NETWORK POLICY SERVER

NPS-käyttöönotto Keravan kaupungilla

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietoliikennetekniikka

Riihimäki, 17.11.2011

Timo-Heikki Pöyhtäri

HAMK
HÄMEEN AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

Tietoliikennetekniikka
Riihimäki

Työn nimi	NPS-käyttöönotto
Tekijä	Timo-Heikki Pöyhtäri
Ohjaava opettaja	Raimo Hälinen
Hyväksytty	17.11.2011
Hyväksyjä	

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Riihimäki
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Tekijä Timo-Heikki Pöyhtäri **Vuosi** 2011

Työn nimi Network Policy Serverin käyttöönottaminen

TIIVISTELMÄ

Opinnäytetyön tavoitteena on saada NPS-palvelu toimimaan Keravan kaupungin opetuspuolen langattomassa verkossa jotta uusi Active Direcotory voitaisiin ottaa käyttöön.

Työni toimeksiantaja toimi Keravan kaupunki Tietotekniikan palvelukeskus, jossa suoritin opintoihini liittyvän työharjoittelun.

Työn teoriaosuus kertoo Active Directorystä sekä NPS-palvelusta.

Työn tuloksena sain konfiguroitua toimivan langattoman ympäristön Keravan kaupungin tietoverkkoon.

Avainsanat Windows Server 2008, NPS, langattomat lähiverkot, palvelimet

Sivut 18 s, + liitteet 2 s.

Riihimäki
Degree Programme in Information Technology
Information Technology

Author Timo-Heikki Pöyhtäri **Year** 2011

Subject of Bachelor's thesis **Network Policy Server installation**

ABSTRACT

The purpose of my thesis was to get NPS-service to work in the wireless network of the educational side of the city of Kerava, in order to take in use the new Active Directory. My thesis writing was commissioned by the city of Kerava information technology service center, in which I conducted my studies related work practice.

The theory part of my thesis consists of Active Directory and NPS-service. As a result of my work I was able to configurate the fully functional wireless environment in the information network of the city of Kerava.

Keywords Windows Server 2008, NPS, WLAN, server

Pages 18 p + appendices 2 p.

SISÄLLYS

1 JOHDANTO

Aiheen opinnäytetyöksi sain Petri Grönbergiltä suorittaessani opintoihini liittyvää työharjoittelua Keravan kaupungin tietotekniikan palvelukeskuksessa.

Opinnäytetyön tarkoituksena on tutkia, onko mahdollista saada NPS palvelu toimimaan kunnolla Keravan kaupungin kouluverkossa. Kyseisellä palvelulla voidaan parantaa langatonta tietoturvaa koulujen verkossa ja samalla ottaa käyttöön automatisoitu ja keskitetty työasemien langattomien verkkojen käytön hallinta.

Opinnäytetyössä kohtasin monia ongelmia, johtuen siitä että työ tuli suoraan käytäntöön olemassa olevaan ympäristöön, ei testikäyttöön. Keravan kaupungin uusi Active Directory ei olisi tullut käyttöön ilman tätä palvelua, eikä tämä palvelu olisi tullut käyttöön ilman uutta Active Directory palvelua. Tämän takia näitä molempia kehitettiin samanaikaisesti joka toi omat haasteensa mm. kehitystiimien aikataulujen kanssa.

2 MICROSOFT ACTIVE DIRECTORY

2.1 Active Directory yleisesti

Active Directory (AD) on Microsoftin kehittämä käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja sovelluksista sekä jakaa tietoa käyttäjille, tietokoneille sekä sovelluksille. Esimerkiksi jokaisella käyttäjälle ei tarvitse asentaa omaa tulostinta vaan he voivat käyttää esim. organisaatioyksikkönsä yhteistä verkkotulostinta tai verkkolevyä.

