtaisesta autentikoinnista, jota käytetään lähiverkkojen tietoliikenneratkaisuissa. Standardin tarkoituksena on estää luvattoman asiakaslaitteen käyttäminen lähiverkon liitäntäpisteen kautta sekä antaa sallitulle asiakaslaitteelle ne verkkoresurssit, joita käyttäjä tarvitsee. Tämä liityntäpiste voi olla langallisissa verkoissa kytkin tai langattomassa verkossa tukiasema.

2.1.1 Terminologia

Seuraavaksi on selitetty lyhyesti muutamia termejä, jotka ovat 802.1x-protokollan ymmärtämisen kannalta oleellisia. Termejä hahmottaa kuva 1.

Asiakas

Asiakkaalla tarkoitetaan laitetta, jolla yhteys verkkoon halutaan muodostaa. Yleensä tämä on tietokone, joka on varustettu langallisella tai langattomalla verkkokortilla.

Liityntäpiste

Liityntäpiste on se kohta verkosta, jonka kautta siihen liitytään. Tämä voi olla joko kytkimen portti tai langattomissa verkoissa tukiasema.

Autentikaattori

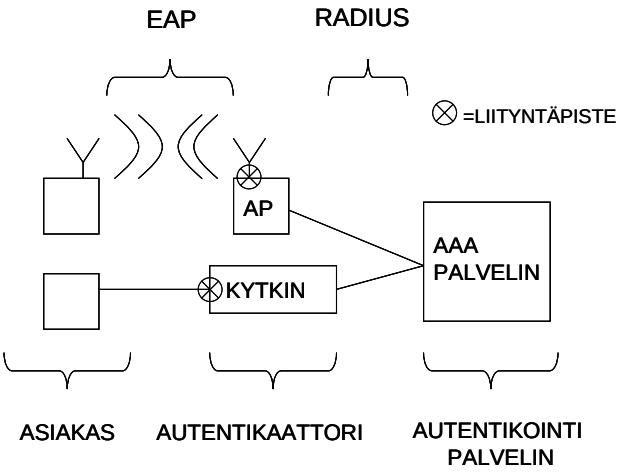
Autentikaattori on verkossa toimiva laite, joka sisältää liityntäpisteen tai liityntäpisteitä. Autentikaattori toimii todennustietojen välittäjänä autentikointi palvelimelle ja toimii sieltä tulevien ohjeiden mukaisesti. Se joko myöntää asiakkaalle luvan käyttää liityntäpistettä ja muuttaa sen sallituksi tai kieltää käytön laittamalla sen ei-sallituksi.

EAP ja EAPOL

EAP on autentikointi protokolla, joka määrittelee miten autentikointiviestit vaihtuvat asiakkaan, autentikaattorin ja AAA-palvelimen välillä. EAPillä on monia eri versioita, joista jokaisella on erilaisia ominaisuuksia.

Autentikointi palvelin - AAA

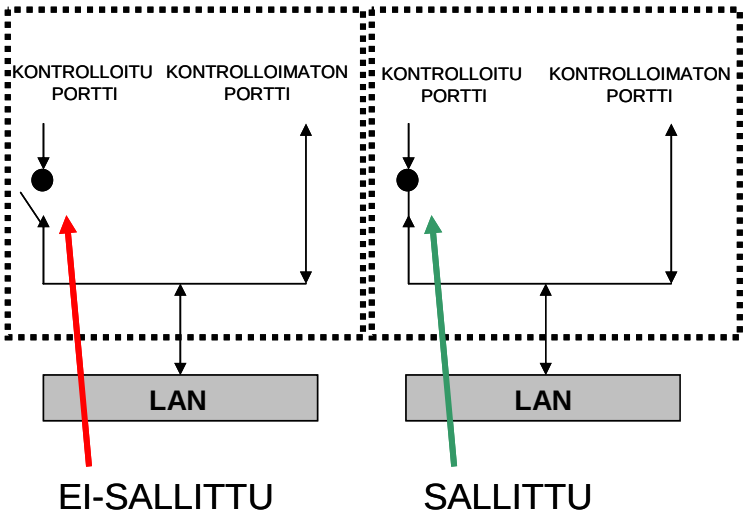
Autentikointipalvelimella on lista käyttäjistä, joilla on lupa käyttää verkkoa. Näiden perusteella palvelin kertoo pyydetyt tiedot autentikaattorille. Käyttäjätietokanta voi sijaita myös ulkoisessa tietokannassa.



Kuva 1. 802.1-terminologia

2.1.2 Arkkitehtuuri

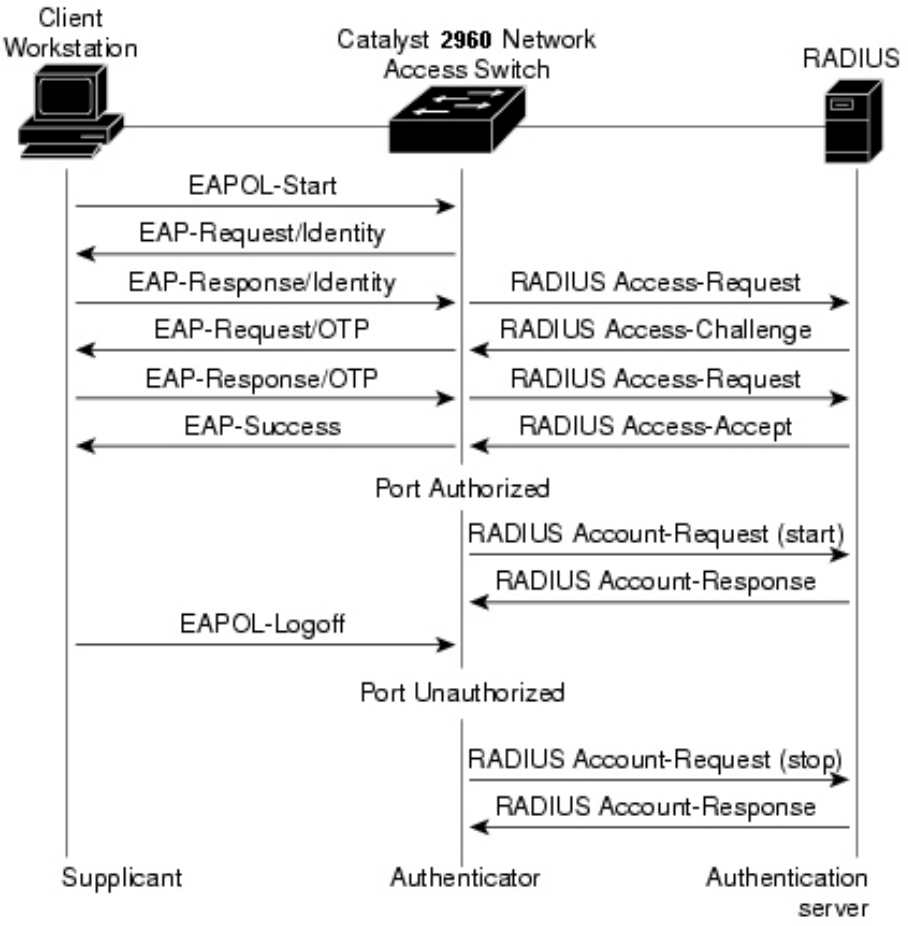
802.1x:n perustana on ajatus siitä että verkkoportti jakautuu kahdeksi erilliseksi portiksi – sallituksi ja ei-sallituksi (kuva2). Kun verkkoportti ei ole käytössä, se on koko ajan ei-sallitussa tilassa. Kun porttiin laitetaan kiinni kone tai joku muu yhteensopiva laite, portti pysyy ei-sallitussa tilassa niin kauan ennen kuin joko käyttäjä tai kone tai kummatkin on autentikoitu. Kun autentikointi on suoritettu, portti menee sallittuun tilaan ja liikennöinti portin kautta voi alkaa. Autentikointi voidaan määrittää tapahtuvaksi tietyin väliajoin. Kun kone otetaan pois verkosta eli linkki sammuu, portti menee takaisin ei-sallittuun tilaan ja on siinä niin kauan, kun seuraava onnistunut autentikointi tapahtuu ja portti menee sallittuun tilaan.



Kuva 2. 802.1X arkkitehtuuri [Lähdettä 4 mukaillen]

2.1.3 Toiminta

Seuraavaksi esitetään kohta kohdalta, miten 802.1x-autentikointi tapahtuu (kuva 3).



Kuva 3. 802.1X autentikointi [Lähdettä 3 mukaillen]

1. Asiakaslaite (supplicant) liitetään verkkoon liityntäpisteen (verkkoportti) kautta. Tämä liityntäpiste voi olla joko kytkimen portti tai langattomissa verkoissa tukiasema. Asiakkaan ja liitäntäpisteen välinen linkki nousee ylös, mutta liityntäpiste menee ”ei-sallittu”-tilaan, jolloin sen kautta ei kulje liikennettä muuta kun linkkitason kautta. Linkkitaso riittää hienosti juuri tähän tarkoitukseen, koska autentikoitumisprosessiin ei tarvita IP-osoitetta. Linkkitason autentikoituminen on helppo ja nopea tapa eikä raskaita IPv4, IPv6, AppleTalk, IPX, SNA ja NetBEUI-tason protokollia tarvitse käyttää.

2. Keskustelu asiakkaan ja autentikaattorin välillä alkaa EAPOL-Start paketilla. EAPoL eli EAP over Lan on vain paketointitekniikka.

3. Autentikaattori vastaa viestiin EAP-Request paketilla ja kysymällä asiakkaan identiteettiä.

4. Asiakas vastaa lähettämällä EAP-Response ja identiteettitiedot.

5. Autentikaattori välittää edelleen asiakkaan antamat tiedot autentikointi palvelimelle. Protokolla riippuu siitä, mitä halutaan käyttää. Yleensä käytetty protokolla on RADIUS, jota voidaan käyttää myös EAPin kanssa. Kaikki autentikaattorin ja autentikointipalvelimen välinen keskustelu tapahtuu RADIUS:n avulla.

6. Autentikointi-palvelin vastaa autentikaattorille haasteella ja varmistaa, että asiakas tukee EAP-autentikointia.

7. Autentikaattori ohjaa viestin asiakkaalle. Samassa viestissä kysytään myös autentikointi tyyppiä.

8. Asiakas tutkii saadun viestin ja päättää tukeeko kysyttyä EAP-autentikointiprotokollaa. Jos asiakas ei tue kyseistä tyyppiä, se lähettää NAK viestin ja yrittää sopia vaihtoehtoisesta autentikointitavasta. Jos asiakas tukee kyseistä tyyppiä, se lähettää tunnistustiedot.

9. Autentikaattori välittää tiedot autentikointipalvelimelle.

10. Jos autentikointipalvelin vahvistaa asiakkaan antamat tunnistetiedot, se autentikoi ja valtuuttaa asiakkaan käyttämään verkkoa. Jos tunnistetietoja ei löydy tai niitä ei pystytä vahvistamaan, asiakkaan pääsy evätään. Tästä autentikointipalvelin ilmoittaa autentikaattorille joko Access-Accept tai Access-Reject viestillä.

11. Autentikaattori saa viestin ja tekee sen perusteella päätöksen, siitä mihin tilaan portin laitetaan.

12. EAPoL keskustelu lopetetaan EAPOL-Logoff -paketilla. [2]

Koko autentikointiprosessin liityntäpiste pysyy ”ei-sallittu”-tilassa. Tällöin asiakaslaitteella ei ole IP-osoitetta eikä mikään autentikointiin liittymätön pysty liikkumaan asiakaslaitteen ja verkon välillä. Jos autentikaattorilta tulee viesti, että autentikointi on epäonnistunut, niin verkon liityntäpiste menee ”suljettu”-tilaan, jolloin kaikki liikenne pysähtyy ja pääsy verkkoon estetään (kuva 2).

2.1.4 Hyödyt

Turvallisuuden kannalta 802.1x on kuin laittaisi jokaisen kytkimen porttiin vartijan, joka tietää kenet päästää sisään. Vartija joko tunnistaa käyttäjän ja päästää hänet sisään tai ohjaa tuntemattoman käyttäjän pois.

Kun käyttäjä on oikein autentikoitunut, kytkimen portti siirtyy oikeaan aliverkkoon. Näin käyttäjä voi käyttää konetta mistä tahansa alueen verkkoportista. Tämä tehostaa liikkuvuutta ja käytön helppoutta ja nostaa tuottavuutta. Käyttäjät, jotka eivät ole autentikoituneet oikein, voidaan laittaa vierasverkkoon tai heiltä voidaan evätä kokonaan pääsy verkkoon. Tällä tavoin voidaan myös estää laittomien langattomien tukiasemien käyttö. Samassa yhdistyy autentikointi, pääsyn valvonta ja käyttäjän profiili käyttö.

802.1x helpottaa verkon kuormaa kun verkkoon pääsy joko sallitaan tai kielletään verkon reunalla. Tällä tarkoitetaan sitä, että kytkin, joka on verkon viimeinen laite, tekee päätöksen siitä, pääseekö käyttäjä verkkoon vai ei. Totta kai tähän prosessiin tarvitaan muitakin laitteita, jotka sijaitsevat syvemmällä verkon topologissa. Tähän käytetty liikenne ei ole kuitenkaan niin suurta että se haittaisi verkon kapasiteettia. 802.1x:n avulla voidaan helpottaa verkon ylläpitäjien työtä ja tällä tavoin aikaa jää muiden tärkeiden asioiden hoitamista varten.

802.1x on avoin standardi, joten se on helppo ottaa käyttöön monenlaisissa eri ympäristöissä ja monilla eri laitekokoonpanoilla. Ainoat edellytykset ovat että työasemien ja kytkinten on tuettava 802.1x-protokollaa ja RADIUS-palvelimen on tuettava EAP-protokollaa.

2.2 EAP-protokollat

EAP eli Extensible Authentication Protocol on autentikointiin käytettävä liikennöinti protokolla. EAP sekoitetaan usein autentikointimetodiksi tai itse autentikointiprotokollaksi. Itse asiassa se on vain standardi miten autentikointi viestit vaihtuvat asiakkaan, autentikaattorin ja autentikointipalvelimen välillä. EAP tukee useita eri autentikointi protokollia, joista osa on laitevalmistajakohtaisia. Eri protokollilla on erilaiset turvaominaisuudet ja salausvahvuudet, joiden pohjalta on helppo valita eri tilanteisiin sopivin protokolla. [2]

EAP on alun perin tarkoitettu toimivaksi PPP:n kanssa ja se onkin kehitetty lähinnä puhelinverkkojen piirikytkentäisiin verkkoihin. Tästä uudempi versio on EAPoL eli EAP over Lan. Tämä on tarkoitettu lähiverkkojen pakettikytkentäisiäverkkoja varten. Nykyään langattomien verkkojen yleistyessä siitä on tullut suosittu niiden autentikointiprosessin salaamisessa. EAP on otettu käyttöön myös monissa 802.1x-langallisten verkkojen autentikoinnissa.

Jokainen eri EAP-protokolla toimii hiukan erilailla. Kaikille samaa kuitenkin on, se että ne liikennöivät linkkitasolla. Tällöin ne eivät tarvitse IP-osoitetta kuljettaakseen viestejä laitteelta toiselle. Tämä sopii hyvin juuri DHCP-pohjaisiin verkkoihin, koska autentikoituminen tapahtuu ennen kuin asiakaslaite saa noudettua DHCP:ltä oikean IP-osoitteen. [2]

EAPin edut:

- EAP tukee automaattisesti monia eri autentikointi protokollia.
- EAP on muunneltavissa.
- Autentikaattori voi autentikoida paikallisia asiakkaita samaan aikaan kun se voi toimia läpikulkukäytävänä esimerkiksi radiukselle tai niille protokollille joita se ei tue. Ainut mitä autentikaattorin pitää tietää onko autentikointi hyväksytty vai hylätty.

Kuten jo aikaisemmin mainittiin, EAP protokollia on monta ja kaikilla niistä on omat ominaisuudet ja toimintatavat. Seuraavaksi on selostettu lyhyesti yleisimpien tyyppien ominaisuudet.

2.2.1 EAP-MD5

EAP-MD5 eli EAP-Message Digest 5 käyttää autentikoinnissa valtuuksina käyttäjänimeä ja salasanaa. Paketit, joissa käyttäjätunnus ja salasana ovat, se suojaa ainutlaatuisella digitaalisella allekirjoituksella. Digitaalisen allekirjoituksen tarkoitus on turvata EAP-viestien aitous.

EAP-MD5-etu on muun muassa sen rakenne, joka on erittäin kevyt. Tämän takia se toimii myös melko nopeasti ja on helppo konfiguroida. Haittapuolina protokollalla on viestien suojauksen heikkous. EAP-MD5 ei käytä salauksessa PKI-sertifikaatteja, joilla todennetaan asiakas tai tehdään vahva suojaus asiakkaan ja palvelimen väliselle autentikoinnille. Tämän takia tämä protokolla on hyvin altis kaappaukselle tai salakuuntelulle. EAP-MD5:n ongelmana on myös se, että asiakkaalla ei ole mitään takuuta siitä, tuleeko paluuviesti valtuutetulta palvelimelta vai onko lähetys kaapattu välissä. Tätä protokollaa tulisikin käyttää vain silloin, kun ei ole uhkaa, että joku pystyisi salakuuntelemaan lähetyksiä. 802.1x protokollan kanssa EAP-MD5:n käyttö ei ole sopivaa, vaan tulisi käyttää vahvempia salauskeinoja. [2][4]

2.2.2 EAP-TLS

EAP-TLS eli EAP-Transport Level Security on turvallisuudeltaan huomattavasti EAP-MD5-protokollaa parempi. EAP-TLS käyttää autentikoinnissa PKI-digitaalisia sertifikaatteja. Tällöin kummallakin, sekä asiakkaalla että palvelimella, tulee olla omat sertifikaatit, joiden perusteella tunnistautuminen tehdään. Kun lähetyksen kummatkin osapuolet ovat todistetusti oikeita, ei vaaraa kaappauksesta ole. Sertifikaattien käyttö on samalla yksi EAP-TLS:n huonoista puolista. Niiden jako jokaiselle asiakkaalle vaatii erittäin paljon työtä, ja niiden kunnossapito on hankalaa. [2][4]

2.2.3 EAP-TTLS

EAP-TTLS eli Tunneled TLS on laajennus aiemmalle EAP-TLS:lle. Tämä protokolla kehitettiin ajatellen vanhempaa protokollaa ja sen vaikeata sertifikaattien hallintaa. Etuna vanhempaan versioon on vahvempi salaus ilman vaikeita asiakkaan ja palvelimen välisiä sertifikaatteja. Protokolla vaatii sertifikaatin ainoastaan palvelimen päähän. Asiakas autentikoituu palvelimelle vain käyttämällä käyttäjätunnusta ja salasanaa. Tämä helpottaa huomattavasti sertifikaattien hallintaa, vaikka käytössä on kuitenkin vahva salaus. [2][4]

EAP-TTLS käyttää hyväkseen tunnelia, ja autentikoituminen tapahtuu kahdessa vaiheessa. Aluksi palvelimen päässä olevan sertifikaatin avulla vaihdetaan salattuja avaimia, joiden avulla luodaan tunneli. Tämän jälkeen asiakaslaite suorittaa varmennetun toisen kättelyn palvelimen kanssa. Toinen autentikointi tehdään toisella EAP-keskustelulla. Tunnelissa voidaan käyttää käyttäjätunnuskohtaisia protokollia kuten RADIUS:ta, LDAP-PAP, CHAP:ta, MSCHAP:ta tai MSCHAPv2:ta. Kun toinen kättely on valmis ja sitä ei enää käytetä, se tuhotaan. [2][4]

EAP-TTLSää ei pidetä aivan täydellisenä, koska sitä voidaan huijata lähettämään tietoja, jos TLS-tunnelia ei käytetä. Kumpikaan CISCO eikä Microsoft tue tätä protokollaa. [2][4]

2.2.4 PEAP

PEAP eli Protected EAP on toinen EAP-TLS sovellus. Protokolla on hyvin samanlainen kuin EAP-TTLS. Sertifikaatti tarvitaan vain palvelimen päähän ja autentikointi tapahtuu samalla lailla kahdessa osassa. PEAPin muodostamassa toisessa tunnelissa ajetaan yleensä radiukselle saakka (autentikaattori toimii vain välittäjänä) esimerkiksi MSCHAPv2:n avulla. MSCHAPv2:aa ei pidetä tarpeeksi turvallisena, jotta sitä voisi käyttää ilman tunnelia. PEAP ei tue CHAP- eikä PAP-protokollia. Cisco ja Microsoft tukevat kummatkin PEAPia. [2][4]

PEAPin etuna on, että se suojaa käyttäjän tietoja, koska ne lähetetään toista tunnelia pitkin. Se turvautuu varmaan TLSään avainten luonnissa ja vaihdossa. PEAP tukee nopeaa yhteyden uudelleen ottamista. PEAPia kutsutaan joskus myös EAP-MSCHAPv2:ksi.

