KYMENLAAKSON AMMATTIKORKEAKOULU
Elektroniikan koulutusohjelma / tietoliikennetekniikka

Kaalikoski Konsta
Kitunen Jaakko

KÄYTTÄJÄN AUTENTIKOINTI, VALTUUTUS JA TILASTOINTI OSANA VERKON ETÄHALLINTAA

Opinnäytetyö 2010

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Elektroniikka

KAALIKOSKI, KONSTA	Käyttäjän Autentikointi, Valtuutus ja Tilastointi osana
KITUNEN, JAAKKO	verkon etähallintaa
Opinnäytetyö	44 sivua
Työn ohjaaja	Yliopettaja Martti Kettunen
Toimeksiantaja	Kotkan kaupunki, ATK-keskus
Tammikuu 2010	
Avainsanat	autentikointi, verkonhallinta, tietoturva, etäkäyttö

Tietoturvan kannalta tunnukset, jotka mahdollistavat verkkolaitteiden etähallinnan olisi syytä vaihtaa säännöllisin väliajoin. Verkon koostuessa sadoista verkkolaitteista, on käyttäjätunnusten vaihtaminen laitekerrallaan hidasta. Erillinen autentikointipalvelin poistaa tämän ongelman, koska kaikki käyttäjätunnukset sijaitsevat keskitetyssä tietokannassa. Käyttäjien hallinta helpottuu, koska käyttäjätunnuksia ei tarvitse enää hallita jokaisessa verkkolaitteessa erikseen.

Työssä käsitellään käyttäjän todennuksen, valtuutuksen ja tilastoinnin toimintaa käytettäessä Ciscon Access Control Server -autentikointipalvelinta. Tavoitteena oli toteuttaa autentikointipalvelin, jonka kautta kirjauduttaisiin verkossa oleviin laitteisiin.

Tietoliikennelaboratorioon suunniteltiin ja toteutettiin toimiva etähallinnan mahdollistava verkko. Käytännön kokeissa todettiin, kuinka autentikointipalvelin toimii etäkäyttäjän tunnistuksessa ja valtuutuksessa. Verkkolaite lähettää käyttäjän antamat tiedot palvelimelle, joka sallii tai estää käyttäjän kirjautumisen.

Autentikointipalvelin helpottaa verkonhallintaa, koska palvelin tallentaa käyttäjän kirjautumisen ja toiminnan. Verkon haltijat pystyvät näin tarkkailemaan verkossa tapahtuvia muutoksia ja sitä, kuka verkkoon on muutoksia tehnyt.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Electronics

KAALIKOSKI, KONSTA	User Authentication, Authorization and Accounting
KITUNEN, JAAKKO	as a part of the network management
Bachelor's Thesis	44 pages
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	City of Kotka, ATK-keskus
January 2010	
Keywords	authentication, network management, data security, remote access

Usernames and passwords that are used to remotely access a network should be changed regularly. On a large network, changing the usernames and passwords one at a time from every device in the network is really slow. A separate authentication server removes this problem and simplifies user management, because all usernames and passwords are in one centralized database.

This thesis concentrates on authentication, authorization and accounting of the remote user. The goal was to configure an authentication server that controls users who can access the network.

A remotely managed network was designed and implemented for the laboratory. The tests demonstrated how the authentication server works when it is identifying the user. The network device sends the username and password to the server, which then accepts or declines the user's attempt to access the device.

The authentication server keeps record of logged in users and the changes users have made to the network devices. From the server's log, network administrators can easily monitor changes in the network.

LYHENTEET

3DES, Triple Data Encryption Standard. DES salauksen muoto, joka käyttää tiedon salaamiseen kahta salausavainta. Tieto salataan kolmeen kertaan; ensin avaimella 1, sitten avaimella 2 ja lopuksi vielä avaimella 1.

AAA, Authentication, Authorization, Accounting. Protokolla jolla tunnistetaan verkon toinen osapuoli.

ACS, Access Control Server. Ohjelma jolla kontrolloidaan verkossa olevia laitteita, sekä niihin pääseviä käyttäjiä.

AD, Active Directory. Windows-palvelinten käyttämä käyttäjätietokanta, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista.

AES, Advanced Encryption Standard. Tietotekniikassa käytettävä lohkosalausjärjestelmä.

CLI, Command Line Interface. Ciscon käyttämien verkkolaitteiden komentorivi käyttöliittymä.

DES, Data Encryption Standard. Tiedonsalausmenetelmä joka perustuu satunnaisesti valittuun 56-bittiseen salausavaimeen.

EAP, Extensible Authentication Protocol. Käyttäjien tunnistusprotokolla.

EAPOL, EAP Over LAN. EAP-paketointitekniikka,

EXEC, Kytkimen tai reitittimen komentorivi istunto.

HTTP, Hypertext Transfer Protocol. Sovelluskerroksen protokolla jota käytetään HTML-kielellä toteutettujen sivujen tiedonsiirtoon.

HTTPS, Hypertext Transfer Protocol Secure. HTTP-protokollan salattu versio.

IEEE, Institute of Electrical and Electronics Engineers. Organisaatio jonka tehtävänä on kehittää viestintä- ja verkkostandardeja

IOS, Internetwork Operating System. Ohjelmisto jota käytetään Cisco Systemsin valmistamissa reitittimissä ja kytkimissä.

IP, Internet Protocol. Verkkokerroksen protokolla joka tarjoaa yhteydetöntä palvelua laitteiden välillä.

LAN, Local Area Network. Tietoliikenneverkko joka on rajoittunut pienelle alueelle, esimerkiksi yhteen kiinteistöön.

MIB, Management Information Base. SNMP-protokollassa käytettyjen muuttujien tietokanta.

NAS, Network Access Server. Laite johon pc-kone kytketään jotta päästään kytkeytymään verkkoon. Voi olla esimerkiksi kytkin tai langaton tukiasema.

NDG, Network Device Group. ACS ohjelmistoon määritetty laiteryhmä johon listätään verkossa olevat kytkimet, reitittimet tai palomuurit.

OOB, Out-of-Band. Tapa ottaa etäyhteys verkossa olevaan kytkimeen tai reititinlaitteeseen käyttäen laitteiden konsoliporttia.

PPP, Point to Point Protocol. Protokolla jota käytetään kahden laitteen välisen yhteyden muodostukseen.

RADIUS, Remote Authentication Dial In User Service. Protokolla jota käytetään käyttäjän tunnistukseen, valtuutukseen ja tilastointiin. Käyttäjätunnusten tietokannat sijaitsevat keskitetyllä palvelimella.

RSA, Rivest Shamir Adleman. Julkiseen salausavaimeen perustuva tiedonsalausalgoritmi. Salausavain muodostetaan kertomalla kaksi suurta alkulukua yhteen.

SMI, Structure of Management Information. Kehysrakenne joka määrittää SNMP-protokollassa käytetyt muuttujat.

SNMP, Simple Network Management Protocol. Verkonhallinta protokolla, joka tarjoaa mahdollisuuden valvoa ja hallita laitteita.

SSH, Secure Shell. Mahdollistaa kahden tietokoneen välisen turvallisen tiedonsiirron.

TACACS+, Terminal Access Controller Access Control System Plus. On etäyhteyden autentikointiprotokolla.Tarjoaa käyttäjien tunnistusta sekä oikeuksien määrittelyä. Käyttäjätunnusten tietokannat sijaitsevat keskitetyllä palvelimella.

TCP, Transmission Control Protocol. Yhteydellinen kuljetuskerroksen protokolla, joka tarjoaa luotettavan kaksisuuntaisen tiedonsiirron.

TELNET. Lähiverkossa tai internetissä käytettävä verkkoprotokolla, jota käytetään tiedonsiirtoon.

UDP, User Datagram Protocol. Yhteydetön kuljetuskerroksen protokolla, ei varmista pakettien perillemenoa.

VLAN, Virtual Local Area Network. Tekniikka jolla fyysinen verkko voidaan jakaa pienempiin loogisiin osiin. Laitteet voivat keskustella keskenään, vaikka verkon eri segmentissä.

VPN, Virtual Private Network. Tekniikka jolla kaksi konetta voidaan kytkeä yhteen julkisen verkon läpi, niin että ne ovat näennäisesti samassa verkossa.

VTY, Virtual Terminal Line. Virtuaalinen päätelaitteen hallintalinja. Etäyhteyksissä kuten TELNET ja SSH.

SISÄLLYS

1 JOHDANTO

Kotka on Kymenlaakson toiseksi suurin kaupunki. Asukkaita Kotkassa on noin 550000. Kotka sijaitsee Suomenlahden itärannikolla, Kymijoen suistossa. Kotkassa sijaitsee muun muassa paperiteollisuutta ja yksi Suomen johtavista vientisatamista.

”Kotkan kaupungin tietohallinto tukee kaupungin toiminnan kehittämistä ja johtamista sekä kuntalaisille suunnattua palvelutuotantoa kilpailukykyisten ja standardien mukaisten tietotekniikkapalvelujen avulla, jotka toteutetaan hyvää tietohallintotapaa noudattaen. Palvelutuotannon toteutuksesta vastaa kaupungin ATK-keskus, jossa työskentelee tietohallintopäällikön johdolla parikymmentä tietotekniikan ammattilaista. Keskuksen tehtäviin kuuluu mm. teknisen arkkitehtuurin ja käyttäjätuen toteutus ja ylläpito sekä kaupungin tietojärjestelmäprojekteihin osallistuminen.” (viite: http://www.kotka.fi/alltypes.asp?d_type=5&menu_id=688&#5)

Insinöörityön tavoitteena oli toteuttaa tietoturvallinen verkkolaitteiden etähallinta. Työhön sisältyi sekä autentikointipalvelimen että verkkolaitteiden konfigurointi. Palvelimen tehtävänä oli tunnistaa käyttäjä, joka ottaa etäyhteyttä verkkolaitteeseen. Verkkolaitteet konfiguroitiin käyttämään TACACS+ -protokollaa käyttäjän tunnistamiseen.

Työ toteutettiin ottamalla käyttöön Cisco Systemsin ACS (Access Control Server) -autentikointipalvelin. Ohjelmaan luotiin käyttäjäryhmät eri tason oikeuksilla. Ryhmiin liitettiin käyttäjätiedot erilliseltä Active Directory -palvelimelta.

Työn suurin osuus oli toimivan konfiguraation laatiminen. Tavoitteena oli saada aikaan selkeä ja yhdenmukainen konfiguraatio, joka toimisi mahdollisimman monessa käytössä olevassa kytkimessä.

2 VERKKOLAITTEIDEN ETÄHALLINTA

Laitteiden ollessa maantieteellisesti kaukana käyttäjästä on mielekästä käyttää etähallintaa aina, kun se on mahdollista. Näin säästyy aikaa sekä rahaa, koska laitteiden luokse ei tarvitse mennä kuin laitteen vikaantuessa tai kytkentöjen muutoksien takia. Laitteisiin tarvittavat konfiguraatiomuutokset voidaan tehdä esimerkiksi toimistolta käsin. Verkkolaitteiden etähallinta on mahdollista toteuttaa monella tavalla. Tässä luvussa käydään läpi erilaisia tekniikoita, joilla voidaan toteuttaa etähallinta Ciscon Catalyst kytkimiin.

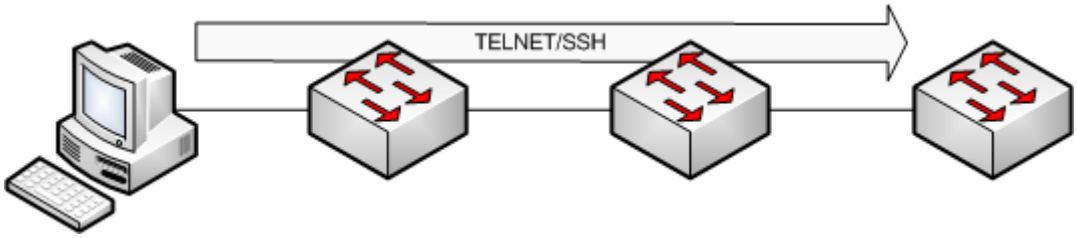
2.1 In-Band -ja Out-of-Band-hallinta

Kirjauduttaessa sisään hallinnoitavaan laitteeseen liikenne isäntäkoneen ja hallittavan laitteen välillä voi kulkea kahdella tapaa. Out-of-Band hallinnassa tieto kulkee omassa hallintaverkossa, jossa ei kulje tuotantoverkon liikennettä. In-band-hallinnassa taas tieto kulkee tuotantoverkossa tai Internetissä muun liikenteen seassa.