2.2 Network Policy Server

Network Policy Server on palvelu, jota käytetään käyttäjien autentikointiin ja työasemien turvallisuuden tarkkailuun. Palvelulla voidaan esimerkiksi tarkastaa tietokoneen virusturvan tila, onko mitään virustorjuntaohjelmistoa asennettu ja onko se ajan tasalla. Mahdollisia toimenpiteitä on eri virtuaalisiin verkkoihin liittäminen tai verkon käytön esto.

NPS palvelu sisältyy Windows Server 2008 – palvelimeen. Sen rooli pitää kuitenkin asentaa koska se ei oletuksena ole asennettuna.

2.3 Radius palvelin

RADIUS -protokolla (Remote Authentication Dial In User Service) on aikoinaan suunniteltu sisäänsoittopalveluissa tapahtuvaan tunnistukseen, jossa se on nykyäänkin laajassa käytössä.

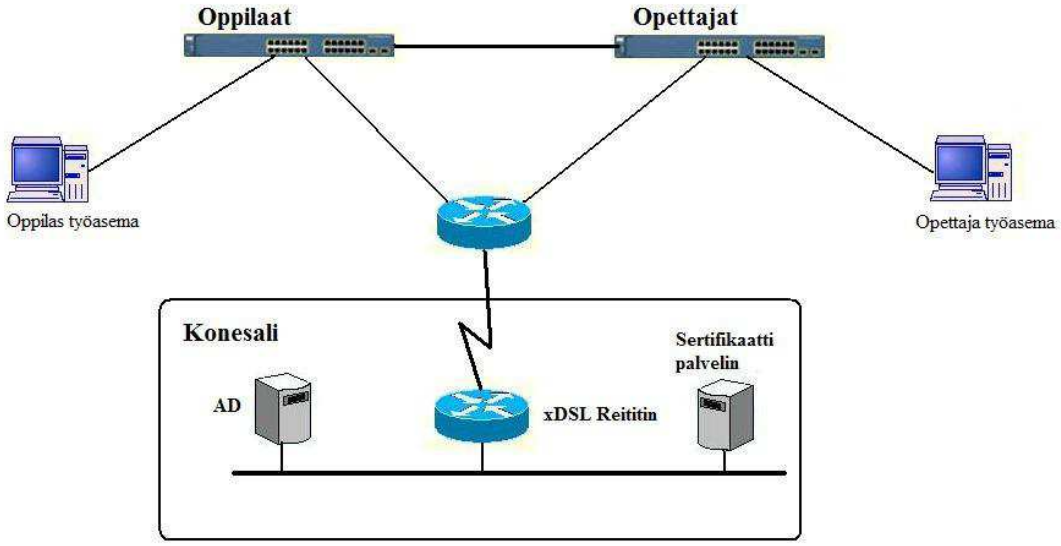
3 VERKKO

Tässä osiossa kerron verkon rakenteesta sekä toiminnasta.

3.1 Verkon rakenne

Alla olevaan kuvaan on piirretty verkon rakenne, josta näkee että oppilas ja opettajaverkko on erotettu toisistaan.

Opetuspuolen koneen käynnistyessä kone ottaa ensin yhteyden sertifikaattipalvelimelle. Palvelin ottaa yhteyden AD:lle ja tarkistaa kyseisen koneen toimialueen. Konetietojen ollessa kunnossa opettajatyöasema pääsee opetusverkkoon.



Kuva 1 Verkon rakenne

4 NPS KÄYTTÖÖNOTTO

Tässä osiossa kerron NPS-palvelun käyttöönoton eri vaiheet.

4.1 NPS-palvelun asennus NPSPALVELIN–palvelimelle

Aloitin työn asentamalla NPS-palvelun roolin NPSPALVELIN-palvelimelle, joka toimii virtuaalikoneena Keravan kaupungin opetusverkossa ja on jäsenkoneena uudessa AD:ssa. Virtuaalisointiin käytin WMware-nimistä ohjelmistoa.

Kirjauduin NPSPALVELIN -palvelimelle ja käynnistin Server Managerin. Valitsin Roles -> Add Roles ja lisäsin palvelimelle Network Policy and Access Services -rooli seuraavin asetuksin:

Taulukko 1 Network Policy and Access Services -rooli

Ikkuna	Asetus	Arvo
Network Policy and Access Services		
Select Role Services	Network Policy Server	Valitse

Lopuksi painoin ”Install”.