2.2.5 LEAP

LEAP eli Lightweight EAP on Ciscon käyttämä autentikointiprotokolla. LEAPissa toisinkuin EAP-TLS käytetään autentikointiin pelkästään käyttäjätunnusta ja salasanaa eikä sertifikaatteja. Tästä johtuen LEAP on helppohoitoisempi.

Autentikoituminen tapahtuu kahdessa osassa. Ensin asiakas autentikoi itsensä autentikaattorille ja tämän jälkeen toisinpäin. Jos kummatkin autentikoinnit ovat menneet läpi, pääsy verkkoon sallitaan.

Koska protokolla on Ciscon kehittämä, se toimii vain Ciscon ja parin muun laitevalmistajan laitteiden kanssa. Protokolla on paljolti käytössä langattomissa verkoissa, joissa tukiasemat ja koneiden verkkokortit ovat LEAP-yhteensopivia. LEAPin avulla pystytään autentikoimaan vain käyttäjäverkkoon, ei konetta. Tämän takia Windows-ympäristössä jotkut group policyt eivät toimi oikein. Vanhentuneita salasanoja ei pysty muuttamaan, jolloin logon scriptit eivätkä roaming profiilit toimi. LEAPissä on todettu olevan myös muutamia haavoittuvuuksia, joten sekään ei ole aivan aukoton autentikointiprotokolla. [2][4]

2.3 AAA

Verkkoon pääsyn valvonnalla voidaan valvoa kenellä on oikeus päästä verkkoon ja mitä resursseja tällöin on mahdollista käyttää. AAA-palvelut tuovat tämmöistä turvallisuutta verkkoon.

AAA-palvelimella on tallennettuna jokaisen käyttäjän profiili, joka sisältää autentikointi- ja valtuutustiedot. Autentikointitieto todentaa käyttäjän ja valtuutustiedon perusteella annetaan valtuudet käyttää tiettyjä verkkoresursseja. Yksi AAA-palvelin voi tarjota monta yhdenaikaista AAA-palvelua soittosarjoille, kytkimille, reitittimille sekä palomuureille. Jokaiselle verkkolaitteelle voidaan tehdä asetukset niin , että se keskustelee AAA-palvelimen kanssa. Tällä tavalla on mahdollista keskitetysti valvoa kaikkien verkkolaitteiden kautta tulevaa ei-valtuutettua käyttöä. [5]

CISCO ACS on Ciscon kehittämä työkalu, jolla voidaan keskitetysti hoitaa kaikki AAA palvelut. Microsoftilta vastaavan palvelun hoitaa Microsoft IAS. Niin sanottuja AAA protokollia ovat RADIUS, TACACS+ ja KERBEROS. Näiden avulla pystytään hoitamaan autentikointi, valtuutus ja tilastointi.

Autentikointi eli todentaminen

Todentamisen tarkoituksena on tunnistaa käyttäjä olemaan oikea käyttäjä käyttämään tiettyä resurssia tai palvelua. Tunnistamiseen voidaan käyttää jotain seuraavista keinoista tai niiden sekoitusta – käyttäjätunnus/salasanaa, kertakäyttöinen avainta, digitaalinen sertifikaattia tai puhelinnumeroa. [6]

Valtuutus

Valtuutuksella määritellään, mitä palveluja käyttäjä saa käyttää tai toisaalta voidaan myös kieltää käyttäjää käyttämästä jotain tiettyä palvelua. Annetut oikeudet voivat olla voimassa aina, ei milloinkaan, tiettyyn aikaan päivästä, ne voivat olla sidottuna johonkin fyysiseen sijaintiin tai ne voidaan myös myöntää tapauskohtaisesti eri käyttäjille. [6]

Tilastointi

Tilastoinnin avulla pystytään seuraamaan esimerkiksi käyttäjän verkkoyhteyden yhteysaikoja. Tämän perusteella pystytään suunnittelemaan verkkoresurssit paremmin tai tietoa voidaan käyttää laskutustietojen perusteella. Tyypillisiä tilastoitavia asioita ovat käyttäjätunnus, käytettävä palvelu ja milloin palvelua on käytetty.[6]

2.3.1 RADIUS

RADIUS eli Remote Authentication Dial-In User Service on palvelin/käyttäjäprotokolla. Tällä tarkoitetaan, että sen käyttöön tarvitaan aina sekä erillinen palvelin että tietty käyttäjä. Radiusta on ennen käytetty lähestulkoon pelkästään yrityksen sisäänsoittopalveluissa (modeemi, ISDN) tapahtuvaan tunnistukseen, mutta nykyään se on otettu myös laajempaan käyttöön. Radiusta käytetään suurilta osilta operaattorin tai yrityksen sisäverkossa. Kummassakin tapauksessa sitä hallinnoi yksi ja sama taho, jolloin palvelua voidaan pitää melko luotettavana.

Radiuksen kehitti aikoinaan Livingstone Enterprises. Tällä hetkellä markkinoilta löytyy monta kaupalliseen käyttöön sekä avoimen koodin radiuspalvelinta ja ohjelmistoa. Nämä kaikki eroavat ominaisuuksiltaan, mutta kaikissa on yhteistä se että radiuksen käyttöön tarvitaan aina keskitetty tietokanta, jossa käyttäjätunnuksia ja salasanoja pidetään. Myös erilliset tietokannat kuten Microsoftin aktiivihakemisto, Novell eDirectory tai vaikka pelkkään tekstitiedostoon kirjoitetut tunnukset kelpaavat. [7]

RADIUS käyttää yhteyden ottamiseen UDP-protokollaa, joka on yhteydetön ja toimii kuljetus tasolla. UDP ei takaa pakettien menoa perille eikä niistä saada minkäänlaista varmennusta. Näin UDP mahdollistaa suuremman yh-

teysnopeuden. RADIUS käyttää autentikointiin ja valtuutukseen portteja 1645 ja 1821 ja tilastointiin portteja 1646 ja 1813. RADIUS-viesteissä vain salasana salataan 16-bittisellä salauksella. Autentikointi ja valtuutus on yhdistetty yhteen pakettiin.[7]

Taulukossa 1 on esitetty RADIUS-paketin koodit. Vasemmassa sarakkeessa näkyy arvo ja oikeassa sitä vastaava kuvaus. Jokaisessa radiuksen lähettämässä paketissa on tämmöinen arvo. Access-Request arvolla varustettu paketti pyytää pääsylupaa. Lupa myönnetään Access-Accept-paketilla ja evätään Acess-Reject-paketilla. Access-Challenge-paketilla pyydetään lisätietoa. Kun halutaan aloittaa tilastointi, lähetetään Accounting-Request. Tähän vastataan Accounting-Responsella.

Taulukko 1. Radius pakettien koodit [Lähdettä 10 mukaillen]

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

Autentikointiprosessi

Radiuksen viestinvaihto autentikointiprosessissa on esitetty kuvassa 4.

1. Asiakaslaite lähettää palvelupyynnön verkonliityntäpisteelle.

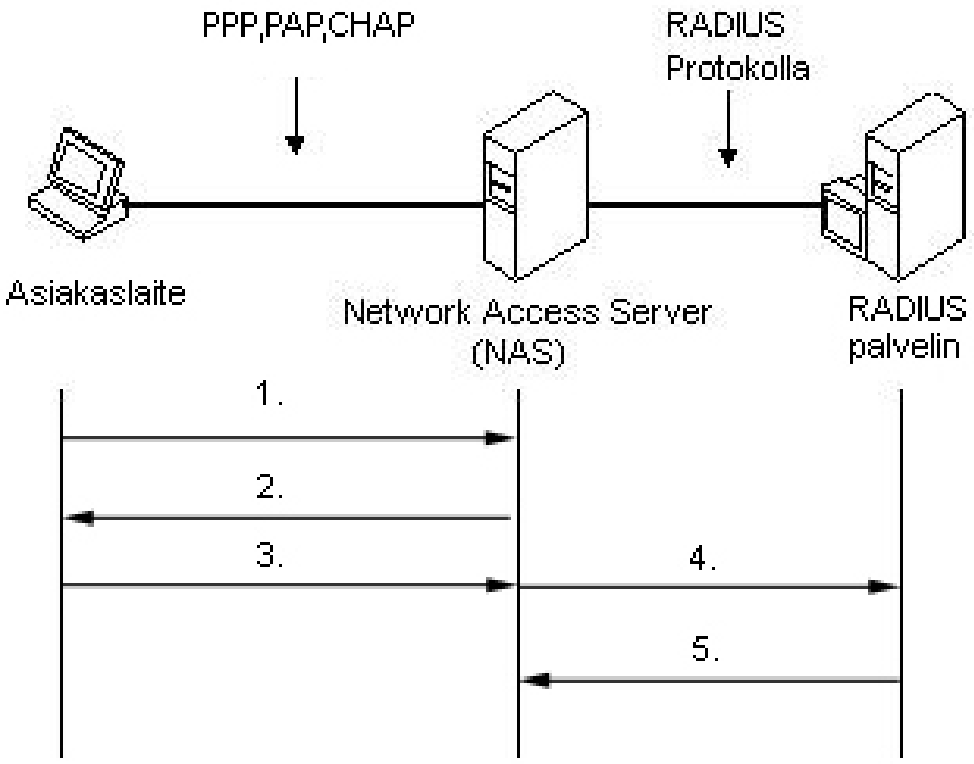
2. Verkonliityntäpiste vastaa pyytämällä asiakaslaitteelta sen käyttäjätunnusta ja salasanaa (jos käytetään Password Authentication Protocol [PAP]), (Point-To-Point [PPP]). tai haastetta (jos käytetään Challenge Handshake Authentication Protocol [CHAP]).

3. Asiakaslaite antaa pyydettävän vastauksen.

4. Verkonliityntäpiste lähettää RADIUS:lle pääsy pyynnön (Access-Request). Tämä pyyntö sisältää asiakaslaitteen antamat tiedot, jotka on koodattu sillä salasanalla, joka on laitettu kiinteästi sekä verkonliityntäpisteeseen että RADIUS-palvelimeen.

5. RADIUS vahvistaa, että pyyntö on tullut valtuutetulta verkonliityntäpisteeltä. Jos näin on, se vahvistaa asiakaslaitteen antamat tiedot omasta kannastaan tai ulkoisesta kannasta ja lähettää vastauksen verkonliityntäpisteelle.

6. Verkonliityntäpiste saa radiukselta joko hyväksytyn (Access-Accept) tai kieltävän (Access-Reject) päätöksen. Tämän mukaan verkonliityntäpiste tekee päätöksen asiakaslaitteen pääsystä. [8]



Kuva 4. Radius viestinvaihto [Lähdettä 22 mukaillen]

Autentikointiesimerkki

Jotkut palveluntarjoajat vaativat käyttäjää syöttämään annetut salasanat Internet-yhteyttä (modeemi, ADSL) muodostaessa. Nämä tunnukset laitetaan verkonliityntäpisteelle PPP-yhteyden läpi. Tämän jälkeen muodostetaan yhteys RADIUS-palvelimelle. Käytössä on RADIUS-protokolla. RADIUS-palvelin tarkistaa, että tunnukset ovat kelvolliset. Tämän jälkeen RADIUS-palvelin todentaa yhteyden. Todentamisen jälkeen RADIUS-palvelin palauttaa verkonliityntäpisteelle tiedon, että yhteys on käytettävissä. Internet-yhteyksien lisäksi radiusta käytetään nykyään VOIP-sovellutusten kanssa. Nykyään RADIUS on otettu suurempaan käyttöön myös lähiverkoissa. Lähiverkkokytkimet ja langattomat tukiasemat voivat ottaa yhteyttä RADIUS-palvelimeen, jolloin myös AAA palvelut ovat käytössä. [9]

Seuraavaksi kerrotaan RADIUS:n ongelmina pidettäviä asioita, jotka heikentävät protokollan tietoturvaa.

Jaettu salasana

RADIUS-protokolla käyttää jaettua salaisuutta. Tällä tarkoitetaan, että sekä RADIUS-palvelimelle että liityntäpisteelle määritetään sama salasana. Jaetun salasanan ongelma on, että se on helppo saada selville. Salasanaa ei saada tarpeeksi monimuotoiseksi, jotta sitä ei olisi helppo arvata. Salasana voidaan saada myös selville salakuuntelemalla palvelimen ja käyttäjän välistä liikennettä ja laskemalla salasana sen perusteella. Jossain systeemeissä tilanne on vielä pahempi, kun salasanaksi hyväksytään vain tietyt perusmerkit. Tällöin mahdollisia salasanoja on murto-osa kaikista mahdollisista. [10]

IP-osoitteen väärennys

Kun viestit saapuvat RADIUS-palvelimelle, se tarkistaa joka kerta mistä osoitteesta lähetys tulee. Lähde-osoite on kuitenkin helppo huijata. Ratkaisuna tähän on lisätä viestiin MD5 (Message Digest 5)-todennusatribuutti. MD5-salauksella tarkoitetaan että annetusta merkkijonosta muodostetaan 128-bittinen tiiviste, joka esitetään 32-merkkisenä heksakoodattuna jonona.

MD5-koodin pystyy kanssa murtamaan kuuntelemalla liikennettä ja sieppaamalla kaksi viestiä, joilla on sama MD5-tiiviste. Tämän jälkeen pystytään laskemaan matemaattisesti oikea merkkijono, koska saman tiivisteen tuottavia merkkijonoja on rajallisesti. Tähän menee kuitenkin melkoisesti aikaa. [10]

2.3.2 TACACS+

TACACS+ eli Terminal Access Controller Access-Control System Plus on autentikointi protokolla, joka on yleisesti käytössä monissa yrityksissä. Yhden tai usean keskitetyn palvelimen kautta pystytään hallitsemaan käyttäjien pääsyä monille erilaisille tietoliikennelaitteille, kuten esimerkiksi kytkimille. Ciscon kaikilla uusilla laitteilla on tuki TACACS+ protokollalle. TACACS+:aa voidaan käyttää myös samalla lailla kun RADIUSta käyttäjien etäyhteyksien autentikointiin.

TACACS+ perustuu aikaisempaan TACACS-protokollaan, mutta on kuitenkin täysin uusi versio, jolla ei ole vanhan protokollan kanssa mitään yhteensopivuutta. TACACS+ kuten RADIUSkin antavat vain hyväksytyille käyttäjille oikeuden verkkoon. Palvelin varmistaa nämä käyttäjät ennen kuin pääsy sallitaan. [11]

Autentikointi

TACACS+ välittää monen tyyppisiä salasanatietoja, kuten ARAa, SLIPaa, PAPia, CHAPia ja telnet:ä. Nämä tiedot se salaa MD5-salauksella. Tämä sallii sen, että käyttäjät voivat käyttää samaa käyttäjätunnusta eri protokollan kanssa. TACACS+ tukee myös uusia salasanoja kuten KCHAP. [12]

Valtuutus

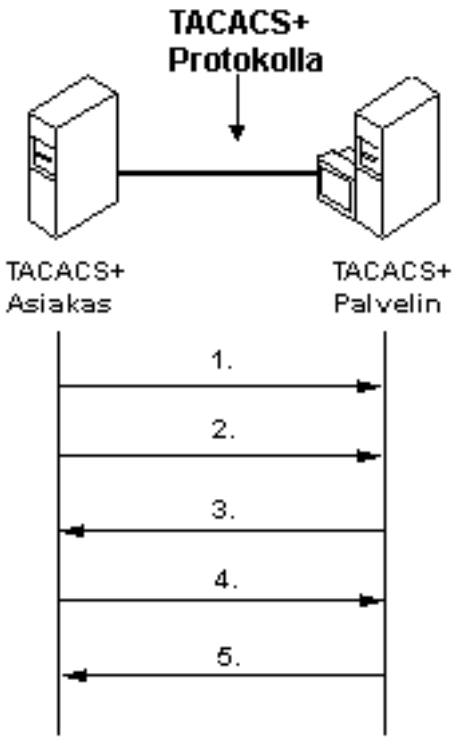
TACACS+:lla on tapa, jolla se kertoo reunapalvelimelle, jolta pyyntö tulee, mitä pääsylistaa käyttäjän, joka on yhteydessä porttiin X, on käytettävä. TACACS+-palvelin hakee käyttäjätunnuksen ja salasanan ja sen jälkeen tunnistaa pääsylistan. Pääsylista korvaa sen, joka reunapalvelimella on. TACACS+-palvelin vastaa käyttäjälle hyväksytty-viestillä, jolloin pääsylista tulee voimaan. [12]

Tilastointi

TACACS+ hankkii tilastointitiedot tietokantaan TCP:n avulla. Tämä varmistaa turvallisemman siirron ja täydellisen tilastointilokin. TACACS+ saa käyttäjän verkko-osoitteen, käyttäjänimen, käytetyn palvelun, protokollan, ajan ja pakettisuodattimen joka aiheutti lokin kirjoituksen. [12]

Toiminta

Periaatteessa TACACS+ antaa samat palvelut kuin RADIUS. Jokainen autentikointiyritys kirjataan lokeihin. TACACS+-autentikointi käyttää kolmea eri pakettityyppiä. Start-pakettien ja Continue-pakettien lähettäjä on aina TACACS+ asiakas. TACACS+-palvelin vastaa näihin viesteihin Reply-paketilla. Reply-paketilla joko sallitaan tai kielletään pääsy. Vain kolme väärää kirjautumisyritystä sallitaan. [11]



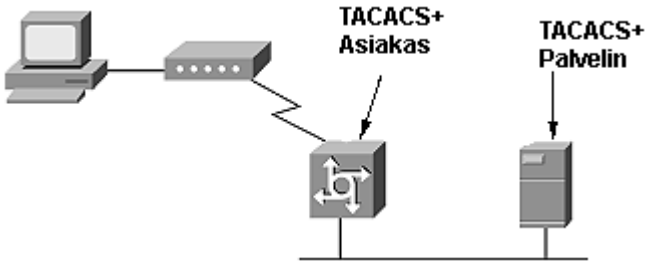
Kuva 5. TACACS+ viestinvaihto [Lähdettä 21 mukaillen]

Kuvassa 5 on esitetty TACACS+ viestinvaihto.

1. TACACS+-asiakas avaa TCP-yhteyden.
2. TACACS+-asiakas lähettää Start -paketin.
3. TACACS+-palvelin vastaa Reply ja voi pyytää käyttäjää antamaan käyttäjätunnuksen, salasanan, pääsynumeron tai jotain muuta tietoa.
4. Kun tiedot on syötetty, TACACS+-asiakas lähettää ne Continue-viestillä.
5. TACACS+-palvelin lähettää Reply-paketin.
6. Kun autentikointi on suoritettu, yhteys suljetaan.