Mikäli käytetään In-Band-hallintaa ja verkkoon on tunkeuduttu, tunkeutujan on mahdollista saada tietoonsa verkkolaitteiden tunnukset ja salasanat. Tästä johtuen Out-of-Band -hallinta on tietoturvan kannalta katsottuna parempi vaihtoehto, koska hallintaverkko on täysin erillään tuotantoverkosta.

2.1.1 In-Band-hallinta

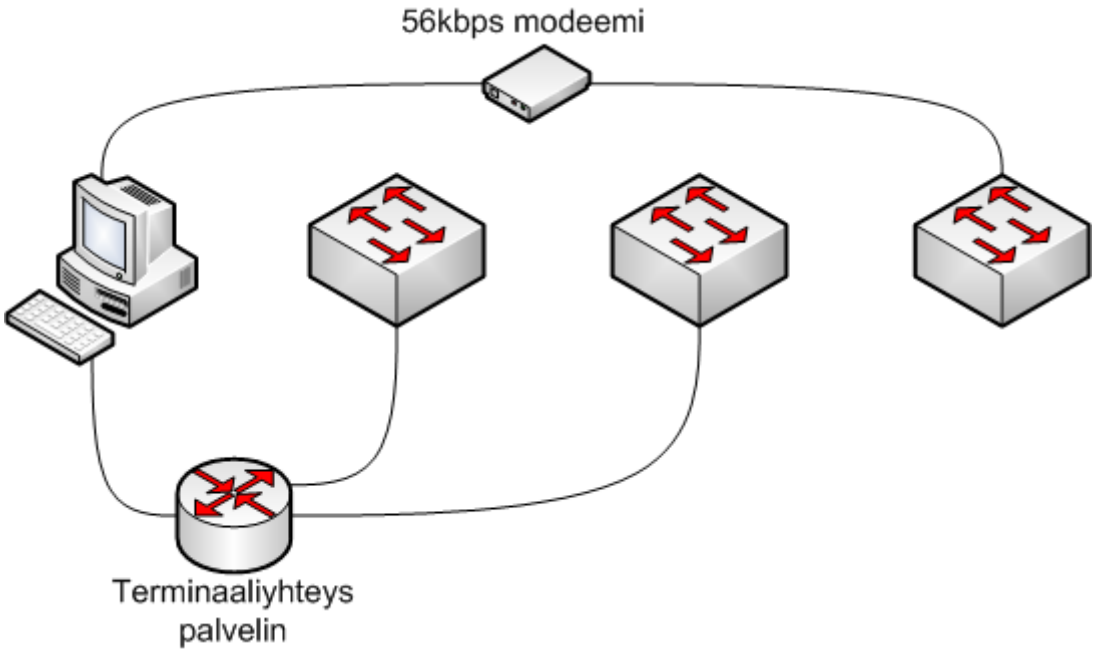
In-Band on paikallista hallintaa verkon läpi käyttäen TELNET-, SSH-, HTTP- tai HTTPS-yhteyttä. In-Band on yleisin tapa ratkaista verkonhallinta. Suurissa verkoissa pelkästään In-Band-hallinta ei ole riittävä. Tämän toteutuksen ongelmana on se, että mikäli verkon toiminta lamaantuu, myöskään hallintayhteyksiä laitteisiin ei tällöin ole. Ongelman johtuessa konfiguratio muutoksesta, tilannetta ei voida korjata etäyhteydenavulla. Tällaisessa tilanteessa tarvitaan vaihtoehtoinen ratkaisu vian aiheuttaneeseen laitteeseen pääsemiseksi. Käytännössä tämä tarkoittaa fyysisesti laitteen luokse siirtymistä tai Out-of-Band (OOB) -hallinnan käyttöä. (OutPost Sentinel)



Kuva 1. In-Band-hallinnan periaatekuva

2.1.2 Out-of-Band -hallinta

Tilanne jossa In-Band-hallintaa ei ole mahdollista käyttää tarjoaa Out-of-Band arvokkaan lisän verkon ylläpitäjälle. Verkossa olevat kytkimet, reitittimet ja palomuurit tarjoavat konsoliportin OOB-yhteyksille. Näitä portteja voidaan käyttää laitteeseen pääsyyn, kun IP-pohjainen kommunikointi ei vastaa. Laitteen konsoliportti kytketään joko modeemin- tai terminaaliyhteyspalvelimen kautta esim. puhelinverkkoa pitkin erilliseen hallintakoneeseen verkossa. Mikäli verkkoon tulee ongelma, joka estää TELNET- tai SSH-yhteyden käytön verkkolaitteisiin, on vielä mahdollista kirjautua esim. modeemin välityksellä. (WTI)



Kuva 2. OOB-hallinnan periaatekuva

2.2 Käyttäjien hallinta ja oikeudet

Tässä luvussa käydään läpi tekniikoita joilla, rajataan käyttäjiltä pois ylimääräisiä ja vaarallisia komentoja. Mikäli käyttäjät tarvitsevat vain joitakin laitteen tilaa näyttäviä komentoja, on turhaa ja vaarallista antaa käyttöön kaikki komennot. On mahdollista, että käyttäjä tietämättään vahingossa tai tahallaan tekee laitteeseen muutoksia, jotka haittaavat verkon toimintaa. Eihän työkoneisiinkaan kirjauduta adminstrator-tunnuksilla.

2.2.1 Privilegio-tasot

Cisco IOS tarjoaa 16 erilaista privilegio-tasoa. Mitä korkeampi privilegio-taso on, sitä enemmän on käyttöoikeuksia. Oletusarvoisesti IOS-ohjelmistossa on kaksi tilaa: user EXEC -ja privileged EXEC -tila.

User EXEC -tila – privilegiotaso 1

Privileged EXEC -tila – privilegiotaso 15

Laitteen ollessa oletusasetuksilla sisään kirjaudutaan user EXEC -tilaan. Tässä tilassa on käytössä vain joitain laitteen tilaa antavia komentoja, eikä laitteeseen ole mahdollista tehdä konfiguraatiomuutoksia. Tämän rajoituksen takia siirrytään enable-komennolla pois user EXEC -tilasta privileged EXEC -tilaan. Oletusarvoisesti enable-komento siirtää käyttäjän suoraan privilegio-tasolle 15. Tämä taso vastaa Windows-käyttöjärjestelmien administrator oikeuksia, eli käyttäjällä on täydellinen pääsy verkkolaitteen hallintaan. (David 2005)

Mikäli osa verkkolaitteita hallinnoivista käyttäjistä tarvitsee vain joitakin laitteen tai porttien tilaa koskevia tietoja tai heidän täytyy vain konfiguroida yksittäisiä portteja, heitä varten voidaan luoda oma käyttäjäryhmä. Tälle privilegio-tasolle lisätään vain ne välttämättömät käskyt, joita käyttäjät tarvitsevat. (David 2005)

2.2.2 Roolipohjainen komentorivin käyttöoikeus

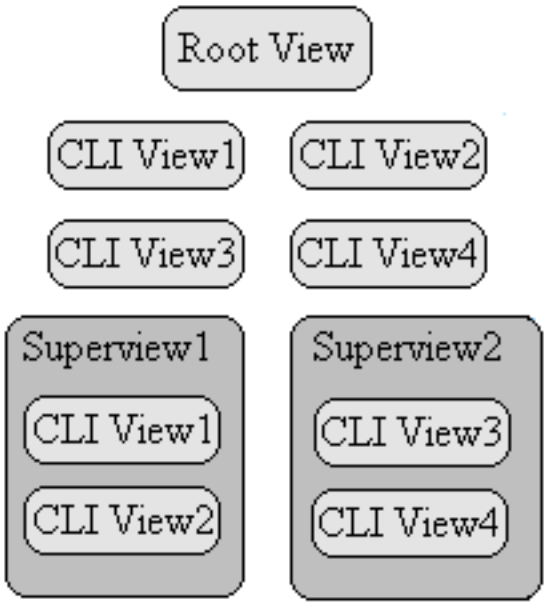
Role Based CLI Access on vapaasti käännettynä roolipohjainen komentorivin käyttöoikeus. Tämä toiminto mahdollistaa sen, että verkon pääkäyttäjä voi luoda eri view-

tiloja. View-tilat ovat joukko komentoja ja konfiguraatio-ominaisuuksia, jotka tarjoavat valikoitua osaa IOS-laitteen EXEC-tilan komennoista. (Role-Based CLI Access 1)

Käytössä on kolme erilaista tilaa: root view, CLI view ja Superview. Järjestelmän ollessa root view -tilassa käytössä ovat kaikki komennot, kuten privilegio-tasolla 15. Ero root view- ja privilegio 15 -tilassa on se, että mikäli käyttäjä haluaa luoda CLI view iloja ja lisätä tai poistaa niistä komentoja, hänen täytyy olla root view -tilassa. (Role-Based CLI Access 2)

CLI view -tilassa käyttäjällä on käytössä vain ne komennot, joita root view -tilassa on tälle ryhmälle määritelty. CLI view- ja superview-tiloja on mahdollista luoda 15. Tähän ei sisälly root view -tila. (Role-Based CLI Access 2)

Superview-tila koostuu yhdestä tai useammasta CLI view -tilasta. Superview mahdollistaa sen, että verkon pääkäyttäjä voi helposti määritellä kerralla käyttäjille yhden superview-tilan eikä käyttäjille tarvitse määritellä useaa erilaista komentorivinäkymää. (Role-Based CLI Access 7)



Kuva 3. Role BASED CLI -tilat.

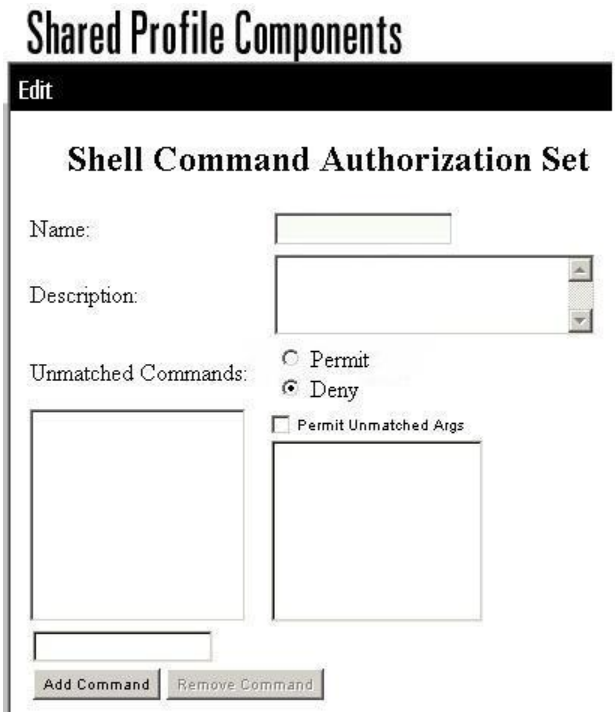
2.2.3 ACS:n kautta valtuutettavat käskyt

Shell command authorization set eli vapaasti suomennettuna käskyjen valtuutuslista mahdollistaa käskyjen keskitetyn hallinnan. Tämä helpottaa käyttöoikeuksien valvontaa ja hallintaa. Käyttäjälle näkyvät käskyt on etukäteen määritelty ACS:ssä, joten niitä ei tarvitse erikseen määritellä jokaiseen käytössä olevaan verkkolaitteeseen. Käskyjä voi valtuuttaa joko tietylle käyttäjäryhmälle tai yksittäiselle käyttäjälle. Esimerkiksi verkonvalvojalla voi olla käytössään kaikki käskyt, joita laitteessa on. Helpdeskillä sitä vastoin voi olla käytössään korkean tason tarkkailukäskyjä, esim. show run, mutta kaikki konfigurointikäskyt on kielletty. (ACS Shell Command Authorization Set)

Kaikki käskyt, joita valtuutuslistassa ei ole määritelty, on automaattisesti kielletty. Tämä helpottaa listan tekemistä, koska ei tarvitse kirjoittaa kuin ne käskyt, jotka sallitaan. Käskyistä täytyy jokainen osa sallia erikseen. Tämä tuo verkonvalvojalle lisää työtä, mutta mahdollistaa hyvin tarkasti käyttäjän oikeuksien määrittelyn. (ACS Shell Command Authorization Set)

Valtuutuslistalle annetaan nimi ja kuvaus. Kuvaus ei ole pakollinen, mutta se helpottaa listan käyttötarkoituksen selvittämistä. Käskyt, jotka eivät täsmää listassa määriteltyihin, voidaan joko sallia tai kieltää. Käsky, joka halutaan sallia, kirjoitetaan tyhjään kenttään ja lisätään ”add command” -painikkeella. Tämän jälkeen kirjoitetaan käskyn lisämääre ja lisätään se ”add command” -painikkeella. (ACS Shell Command Authorization Set)

Jos halutaan sallia sellaiset määreet, jotka eivät vastaa listaa, käskyn lisämääreet voidaan sallia ”Permit unmatched arguments” toiminnolla. Kun valtuutuslistaa tehdään, täytyy tietää, missä muodossa laite lähettää käskyn palvelimelle. Esimerkiksi jos halutaan sallia käsky ”interface fastethernet0/1”, täytyy määre fastethernet0/1 laittaa muodossa ”permit fastethernet 0 1”. Tämä johtuu siitä, että laite näkee monta määrettä, jotka täytyy tarkistaa. Laite poistaa kenoviivan numeroiden välistä ja näkee numerot erillisinä määreinä, eli 0/1 ei ole yksi määre, vaan 0 ja 1 ovat erilliset määreet. (ACS Shell Command Authorization Set)



Kuva 4. ACS:n valtuutuslistan konfigurointi ikkuna

2.3 Yhteyskäytännöt

Jotta verkossa olevaa laitetta olisi mahdollista hallita etäyhteyden avulla, tarvitaan yhteyskäytäntö etäyhteyttä varten. Tässä luvussa tarkastellaan neljää verkonhallinnan yhteyskäytäntöä. Kaikilla on mahdollista muokata verkossa olevan laitteen toimintaa.