4.2 WLAN-asetusten määrittely työasemille keskitetysti

Tässä työvaiheessa kerron kuinka loin tarvittavat Group Policyt joiden avulla WLAN-asetukset levitetään työasemille.

Ensimmäiseksi käynnistin Active Directory Users and Computers- ohjelman jonne loin kaksi uutta universaalia tietoturvaryhmää toimialueen edutipake.lan Koneryhmät OU:hun nimeltään EPK_koneet_JANNPS_US ja EPK_koneet_KENPS_US, eli tein sekä Keravan kaupungille että Järvenpään kaupungille omat ryhmänsä.

Seuraavaksi tein universaalit tietoturvaryhmät toimialueelle eduker245.edutipake.lan\ryhmat\koneryhmät OU:n alle nimeltään EKE_koneet_NPS-US, EKE_koneet_XP-US ja EKE_koneet_Win7-US eli XP sekä Win7 koneille omat ryhmänsä, koska tällä tavoin voidaan jakaa XP-koneille omia paketteja ja Win7-koneille omia paketteja.

Tämän jälkeen liitin äsken luodut XP- ja Win7- ryhmät jäseneksi ryhmään EPK_koneet_NPS-US ja kyseinen ryhmän liitin jäseneksi tietoturvaryhmään EPK_koneet_KENPS_US.

Seuraava työvaihe oli Group Policyn luominen. Avasin Group Policy Management- hallintakonsolin, ja menin polkuun

Forest:edutipake.lan\Domains\eduker245.edutipake.lan\Työasemat –OU ja hiiren toisella näppäimellä valitsin
Create a GPO in this domain, and Link it here…
Group Policyt nimesin seuraavasti: EKE_NPSpolicy_XP_C ja EKE_NPSpolicy_Win7_C.

Tämän jälkeen aloin muokkaamaan äsken luotua XP-koneen Group Policyä valitsemalla sen ja menemällä Scope – välilehden Security Filtering kohtaan josta poistin Authenticated Users ja lisäsin EKE_koneet_XP-US –ryhmän. Samat muutokset tein myös WIN7 ryhmälle.
Seuraava työvaihe oli muokata EKE_NPSpolicy_XP_C Group Policyä. Valitsin kyseisen policyn ja hiiren toisella näppäimellä klikkasin Edit…, jolloin Group Policy Management Editor avautui. Siirryin polkuun Computer Configuration\Policies\Windows Settings\Security Settings\Wireless Network (IEEE 802.3) Policies, ja klikkasin hiiren toisella näppäimellä kohtaa Wireless Network (IEE 802.3) Policies ja valitsin Create A New Windows XP Policy. Määrittelin uuden XP Wireless Network Policyn oheisen taulukon mukaisesti:

Taulukko 2 XP Wireless Network Policy

Välilehti	Asetus	Arvo
General	Policy Name: Description Network to access: Use Windows WLAN Autoconfig service for clients	Eduker 245 Keravan Opetusverkko Access point (infrastructure) networks only Valittuna
Preferred Networks	Add… Infrastucture	
	New Preferred Setting Properties Network name (SSID) Connect even if network is not broadcasting Authentication: Encryption: IEEE 802.1X EAP Type: Settings…	 Opetus245 Valittuna WPA2 AES Microsoft: Protected EAP (PEAP)

	Validate server certicate Select Authentication method: Eapol-Start Message Authentication mode:	Ei valittuna Secure password (EAP-MSCHAP v2) Transmit Computer only

EKE_NPSpolicy_WIN7_C määritykset löytyvät seuraavasta taulukosta:

Taulukko 3 WIN7 Wireless Network Policy

Välilehti	Asetus	Arvo
General	Policy Name: Description Use Windows WLAN Autoconfig service for clients	Eduker 245 Keravan opetusverkko. Valittuna
General	Add… Infrastructure	
	New Preferred Setting Properties Profile Name: Network name (SSID) Connect automatically when this network is in range. Connect to a more preferred network if available. Connect even if network is not broadcasting Security Authentication: Encryption: Select a network authentication method: Properties… Validate server	 Opetus245 Opetus245 Valittuna Valittuna Valittuna WPA2-Enterprise AES Microsoft: Protected EAP (PEAP) Ei valittuna

	certicate Select Authentication method: Authentication mode: Advanced… Enforce advanced 802.1x settings	 Secure password (EAP-MSCHAP v2) Computer Authentication Valittuna
Network Permissions	Prevent connections to ad-hoc networks	Valittuna

Hallintopuolella on käytössä vastaava Wireless Network Policy, joten asetuksien pitää olla samat. Hallintopuolta ei alettu muokkaamaan tämän takia, joten tämä muokattiin sen mukaiseksi.

Seuraavilla asetuksilla saatiin tietoturvaa parannettua:

Vain tietokone tunnistautuminen:
Ainoastaan ne koneet jotka ovat Active Directory – tietokannassa pääsevät verkkoon.
Yhdistä vaikka verkko ei lähetä:
SSID voidaan piilottaa, jolloin asiattomat koneet eivät näe verkkoa.
AD-HOC – estetty: Nyt koneisiin ei voi murtautua helposti.

4.3 WLAN-controllerien esittely NPS –palvelimella

Tässä työvaiheessa kerron kuinka WLAN-controllerit esitellään radius-asiakkaaksi NPSPALVELIN –palvelimelle. Avataan Server Manager NPSPALVELIN – palvelimelta ja siirrytään seuraavaan polkuun:

Roles\Network Policy and Access Services\NPS (Local)\RADIUS Clients and Servers\RADIUS Clients

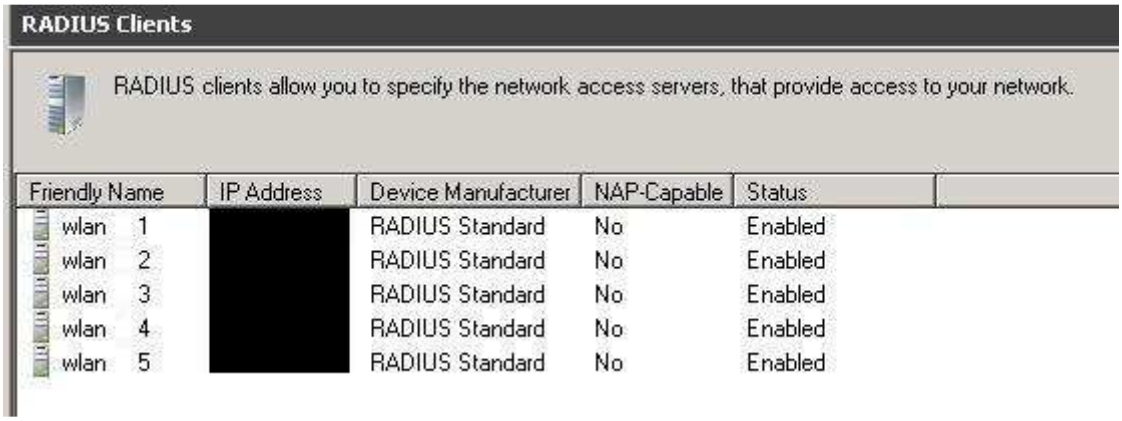
Napsautetaan hiiren oikealla toisella näppäimellä RADIUS Clients ja valitaan valikosta New.

Lisäsin seuraavat WLAN-controllerit Radius Clienteiksi. Salasanaksi laitoin salasana123.

Taulukko 4 WLAN-controllerit

Nimi	IP-osoite
wlan1	10.0.0.1
wlan2	10.0.0.2
wlan3	10.0.0.3

Alla olevassa kuvassa näkyy myös wlan4 ja wlan5. Nämä ovat Järvenpään kaupungin radius clientteja, jotka lisäsin palvelimelle että virhelokiin ei tulisi turhia virheilmoituksia.