Autentikointiesimerkki

Kun käyttäjä yrittää tunnistautua PAPin tai CHAPin avulla puhelinliittymän kautta reunapalvelimelle. Reunapalvelin ottaa yhteyttä verkon läpi autentikointipalvelimeen TACACS+:n avulla ja pyytää vahvistusta. Tämä vahvistus voi sisältää tunnuksen ja salasanan lisäksi muita parametrejä, kuten soittolinjan ja pyynnön käyttää jotain tiettyä IP-osoitetta. TACACS vahvistaa tiedot oikeiksi tietokannastaan, kirjoittaa tapahtumasta lokin ja lähettää hyväksymisviestin reunapalvelimelle. TACACS antaa reunapalvelimelle luvan ilmoittaa, milloin yhteys katkaistaan. [13]



Kuva 6. TACACS+ autentikointi esimerkki. [Lähdettä 21 mukaillen]

RADIUS:n ja TACACS+:n erot

TACACS+ eroaa radiuksesta siten, että siinä on autentikoinnille, valtuutukselle ja tilastoinnille eri palvelut. Nämä kaikki kolme palvelua käyttävät pelkästään porttia 49. TACACS+ tarjoaa myös turvallisemman TCP-siirto protokollan ja koko paketin salauksen. Näiden kahden protokollan erot ovat esitetty taulukossa 2. [14]

Taulukko 2. TACACS+ ja RADIUS erot [Lähdettä 14 mukaillen]

	TACACS+	**RADIUS**
Lähetys protokollalla	TCP - yhteyksellinen	UDP - yhteydetön
Käytetty portti	49	Autentikointi ja valtuutus 1645 ja 1812 Tilastointi 1646 ja 1813
Salaus	Koko paketin salaus MD5	Vain salasanan salaus 16-bit
AAA arkkitehtuuri	Eri palvelut autentikoinnille, valtuutukselle ja tilastoinnille	Autentikointi ja valtuutus yhdistetty yhdeksi palveluksi.
Käyttö	Laitteiden hallinta	Käyttäjien pääsyn hallinta

2.4 CISCO IOS

Cisco IOS (Internetwork Operating System) on hallitseva käyttöjärjestelmä Ciscon reitittimissä ja kytkimissä. IOS:n avulla pystytään hallitsemaan kyseisten tietoliikennelaitteiden toimintoja. Cisco IOSlle ominaista on sen komentoperusteinen käyttöliittymä. Siinä siis kirjoitetaan komennot peräkkäisille komentoriveille. Yleensä komennot koostuvat monesta sanasta. Kirjoitushetkellä uusin IOS-version on 12.4. Version perässä voi olla myös erinäisiä numeroita ja kirjaimia, jotka kertovat, minkälainen versio on kyseessä ja kenelle se on kohdennettu. [15]

IOS:ään pääsee käsiksi kytkemällä tietokoneen sarjaportista Rollover-kaapeli kytkimen konsoliporttiin. Tietokoneelta yhteyden saa esimerkiksi Windowsin HyperTerminalin tai ilmaisen Puttyn avulla. Puttyn kautta pystyy ottamaan yhteyden joko Telnet-muodossa tai SSH:n avulla, jos laite tukee kyseistä standardia. IOSsään saa myös yhteyden keskitettyjen hallintaohjelmien avulla, kuten esimerkiksi CiscoWorks Small Network Management Solutionin eli SNMS:n.

Rakenne

CISCO IOS jakautuu kahdelle eri käyttäjätasolle. Alempi käyttäjätaso on nimeltään user exec mode. Tällä tasolla käyttäjällä ei ole minkäänlaisia oikeuksia tehdä muutoksia asetuksiin. Taso on tarkoitettu lähinnä vain asetusten tutkimista varten, ja yleisin komento tällä tasolla onkin show. Komentorivillä User exec moden tunnistaa laitteelle asetetusta nimestä ja nuolesta, esim. Switch>. Pelkästään konsoliporttia käyttämällä tälle user exec modelle ei pysty asettamaan salasanaa.

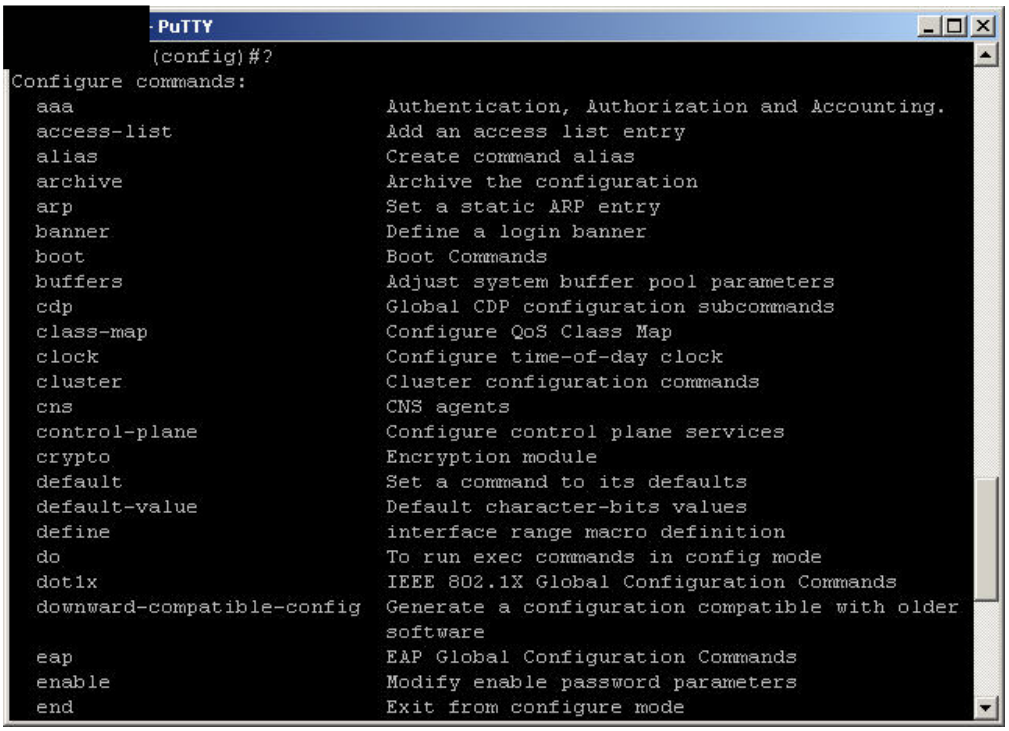
Komentoja on paljon eikä niitä pysty aina muistamaan ulkoa. Tätä varten komentoriville voi kirjoittaa kysymysmerkin ’?’. Tämä listaa kaikki mahdolliset komennot, jotka ovat käytettävissä. Yleensä jokaisen pääkomennon alta löytyy useita lisävalintoja. Nämä lisävalinnat saadaan esiin kirjoittamalla ensimmäinen komento-osa ja sen perään kysymysmerki, esimerkiksi show ?:n (kuva 7). Tärkeimpiä show käskyjä on show running-config, jolla saadaan näkyviin tällä hetkellä käytössä oleva konfiguraatio. Show interface status:lla nähdään laitteen eri liitäntöjen tilat. Show version-komennolla nähdään muun muassa käyttöjärjestelmän versio, käynnissäoloaika sekä paljon muuta itse laitteeseen sidonnaista tietoa.

Kuva 7. Cisco IOS Show ?

Kun asetuksia halutaan muuttaa, joudutaan user exec modesta siirtymään privileged exec modeen. Siirtyminen tapahtuu kirjoittamalla enable. Tämän takia ylempää käyttäjätasoa yleensä kutsutaankin enable modeksi. Jos halutaan siirtyä takaisin alemmalle tasolle, kirjoitetaan yksinkertaisesti disable. Privileged exec moden tunnistaa laitteen nimestä ja risuaidasta, esimerkiksi Switch#:sta.

Enable modesta löytyy huomattavasti enemmän komentoja, joita voidaan käyttää. Tärkeitä ovat muun muassa user exec modessa show –komennot ja debug –komennot, joilla pystytään tarkastelemaan tapahtumia.

Seuraavaksi tarkastellaan hieman komentoa, jonka alta tehdään kaikki muutokset asetuksiin. Enable modessa kirjoitetaan configure terminal ja kysymysmerkki, jolla saadaan näkyviin käytettävät komennot. Kuvassa 8 näkyy osa kaikista mahdollisista komennoista. Tämän alta pystytään laittamaan asetukset liittymille, käytettäville protokollille sekä kaikkeen muuhun laitteen toimintaan liittyvään.



Kuva 8. Cisco Conf t

Komentoja voi syöttää myös lyhyemmässä muodossa, kuten esimerkiksi configure terminal on lyhennettynä conf t (kuva 8). Nämä lyhennyssäännöt pätevät niin kauan kuin lyhennettävällä käskyllä ei ole kuin yksi mahdollisuus. Show voidaan lyhentää sh, mutta ei pelkästään s, koska s:llä alkavia komentoja on muitakin. Komentoja ei myöskään tarvitse aina kirjoittaa loppuun asti sillä tab-näppäimellä pystytään täydentämään käsky, kun sitä on jo kirjoitettu sen verran, että se ei voi mennä sekaisen muiden samalla lailla alkavien käskyjen kanssa. [18]

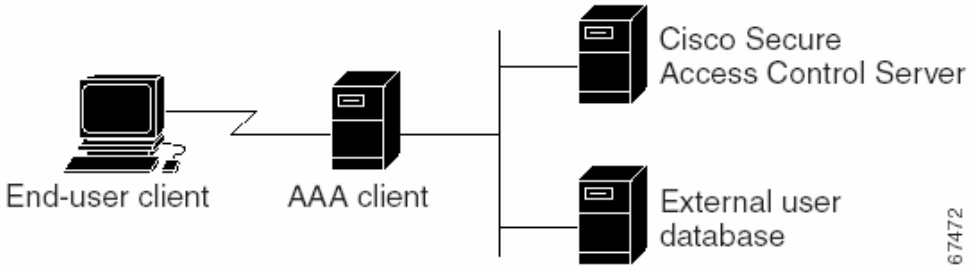
2.5 CISCO ACS

ACS eli Cisco Secure Access Control Server on Ciscon kehittämä hallintaohjelma. Ohjelman avulla pystytään kontrolloimaan pääsyä verkon laitteille sekä käyttäjien pääsyä verkkoon. Ohjelma vaatii alustaksi joko Windows- tai Unix-palvelimen. ACS tarjoaa keskitetyn tietokannan, jonka avulla pystytään hallitsemaan kaikkia AAA-palveluita.

2.5.1 Yleistä

ACS tarjoaa keskitetyn tietokannan AAA-palveluille ja yksinkertaistetun käyttäjien hallinnan kaikille Ciscon laitteille. ACS:n avulla verkonvalvojien on helpompi määritellä, ketkä saavat kirjautua verkkoon ja mitä palveluja kirjautuneella käyttäjällä on käytössä. Tämän lisäksi se pitää kirjaa kirjautumisista ja hoitaa vaadittavan tilastoinnin. [18]

Cisco ACS tarjoaa AAA-palveluita kaikille verkon laitteille, jotka toimivat AAA-asiakkaina. Tällaisia voivat olla esimerkiksi kytkimet ja reitittimet. Kuvassa 9 nähdään periaatekaavio siitä, miten verkossa oleva ACS-palvelin toimii. AAA-asiakas ottaa yhteyden AAA-palvelimeen käyttämällä joko TACACS+- tai RADIUS-protokollaa. AAA-asiakas tunnistetaan käyttämällä ACSn sisäistä tietokantaa, johon AAA-asiakkaat on tallennettu. Jokaiselle AAA-asiakkaalle määritetään salasana, jota TACACS+ tai RADIUS käyttää. Sama salasana on laitettava myös AAA-asiakaslaitteeseen. ACS:ään voidaan tehdä asetukset myös niin, että se hakee tunnukset jostain ulkoisesta tietokannasta. [18]



Kuva 9. Cisco ACS AAA-palvelin [Lähdettä 23 mukaillen]

ACS:stä löytyy suuri määrä erilaisia ominaisuuksia, jotka tekevät siitä hyvin käyttökelpoisen. Tässä on niistä muutama:

- ODBC- ja LDAP-yhteensopivuus
- monta joustavaa 802.1x-autentikointityyppiä, kuten EAP-TLS, PEAP, LEAP, EAPS-FAST ja EAP-MD5
- palveluiden automaattinen monitorointi, tietokantojen synkronointi ja datan tuonti työkalut
- ladattavat pääsylistat kaikille Tason 3 laitteille, kuten Ciscon reitittimille, palomuureille ja VPN:lle
- verkkoon pääsyn rajoituksen
- käyttäjien ja järjestelmänvalvojien pääsyn raportointi.

Näiden ominaisuuksien ansiosta Cisco ACS sopii erittäin hyvin käytettäväksi 802.1x-ympäristöihin. Se sisältää AAA-palvelimen, tukee erilaisia EAP-autentikointiprotokollia ja pystyy hakemaan käyttäjätiedot ulkoisesta tietokannasta. [16]

2.5.2 Sisäinen rakenne

ACS:n toiminnallisuus perustuu seitsemään prosessiin, joita Windows palvelin pyörittää. Jokainen näistä prosesseista pystytään pysäyttämään ja käynnistämään erikseen sekä Windows palvelimelta tai ACS:n käyttöliittymästä. Seuraavassa on lyhyesti kuvattu, mistä mikäkin prosessi vastaa.

CSadmin

CSadminilla tarkoitetaan sisäänrakennettua web-palvelinta ACS:n hallintaa varten. Palvelin sallii ohjelmaan monta yhdenaikaista istuntoa. Vakiona käytetään http porttia 2002.

CSAuth

CSAuth vastaa käyttäjien autentikoinnista, se sallii tai kieltää palvelujen käytön. Hallitsee ACS-tietokantaa ja välittää eteenpäin autentikoinnit, jotka kohdistuvat ulkoisiin tietokantoihin.

CSDBSync

CSDBSync vastaa ACS-tietokannan synkronoinnista ja kopioinnista toisiin ACS-palvelimiin.

CSLog

CSLog monitoroi ja pitää kirjaa seuraavista asioista: käyttäjien ja järjestelmänvalvojien tapahtumista, varmistukset ja palautukset, tietokantojen kopioinnit ja synkronoinnit, ACS:n ydinpalvelut, TACACS+:n ja RADIUS:n tilastoinnit ja VoIP-tilastointi.

CSTacacs ja CSRadius

CSTacacs ja CSRadius kommunikoivat verkkolaitteiden ja CSAuth modulin kanssa.

CSMon

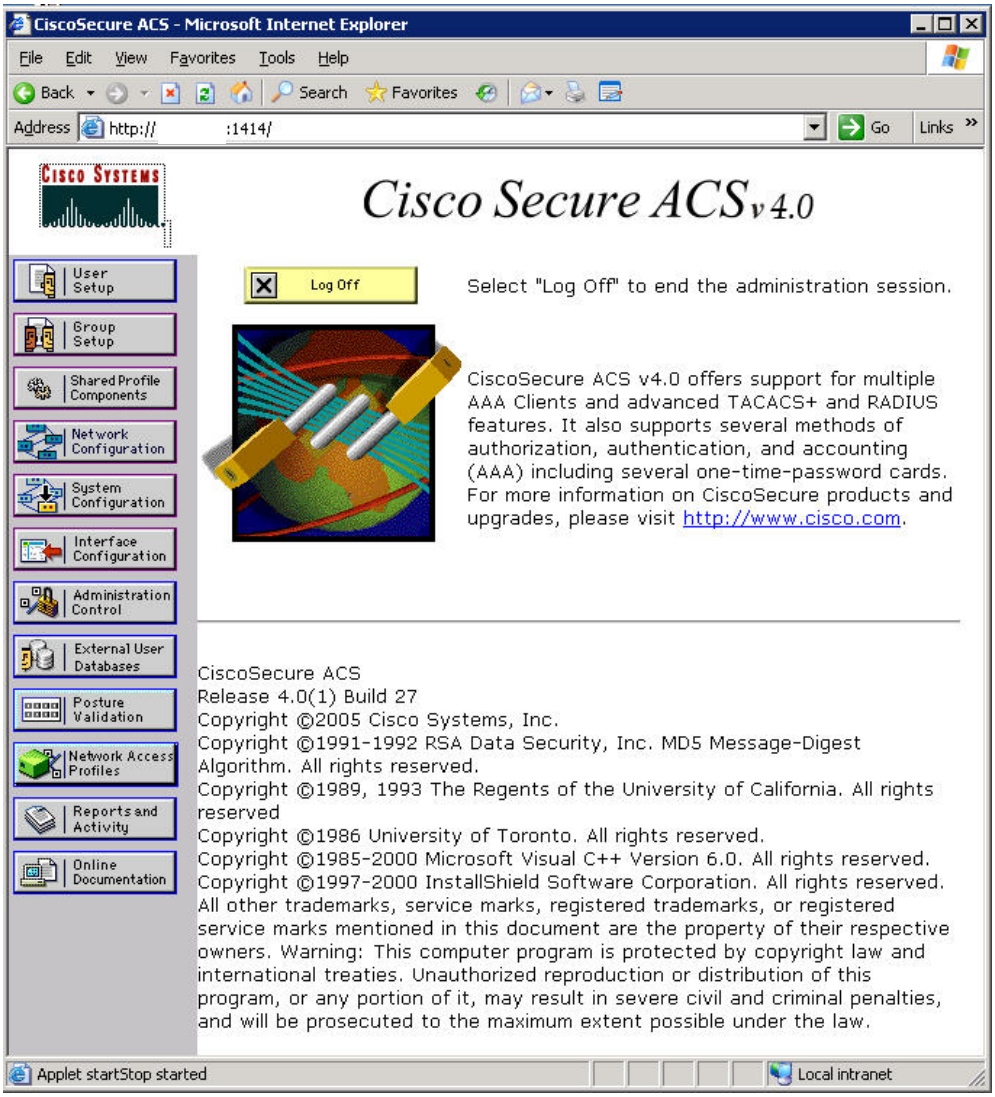
CSMon monitoroi ACS palveluiden tilaa ja palvelimen resursseja. Raportoi ja kirjoittaa kriittiset virheet lokiin. Lähettää mahdollisista ongelmista sähköpostia järjestelmänvalvojalle. Tunnistaa automaattisesti ja käynnistää uudelleen ACS palvelut. [18]

2.5.3 ACS käyttöliittymä

Cisco ACS:ään pääsee käsiksi selaimella kirjoittamalla osoiteriville palvelimen nimen ja laittamalla portiksi 2002 (kuva 10).

Kuva 10. Cisco ACS kirjautumisivu

ACS:lle kirjautumisen jälkeen avautuu päävalikkosivu, jossa vasemmalla palkissa on eri valintoja, joiden kautta asetuksia pystytään muuttamaan (kuva 11). [18]



Kuva 11. Cisco ACS päävalikko

User Setup

User Setupin alta pystytään lisäämään käyttäjä ACSn sisäiseen kantaan. Käyttäjälle pystytään määrittämään salasanan lisäksi paljon eri toimintoja, kuten esimerkiksi rajoitukset käyttöajankohdan suhteen ja ryhmän, johon käyttäjä kuuluu.

Group setup

Group setupin alta pystytään tekemään ja muokkaamaan erilaisia ryhmiä. Näille ryhmille voidaan laittaa myös jotain yhteisiä sääntöjä, jotka pätevät kaikkiin sen alla oleviin käyttäjiin.

Shared Profile Components

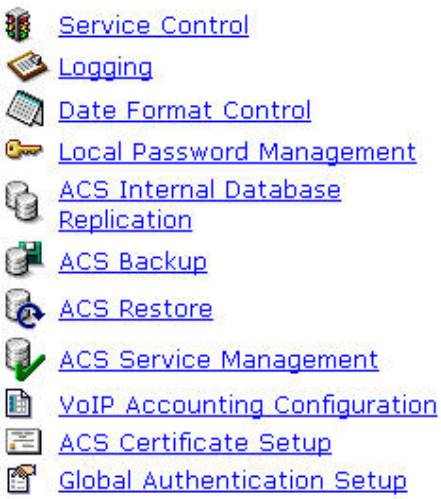
Shared Profile Components:n alta pystytään määrittelemään tiettyjä jaettuja komponentteja, jotka asetetaan kerran ja voidaan tämän jälkeen kohdistaa tietylle käyttäjälle tai ryhmälle. Tämmöisiä komponentteja ovat muun muassa ladattavat pääsylistat.

Network Configuration

Network Configurationin alta pystytään määrittelemään AAA-asiakkaat ja antamaan niille salasanat. Täällä pystytään myös määrittämään, jos käytössä on jotain muita AAA-palvelimia.

System Configuration

System Configurationin alta löytyy paljon erilaisia valintoja, joilla pystytään vaikuttamaan järjestelmän toimintaan. Tämmöisiä ovat muun muassa palvelujen uudelleen käynnistys, päivämäärän ja ajan säätö, paikallisten salasanojen hallinta, varmistukset, IP-osoitteiden jakelu, sertifikaattiasetukset ja autentikointi asetukset.



Kuva 12. Cisco ACS - System Configuration

Interface Configuration

Interface configurationin alta pystytään määrittelemään muutamia lisävaihtoehtoja, jotka näkyvät vain tietyissä valikoissa. Kategorioita on neljä: User data, TACACS+, RADIUS ja Advanced. Esimerkiksi TACACS+- ja RADIUS-valinnat näkyvät vain AAA-valikoissa.