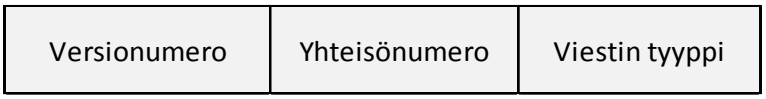
2.3.1 SNMP-yhteyskäytäntö

SNMP-protokolla toimii pyyntö-vastaus-periaatteella. Sen tarkoituksena on lukea ja muuttaa verkkolaitteiden, eli hallinnoitavien laitteiden, asetuksia. Normaalisti protokolla toimii UDP-protokollan päällä, mutta TCP:n käyttökin on mahdollista. SNMP toimii epäsymmetrisesti hallinta-aseman ja hallinnoitavan laitteen välillä. Hallinnoitavan laitteen ohjelmiston tehtävänä on toteuttaa hallinta-asemalta tulevat käskyt. Hallinta-asema on varustettu käyttöliittymällä, jonka kautta verkon hallinnoitavat laitteet konfiguroidaan. (Baccala. 1997)

Hallinta-asema ja hallinnoitava laite kommunikoivat SNMP-viestien välityksellä. Yhteyden alussa hallinta-asema muodostaa SNMP-pyyntöviestin käyttäjän antamien tie-

tojen perusteella. Viesti lähetetään hallinnoitavalle laitteelle, jossa se käsitellään. Hallinnoitava laite suorittaa viestissä määritetyt tehtävät. Tämän jälkeen hallinnoitava laite lähettää hallinta-asemalle SNMP-vastausviestin, joka sisältää pyydetyt tai muutetut tiedot. Lopuksi hallinta-asema käsittelee saamansa viestin. (Kozierok 2005a)

SNMP-viestin ensimmäinen kenttä on versionumero, joka kertoo, mitä protokollan versiota käytetään. Toinen kenttä on yhteisönumero, jonka avulla hallinta-asema ja hallinnoitava laite tunnistavat toisensa. Kolmas kenttä on viestin tyyppi, jolla määritellään viestin käyttötarkoitus. Viestin tyyppi vaihtelee sen mukaan, luetaanko vai muutetaanko tietoa. GetRequest/SetRequest toimittaa listan hallinnoitavan laitteen asetuksista joita, halutaan lukea tai muuttaa. GetResponse on vastausviesti, jonka hallinnoitava laite lähettää hallinta-asemalle. Viesti sisältää pyydetyt tai muutetut tiedot sekä mahdolliset vikatilanteet, joita viestin käsittelyssä ilmeni. Trap on ainoa viestityyppi, jonka hallinnoitava laite lähettää oma-aloitteisesti hallinta-asemalle. Viesti sisältää tiedot sellaisista laitteen kohtaamista vikatilanteista, jotka vaativat käyttäjän huomiota. (Kozierok, 2005a)



Kuva 5: SNMP-viestin rakenne

2.3.2 TELNET-yhteyskäytäntö

TELNET-protokollan tarkoituksena on muodostaa yhteys kahden eri koneen välille ja se toimii monen muun TCP/IP-protokollaperheen protokollan tavoin asiakas/palvelin-periaatteella. Tyypillisesti asiakas on ohjelma, joka välittää käyttäjän antamat käskyt palvelimelle ja palvelimen vastineet käyttäjälle. Palvelin on etäkoneella toimiva ohjelma, jonka on sallittu muodostaa etäyhteyksiä. (Kozierok, 2005b)

TELNET käyttää yhteydellistä TCP-protokollaa yhteydenmuodostukseen ja tiedonvälitykseen. TELNET-palvelin käyttää porttia 23, ja kun asiakas ottaa yhteyttä palvelimeen, palvelin muodostaa yhteyden käyttäen TCP:n kolmivaiheista kättelyä. Koska TCP toimii kaksisuuntaisesti, sekä asiakas että palvelin voivat lähettää toisilleen tietoa samanaikaisesti. TELNET-palvelimella voi olla auki monia yhteyksiä samanaikaisesti

eri asiakkaisiin. Palvelin erottaa asiakkaat toisistaan asiakkaan IP-osoitteen ja porttinumeron avulla. (Kozierok, 2005b)

Kun TCP-yhteys on muodostettu ja TELNET-istunto aktiivinen, palvelin lähettää käyttäjälle kyselyn käyttäjänimestä ja salasanasta. TELNET-asiakas lähettää tiedot palvelimelle, ja mikäli tiedot ovat oikein, käyttäjä saa pääsyn verkkoon niillä oikeuksilla, jotka käyttäjätilille on määritetty. (Kozierok, 2005b) Yhteydenmuodostuksen jälkeen TELNET-protokollan ainoa tehtävä on välittää käyttäjän komennot palvelimelle ja palvelimen vastineet käyttäjälle. (Kozierok, 2005c)

2.3.3 Secure Shell -yhteyskäytäntö

SSH-protokollan tarkoituksena on muodostaa suojattu yhteys kahden tietokoneen välille. SSH toimii asiakas-palvelin-periaatteella. Asiakas on tietokone, joka aloittaa yhteydenmuodostuksen. Palvelin on tietokone, joka vastaa yhteydenottopyyntöön. Koska tietokoneiden välinen liikenne on salattu, sitä ei voi lukea. Koska SSH salaa kaiken liikenteen, sitä voi myös käyttää salaamaan salaamattomien protokollien liikennettä. Tämä tapahtuu port forwarding -tekniikalla. (SSH Protocol. Red Hat Inc. 2002)

Salatun yhteyden muodostus alkaa asiakkaan ja palvelimen välisellä neuvottelulla käytettävästä salaustavasta. SSH on suunniteltu tukemaan montaa erityyppistä salaustapaa (esim. AES, 3-DES ja RSA). Seuraavaksi palvelin lähettää julkisen avaimensa asiakkaalle. Asiakas muodostaa 256-bittisen istuntoavaimen, jonka se salaa palvelimen julkisen avaimen kanssa. Asiakas lähettää salatun istuntoavaimen palvelimelle, yhdessä käyttämänsä salaustavan kanssa. Palvelin avaa istuntoavaimen yksityisellä avaimellaan. Tämän jälkeen palvelin lähettää salatun varmistusviestin asiakkaalle. Nyt palvelimella ja asiakkaalla on yhteinen istuntoavain ja käytössä sama salaustapa. Näiden varmistusten jälkeen kaikki liikenne kulkee salattuna asiakkaan ja palvelimen välillä. Varmistusten tietoturvallisuus perustuu luottamukseen siitä, että vastapuolen avaimet ovat oikeat. (Cryptography – Secure Shell. 2008)

SSH:lla on kaksi tapaa muodostaa yhteys asiakkaan ja palvelimen välille. Ensimmäinen tapa on kysyä käyttäjältä, halutaanko yhteys muodostaa. Toisessa tavassa palvelin haastaa asiakkaan. Asiakkaan ottaessa ensimmäistä kertaa yhteyttä palvelimeen käyttäjältä kysytään, halutaanko yhteys muodostaa (ja saatetaan näyttää palvelimen avaimen tarkistussumma). Mikäli käyttäjä päättää muodostaa yhteyden, asiakas tallentaa

palvelimen avaimen. Palvelin voi myös lähettää asiakkaalle salatun viestin käyttäen salaamiseen asiakkaan julkista avainta (joka palvelimella on tietokannassaan). Mikäli asiakas pystyy avaamaan viestin yksityisellä avaimellaan, palvelin muodostaa yhteyden. Tätä tapaa kutsutaan haasteeksi. (Cryptography – Secure Shell. 2008)

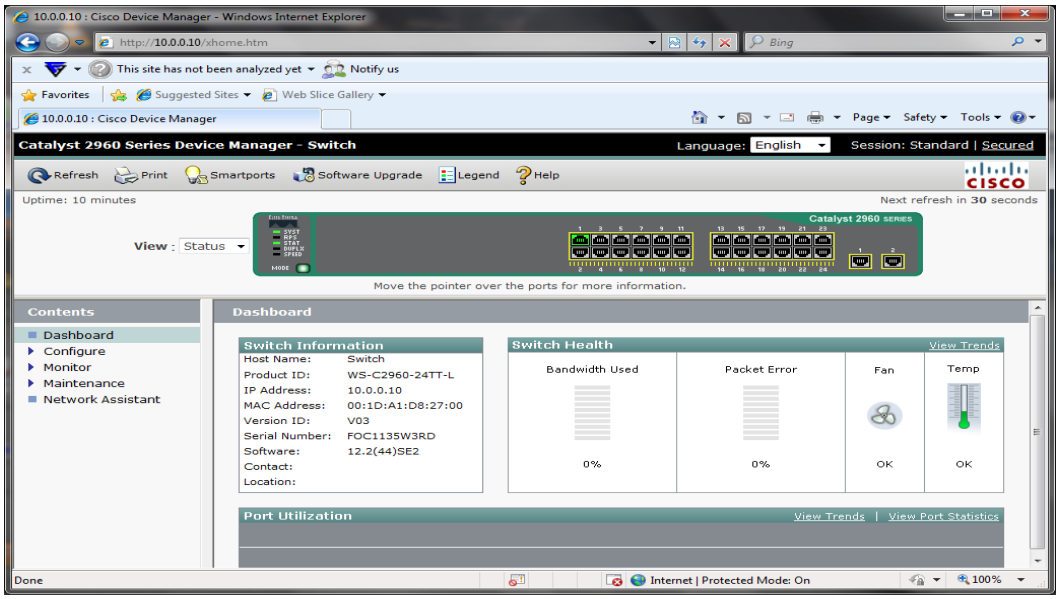
Yhteydenmuodostuksen jälkeen käyttäjän täytyy kirjautua palvelimelle. Kirjautumiseen on mahdollista käyttää kahta tapaa. Yleisin käytössä oleva on käyttäjänimi-salasana-pari. Toinen, vähemmän käytetty tapa on julkiset avaimet. Salasana tunnistuksessa käyttäjältä kysytään käyttäjänimeä ja salasanaa. Yhteys muodostetaan mikäli käyttäjän antamat tiedot vastaavat palvelimen tietokannassa olevia. Joustavampi tapa on haastaa asiakas. Yhteys muodostetaan, mikäli asiakas saa haasteviestin avattua. (Cryptography – Secure Shell. 2008)

2.3.4 WEB-pohjainen hallinta

Ciscon IOS-ohjelmisto sisältää Web-selaustoiminnon, jossa on mahdollista antaa Ciscon IOS-komentoja. Tämän ominaisuuden avulla päästään käsiksi kytkimen kotisivulle, josta laitetta hallitaan. Sivuston kautta on mahdollista antaa useampia IOS-komentoja laitteelle. (Using the Cisco Web Browser 1)