Kuva 2 Radius Client –ikkuna. Kuvasta on piilotettu oikeat IP-osoitteet.

4.4 802.1X -konfiguraatio NPSPALVELIN – palvelimella

Tässä kohdassa kerron miten määrittelin NPSPALVELIN –palvelimella 802.1x –asetukset. Kirjauduin NPSPALVELIN – palvelimelle toimialueen pääkäyttäjänä ja käynnistin ohjelma inetmgr.exe. Avasin konsolin navigointipuussa NPSPALVELIN ja valitsin keskimmäisestä ikkunasta Server Certificates. Napsautin oikeasta reunasta Create Self-Signed Certificate ja nimesin sertifikaatin NPSPALVELIN NPS-varmenne. Viimeiseksi napsautin OK. Sertifikaatin voimassaoloajaksi annoin yhden vuoden, eli se vanhenee 27.5.2012 klo. 03:00.

Kuva 3 Valmis certifikaatti. Kuvasta on peitetty palvelimen nimi

Kun olin luonut sertifikaatin, pääsin viimeinkin tekemään NPS-asetuksia. Avasin Server Managerin (NPSPALVELIN)\Roles\Network Policy and Access Services\NPS (Local). Valitsin keskimmäisen ikkunan alavetovalikosta Radius server for802.1X Wireless or Wired Connections ja painoin Configure 802.1x. Määritin 802.1x – toiminnon käyttöön seuraavin asetuksin:

Taulukko 3

Ikkuna	Asetus	Arvo
Select 802.1X Connections Type	Secure Wireless Connections	
Specify 802.1X Switches	RADIUS clients	wlan1 wlan2 wlan3
Configure an Authentication Method	NPS Server Certificate EAP Types:	NPSPALVELIN NPS-varmenne Secure Password (PEAP-MS-CHAP v2) Valittuna
Speficy User Groups	Groups	Add…
		EPK_koneet_KENPS_US
Configure Traffic Controls	Full access network	Katso teksti alapuolella

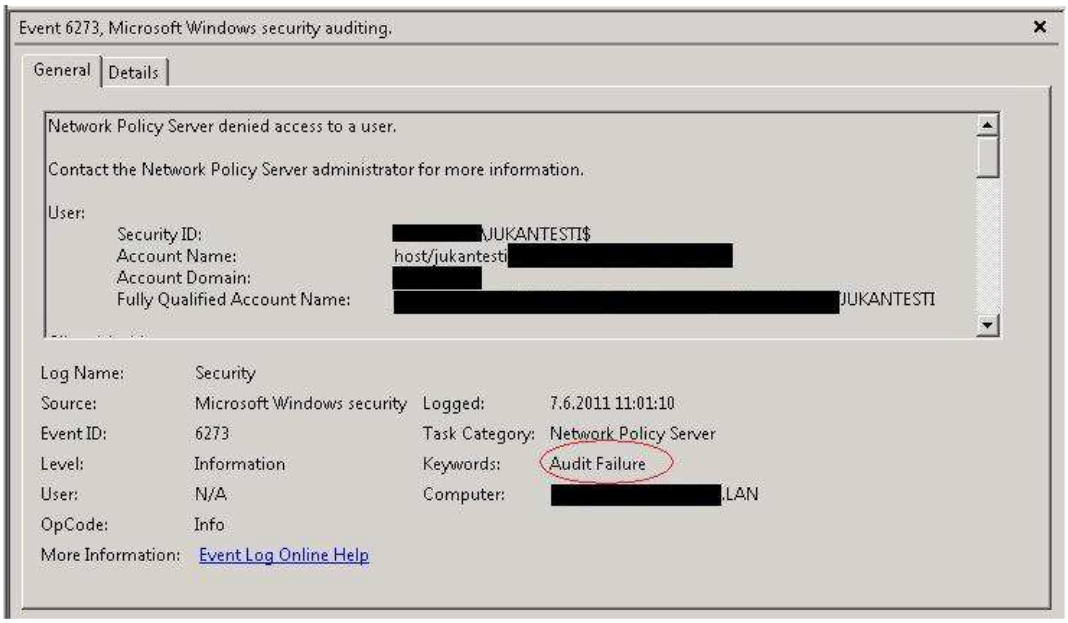
Tässä kohdassa kerron mitkä asetukset valitsin kohtaan Configure Traffic Controls - Full access network:

Napsautin hiirellä Full Access network kohdasta Configure, jonka jälkeen valitsin RADIUS Standard Attributes – välilehdeltä Tunnel-Type ja Edit. Attribute Information – ikkunassa painoin Add, ja valitsin seuraavan asetuksen: Commonly used for 802.1x alta Virtual LANs (VLAN). Tämän jälkeen suljin ikkunan painamalla OK.

Seuraavaksi muokkasin Radius Standard Attributes – välilehdellä olevaa Tunnell-Medium-Type -asetusta. Attribute Information – ikkunassa klikkasin Add ja valitsin asetuksen Commonly used for 802.1x alta 802 (includes all 802 media plus Ethernet canonical format) ja suljin ikkunan klikkaamalla OK-painiketta. RADIUS Standard Attributes – välilehdeltä valitsin Tunnel-Pvt-Group-ID ja Edit. Attribute Information – ikkunasta Add ja valitsin Enter the attribute value in: alta String ja määritin arvoksi 124. Tämän jälkeen suljin ikkunan klikkaamalla OK. Configure RADIUS Attributes – ikkunassa siirryin Vendor-Specific Attributes –välilehdelle jossa painoin Add. Vendor alasvetovalikosta valitsin Custom ja Attributes kohdasta Tunnel-Tag. Ja lopuksi painoin taas kerran Add. Attribute value –kenttään laitoin arvoksi 1 ja painoin OK. Lopuksi suljin Add Vendor Specific Attribute –ikkunan klikkaamalla Close ja Configure RADIUS Attributes –ikkunan klikkaamalla OK.