Administrator Control

AdministratorControlin alta pystytään hallinnoimaan järjestelmänvalvojien tilejä.

External User Database

External User Databasen alta pystytään asettamaan että ACS hakee käyttäjätiedot jostain toisesta käyttäjätietokannasta. Tuettuja ulkoisia kantoja ovat muun muassa Windows AD-, Novell-NDS- ja erilaiset ODBC-tietokannat.

Reports and activity

Raportit ja aktiviteetit ovat yksi ACS:n tärkeimpiä analysointityökaluja. Tämän alta pystytään tutkimaan, ovatko autentikoinnit menneet läpi vai eivät ja muun muassa RADIUS- ja TACACS+-tilastointi. Täältä näkyvät myös kirjautuneet käyttäjät ja ne, joilta käyttö on kielletty.

Online Documentation

Online Documentationin Tämän alta löytyvät verkossa olevat Ciscon dokumentit.

2.6 AD

AD aktiivihakemisto on Windows Server 2000 ja Windows Server 2003 palvelimien yhteydessä markkinoille tullut keskitetty integroitu hakemistopalvelu. AD:n edeltäjä NT-maailmassa tunnetaan nimellä NTDS eli NT Directory Services. Muita samantyylisiä hakemistopalveluita ovat esimerkiksi Novell eDirectory ja OpenLDAP. Active Directory on rakennettu Domain Name System eli DNS ja Lightweight Directory Access Protocol:n (LDAP) ympärille. Nämä protokollat on valittu, koska kummatkin ovat alustavapaita protokollia ja toimivat kaikkien järjestelmien kanssa.

Aktiivihakemistossa on yhdistettynä monta toimintoa, jotka aikaisemmin ovat olleet hajautettu moneen eri järjestelmään ja aiheuttaneet järjestelmän ylläpitäjille ylimääräistä vaivaa. Aktiivihakemiston avulla järjestelmänylläpitäjä pystyy helposti lisäämään yksittäisen käyttäjän, antaa tälle oikeuden käyttää etäyhteyttä verkkoon, antaa oikeudet käyttää sähköpostia (jos käytössä on Windows Exchange sähköpostipalvelin) ja antaa oikeudet eri verkkoresursseille.

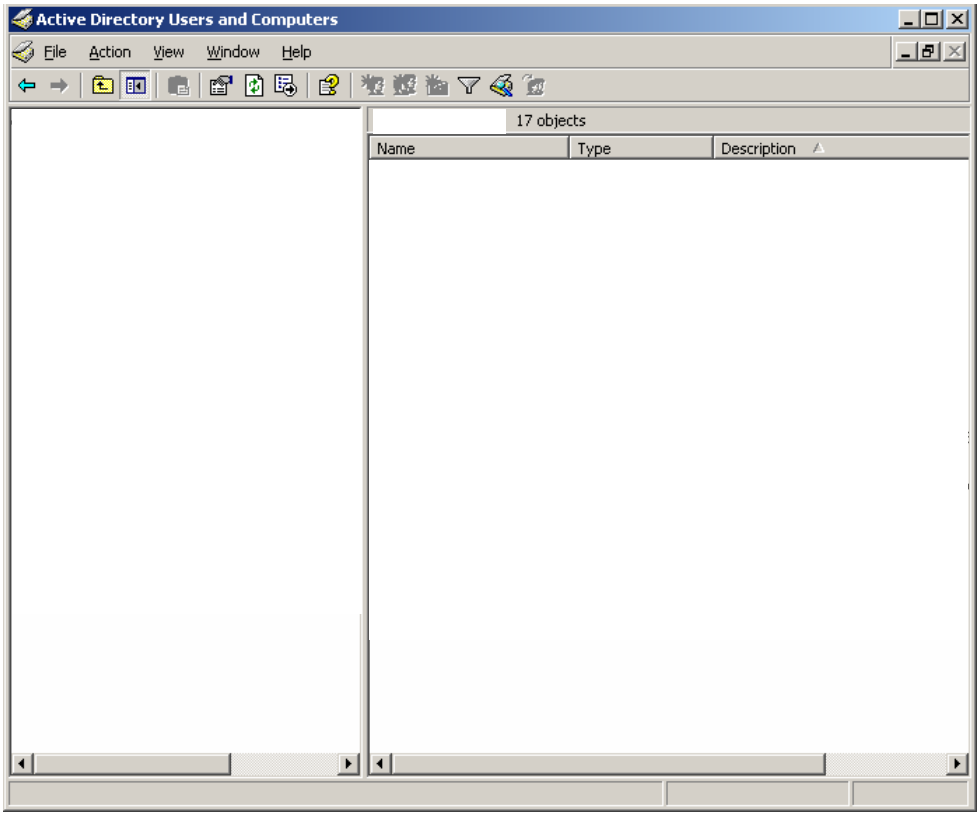
Kun tavallinen käyttäjätili, sähköpostitili ja ohjelmat linkitetään aktiivihakemistoon, se helpottaa huomattavasti käyttäjätilien lisäämistä, muokkaamista ja poistamista. Kun esimerkiksi käyttäjän sukunimi vaihtuu, sen tarvitsee muuttaa vain yhteen paikkaan, jonka jälkeen käyttäjätiedot ovat taas ajan tasalla. Käyttäjän voi myös määrittää kuulumaan tiettyyn ryhmään, jolloin käyttäjään kohdistuu ryhmälle annetut oikeudet. Käyttäjien lisäksi aktiivihakemistoon voi tehdä myös konetilejä verkossa oleville työasemille, joiden avulla pystytään asentamaan ohjelmia, lisäämään kone tiettyyn ryhmään ja antaa koneelle tiettyjä oikeuksia.

Aktiivihakemiston käytön avulla saavutetaan monia etuja, joista tärkeimpiä ovat käyttäjien tuottavuuden lisääminen, ylläpitäjien työn helpottaminen, palvelujen alhaallaoloajan minimoiminen ja turvallisuuden lisääminen. [19]

Rakenne

AD:ta käytetään MMC eli Microsoft Management Consolen kautta. MMC jakautuu kolmeen eri ryhmään: Active Directory Manager, Active Directory Tree Manager ja Active Directory Sites and Services Manager. Tärkein näistä on Active Directory Manager, jonka kautta päästään hallinnoimaan erilaisia ryhmiä ja käyttäjätilejä.

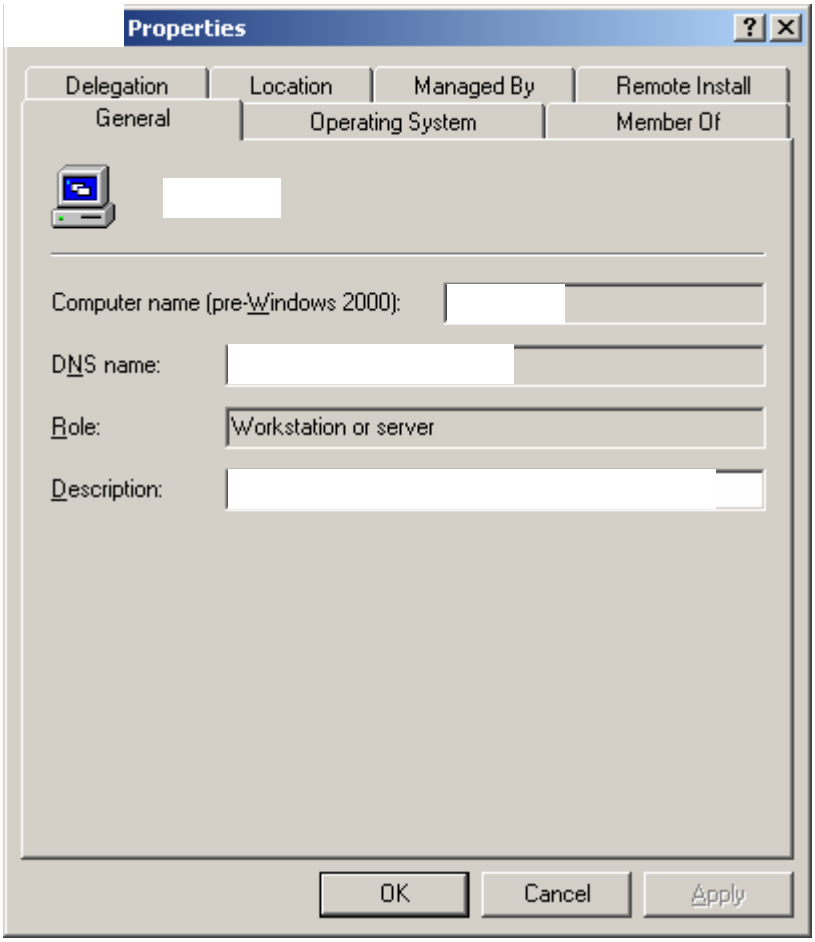
Kuvassa 13 näkyy, miten toimialue on jaettu erilaisiin ryhmiin. Ryhminä löytyy esimerkiksi admin-ryhmä, jonka alta löytyvät järjestelmän valvojat, joiden tunnuksille on annettu tavallista käyttäjää enemmän oikeuksia. Seuraavina ryhminä löytyvät computer, user ja. Computerin alta löytyvät verkossa olevat tietokoneet. Usersin alta löytyvät tavalliset käyttäjät.



Kuva 13. Microsoft AD -rakenne

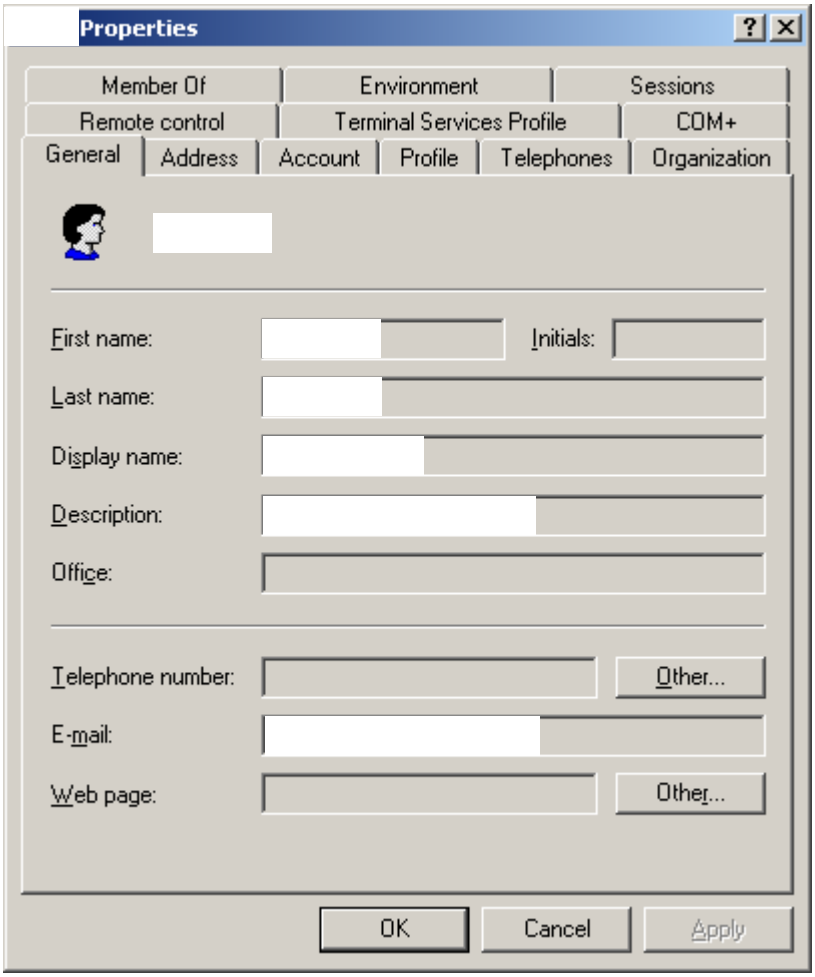
Käytännössä AD:n avulla pystytään helposti jakamaan niin käyttäjät kuin koneetkin eri alaryhmiin esimerkiksi osaston mukaan, kuten markkinointi, myynti ja talous. Tällöin eri osastojen koneille pystytään helposti pudottamaan kunkin osaston käyttämiä ohjelmia niin sanottujen group policyjen avulla. Tämän avulla säästetään aikaa kun asentajan ei tarvitse juosta koneelta toiselle samaa ohjelmaa asentaen. Samalla tavalla voidaan helposti yhtenäistää tietoturva-asetukset, selaimen asetukset, käyttöliittymän ja järjestelmän asetukset.

Kuvassa 14 on kuvattu yksittäinen tietokonekortti. Kortissa ovat koneen nimitiedot, jotka kannattaa pitää järjestyksessä antamalla koneelle kuvaava nimi. Koneen nimen eteen voidaan merkata LapTop tai DeskTop. Kuvauskenttään annetaan koneelle yksilöllinen kuvaus kuten käyttäjän nimi ja osasto.



Kuva 14. Microsoft AD -konekortti

Kuvassa 15 on kuvattu yksittäisen käyttäjän käyttäjäkortti. Korttiin syötetään käyttäjästä muun muassa nimitiedot. Korttien avulla on helppo hallinnoida käyttäjän oikeuksia ja ryhmiin kuulumista.



Kuva 15. Microsoft AD – käyttäjätili

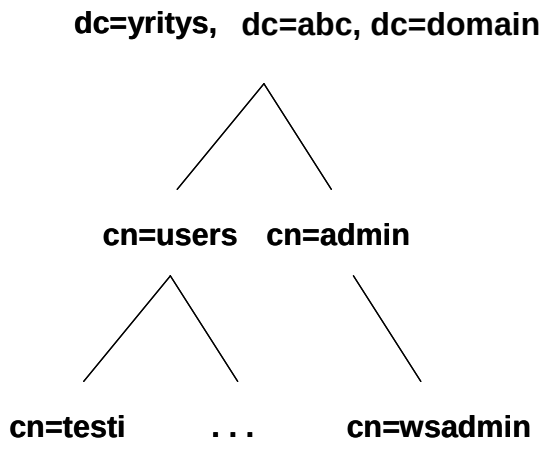
2.7 LDAP

AD on Microsoftin kehittämä LDAP sovellus Microsoft ympäristöön. LDAPilla eli Lightweight Directory Access Protocol:lla tarkoitetaan tietoliikenneprotokollaa, jolla haetaan ja muokataan hakemistopalveluja TCP/IP ympäristössä. LDAPin avulla pystytään tekemään hakemistopalveluista hakuja, joiden avulla pystytään käyttämään voimassa olevan käyttäjän tietoja muissa järjestelmissä.

LDAP-yhteys alkaa, kun asiakas ottaa yhteyttä LDAP-palvelimeen (esimerkiksi AD:iin). Vakiona käytetään porttia 389. Asiakas lähettää toimintopyynnön palvelimelle, joka vastaa siihen. Yleensä asiakas joutuu aina odottamaan vastausta ennen seuraavan pyynnön lähettämistä.

Perusoperaatioita ovat etsintä, vertaaminen, lisäys ja poisto. Näiden avulla toinen ohjelma pystyy hakemaan tietoa LDAPin avulla. LDAPin on yleensä rakennettu puuksi, joka on nimetty eri maantieteellisten nimien tai organisaation rakenteen perusteella. LDAPissa käytetään DNS-nimiä hierarkian nimeämisessä.

Otetaan malliesimerkiksi domain nimi domain.abc.yritys ja henkilö nimeltä testi, joka sijaitsee ryhmän users alla. Tämä esitettäisiin muodossa cn=testi, cn=users, dc=yritys, dc=abc, dc=domain. LDAP palvelimen osoite tässä tapauksessa olisi: ldap://ldap.domain.abc.yritys/dc=yritys,dc=abc,dc=domain (kuva 16). Tässä cn tarkoittaa common namea ja dc domain componentia.[20]



Kuva 16. LDAP hierarkia malliesimerkki

3 KÄYTÄNNÖN OSUUS

Työn ensimmäisessä kappaleessa kerrottiin työhön liittyvien ja työssä tarvittavien komponenttien toiminta teorian kannalta. Tässä kappaleessa käydään läpi komponenttien asetukset, joilla 802.1x-autentikointi on saatu toimimaan kyseisessä ympäristössä.

Vaikeuksia työn tekemisessä tuotti verkkoympäristö, johon autentikointia yritettiin implementoida. Koska verkkoympäristö oli jo valmiiksi olemassa ja ollut käytössä nykyisen mallisena jo monia vuosia, sitä ei pystynyt muokkaamaan mielettömiä määriä.

Koska työn toiminnan edellytyksenä oli, että se toimii nykyisessä ympäristössä, se oli pakko muodostaa suoraan olemassa olevaan toimistoverkkoon. Testiympäristön olisi voinut rakentaa, mutta siitä ei olisi ollut kovin paljoa helpotusta, kun oikea verkkoympäristö ja palvelinverkosto on kehittynyt monen vuoden ajan perus-asetuksista poikkeavaksi.

Työllä ja sen käyttöönotolla haluttiin parantaa verkon reunapisteiden toiminnallisuutta, lisäämällä niihin ”älyä”. Samalla haluttiin päästä eroon paljon aikaa ja työtä vievien MAC-lukkojen käytöstä. Tällä tarkoitetaan sitä, että koneen vaihdon yhteydessä koneen MAC-osoite vaihtuu ja kytkimen MAC-lukko menee päälle. Tämä pitää manuaalisesti vapauttaa.

Lisäksi haluttiin päästä eroon verkkoporttien staattisesta vlan määrittelystä, ottamalla käyttöön dynaaminen vlan määrittely käyttäjätietojen perusteella. Koska olemassa on jo yksi käyttäjien tietokanta, Microsoftin Active Directory, käytettiin sitä hyväksi.

3.1 ASC

Vaikka kyseissä ympäristössä on toiminnassa jo kaksi ACS-palvelinta, haluttiin tätä varten kokonaan uusi palvelin. Lisäksi työtä tehdessä ja oheismateriaalia lukiessa huomattiin, että ACS palvelimen pitää olla osa sitä toimialuetta, jonka käyttäjiä halutaan Active Directorista hakea. Nämä kaksi edellistä palvelinta olivat kokonaan toisessa toimialueessa. Lisäksi puhdas ACS oli eduksi, ettei mihinkään jo toimiviin järjestelmiin tulisi muutoksia ja näin käyttökatkoja.

Uuden ACS palvelimen pohjalle asennettiin Windows Server 2003. Asennuksen jälkeen kone liitettiin toimialueeseen. Sitten Windowsin päälle asennettiin ACS versio 4.0.

Seuraavaksi ACSään laitetaan kuntoon sertifikaatit. Sertifikaattipalveluiden alta valitaan Generate Self-Signed Certificate (kuva 17). Tämän tarkoituksena on luoda palvelimelle sertifikaatti, jolla asiakkaat saadaan uskomaan että kyseessä on varmennettu palvelin.

Kuva 17. ACS sertifikaatti palvelut

Sertifikaatti luodaan seuraavilla tiedoilla. Nimeksi laitetaan acstesti. Tallennuspaikaksi sertifikaatille sekä yksityiselle avaimelle c:\acstesti.cer ja c:\acstesti.pvk. Yksityiselle avaimelle annetaan salasanaksi testi. Avaimen pituudeksi laitetaan 1024bit, koska kaikki protokollat eivät tue pidempää salausavainta. Salausmetodi on SHA1. Valitaan ruksi että sertifikaatti asennetaan. Tiedot näkyvät kuvassa 18.