Web-hallinta on oletusarvoisesti pois päältä. Graafinen hallinta on mahdollista ottaa käyttöön käynnistämällä laitteessa HTTP- tai HTTPS-palvelin. Tämä mahdollistaa verkkolaitteen tilan seuraamisen ja konfiguroinnin Web-sivun kautta. (Using the Cisco Web Browser 2)

Jotta selainkäyttöliittymää olisi mahdollista käyttää, koneessa on oltava www-selain. Yhteys laitteeseen otetaan kirjoittamalla selaimen osoiteriville laitteen käyttämä protokolla sekä verkkolaitteen IP-osoite. Graafinen liittymä ei mahdollisesti tue kaikkia kytkimen toimintoja. Graafinen liittymä helpottaa kuitenkin oleellisesti esimerkiksi laitteen läpi kulkevan liikenteen ja prosessorikuorman seurantaa. (Using the Cisco Web Browser 3)



Kuva 6. Ciscon Catalyst 2960-selainhallinnan etusivu IE 8-selaimessa

Hypertext Transfer Protocol (HTTP) eli hypertekstin siirtoprotokolla on asiakas/palvelin-protokolla. Web-hallinnassa palvelimena toimii verkossa oleva kytkin tai reititin laite. HTTP käyttää tiedonsiirtoon TCP-protokollaa tyypillisesti porttinumerolla 80, myös porttinumerot 8000 ja 8888 ovat mahdollisia. (Anttila 2000, 431)

3 AUTENTIKOINTI

Autentikointi on prosessi, jolla varmistutaan siitä, että käyttäjä on se, kuka hän väittää olevansa. Varmennus voidaan suorittaa kolmella tavalla eli jollakin, mitä käyttäjä tietää, kuten salasana, tai jollain mitä käyttäjällä on, kuten varmennuspoletti, tai jollakin mitä käyttäjä on, kuten biometriikka. (Huntington 2009)

3.1 Autentikointitapoja

Käyttäjätunnus ja salasana on yleisin käytössä oleva tapa varmentaa käyttäjä. Se on valitettavasti myös turvattomin lyhyiden ja helposti arvattavien salasanojen takia. Tunnistus vaatii käyttäjätunnuksen ja salasanan kirjautumiseen. Salasanan pituus, käytettyjen merkkien tyyppi sekä salasanan voimassaoloaika ovat tärkeitä kriteereitä. (Huntington 2009)

Käyttäjä voidaan tunnistaa käyttäen tunnistukseen jotain, mitä vain käyttäjällä on. Esimerkiksi varmennuspolettia käytetään todennukseen sisään kirjautumisen yhtey-

dessä. Tunnistuksen aikana käyttäjä luo hallussaan olevalla poletilla kertakäyttöisen avaimen. Tällä avaimella hän kirjautuu järjestelmään. (Huntington 2009)

Käyttäjä voidaan tunnistaa myös fyysisten ominaisuuksiensa avulla. Tunnistuksessa käyttäjältä otetaan esimerkiksi kuva sormenjäljestä tai silmän värikalvosta ja verrataan saatua tietoa tietokannassa olevaan tietoon. (Huntington 2009)

3.2 ACS -autentikointipalvelin

Opinnäytetyössä käyttäjän tunnistukseen käytettiin Ciscon ACS-autentikointipalvelinta. Cisco Secure Access Control Server (ACS) on Ciscon kehittämä hallintaohjelmisto. Ohjelman avulla on mahdollista mm. kontrolloida verkkolaitteisiin pääseviä käyttäjiä sekä hallita verkkoon kirjautuneita henkilöitä.

3.2.1 Yleistä ohjelmasta

ACS on skaalautuva korkean suorituskyvyn TACACS+- ja RADIUS palvelin. Se toimii keskusohjauspisteenä hallinnoitaessa verkonkäyttäjiä ja verkonvalvojia sekä verkkoinfrastruktuurin resursseja. ACS tarjoaa yhdenmukaisen AAA-palveluille keskitetyn tietokannan sekä käyttäjien hallinnan Ciscon laitteille. (User Guide for Cisco Secure Access Control Server 45)

ACS tukee monenlaisia Ciscon verkkoon pääsyn mahdollistavia laitteita, joita kutsutaan AAA-asiakkaiksi. Näitä laitteita ovat esimerkiksi langalliset tai langattomat LAN-kytkimet ja tukiasemat, reitittimet, palomuuri ja VPN-laitteet. (User Guide for Cisco Secure Access Control Server 45)

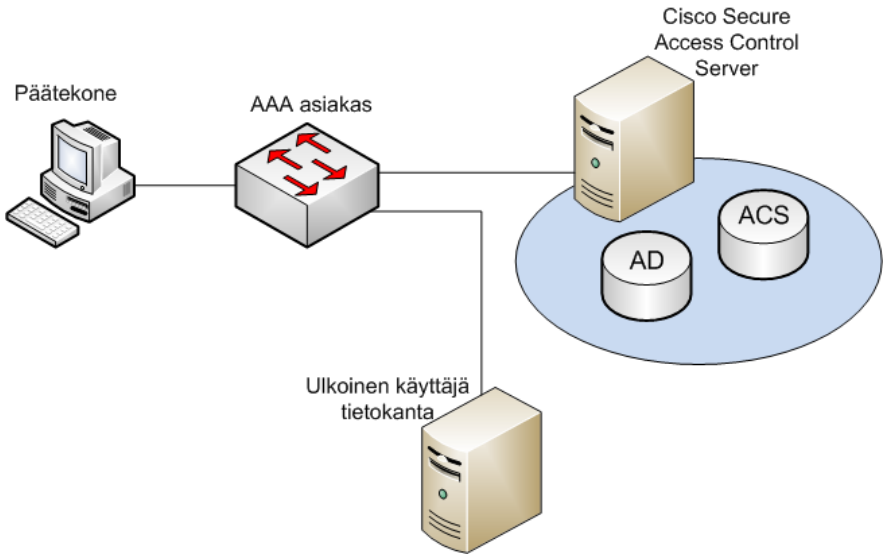
Verkonhallinnassa verkonvalvojan on helppoa määritellä ACS tietokantaan käyttäjät, joilla on oikeus kirjautua verkkoon. ACS mahdollistaa myös käyttäjien oikeuksien määrittelyn ja lisäksi se kirjaa käyttäjän tekemät toimenpiteet verkossa.

Kuva 7. ACS palvelimen käyttöliittymä

3.2.2 Toiminnan periaate

ACS tarjoaa AAA-palveluita kaikille Ciscon verkkolaitteille, jotka ovat verkossa AAA-asiakaskoneina. Näitä laitteita voivat olla esimerkiksi kytkin, reititin ja palomuurilaitteet. Kuvassa 8 on periaatekuva ACS -palvelimen toiminnasta.

Käyttäjä ottaa yhteyden AAA-asiakas koneeseen. Seuraavaksi AAA-asiakas ottaa yhteyden ACS-palvelimeen käyttäen joko TACACS+- tai RADIUS protokollaa. Käyttäjä tunnistetaan joko ACS palvelimen tietokannassa tai jostain ulkoisesta tietokannasta, kuten Active Directory. Jokainen käytössä oleva AAA-asiakaskone on liitettävä ACS-palvelimen tietokantaan ja molempiin laitteisiin on määriteltävä sama salasana tunnistamista varten. (User Guide for Cisco Secure Access Control Server)



Kuva 8. ACS- palvelimen toiminnan periaatekuva

3.2.3 Rakenne

ACS pitää sisällään seitsemän palvelumoduulia. Windows järjestelmä, johon ACS on asennettu, pyörittää näitä moduuleita. (User Guide for Cisco Secure Access Control Server 725)

- CSAdmin
- CSAuth
- CSDBSync
- CSLog
- CSMon
- CSTacacs
- CSRadius

Nämä palvelut, pois lukien CSAdmin, voidaan sulkea, käynnistää tai uudelleen käynnistää käyttämällä ACS:n web-käyttöliittymää tai Windows-palvelimen ohjauspaneelista. Seuraavaksi on lyhyesti kuvattu jokaisen prosessin tarkoitus. (User Guide for Cisco Secure Access Control Server 725)

CSAdmin on palvelu, joka tarjoaa web-palvelimen ACS:n web-käyttöliittymälle. Web-palvelin käyttää liikennöintiin porttia 2002 normaalin 80:n sijaan. Samassa palvelimessa on siis mahdollista käyttää toista web-palveluita tarjoavaa www-palvelinta.

CSAuth on todennus- ja valtuutuspalvelu. Se sallii tai kieltää pääsyn käyttäjille käsittelemällä todennus- ja valtuutuspyyntöä. Mikäli pääsy on myönnettävä, se määrittelee käyttäjälle oikeudet. CSAuth on myös ACS-tietokannan ylläpitäjä.

CSDPSync on palvelu, jolla synkronoidaan ACS:n tietokanta kolmannen osapuolen relaatiotietokannan hallintajärjestelmän (RDBMS) järjestelmään. CSDBSync synkronoi AAA-asiakkaat, AAA-palvelimet, NDG:t ja Proxy-taulukon tiedot ulkoiseen relaatiotietokantaan.

CSLog-palvelulla monitoroidaan ja kerätään lokitietoja. Se kerää tietoja järjestelmänvalvojan toimista, varmistuksista ja palautuksista, tietokantojen kopioinneista, ACS:n ydinpalveluista ja TACACS+:n ja RADIUS:n tilastoinnista.

CSMon-palvelu auttaa minimoimaan sitä aikaa, jolloin palvelin on poissa toiminnasta. Se toimii sekä TACACS+- että RADIUS -yhteyskäytännöillä ja havaitsee automaattisesti, kumpi protokolla on käytössä.

CSTacacs- ja CSRadius-palvelut kommunikoivat CSAuth-moduulin ja todennus- ja valtuutuspalveluja pyytävän verkkolaitteen välillä. CSTacacs liikennöi TACACS+-laitteisiin ja CSRadius liikennöi RADIUS-laitteisiin. Molemmat palvelut voivat olla samaan aikaan käytössä. Jotta CSTacacs ja CSRadius toimisivat kunnolla, palveluiden on kyettävä liikennöimään verkkolaitteeseen, yhtenevä salausavain on määritetty ja verkkolaitteen IP-osoite on määritelty ACS:ään. (User Guide for Cisco Secure Access Control Server 727- 730)

4 TODENNUS, VALTUUTUS JA TILASTOINTI

Kaikki on kiellettyä, ellei sitä erikseen sallita. Järjestelmiä on suojeltava joko tahalliselta tai tahattomalta väärinkäytöltä. Verkkoon kirjautuessaan käyttäjä tarvitsee todennuksen (Authentication), valtuutuksen (Authorization) ja yleensä myös tilastointia (Accounting). Nämä kolme muodostavat kirjain lyhenteen AAA. (Thomas 2005, 115)

4.1 Todennus

Todennuksella varmistetaan, että käyttäjä on se, kuka hän väittää olevansa. Todennukseen käytetään yleensä jotakin yksilöllistä, jonka vain käyttäjä tietää, kuten salasana,

tai joka käyttäjällä on, esim. sormenjälki tai silmän värikalvo. Todennuksella määritetään, ketkä voivat muodostaa yhteyden verkkoon. (Thomas 2005, 115)

4.2 Valtuutus

Valtuutus tehdään tunnistuksen jälkeen. Tässä vaiheessa käyttäjälle annetaan hänelle kuuluvat oikeudet. Työntekijältä voidaan esimerkiksi rajata kokonaan pääsy tärkeille palvelimille tai sallia luku verkkokiintolevyiltä muttei kirjoittamista niille. Esimerkkinä ovat Cisco verkkolaitteissa käytössä olevat käyttäjätasot 1-15 (privilege levels). Käyttäjätasolla 1 käyttäjä voi vain katsoa joitakin porttien tiloja, mutta hän ei voi tehdä muutoksia laitteen toimintaan. Tasolla 15 käyttäjän on mahdollista tehdä kaikkia muutoksia, joita verkkolaitteeseen on mahdollista tehdä. (Thomas 2005, 115)

4.3 Tilastointi

Tilastoinnilla kerätään tietoa käyttäjän toimista. Tilastoinnin avulla voidaan seurata esimerkiksi, mitä komentoja käyttäjä on antanut verkon reititin- tai kytkinlaitteille. Myös verkon ongelmatapauksissa, joita on syytä epäillä tahalliseksi häirinnäksi tai kiusanteoksi, on käyttäjä helppo jäljittää päivämäärä- ja kellonaikamerkintöjä käyttäen. Mikäli palkkaa maksetaan työssäoloajan mukaan, voidaan tilastointitietoja käyttää palkanmaksussa. (Thomas 2005, 115)

5 TACACS+ JA RADIUS AUTENTIKOINNIN OSANA

AAA-protokollaa käytetään käyttäjän tunnistukseen tietoverkossa. AAA-protokollia ovat TACACS+ ja RADIUS. Näitä protokollia käytetään esimerkiksi lähiverkossa tapahtuvaan asiakas- ja isäntälaitteen väliseen yhteyden tunnistukseen. Molemmat protokollat tarjoavat sekä käyttäjän tunnistuksen että valtuutuksen. Radiuksen pääasiallisena tehtävänä on estää luvattomat yhteydet verkossa. TACACS+ tarjoaa keskitettyä kelpuutusta verkkolaitteisiin pääsylle. Molemmat protokollat tarvitsevat AAA:n toimiakseen. Nämä protokollat toimivat vain NAS laitteen ja AAA-palvelimen välillä. Käyttäjälle ei välity tietoa protokollien toiminnasta, koska käyttäjän ja NAS laitteen välinen yhteys hoidetaan EAPOL protokollalla.