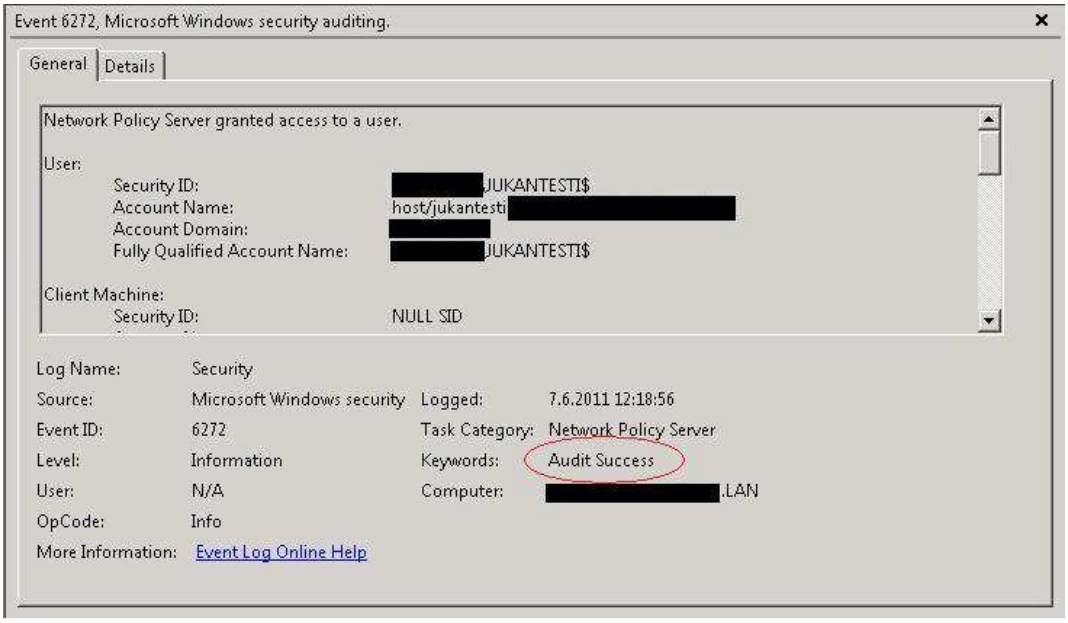
5 TYÖN TULOKSET

NPS-palvelimen toimivuutta testasin kannettavalla tietokoneella. Ensin en liittänyt kyseistä konetta oikeaan tietoturvaryhmään, jolloin koneella ei ollut pääsyä eduker245 verkkoon. Alla oleva kuva on otettu palvelimen lokitiedostosta.



Kuva 4 Ei toimi

Kun olin lisännyt koneen oikeaan tietoturvaryhmään, verkkoyhteys toimi normaalisti, kuten alla olevasta kuvasta näkyy.



Kuva 5 Toimii

Työssäni kohtasin monta eri ongelmaa, johtuen mm. siitä, että NPS-palvelin asennettiin jo olemassa olevaan verkkoon. Ensimmäinen ongelma oli se, että NPS ei osannut käyttää olemassa olevaa DHCP:tä sotkematta ko. VLANin IP-osoitteita. Tästä ongelmasta päästiin eroon luomalla omat VLANit NPS-palvelua varten.

Toinen ongelma oli tiedon puute. Yritin etsiä Internetistä sekä kirjallisuudesta tietoa tähän aiheeseen mutta en löytänyt mitään luotettavaa tietolähdettä aiheesta, yleensä tietolähteet olivat ristiriidassa keskenään tai sitten ne osoittautuivat toisensa kopioiksi jostain täysin toimimattomasta työstä eikä niillä ollut mitään tekemistä todellisuuden kanssa. Luin läpi muutaman opinnäytetyön koskien NPS-palvelua, mutta koska kyseiset työt oli tehty testilaboratoriossa eikä valmiissa ympäristössä niin niistä ei ollut paljoa apua. Eli saatavilla olevat tiedot olivat lähinnä teoreettisia.

Työskentely eri kehitystiimien sekä henkilöiden kanssa ei ollut aivan mutkatonta. Esimerkkinä voisi mainita sen, että eräs tärkeä henkilö verkkopuolen työryhmässä tekee etätöitä toisella puolella maapalloa, joten häntä ei aina saanut kiinni heti tarvittaessa.

LÄHTEET

McIllece James and Somohano Scott (2008), Network Policy Server (NPS) Operation Guide,

KYTKIMEN AAA- JA RADIUS-ASETUKSET

```
! Käynnistetään AAA
Switch(config)#aaa new-model

! Poistetaan Radius autentikointi kytkimen hallintayhteyksiltä
Switch(config)#aaa authentication login default none

! Konfiguroidaan 802.1x käyttämään AAA autentikointia radiuksella
Switch(config)#aaa authentication dot1x default group radius

! Konfiguroidaan dynaaminen VLAN-konfigurointi mahdollisuus radiukselta
Switch(config)#aaa authorization network default group radius

! Konfiguroidaan 802.1x istuntojen alkamis ja päättymis aika Radiukselle
Switch(config)# aaa authentication dot1x default group radius

! Konfiguroidaan tieto käytettävästä Radius-palvelimesta ja sen avaimesta
radius-server host 10.48.66.102 key kerava
```

KYTKIMEN PORTTIASETUKSET

```
! Konfiguroidaan kytkimen portti Access-tilaan
Switch(config-if)#switchport mode access

! Konfiguroidaan kytkimen portti kiinteästi Hallinto-VLANiin x
Switch(config-if)#switchport access vlan x

! Konfiguroidaan 802.1x autentikointi ko portissa aktiiviseksi
Switch(config-if)#dot1x port-control auto

! Konfiguroidaan Vieras-VLANiksi esim VLAN 2
Switch(config-if)#dot1x guest-vlan 2

! Käynnistetään 802.1x autentikointi kytkimen globaalitasolla
Switch(config)#dot1x system-auth-control
```