Kuva 18. ACS sertifikaatin tiedot

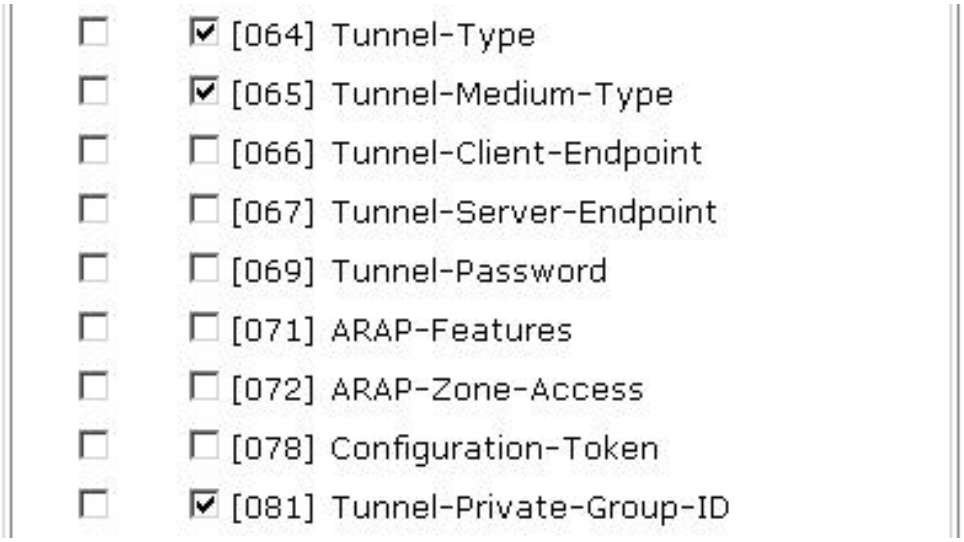
Varmistetaan vielä, että sertifikaatti on asentunut ja että se on toiminnassa (kuva 19).

Kuva 19. ACS Sertifikaatti on asentunut oikein

Seuraavaksi valitaan päävalikosta Interface Configuration. Tämän alta pystytään vaihtamaan esimerkiksi käyttäjätiedot sisältäviä kenttiä sekä niitä kenttiä, jotka näkyvät kun käyttäjän tietoja muokataan. Valitaan kuitenkin RADIUS (IETF), jonka alta lisätään kolme valintaa (kuva 20).

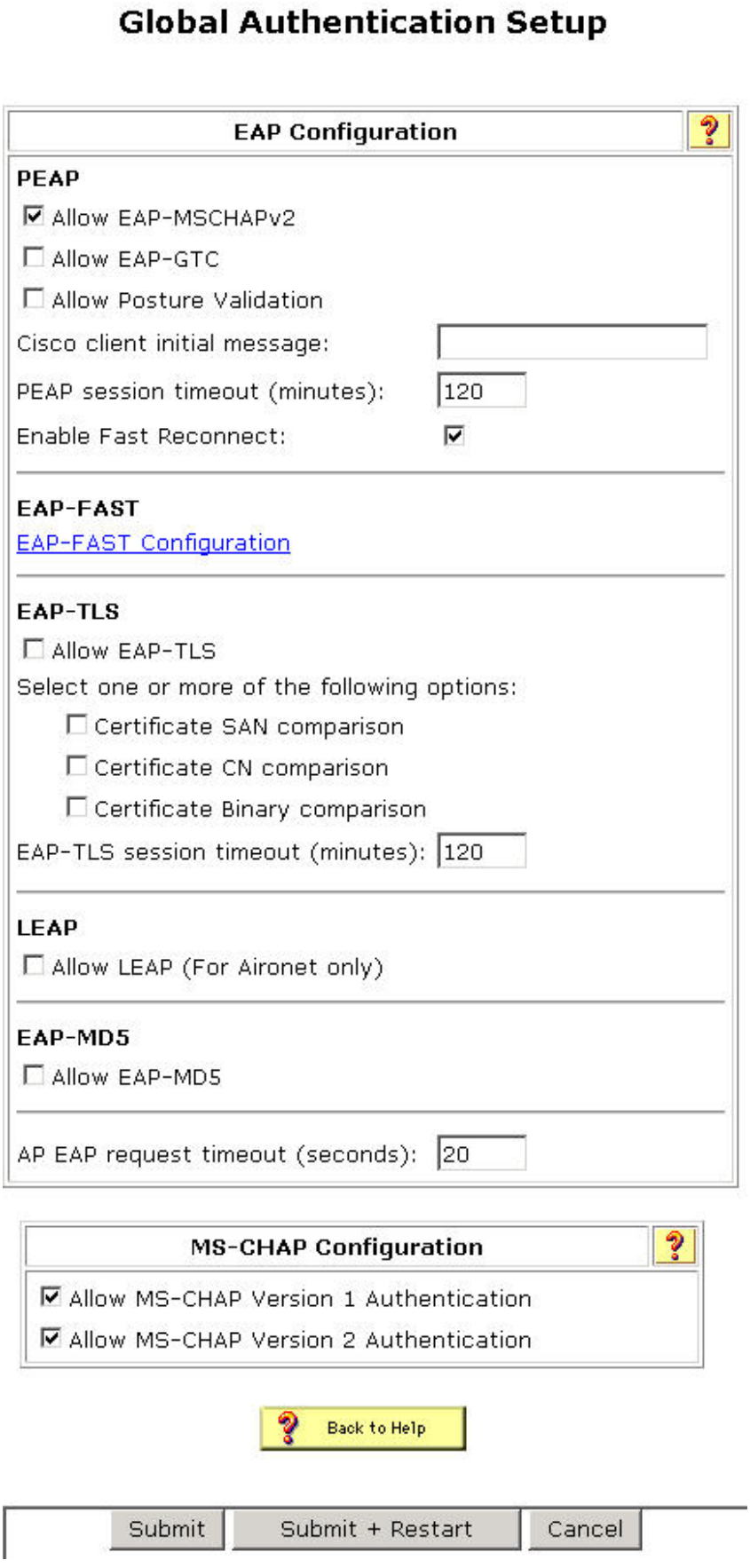
Kuva 20. Interface Configuration

Kuvassa 21 nähdään valitut attribuutit. Näitä ovat [64], [65] ja [81]. Myöhemmin selvitetään mitä näillä arvoilla tarkoitetaan. Valitaan, että attribuutit näkyvät vain ryhmille.



Kuva 21. ACS RADIUS attribuutit

Seuraavaksi vuorossa on autentikointiprotokollan valinta ja niiden asetusten laittaminen. Valitaan Päävalikosta System Configuration ja Global Authentication Setup. PEAP valikosta valitaan vain Allow EAP-MSCHAPv2 ja Enable Fast Reconnect. Näiden kahden raksin lisäksi valitaan Allow MS-CHAP version 1 authentication ja Allow MS-CHAP version 2 authentication. Oikeat asetukset ovat vielä kuvassa 22.



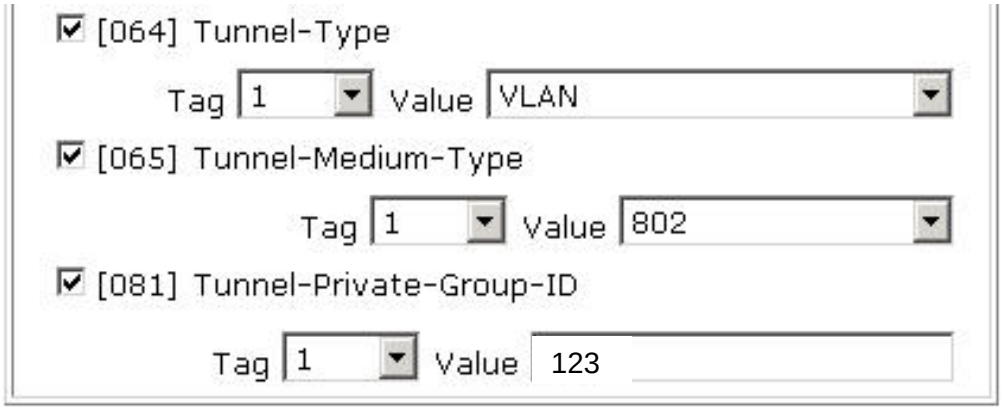
Kuva 22. ACS autentikointiprotokollan asetukset

Seuraavaksi muodostetaan ACS:ssään ryhmät eri vlan-käyttäjiä varten. Valitaan etusivulta Group Setup. Valitaan ryhmäksi esimerkiksi Group 2 ja muutetaan sen nimi VLAN123. Tämän jälkeen muokataan ryhmän asetuksia, Edit settings. Ainoat muutokset tehdään kohtaan IETF RADIUS Attributes.

Tunnelin tyypiksi [64] valitaan VLAN ja Tag laitetaan kohtaan yksi, jolloin sääntö on päällä. Tunnelin mediatyypiksi pannaan 802 ja Tunnelin privaattiryhmä ID on tässä tapauksessa 123. Arvo määräytyy aina sen ryhmän mukaan, jolle dynaaminen vlan määritys halutaan tehdä.

Jos [64] ja [65] attribuuteissa ei ole tuettua arvoa, niin vaikka RADIUS-palvelin antaa kytkimelle hyväksymispaketin access-accept, se tulkitsee paketin hylätyksi access-reject.

Muita arvoja ei tarvitse ruksittaa. Nämä kolme riittävät. Oikeat asetukset VLAN 123 ryhmälle näkyvät kuvassa 23.



Kuva 23. ACS RADIUS attribuutit ryhmä asetusten alla

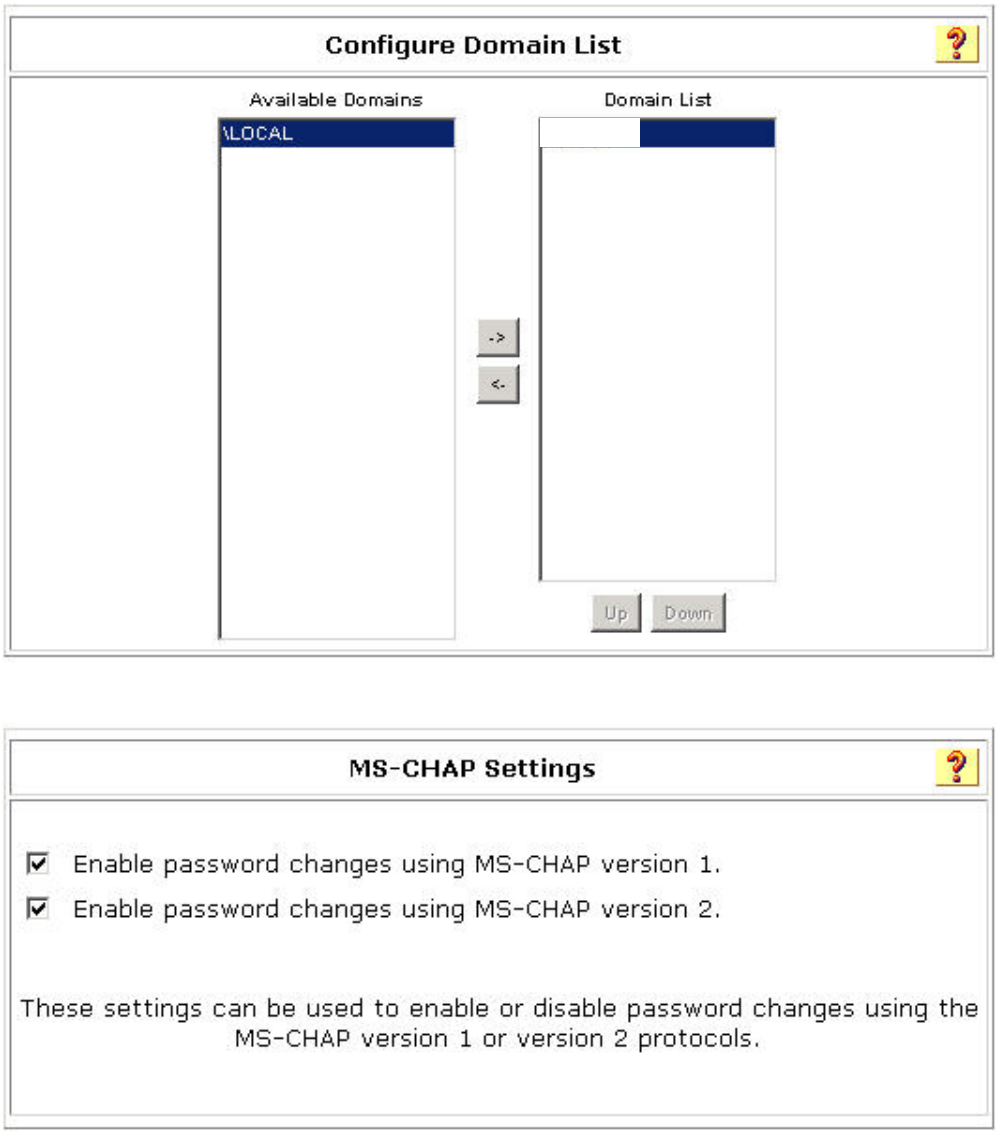
Seuraavana vuorossa on käyttäjien hallinta. Tarkoituksena on valita niin että, RADIUS:lle tulevat käyttäjätunnukset tarkastetaan AD:sta ja tämän tiedon perusteella päätetään, saako käyttäjä käyttää verkkoa. Valitaan External user database ja aluksi Database Configuration (kuva 24).

Kuva 24. ACS External user Database

Valitaan Windows Database ja Configure (kuva 25).

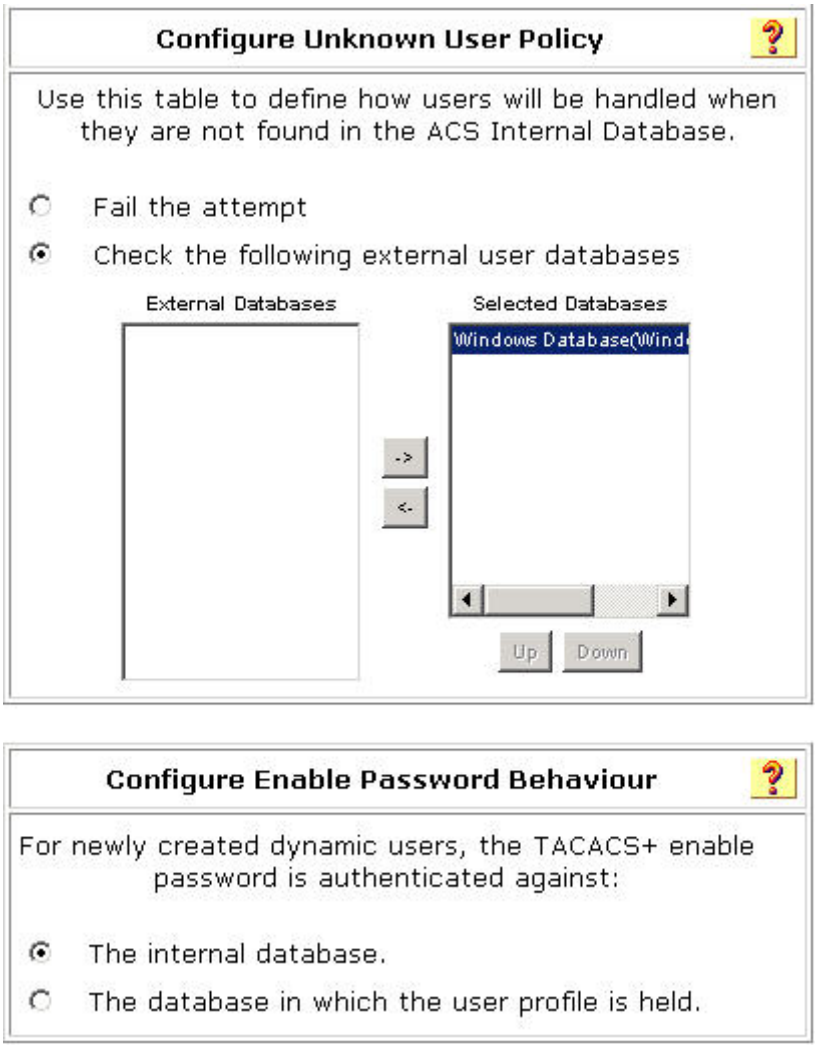
Kuva 25. ACS External User Database jälkeen valitaan Windows Database

Ainoat muutokset tässä vaiheessa tehdään Configure Domain Listiin. Domain List -kohdasta siirretään olemassa oleva toimialue oikealle puolelle. Lisäksi valitaan käytettäväksi kummatkin versiot MS-CHAPstä. Muut ruksit voi poistaa (kuva 26).



Kuva 26. ACS Windows database määritykset

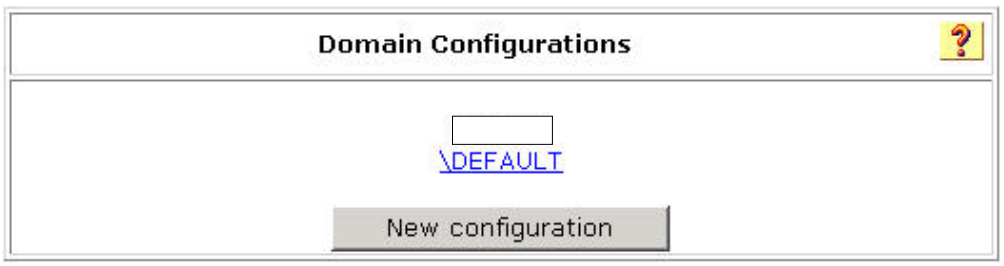
Palataan pari askelta takaisin päin ja valitaan Unknown user policy. Valitaan Check the following external user databases. Siirretään External database kohdasta Windows database valittujen puolelle (kuva 27).



Kuva 27. ACS määritellään tarkastettavaksi Windows database

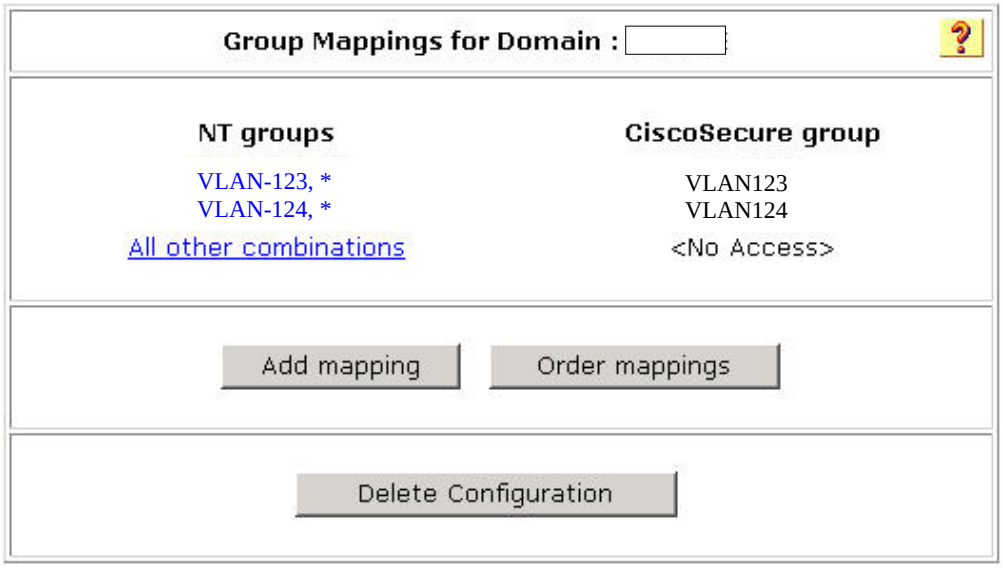
Seuraavaksi valitaan Database Group Mappings ja Windows Databasesta valitaan New Configuration (kuva 28 ja 29). Täältä lisätään haluttu toimialue. Tässä tapauksessa se on DOMAIN. Painetaan submit ja avautuvasta ikkunasta valitaan juuri valittu DOMAIN.