5.1 TACACS+

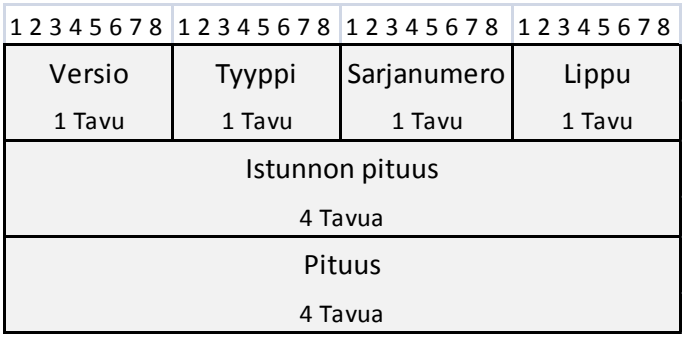
Terminal Access Controller Access Control System Plus (TACACS+) on protokolla, joka tarjoaa joustavaa tapaa hallita todentamis- ja valtuutusprosesseja. TACACS+ on Ciscon kehittämä AAA-protokolla, joka on kehitetty TACACS- ja laajennetusta TACACS (XTACACS) -protokollasta. (Carroll 2004, 15)

TACACS ja XTACACS käyttävät molemmat tiedonsiirtoon UDP-protokollaa, kun taas TACACS+ käyttää TCP-protokollaa. TACACS ja XTACAS ovat myös yhteensopimattomia TACACS+:n kanssa. Uusin TACACS+ kuitenkin korvaa aiemmat versiot ja se kykenee käyttämään AAA:ta aiempia versioita paremmin. (Carroll 2004, 15-16)

TACACS+ on laajasti käytössä oleva pääsynvalvontaprotokolla, jolla verkon pääsypalvelin (NAS) tunnistaa käyttäjän. NAS voi esimerkiksi olla WLAN tukiasema tai LAN-kytkin. TACACS+ toimii yleensä Windows Server- tai UNIX käyttöjärjestelmän päällä käyttäen tiedonsiirtoon TCP-protokollaa. Tämä takaa näin luotettavan tiedonsiirron. TACACS+ salaa kaiken liikenteen AAA-asiakkaan eli NAS-laitteen ja AAA-palvelimen välillä.

5.1.1 TACACS+-paketin otsikko

Kaikki TACACS+-paketit alkavat aina samanlaisella kahdentoista tavun otsikolla. Otsikko on esitetty kuvassa 9. Otsikko koostuu neljästä kahdeksan bitin pituisesta kentästä versiosta, tyypistä, sarjanumerosta ja lipusta. Istuntotunnus sekä pituus ovat 32 bitin mittaiset. (Carrel & Grant 1997, 4)



Kuva 9. TACACS+ paketin kehys

Versiokenttä on yhden tavun mittainen ja jakautuu kahteen neljän bitin kokoiseen kenttään. Nämä ovat pää- ja pikkuversio. Pääversio on merkittävä TACACS+-version numero. Minor- eli vähemmistöversio on tarkoitettu takaamaan yhteensopivuus protokollan vanhempien versioiden kanssa. (Carrel & Grant 1997, 4)

Typpi-, sarjanumero- ja lippukenttä ovat kaikki kahdeksan bitin pituisia. Tyyppikentässä määritellään, onko kyseessä todennus-, valtuutus- vai tilastointiviesti. Todennusviestin (TAC_PLUS_AUTHEN) arvo on 0x01. Valtuutusviestin (TAC_PLUS_AUTHOR) arvo on 0x02, ja tilastointiviestin (TAC_PLUS_ACCT) arvo 0x03. (Carrel & Grant 1997, 5)

Sarjanumerokentässä on nykyisen istunnon senhetkisen paketin numero. Istunnon ensimmäinen TACACS+-paketti saa aina arvon yksi. Seuraavat paketit kasvattavat kentän arvoa yhdellä aina jokaista pakettia kohden. Täten TACACS+-asiakkaat lähettävät aina paketteja, joiden sarjanumero on pariton, ja TACACS+-palvelimet paketteja, joissa sarjanumero on parillinen. (Carrel & Grant 1997, 5)

Lippukentässä märitellään, onko TACACS+-viesti salaamaton vai salattu. Mikäli paketin arvo 0x01 (TAC_PLUS_UNENCRYPTED_FLAG) on päällä, viestin sisältöä ei salata. Vastaavasti mikäli lippukenttä on tyhjä, TACACS+-viesti lähetetään suojattuna. Suojaamattomat TACACS+-viestit on tarkoitettu vain testaukseen eikä niitä suositella käytettäväksi toimivassa verkossa. Kentän arvo 0x04 (TAC_PLUS_SINGLE_CONNECT_FLAG) kertoo TCP yhteyden kanavoinnista. Jos NAS-laite asettaa lipun arvon, se tarkoittaa, että laite tukee useaa samanaikaista TACACS-istuntoa yhdellä TCP-yhteydellä. (Carrel & Grant 1997, 5)

Istuntotunnus-kentässä sijaitsee TACACS+-istunnon tunnus. Tunnuksen on oltava aina satunnaisesti valittu. Tämä tunnus ei muutu TACACS+-istunnon aikana. Tämän arvon täytyy olla salaustekniikaltaan vahva, sillä muutoin se asettaa protokollan turvallisuuden kyseenalaiseksi. (Carrel & Grant 1997, 6)

Pituuskenttä pitää sisällään TACACS+-paketin koko pituuden. Kenttä ei kuitenkaan pidä sisällään TACACS+-otsikon pituutta, koska se on aina kahdentoista tavun mittainen. (Carrel & Grant 1997, 6)

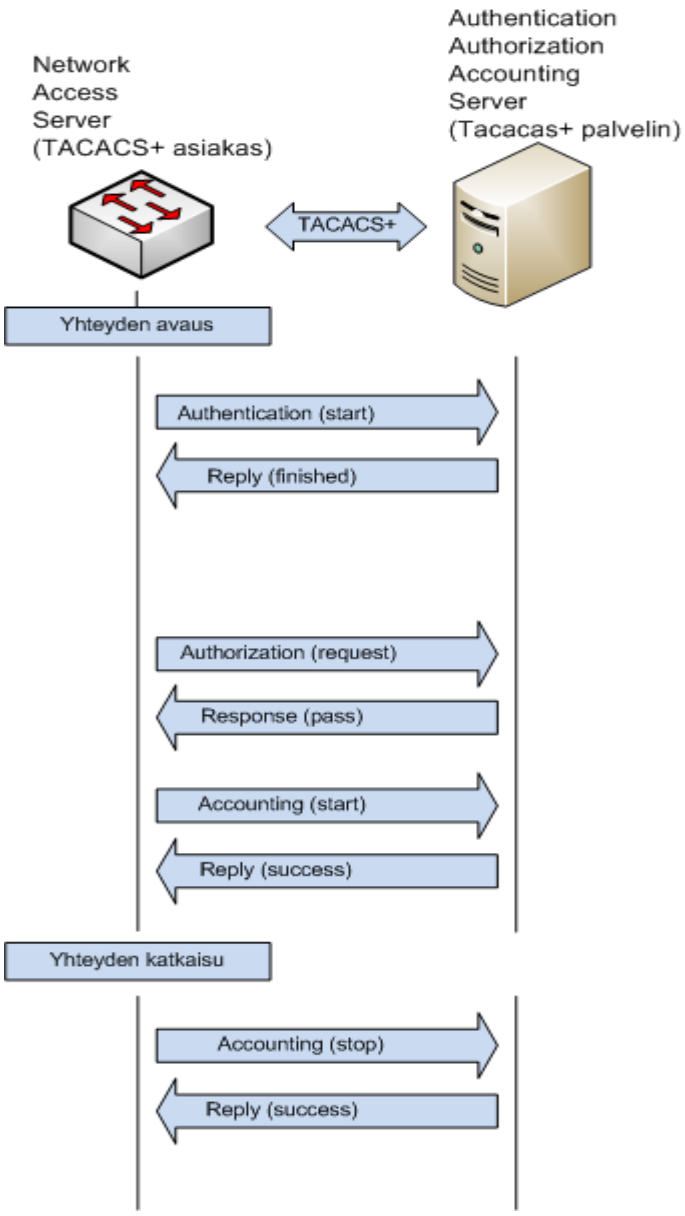
5.1.2 TACACS+ autentikointiprosessi

Autentikointiprosessi alkaa, kun käyttäjä ottaa yhteyden laitteeseen. Ensiksi häneltä kysytään käyttäjätunnus ja salasana. Käyttäjä antaa tunnuksen ja salasanan NAS laitteelle. NAS toimii asiakkaana ja lähettää TACACS+-palvelimelle authentication (start)-viestin. Viesti pitää sisällään käyttäjän antaman käyttäjätunnuksen ja salasanan. Tunnuksen ja salasanan oikeaksi todennuksen jälkeen TACACS+-palvelin lähettää Reply (Finished)-viestin NAS-laitteelle. (The Internet NG Project, TACACS+)

Kun käyttäjä on tunnistettu, NAS pyytää käyttäjältä valtuutustietoja. Käyttäjä vastaa NAS-laitteelle. Saatuaan tiedot NAS lähettää Authorization (request) viestin palvelimelle. Palvelin vastaa Response (Pass)-viestillä. Viesti pitää sisällään pyydetyn valtuutustiedon. (The Internet NG Project, TACACS+)

Viimeiseksi NAS lähettää palvelimelle Accounting (start)-viestin. Viesti ilmoittaa, että käyttäjä on kirjautunut verkkoon. Palvelin vastaa Reply (success)-viestillä, joka kertoo NAS-laitteelle, että kirjanpitoviesti on onnistuneesti tallennettu. (The Internet NG Project, TACACS+)

Käyttäjän katkaistaessa yhteyden NAS lähettää TACACS+-palvelimelle Accounting (stop)-viestin. Viesti sisältää tiedot käyttäjän kirjautumisen aloitus- ja lopetusajasta, lähetettyjen ja vastaanotettujen tavujen määrän, lähetettyjen ja vastaanotettujen pakettien määrän sekä syyn, miksi käyttäjä kytkeytyi irti verkosta. Palvelin vastaa NAS-laitteelle Reply (success)-viestillä, joka kertoo NAS-laitteelle, että kirjanpitoviesti on onnistuneesti tallennettu. (The Internet NG Project, TACACS+)



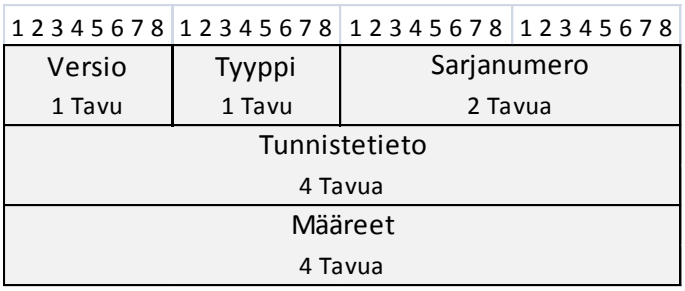
Kuva 10. TACACS+ autentikoitiprosessi

5.2 RADIUS

RADIUS on käyttäjien tunnistamiseen, valtuutukseen ja tilastointiin käytettävä protokolla joka toimii asiakas-palvelin-periaatteella. Asiakaslaite on yleensä kytkin tai reititin. RADIUS-palvelin on ohjelmisto, joka toimii esim. Windows-palvelimessa. Asiakaslaitteen ja RADIUS-palvelimen välinen liikenne toimii UDP-protokollalla. Tästä johtuen RADIUSta pidetään yleisesti yhteydettömänä protokollana. Palvelimen ja asiakaslaitteen välinen liikenne tunnistetaan jaetun salausavaimen kautta. Avainta ei koskaan lähetetä verkon yli vaan se määritellään sekä palvelimeen että asiakaslaitteeseen paikallisesti. (How does RADIUS work? 2006)

5.2.1 RADIUS-viestin rakenne

RADIUS-viesti noudattaa aina kuvassa 11 esitettyä rakennetta. Viestin rakenne on vakio lukuun ottamatta viimeistä kenttää. Viimeisen kentän pituus vaihtelee sen mukaan, mitä tietoja kulloinkin asiakkaan ja palvelimen välillä lähetetään.



Kuva11. RADIUS-paketin rakenne

Ensimmäisenä viestissä on tyyppikenttä, joka on yhden oktetin pituinen. Se määrittää paketin tyypin. Mikäli paketilla on väärä tyyppikenttä, se pudotetaan pois. Kentän arvo 1 on pääsynpyyntöviesti (Access-Request). Arvo 2 on pääsynsallintaviesti (Access-Accept). Arvo 3 on pääsynestoviesti (Access-Reject). Arvo 4 on tilastoinninpyyntöviesti (Accounting-Request). Arvo 5 on tilastoinnin vastausviesti (Accounting-Response). Arvo 11 on haasteviesti (Access-Challenge). (Rigney 2000)

Tunnistekenttä on myös yhden oktetin pituinen. Sitä käytetään yhdistämään oikeat pyyntö- ja vastausviestit. RADIUS-palvelin voi tunnistaa päällekkäiset viestit, mikäli viestien lähdeosoitteet ja -portit sekä tunnistekentät ovat samat lyhyen aikavälin sisällä. (Rigney 2000)

Pituuskenttä on 2 oktettia. Se määrittää paketin pituuden sisältäen kaikki kentät. Paketin minimipituus on 20 ja maksimipituus 4096 oktettia. Mikäli paketti on pitempi kuin pituuskentän ilmoittava arvo, kaikki määritellyn pituuden ylittävät kentät jätetään huomiotta. Jos paketti on lyhyempi kuin pituuskentän ilmoittava arvo, koko paketti hylätään. (Rigney 2000)

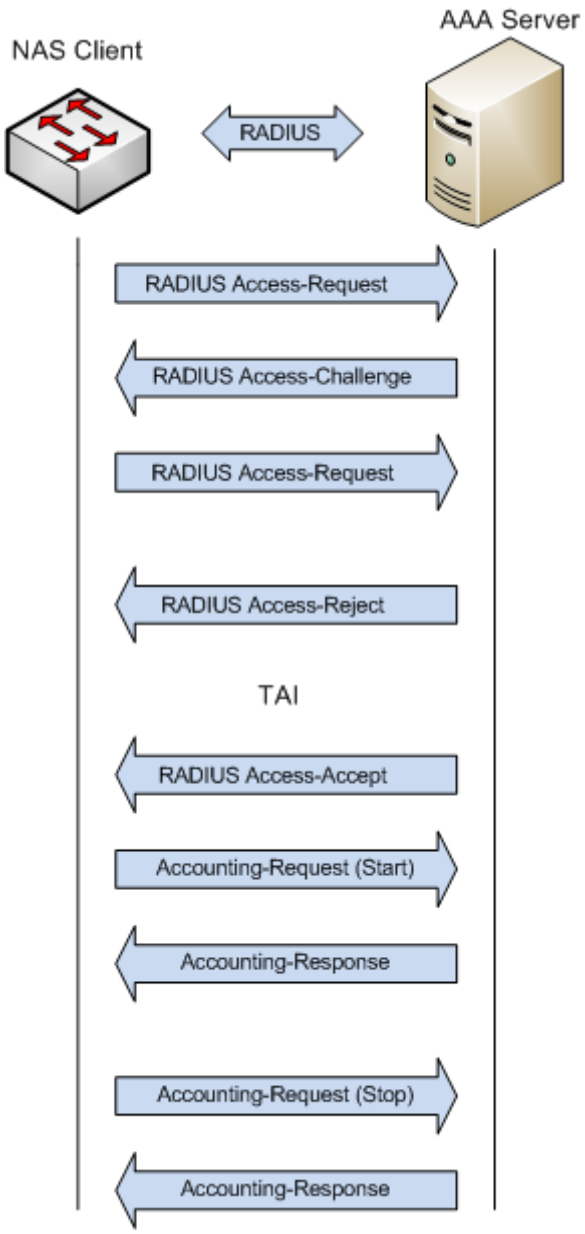
Tunnistetietokenttä on 16 oktettia pitkä, ja palvelin ja asiakas käyttävät sitä toistensa tunnistamiseen. (The RADIUS Protocol 2000)

Määreet-kenttä on vaihtelevan pituinen. Se sisältää monenlaisia tietoja, joita käytetään muun muassa tunnistukseen, valtuutukseen, tilastointiin ja yhteydenmuodostukseen. (Rigney 2000)

5.2.2 RADIUS-autentikointiprosessi

RADIUS-protokollassa käyttäjän tunnistus ja valtuutus on liitetty yhteen, toisin kuin TACACSissa. RADIUS-palvelin tukee useaa erityyppistä käyttäjäntunnistusmenetelmää (mm. PPP, PAP ja CHAP). Käyttäjän tunnistus perustuu asiakaslaitteen pyyntöviestiin (Access-request) ja palvelimen vastausviestiin (Access-accept tai Access-reject). Pyyntöviesti sisältää käyttäjänimen, salatun salasanan, asiakaslaitteen IP-osoitteen sekä portin. (How does RADIUS work? 2006)

Saatuaan pyyntöviestin palvelin etsii käyttäjänimeä tietokannastaan. Mikäli käyttäjänimeä ei löydy, ladataan joko jokin perusprofiili tai lähetetään asiakaslaitteelle pääsynestoviesti (Access-reject). Pääsynestoviestissä voi olla käyttäjälle viesti, joka kertoo pääsyneston syyn. Mikäli käyttäjänimi löytyy tietokannasta, palvelin lähettää pääsynsallintaviestin (Access-accept). Viestissä on määritelty käyttäjän oikeudet, palvelun tyyppi, käytettävä protokolla ja käyttäjälle annettava IP-osoite. Viesti voi myös sisältää tiedon käytettävästä pääsylistasta tai staattisesta reitistä, joka lisätään asiakaslaitteen reititystauluun. (How does RADIUS work? 2006)



Kuva 12. RADIUS-protokollan yhteydenmuodostus

5.3 TACACS+ ja RADIUS protokollien vertailu

Seuraavassa on vertailtu edellä käsiteltyjä protokollia. TACACS+ käyttää TCP-protokollaa ja RADIUS UDP-protokollaa. TCP:n etuna on se, että se on yhteydellinen protokolla. UDP sitä vastoin on yhteydetön protokolla.

RADIUS salaa vain salasanan access-request paketissa asiakaskoneelta palvelimelle. Muut paketit ovat suojaamattomia ja muut tiedot, kuten käyttäjänimi, valtuutus palvelut ja kirjanpito, ovat kaapattavissa. TACACS+ taas salaa viestin rungon mutta jättää otsikon salaamatta.

	TACACS+	RADIUS
Yhteys protokolla	TCP	UDP
Portti	49	1812 & 1813
Salaus	Koko paketti	Vain salasanat
AAA arkkitehtuuri	Eri palvelut jokaiselle AAA:n osalle	Tunnistus ja valtuutus yhdessä palvelussa
Käyttötarkoitus	Verkkolaitteiden hallinta	Käyttäjien hallinta

Taulukko 1. TACACS+- ja RADIUS-protokollien vertailu

6 KÄYTÄNNÖN TUTKIMUS JA TOTEUTUS

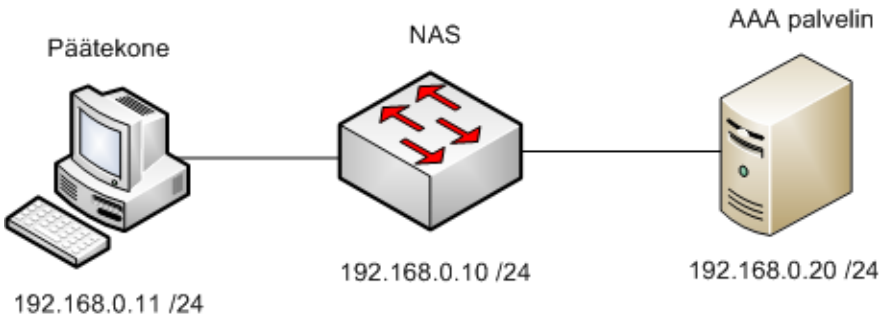
Etäkäyttäjän varmentamista tutkittiin Kymenlaakson ammattikorkeakoulun tietoliikennelaboratoriossa. Tarkoituksena oli kehittää esimerkkiratkaisu, jolla etäkäyttäjän varmennus voitiin toteuttaa Kotkan kaupungin tietoliikenneverkkoon.

Tässä luvussa on kuvattu esimerkin avulla sitä, kuinka verkkolaitteen etäkäyttäjän todentaminen on toteutettu. Kytkennässä käytetyt IP-osoitteet ja salausavaimet ovat keksittyjä ja kytkentä on simuloitu Kymenlaakson ammattikorkeakoulun tietoliikennelaboratoriossa. Tämä esimerkkikytkentä ei liity mitenkään Kotkan kaupungin verkkoon tai siellä käytössä oleviin ratkaisuihin.

6.1 Kytkennän esittely

Kytkennässä käytettiin yhtä Ciscon Catalyst 2960 LAN -kytkintä, yhtä päätetyöasemaa Windows XP -käyttöjärjestelmällä sekä yhtä AAA-palvelinta Windows 2003 -käyttöjärjestelmällä.

Kytkennän toimintana on käyttäjän ottaessa etähallintayhteyden kytkimeen varmentaa käyttäjä ACS-palvelimen tietokannasta. Käyttäjä kirjautuu suoraan kytkimen EXEC tilaan käyttäjätasolla 15.



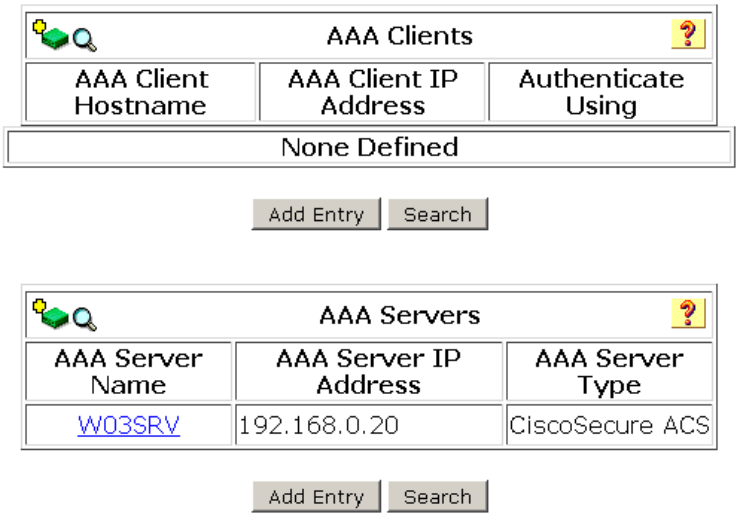
Kuva 13. Laboratorioon rakennettu kytkentä

6.2 Kytkimen sekä ACS-palvelimen konfigurointi

Seuraavassa käydään läpi kuinka konfiguroidaan ACS palvelin sekä kytkin niin, että otettaessa päätekoneelta etäyhteys kytkimeen käyttäjä kirjautuu ACS palvelimella olevilla tunnuksilla suoraan käyttäjätasolle 15.