Kuva 28. ACS Valitaan Windows database



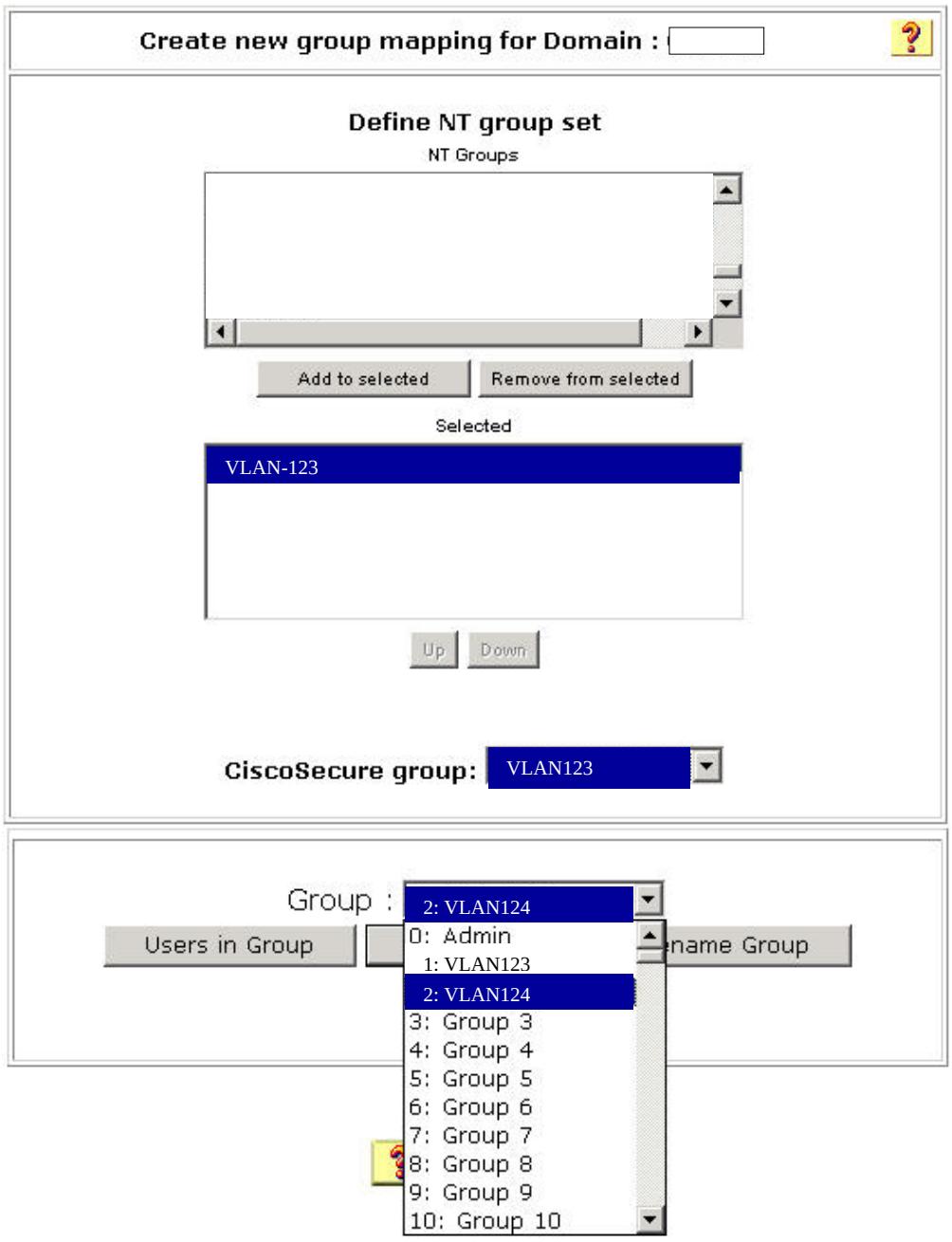
Kuva 29. ACS valitaan New Configuration

Tarkoituksena on saada seuraavan näköinen kokoonpano (kuva 30). ADn ryhmässä VLAN-123 olevat käyttäjät liitetään ACS-ryhmään VLAN123. Näin tehdään kaikille halutuille ryhmille.



Kuva 30. ACS haluttu sidos ADn ja ACSn ryhmien välillä.

Kuvassa 31 näkyy, miten VLAN-123 on valittu ACS ryhmän VLAN123 kanssa sidoksiin.

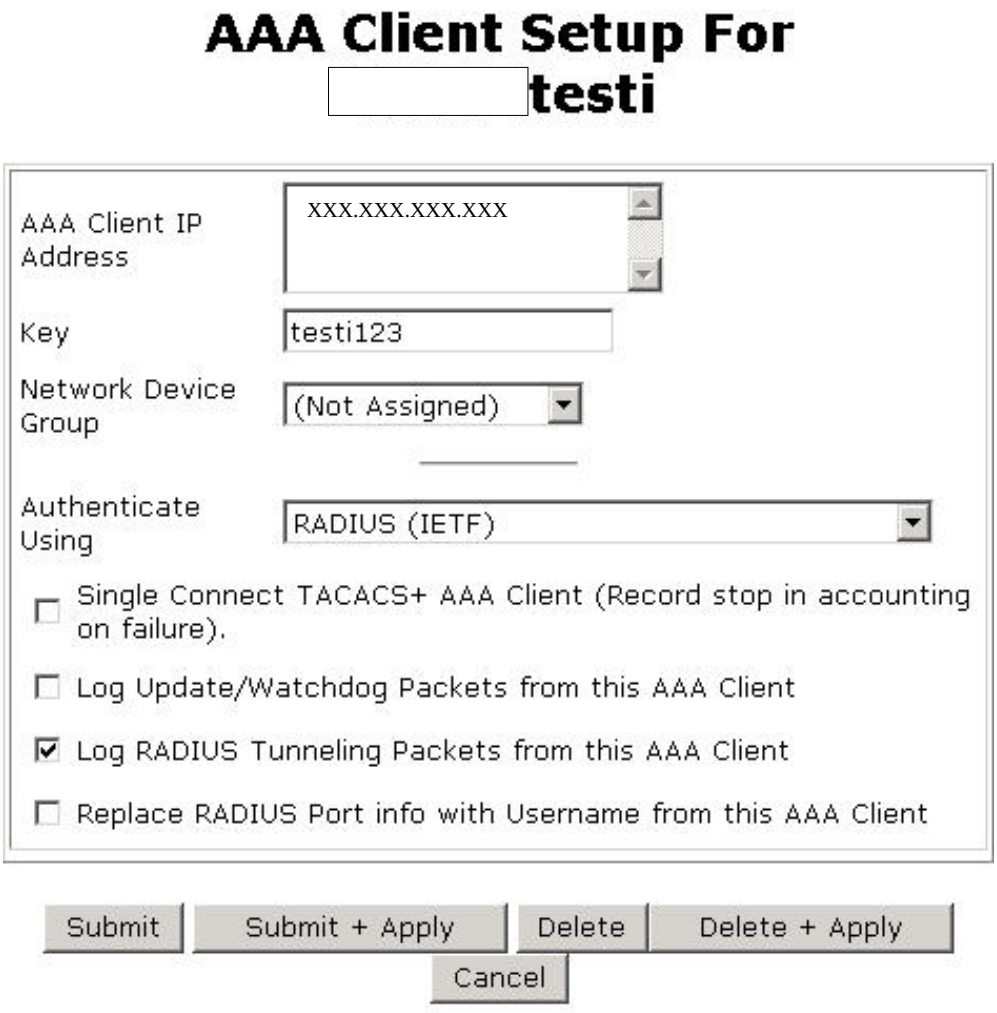


Kuva 31. ACS ryhmiin liittäminen

3.2 RADIUS

RADIUS-palvelimena työssä käytettiin Ciscon ACS-palvelinta. ACS:ltä luotiin aluksi uusi AAA-asiakas valitsemalla Network Configuration, AAA clients, Add Entry.

IP-osoitteeksi valitaan kytkimille tarkoitetusta IP-avaruudesta vapaa osoite, joka tässä tapauksessa on xxx.xxx.xxx.xxx. Avaimeksi keksitään esimerkiksi testi123. (Tämä pitää myös olla täysin sama kytkimellä, muuten yhteys ei toimi). Autentikointiin käytetään RADIUS (IETF) valintaa. Lisäksi aivan valinnaisena laitetaan ruksi kohtaan Log RADIUS Tunneling Packets from this AAA client. Tällöin saamme täydellisen lokin siitä, mitä palvelimen ja asiakkaan välillä tapahtuu. Oikeat asetukset ovat kuvassa 32.



Kuva 32. ACS RADIUS palvelimen asetukset

3.3 CISCO KYTKIN

Työn tekeminen aloitettiin vaihtamalla kaikki talossa sijaitsevat vanhat kerroskytkimet uusiin malleihin. Vanhat kerroskytkimet olivat sen verran vanhoja ja kyvyttömiä 802.1x autentikointia silmälläpitäen, että oli parempi samalla uusia ne. Uudet kytkimet ovat mallia Cisco XXXX.

Kytkimille tehtiin aluksi yksi perusasetus konfiguraatio, jossa oli mukana TACACS+:n vaatimat AAA-palvelut ja lisäksi paljon muuta, mikä on työn tekemiselle epäoleellista. Autentikointia varten kytkimelle laitettiin seuraavat asetukset:

```
hostname ABCDE_testi
!
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
dot1x system-auth-control
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan 502
 name testi_fail
!
vlan 501
 name testi_vieras
!
vlan 123
 name testi123
!
interface GigabitEthernet0/10
 description 802.1x
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x guest-vlan 501
 dot1x auth-fail vlan 1
!
radius-server host xxx.xx.xx.xxx auth-port 1645 acct-port 1646
radius-server source-ports 1645-1646
radius-server key 7 010703174F02575D72
```

aaa authentication dot1x default group radius

Kerrotaan kytkimelle, että käytetään 802.1x autentikointia ja että protokollana toimii RADIUS.

aaa authorization network default group radius

Kerrotaan kytkimelle että valtuutuksessa käytetään RADIUSta. Tämä mahdollistaa dynaamisen vlan määrityksen.

dot1x system-auth-control

Kerrotaan kytkimelle, että käytetään autentikoinnissa 802.1x:ää.

dot1x pae authenticator

Kytketään portissa 802.1x-autentikointi päälle perusasetuksilla.

dot1x port-control auto

Kytkee 802.1x-autentikoinnin päälle liitynnässä.

dot1x auth-fail vlan 502

Jos autentikointi epäonnistuu, portti siirtyy vlaniin 502.

dot1x guest-vlan 501

Määrittelee portin siirtymään vlaniin 501, jos käyttäjää ei tunnisteta.

radius-server host xxx.xx.xx.xxx auth-port 1645 acct-port 1646

Määritetään radius-palvelimen osoite ja autentikointiportti 1645 ja valtuutusportti 1646.

radius-server source-ports 1645-1646

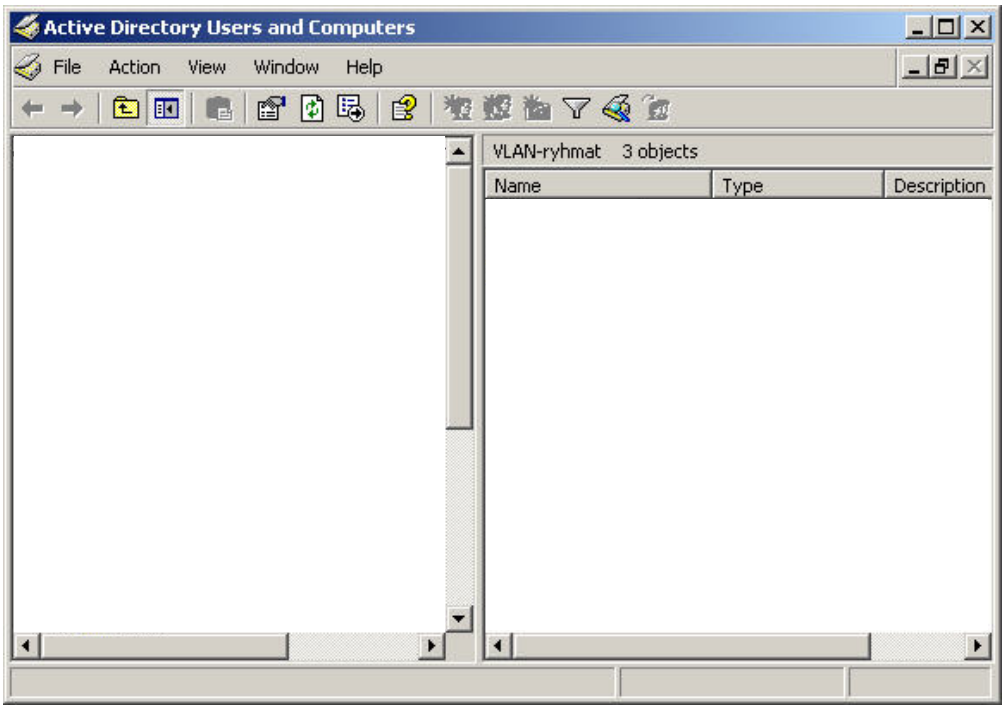
Portit joista radius-palvelin lähettää tiedot takaisin.

radius-server key 7 010703174F02575D72

Määritetään radius-avain. Avain näkyy salattuna, mutta ASCII-merkkeinä se on testi123.

3.4 AD

Windowsin aktiivihakemistoon AD:hen ei tarvittu kovin paljon muutosta. Testimielessä sinne tehtiin kaksi ryhmää, VLAN123 ja VLAN124. Näihin ryhmiin lisättiin pari käyttäjää sen mukaan, mihin vlaniin käyttäjän kone kuuluu. Käyttäjän haku olisi toiminut myös ilman näitä ryhmiä, mutta se selventää asiaa hieman.

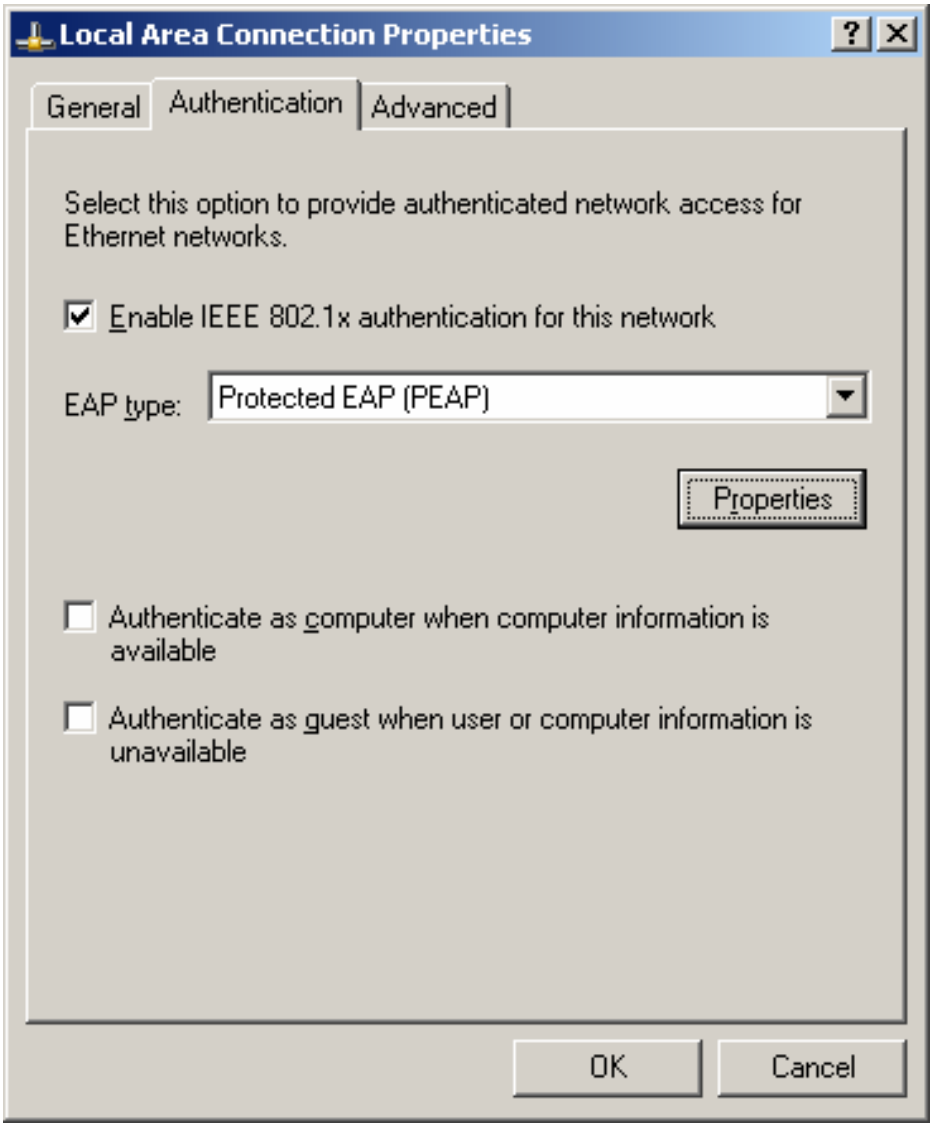


Kuva 33. AD ympäristöön tehdyt VLAN-ryhmät.

3.5 WINDOWS XP

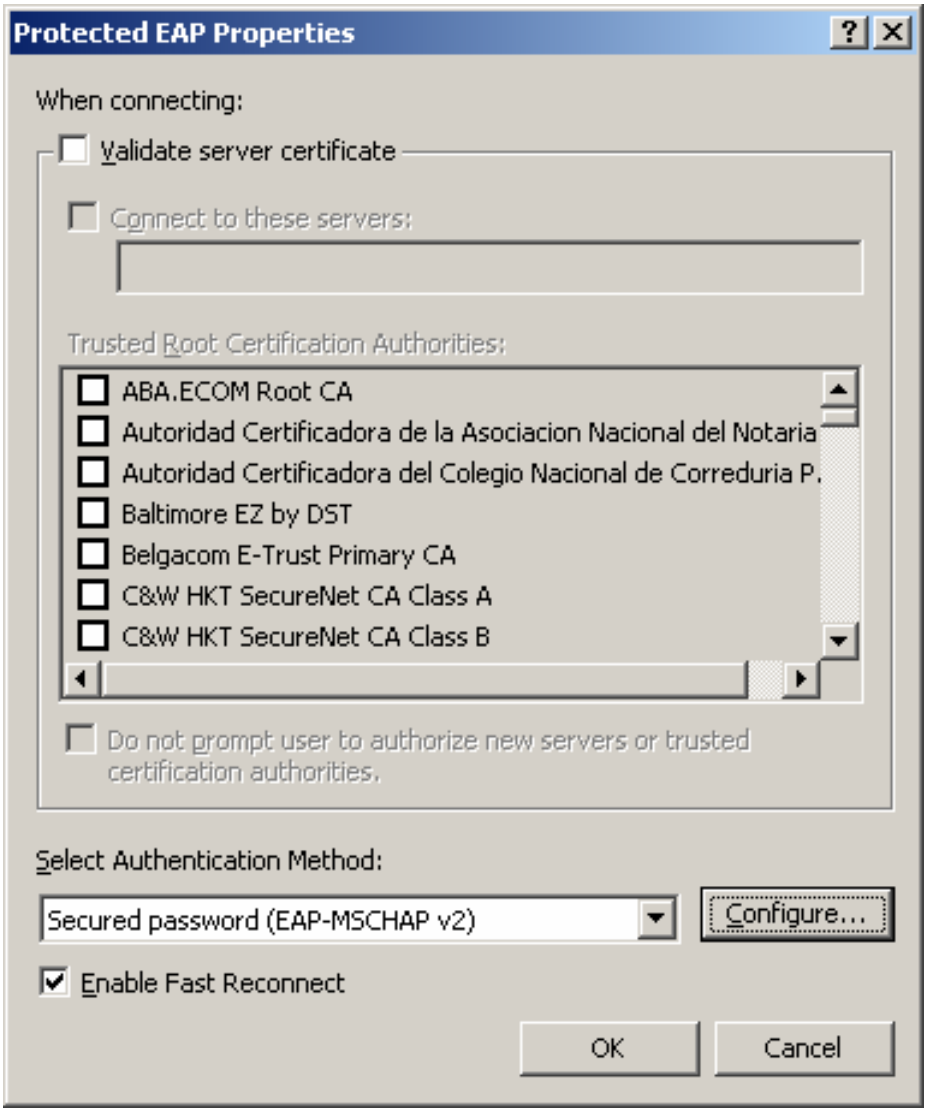
Yrityksessä käyttöjärjestelmänä käytetään lähestulkoon pelkästään Windows XP:tä. Koska windows XP:stä löytyy sisäänrakennettu tuki 802.1X-protokollalle, ei ylimääräisiä ohjelmia tarvita.

Asetukset Windows XP -ympäristössä laitetaan seuraavalla tavalla. Valitaan lähiverkkoyhteyksistä ominaisuudet. Laitetaan ruksi että käytetään 802.1X-autentikointia tässä verkossa. Valitaan oikea EAP tyyppi eli Protected EAP (PEAP). Lisäasetuksia varten valitaan vielä omaisuudet.



Kuva 34. Windows XP lähiverkkoyhteyden asetukset

Valitaan, että sertifikaattia ei tarkasteta. Laitetaan oikea autentikointi tapa EAP-MSCHAPv2. Laitetaan ruksi, jolla sallitaan nopea takaisin yhdistäminen. Valitaan vielä Configure -valinnan alta, että automaattisesti käytetään Windowsin käyttäjänimeä ja salasanaa.