6.2.1 ACS palvelimen konfigurointi

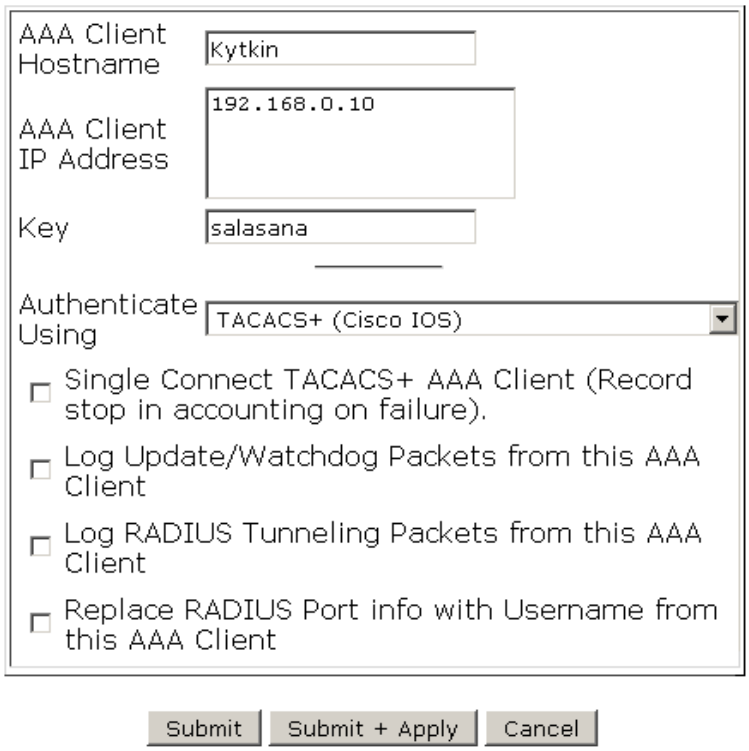
Ensiksi ACS-palvelimeen lisätään AAA-asiakkaan eli kytkimen tiedot. Vasemmasta valikosta valitaan Network Configuration. Aukeavasta valikosta valitaan AAA Clients -otsikon alta Add Entry.



Kuva 14. AAA asiakaslaitteen lisääminen ACS-tietokantaan

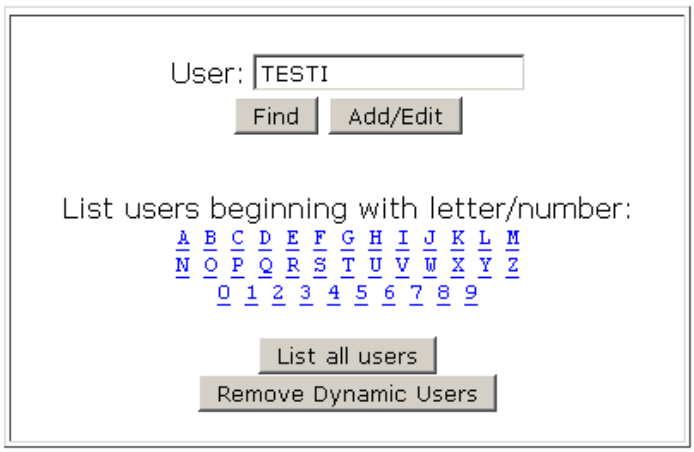
Lisätään AAA-asiakkaan nimeksi Kytkin, IP-osoitteeksi 192.168.0.10 ja avain-kenttään salasana. Laitteelle annettavan nimen ei tarvitse olla sama kuin itse laitteen,

koska ACS tunnistaa laitteen sen IP-osoitteen perusteella. Asetukset tallennetaan Submit + Apply -painikkeella.



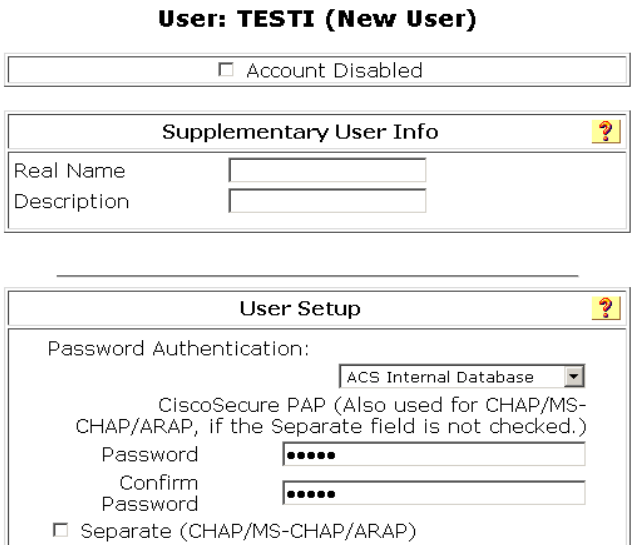
Kuva 15. ACS tietokantaan liitettävän kytkimen asetukset

Seuraavaksi ACS-palvelimelle määritellään käyttäjätunnus ja salasana, jolla kytkimeen kirjaudutaan. Vasemmasta valikosta valitaan User Setup. Käyttäjätunnus TESTI kirjoitetaan User-kenttään ja lisätään se ACS-tietokantaan Add/Edit-painikkeella.



Kuva 16. Käyttäjän lisääminen ACS-tietokantaan

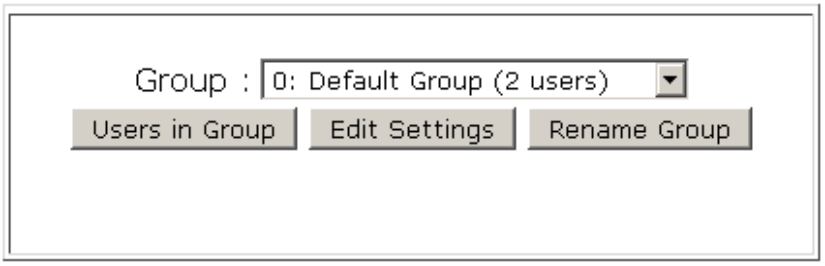
Seuraavaksi käyttäjälle määritetään salasana TESTI. Tämä lisätään password-kenttään ja tiedot tallennetaan Submit painikkeella.



Kuva 17. Käyttäjän salasanan määritys

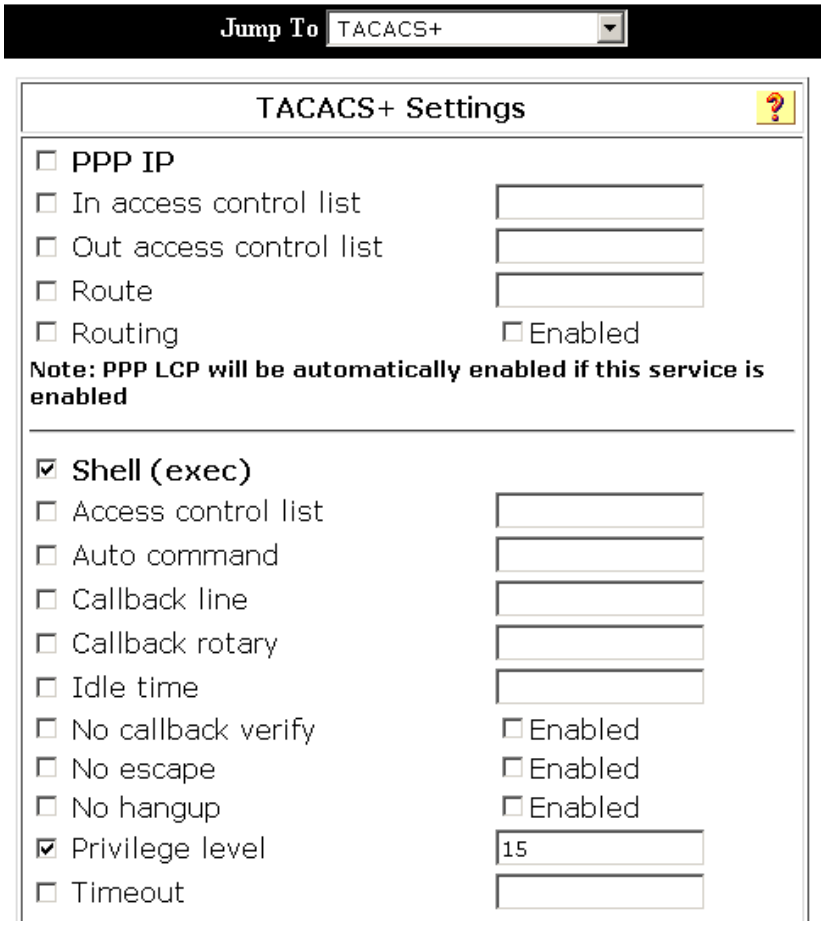
Nyt ACS-tietokannassa on käyttäjätunnus TESTI, jonka salasana on TESTI. Kytkimeen kirjaudutaan nyt käyttäen tätä käyttäjätunnusta ja salasanaa.

Kolmanneksi muutetaan käyttäjäryhmän asetuksia niin, että kirjautuminen tapahtuu suoraan EXEC-tilaan. Valikosta valitaan Group Setup. Listasta valitaan default group, minkä jälkeen painetaan Edit settings -painiketta.



Kuva 18. Käyttäjäryhmän valinta

Yläreunan jump-valikosta valitaan TACACS+. TACACS+ Settings valikosta asetetaan päälle Shell (exec) ja Privilege level. Privilege level -arvoksi annetaan 15.



Kuva 19. Käyttäjäryhmän TACACS+ asetukset

6.2.2 Kytkimen konfigurointi

Tässä luvussa käydään läpi kytkimen konfigurointi niin, että käyttäjä kirjautuu sisään ACS-palvelimella olevalla käyttäjätunnuksella. Mikäli palvelimeen ei saada yhteyttä, kytkimeen kirjaudutaan käyttäen paikallista tunnusta. Lähtökohtana on tyhjä kytkin, jossa ei ole minkäänlaista konfiguraatiota.

Ensiksi kytkimeen määritetään verkonhallinta vlan 50. Tähän vlaniin määritellään hallinta-IP-osoite ja liitetään liityntäportit. Luodaan myös paikallinen tunnus. Tätä käytetään, mikäli autentikointipalvelimeen ei saada yhteyttä.

switch#vlan database

switch(vlan)#vlan 50 name testi_vlan

switch(config)#interface vlan 50

switch(config-if)#ip address 192.168.0.10 255.255.255.0

switch(config)#interface range f0/1 - 2

switch(config-if)#switchport mode access

switch(config-if)#switchport access vlan 50

switch(config)#username cisco privilege 15 password cisco

Seuraavaksi otetaan käyttöön AAA ja konfiguroidaan kytkin vastaanottamaan todennus- ja valtuutustiedot AAA-palvelimelta. Tämä mahdollistaa sen että kytkimeen on mahdollista kirjautua hallintayhteydellä vain niillä tunnuksilla, jotka on määritelty AAA-palvelimen tietokantaan. NAS-laitteen ja AAA-palvelimen välille muodostettavaan yhteyteen käytetään samaa salasanaa, jotta laitteet tunnistavat toisensa. None-parametri takaa sen, että kytkimeen on mahdollista kirjautua ilman AAA-palvelinta ja paikallista tunnusta. Näin menetellään siksi, että ei pääse muodostumaan tilannetta, että kytkimeen ei pysty mitenkään kirjautumaan.

switch(config)#aaa new-model

switch(config)#aaa authentication login TELNET group tacacs+ local none

switch(config)#aaa authorization exec TELNET group tacacs+ local none

switch(config)#tacacs-server host 192.168.0.10 key salasana

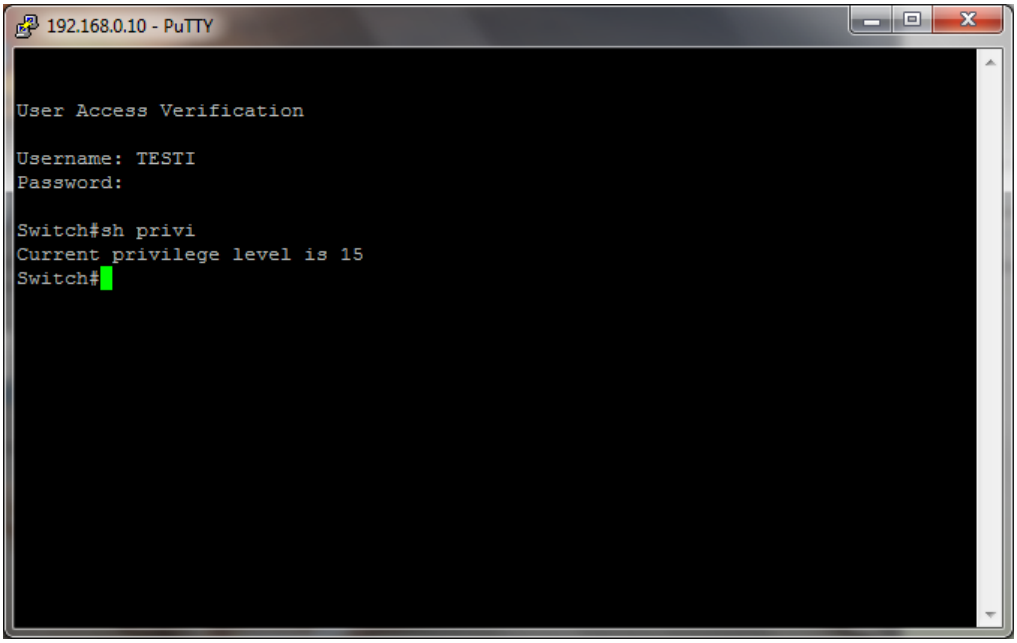
Seuraavaksi todennus ja valtuutus listat liitetään kytkimen vty-linjaan.

switch(config)#line vty 0 4

switch(config-line)#login authentication TELNET

switch(config-line)#authorization exec TELNET

Kytkennän toimivuus on testattavissa ottamalla päätekoneelta telnet-yhteys kytkimeen. Kytkimen kysyessä käyttäjätunnusta ja salasanaa käytetään ACS:ään määritettyä tunnusta TESTI.