Kuva 35. Windows XP lähiverkkoyhteyden lisäasetukset

4 TESTAUS

Seuraavaksi tarkastellaan, miten autentikointia voidaan analysoida. Analysoitavana on kolme eri lokia, kolmesta eri paikasta. Lokeja analysoidaan samalla tasolla, kuten ne on käyty teoriassa läpi. Lisäksi tutkitaan, mitä eri protokollat pitävät sisällä. Näiden lisäksi varmistetaan, että käytössä ovat halutut protokollat.

Onnistunut autentikointi toimia periaatteessa näin: Tietokoneeseen kirjaudutaan esimerkiksi tunnuksilla DOMAIN/TESTI. Laitetaan verkkokaapeli verkkorasiaan kiinni ja autentikointiprosessi alkaa. Tietokone lähettää käyttäjätunnukset kytkimelle EAP-MSCHAPv2:n avulla. Kytkin lähettää tunnukset RADIUS:n avulla ACS-palvelimelle, joka toimii myös AAA-palvelimena. AAA-palvelin kysyy käyttäjätunnuksia LDAP:n avulla Windows AD-tietokannasta. Jos tunnus löytyy, antaa AAA-palvelin kytkimelle luvan käyttää verkkoa. Luvan mukana AAA-palvelin kertoo, mihin vlaniin kytkin kyseisen portin laittaa. Tämän jälkeen verkko on käytettävissä.

Kaikkia liitteinä olevien lokien tapahtumia ei selitetä, eivätkä ne välttämättä esiinny liitteissä kokonaisina. Rivien eteen on lisätty rivinumerot, jotta selittämien kävisi helpommin.

Ensimmäiseksi tutkimme, että kytkimen autentikointi-asetukset ovat laitettu oikein. Tämän näemme kytkimestä show dot1x all -komennolla. Kuvassa 36 näkyvät asetukset. Kuvan mukaan autentikointi on käytössä vain portissa 10.

```
      testi#sh dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            2
Critical Recovery Delay         100
Critical EAPOL              Disabled

Dot1x Info for GigabitEthernet0/10
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Auth-Fail-Vlan            = 502
Auth-Fail-Max-attempts    = 3
Guest-Vlan                = 501
```

Kuva 36. Kytkimen show dot1x all-komento

4.1 Onnistunut autentikointi

Seuraavaksi voimme tutkia Liitettä 1, jossa näkyvät kytkimellä tapahtuvat autentikointitapahtumat. Nämä tapahtumat saadaan esiin komennolla debug dot1x all ja tämän jälkeen show logging.

Ensimmäisessä kohdassa Liitteessä 1 on onnistunut autentikointi. Riveillä 1-8 kytkin tekee alkuvalmistelut, jolloin se herättää portin, muuttaa sen ei-sallittuun tilaan ja näin estää portin liikenteen. Rivillä 9 aktivoidaan 802.1X portissa 10.

Riveillä 10-11 lähetetään ensimmäinen EAPOL-paketti. Tämä aloittaa EAP-keskustelun. Rivillä 12 ensimmäinen EAP-paketti saadaan takaisin. Riveillä 13 lähetetään EAP-pyyntö käyttäjästä. Rivillä 14 nähdään, että käytössä EAP, tapahtuma 6(eapolEap). Rivillä 15 tehdään EAP-pyyntö ja tapahtuma on 7(eapReq)

Rivillä 16-19 kerrotaan, että EAP-prosessi on onnistunut ja viesti on lähetetty myös käyttäjälle. Tämä näkyy rivillä 18 tapahtumasta 11(eapSuccess). Rivillä 20-24 määritellään porttiin RADIUS:lta saatu vlan. Portin määritystapahtuma on 12(authSuccess_portValid). Riveillä 25-28 ilmoitetaan käyttäjälle, että autentikointi on onnistunut. Tapahtuma on 22(authcSuccess). Riveillä 29-33 kerrotaan, että onnistunut autentikointi on tapahtunut. Tapahtuma on 25(authzSuccess).

Onnistuneen autentikoinnin tapahtuessa, Windows XP kertoo nopeasti autentikoinnin onnistuneen ja rupeaa hakemaan DHCPltä osoitetta. ACSltä onnistuneen autentikoinnin näkee valitsemalla päävalikosta Reports and Activity ja Passed Authentications. Kuvassa 37 näkyy millaiselta se näyttää. Lokista näkee kuka on autentikoitunut, mihin vlaniin käyttäjä on sijoitettu, käyttäjän MAC-osoite, kytkimen IP-osoite, AAA-palvelin ja käytetty autentikointityyppi. Kuten loki kertoo, että protokolla on MS-PEAP.

02/04/2007	13:02:40	Authen OK	DOMAIN/TESTI	VLAN412	AA-BB-CC-DD-EE-FF	
50010	XXX.XXX.XXX.XX	acstesti	..	25	MS-PEAP	

Kuva 37. Onnistunut autentikointi ACS Passed authentications

Onnistunutta autentikointia pystytään analysoimaan myös ACS palvelimelta Auth.log:sta. Lokista näkee kaikki palvelimella tapahtuvat autentikointiin liittyvät tapahtumat. Liitteenä 2 on ote Auth.log:sta. Riviltä 3 löytyy käyttäjänimi. Rivillä 6 on sen palvelimen MAC-osoite, johin on otettu yhteys ja rivillä 7 yhteyttä ottavan palvelimen MAC-osoite. Riviltä 8 löytyy EAP-viesti. Riveillä 10-13 on reunapalvelimen tietoja. Rivillä 22 ja 23 yritetään autentikoida käyttäjää DOMAIN/TESTI. Riveillä 28-32 ilmoitetaan, että käyttäjää ei löydy, haetaan tieto ulkoisesta tietokannasta. Rivillä 33 sidotaan käyttäjä oikeaan ryhmään. ACSään on tehty määritys, jonka mukaan DOMAIN/TESTI kuluu ryhmään 2 eli VLAN123. Rivillä 42 ilmoitetaan että autentikointi on onnistunut. Rivillä 43-48 muodostetaan ACS käyttäjätili DOMAIN/TESTI. ACSltä saa tehtyä valinnan käytetäänkö tulevaisuudessa tätä varastoitua profiilia vai haetaanko ulkoisesta tietokannasta joka kerta tili uudelleen.

Liitteessä 4 on ote ACSn RDS.log:sta. Siitä käy selville paljon samoja asioita kuten Auth.log:sta, esimerkiksi riveillä 2-11 olevat käyttäjän- ja laitteistontiedot.

Liitteenä 3 on ACS-palvelimen ja ADn väliseltä muurilta otettu keskustelu. Tässä keskustelussa ACS-palvelin pyytää ADlta kirjautuneen käyttäjän tietoja ja AD vastaa antamalla tiedot. Vaikka LDAPin pitäisi käyttää pelkästään porttia 389, on näkyvissä paljon muitakin portteja. Nämä kaikki portit ovat UDP portteja. Muiden porttien käyttö perustuu siihen että ACSstä ei ole valittu pelkästään LDAP haku, vaan Microsoft Database. Tällöin ei käytetä puhdasta LDAP hakua. Palomuurin lokin keskustelu alkaa rivillä, jonka kohdeosoitteen perässä on iso S-kirjain. Keskustelu lopetetaan vaihtamalla S-kirjain F-kirjaimen. Kaikki näiden välinen viestien vaihto liittyy dataan.

4.2 Epäonnistunut autentikointi

Tässä luvussa kerrotaan ja esitetään pari virhettä, joista epäonnistunut autentikointi voi johtua. Ensimmäisenä voidaan ottaa ongelma, joka liittyy toimialueeseen. Jos ACS-palvelin ei kuulu sille toimialueelle, jonka käyttäjiä halutaan tunnistaa, autentikointi ei toimi. Tällöin ACS-palvelin on saatava osaksi kyseistä toimialuetta, Domain Member Server riittää.

Toiseksi Active Directoryssä on oltava ACS-palvelimelle konetili. Tämän pystyy tekemään liittämällä palvelin toimialueeseen. Jos konetiliä ei löydy, au-

tentikointi ei onnistu. Näiden lisäksi Active Directoryyn on oltava määriteltynä millä tunnuksilla LDAP-hakuja saa tehdä. Jos määritykset ovat tiukat ja hakuja saa tehdä pelkästään toimialueen järjestelmän valvoja-tunnuksilla, ACS-palvelimen palveluiden on pyörittävä toimialueen järjestelmän valvojan-tunnuksilla. Jos AD:ssa on määritelty että hakuja saa tehdä millä tahansa tunnuksella, voivat ACS-palvelimen palvelut pyöriä paikallisilla järjestelmän valvojan-tunnuksilla.

Yhtenä ongelmana on sertifikaattien käyttö. Käytettävä PEAP-protokolla tarvitsee toimiakseen sertifikaatin. Tämä pitää muistaa antaa ACS-palvelimelle ennen testien aloittamista, muuten autentikointi ei onnistu. Käytettäessä EAP-MD5-protokollaa sertifikaattia ei tarvitse. Tällöin ongelmaksi tulee käyttäjien haku ADn kannasta. AD ei nimittäin ymmärrä MD5-protokollaa. EAP-TLS autentikointi vaatii toimiakseen sertifikaatin kummallekin osapuolelle, sekä ACS-palvelimelle että asiakkaalle. Tässä tapauksessa on hyvä käyttää yhteistä sertifikaattipalvelua, joka myöntää kummallekin omat sertifikaatit.

Epäonnistuneeseen autentikointiin voi olla erittäin paljon muitakin syitä. Syyt voivat johtua 802.1X tuen puutteesta asiakkaan päässä. Ne voivat johtua asetusten virheellisistä määrittelyistä kytkimellä, AAA-palvelimella, ACS-palvelimella, AD-ympäristössä tai jossain näiden välisessä tiedonsiirrossa. Epäonnistuneen autentikoinnin tapahtuessa on hyvä osata lukea lokeja, joista saa paljon apua vaikeiden ongelmien ratkomiseen.

Seuraavana Liitteessä 1 on epäonnistunut autentikointi. Läpi käydään ainostaan tapa, jolla epäonnistuminen ilmaistaan. Seuraavat lokin rivit tulevat vasta siinä vaiheessa kun onnistuneen autentikoinnin kohdalla tuli autentikointi onnistunut. Rivillä 1 saadaan EAP epäonnistuminen ja rivillä 2 sanotaan syyksi että AAA-palvelimelta ei saatu tarvittavia attribuutteja. Riveillä 4-12 ilmoitetaan että autentikointi ei ole hyväksytty ja sama viesti välitetään Windows XP käyttäjälle. Riveillä 13-15 portti siirretään takaisin ei-sallittuun tilaan.

4.3 Muuta autentikoinnista

Joskus autentikointi ei mene läpi ensimmäisellä kerralla, vaan joudutaan kokeilemaan sitä toistamiseen. Kytkimelle voidaan määrittää, että autentikointi yrityksiä on tietty määrä. On myös hyvä tietää mitä tapahtuu kun tietokone otetaan pois verkosta.

Autentikoinnin uusiminen

Jos autentikointi ei mene läpi ensimmäisellä kerralla, voi kytkimelle laittaa komennon, joka käynnistää autentikoitumisprosessin uudestaan. Liitteessä 1 autentikoinnin uusimisen alla, on ote kytkimen lokista, kun autentikointi ei ole mennyt läpi. Tällöin käyttäjä lähettää RESTART-viestin ja autentikointiprosessi alkaa uudestaan, tapahtuma 13(restart). Lokissa on kuvattu vain se osa autentikoitumisesta, joka käsittelee uudelleen autentikoinnin aloittamista. Tämän jälkeen palataan taas onnistuneen autentikoinnin rytmiin ja pyydetään autentikointia tapahtumalla 7(eapReq).

Autentikoinnin päättyminen

Liitteessä 1, kohdassa autentikoinnin päättyminen, kuvataan mitä käy kun kone otetaan pois verkosta. Rivillä 1 verkkoportin linkki muuttuu. Riveillä 2-6 ja 8-11 poistetaan kaikki käyttäjää koskevat tiedot ja rivillä 7 portti laitetaan takaisin ei-sallittuun-tilaan. Ja rivillä 12 verkkoportti menee kokonaan pois päältä.

5 YHTEENVETO

Tämän insinöörityön tarkoitus oli tutkia mitä 802.1X-autentikointi tarkoittaa ja mitä sen käyttöönotto vaatii. Taustatietoja tarvittiin eri komponenttien toiminnasta ja miten ne keskustelevat keskenään. Työn alussa tutustuttiin 802.1X-terminologiaan ja -arkkitehtuurin sekä selvitettiin protokollan toiminta ja käytöstä saatavat hyödyt. Tämän jälkeen keskityttiin mitä EAP-protokolla tarkoittaa, miten se toimii ja mitä eri muotoja sillä on. Seuraavaksi perehdyttiin AAA-palvelimien ja AAA-protokollien toimintaan. Työssä tutustuttiin myös Ciscon kytkimissä olevaan IOS-käyttöjärjestelmään sekä Ciscon ACS-järjestelmään. Cisco ACS:llä oli tässä työssä suuri osa, koska se toimi myös samalla AAA-palvelimena. Lisäksi luotiin nopea vilkaisu Active Directory-järjestelmään sekä LDAP:iin.

Kun taustietojen keräys oli suoritettu ja niihin oli perehdytty kunnolla, oli aika viedä teoria käytäntöön ja tehdä 802.1X-autentikointi mahdolliseksi käyttäen jo olemassa olevia resursseja. Työssä käydään yksityiskohtaisesti läpi mitä asetuksia 802.1X-autentikointi vaatii ACS-palvelimella, Ciscon kytkimillä, Microsoft AD:lla ja Windows XP:ssä. Nämä ohjeet jäävät työn jälkeen myös työntekopaikalle, jotta työ pystytään tarpeen mukaan uusimaan ilman suurta vaivaa. Lopuksi käydään läpi miltä onnistunut ja epäonnistunut autentikointi näyttää lokien perusteella ja esitetään yleisimpiä syitä miksi autentikointi ei toimi.

Työn tavoitteena ollut 802.1X-autentikointi toimistoverkossa saatiin toimimaan, kuten haluttiinkin. Käytössä on siis porttikohtainen autentikointi käyttäjän tunnuksilla. Tällä pyritään estämään asiattomien koneiden liittäminen yrityksen lankaverkkoon. Tämän on tarkoitus parantaa turvallisuutta ja helpottaa verkonhoitajien työtaakkaa. Lisäksi 802.1X-autentikoituminen helpottaa työntekijöiden työntekoa, kun tietokoneen voi laitaa verkkoon missä tahansa talossa ja kone on heti käytössä omassa aliverkossa.

Työn valmiiksi saamisella oli kiire työnantajankin puolesta, koska 802.1X-autentikointi oli tarkoitus ottaa vakituiseen käyttöön. Työ oli ollut erittäin opettavainen erilaisten autentikointi tapojen suhteen. Tämän lisäksi kaikki työn ohessa tullut tieto on ollut erittäin palkitsevaa. Itsessään autentikointi-ratkaisun suunnittelu ja rakentaminen sekä sen testaaminen ja käyttöönotto on ollut erittäin mielenkiintoista. Onnistuneen autentikointi-ratkaisun saami-

nen toimintaan näinkin suuressa ja monimutkaisessa ympäristössä on omasta mielestäni erittäin hieno asia. Samoilla asetuksilla autentikoinnin toimintaan saaminen eri ympäristössä voi olla vaikeaa, mutta pienellä hienosäädöllä sen pitäisi olla mahdollista.

Tulevaisuudessa samaan 802.1X-autentikointiin voisi liittää nykyisin käytössä oleva WLAN-autentikointi. Nykyään autentikointi hoidetaan käyttämällä LEAPia ja hakemalla käyttäjän tiedot ACS:n paikallisesta tietokannasta. Tämä systeemi voitaisiin helposti vaihtaa 802.1X-autentikointiin, käyttämällä MSCHAPv2:ia ja autentikoimaan käyttäjät AD:n tietokannasta.

VIITELUETTELO

[1] Fisher, Arthur, Authentication and Authorization: The Big Picture with IEEE 802.1X. [verkkojulkaisu, viitattu 9.4.2007]. Saatavissa http://www.sans.org/reading_room/whitepapers/authentication/123.php.

[2] Kwan Philip, WHITE PAPER: 802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP) [verkkojulkaisu, viitattu 9.4.2007]. Saatavissa http://www.foundrynet.com/pdf/wp-8021x-authentication-eap.pdf.

[3] Cisco Documentation, Configuring 802.1X Port-Based Authentication [verkkojulkaisu, viitattu 9.4.2007]. Saatavissa http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_2_31s/conf/dot1x.htm.

[4] Strand, Lars, 802.1X Port-Based Authentication HOWTO [verkkojulkaisu, viitattu 9.4.2007]. Saatavissa http://tldp.org/HOWTO/8021X-HOWTO/intro.html#what8021x.

[5] Cisco Documentation, User Guide for Cisco Secure ACS for Windows Server [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://www.cisco.com/application/pdf/en/us/guest/products/ps2086/c2001/ccmigration_09186a0080314477.pdf.

[6] Wikipedia, AAA_protocol [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://en.wikipedia.org/wiki/AAA_protocol.

[7] Cisco Documentation, How Does RADIUS Work? [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://www.cisco.com/warp/public/707/32.html.

[8] Symantec Documentation, Overview of the RADIUS authentication protocol [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://entkb.symantec.com/security/output/n2004041309223454.html.

[9] Wikipedia, RADIUS [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://en.wikipedia.org/wiki/RADIUS.

[10] Hill, Joshua, An Analysis of the RADIUS Authentication Protocol [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://www.untruth.org/~josh/security/radius/radius-auth.html.

[11] Juniper Networks, [verkkodokumentti, viitattu 9.4.2007] . Saatavissa http://www.juniper.net/techpubs/software/erx/junose53/swconfig-broadband/html/tacacs-config2.html.

[12] Cisco Documentation, Single-User Network Access Security TACACS+ [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://www.cisco.com/warp/public/614/7.html.

[14] Peking University, Network Access Servers [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://www.pku.edu.cn/academic/research/computer-center/tc/html/TC0202.html.

[15] Cisco Documentation, Overview of Cisco Secure ACS [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs31/acsuser/o.htm.

[16] Wikipedia, Cisco IOS [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://en.wikipedia.org/wiki/Cisco_IOS.

[17] Cisco Documentation, White Paper: Cisco IOS Reference Guide [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml.

[18] Cisco Documentation, Cisco Secure Access Control Server for Windows [verkkodokumentti, viitattu 10.4.2007]. Saatavissa http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html.

[19] Cisco Documentation, Cisco Secure Access Control Server (ACS) v3.0 [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://www.cisco.com/application/pdf/en/us/guest/products/ps2086/c1161/ccmigration_09186a0080159f3f.pdf.

[20] Wikipedia, Active Directory [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://en.wikipedia.org/wiki/Active_Directory.

[21] Wikipedia, Lightweight Directory Access Protocol [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol.

[22] Microsoft Online Documentation, RADIUS Authentication and Accounting [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://msdn2.microsoft.com/en-us/library/ms688418.aspx.

[23] Kirjoittaja tuntematon, [Kreikankielinen verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://www.epmhs.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/kefalaio5.htm.

[24] Cisco Documentation, ACS Documentation [verkkodokumentti, viitattu 9.4.2007]. Saatavissa http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs32/user02/o.htm.