Kuva 20. Kirjautuminen kytkimeen käyttäen ACS-palvelimella olevaa TESTI käyttäjätunnusta.

7 JATKOKEHITTELY

Tässä luvussa on käyty läpi ideoita, joita syntyi työn aikana. AAA:n toiminnan vakaus ja palvelun saatavuus on erittäin tärkeää, joten autenikointipalvelimen kahdennus tuli ensisijaisena mieleen. Myös dot1x eli porttikohtainen käyttäjän autentikointi parantaisi merkittävästi verkon tietoturvaa.

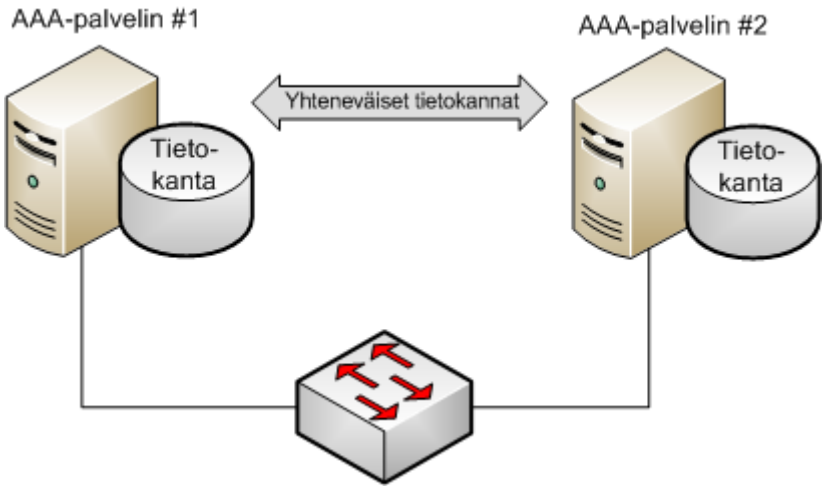
7.1 Palvelimen kahdennus

Mahdollisten vikatilojen varalta käyttöön otettu autentikointipalvelin olisi hyvä kahdentaa. Tämä tarkoittaa sitä, että palvelimesta tehdään toissijainen kopio, joka sijoitetaan johonkin toiseen laitetilaan. Mikäli käytössä oleva ensisijainen palvelin hajoaa, autentikointipalvelut siirtyvät toissijaisen palvelimen tehtäväksi. Tämä lisää verkon

toimintaan sekä varmuutta että joustavuutta, koska toiseen palvelimeen voidaan tehdä katkoksia aiheuttavia huoltoja tai päivityksiä ilman, että palveluun tulee katkoksia.

Varmistuspalvelin täytyy sijoittaa eri laitetilaan, kuin missä ensisijainen palvelin on. Tämä johtuu siitä, että esim. mahdollinen tulipalo tuhoaisi molemmat palvelimet ja kahdennuksesta ei olisi mitään hyötyä.

Mikäli autentikointipalvelimeen ei saada yhteyttä, verkkolaitteeseen kirjautuva käyttäjä ei pääse kirjautumaan sisään autentikointipalvelimeen määritetyillä tunnuksilla. Kytkimiin on mahdollista tehdä määrittelyt, jotka mahdollistavat laitteeseen pääsyn myös ilman autentikointipalvelinta.



Kuva 21. Palvelimen kahdennuksen periaatekuva

7.2 802.1X-autentikointi

IEEE-protokolla 802.1X tarjoaa mahdollisuuden porttikohtaiseen autentikointiin. Protokolla toimii RADIUS-protokollan kanssa, keskittyen näin käyttäjien autentikointiin. Käyttäjältä vaaditaan autentikointia aina hänen yrittäessä ottaa yhteyttä verkkoon eikä vain silloin, kun käyttäjä aikoo hallita verkon laitteita. Tämä parantaa verkon tietoturvaa huomattavasti. Kun kaikki verkon laitteet ovat konfiguroitu käyttämään 802.1X-protokollaa, ei ole väliä, mistä kohtaa verkkoa käyttäjä yrittää verkkoon päästä. Koska autentikointi on porttikohtaista, voidaan hyvin tarkkaan määritellä, missä autentikointia käytetään.

Verkkolaitteiden täytyy tukea 802.1X-protokollaa, jotta porttikohtainen autentikointi toimisi. Käyttöönotto on melko yksinkertaista, mutta suurissa verkoissa se voi tarkoittaa paljon työtä. Kaikki verkkolaitteet, joihin halutaan porttikohtainen autentikointi, on konfiguroitava erikseen. Koska 802.1X käyttää RADIUS-protokollaa, täytyy verkossa olla RADIUS-palvelin. Mikäli verkossa ei palvelinta ole, se hankaloittaa käyttöönottoa. Työtä tulee lisää ja mahdolliset palvelimenhankintakustannukset täytyy ottaa huomioon. Ehdoton vaatimus 802.1X:n toiminnalle verkossa on se, että autentikointipalvelin tukee EAP-protokollaa.

Verkon käyttäjälle porttikohtainen autentikointi voi tuntua rasitteelta. Käyttäjän täytyisi aina antaa käyttäjänimi ja salasana ottaessaan yhteyttä verkkoon. Verkon tietoturva paranee huomattavasti 802.1X:n käyttöönoton myötä. Täytyy vain miettiä, vaikuttaako lisääntynyt tietoturva liikaa verkon sujuvaan käyttöön.

8 LOPPUPÄÄTELMÄT

Verkonhallinta on haastavaa, kun kyseessä on suuri verkko. Tarvitaan useampi henkilö hallintatehtäviin, jotta tarvittavat muutokset ja vikojen korjaukset ovat toteutettavissa nopealla aikataululla. Mitä useampi henkilö tietää verkkolaitteen käyttäjätunnuksen ja salasanan, sitä tärkeämpää on vaihtaa ne tietyin väliajoin. Mikäli verkkoa hallinnoi useita henkilöitä, kaikki eivät välttämättä tarvitse käyttöön kaikkia komentoja. Näille käyttäjille on hyvä luoda erillinen käyttäjätaso, johon on määritelty vain ne komennot, joita he tarvitsevat.

Usean käyttäjän hallinnoimassa verkossa pääkäyttäjän on tiedettävä, mitä muutoksia verkon toimintaan on tehty. Mahdollisen vikatilanteen kohdalla pääkäyttäjän on tärkeää tietää, mitä muutoksia verkkoon on tehty ja kuka muutokset on tehnyt.

Jokaisessa verkkolaitteessa on konfiguroitu käyttäjätunnukset sekä käyttäjätasot. Käyttäjätunnuksien vaihto tai komentojen muokkaus on tehtävä jokaiseen laitteeseen yksi kerrallaan. Pienissä verkoissa tässä ei mene kauan, mutta suurissa verkoissa käyttäjätunnusten ja komentolistojen muokkaaminen vie kauan.

Autentikointipalvelin tarjoaa keskitetyn tietokannan käyttäjille. Se korvaa yhden käyttäjätunnuksen jokaisen käyttäjän omalla tunnuksella. Palvelin helpottaa verkon pääkäyttäjän työtä, koska kaikki käyttäjätiedot ovat yhdessä paikassa. Tunnusten lisääminen, poistaminen tai muuttaminen onnistuu yhdestä paikasta. Mikäli käyttäjien oikeudet määritellään palvelimelta, voidaan tarpeen vaatiessa joko lisätä tai poistaa käyttöoikeuksia. Muutoksia ei tarvitse tehdä jokaiseen verkkolaitteeseen vaan riittää, että muutokset tehdään palvelimen tietokantaan.

9 LÄHTEET

ACS Shell Command Authorization Set. Cisco Systems Inc. 2007. Saatavilla: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_configuration_example09186a00808d9138.shtml [Viitattu 5.11.2009]

Anttila, Aki.2000. TCP/IP-tekniikka. Juva: WSOY

Baccala, B. SNMP Protocol Overview. 1997. Saatavilla: http://www.freesoft.org/CIE/Topics/108.htm [Viitattu 23.10.2009]

Carrel,D., Grant, L. 1997. Network Working Group, TACACS+ protocol. Saatavissa: http://tools.ietf.org/html/draft-grant-tacacs-02 [viitattu 4.11.2009]

Carroll, Brandon. 2004. Cisco Access Control Security: AAA administration Services. Indianapolis: Cisco Press

Cryptography – Secure Shell. Kioskea.net. 2008 Saatavilla: http://en.kioskea.net/contents/crypto/ssh.php3 [Viitattu 27.10.2009]

David,D. 2005. Understand the levels of privilege in the Cisco IOS. Saatavissa: http://articles.techrepublic.com.com/5100-10878_11-5659259.html [Viitattu 21.10.2009]

How does RADIUS work? Cisco Systems Inc. 2006. Saatavilla: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml [Viitattu 27.10.2009]

Huntington 2009. The Business of Authentication. Saatavissa: http://www.authenticationworld.com/ [viitattu 4.11.2009]

Kozierok, C. SNMP Basic Request/Response Information Poll. 2005a Saatavilla: http://www.tcpipguide.com/free/t_SNMPProtocolBasicRequestResponseInformationPollUsi.htm [Viitattu 23.10.2009]

Kozierok, C. Telnet Connections and Client/Server Operation. 2005b Saatavilla: http://www.tcpipguide.com/free/t_TelnetConnectionsandClientServerOperation.htm [Viitattu 30.9.2009]

Kozierok, C. Telnet Communications Model and the NVT. 2005c Saatavilla: http://www.tcpipguide.com/free/t_TelnetConnectionsandClientServerOperation.htm [Viitattu 30.9.2009]

OutPost Sentinel. Saatavissa: http://www.outpostsentinel.com/inband.shtml [viitattu 12.10.2009]

Rigney, C. 2000. Remote Authentication Dial In User Service. Saatavilla: http://www.faqs.org/rfcs/rfc2865.html [Viitattu 27.10.2009]

Role-Based CLI Access. Cisco Systems Inc. Saatavilla: http://www.cisco.mn/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.pdf [viitattu 4.11.2009]

SSH Protocol. Red Hat Inc. 2002. Saatavilla: http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/ref-guide/ch-ssh.html [Viitattu 27.10.2009]

The Internet NG Project, TACACS+. Saatavissa: http://ing.ctit.utwente.nl/WU5/D5.1/Technology/tacacs+/ [viitattu 4.11.2009]

The RADIUS Protocol. Microsoft Corporation. 2000. Saatavilla: http://technet.microsoft.com/en-us/library/bb742390.aspx [Viitattu 27.10.2009]

Thomas, Tom. 2005. Verkkojen tietoturva: perusteet. Helsinki: Edita Prima Oy

User Guide for Cisco Secure ACS Control Server. Cisco Systmes Inc.2007. Saatavilla: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/ACSugP.pdf [Viitattu 6.11.2009]

Using the Cisco Web Browser. Cisco Systems Inc. Saatavilla: http://www.cisco.com/en/US/docs/ios/12_0/configfun/configuration/guide/fcweb.pdf [Vittattu 4.11.2009]

WTI. Out of Band Network Managementi In The Data Center. Saatavissa: http://www.wti.com/wti-white-paper-oobdc.html [Viitattu 12.10.2009]