OTTEITA KYTKIMEN AUTENTIKOINTITAPAHTUMISTA:

ONNISTUNUT AUTENTIKOINTI

1 Apr 11 09:30:50: dot1x-ev:dot1x_switch_is_dot1x_forwarding_enabled: Forwarding is disabled on Gi0/10
2 Apr 11 09:30:50: dot1x-registry:dot1x_switch_port_linkcomingup invoked on interface Gi0/10
3 Apr 11 09:30:50: dot1x-ev:dot1x_mgr_if_state_change: GigabitEthernet0/10 has changed to UP
4 Apr 11 09:30:50: dot1x_auth Gi0: initial state auth_initialize has enter
7 Apr 11 09:30:50: dot1x-ev:Sending create new context event to EAP for 0000.0000.0000
8 Apr 11 09:30:50: dot1x-ev:Created a default authenticator instance on GigabitEthernet0/10
9 Apr 11 09:30:50: dot1x-ev:dot1x_switch_enable_on_port: Enabling dot1x on interface GigabitEthernet0/10

10 Apr 11 09:30:51: dot1x-ev:GigabitEthernet0/10:Sending EAPOL packet to group PAE address

11 Apr 11 09:30:51: dot1x-ev:dot1x_mgr_send_eapol: Sending out EAPOL packet on GigabitEthernet0/10

12 Apr 11 09:30:51: dot1x-packet:Received an EAP request packet from EAP for mac 0008.02d5.c547
13 Apr 11 09:30:51: dot1x-sm:Posting EAP_REQ on Client=1937558
14 Apr 11 09:30:51: dot1x_auth_bend Gi0: during state auth_bend_request, got event 6(eapolEap)
15 Apr 11 09:30:51: dot1x_auth_bend Gi0: during state auth_bend_response, got event 7(eapReq)

16 Apr 11 09:30:58: dot1x-packet:Received an EAP Success on the GigabitEthernet0/10 for mac 0008.02d5.c547
17 Apr 11 09:30:58: dot1x-sm:Posting EAP_SUCCESS on Client=1937558
18 Apr 11 09:30:58: dot1x_auth_bend Gi0: during state auth_bend_response, got event 11(eapSuccess)
19 Apr 11 09:30:58: dot1x-sm:Posting AUTH_SUCCESS on Client=1937558

20 Apr 11 09:30:58: dot1x_auth Gi0: during state auth_authenticating, got event 12(authSuccess_portValid)
21 Apr 11 09:30:58: dot1x-ev:dot1x_vlan_assign_authc_success called on interface GigabitEthernet0/10
22 Apr 11 09:30:58: dot1x-ev:RADIUS provided VLAN name 123 to interface GigabitEthernet0/10
23 Apr 11 09:30:58: dot1x-ev:dot1x_switch_pm_port_set_vlan: Setting vlan 412 on interface GigabitEthernet0/10
24 Apr 11 09:30:58: dot1x-ev:Successfully assigned VLAN 123 to interface GigabitEthernet0/10

25 Apr 11 09:30:58: dot1x-sm:Posting AUTHC_SUCCESS on Client=1937558
26 Apr 11 09:30:58: dot1x_auth Gi0: during state auth_authc_result, got event 22(authcSuccess)
27 Apr 11 09:30:58: @@@ dot1x_auth Gi0: auth_authc_result -> auth_authz_success
28 Apr 11 09:30:58: dot1x-sm:Gi0/10:0008.02d5.c547:auth_authz_success_enter called
29 Apr 11 09:30:58: dot1x-ev:dot1x_switch_port_authorized: set dot1x ask handler on interface GigabitEthernet0/10
30 Apr 11 09:30:58: dot1x-ev:Received successful Authz complete for 0008.02d5.c547
31 Apr 11 09:30:58: dot1x-sm:Posting AUTHZ_SUCCESS on Client=1937558
32 Apr 11 09:30:58: dot1x_auth Gi0: during state auth_authz_success, got event 25(authzSuccess)
33 Apr 11 09:30:58: @@@ dot1x_auth Gi0: auth_authz_success -> auth_authenticated

EPÄONNISTUNUT AUTENTIKOINTI

1 Apr 11 09:30:57: dot1x-ev:Received an EAP Fail on GigabitEthernet0/10 for mac 0008.02d5.c547
2 Apr 11 09:30:57: dot1x-ev:No reply attributes received from AAA for 0008.02d5.c547
3 Apr 11 09:30:57: dot1x-sm:Posting EAP_FAIL on Client=1937558
4 Apr 11 09:30:57: dot1x_auth_bend Gi0: during state auth_bend_response, got event 10(eapFail)

5 Apr 11 09:30:57: dot1x_auth Gi0: during state auth_authenticating, got event 15(authFail)
6 Apr 11 09:30:57: @@@ dot1x_auth Gi0: auth_authenticating -> auth_authc_result
7 Apr 11 09:30:57: dot1x-sm:Gi0/10:0008.02d5.c547:auth_authenticating_exit called
8 Apr 11 09:30:57: dot1x-sm:Gi0/10:0008.02d5.c547:auth_authc_result_enter called
9 Apr 11 09:30:57: dot1x-ev:dot1x_auth_fail_authc_fail: Handling authentication failure on port GigabitEthernet0/10
10 Apr 11 09:30:57: dot1x-ev:dot1x_auth_fail_authc_fail: Ignoring - authentication attempts 1 <= max 3
11 Apr 11 09:30:57: dot1x-sm:Posting AUTHC_FAIL on Client=1937558
12 Apr 11 09:30:57: dot1x_auth Gi0: during state auth_authc_result, got event 23(authcFail)
13 Apr 11 09:30:57: dot1x-ev:dot1x_switch_port_unauthorized: Unauthorizing interface GigabitEthernet0/10
14 Apr 11 09:30:57: dot1x-ev:dot1x_switch_is_dot1x_forwarding_enabled: Forwarding is disabled on Gi0/10
15 Apr 11 09:30:57: dot1x-ev:dot1x_vlan_assign_authz_fail on interface GigabitEthernet0/10

AUTENTIKOINNIN UUSIMINEN

1 Apr 11 09:30:57: dot1x-sm:Posting RESTART on Client=1937558
2 Apr 11 09:30:57: dot1x_auth Gi0: during state auth_held, got event 13(restart)
3 Apr 11 09:30:57: @@@ dot1x_auth Gi0: auth_held -> auth_restart
4 Apr 11 09:30:57: dot1x-sm:Gi0/10:0008.02d5.c547:auth_held_exit called
5 Apr 11 09:30:57: dot1x-sm:Gi0/10:0008.02d5.c547:auth_restart_enter called
6 Apr 11 09:30:57: dot1x-ev:Resetting the client 0008.02d5.c547
7 Apr 11 09:30:57: dot1x-sm:Posting !EAP_RESTART on Client=1937558
8 Apr 11 09:30:57: dot1x_auth Gi0: during state auth_restart, got event 6(no_eapRestart)
9 Apr 11 09:30:57: @@@ dot1x_auth Gi0: auth_restart -> auth_connecting
10 Apr 11 09:30:57: dot1x-sm:Gi0/10:0008.02d5.c547:auth_connecting_enter called
11 Apr 11 09:30:57: dot1x-sm:Gi0/10:0008.02d5.c547:auth_restart_connecting_action called
12 Apr 11 09:30:58: dot1x-packet:Received an EAP request packet from EAP for mac 0008.02d5.c547
13 Apr 11 09:30:58: dot1x-sm:Posting RX_REQ on Client=1937558
14 Apr 11 09:30:58: dot1x_auth Gi0: during state auth_connecting, got event 10(eapReq_no_reAuthMax)
15 Apr 11 09:30:58: @@@ dot1x_auth Gi0: auth_connecting -> auth_authenticating
16 Apr 11 09:30:58: dot1x-sm:Gi0/10:0008.02d5.c547:auth_authenticating_enter called
17 Apr 11 09:30:58: dot1x-sm:Gi0/10:0008.02d5.c547:auth_connecting_authenticating_action called
18 Apr 11 09:30:58: dot1x-sm:Posting AUTH_START on Client=1937558
19 Apr 11 09:30:58: dot1x_auth_bend Gi0: during state auth_bend_idle, got event 4(eapReq_authStart
20 Apr 11 09:30:58: @@@ dot1x_auth_bend Gi0: auth_bend_idle -> auth_bend_request

AUTENTIKOINNIN PÄÄTTYMINEN

1 Apr 11 09:30:59: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/10, changed state to up
2 Apr 11 09:31:14: dot1x-registry:** dot1x_switch_vp_statechange:
3 Apr 11 09:31:14: dot1x-ev:vlan 123 vp is removed on the interface GigabitEthernet0/10
4 Apr 11 09:31:14: dot1x-registry:dot1x_switch_pm_handle_vlan_removal invoked oninterface GigabitEthernet0/10 removed_vlan= 123
5 Apr 11 09:31:14: dot1x-ev:Deleted all Authenticator clients on GigabitEthernet0/10
6 Apr 11 09:31:14: dot1x-registry:dot1x_switch_port_physical_linkchange invoked on interface Gi0/10
7 Apr 11 09:31:14: dot1x-ev:dot1x_switch_port_unauthorized: Unauthorizing interface GigabitEthernet0/10
8 Apr 11 09:31:14: dot1x-ev:dot1x_switch_pm_port_set_vlan: Setting vlan 0 on interface GigabitEthernet0/10
9 Apr 11 09:31:14: dot1x-ev:dot1x_switch_is_dot1x_forwarding_enabled: Forwarding is disabled on Gi0/10
10 Apr 11 09:31:14: dot1x-ev:dot1x_switch_addr_remove: Removed MAC 0008.02d5.c547 from vlan 412 on interface GigabitEthernet0/10
11 Apr 11 09:31:14: dot1x-ev:dot1x_vlan_assign_client_deleted on interface GigabitEthernet0/10
12 Apr 11 09:31:14: dot1x-ev:dot1x_mgr_if_state_change: GigabitEthernet0/10 has changed to DOWN

OTE ACS AUTH.LOG:N ONNISTUNEESTA AUTENTIKOINNISTA:

1 AUTH 01/04/2007 23:45:38 I 5081 0492 Start RQ1152, client 2 (127.0.0.1)
2 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PolicyMgr::CreateContext: new context id=1
3 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: User-Name=DOMAIN\testi
4 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: Service-Type=2
5 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: Framed-MTU=1500
6 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: Called-Station-Id=00-18-BA-57-2A-8A
7 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: Calling-Station-Id=00-08-02-D5-C5-47
8 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: EAP-Message=(binary value)
9 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: Message-Authenticator=(binary value)
10 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: NAS-Port=50010
11 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: NAS-Port-Type=15
12 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: NAS-IP-Address=10.166.6.80
13 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: PDE-NAS-Vendor-14=0
14 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PdeAttributeSet::addAttribute: PDE-Service-ID-0=0
15 AUTH 01/04/2007 23:45:38 I 0143 0492 [PDE]: PolicyMgr::SelectService: context id=1; no profile was matched - using default (0)
16 AUTH 01/04/2007 23:45:38 I 5081 0492 Done RQ1152, client 2, status 0
17 AUTH 01/04/2007 23:45:38 E 5103 3852 AllocateThread returned 5
18 AUTH 01/04/2007 23:45:38 S 5100 3852 Listening for new TCP connection ----------
19 AUTH 01/04/2007 23:45:38 A 5086 3504 Worker 5 established conn 6 with 127.0.0.1:3147
20 AUTH 01/04/2007 23:45:38 I 5094 3504 Worker 5 processing message 1.
21 AUTH 01/04/2007 23:45:38 I 5081 3504 Start RQ1026, client 50 (127.0.0.1)
22 AUTH 01/04/2007 23:45:38 I 5397 3504 Attempting authentication for Unknown User 'DOMAIN\testi'
23 AUTH 01/04/2007 23:45:38 I 1554 3504 pvAuthenticateUser: authenticate 'DOMAIN\testi' against CSDB
24 AUTH 01/04/2007 23:45:38 I 5081 3504 Done RQ1026, client 50, status -2046
25 AUTH 01/04/2007 23:45:39 I 5094 3504 Worker 5 processing message 2.
26 AUTH 01/04/2007 23:45:39 I 5081 3504 Start RQ1027, client 50 (127.0.0.1)
27 AUTH 01/04/2007 23:45:39 I 0897 3504 AuthenProcessResponse: process response for 'DOMAIN\testi'
28 AUTH 01/04/2007 23:45:39 I 1554 3504 pvAuthenticateUser: authenticate 'DOMAIN\testi' against CSDB
29 AUTH 01/04/2007 23:45:39 I 1554 3504 pvAuthenticateUser: authenticate 'DOMAIN\testi' against Windows Database
30 AUTH 01/04/2007 23:45:39 I 0376 3504 External DB [NTAuthenDLL.dll]: Starting MSCHAP authentication for user [DOMAIN\testi]
31 AUTH 01/04/2007 23:45:39 I 0376 3504 External DB [NTAuthenDLL.dll]: Attempting Windows authentication for user testi
32 AUTH 01/04/2007 23:45:39 I 0376 3504 External DB [NTAuthenDLL.dll]: Windows authentication SUCCESSFUL (by DOMAIN-CONTROLLER)
33 AUTH 01/04/2007 23:45:39 I 0376 3504 External DB [NTAuthenDLL.dll]: User mapped to ACS group id [2]
34 AUTH 01/04/2007 23:45:39 I 5081 3504 Done RQ1027, client 50, status -2046

35 AUTH 01/04/2007 23:45:39 I 5094 3504 Worker 5 processing message 7.
36 AUTH 01/04/2007 23:45:39 I 5081 3504 Start RQ1027, client 50 (127.0.0.1)
37 AUTH 01/04/2007 23:45:39 I 0897 3504 AuthenProcessResponse: process response for 'DOMAIN\testi'
38 AUTH 01/04/2007 23:45:39 I 5081 3504 Done RQ1027, client 50, status -2046
39 AUTH 01/04/2007 23:45:39 I 5094 3504 Worker 5 processing message 8.
40 AUTH 01/04/2007 23:45:39 I 5081 3504 Start RQ1027, client 50 (127.0.0.1)
41 AUTH 01/04/2007 23:45:39 I 0897 3504 AuthenProcessResponse: process response for 'DOMAIN\testi'
42 AUTH 01/04/2007 23:45:39 I 0361 3504 EAP: PEAP: Second phase: 26 authentication finished SUCCESSFULLY
43 AUTH 01/04/2007 23:45:39 I 1329 3504 User DOMAIN\testi account created
44 AUTH 01/04/2007 23:45:39 I 4372 3504 User DOMAIN\testi password type changed
45 AUTH 01/04/2007 23:45:39 I 4327 3504 User DOMAIN\testi enable password type changed
46 AUTH 01/04/2007 23:45:39 I 2830 3504 New external User ' DOMAIN\testi ' has had enable flag set to 100
47 AUTH 01/04/2007 23:45:39 I 2127 3504 User DOMAIN\testi feature flags changed
48 AUTH 01/04/2007 23:45:39 I 2127 3504 User DOMAIN\testi feature flags changed
49 AUTH 01/04/2007 23:45:39 I 0143 3504 [PDE]: PdeAttributeSet::addAttribute: PDE-Group-ID-16=2
50 AUTH 01/04/2007 23:45:39 I 0143 3504 [PDE]: PolicyMgr::Process: request type=4; context id=1; applied default profiles (0) - do nothing
51 AUTH 01/04/2007 23:45:39 I 5081 3504 Done RQ1027, client 50, status 0

OTE ACS PALVELIMEN JA AD:N VÄLISESTÄ KESKUSTELUSTA:

SALAINEN

OTE ACS RADIUS RDS.LOG:N ONNISTUNEESTA AUTENTIKOINNISTA:

1 RDS 01/04/2007 23:45:38 D 0245 2768 Request from host 10.166.6.80:1645 code=1, id=126, length=139 on port 1645
2 RDS 01/04/2007 23:45:38 I 2999 2768 [001] User-Name value: DO-MAIN\testi
3 RDS 01/04/2007 23:45:38 I 3017 2768 [006] Service-Type value: 2
4 RDS 01/04/2007 23:45:38 I 3017 2768 [012] Framed-MTU value: 1500
5 RDS 01/04/2007 23:45:38 I 2999 2768 [030] Called-Station-Id value: 00-18-BA-57-2A-8A
6 RDS 01/04/2007 23:45:38 I 2999 2768 [031] Calling-Station-Id value: 00-08-02-D5-C5-47
7 RDS 01/04/2007 23:45:38 I 2999 2768 [079] EAP-Message value: ..... DO-MAIN\testi
8 RDS 01/04/2007 23:45:38 I 2999 2768 [080] Message-Authenticator value: 17 53 BA D9 66 37 04 77 05 FD 70 BC 23 26 4B 98
9 RDS 01/04/2007 23:45:38 I 3017 2768 [005] NAS-Port value: 50010
10 RDS 01/04/2007 23:45:38 I 3017 2768 [061] NAS-Port-Type value: 15
11 RDS 01/04/2007 23:45:38 I 3042 2768 [004] NAS-IP-Address value: 10.166.6.80
12 RDS 01/04/2007 23:45:38 I 0299 2768 ExtensionPoint: Initiating scan of configured extension points...
13 RDS 01/04/2007 23:45:38 I 0331 2768 ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
14 RDS 01/04/2007 23:45:38 I 0336 2768 ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [11 - challenge]
15 RDS 01/04/2007 23:45:38 I 0366 2768 ExtensionPoint: Start of Attribute Set
16 RDS 01/04/2007 23:45:38 I 2999 2768 [079] EAP-Message value: .....!
17 RDS 01/04/2007 23:45:38 I 2999 2768 [024] State value: EAP=0.ffffffff.1.1;
18 RDS 01/04/2007 23:45:38 I 0368 2768 ExtensionPoint: End of Attribute Set
19 RDS 01/04/2007 23:45:38 D 3934 2768 Sending response code 11, id 126 to 10.166.6.80 on port 1645
20 RDS 01/04/2007 23:45:38 I 2999 2768 [079] EAP-Message value: .....!
21 RDS 01/04/2007 23:45:38 I 2999 2768 [024] State value: EAP=0.ffffffff.1.1;SVC=0.1;
22 RDS 01/04/2007 23:45:38 I 2999 2768 [080] Message-Authenticator value: 4E 4F 54 20 43 4F 4D 50 55 54 45 44 20 59 45 54
23 RDS 01/04/2007 23:45:39 D 0245 2768 Request from host 10.166.6.80:1645 code=1, id=127, length=263 on port 1645
24 RDS 01/04/2007 23:45:39 I 2999 2768 [001] User-Name value: DO-MAIN\testi
25 RDS 01/04/2007 23:45:39 I 3017 2768 [006] Service-Type value: 2
26 RDS 01/04/2007 23:45:39 I 3017 2768 [012] Framed-MTU value: 1500
27 RDS 01/04/2007 23:45:39 I 2999 2768 [030] Called-Station-Id value: 00-18-BA-57-2A-8A
28 RDS 01/04/2007 23:45:39 I 2999 2768 [031] Calling-Station-Id value: 00-08-02-D5-C5-47
29 RDS 01/04/2007 23:45:39 I 2999 2768 [079] EAP-Message value: ...p.....f....a...]..F...L.J_...&.....T..T.R..#....j. ..".i..<.b2.Z.....w....*r..R`.<.....d.b.....c..
30 RDS 01/04/2007 23:45:39 I 2999 2768 [080] Message-Authenticator value: A0 A3 8F 58 77 C2 97 5F E6 4A 83 0A C0 E3 95 61
31 RDS 01/04/2007 23:45:39 I 3017 2768 [005] NAS-Port value: 50010
32 RDS 01/04/2007 23:45:39 I 3017 2768 [061] NAS-Port-Type value: 15
33 RDS 01/04/2007 23:45:39 I 2999 2768 [024] State value: EAP=0.ffffffff.1.1;SVC=0.1;
34 RDS 01/04/2007 23:45:39 I 3042 2768 [004] NAS-IP-Address value: 10.166.6.80

35 RDS 01/04/2007 23:45:39 I 0299 2768 ExtensionPoint: Initiating scan of configured extension points...
36 RDS 01/04/2007 23:45:39 I 0331 2768 ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
37 RDS 01/04/2007 23:45:39 I 0336 2768 ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [4 - accept_continue]
38 RDS 01/04/2007 23:45:39 I 0366 2768 ExtensionPoint: Start of Attribute Set
39 RDS 01/04/2007 23:45:39 I 2999 2768 [079] EAP-Message value: ....
40 RDS 01/04/2007 23:45:39 I 3047 2768 [026] Vendor-Specific vsa id: 311
41 RDS 01/04/2007 23:45:39 I 3089 2768 [016] MS-MPPE-Send-Key value: .....\.W.A.0B>.9I.....k{.k&...n.t..x.RIec]....nS.F
42 RDS 01/04/2007 23:45:39 I 3047 2768 [026] Vendor-Specific vsa id: 311
43 RDS 01/04/2007 23:45:39 I 3089 2768 [017] MS-MPPE-Recv-Key value: .H"..:/..8IR....._.t...E.f...\.B+.}.6..|.r...>